Bitcoin: A Reader's Guide (The Beauty of the Very Idea)

Frances Ferguson

There are many accounts of the history of Bitcoin and many predictions of its future. Some commentators report its imminent demise—others point to its latest uptick in price. The writing I read on Bitcoin, excellent though much of it is, increased my desire to understand it. This essay is a report on my effort to puzzle out this financial innovation, the extent to which it is an innovation, and the extent to which it has political implications.

Most accounts of money talk about it as a byproduct of social interactions that have become highly elaborated over time, elaborated enough for money to be so efficient as a token of trust that we accept paper currency from strangers and temporarily hand over credit cards to other strangers without interrogating them or being interrogated. The blockchain-Bitcoin combination, by contrast, is an attempt to launch a monetary system that sees itself as replacing older mechanisms for storing societal trust. It aims to build a language from the ground up. For that reason Bitcoin can seem too large a project to comprehend. It can be a surrogate for a committed embrace of an increasingly technologized future. It can look, as it does to Paul Krugman and Nuriel Roubini, like smoke and mirrors.[1]

This essay is based on desultory reading about Bitcoin and more concentrated reading in April, May, and June of 2019. I am grateful to Peter de Bolla, John Naughton, Christopher Prendergast, Tim Griffin, W. J. T. Mitchell, Orit Bashkin, Bill Brown, Elizabeth Helsinger, Heather Keenleyside, and Françoise Meltzer for discussing an earlier version of this essay with me, and I'm particularly grateful to Patrick Jagoda for having prompted me to write it.

[1] Paul Krugman cites Robert Shiller's observation that "asset bubbles are like 'naturally occurring Ponzi schemes'" (Paul Krugman, "Bubble, Bubble, Fraud and Trouble," *New York Times*, 29 Jan. 2018, www.nytimes.com/2018/01/29/opinion/bitcoin-bubble-fraud.html). See also Leonid Bershidsky, "Dr. Doom v. Mr. Ethereum: Crypto Pitts Economists against Engineers," *Bloomberg*, 12 Oct. 2018, www.bloomberg.com/opinion/articles/2018-10-12/roubini-v-buterin-crypto-pits-economists-against-engineers

While the scale of Bitcoin's stated ambitions can be daunting, what you might call the Bitcoin archive presents another challenge to understanding. It's very hard to know what to trust. Andrew O'Hagan has written well about this issue. He was once recruited to write a book on Craig Wright, who claimed to have developed the blockchain-Bitcoin model under the pseudonym Satoshi Nakamoto, a pseudonym that may also have housed the identity of a collaborator. O'Hagan interviewed Wright extensively and was present for an event that promised to be the big reveal, the occasion on which Wright would sign with the private key for one of Nakamoto's original blocks in the blockchain and would thus confirm that he and Nakamoto were one and the same. The event ended when Wright signed with a key that only fleetingly looked like the real thing, and that turned out to be a reengineered version of an alphanumeric string available on the internet. The entire project, which revolved around O'Hagan's writing a history of an invention and an inventor, dissipated into almost nothing when Wright was unable to establish that he was Nakamoto. It was as if Steve Jobs had not been able to show that he was Steve Jobs, leaving all would-be biographers in the lurch.

O'Hagan concluded after much labor that the story eluded the tools of journalism. "A reporter," he wrote, "was once a person who could rely on visible evidence, recordings, notes, statements of fact, and I gathered these assiduously, but this was a story that challenged the foundations on which reporting depends."[2] Why, O'Hagan wondered, would someone work with various lawyers, as Wright had done, to recruit O'Hagan to write a business biography if he ultimately wouldn't claim the identity that he had said was his? Why, O'Hagan wondered again, would Wright continue to claim to be Nakamoto (or a portion of him) even after Wright failed to reveal himself and establish his identity?[3] For that's what Wright did immediately after the abortive reveal; he posted on his blog that he had scrubbed the reveal

[2] Andrew O'Hagan, "The Satoshi Affair," *London Review of Books*, 30 Jun. 2016, www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair

[3] O'Hagan's association with Wright began in 2015, and the abortive reveal took place in 2016. Wright has, however, recently renewed his claim to be Nakamoto. At the time of this writing his claim is being actively disputed by John McAfee, a security software developer and self-described great hacker, who affirms that he has identified the real Nakamoto and that Wright is not he.

Frances Ferguson is the Ann L. and Lawrence B. Buttenwieser Professor in the Department of English at the University of Chicago. Her most recent book is *Pornography, the Theory: What Utilitarianism Did to Action* (2005). She is also a coeditor of *Critical Inquiry*.

because authorities in the UK wanted to question him about the use of Bitcoin for weapons purchases by terrorists. That explanation, however, seemed maddeningly incomplete. Had he only suddenly, just now, realized that the authorities might want to raise such questions when they had presumably been hovering throughout the entire time that Wright was talking with O'Hagan and the lawyers who were promoting the biography? Didn't he realize that his blog post would not exactly end the authorities' interest in him? The Cretan liar paradox here confronts real life or real journalistic life. And only recently the story has taken yet another turn. Wright has publicly renewed his claims to Nakamoto's identity, and various members of the cryptocurrency world have disputed them.

Moreover, there are problems with the blockchain-Bitcoin archive that extend past Craig Wright and his intermittent desire to identify himself as Nakamoto. There is a great deal written, much of it on websites that I, at least, don't know how to evaluate. The *Bloomberg* site, the *New York Times*, and others seem straightforward in reporting what the journalists know and what they don't. Some other sites, however, seem so partisan that it's hard to credit the *a*, *an*, and *the* of their reporting (as Mary McCarthy said of Lillian Hellman: she lies even when she uses articles). I gave up trying to canvas more sites when a pornographic site suddenly appeared on my screen, and I realized that one of the sites I had checked was less interested in purveying Bitcoin news than in making referrals. I had stumbled into troll land.

This essay is the record of my attempt to work through to an understanding of how the blockchain and Bitcoin work. It is also a modest effort in thinking about the experience of reading the news. I try to report on descriptions of Bitcoin and then particularly on how some members of the Bitcoin culture talk of it, around it, and to it. As Benedict Anderson has argued, journalism links people into a virtual community even when they have no direct connections with one another. That community distributes its attention very unequally, but it is increasingly global. Journalism continually reminds us of our membership in that global community. And it also enjoins us to think as if we were legislators, developing positions and acting or recommending them. Reading the news is an exercise in evaluating the constant stream of policy proposals that the world offers up to us on a daily basis: to take or not to take dietary supplements; to use or avoid a particular brand of sunscreen; to accept a plastic takeout container or shun it.

The blockchain is a distributed public ledger, a way of keeping a record of transactions that would be public in its very creation. Individual firms and corporations maintain records on their own transactions, publish statements on their financial situation, and make their financial records available for audit. The blockchain is, by contrast, born public. It crosses corporate and individual boundaries. Bitcoin is the currency that is complementary to blockchain, what can be spent and what can be earned in relation to blockchain. (There are now multiple blockchains and scores upon scores of cryptocurrencies related to them. Late in this essay I will touch on the relationship between Bitcoin and other cryptocurrencies, but for the moment I focus on Bitcoin as the original cryptocurrency.)

The blockchain and Bitcoin offer particularly striking ways of addressing ambiguity. The blockchain aims to eliminate ambiguity by focusing on individual transactions. It records them as unique events arranged merely by their place in an unfolding and unalterable sequence. It provides what Donald MacKenzie has aptly described as "a single version of history."[4] Blockchain makes the transaction rather than the person the central unit of identity and in the process eliminates ambiguity by not extending it in time. Bitcoin reintroduces that ambiguity. The renewed ambiguity stems in part from the way that personal identity is shrouded in the first instance, appearing in the form of an address that is tied to a proper name only when needed. The Bitcoin view is that beginning with the declaration of a name, as most of us do when we introduce ourselves, and presenting driver's licenses and passports to confirm it, is entirely the wrong place to start. As Wright said to O'Hagan on 16 December 2015, "Where we are . . . is a place where people can be private and part of that privacy is to be someone other than who they were."[5] Continuous personal identity over time, from this standpoint, is treated as if it were an onerous reporting requirement introduced by national governments and an impediment to personal growth.

Ambiguity, moreover, reappears in one particularly striking form: it is unclear that anyone knows how many functioning Bitcoins there are in the world. Homicide detectives and crime novelists have a term of art, *ambiguous loss*, that applies in a situation in which they are convinced that a murder has taken place even though no body has been found.[6] The relevance of that notion to the blockchain-Bitcoin world became apparent when observers started noticing Nakamoto's silence. Many have presumed that Nakamoto is dead because no messages have gone out from his account in recent years

[4] Donald MacKenzie, "Pick a Nonce and Try a Hash," *London Review of Books*, 18 Apr. 2019, www.lrb.co.uk/v41/n08/donald-mackenzie/pick-a-nonce-and-try-a-hash; hereafter abbreviated "P."

[5] Quoted in O'Hagan, "The Satoshi Affair."

[6] A brief search informs me that most of the current writing about ambiguous loss focuses on the problem that mourners face when they assume the death of a loved one but don't know for a fact that it has occurred. The detective fiction writer Fred Vargas is, I believe, the person whose work introduced me to the homicide detective's use of the phrase.

and none of the nearly one million Bitcoins he is thought to have amassed have moved in ten years. The ambiguity introduced by the claim that Nakamoto might be a pseudonym for various people is one thing—it's hard to mourn a pseudonymous existence. But the link between personal identity and Bitcoin ownership is another. While people make statements about the size of what Olga Kharif calls "the entire circulating supply," the notion of "the entire circulating supply" is clearly highly elastic. Were someone who had been presumed dead to reappear Robinson Crusoe-like and sell substantial quantities of coins, the supply would increase drastically. (Kharif reports that Nakamoto's account holds "nearly 1 million" Bitcoins, out of approximately 17.6 million coins.)[7]

The blockchain is an open distributed ledger, what Satoshi Nakamoto identified as a "'peer-to-peer electronic cash system.'" It provides not just a history in the way that all ledgers do for their particular niches of commerce, but that "single version of history" that MacKenzie has spoken of ("P"). The cleverness of the blockchain is that it never collects things and tries to sort them. It does not adopt a clearing house model in which payments are amassed and need to be directed. It does not worry about where things belong, where they might be arranged and classified, put into folders. It can take all the elements of Jorge Luis Borges's Chinese encyclopedia and simply report the transactions governing them in sequence, observing only chronological order. One might be tempted to say that in this respect it simply does what the reports on trades on the London Stock Exchange, the New York Stock Exchange, or the Chicago Board of Trade do. But the blockchain does not restrict its reports to transactions in the commercial markets. A short message commenting on the blockchain, *Ulysses*, and game tokens picked up in playing the *World of Warcraft* can all equally be assigned a name, which for all its being a name is expressed in strings of letters and numbers. The old worries about ambiguity in language that arose as soon as one tried to hold a name to a particular person or thing over time disappear in the blockchain because the chain represents transactional identity, a series of names for the things governed by transactions. The identity of the things—the objects of possession, the goods, the services being exchanged—no longer rests on continuing existence.[8] The name, that string of numbers, is a time-and-date stamp, and the exchange of something—information, a currency, a service, real estate—at a particular moment constitutes its baptism.

[7] Olga Kharif, "John McAfee Vows to Unmask Crypto's Satoshi Nakamoto, Then Backs Off," *Bloomberg*, 23 Apr. 2019, www.bloomberg.com/news/articles/2019-04-23/john-mcafee-vows-to-unmask-crypto-s-satoshi-nakamoto-within-days

[8] This is part of what Warren Buffett means when he says that there's no product in blockchain.

The uniqueness of each transaction makes it possible to establish possessive claim more efficiently than the naming practices of our ordinary language and even our ordinary legal language. Ordinary conversation has us continually losing track of exactly which proper name should be attached to a particular pronoun and needing to sort out what you mean by *she* or *he*. Legal contracts resort to merism, the multiplication of synonyms and near synonyms, as if to use so many different names for descriptors or persons or things that some one of them must be seen to apply.

For individual users of the blockchain, transactional uniqueness makes it particularly easy to mark possession (the control of money, the ownership of debt). And it is this feature of the blockchain, its ability to record transactions publicly and indelibly, that has attracted the attention of a range of businesses, from food suppliers to art dealers. It promises to improve food safety by making it easy to trace food-borne illness back to a particular supplier. It thus interests a corporation like Walmart that sells foodstuffs on a massive scale because it would give them something new to sell, an improved level of food safety—always desirable in a world that is regularly described as toxic. And it interests art galleries for promising a permanent record; it can create an unalterable birth certificate and record of transmission for a work of art. It would seem to eliminate the possibility of art forgeries of the kind that forced the Knoedler Gallery in New York to close when it turned out that they had sold paintings represented as Jackson Pollock's that were discovered to be forgeries. Moreover, it would eliminate the need to rely on individuals to vouch for the authenticity of a work of art after the fact. No one would need, as art collectors once did, to call on a scholar like Bernard Berenson to attribute a painting. It would no longer be a problem for art dealers that contemporary scholars are increasingly reluctant to vouch for a work of art and to put their personal credibility at risk in the process.

At first blush, the peer-to-peer version of electronic cash might look simply like a way of eliminating the middle man, a way of putting parties to a transaction into direct communication with one another without any need for third-party mediation. That is certainly a key element of its self-description. But the blockchain-Bitcoin model is distinctive in the sweepingness of its claim to eliminate the need for trust—by which Nakamoto seems to have meant the need for demonstrations of trust outside the particular transaction. Being open, distributed, and unalterable, the ledger would, in theory, provide no openings for what Jeremy Bentham called "sinister interest."[9] The idea was to design a machine that would run itself and a machine that would replace

[9] See Philip Schofield, *Utility and Democracy: The Political Thought of Jeremy Bentham* (New York, 2009), esp. pp. 117–40, 344–49.

things like constitutions that had sometimes also been described in such mechanical terms. It would allow for "the possibility for small casual transactions" that did not present any occasion for a merchant to ask for a driver's license or a passport.[10] It would eliminate the need for banks to vouch for the reliability of their customers' proposed transactions, the need for credit bureaus to collect and confirm information about someone's credit worthiness, and the need for central banks to stand behind the transactions of banks, corporations, and the like.

Nakamoto's prospectus-cum-manifesto made clear how sweeping the aim of eliminating the need for trust was. For the real target of the white paper "Bitcoin: A Peer-to-Peer Electronic System" was the notion of mediation itself, the fact that the monetary system relies on trusted third parties acting as intermediaries to prevent fraud. Financial institutions, Nakamoto insisted, traffic in trust every time they approve purchases up to the limit on one's credit card or line of credit and thus vouch for the financial reliability of a purchaser. But he branded this version of trust costly and inefficient. "The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility of small casual transactions. . . . With the possibility of reversal [of transactions], the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need."[11] Even organizations such as Uber and Lyft and rental arrangements like Airbnb and FRBO (For Rent By Owner) are trust intermediaries from the standpoint of the Nakamoto model. While they may reduce transaction costs by comparison with car rental companies and hotel chains, they are still in the business of marketing trust by effectively vouching for riders and drivers, assuring that riders will pay and drivers will actually deliver passengers to their destinations and that renters will pay property-owners and property-owners will supply lodging for short-term renters.

The blockchain, as a single version of history and a distributed public ledger, aimed to verify and document transactions so accurately that it dispensed with the need for humans to exercise trust in their relations with other humans. By making the ledger speak directly to the Bitcoin addresses of account holders, it eliminated the credit report and the delays and possibilities for error that it might introduce. But the ledger could not run itself. It depended on labor, and it had to figure out how to get that labor without setting up a human relations department with all the reference

[10] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org /bitcoin.pdf

[11] Nakamoto, "Bitcoin."

checking that would replay the problem of mediation that it wanted to avoid. The ledger, moreover, could not rely on ordinary crowdsourcing of the kind that Wikipedia and reviewing sites regularly use because those reintroduced the ambiguity of multiple histories that the blockchain was eager to eliminate.

The solution to the labor problem was to rely on a virtual army of volunteers and to make the work game-like and reward directed. The solution was, that is, to offer rewards with as little semantic content as possible. As MacKenzie more neutrally put it, "the software system offers the prospect of rewards, in the form of bitcoin, as an incentive to users to have their computers continuously check the validity of bitcoin transactions, pack them into an evolving public record . . . and check other users' additions to the record" ("P").

Thanks to Bitcoin, the reward for the work of competing to maintain the ledger, the ledger is, in MacKenzie's concise description: "a near-immutable, fully consensual record without a central record-keeper" ("P"). The workers who maintain it race to solve a mathematical puzzle that provides a unique identification number for each transaction. They collaborate by competing. Although it is a competition at mathematics and might thus look like work for the math averse, maintaining the ledger is essentially a game. As with games, there are first-place finishers, who win Bitcoin, and there are losers, all those who try and fail to win the mathematical footrace that confirms a transaction and assigns it a new, unique number/name.

The blockchain's reliance on a game structure initially allowed it to look autotelic. The point of the ledger was to produce the ledger—its very existence seeming to eliminate the need to do anything more about it. In the beginning, the value of Bitcoins was negligible. They were not worth much more than tokens at a Chuck E. Cheese restaurant. The ledger looked as though it minimized disputes over pride of place by veiling the identities of its wallet holders. A bridge tournament or a tennis match might declare cumulative winners, hand out special prizes, and offer the temporary rush of identity enhancement that such an award might bring. The blockchain-Bitcoin ledger didn't. It did not collect its own history and report on it; it merely reopened continually new competitions among the players.

The game-like structure of the blockchain-Bitcoin ledger was initially very important. Even when Bitcoins carried almost no value, they attracted worker players under the customs that attach to games—and particularly the custom that we didn't once expect the rewards assigned in games to have any value outside the game. The virtual value of scores in games was for centuries a major part of their appeal. It was a conspicuously fictional value: fictional in that it didn't lay direct claim to otherwise recognized actualities, and fictional in that it was a made thing. It was value that was recognizable and conspicuous even though it never broke free from the context of the game, except when it was delivered to particular individuals in the form of a bridge trophy or a most-valuable-player award.

In both the digital world and the nondigital world most people who play games were accustomed to think of the prizes they won for outstanding performance as merely symbolic tokens that would never be anything other than symbolic. Many continue to function in that way. The trophy that a twelve-year-old receives for being the best player on her or his football team is a paradigmatic example of sentimental value. Only the possessor would pay anything for it. But recognizing the motivational power of such prizes has been a central insight of various social organizations over at least the past two centuries. Joseph Lancaster's monitorial schools of the early nineteenth century took advantage of the game-and-prize model when they aimed to have only one schoolmaster supervising as many as a thousand pupils. His schools minimized the need for centralized oversight and an army of teachers by organizing classrooms as so many small-scale games and creating an economy of prizes—usually engravings cut out of cast-off books. These games and their prizes rewarded the students and made them one another's teachers in the process.[12] Organizations such as the Boy Scouts went even further in thinking about the place of rewards in such systems: not only did/do scouts work for the symbolic reward of a badge, they also paid/pay for their badges and uniforms and pay to be allowed to claim and assert their accomplishment and make it walk around in the world.

The blockchain began with all the logical simplicity of counting. But then necessity took over. The survival of the blockchain depended on labor. And what had been volunteer labor needed to become reliable. Bitcoin, for its survival as an incentive, needed for that labor to have an actual rather than merely virtual value. Bitcoin had to develop into an economy that would speak to actual existent economies. And it needed to do this more thoroughly than loyalty programs do. It would not be enough to point out that someone could buy a set of tableware for either two complete books of S&H Green Stamps or forty dollars or that it was easy to translate frequent-flyer miles into some equivalents of US dollars or UK pounds.

It was only in 2012, some three years after the Nakamoto prospectus, that various computer games began directly awarding Bitcoin to players, but one key to Bitcoin's relative success is that it has seen the possibilities for directly trafficking in a market for rewards that once had only symbolic value, value within a particular game. Brock Pierce, someone who has been highly

[12] See Joseph Lancaster, *Improvements in Education* (London, 1807).

prominent in the Bitcoin world, monetized *World of Warcraft* rewards such as eight-piece suits of Skyshatter chain mail, selling these bundles of fiction and code on eBay. He recognized the value of simultaneous scarcity—that Skyshatter chain mail is a rare prize—and he also recognized the value of its being plentiful enough for people to imagine that they too could want it, buy it, and come to own it. Virtual currency no longer looked like currency trapped in a game, as it does in a game like Monopoly. Having a market, it became a commodity. It was now worth what other players were willing to pay because it could move out of one player's game and back into another's. Hiring numbers of expert low-wage Chinese players to create and supply demand, Pierce established a virtual factory, a small-scale industry of game rewards.

The importance of the labor of individual game players has diminished with the advent of computer chips that are already programmed to perform the lengthy calculations necessary for confirming the uniqueness of blockchain-Bitcoin transactions. Computers themselves now largely provide the labor necessary to maintain the blockchain—requiring only enormous amounts of energy to continue to show up at the factory gate (as much as all of Ireland, as much as several states in the US combined) (see "P"). But the link between online gaming and blockchain Bitcoin has been important for showing how a game might be more than a vendible product and might, in throwing off rewards, produce more monetary value. Games began to pay for themselves—and then some.

The thing that attracted Bentham to Lancaster's monitorial model was that it effectively capitalized the students by awarding them what he called "proportionable shares of general respect," in the form of prizes for having performed best on a particular test.[13] In the spelling-bee model that Lancaster's monitorial schools featured, it's possible to discern, in miniature and in face-to-face interaction, a version of the open and public nature of the blockchain-Bitcoin process. The schools handled the problem of trust by bringing the entire question-and-answer scheme into visibility; all the participants were able to see at every moment when any one participant correctly spelled a word or completed a math problem or failed in the attempt. But the field in which it operated was restricted. Lancaster's monitorial school aimed to equip students with the ability to tap their own resources in extramural activities, not to sell their positions at a particular moment in the ongoing examination.[14]

[13] Jeremy Bentham, *Chrestomathia*, ed. M. J. Smith and W. H. Burston, vol. 7 of *The Collected Works of Jeremy Bentham*, ed. Schofield (New York, 1983), p. 19.

[14] For an account of a nearly applicable account of game principles to education, see the introduction to Frances Ferguson, *Pornography, the Theory: What Utilitarianism Did to Action* (Chicago, 2004), pp. 1–33. For recent important work on the permeability of games and the

The buying and selling of digital rewards won in games like *World of Warcraft* and *Second Life* was controversial. At least one player of *World of Warcraft* brought suit, complaining that digital sales of in-game prizes were "'substantially impairing' . . . [players'] enjoyment."[15] And for good reason. At least one pleasure of playing a game is to demonstrate one's own activity to oneself and others, to put oneself in a position to judge it. The pleasure of buying assistance in a game is a lesser pleasure (a statement one doesn't need John Stuart Mill's account of higher and lower pleasures to make). And the pleasure of seeing others buy assistance into a game even less than that.

Nakamoto initially thought of himself/themselves as eliminating worries about trust by setting up the ledger as a perfect history, but the sale of game trophies made it clear that the problem of trust had simply relocated itself. The transaction—the sale of the game trophy from one party to another—may be verified as unique and documented in the blockchain. It is, however, within the transaction that the issue of trust becomes particularly vexed.

Discussions of blockchain and Bitcoin have a tendency to rehearse the story of money and to point out that all money is fiat money. That is, currency is not exchanged because it is valuable in and of itself but rather because someone may offer it as valuable and someone else will accept it as valuable. Money is a social product. Various libertarians in the US inveigh against the fiat money of national governments, which they see as money brought into being by the say-so of national governments and effectively manipulated and exploited through central national reserves. But even so conservative an economist as Milton Friedman is regularly cited for his illustration of the fiat character of money: the island of Pau, which took stone only available on another island as the notional support for its currency (so that it could not be counterfeited—that is, duplicated) and allowed exchanges to be made in relation to portions of this stone even when the stone was entirely physically unavailable, irretrievable at the bottom of the ocean. Friedman essentially described Pau as an economy operating on a ledger, that for all that it was notionally connected with the stone, was as much a product of social value as any. Only by imagining that the society of Pau hadn't actually developed social institutions that would give it the capacity to keep a ledger could one imagine that it didn't have fiat money.[16]

nongame world, see David Golumbia, "Games without Play," *New Literary History* 40 (Winter 2009): 179–204, and Patrick Jagoda, "Gamification and Other Forms of Play," *boundary 2* 40 (Summer 2013): 113–44.

[15] Julian Dibbel, "The Decline and Fall of an Ultra Rich Online Gaming Empire," *Wired*, 24 Nov. 2008, www.wired.com/2008/11/ff-ige/

[16] See John Lanchester, *How to Speak Money: What the Money People Say—And What It Really Means* (New York, 2014).

The libertarian claim about fiat money seems ultimately to be that there is something inherently suspect about currency that has the backing of a government. Libertarian cryptocurrency partisans see banks, which tend to think of themselves as extragovernmental, as governmental subsidiaries, part of a system designed to compel participation in the money of the particular government. They see the requirement that one use a national currency within particular national boundaries as an involuntary tax and coercive. The libertarian continually questions whether an individual should pay the costs associated with that use. The libertarian instead points to the value of the population that Bitcoin is able to muster for its communications and its transactions, its ability to deliver people who will pay for virtual goods like a full set of Skyshatter chain mail. That is, to value the virtual currency over the national currency announced and supported by national institutions.

Or rather, to put it into competition with that currency by posing challenges to the accumulated value that national governmental institutions and the networks of corporations, trusts, universities, and the like have built up over time and that they continually distribute to individuals. For the conjuring trick that translates game gold into money operates as a way of casting suspicion on longer-standing and slower-moving institutions and organizations and the legitimacy of their ways of confirming and distributing value. In the terms of the Bitcoin manifesto, the Federal Reserve and the US Government are to be criticized for having propped up destabilized banks, insurers, and automakers in the financial upheaval of 2008. And institutions like universities, in the libertarian account, offer education as a prize ultimately no more substantial and worthy of acknowledgement than so much Skyshatter chain mail. A degree from a prestigious university looks, from this perspective, merely like a prestige hack, a reward less for accomplishment than for money.

Bitcoin promotes jurisdictional disputes and pits evaluation systems against one another. Bitcoin users are, among other things, currency traders, continually weighing the merits of one currency against another. And while national currencies have mainly had value in specific geographical areas, Bitcoin extends beyond any one national currency zone. If I can find someone to take my Bitcoin, I need never be confined to any national currency. Thus, one Bitcoin user writes an op-ed for the *New York Times* to testify that it is only his ability to spend Bitcoin that keeps him and his family supplied with bread and other essential products in the wake of rampant inflation in Venezuela.[17] Even if the Bitcoin he is spending is worth substantially less than it was at its high of nearly twenty thousand dollars at the end of 2017, it

[17] Carlos Hernández, "Bitcoin Has Saved My Family," *New York Times*, 23 Feb. 2019, www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html

has held buying power more efficiently than the Venezuelan bolivar. Most Americans can't imagine why they would use Bitcoin to buy a loaf of bread, because the transaction costs are higher than for using a credit card or cash. But for anyone with a reason to avoid holding cash in US dollars, Bitcoin offers a gray alternative to both those dollars and the black market. A company called Cottonwood runs ATMs that charge a mere nineteen percent to convert cash into Bitcoin, a savings over the thirty percent that is said to be the going rate in extra-legal currency markets.

The Venezuelan op-ed author represents himself as someone whose use of Bitcoin constitutes an implicit rebuke to the Venezuelan government and its inability to maintain a working monetary system. Money launderers typically don't represent their problems with the national government so explicitly. They don't typically flaunt their disapproval of their government but are usually content to remain relatively quiet, in the knowledge that their government disapproves of them. Both the Venezuelan and the money launderer, however, are engaged in direct renegotiation of their relationship with the governments of the countries in which they live. David Golumbia has written extensively on the civil libertarian view of money. He has in the process identified a politico-economic genealogy for Bitcoin partisans in the John Birch Society and has attached names—those of the Koch brothers, Ron Paul, Rand Paul, and others—to the anonymized transactions of Bitcoin. In the process he has expressed both astonishment and frustration that many continue to imagine that they could simply do away with governmental institutions like central banks and government-backed institutions like commercial banks and still have a functioning economy. In his view, libertarians imagine that regulation is a tax that one ought to be able to choose not to pay—that one ought to be able to be, in effect, persons without a country—what Steve Bannon called "these rootless white males [who] had monster power" when he described the Bitcoin anarchists he worked with when he headed Internet Gaming Entertainment.[18]

In 2013 Evan Soltas described Bitcoin as "an existential threat to the modern liberal state." "If widely adopted," he observed, "cryptocurrencies would cripple a government's three central functions: taxation, police, and macroeconomic stabilization."[19] The policing that underwrites the rule of

[18] Quoted in Neil Strauss, "Brock Pierce: The Hippie King of Cryptocurrency," *Rolling Stone*, 26 Jul. 2018, www.rollingstone.com/culture/culture-features/brock-pierce-hippie-king-of-cryptocurrency-700213/; hereafter abbreviated "BP." See also Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism* (Minneapolis, 2016).

[19] Evan Soltas, "Bitcoin Really Is an Existential Threat to the Modern Liberal State," *Bloomberg*, 5 Apr. 2013, www.bloomberg.com/opinion/articles/2013-04-05/bitcoin-really-is-an-existential-threat-to-the-modern-liberal-state

law is made more difficult and more costly because the anonymized ledger does not flag very substantial transactions in the way that nationally recognized banks are required to do. Suspicious money moves through Bitcoin noiselessly; it must leave tracks of other kinds to trigger investigation. At the same time, Bitcoin's tax-avoidance measures make policing an unfunded mandate.

So far, I've been describing Bitcoin from the outside. But I'd like to shift now to talk about how Bitcoin talks to itself and among itself.

The controversy that has recently reignited over Nakamoto's identity is a particularly interesting one: there are now two candidates, one of whom continues to be reluctant. Wright, who did not confirm his Nakamoto identity in 2015 but did not deny it either, is now claiming to take it up. John McAfee, who developed McAfee antivirus software, is disputing Wright's claim, saying that he, McAfee, has identified the real Nakamoto—alive, well, living in the US—and unhappy that McAfee has tracked him down.

I don't have a candidate for the post of Nakamoto. Instead, I want to pose a question: Why would someone not be happy to be Nakamoto, someone who may not have traded for a number of years but who might, if alive, control nearly one million Bitcoins? The answer has everything to do with such things as the rule of law and the police function of the state. As Kharif has reported, a number of people have speculated that the title looks more dangerous than rewarding. As of 8 May 2019, there were said to be 17,687, 562.50 Bitcoins in existence, so that a living Nakamoto would hold more than 5.5 percent of the extant supply. And in controlling such a substantial fraction of the total stock of Bitcoins, a Satoshi Nakamoto who suddenly reentered the market could single-handedly drive down the price of Bitcoin. Exposing Nakamoto as an individual controlling an enormous portion of the market would expose how much the presumption of Nakamoto's death has meant to that market.

For the Bitcoin market has not merely made a point of emphasizing that Bitcoin mining would end when the twenty-one millionth Bitcoin was mined. It has also implicitly relied on the idea that a portion of that supply was continually being retired—by the fragility of the individuals holding their private keys. Individuals directly affect the circulating supply: with their deaths, their failures of memory, and their absent-minded housecleaning in which they send the wrong computer to the landfill. The initial veiling of identity in an alphanumeric string ends up putting extraordinary pressure on personal identity; someone needs to be able to remember how to collect one's identity.

Recently one commentator observed that Bitcoin is, in effect, cash. Such an assertion looks preposterous on the face of it, but of course it's perfectly accurate at bottom. Even if people are willing to pay Cottonwood's ATMs a nineteen percent fee to change their cash into Bitcoin, their individual possession of their private key ties them in their very physical being to their Bitcoin. Bitcoin lives in and through their persons and their working memories. Bitcoin is, in many respects, more cash-like than cash in that it evaporates with the death, dementia, of sheer distractedness of the holder of the private key and doesn't linger in the possibility that a new possessor will take it up.

The saga of the presumed death and possible return of Nakamoto—and the reveal that keeps being aborted or postponed—keeps pointing up a danger that Nakamoto never quite anticipated. The very necessity for him to be an individual continuing in life and functioning memory may have come to seem a Nessus's shirt, at least as much a liability as an asset. The considerable rise in the price of Bitcoin in late 2017 may have made this liability particularly apparent. If dead, Nakamoto is the patron saint of Bitcoin. If alive, he is one of the largest of whales. As an anonymous poster defined Bitcoin whales on the internet, whales are the one thousand people or hedge funds who own 40 percent of the market. As this digital lexicographer also said on 8 December 2017 before the price of Bitcoin reached its high of 19,783.06 dollars on 17 December 2017, "and they're becoming a worry. . . . They can send prices plummeting by selling even a portion of their holdings."[20]

The lexicographer may simply have written for the edification of the public. But Bitcoin and other cryptocurrencies have been slow to gain recognition from government regulators in part because their participants appear to speak simultaneously in the public language of social media ("I'm in; you come too") and in a private language. John Griffin and Amin Shams, a professor and a graduate student in the Finance Department of the University of Texas-Austin, have recently argued that the numbers in Bitcoin trades don't stand as far from ordinary speech as they do—and should do—in regulated markets. Griffin and Shams have noticed, for example, mutually offsetting matching transactions in Tether, transactions going out to many decimal places. Such transactions have struck their attention in part because of the probable cost of the transactions themselves (which may well have been as high as forty-two dollars each). And the transactions would also have been notable because regulated stock exchanges prohibit wash sales, sales in which one transaction immediately

[20] Kharif, "The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market," *Bloomberg*, 8 Dec. 2017, www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market

cancels out a previous one. Wash sales are prohibited because they function not as sales but as signals, as cues for sustaining or driving up prices. They are ways of talking without talking, speaking in public but to a private audience. For something like Bitcoin that, as Warren Buffett says, has no product, a wash sale looks very much like a moment in which the merely sequential iteration of transactions looks as though it is breaking into articulate speech. Griffin and Shams are suggesting that market manipulators are creating a language within a language, taking the rigidity of the merely alphanumerical language of the ledger and subjecting it to the semantics of human suggestion and command. And their work helps to bring out a theme in the narratives of people whose lives have been changed by Bitcoin.[21]

A man named Kristoffer Koch is the protagonist of one widely repeated story. In 2009 he bought five thousand Bitcoins for kroner worth a bit over twenty-five dollars and only remembered that he had them in April 2013, when they were worth about five million Norwegian kroner, just shy of nine hundred thousand dollars. The story rounded itself off in an entirely satisfying way. Koch used his newly located coins to buy a flat in a fancy neighborhood in Oslo. But wait—the news report also mentioned that it was only one-fifth of his coins that he sold. He cashed out, but he didn't cash out completely.[22]

Bitcoin stories tend to have this structure. They accumulate expectations of a big reveal or a big transaction and then retreat from it. One might think that Koch, suddenly remembering his Bitcoin after four years, would sell his entire holdings. But instead he continued to hold the remaining four thousand coins, as if he were confident of both Bitcoin's prospects for further growth and his memory. The Bitcoiner benefited enormously, on the one hand, and he also demonstrated his loyalty to Bitcoin by not liquidating his holdings.

Neil Strauss, profiling Brock Pierce for *Rolling Stone* in 2018, presented one spectacular example of a similar pattern of combining the display of newly minted wealth with loyalty to Bitcoin. Strauss opened by quoting Pierce: "'I've committed to give away everything I have'"—not later, in a will to be executed after his death, but now ("BP"). The story included various elements that give a sense of the scale of Pierce's wealth: he was ninth on the *Forbes* list of cryptocurrency billionaires as of late January 2018; he

[21] See John M. Griffin and Amin Shams, "Is Bitcoin Really Un-Tethered?" 13 June 2018, papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066

[22] See Samuel Gibbs, "Man Buys $27 of Bitcoin, Forgets about Them, Finds They're Now Worth $886k," *The Guardian*, 23 Oct. 2013, www.theguardian.com/technology/2015/dec/09/bitcoin-forgotten-currency-norway-oslo-home

moved to Puerto Rico in 2017 to shield his Bitcoin wealth from taxation after Puerto Rico passed the Individual Investors Act to create a tax haven for businesses and wealthy individuals; and living in Puerto Rico (for at least half the year) enabled him to avoid the tax laws that made Bitcoin transactions taxable events as of 1 January 2018. All of which point to his wealth and his interest in its maximal value.

Prices of Bitcoin were steadily climbing during the fall of 2017, reaching the aforementioned sum of 19,783.06 dollars on 17 December 2017. One might think that moving to a tax haven and seeing coin prices at a spectacular high would seem like reasons to sell. And the arrival of Hurricane Maria, which made landfall on Puerto Rico on 20 September 2017, would seem to have created one reason more. When, if not then, would it make sense to sell out and give all one's wealth to charity? But Strauss ended his profile of Pierce in *Rolling Stone* by saying that he hadn't been able to find any evidence of the charity's having come to pass: "As of this writing, it has been nine months since Pierce first mentioned giving away $1 billion, and there still hasn't been a white paper released or a penny given" ("BP").[23]

Plans change. But a recent interview on *Bloomberg* helps to bring the structure of the Bitcoin narrative into sharper relief. Antoni Trenchev, co-founder and managing partner of Nexo, described the launch of his Bitcoin-backed mortgage business and elaborated on the situation of the company's first customer. Pierce, Trenchev said, "borrowed from us to buy a house in Amsterdam" and is paying "between eight and sixteen per cent a year," "which is not crazy" in view of the volatility of Bitcoin. It's only crazy in view of another financial fact that Trenchev brought into view: the "extremely low interest rates" that he thanked "the Federal Reserve and the ECB" for maintaining. Nexo's client Pierce, Trenchev said, has ninety-five percent of his wealth in crypto, and doesn't want to sell. What Trenchev didn't report makes the mortgage puzzling—that even if Pierce's wealth looked only half as extensive as it had to *Forbes* in January of 2018, the cost of the Amsterdam property at either 1.2 or 1.3 million dollars looks as though it could be covered by Pierce's pocket change. (And this consideration leaves aside a question about whether the mortgage is also backed in the usual way, by title to the real estate itself.) A real estate deal that would draw on a trivial portion of reputed wealth enters the public stage as the beginning of a new kind of business—the Bitcoin-backed mortgage—and as a declaration

[23] See also Nellie Bowles, "Making a Crypto Utopia in Puerto Rico," *New York Times*, 2 Feb. 2018, www.nytimes.com/2018/02/02/technology/cryptocurrency-puerto-rico.html; Ben Hoyale, "Brock Pierce: From Hollywood Child Star to Bitcoin Billionaire," *The Times*, 9 Feb. 2019, www.thetimes.co.uk/article/brock-pierce-from-hollywood-child-star-to-bitcoin-billionaire-sznvxvoh7; and Nick Stockton, "What Tech Has—and Hasn't Done for Puerto Rico," *Wired*, 23 Aug. 2018, www.wired.com/story/puerto-rico-hurricane-maria-tech/

of a commitment to the coin itself for retail mortgages and for long-term investment ("He doesn't want to sell any of his Bitcoin").[24]

For small purchasers—nonwhales—Bitcoin may no more bind up their identities than buying a lottery ticket does. Yet for others, Bitcoin has also spun off fables of identity even as it has provided anonymity in the first instance. "Bitcoin, c'est moi" is amended to "I'm Bitcoin but I can't say so." A whale establishes that he's not so charitably minded as to sell out—and that, besides, he may not really be so large a whale as *Forbes* thinks. A mortgage business launch conveys a message of intense loyalty to Bitcoin. It's a drama of the valuation of a currency that revolves around its being secured by whales, who discover that they, in all their scorn for the central banks of national governments, have themselves become central bankers of a sort, needing to go public with their loyalty to Bitcoin.

Pierce's statements—"I'll give a billion dollars away immediately" and, indirectly through Trenchev, "I have ninety-five per cent of my wealth in Bitcoin, and I don't want to sell"—may look like simple contradictions of one another, and someone might dismiss them as empty on that account. I think, however, that Pierce, who gives an astonishingly large number of interviews, is one of the best guides to Bitcoin, its situation, and its conception of its way forward. For Pierce speaks to the double-face of Bitcoin: its standing, on the one hand, as an investment vehicle that might constantly increase in value so long as its largest owners don't sell and its functioning, on the other, as a currency for small transactions.

Over time Pierce has ceased to mention the charitable donation of a billion dollars, and he may well have started thinking that it wasn't feasible as he saw the price of Bitcoin dropping to its 2018 low below four thousand dollars. My guess, however, is that he began to feel that his promised generosity to charities in a Puerto Rico devastated by Hurricane Maria was a semiexistential threat to Bitcoin as an investment vehicle, that he realized that his very promise made him look like a whale on the verge of selling out. For even if he had given Bitcoin rather than US dollars to a charity dealing with an unfolding disaster, the Bitcoin would soon have gone to cash. Pierce would have ceased to be a whale. In signing out as a whale and signing on as a philanthropist, he would have identified himself as a virtual enemy of Bitcoin and its market price.

[24] "Nexo Co-Founder Weighs In on Tether and Crypto Market Landscape" *Bloomberg*, 26 Apr. 2019, www.bloomberg.com/news/videos/2019-04-26/nexo-co-founder-weighs-in-on-tether-and-crypto-market-landscape-video. In December 2018, Trenchev reported that his firm had recently lent 1.5 million dollars to someone prominent in the blockchain world so that he could purchase a property in Amsterdam; see Antoni Trenchev, "Blockchain and Cryptocurrencies in 2019—Interview with Antoni Trenchev," *Buisness Live ME*, 12 Dec. 2018, www.businessliveme.com/blockchain-and-cryptocurrencies-in-2019-interview-with-antoni-trenchev/

A fair number of Pierce's remarks in the recent past seem designed to convey not just that his net worth is lower than it was in late 2018 but that he's a loyal whale, content to swim with the others in the pod. I take that to be the message of his mortgage banker—or at least one message. And what Pierce seems actually to have put in place is a five million dollar organization designed to provide money to start-ups in Puerto Rico—and, I'm guessing, to small businesses that will be happy to take Bitcoin in furtherance of the "small casual transaction" of which Nakamoto wrote. Whether Bitcoin has been high or low in the financial markets, it has lagged in small-scale operations—those moments that Nakamoto once described in which Bitcoin would relieve a merchant of the need to hassle a customer for more proof of identity.

Those small-scale, peer-to-peer transactions in Bitcoin have not become common. A Venezuelan like the one who wrote to the *New York Times* may buy bread with Bitcoin, but scarcely anyone uses Bitcoin for daily life. It is not, as Lionel Laurent pointed out, "a convenient global spending currency, as retailers found out when transaction fees surged in 2017."[25] So it's no wonder that Pierce speaks of one of his friends in Puerto Rico as a hero; she has managed to figure out how to make all of her purchases—down to the last latte—in Bitcoin.

Bitcoin, it turns out, is happy to accept loyalty wherever it finds it—from potential sellers too loyal to sell to vendors happy to take only digital coins. Last year around this time crypto partisans gathered for one of their many conventions, with Lamborghini owners putting their cars and themselves on display in the wake of the coin's fall of more than 80 percent. This year, the Ethereal Summit in Brooklyn offered attendees a more community-building coin, complete with "sound baths, meditation and lunch from food trucks paid via digital coins."[26]

As I was writing, members of the Bitcoin and broader cryptocurrency community were assembling again, in another installment in what seems like an almost uninterrupted traveling conference. Bitcoin enthusiasts may well find more food trucks willing to take digital coins and may in the process convince more people that they should buy Bitcoin for investment because of its expanded adoption for retail transactions. Only a few days after Bitcoin broke through six thousand dollars, it climbed above eighth thousand, apparently on the strength of rumors that eBay and Whole Foods

[25] Lionel Laurent, "Bitcoin's Bulls Are Revving Up the Lamborghinis," *Bloomberg*, 13 May 2019, www.bloomberg.com/opinion/articles/2019-05-13/bitcoin-s-bulls-are-revving-up-the-lamborghinis-again

[26] Vildana Hajric, "New York Blockchain Week Begins with Fewer Lamborghinis," *Bloomberg*, 13 May 2019, www.bloomberg.com/news/articles/2019-05-13/blockchain-devotees-swap-lambos-for-sound-baths-at-conferences

were about to accept payments in Bitcoin and other cryptocurrencies.[27] But Bitcoin's surge over a matter of a few days in mid-May may not be an entirely happy development. For its wildly enhanced value is just the opposite number to the wildly depleted value of the Venezuelan currency and to its own losses of more than 80 percent at earlier moments. Its volatility would make it clear how much the small-scale retail transaction matters to our use of money. It might not be insuperably cumbersome for merchants continually having to recalculate prices in Bitcoin, but it would tax a basic confidence in commercial trust that national currencies try to maintain. In the *Metaphysics of Morals*, Immanuel Kant observed that it is a merchant's moral duty to charge the same price to all comers. A little boy who is sent to the store for a bottle of milk should not be asked to pay twice as much as the father would pay. From the standpoint of currencies, Kant's moral duty is merely practical advice. For a currency to be useful in daily life, it must be stable enough so that it doesn't immediately raise questions about favoritism—even favoritism of an entirely accidental kind—in which a merchant is setting a new price for every comer ("For you, this amount"; "And for you, that amount"). For it's at that level of routine transactions that trust emerges as an issue and opens the question: Can Bitcoin's loyalty on the investment side ever become an effective substitute for trust on the level of the small-scale transaction?

Readers who have been following news on the full range of cryptocurrencies will immediately protest that the problem of volatility that I've just raised is a problem that stable coins have been developed to solve. If customers in the same checkout line in a store realized that they were paying conspicuously different prices for the same item, they might well feel that Bitcoin was effectively making a special deal with each customer. They might well feel that it was an unfairness that was no less unfair for being formulaic and mechanical; and they might certainly feel that they didn't want their smallest everyday transactions to be subject to so much risk. Stablecoins, cryptocoins pegged to a currency like the dollar or the pound, aim to make it possible to conduct everyday transactions reliably, without introducing adventure and high drama into daily life. Stablecoins aim to hold reserves in national currencies that will enable them to be as stable, or nonvolatile, as the currencies they tie themselves to.[28]

[27] See Joanna Ossinger and Eddie van der Walt, "Bitcoin's Surge to Almost $8,000 Rekindles Memories of Bubble," *Bloomberg*, 13 May 2019, www.bloomberg.com/news/articles/2019-05-13/bitcoin-vaults-above-7-000-as-cryptocurrency-rally-gains-steam

[28] The reliability of the stablecoin Tether came into question in late April 2019 when the New York Attorney General's Office announced its investigation of Tether and the associated Bitfinex. After Bitfinex lost as much as 850 million dollars to a currency converter, it borrowed

I've been focusing on Bitcoin and largely ignoring other cryptocurrencies. Now that there are more than 150 of such currencies, it would complicate this discussion immensely and, I think, needlessly to detail their various features and strategies. But the relationship between Bitcoin, as the original twenty-first century version of cryptocurrency, and various other cryptocurrencies is worth addressing. It seems to have become particularly fraught most recently when Wright announced that he had registered the Nakamoto white paper and "early computer code underlying the original cryptocurrency."[29] Yet Wright's claim to copyright protection was not his last word. In an email to *Bloomberg*, he wrote

> "BTC [the trading name for Bitcoin] is not Bitcoin. . . . It is an air drop copy that has been designed to slowly alter the protocol allowing the system to be anonymized to such an extent that criminal activity can happen. The goal is to create a system that allows people to commit crimes, extort money, have automated ransomware and worse. This is not the goal of Bitcoin."[30]

Wright now calls the cryptocoin he endorses Bitcoin SV (Satoshi Version), and the statement I've quoted suggests how much more he is claiming than to be first among equals. His is the original—and blameless—cryptocurrency. It is the version of Bitcoin that was supposed to eliminate the need for interpersonal trust—not to tax human capacities for trust as phenomenally as other cryptocurrencies, including Bitcoin (BTC). For Bitcoin (BTC) is, in Wright's account, an imposter, an evil twin that has taken over the very name of Bitcoin. The original Nakamoto white paper addressed the problem of double spending within the blockchain-Bitcoin environment in clear recognition of the fact that double spending was the equivalent of the counterfeiting that goes on in the world of paper currency. Yet Wright claims that a much more serious doubling occurred: namely, that the entire blockchain-Bitcoin nexus has itself been doubled. Bitcoin (BTC) is a changeling, left in the cradle of the original Bitcoin.

Wright may simply be seeking to improve market share for Bitcoin SV by making statements that aim to discredit the competition in the course

more than 600 million dollars from Tether, leaving Tether only seventy-four percent backed by cash and equivalents. See Nikhilesh De, "Tether Lawyer Admits Stablecoin Now 74% Backed by Cash and Equivalents," *Coindesk*, 30 Apr. 2019, www.coindesk.com/tether-lawyer-confirms-stablecoin-74-percent-backed-by-cash-and-equivalents

[29] Kharif and Christopher Yasiejko, "Man Who Claims to Be Bitcoin's Inventor Registers Copyright for Its Code," *Bloomberg*, 21 May 2019, www.bloomberg.com/news/articles/2019-05-21/bitcoin-s-supposed-inventor-says-he-won-copyright-registration

[30] Ibid.

of vouching for the superiority of his own cryptocurrency. His competitors, meanwhile, may think of themselves as merely trying to help the technology evolve so as to be more user-friendly and increase the likelihood of widespread adoption. They may see the storage they offer their clients as a service designed to minimize the problem of individual possession of one's key, the problem that the Winklevoss twins address by dividing their key into the portions that they store in a number of different safe deposit boxes. Other cryptocurrency exchanges may think of themselves as simply solving the problem of volatility with stable coins or expediting transactions by serving as the equivalent of mortgage brokers who connect initial coin offerings with prospective buyers.

But it's clear that Bitcoin news in recent weeks has scarcely made it look like a mechanism for installing trustworthiness into the financial world. The Mueller Report describes how Bitcoin was the currency of choice for the Russian hackers who intruded upon the Democratic National Committee email server and for the Russian trolls and bots who established and maintained Twitter accounts packed with statements that were false or at least misleading and divisive. The city government of Baltimore reports that the hackers who installed malware on its servers demanded payment in Bitcoin if the city was to ransom its financial records. The Dutch reality-TV producer who originated *Big Brother* has sued Facebook for "failing to stop fraudsters flooding its networks with fake Bitcoin ads that featured his image."[31] The cryptocurrency exchange Binance lost seven thousand coins to hackers. And a New Zealand cryptocurrency exchange was "hacked to death" and forced to seek bankruptcy protection.[32]

These stories would hardly seem to inspire anyone who reads them to begin buying and spending Bitcoin, and Bitcoin mining has long since ceased to be a way of increasing the user group now that mining is concentrated in large-scale operations. Bitcoin may describe itself in terms of the publicness of the blockchain, but it has not broken out of the semiprivacy of a small group of investors. Yet even though it has not yet succeeded in being widely adopted, Bitcoin has been important for focusing attention on the fact that the value of currencies lies in their use and for making it possible for people to imagine using a monetary technology other than dollars or pounds or bolivars. It has, thus, highlighted how a national

[31] Ellen Proper, "'Big Brother' Founder Takes Facebook to Court Over Ad Scams," *Bloomberg*, 5 Jun. 2019, www.bloomberg.com/news/articles/2019-06-05/big-brother-founder-takes-facebook-to-court-over-bitcoin-scams

[32] See Josh Saul, "New Zealand Crypto Firm Hacked to Death, Seeks U.S. Bankruptcy," *Bloomberg*, 24 May 2019, www.bloomberg.com/news/articles/2019-05-24/new-zealand-crypto-firm-hacked-to-death-seeks-u-s-bankruptcy

currency has a distinct advantage over a newly invented currency; it has a substantial population of users, people who, when they buy and sell and hold, are most often conducting their transactions in their national currency or the currency of the nation they are traveling in. The supreme gamble of the blockchain-Bitcoin combination was that it would draw a substantial enough population of users to rival or perhaps eventually replace national currencies. It would in the process create a new borderless imagined community with a reach well past those that Anderson saw the novel and the newspaper creating.

How has Bitcoin been used in the ten and a half years since its introduction? Kharif's answer, in an article of 31 May 2019, is that "almost nobody uses it."[33] Bitcoin has fallen short of the aim that Nakamoto announced for it: practical everyday use. Kharif cites blockchain research from Chainalysis, Inc., which reports that merchant transactions in Bitcoin amounted to only 1.3 percent of economic transactions in the first four months of 2019, suggesting that it hasn't made headway against credit cards and cash. And while Chainalysis has interesting information on Bitcoin's use in merchant transactions, it sheds even more light on the distribution of activity within Bitcoin: 89.7 percent of all Bitcoin transactions were related to exchanges, the buying and selling of Bitcoins in peer-to-peer Bitcoin transactions.

Yet perhaps the most remarkable thing about Bitcoin is that a steady stream of disheartening news never seems to dampen the hopefulness about the future of cryptocurrencies. There is talk that the Chinese renminbi may be linked to the blockchain. More institutions are said to be studying possibilities for adoption, and Facebook is launching its own cryptocurrency.

Will Bitcoin dwindle into nothingness, or will it expand? Even if it fails, it will have raised important questions about the relationship among languages, games, and technologies. Ludwig Wittgenstein, in his descriptions of language, pointed to instances in which people know how to go on and know what to say next. He implicitly pointed up how people regularly see a conversation as something already partially made. For all that the rules of language games may be implicit and legally unenforceable, they act as guidance. Games of the kind that Golumbia and Patrick Jagoda describe more explicitly direct a range of responses that count as continuation of play. And the transfer of game rewards from one person to another and the evolution of virtual rewards into money outside the game pointed up the inherently

[33] See Kharif, "Bitcoin's Rally Masks Uncomfortable Fact: Almost Nobody Uses It," *Bloomberg*, 30 May 2019, www.bloomberg.com/news/articles/2019-05-31/bitcoin-s-rally-masks-uncomfortable-fact-almost-nobody-uses-it

technological claim on behalf of cryptocurrency. Technology allows us to pick up and start playing at a higher level. In the world of technology, none of us needs to invent the wheel, fashion a dustpan and a broom, or go on to devise and assemble an ordinary domestic small appliance like the vacuum cleaner.

The question that the blockchain-Bitcoin nexus raises is a question about how efficiently a currency can be a technology—which is in part a question of whether it can allow anyone who uses to enter into its use/play without rehearsing the history of its development. The attachment to the blockchain enables Bitcoin not just to claim that entries in the ledger have been independently arrived at. It is worthwhile for Bitcoin to drag its ever more extensive and ever more electrical energy-intensive history around with it—not to be the Lares and Penates of family history that reminded Aeneas of who he was and served as moral motivation. Instead, the ledger purports to keep the historical record so accurately that it never has to be subjected to revisionary accounts. Having developed outside of the field of moral motivation, it aims to minimize the appeal to moral motivation.

But it's precisely because the ledger needs to be a point of stability that it must remain legible. Which means that Bitcoin and its ledger must continually update themselves both with new transactions and with new ways of making code speak to and in continually evolving computer languages.

Wright's insistence that there was an original unfallen Bitcoin pits itself against the governance group who try to make a relatively minimal number of policy decisions to respond to the ways Bitcoin is continually tested by use. But we might also hear him as imagining that Bitcoin might never have needed governance at all. That image of a currency that never needs a bank or a central bank, that never really needs even a governing body, and that develops from within, taps into the original and continuing lure of Bitcoin. It represents the very idea of a universal and immaterial currency that communicates between persons and entities so directly that it never needs adjustment.

It remains to be seen whether Bitcoin can successfully meet the tests of use and whether it can attract enough legitimate users and strong enough security systems to drive out the forces of web darkness that try to attach themselves to it. As with any technology, Bitcoin is and will continue to be in an existential crisis with itself. For technology continually pits its next iteration against its present configuration. It is always in search of the new model that will make earlier models look clumsy and impractical. Technology is continually bidding farewell to an idea—or destroying the current version in the name of the purest and undefined version of the original idea.

Technology's relationship to itself—its presentation of itself as both the beautiful new and the instantly obsolescent—has prompted a number of artists in recent years to incorporate Bitcoins into their work. But perhaps the most trenchant statement of the problem appeared nearly thirty years before the Nakamoto white paper, when Jeff Koons put on display his Hoover series that he began exhibiting in 1980. His Hoovers may have been designed and manufactured as small domestic appliances. Machines meant for use. But Koons took them out of circulation, encasing them in plexiglass vitrines sealed so as to remain unopened. These cases recalled store windows but forestalled any thought that someone might ask to have a model removed from the window and tried out. Koons found material expression for an idea—not just the recognizable beauty of the already made, but an art that saw itself as making art by putting its object outside of the reach of use. "If one of my works was to be turned on," Koons said, "it would be destroyed."[34] Its encasement converts a beautiful thing into a beautiful idea.

The question for Bitcoin is whether the beauty of its idea will survive its use.

Coda

Since I completed a draft of this essay, Facebook has announced plans to launch its own cryptocurrency, the Libra. The beauty of the scheme is that it would harness the global population of Facebook users. It has taken a certain effort for people to figure out how to buy and sell Bitcoin, as colleges that have received Bitcoin donations have discovered. Yet Libra will be difficult to avoid because its hold on an immense global population will mean that any Facebook user who decides to send payments to other Facebook users will effectively recruit them for Libra. The old "friends and family" plans of telephone companies will come to look like a quaint chapter in marketing history, as one friend or family member on Facebook can serve their own convenience by paying with Libra and requiring their friends or family to join to collect, as "you've got mail" becomes "you've got money."

The problem that Libra poses is that we may soon come to live in a world that has not solved the problem of trust in social and political institutions but simply declared it obsolete, acting as if we ought to accept the idea that it has successfully been engineered into the distributed ledger—a settled matter for a currency that treats itself as a commercial product.

[34] Quoted in "Jeff Koons: Banality, Decadence and Easyfun," *Tate*, www.tate.org.uk/art/artists/jeff-koons-2368/jeff-koons-banality-decadence-and-easyfun

Many of the early responses to the Libra scheme focus on this issue of trust and imagine either that Facebook stands to gain trust by implementing Libra or that we ought to continue to remain skeptical about Facebook's intentions towards us. One commentator, Kevin Werbach, has said that "Libra is the last, best hope to re-establish trust between Facebook and the world," and that "Bitcoin, and the blockchain technology it popularized, . . . create[s] the foundation for a new form of trust."[35] Others have pointed to the difficulties of imagining a technological fix for Facebook's problems with trust. As Megan McArdle put it, "too many people hate it."[36] And John Naughton has wondered if we are "comfortable with the idea of a new global currency controlled by a consortium of corporate bosses" assembled by Facebook, the company that made Cambridge Analytica a household name.[37]

Yet all of these commentators, insightful as they are, continue to imagine that Facebook needs for us to trust, that our view of it matters. By contrast, Evgeny Morozov describes Libra as a full-out assault on the global financial system, one that puts itself out of the reach of national regulatory systems.[38] What he calls Facebook's faux populism might well, I think, recruit lots of individuals to small-scale criminality that wouldn't look like criminality to them because it seemed only to cheat the government. It would be virtually impossible to regulate the virtual currency. And if we were to take comfort in the idea that Libra would make it possible for us to withhold our assent to governmental actions such as tariffs that we did not approve of, the real issue may ultimately be that questions of trust, endorsement, and legitimacy become irrelevant. Morozov suggests that Facebook "stands to curry favor with Donald Trump," in offering Libra in direct competition to Chinese competitors who have "already shown that payments and communications go together and produce a very profitable mix." If Donald Trump ever sees the question in those terms, and it's hard to imagine that Facebook won't encourage him to, his decision

[35] Kevin Werbach, "The Real Reason for Facebook's New Cryptocurrency," *New York Times*, 20 June 2019, www.nytimes.com/2019/06/20/opinion/facebook-libra-cryptocurrency.html

[36] Megan McArdle, "Facebook Must Like Trouble, Because Its New Cryptocurrency Just Means More of It," *Washington Post*, 20 Jun. 2019, www.washingtonpost.com/opinions/2019/06/20/facebook-must-like-trouble-because-its-new-cryptocurrency-just-means-more-it/?utm_term=.5d05142e50b0

[37] John Naughton, "Libra Cryptocurrency: Dare You Trust Facebook with Your Money?" *The Guardian*, 23 Jun. 2019, www.theguardian.com/commentisfree/2019/jun/23/libra-cryptocurrency-dare-you-trust-facebook-with-your-money

[38] See Evgeny Morozov, "Facebook's Plan to Break the Global Financial System," *The Guardian*, 22 Jun. 2019, www.theguardian.com/commentisfree/2019/jun/21/facebooks-plan-to-break-the-global-financial-system

would be less a decision than a recognition of necessity, the need to fight the war of the worlds in data.

As dystopian as Morozov's vision is, it is perhaps not dystopian enough. He eloquently describes how firms that traffic in data—"as long as data remains the lifeblood of democracy and economy alike"—"will exercise disproportionate and undue influence over decisions that ought to be decided in parliaments, not in marketplaces."[39] It may be that the business model that aims to replace democratic discussion with monetized communication may already be well on its way to its eventual triumph, that it may be replacing constitutional democracies themselves by pointing to the accuracy of the ledger as if to ask, "What are you worried about? We told you that we had created a financial product suitable for functioning in a post-truth and post-trust world, in which the only demand of citizenship is that you remember that you're playing against the Chinese team."

[39] Ibid.