Two Paradoxes of Crypto

John O. McGinnis[*]

INTRODUCTION

A lot of financial innovation is now encompassed by the term "crypto"—Bitcoin, Ethereum, stablecoins, crypto-exchanges, and digital central bank currencies, to name just a few. But what we should think about these financial innovations and what, if anything, the law should do about them depends on making sharp distinctions among different phenomena that are covered by the same meme. In this brief talk, I will argue that one distinction is central: to what degree are the financial innovations decentralized, in that they are not controlled by the government or any intermediary? If the financial innovations are genuinely decentralized and transparent, there is no longer a need for

[*] George C. Dix Professor in Constitutional Law at Northwestern University Pritzker School of Law. This is an edited version of a luncheon speech given at a conference entitled "Blockchain and Beyond: The Interaction between Distributed Ledger Technology and the Law" at Chapman University Fowler School of Law on January 27, 2023.

regulations that are focused on constraining agency costs. Such innovations have created a new mechanism for trust that does not generate the usual principal–agent problems of financial intermediaries. There may still be a need for regulation for other reasons—for instance, to prevent externalities—but much regulation of financial institutions concerns agency costs.

The second theme of this talk is the paradoxes of crypto. Both paradoxes concern the relation of centralized and decentralized finance. The first is how currently decentralized and novel institutions like Bitcoin depend on an ecosystem that is filled with institutions closely resembling more centralized financial intermediaries of the past. The intertwining of decentralization and centralization in this ecosystem is one of the central features of crypto today. These financial intermediaries are, in turn, regulated by the most centralized entity of all—the state. Thus, one emerging question for crypto today is how much even decentralized financial institutions need more centralized financial intermediaries to operate. Here, my view is that initially institutions like Bitcoin do need such intermediaries, and thus their ecosystem will be subject to regulation for agency costs reasons, even if Bitcoin itself is not. The longer-term question is whether many of these intermediaries can also be decentralized with the aid of the blockchain.

The second paradox is that while Bitcoin began as a radical libertarian project, it now inspires central bank digital currency, which ironically can give far more power to the government over the financial lives of its citizens than it has today. Perhaps even more ironically, the presence of that power and its possible abuse may give greater impetus to Bitcoin as citizens flee a kind of currency that can give the government more authority over their lives. Decentralized and centralized financial institutions remain in fundamental tension in their structures, even when they both use the blockchain and are called digital currencies. Nevertheless, they can both intertwine and feed off one another.

I. BITCOIN—THE PARADIGM OF THE NEW DECENTRALIZED FORM OF TRUST

Let us begin with Bitcoin, both because Bitcoin was the big bang of the crypto universe and because it provides a clear model of innovation that is radically decentralized and aspires to the status of a currency.

Bitcoin is the brainchild of Satoshi Nakamoto, whoever he, she, or they were.[1] Nakamoto figured out how to solve the greatest problem with a digital currency—how to determine who possessed it without relying on any central authority since any single authority would be difficult to trust. His brilliant idea was to link the creation of the currency to verifying transactions in the currency. To simplify: when someone wants to transfer Bitcoin to another person, he sends the Bitcoin from his digital wallet (a kind of encrypted computer file) to the other person's digital wallet.[2] The digital wallets are identified by public keys, but the sender can release the Bitcoin by a private key known only to him.[3] The transaction is then broadcast publicly so it can be verified in a way that everyone knows that the sender has the private key, but cannot see the actual key. The verification process requires the solving of complex computer equations that are linked to the particular transaction.[4] Through solving the equations with computers, individuals called "miners" can then verify the transaction.[5]

The miner who most likely verifies the transaction by adding it to the "blockchain" (a public ledger) of all Bitcoin transactions gets paid in Bitcoins for his work.[6] Other miners essentially agree by a majority vote, as measured by computation power, which miner has triumphed.[7] Thus, the creation of new currency is linked to the process of verifying it. In other words, the process itself gives incentives to deploy the substantial computer processing power that keeps the system going. The currency also is defined to have a finite amount of Bitcoin, preventing inflation. Most Bitcoin has in fact already been created. Each year, the amount that is created to pay the miners for verifying the

1 There is no conclusive evidence as to the identity of Bitcoin's creator. *See Who Is Satoshi Nakamoto?*, COINDESK (Feb. 9, 2023, 5:25 AM), http://www.coindesk.com/learn/who-is-satoshi-nakamoto/ [http://perma.cc/PJZ6-MSY7].

2 *See* DANIEL DRESCHER, BLOCKCHAIN BASICS: A NON-TECHNICAL INTRODUCTION IN 25 STEPS 103–09 (2017).

3 *See id.* at 93–101.

4 *See id.* at 153–64.

5 *See id.*

6 For a discussion on Bitcoin's mining incentives, see Chris Pacia, *Bitcoin Mining Explained Like You're Five: Part 1 – Incentives*, ESCAPE VELOCITY (Sept. 2, 2013), http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/ [http://perma.cc/8RYS-ZSW9].

7 *See generally* Nathaniel Popper, *Into the Bitcoin Mines*, N.Y. TIMES: DEALBOOK (Dec. 21, 2013, 1:42 PM), http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines [http://perma.cc/62TL-W4BP] (describing the Bitcoin mining technology and the miners' roles in the Bitcoin system).

transaction is halved, until 2140, when all of the preset amount of Bitcoin will have been created.[8]

Although the creation of Bitcoin is impressive as a technological innovation, Bitcoin's central innovation is in trust—the essential characteristic of any currency that will have long-term success and of any payment system. To understand this, contrast Bitcoin with older forms of currencies—one public and one also private. The more familiar, of course, is public money.

Bitcoin does not require faith in any public institution that creates money.[9] In this, it aspires to make a radical break with our current monetary order because that order is strongly centralized by the state. So-called fiat currency, like the dollars in your pocket, depends not on trust in an algorithm and a group of individuals who have the incentive to maintain it, but in the state. Indeed, the entire idea of modern monetary theory is built on the view that it is only a government agent, like a monarch, the Federal Reserve, or some other centralized authority that can instill trust.[10]

But the difficulty is that there are many reasons not to trust government currency. That is obvious in what I have elsewhere called monetarily oppressive regimes like Venezuela, where dictatorial regimes subordinate maintaining the value of the currency to other non-public regarding values.[11] But it is even true of a much better currency like the dollar. The Federal Reserve has maintenance of the value of the currency as only one of its objectives. For instance, it wants to make sure that the currency functions in such a way as to create full employment.[12] Full employment is a value that can be understood as public regarding. Assuring that everyone has a job is good for personal happiness and political stability. But nevertheless, this objective creates an agency cost between the individual who is only interested in maintaining the value of the currency and the government that has other objectives. Thus, Bitcoin is distinguished from fiat money precisely because it does not have the agency costs of public money.

---

8 *See* Gareth Jenkinson, *A Glimpse into the Future - What Happens When There Are No More Bitcoin to Mine?*, COINTELEGRAPH (May 6, 2018), http://cointelegraph.com/news/a-glimpse-into-the-future-what-happens-when-there-are-no-more-bitcoin-to-mine [http://perma.cc/9HZ8-NPTV].

9 John O. McGinnis & Kyle Roche, *Bitcoin: Order Without Law in the Digital Age*, 84 IND. L. REV. 1497, 1500 (2019).

10 *See* GEORG FRIEDRICH KNAPP, THE STATE THEORY OF MONEY 2 (1924).

11 *See id.* at 171.

12 *See* 12 U.S.C. § 225a.

There have been previous experiments in creating private currency by using private bank notes. Unlike the government currencies, banks do not have public regarding interests that may conflict with maintaining the value of the money. But banks are financial intermediaries that are run for profit. Thus, their profit motivation creates another kind of agency cost. They may seek profits at the expense of sound currency. Certainly, private banks have historically engaged in imprudent lending and investments and thus, the value of their currency has dropped.[13]

Thus, Bitcoin is potentially superior to both public and private currency in terms of reducing agency costs. I say potentially superior because it does not yet function as a currency in any but the most monetarily oppressive regimes. It is too volatile in value to be a good store of value or unit of account.[14] But the absence of agency costs shows that one traditional reason for regulating financial intermediaries is absent for Bitcoin. There is no intermediary to create these costs and the need for regulation to constrain agency costs and prevent fraud because of Bitcoin itself. The consensus mechanism which the minting of Bitcoin pays for is itself the antidote to agency costs.

II. BITCOIN V. FIAT MONEY

Nevertheless, if Bitcoin succeeds in its aspiration to become a currency, it will ultimately do so at the expense of fiat money. Thus, if one thinks that Bitcoin might succeed and believes that fiat money has many virtues, that prospect furnishes a reason for regulation now, because as Bitcoin becomes more valuable and attracts more stakeholders, it will be politically more difficult to regulate. But the most plausible reason for regulation is not rooted in agency costs, but in externalities. For instance, those who favor public money believe it has public benefits such as stabilizing the government and promoting full employment. Thus, it needs to be protected against an upstart that lacks these public benefits.[15]

The question of the attractiveness, in theory, of a private currency like Bitcoin versus fiat money is a classic debate between libertarians and supporters of greater governmental power. The

---

13 *See* RICHARD HOFSTADTER, THE AMERICAN POLITICAL TRADITION: AND THE MEN WHO MADE IT 51 (1948) (describing the era of free banking in which banks failed due to imprudent actions).

14 *See* John Crawford, *Safe Money*, 104 MARQ. L. REV. 411, 452–53 (2020).

15 *See* William J. Luther, *Regulating Bitcoin – On What Grounds?*, *in* REFRAMING FINANCIAL REGULATION: ENHANCING STABILITY AND PROTECTING CONSUMERS 391, 406 (Hester Peirce & Benjamin Klutsey eds., 2016).

latter have confidence that wise government oversight has large public benefits, like promoting full employment or shortening recessions. More libertarian theorists would respond that the government lacks the knowledge to achieve those benefits, and in some cases, leaders will use their authority to benefit themselves, creating better conditions for their reelection at the expense of future prosperity. On this view, government intermediaries, like private intermediaries, create agency costs that may outweigh their potential public benefits.[16]

III. THE FIRST PARADOX OF CRYPTO: BITCOIN'S CURRENT DEPENDENCE ON CENTRALIZED FINANCIAL INTERMEDIARIES

If Bitcoin is to grow into a more stable currency, it will need financial intermediaries to do so. Now let me touch on the first paradox of crypto: its immediate future is intertwined with the kind of financial institutions that one might think blockchain is designed to replace. For instance, most people lack the ability to hold Bitcoin on their own—there is too much danger that they will lose the keys that allow them to transact on the blockchain. They will thus lose their investment as a whole. There are many sad stories of people who are searching for millions of dollars of Bitcoin because they discarded a piece of paper or a laptop with the information.[17]

Thus, cryptocurrency wallets and exchanges are needed to popularize Bitcoin. But these wallets and exchanges resemble traditional financial intermediaries. Let me be clear: financial intermediaries are valuable. They provide third party verification and reduce information asymmetries.[18] But they also introduce problems of opportunism, including new kinds of informational asymmetries and agency costs. Even while they verify the actions of others, there remains the question of who will verify their own actions. *Quis custodiet ipsos custodes?*[19]

Thus, the case for regulating them is as strong as the case for regulating any financial intermediary. The implosion of FTX is

---

16 On government agency costs, see M. TODD HENDERSON & SALEN CHURI, THE TRUST REVOLUTION: HOW THE DIGITIZATION OF TRUST WILL REVOLUTIONIZE BUSINESS AND GOVERNMENT 33–34 (2019).

17 *See, e.g.*, Aatif Sulleyman, *Man Who 'Threw Away' Bitcoin Haul Now Worth over $80M Wants to Dig Up Landfill Site*, INDEPENDENT (Dec. 4, 2017, 5:41 PM), http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-value-james-howells-newport-landfill-hard-drive-campbell-simpson-laszlo-hanyecz-a8091371.html [http://perma.cc/E4SB-J4Z9].

18 Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* 6 (Rotman Sch. of Mgmt., Working Paper No. 2874598, 2019), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598 [http://perma.cc/99KB-SJ5V].

19 Translates to "who will guard the guards themselves?"

itself a story of agency costs. It is alleged to have used its customer cryptocurrency to support speculative trading in cryptocurrency on its own account.[20] The problem is no different than if the firm had used, for its own speculation, traditional financial securities like stocks and bonds, which it held in its customers' accounts.

To succeed as a currency, Bitcoin and any other similar crypto will also need the same kind of financial mechanisms used to deepen the market for other financial assets.[21] These include future markets to facilitate price discovery and exchange-traded funds ("ETFs") that allow smaller investors to participate more effectively in owning the asset. If these structures require financial intermediaries immediately, they will need regulation as well. For instance, the Securities and Exchange Commission has so far denied a Bitcoin-focused ETF because of dangers of fraud in the underlying exchanges.[22] That may well not be the right decision, but it is the kind of decision that it makes in evaluating other ETFs. Thus, even for a cryptocurrency like Bitcoin that should not itself be regulated, there is this paradox: to succeed, these structures currently seem to require financial intermediaries to function optimally and those intermediaries create the very agency problems that Bitcoin is designed to avoid.

IV. DECENTRALIZING THE ECOSYSTEM OF DECENTRALIZED CRYPTOCURRENCIES

One possible way out of the paradox is to develop financial institutions, like exchanges, that do not resemble the financial intermediaries of old because, like Bitcoin, they themselves are radically decentralized in their control. Such decentralized organizations could be a community organized around a blockchain and smart contracts.[23] All the decisions of such a blockchain would depend on consensus rules and the smart contracts that are run on them. Smart contracts automatically execute agreements without the need for human decision-making

---

20 *See* Paige Tortorelli & Kate Rooney, *Sam Bankman-Fried's Alameda Quietly Used FTX Customer Funds for Trading, Says Sources*, CNBC (Nov. 14, 2022, 8:08 AM) http://www.cnbc.com/2022/11/13/sam-bankman-frieds-alameda-quietly-used-ftx-customer-funds-without-raising-alarm-bells-say-sources.html [http://perma.cc/FDL8-TS5W].

21 *See* Vildana Hajric, *With Its Volatility on the Decline, Is Bitcoin Fading Away or Just Maturing?*, L.A. TIMES (Oct. 5, 2018, 3:55 PM), http://www.latimes.com/business/la-fi-bitcoin-volatility-20181005-story.html [http://perma.cc/M33J-W6MG].

22 *See* Self-Regulatory Organizations; Bats BZX Exchange, Inc., Exchange Act Release No. 34-83723, 2018 WL 3596768 (July 26, 2018).

23 *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 29 (2018).

when a set of preconditions are met.[24] I believe that we can expect more such entities acting as exchanges and other financial intermediaries. The costs of decentralization are likely to continue to fall, being driven down by advances in computation and cryptography.

This structure is a new form of corporate governance—a digital instantiation of the idea that the corporation is ultimately a nexus of contracts.[25] It eliminates the need for the managers. It thus also gets rid of the agency costs between shareholders and managers that beset corporate governance.[26] But the particular need for regulation of financial intermediaries generally focuses on the agency costs between customers, like depositors, because a financial institution does not bring together only investors and managers, but also financial asset holders of various kinds.

The hope is that such entities running on the blockchain will reduce or even eliminate the agency costs to which financial intermediaries are peculiarly subject. The argument for their ability to reduce such agency costs derives from the kind of rules under which they operate. They are consensus made and thus impervious to rapid change. Moreover, the contracts which execute their operations are transparent or can be made so. Thus, anyone dealing with the intermediary can know just what the blockchain-run intermediary can and cannot do with their money. They will then reduce or perhaps eliminate the opportunism inherent in more centralized financial intermediaries. They will have extended the range of the pure and spontaneous order of the market at the expense of hierarchical organizations that formed traditional intermediaries.[27]

But what about the incentives to create such platforms or exchanges? Few people are likely willing to set up or, to be more precise, be the coordinator of the consensus rules for nothing. The most obvious way for a founder of such a platform to be compensated is to create some token that is used for payment of transactions on the site. Assuming the platform is successful, that token will become more valuable. But, as I will discuss in more detail below, the law likely regards such tokens as

---

24 *See id.*

25 *See, e.g.*, Frank H. Easterbrook & Daniel R. Fischel, *Corporate Control Transactions*, 91 YALE L. J. 698 (1981).

26 *See* Manuel A. Utset, *Towards a Bargaining Theory of the Firm*, 80 CORNELL L. REV. 540, 553–54 (1995).

27 Sinclair Davidson et al., *Economics of Blockchain*, SSRN 1, 2–7 (Mar. 8, 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751 [http://perma.cc/A8CR-X4JA].

securities and regulates them because they create agency costs between the seller and buyer of the token. The buyer is dependent for the value of the token on the actions of the seller in coordinating the establishment of the blockchain and its rules. Now perhaps the answer to this difficulty is that while the initial offering may be regulated, it will cease to be so if the token becomes widely held and if its value no longer depends on the actions of the seller, but only on the transparent consensus rules of the blockchain.[28]

Another possible counterargument is that these rules can be transparent, yet very complex. Calculating their effects could require substantial knowledge and expense. It may be that even in the best case, such blockchains would thus not completely eliminate agency costs, particularly for less sophisticated holders of financial assets. But as the cost of computation falls, services would develop that would make it easier for everyone to predict the effects of the rules. Thus, in my view, the jury is still out on whether the ecosystem for cryptocurrencies can itself be decentralized in a manner that will radically reduce, if not eliminate, the agency costs that justify the peculiar regulation of financial intermediaries.

V. CRYPTO THAT IS PART OF A CENTRALIZED FINANCIAL INTERMEDIARY

So far, we have looked at crypto that is decentralized and the centralized intermediaries that deal in crypto. There are also financial intermediaries that are constituted by crypto, but themselves remain centralized financial intermediaries. Such intermediaries and the crypto assets they use, while they may be labeled as crypto finance, should be regulated because, unlike Bitcoin, they raise the agency cost problems of traditional financial intermediaries.

---

28 The possibility that a token may cease to become a security is recognized by the test that M. Todd Henderson and Max Raskin propose to determine whether a token is a security. *See* M. Todd Henderson & Max Raskin, *A Regulatory Classification of Digital Assets: Toward an Operational Howey Test for Cryptocurrencies, ICOs, and Other Digital Assets*, 2019 COLUM. BUS. L. REV. 443, 460–62 (2019). They offer the so-called "Bahamas Test" that asks whether a token has become sufficiently decentralized such that it is no longer dependent on the managerial actions of actors, like a founder. *Id.*

A. Initial Coin Offerings

For instance, some firms try to fund themselves through what are called initial coin offerings or ICOs.[29] These security tokens attempt to raise money for some enterprise by selling tokens that can be redeemed from those using services, functions, or utilities on the blockchain.[30]

It is clear that the buyer of a security token has a principal-agent relation with the issuer. To realize the value of the token, like the value of a security, the buyer is dependent upon the issuer—the agent—for fulfilling its promises. In securities law, the question of whether the relation creates an investment contract subject to federal securities law turns on the *Howey* test.[31] That test has been seen to contain four elements.[32] First, there must be an investment of money.[33] Second, the investment of money must be in common enterprise.[34] Third, there must be an expectation of profit.[35] Fourth, that expectation must depend on the enterprise of others.[36]

Bitcoin does not qualify as a security as the Securities and Exchange Commission itself recognizes.[37] Bitcoin is no more a common investment enterprise than any other currency. Its value does not now depend on any promoter or set of promoters. Instead, Bitcoins are paid for by those who verify the blockchain—a very decentralized group.[38]

But those who engage in initial coin offerings are holding out that the token has value either because, like a security, that token will participate in the profits of the enterprise or enable the purchase of something valuable the enterprise builds.[39] It does not follow that the details of regulating initial coin offerings must follow all of those for security offerings. It may well be that some modifications are needed but, assuming that one believes

---

29 *See* Randolph A. Robinson II, *The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings*, 85 TENN. L. REV. 897, 924–27 (2018) (describing the explosive growth in ICOs).

30 *See id.* at 925.

31 *See* SEC v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946).

32 *Id.*

33 *Id.*

34 *Id.*

35 *Id.*

36 *Id.*

37 *See* William Hinman, Dir., Div. of Corp. Fin., Sec. and Exch. Comm'n, Remarks at the Yahoo Finance All Markets Summit: Crypto (June 14, 2018), http://www.sec.gov/news/speech/speech-hinman-061418 [http://perma.cc/WM5G-4XWP].

38 *See* Henderson & Raskin, *supra* note 28, at 470–71.

39 *See* Carol Goforth, *Securities Treatment of Tokenized Offerings Under U.S. Law*, 46 PEPP. L. REV. 405, 434 n. 194 (2019).

securities regulation is justified, there is no reason not to apply regulation similar in concept to security tokens.

B. Stablecoins

Another kind of crypto—the stablecoin—is also a new kind of financial intermediary. Stablecoins are digital assets like Bitcoin, but their value derives from being backed by other assets.[40] The assets backing the stablecoin may in fact be traditional fiat currency like the dollar.[41] Others are backed by other digital assets or a basket of digital assets.[42] The stablecoin can then be traded digitally or used to purchase assets like other cryptocurrencies.[43]

Stablecoins are financial intermediaries. Insofar as they are controlled by companies or individuals, they are not decentralized financial intermediaries like Bitcoin. It is the company or individuals who make the decisions about what assets and what amounts of assets to back the stablecoin. Those using the stablecoins depend on these representations for their confidence in the stablecoins' value. Much of the controversies about stablecoins revolve around whether that confidence is justified. Some issuers of stablecoins have engaged third-party audits to increase that confidence.[44] That effort underscores their agency cost problem as does the continued skepticism about some of the audits.

Stablecoins in fact resemble the private bank notes that were issued in the nineteenth century. These banks also created money issued by private intermediaries.[45] Some of those private banks did not have sufficient backing in gold or other assets to repay depositors.[46] That is essentially the same problem facing stablecoins that have gotten them into trouble. Unlike Bitcoin itself, stablecoins are not a new mechanism for trust. It does not follow that they are a worse mechanism than public fiat money. Just as there remains a debate about how problematic private currency was

---

40 *See* ESWAR S. PRASAD, THE FUTURE OF MONEY: HOW THE DIGITAL REVOLUTION IS TRANSFORMING CURRENCIES AND FINANCE 155 (2021).

41 *See id.*

42 *See id.*

43 *See id.*

44 *See, e.g.*, Oluwapelumi Adejumo, *Third Party Auditor Confirms Binance Bitcoin Reserve is Over Collateralized*, CRYPTOSLATE (Dec. 7, 2022, 3:05 PM), http://cryptoslate.com/third-party-auditor-confirms-binance-bitcoin-reserve-is-over-collateralized/ [http://perma.cc/K4RW-CPPX].

45 *See* LAWRENCE H. WHITE, COMPETITION AND CURRENCY: ESSAYS ON FREE BANKING AND MONEY 31–34 (1989).

46 *See* Shirley J. Gedeon, *The Modern Free Banking School: A Review*, 31 J. ECON. ISSUES 209, 220 (1997).

in the nineteenth century, there will likely develop a similar debate today about the virtues of stablecoins versus fiat currency.

The reasons for that debate will be similar. Even if stablecoins have agency costs and thus reasons for distrust, so does government money. The best way to understand how great that distrust may become in the modern era is to describe yet another kind of digital asset—this one minted and controlled by the government.

VI. CENTRAL BANK DIGITAL CURRENCY AND THE SECOND PARADOX OF CRYPTO

Now let me turn to the final paradox of crypto. While crypto began as a libertarian movement to free people's financial affairs from the state, now the government may be getting into the digital asset game with central bank digital currency ("CBDC"). Cryptocurrency does not necessarily need to be private. Governments could issue their own digital currency—dollars, euros, and renminbi could all become digital, available to everyone, and even eventually the exclusive form of the government's currency.[47] The rise of CBDCs would provide a dramatic counterpoint to the libertarian vision of cryptocurrency. The form will be digital, but the trust required will still be in the government.

Central banks may well adopt cryptocurrencies that are available to consumers because they have other advantages over paper money, particularly from the viewpoint of the state. For instance, they allow governments to track the use to which the money is put because the government keeps the ledger of transactions.[48] As a result, they inhibit black markets and criminal activity facilitated by cash.

CBDCs also permit central banks to manage monetary policy more effectively. For instance, CBDCs would allow a central bank to break through what central bankers regard as the zero rate interest boundary.[49] Currently, central banks cannot create negative interest rates easily because if banks are forced to charge citizens for holding their nation's money, citizens will take their money out of banks and hold it under the mattress or perhaps in a more secure personal vault. But if all currency is digital, the

47 *See* PRASAD, *supra* note 40, at 194–95. There would also be a more limited kind of CBDC available only to banks—a wholesale, as it were, CBDC as opposed to a retail CBDC. *See id.* This more limited form would not have the dramatic implications described here. *See id.* at 195.

48 *See id.* at 217.

49 *See id.* at 204.

central bank can itself reduce the absolute value of people's money over time by varying the algorithm that creates the money.

According to some economists, CBDCs also increase the effectiveness of the tools of fiscal policy by allowing the government to target economic stimulus more effectively. With CBDCs, the government could distribute money with an algorithm that would make it valueless unless it is spent within a certain time or for certain kinds of transactions.[50]

But simply stating these "advantages" shows how government digital cryptocurrencies might provide enormous new powers to the state. The central bank could potentially track all your purchases. It could reduce even the nominal value of your money. It could tell you what you are permitted to buy. The state might become a monetary panopticon and a potential central controller of a citizen's economic life. If one trusts the government, it will use these powers benevolently. But there are agency costs for the government as well. Public choice theories show that citizens, because of ignorance, both rational and otherwise, very imperfectly control the state.

A CBDC thus confirms the worst libertarian fears of those who launched private cryptocurrency. Given that a CBDC would give the government so much more power, CBDCs would require even more trust in the government—a trust that is hard to justify. Even the past performance of the Fed has made many people wary of giving it power. For instance, the current value of the dollar is only three percent of what it was when the Federal Reserve was founded.[51] Moreover, trust in the government in general is falling and that decline also affects the Fed.

As a result, there is yet another paradox in the crypto space that would be raised by the introduction of CBDCs. They are being conceived in large measure to mirror and compete with private cryptocurrencies. But, because they may threaten to empower the state in ways that many individuals fear, their effect may cause citizens to flee from fiat currency to private crypto. They may improve the prospects that private cryptocurrency, rather than government cryptocurrency, will ultimately govern our monetary world.

---

50 *See id.* at 222–24.

51 *See Consumer Price Index for All Urban Consumers: Purchasing Power of the Consumer Dollar in U.S. City Average*, FED. RSRV. BANK OF ST. LOUIS (Mar. 14, 2023), http://fred.stlouisfed.org/series/CUUR0000SA0R [http://perma.cc/933Y-EF2C].

Thus, we may witness a grand competition between government and private cryptocurrency. The digital age has not guaranteed a victory for private currency so much as set up another fierce battle between private and public ordering between the collective force of the state and the innovation of human genius.

CONCLUSION

The internet began in 1983.[52] For its first fifteen years, it had relatively limited effects on the economy and our lives. But its importance has grown exponentially so that people today spend much of their lives online. The introduction of Bitcoin—the big bang of crypto—happened less than fifteen years ago. Since then, there has been a profusion of many kinds of crypto, a kind of Cambrian explosion in the monetary and investment space. It still has yet to dominate our financial lives as the internet does our personal lives.

But assume, as I do, that Blockchain is to value as the internet is to information—a mechanism for increasing the efficiency of its exchange—then we just need to give it time. In this talk, I have tried to lay out two of the paradoxes that will accompany its growth and whose resolution will determine its success.

---

[52] *See A Brief History of the Internet*, UNIV. SYS. OF GA., http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:~:text=January%201%2C%201983%20is%20considered,Protocol%20(TCP%2FIP) [http://perma.cc/KS9H-7YN3] (last visited Mar. 15, 2023).