11 FEBRUARY 2021

TRADING IN ATOMS FOR BITS

The long history of digital currencies

Finn Brunton

All forms of exchange necessarily depend on differences in voltage.[1]
—Fernand Braudel

The history of digital cash consists of scientific discoveries from the 1970s, hardware from the 1980s, and networks from the 1990s, shaped by theories from the previous three centuries and beliefs about the next ten thousand years. It speaks ancient ideas with a modern twang, as we might when we say "quid pro quo" or "shibboleth": the sovereign right to issue money, the debasement of coinage, the symbolic stamp that transfers the rights to value from me to thee. Digital cash has the hovering, unsettled realness (not reality) of all money, a matter of life and death that is also symbolic tokens, rules of a game, scraps of cotton blend and polymer, entries in a database, promises made and broken, gestures of affection and trust. The long history we are discussing here is at its heart the history of a debate about *knowledge,* an epistemological argument conducted through technologies.

It is a debate broadly familiar to anyone who has taken an interest in the nature of money, or even looked idly at a banknote for a bit: how do I know that money is real? I want to phrase the question in this somewhat awkward way to capture how it can be reasonably answered. We can ask it at the level of a particular token of money—how do I know this money is real?—with the feel and texture of a note, the security threads, watermarks, and ultraviolet inks. We can ask it at the level of some type or variety of money, perhaps expressed as a preference for one currency as more "solid" than another, for instance, or for cash over credit, or gold over both: how do I know this kind of money is real? Finally, we can ask it at the level of money as such—what is money that it has value for us, and how do we know that value? How do I know that money is real?

I'm sure the reader has already noticed that this set of questions is fundamentally confused: "real" sometimes means "valuable," sometimes "reliable," "genuine," or

"authentic." They muddle different kinds of knowledge together, from the empiricism of handling cash, to the accumulated experience of shared social norms about money, to beliefs and bets about the future based on all manner of conviction, habit, and hope. They conflate fundamentally unlike things into the category of "money." I hope this very confusion is useful in showing us the kinds of realness that co-exist in even ordinary cash experience—holding a US twenty-dollar bill, for instance, with its ostensible realness scaling up from your fingertips all the way to the stable monetary sovereignty of the nation, however distant it may be. I want us to dwell on this, because attempts to resolve these uncertainties (what do you mean by money, by real money, by valuable money?) constitute the long history of digital cash. How do I know that a digital object is unique—that it is genuine and not a copy? How do I know that it is worth something? How do I know that any of this is real (and real in what sense)?

For digital cash, the answers to these questions lay in the future, in two senses: its creation relied on technologies of trust and proof that barely existed or were in the process of being developed, and it needed predictions and stories of the future to drive adoption and acceptance in the present. The two central future narratives of early digital cash experiments were crisis and transcendence.

Examples of Bernard von NotHaus's silver-backed Liberty Dollar "warehouse receipts." These paper certificates were introduced in 1998, at the same time as Liberty Dollar metal "medallions."

Devotees of metallic money—of cash backed by gold and silver, and coins made of them—cherish the bodily, empirical knowledge that metal gives: the way it warms in the palm and between the fingers, the chime of a round of pure silver cast onto a marble tabletop. It is just elementally *there,* with its "magnificent stupid honesty" (as H. G. Wells once described the gold standard). "Do you take silver?" customers of Bernard von NotHaus's American Liberty Dollar coinage scheme would ask checkout clerks, before they performed "the Drop": releasing the coin into someone's hand so they could feel the weight of the silver, as a prelude for their buying into its value.[2] In 1974, Von NotHaus had coauthored "To Know Value—An Economic Research Paper," a manifesto outlining a rationale for a new, deflationary, gold-based financial system, which he would go on to build over the following decades with various companies and mints that issued coins as a "private voluntary barter currency."[3] The distinction was a delicate one. Von NotHaus's Liberty Dollar coins were technically "medallions," collectibles that were not, *not,* they repeated emphatically, trying to pass as legal US currency. Why would they want to? Already in 1974, he was predicting runaway inflation and tyrannical crackdowns; his money was envisioned as a way out of government-induced crises.

Likewise, his "eLibertyDollars" were not posing as dollars as such—as legal tender—but were instead just digital "warehouse receipts."[4] These receipts could be redeemed for a quantity of precious metal stored in a warehouse outside Coeur d'Alene, Idaho. They were seldom redeemed, though. They are better understood as the right to transact part of an ingot of silver sitting on a pallet somewhere, without needing to handle or physically subdivide it. On the internet, the receipts could be bought, sold, speculated on, and used as collateral (until the business was raided by the FBI and the US Secret Service in 2007). They were an example of a digital gold currency (DGC).[5] DGCs had names like IntGold, e-Bullion, the Aspen Dollar, Pecunix, GoldMoney, and E-Gold; they were one of the two main threads of digital cash's development, and by far the most consequential prior to Bitcoin. Their model of money was the token, and their future was crisis.

Von NotHaus displaying his currency, 2007. In November of that year, the federal government raided both his headquarters in Evansville, Indiana, and the warehouse in Coeur d'Alene, Idaho that held the company's reserves of gold and silver.

A second delicate distinction needs to be made here to understand how this worked and what it meant. DGCs were not primarily about investing in gold and silver as commodities, a viewpoint that guides those who still have faith in such currencies. Though investment might be an indirect byproduct of holding a lot of DGC receipts, they are not competing with investments in commodity futures or shares in an exchange-traded fund specializing in metal. They do not want to be an asset into which you put money, but to be the money itself.

There's a loop in this argument: DGCs should be transacted because they are superior to

fiat money, say their creators, and yet the evidence for this is measured in their value in that very fiat money. The dollar is the standard of measurement, and unfit to measure—at once proof of worth, and proved worthless. Like many paradoxes in practice, the resolution to this confusion happens on the plane of theory and symbolism. You should own and transact in DGCs because by doing so, you handle something with "intrinsic" and "objective" value (favorite adjectives of this movement). The act of passing objective value as currency would, they believe, rebase *exchange itself* into a newly meaningful act. "Why buy gold?," asked von NotHaus in 1974. "Because it is gold" (or, as a private-issue minter said to me in New Hampshire, "Silver is silver, and the weight is the weight"). This is not economics, but an epistemology and a way of life: to spend and accept metal, or a digital pointer to metal, is to affirm a shared commitment to an extrahuman, supersocial order of values. It is one step on a path of knowledge that will take you outside fiat, outside the state, and into a different system of beliefs.[6]

Their goal is therefore transaction, not return on investment. Ideologically, getting someone to accept payment in a private currency not issued by a sovereign central bank was, and is, a revolutionary act. They measure success in circulation and velocity, and by those measures the original wave of DGCs were indeed successful.

DGCs preceded companies like PayPal by years, and the biggest among them were handling billions of dollars of transactions in their currencies annually by the early 2000s. They pioneered mobile transactions and micropayments in units as small as ten-thousandths of an ounce of gold. Their framework for digital currency was tokens corresponding to specific portions of specific bars of metal in safe deposit boxes and secure warehouses from London to Idaho to Dubai. Another subtle distinction arises here. The tokens worked as pointers to the gold, which you need never see or touch. What you were really transacting with DGCs was the right to transact that gold in the future. To spend this "currency" was to assign the rights, in whole or in part, to someone else.

Worker at the New York Federal Reserve, 1960s. Note the steel-toed shoes designed to protect employees when moving heavy bars of gold bullion.

For contrast, consider the work of David Chaum, a cryptographer, entrepreneur, and the most foresightful of the digital currency developers. Beginning with papers in the early 1980s, Chaum laid out a vision of digital cash.[7] The company he created to bring this to market, DigiCash, was so very nearly successful that you can glimpse the Web we could have had, one where surveillance advertising was not the dominant business model. Chaum understood digital cash as a format into and out of which existing money could be converted. In the DigiCash model, you could withdraw money from your bank account in the form of anonymous, cryptographically authenticated digital notes, just as you would paper banknotes from a cash machine. You could hold the notes on a physical card, or in a digital wallet linked to your web browser. After you spent them, the merchant would deposit them back in the bank just as they would have walked the contents of the register to the night drop after closing.

There were major inventions and innovations in the DigiCash system: ways that the money could prove itself, as cash in hand does, without providing any information about you or your activities, and ways that it could protect itself from being spent multiple times by the same person. It was a template for many other digital cash projects. But DigiCash was a way of *translating* existing money, issued and managed by existing banks, not creating something new. It could give dollars or dirhams a format and a protocol so they could circulate online. It was a way of making currency digital, not making digital

currency. Whereas it interoperated with the world as it was, DGCs were tools and practices informed by a vision of the future.

Their narrative was one of imminent, inexorable doom, a precipice we were fast approaching. Libertarian science fiction, from widely read work by Ayn Rand and Robert Heinlein to deeper cuts like J. Neil Schulman's 1979 dystopian political economy thriller *Alongside Night* (a major influence on online contraband marketplaces like Silk Road), outlined the disaster. Statist central banks with control of money would lead to worthless ink-smeared cash with value enforced at gunpoint, ration books, crumbling infrastructure, and federal thugs kicking down the doors of renegade bankers. This could be survived, or even averted, by moving to private monies issued by free banks.

"Just what is a 'digital bank'?" asked the militant crypto-anarchy theorist and software developer Timothy C. May in 1994.[8] The community of "cypherpunks" he was addressing had built systems for encrypting messages and anonymizing authors, in part because the cypherpunks had a more or less clear conceptual agreement as to what those systems would do—disagreements could be at the practical level of tools and techniques. But what was a "digital bank"? What was a "digital coin"? Digital gold currencies were digital banks, of a sort, but they were at heart profoundly analogue: inventive software script pointing back to a wedge of gleaming material so obdurately solid that it would break bones if dropped. In the answer to this question lay the other thread of the genesis of digital currency, whose model of money was the ledger, and whose future was transcendence.

Bitcoin traders Kolin Burges (right) and Aaron (who declined to give his last name) protesting outside the headquarters of the Tokyo-based Bitcoin exchange Mt. Gox, February 2014. The two men were trying to pressure the exchange to allow withdrawals, which had been suspended following what Mt. Gox claimed was a "transaction malleability" bug in Bitcoin itself. The exchange soon went bankrupt after it declared that a hack had led to the loss of almost all of the Bitcoins it held on behalf of its customers.

"Money is not about atoms, it is about bits," wrote May's fellow cypherpunk Hal Finney in 2002.[9] (Finney would go on to be a correspondent of Satoshi Nakamoto's and play a major role in the design and development of Bitcoin.) A truly digital bank should take as its starting point that money must be information: not a format into which money can be put, nor a pointer to real value elsewhere, but digital information as such.

Finney was expanding on a proposal by still another cypherpunk developer, Wei Dai, who was in turn responding to an idea of May's. Dai's proposal was called "b-money," and the premise was that a digital bank was not something that ran on top of a network; it was a network itself.[10] The bank was constituted out of the sum of its account holders, all of whom kept copies of the ledger of all the accounts—"everyone keeping track of how much money everyone has," as Finney put it. Every transaction between accounts is recorded and reconciled on all the ledgers. (All the accounts are pseudonyms, authenticated by a cryptographic key, without needing a formal identity.) Significantly, anyone on the network could mint new currency under a set of agreed-upon rules by solving a computational problem—what we would now call a "proof of work"—whose difficulty could be increased or decreased to keep the buying power of the currency more or less stable relative to a basket of commodities.

This description is deceptively simple, though, for what it actually means: at the center of digital currency, where DGCs put gold ingots, b-money placed a particular, mediated, anonymous version of consensus. B-money didn't need to point to anything but itself. The people who minted it were the people who used it and the people who ran the bank where it was held—it is as if everyone with a bank account also had a seat on the board of the Fed. (The decentral bankers!) The problem of value was elegantly solved by this consensus model: you wouldn't be a part of the network if you didn't think it could be valuable. You invested time and energy in the form of computational work into the production of new currency, a sweat equity theory of worth validated by everyone else who shared it. B-money was not unique in this idea, exactly—there were variations and elements being developed by other people in the community, from Nick Szabo's "bit gold" proposal to a "Reusable Proof of Work" platform developed by Finney himself.[11] It was exemplary, though: a clear and carefully thought-through assembly of different

pieces, it was one of the projects that Nakamoto later credited as contributing to Bitcoin.[12]

B-money was inspired by imagining a society in which "violence is impossible because its participants cannot be linked to their true names or physical locations"—the prospective society of Timothy May's doctrine of crypto-anarchy.[13] "Encryption," May wrote, starting a list: "digital money, anonymous networks, digital pseudonyms, zero knowledge, reputations, information markets, black markets, collapse of governments."[14] It was a future projected in nine clauses, as new technologies of money begin a steady exodus of value from taxable channels into contexts not just outside the state apparatus but opposed to it, with old governments collapsing under their own weight and new social forms spontaneously assembling out of network infrastructure—social systems as new as the currency whose transactors are also an anonymous self-governing fiscal consensus. Whereas the bullion of digital gold currencies offered shelter from the storm, digital currencies like b-money *were* the storm.

It was to be a future that digital currency would not just occupy, but have a role in bringing about: a new society of networked anonymity, pseudonymity, and privacy, the cypherpunks hoped. Their contemporary fellow-travelers, a philosophical subculture called the Extropians, hoped for far more. They saw themselves not in the twilight of ruin, riding out the failure of the modern order, but as the accelerant of a new age of posthuman flourishing to come. They would underwrite and prototype new forms of politics, new forms of markets, and new ways of living—and dying.

Bitcoin and blockchain advocates at a Yellow Vest demonstration in Paris, February 2019. Some Gilets Jaunes activists have advocated switching to the cryptocurrency as a way of undermining the French banking system.

The groups had a lot of overlap in membership and interest and mailing lists, but for the Extropians, digital currency didn't just aid in the creation of a newly private society and its secret markets. It would spur new economic systems, which would in turn accelerate innovation, discovery, and invention into a cascade of breakthroughs that would ultimately lead to ultra-longevity, off-planet migration, robust general artificial intelligence, and the end of the human condition as we know it. Their closest analogue might be Russian Cosmists and Biocosmists, thinking on a galactic scale and understanding the end of death as a goal and a demand; both groups also shared an interest in "anabiosis," the freezing and cryonic preservation of the organism for future resurrection, whether in body or in digitized mind.[15] Finney was frozen when he passed away in 2014, joining several other people in the history of digital currency who await the civilizational breakthroughs that might restore them to consciousness forever.

The complex realness of money is always anticipatory. It is tied into the future, from accepting a banknote on the assumption that someone else will accept it from you, to believing or doubting in the stability of a currency, or even currency as a whole. (The very definition of currency, the "passing current," defines money as what one is willing to be passed and to pass on in turn.) To write a history of money is also to write a history of the future and "what people … *expected* the future to be like," in the perfect phrase of the historian Rebecca Spang.[16] This goes double for the history of digital currency, a futuristic project in every sense. To document the long history of digital cash is to know the futures feared and longed-for; to read this history, I hope, is to understand how much their legacies shaped the new currency technologies around us now.

1. Fernand Braudel, *Civilization and Capitalism, 15th–18th Century*, vol. 1, *The Structure of Everyday Life* (Berkeley: University of California Press, 1992), p. 441.
2. This process was described to an undercover FBI agent, as recounted in the evidence filed with the affidavit: Shelter Systems, LLC, "Motion for Return of Property," case no. MS-07–6337-MHW, 17 June 2008, p. 11.
3. Bernard von NotHaus and Telle Presley, "To Know Value—An Economic Research Paper," 1974. Available at bernardvonnothaus.org/wp-content/uploads/To-Know-Value.pdf.
4. The phrase "eLiberty Dollars" appears in the text on the warehouse receipts and can be seen reproduced on a specimen copy. For instance, see Exhibit C entered into evidence on the Shelter Systems "Motion," p. 33.
5. For an outstanding general history and analysis of DGCs, see P. Carl Mullan, *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (New York: Palgrave, 2016). The details on E-Gold's operation in chapter 2 are particularly interesting.
6. For much more on the culture, and cult, of the gold standard and its relationship to the history of digital currencies, see David Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism* (Minneapolis: University of Minnesota Press, 2016).
7. Two exemplary early Chaum papers are "Blind Signatures for Untraceable

Payments," in *Advances in Cryptology: Proceedings of Crypto 82,* ed. David Chaum, Ronald L. Rivest, and Alan T. Sherman (New York: Plenum Press, 1983), and "Security without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM*, vol. 28, no. 10 (October 1985).

8. See Timothy C. May, "The Cyphernomicon: Cypherpunks FAQ and More," September 1994, section 17.3.1. Available at web.archive.org/web/20170805063522/http://www.cypherpunks.to:80/faq/cyphernomicron/cyphernomicon.txt.
9. Hal Finney, "Re: Currency Based on Energy," Exl-list archive, 22 February 2002. Available at extropians.weidai.com/extropians.1Q02/3361.html.
10. Wei Dai, "PipeNet 1.1 and b-money," Cypherpunks list archive, 27 November 1998. Available at cypherpunks.venona.com/date/1998/11/msg00941.html.
11. For Nick Szabo's most formal explanation of "bit gold," see his "Bit Gold," *Unenumerated* (blog), 29 December 2005. Available at unenumerated.blogspot.com/2005/12/bit-gold.html. Szabo had made reference to aspects of the system as early as 1998; see his "Secure Property Titles with Owner Authority." Available at nakamotoinstitute.org/secure-property-titles. On Finney's Reusable Proof of Work system, see "RPOW Theory," RPOW.net. Available at web.archive.org/web/20070528042614/http://rpow.net:80/theory.html.
12. Satoshi Nakamoto, "Citation of Your B-Money Page," email to Wei Dai, 22 August 2008. Available at www.gwern.net/docs/2008-nakamoto.
13. This phrase is Dai's, from "PipeNet 1.1 and b-money."
14. This list was in Timothy May's email signature and also used in many of his Usenet posts; it can be found throughout his correspondence.
15. There has been a flurry of recent publications about the amazing social-philosophical movement of the Cosmists and Biocosmists. See *Russian Cosmism*, ed. Boris Groys (Cambridge, MA: The MIT Press, 2018) and Anya Bernstein, *The Future of Immortality: Remaking Life and Death in Contemporary Russia* (Princeton, NJ: Princeton University Press, 2019).
16. Rebecca Spang, *Stuff and Money in the Time of the French Revolution* (Cambridge, MA: Harvard University Press, 2015), p. 20.

Finn Brunton is a professor at the University of California, Davis. He is the author of *Spam: A Shadow History of the Internet* (MIT Press, 2013) and *Digital Cash: The Unknown History of the Anarchists, Technologists, and Utopians Who Created Cryptocurrency* (Princeton University Press, 2019). He is currently working on a book about the history and media of rationalist utopians.