

Why the U.S. Should Reject Central Bank Digital Currencies (CBDCs)

Preserving the American Model of Political Economy Against Growing State Control
of Economic Life

Natalie Smolenski, PhD
with Dan Held

Table of Contents

<u>A CHINESE CENTURY?</u>	2
<u>AN OVERVIEW OF CBDCS</u>	13
PROGRAMMABLE CASH	16
ELIMINATION OF PHYSICAL CASH	18
<u>STRUCTURAL PROBLEMS WITH CBDCS</u>	21
CONTRACTION OF COMMERCIAL BANKING	21
PENALIZATION OF LOW-INCOME HOUSEHOLDS	21
GOVERNMENTS ARE NOT TECHNOLOGY SERVICE PROVIDERS	22
SECURITY RISK	23
CENTRALIZED BLOCKCHAINS: AN OXYMORON?	24
<u>ALTERNATIVES TO CBDCS</u>	27
THE U.S. DOLLAR IS ALREADY DIGITAL	27
BITCOIN	28
STABLECOINS	39
<u>CONCLUSION</u>	45

A Chinese Century?

The 20th century has been called “The American Century” as a result of America’s global projection of political power and cultural influence. It is not an exaggeration to suggest that the 21st century is shaping up to be “The Chinese Century” for similar reasons. Of course, China’s modes of power projection—and its foreign policy objectives—differ in significant ways from those of the United States. However, it should go without saying that there is more than one way to establish military, economic, or cultural hegemony.

The growing power of China has highlighted the appeal of what we call “The Chinese Model” of political economy—a model where a strong state takes responsibility for directing the social and economic destiny of populations at scale. While China has not made exporting this model to other countries a central part of its geopolitical strategy, China’s success as the world’s leading exporter, its rapid GDP growth and improvements in standard of living, its military strength and its increasing ownership of hard assets worldwide have unquestionably made it a success story with significant appeal and material purchase. Accordingly, China’s influence is likely to grow rapidly in the coming decades.

This poses a challenge to America’s presumptions about the self-evidence of the superiority of its model of political economy, which emphasizes the need to check state power by separating and federating it. After the end of the Cold War, the belief was widespread in the United States that the world had reached “the end of history”: liberal democracy and free market capitalism would henceforth prevail globally, forever. In the ensuing decades, however, this assumption has proved to be manifestly incorrect. Today, “the American Model” of political economy no longer carries the global appeal it once did. Even within the United States, support for this model has been contentious at best. Recent research suggests that today only 3.5-11.7% of Americans, regardless of party and ideological persuasion, are willing to *not* vote for candidates they like—for reasons of policy or identity—who also undermine democratic norms.¹ In an electoral democracy, of course, the main way to meaningfully punish elected office holders for unacceptable conduct is to not vote for them. The fact that so few Americans appear willing to use this remedy suggests that American democracy may be poised to unravel in part as a result of the electoral model of democracy itself.

¹ Graham, Matthew H. and Milan W. Svobik. “Democracy in America? Partisanship, Polarization, and the Robustness of Support for Democracy in the United States.” *American Political Science Review*, Vol. 114, No. 2, pp.392-409. <https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/6/1038/files/2020/06/Graham-and-Svobik-2020-APSR.pdf>.

In addition, trust in the American federal government has dropped sharply since the mid-20th century; despite this, majorities in both parties want government to play a “major” role in addressing many social and economic problems.² A broad social consensus is forming that the federal government should break up large companies; raise the minimum wage; impose a wealth tax on billionaires; provide universal childcare; and significantly invest in education, public infrastructure, clean energy, and manufacturing.³ Conversely, however, most Americans also believe that the federal government has too much power, while a plurality say that government regulates businesses too much.⁴ Political partisans tend to shift their perception of whether these statements are true based on which party is in power, but the overall trends remain strong. In other words, Americans’ commitments to both liberal democracy and free markets persist abstractly, but in practice they are highly situational, depending on both social context (i.e., whether there is a recession, a pandemic, or a terrorist threat) and which politician or political party is in power.

Perhaps the most concise summary of this state of affairs is that most Americans want “good” government, but *actual* government never seems to live up to their ideal of the good. One response to this conundrum is to continue to expand the scope of authority for the government and campaign for “good” leaders to run it. That seems to be the prevailing response; but, as we have seen, it has done little to restore trust in government as such, a trust which continues to plummet despite the election of what one faction or another considers “good” leadership.⁵

The early American political project emerged from a model of political economy that posited, quite simply, that the human beings who run governments should not be trusted. Not because any particular politician is or is not a “trustworthy” person as such, but because those with power inevitably abuse it. As David Hume, an influential Enlightenment-era political theorist, wrote in 1777: “It is, therefore, a just *political* maxim, *that every man must be supposed a knave*: Though at the same time, it appears somewhat strange, that a maxim should be true in *politics*, which is false in *fact*.”⁶ In other words, in the view of America’s founding generation, the best form of government is

² Pew Research Center, “Americans See Broad Responsibilities for Government; Little Change Since 2019.” May 17, 2021. <https://www.pewresearch.org/politics/2021/05/17/americans-see-broad-responsibilities-for-government-little-change-since-2019/>.

³ N.A., “The Free Market is Dead: What Will Replace It?” *Time*, April 26, 2021. <https://time.com/5956255/free-market-is-dead/>.

⁴ Jeffrey M. Jones, “Americans Revert to Favoring Reduced Government Role.” *Gallup*, Oct. 14, 2021. <https://news.gallup.com/poll/355838/americans-revert-favoring-reduced-government-role.aspx>.

⁵ Pew Research Center, “Americans See Broad Responsibilities for Government.”

⁶ Hume, David. “Of the Independency of Parliament.” In Eugene F. Miller (ed.), *Essays: Moral, Political, and Literary*. Essay VI, pp. 42-46. Indianapolis, IN: Liberty Fund, Inc., 1985 [1777]. pp. 42-43.

characterized by institutions that minimize the trust required in government officials, even if these officials are themselves trustworthy in their personal capacity.

For Hume and other Enlightenment-era political theorists, one of the primary areas where the government of their time had compromised its trustworthiness was by over-regulating individual economic activity. They argued that state control of private transacting is both inimical to political liberty and slows the engine of economic growth. We suggest that historical evidence has borne out their thesis. Insofar as the U.S. government has honored the individual freedom to transact, it has enabled the generation of business models and technologies that are now engines of economic prosperity even in countries where state-led economies are the norm.⁷ In other words, when a political jurisdiction anywhere in the world enables individual economic freedom, countries across the world stand to benefit, regardless of their political-economic models.

This historical argument is not unique to our era. Indeed, the rise of self-governing cities and national parliaments in Western Europe after 1200 CE were critical for fostering zones of “economic liberty” that had spillover effects into more authoritarian, monarchical European jurisdictions.⁸ A regional emphasis on free trade also created a significant competitive impetus to discover new, direct trade routes that were not already controlled by established merchant networks. This, in turn, led to advances in seafaring, which spurred discoveries like the Cape trade route by Vasco Da Gama (the circumnavigation of Africa via the Cape of Good Hope). It is difficult to overstate the magnitude of this globally disruptive event, which disintermediated major medieval trade hubs including Venice, Genoa, Aleppo, Cairo, and Mecca, giving Western Europe direct access to the ports of the Far East.⁹ Simultaneously, the discovery of the New World and the establishment of the Columbian trade created pathways for prosperity for Western Europe without historical precedent—and gave rise to the centuries-long struggle by conquered and enslaved populations to establish liberties for themselves that mirrored those enjoyed by the colonial classes.

The freedom to transact is not, therefore, an American invention or the exclusive purview of Americans—it is central to theories of political economy developed by intellectual founders like Hume,

⁷ Baldwin, Richard. *The Great Convergence: Information Technology and the New Globalization*. Cambridge, MA: Belknap Press, 2016.

⁸ Cox, Gary W. “Political Institutions, Economic Liberty, and the Great Divergence.” *The Journal of Economic History*, Vol. 77, No. 3 (Sep. 2017). <https://www.cambridge.org/core/journals/journal-of-economic-history/article/political-institutions-economic-liberty-and-the-great-divergence/BF095246D91A9729C1A575B9A6706C95>.

⁹ Blaydes, Lisa and Christopher Paik. “Muslim Trade and City Growth before the 19th Century: Comparative Urbanization in Europe, the Middle East and Central Asia.” *British Journal of Political Science*, Vol. 51, No. 2, April 2021, pp. 845 - 868. [https://leitner.yale.edu/sites/default/files/files/blaydes_paik%20\(002\).pdf](https://leitner.yale.edu/sites/default/files/files/blaydes_paik%20(002).pdf).

Adam Smith, Frédéric Bastiat, Jean-Baptiste Say, John Stuart Mill, Ludwig von Mises, Friedrich Hayek, and others from across the European continent.¹⁰ There are also older intellectual traditions from other parts of the world—for example, the Islamic legal tradition—that foreground the need to restrict the state’s over-involvement in markets while encouraging free enterprise.^{11 12 13} The importance of separation between market and state therefore can be described as a project without geographic or temporal boundaries—it is a universal project. But that does not mean it enjoys *de facto* universal acceptance.

In describing the models of political economy we foreground here as “Chinese” and “American,” therefore, we refer not to their “ethnic essence” or to the personal dispositions of Chinese or American people. Rather, we refer to the nation-state empires that play highly influential roles in instantiating these models and carrying them forward in this historical moment. This distinction matters because, as information technologies continue to serve as a homogenizing force in global culture, and as jurisdictional arbitrage becomes more common, nation-states will increasingly attract and retain populations based on their models of political economy, rather than, say, their language, religion, or culture. These national models of political economy will serve as the primary material differentiators for increasingly mobile populations across the socioeconomic spectrum who are seeking a good life. Understanding the differences between approaches to political economy in various jurisdictions is therefore key to navigating the opportunities and obstacles presented by the 21st century world.

Perhaps the most salient difference, then, between Chinese and American political cultures is the centrality of the state to the Chinese political economy—both in theory and in practice. The Chinese state has been an agent of institutional continuity for thousands of years and across significant religious, economic, and cultural disruptions.¹⁴ Its pedagogy and institutional structure give it a vaunted role in ensuring the stability and harmony of economic life and social relations. This does not mean, of course, that there is no resistance to the state in China—in fact, such resistance is a cause for

¹⁰ See, for example, Boettke, Peter J. and Peter T. Leeson, eds. *The Economic Role of the State*. Cheltenham, UK: Edward Elgar Publishing Limited, 2015.

¹¹ Labib, Subhi Y. “Capitalism in Medieval Islam.” *The Journal of Economic History*, Vol. 29, No. 1. Pp. 79-96. <https://www.jstor.org/stable/2115499>.

¹² Goldberg, Jessica L. *Trade and Institutions in the Medieval Mediterranean: The Geniza Merchants and Their Business World*. Cambridge: Cambridge University Press, 2012.

¹³ Chaudhuri, K. N. *Trade and Civilisation in the Indian Ocean: An Economic History from the Rise of Islam to 1750*. Cambridge: Cambridge University Press, 1985.

¹⁴ Acemoglu, Daron and James A. Robinson. *The Narrow Corridor: States, Societies, and the Fate of Liberty*. New York: Penguin Press, 2019.

strong and ongoing concern for the state.^{15 16 17} Moreover, even in the absence of direct resistance, the Chinese government is aware of the widespread appeal of beliefs that differ from state policy and which are held silently by large percentages—if not majorities—of its population.¹⁸ Nevertheless, it is relatively uncontroversial to say that the opportunities for political contestation are narrower in China than they are in the United States, and decision-making hierarchies are clearer. China has one of the most heavily censored media environments in the world, and the government routinely intimidates journalists through tactics including libel lawsuits, arrests, detentions, and other means.¹⁹ The Chinese government has engaged in extensive efforts to censor and proxy the open internet through its “Great Firewall” initiative, which blocks many foreign and unapproved websites, including global social media platforms, either permanently or temporarily.²⁰ Approved media outlets must hew to the censorship guidelines disseminated by party leaders on a weekly basis.²¹

Perhaps the most striking illustration of Chinese state power, however, has been the rapid development of its surveillance régime. Under President Xi Jinping, who ascended to the presidency in 2013, China has become the world’s leading market for surveillance technology.²² Startups and large companies specializing in the recognition of faces, clothing, and gait share data with the Chinese government, mapping it against vast government databases of personal information to identify and arrest, fine, publicly shame, or otherwise punish not only those who have broken the law or violated social norms, but those who are deemed *likely* to do so by proprietary algorithms.²³ Ethnic minorities, migrant workers, and those with histories of mental illness are watched particularly closely.²⁴ Also explicitly monitored is a group called “petitioners”—those who file complaints about Chinese

¹⁵ Economy, Elizabeth. “30 Years After Tiananmen: Dissent Is Not Dead.” *Journal of Democracy*, Vol. 30 No. 2, 2019, pp. 57-63. *Project M.U.S.E.* doi:10.1353/jod.2019.0024.

¹⁶ Wasserstrom, Jeffrey. “Repression in Xi’s China.” *Dissent*, Winter 2021.
<https://www.dissentmagazine.org/article/repression-in-xis-china>.

¹⁷ Wong, Chun Han. “‘Their Goal Is to Make You Feel Helpless’: In Xi’s China, Little Room for Dissent.” *The Wall Street Journal*, Nov. 27, 2020. <https://www.wsj.com/articles/their-goal-is-to-make-you-feel-helpless-in-xis-china-little-room-for-dissent-11606496176>.

¹⁸ Mazzocco, Ilaria and Scott Kennedy. “Public Opinion in China: a Liberal Silent Majority?” *The Center for Strategic and International Studies (CSIS)*. Feb. 9, 2022. <https://www.csis.org/features/public-opinion-china-liberal-silent-majority>.

¹⁹ Xu, Beina and Eleanor Albert. “Media Censorship in China.” *The Council on Foreign Relations*. Feb. 17, 2017.
<https://www.cfr.org/backgrounder/media-censorship-china>.

²⁰ Xu and Albert, “Media Censorship in China.”

²¹ Xu and Albert, “Media Censorship in China.”

²² Mozur, Paul. “Inside China’s Dystopian Dreams: A.I., Shame and Lots of Cameras.” *The New York Times*. July 8, 2018.
<https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>.

²³ Mozur, Paul, Muyi Xiao and John Liu. “‘An Invisible Cage’: How China Is Policing the Future.” *The New York Times*. June 25, 2022. <https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html>.

²⁴ Mozur, Xiao and Liu, “An Invisible Cage.”

government authorities.²⁵ Basic elements of daily life—like access to one’s home or entry into local businesses—are increasingly mediated by predictive technologies like facial recognition.²⁶ In short, a panopticon has been created in which residents of China, unsure of whether or not they are being watched at any given time, increasingly self-censor and self-police. Opposition to the intensification of this predictive data dragnet by Chinese civil society has of course occurred, but it has had little effect on the overall trajectory of its build-out.²⁷

A key element of the Chinese government’s surveillance efforts has been bringing state visibility to all financial transactions that are not already observed through the digital banking system. While financial transactions that pass through banks are widely monitored in virtually all countries, physical cash remains opaque because of its anonymous nature. Accordingly, the Chinese government has spearheaded the creation and deployment of a central bank digital currency, or CBDC. The People’s Bank of China, the country’s central bank, has been researching and developing a CBDC—the digital yuan, or e-CNY—since 2014.²⁸ The digital yuan uses a state-run, private blockchain network to issue digital cash that is a direct liability of the Chinese central bank. This network records all transactions made with its native digital asset. As of mid-2022, the digital yuan has been [successfully piloted in several](#) major Chinese cities and is poised for a national rollout.^{29 30}

Yet the reality is that China is far from the only country on path to implement a CBDC—or a surveillance state, for that matter. Indeed, many Chinese surveillance companies use technology developed in the United States and Europe.³¹ The United States government’s Office of the Director of National Intelligence regularly holds open competitions for facial recognition algorithms, some of which have been won by Chinese companies.³² [Predictive policing](#) is already widespread in U.S. cities, although U.S. government officials tend to be quieter about its implementation than do their Chinese

²⁵ Mozur, Xiao and Liu, “An Invisible Cage.”

²⁶ Mozur, Paul and Aaron Krolik. “A Surveillance Net Blankets China’s Cities, Giving Police Vast Powers.” *The New York Times*. Dec. 17, 2019. <https://www.nytimes.com/2019/12/17/technology/china-surveillance.html>.

²⁷ Mozur and Krolik, “A Surveillance Net Blankets China’s Cities.”

²⁸ Working Group on E-CNY Research and Development of the People’s Bank of China. “Progress of Research & Development of E-CNY in China.” July, 2021. <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>.

²⁹ Huld, Arendse. “China Launches Digital Yuan App – All You Need to Know.” *China Briefing: from Dezan Shira and Associates*. April 13, 2022. <https://www.china-briefing.com/news/china-launches-digital-yuan-app-what-you-need-to-know/>.

³⁰ Reuters. “China central bank expands digital yuan pilot scheme to more cities.” Apr. 2, 2022.

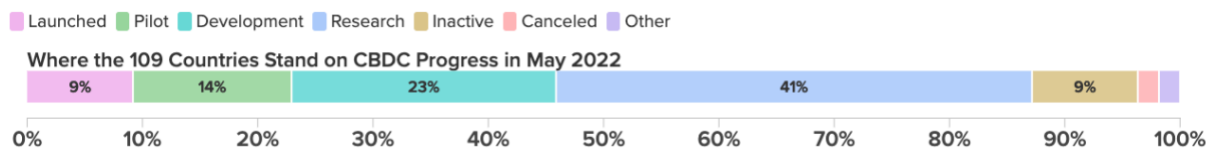
<https://www.reuters.com/world/china/china-central-bank-expands-digital-yuan-pilot-scheme-more-cities-2022-04-02/>.

³¹ Metz, Cade and Adam Satariano. “An Algorithm That Grants Freedom, or Takes It Away.” *The New York Times*. Feb. 7, 2020. <https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html>.

³² Mozur, “Inside China’s Dystopian Dreams.”

government counterparts.³³ It is a mistake, therefore, to believe that the capabilities currently being deployed by the Chinese state against its people are not already being used in the United States by both government and private industry. Indeed, the U.S. surveillance economy is only growing—and the U.S. government largely treats this as an unambiguous benefit.

In a reflection of this alignment of state interests, the U.S. Federal Reserve has partnered with the Bank for International Settlements (BIS), the “central bank of central banks,” to explore the creation of a CBDC in the United States.³⁴ The BIS itself has been conducting CBDC pilots, in partnership with the Swiss National Bank, since 2020.³⁵ In total, over 100 countries representing over 95% of global GDP were either actively exploring or had previously explored a CBDC as of May 2022,³⁶ up from 35 in May 2020. By May 2022, 10 countries had already fully launched a CBDC: these include Jamaica, The Bahamas, Nigeria, and seven countries in the Eastern Caribbean.



Source: *The Atlantic Council Geoeconomics Center.*

It may be tempting, for some, to view the acceleration of U.S. government power through the lens of “global competitiveness.” For example, the introduction of a CBDC by China has prompted concern by some American lawmakers that the U.S. is “falling behind” technologically. In a hearing of the House Subcommittee on National Security, International Development and Monetary Policy in 2021, “Rep. Jim Himes (D-CT) and Rep. Andy Barr (R-KY) both opened with concerns of ‘inaction.’” Himes wondered what time horizon of inaction would cause the U.S. to lose ‘the ability to lead and

³³ Lau, Tim. “Predictive Policing Explained.” *The Brennan Center for Justice*, Apr. 1, 2020. <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>.

³⁴ Federal Reserve Bank of New York. “New York Fed Launches the New York Innovation Center to Support Financial Technology Innovation in Central Banking.” *Press Release*, Nov. 29, 2021. <https://www.newyorkfed.org/newsevents/news/aboutthefed/2021/20211129>.

³⁵ Bank for International Settlements. “BIS, Swiss National Bank and SIX announce successful wholesale CBDC experiment.” Dec. 3, 2020. <https://www.bis.org/press/p201203.htm>.

³⁶ The Atlantic Council Geoeconomics Center. “Central Bank Digital Currency Tracker.” Accessed April 25, 2022. https://www.atlanticcouncil.org/cbdctracker/?mkt_tok=NjU5LVdaWC0wNzUAAAF-bWHdvD9F6hi9A9SE9YFXBT-EY6Ks28WZG_QGvUhbPpPQS2vJg3pLDabHqywLcbar4FapCoQNjMYSK6iUHHiPHcQgJMaAmAN8Z-V45Ui.

innovate' in the CBDC landscape."³⁷ In June of 2022, Representative Himes published a white paper arguing that the United States should quickly move forward with the implementation of a CBDC.³⁸

Yet this concern assumes that a sophisticated deployment of surveillance power by the state represents "innovation." But innovation for whom? What effect would rapid increases in state surveillance have on the ability of a country's people to generate innovation in the future? The historical record has demonstrated that government use of technologies to monitor and control populations has a chilling effect on experimentation with new technologies and business models. Quite simply, state surveillance kills economic dynamism.

The U.S. Federal Reserve has been open about the fact that any CBDC it implements must enable surveillance of all digital cash transactions. In a January 2022 white paper, the Federal Reserve stated that a U.S. CBDC would need to be fully identity-verified:

"Financial institutions in the United States are subject to robust rules that are designed to combat money laundering and the financing of terrorism. A CBDC would need to be designed to comply with these rules. In practice, this would mean that a CBDC intermediary would need to verify the identity of a person accessing CBDC, just as banks and other financial institutions currently verify the identities of their customers."³⁹

In other words, despite a push to preserve transaction anonymity from some CBDC advocates (about which more below), in practice the introduction of a U.S. CBDC would very likely spell the end of anonymous cash transactions, completing the state's visibility into the day-to-day economic life of individuals. Advocates for CBDCs maintain that this new control will only be used benevolently, with the interests of public safety and financial inclusion of the most vulnerable populations in mind. But this alleged "benevolence" of government flies in the face of the Enlightenment-era political tradition that brought about the founding of the United States: our institutions were founded on the premise that the state should not be trusted and that it should be delegated power by the people only with the

³⁷ Keely, Aislinn. "Lawmakers voice anxiety about China's digital yuan during CBDC hearing." *The Block*, Jul. 27, 2021. <https://www.theblockcrypto.com/post/112684/lawmakers-voice-anxiety-about-chinas-digital-yuan-during-cbdc-hearing>.

³⁸ Himes, Representative Jim. "Winning the Future of Money: A Proposal for a U.S. Central Bank Digital Currency." June 2022. <https://himes.house.gov/cache/files/3/d/3da9ff6d-4e8a-47b7-be28-ced21ecb5724/2F46398524B2AD91FD40BDC5263F4F23.himes-cbdc-white-paper.pdf>.

³⁹ Board of Governors of the Federal Reserve System. "Money and Payments: The U.S. Dollar in the Age of Digital Transformation." Jan. 2022. p. 14. <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>.

greatest care. The violence of the state is exercised with the greatest ease and impunity against marginalized peoples—often in the name of “helping” or “saving” them.

CBDCs represent a new conferral of powers by governments to governments, and it is taking place outside of any democratic process of deliberation, confined to the rarified gatherings of central bank leaders and other high-ranking government officials. While the Federal Reserve has requested that Congress either authorize or prevent the creation of a CBDC, the issue—and its magnitude—have not even begun to percolate into wider political discourse among the electorate, whom Congress ostensibly represents.

For this reason, we argue that “the Chinese Model” of political economy is shaping up to be the 21st century norm rather than the exception. The United States is therefore at a crossroads: shall we go the way of the rest of the world, which is adopting the Chinese model? Or will we choose a route consistent with the ideas upon which our country was founded?

What we call “the American Model” of political economy—one in which society refuses to delegate most of its inherent powers to the government—only stands a chance of preservation if we choose to preserve it. Otherwise, we will join the rest of the world in adopting a state-led political economy. That would render the United States merely a less efficient—or less honest—version of China. We would lose our most significant material differentiators and become yet another country implementing its own local version of authoritarianism. As Minnesota Representative Tom Emmer emphasized during a recent Congressional hearing:

“Any attempt to craft a central bank digital currency that enables the Fed to provide retail bank accounts and mobilizes the CBDC rails into a surveillance tool, able to collect all sorts of information on Americans, would do nothing but put the United States on par with China's digital authoritarianism.”⁴⁰

Congressman Emmer followed up his comments by introducing a bill in January 2022 that would ban Federal reserve banks from issuing a CBDC directly to individuals and maintaining accounts on their

⁴⁰ Keely, “Lawmakers voice anxiety about China's digital yuan during CBDC hearing.”

behalf.^{41 42 43} Two months later, Texas Senator Ted Cruz introduced a virtually identical companion bill in the U.S. Senate.^{44 45}

However, only a few days before Senator Cruz introduced his bill, Massachusetts Representative Stephen Lynch introduced the ECASH Act, a bill that would require the U.S. Treasury to develop a CBDC.^{46 47} The ECASH Act stipulates that the purpose of a CBDC is ostensibly to promote financial inclusion and technological innovation. However, at its heart lies a contradiction: it requires the CBDC design to both comply with full AML/KYC requirements *and* offer individuals the ability to transact anonymously. Some have attempted to resolve this seeming contradiction by designing systems that enforce AML/KYC at the point of currency issuance, but not at the point of transaction.^{48 49} However, this already departs significantly from the physical cash model, which does not entail direct issuance of cash to named individual accounts before it can be transacted.

A centralized, central bank-administered ledger that tracks currency issuance and transacting faces no significant technical obstacles to enforcing identity verification at every point of transaction. Moreover, the federal government is significantly incentivized to enforce this surveillance. As the

⁴¹ Press Release. “Emmer Introduces Legislation to Prevent Unilateral Fed Control of a U.S. Digital Currency.” *Newsroom of Congressman Tom Emmer*. Jan. 12, 2022. <https://emmer.house.gov/2022/1/emmer-introduces-legislation-to-prevent-unilateral-fed-control-of-a-u-s-digital-currency>.

⁴² “A Bill to amend the Federal Reserve Act to prohibit the Federal reserve banks from offering certain products or services directly to an individual, and for other purposes.” H.R. 6415, 117th Cong (2022). <https://emmer.house.gov/cache/files/e/3/e3f3f683-d983-4456-9f34-8ac493730582/6724255AB4BCC4F46F5F41DAE08F63BD.emmer-045-xml.pdf>.

⁴³ Press Release. “Emmer CBDC Bill Selected as FreedomWorks Bill of the Month.” *Newsroom of Congressman Tom Emmer*. Feb. 17, 2022. <https://emmer.house.gov/2022/2/emmer-cbdc-bill-selected-as-freedomworks-bill-of-the-month>.

⁴⁴ Press Release. “Sen. Cruz Introduces Legislation Prohibiting Unilateral Fed Control of a U.S. Digital Currency.” *Newsroom of Senator Ted Cruz*. Mar 30, 2022. <https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-introduces-legislation-prohibiting-unilateral-fed-control-of-a-us-digital-currency>.

⁴⁵ “A Bill to amend the Federal Reserve Act to prohibit the Federal reserve banks from offering certain products or services directly to an individual, and for other purposes.” S. 3954, 117th Cong (2022). <https://www.cruz.senate.gov/imo/media/doc/cbdc.pdf>.

⁴⁶ Press Release. “Rep. Lynch Introduces Legislation to Develop Electronic Version of U.S. Dollar.” *Newsroom of Congressman Stephen F. Lynch*. Mar. 28, 2022. <https://lynch.house.gov/press-releases?id=5A0DA9DE-8884-4E06-AC0A-BCA08850F05E>.

⁴⁷ “The Electronic Currency and Secure Hardware (ECASH) Act.” H.R. 7231, 117th Cong (2022). Mar. 28, 2022. <https://www.congress.gov/bill/117th-congress/house-bill/7231>.

⁴⁸ N.A. “U.S. legislators publish multiple CBDC Bills with privacy emphasis.” *Ledger Insights*. Apr. 1, 2022. <https://www.ledgerinsights.com/u-s-legislators-publish-multiple-cbdc-bills-with-privacy-emphasis/>.

⁴⁹ N.A. “A digital dollar CBDC may use this privacy preserving design.” *Ledger Insights*. Sep. 27, 2021. <https://www.ledgerinsights.com/a-digital-dollar-cbdc-may-use-this-privacy-preserving-design/>.

White House Office of Science and Technology Policy noted in its September 2022 report on CBDC design, developed pursuant to President Biden’s Executive Order (EO) 14067:

“Keeping some pieces of identity-related information anonymous from the central bank and intermediaries could help enable cash-like privacy for those pieces of information. This may not be possible or sensible for some pieces of sensitive identity-related information. Given that a CBDC is not subject to the same physical limitations as cash, such an approach might make it harder to identify, trace, and disrupt money laundering and the financing of terrorism and for relevant financial institutions to comply with existing AML/CFT obligations. If “no one” was the design choice chosen for many pieces of sensitive identity-related information, it may functionally provide some level of anonymity, which may complicate intermediaries’ compliance with AML/CFT obligations and may be out of line with global AML/CFT standards.”⁵⁰

In other words, those calling for the rollout of a CBDC are naïve to believe that this can be done without establishing a centralized surveillance system for all financial transacting. Quite simply, even if such surveillance is not included in the V1 system design, it would be trivial to add it at a later stage. Once a door to surveillance is opened, it is virtually impossible to close.

Central bank digital currencies are only one issue among many that raises the question of what the role of the state should be in human economic life. Nevertheless, whether or not to adopt a CBDC has now become a critical and urgent issue, for two reasons: 1) Deliberations by the Federal Reserve, the Treasury, and the Office of Science and Technology Policy as to whether or not to launch a CBDC are already well underway, with design recommendations already published and draft legislation expected from Congress by the end of 2022.⁵¹ 2) Legislation to require the introduction of a CBDC (the ECASH Act) is garnering support in Congress. 3) Technological development does not slow down; it only accelerates. As a result, the temptation for the U.S. government to use exponentially increasing surveillance power to control populations will only grow; CBDCs are only one element in an ever-tightening surveillance landscape.

⁵⁰ The Office of Science and Technology Policy (OSTP). “Technical Design Choices for a U.S. Central Bank Digital Currency System.” September 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Design-Choices-US-CBDC-System.pdf>.

⁵¹ Board of Governors of the Federal Reserve System, “Central Bank Digital Currency (CBDC).” <https://www.federalreserve.gov/central-bank-digital-currency.htm>.

Technology is a tool used to encode human values in the built environment. For this reason, we examine CBDCs as a prism through which central questions about political economy—and our values—are refracted. To illustrate how our approach to CBDCs will influence what kind of country the United States chooses to become, we will first describe what a CBDC is and how CBDCs alter the relationship between state and society. Next, we will discuss some structural problems related to the implementation of CBDCs. Finally, we will consider alternatives to CBDCs that preserve a sphere of individual economic liberty in the United States and beyond.

An Overview of CBDCs

CBDC stands for “central bank digital currency,” a digital fiat currency issued, controlled, and run by a central bank. CBDCs are direct liabilities of central banks, meaning they correspond to M0 money supply.⁵² This also means they have “no liquidity risk, no credit risk, [and] no market risk.”⁵³

In other words, CBDCs are not digital representations of fiat currencies, like the money held in online bank accounts. Account-based money is the form of digital money most people use today—it is credit money issued by commercial banks, as opposed to cash. (We will discuss existing forms of digital money in more detail below.) CBDCs are digital cash—digital versions of paper banknotes. Because cash is issued by central banks, CBDCs enable consumers to have direct relationships with central banks rather than relying on commercial banks to serve as intermediaries between the two.

Some central banks make a distinction between “wholesale CBDCs,” which facilitate inter-bank settlements, and “retail CBDCs,” which are used by consumers.⁵⁴ However, in practice, the vast majority of central banks are contemplating retail CBDCs.⁵⁵ Once a wholesale CBDC is implemented, the technological lift to extend its usability to the general public is well within reach.

⁵² Deutsche Bank. “Digital yuan: what is it and how does it work?” July 14, 2021.

<https://www.db.com/news/detail/20210714-digital-yuan-what-is-it-and-how-does-it-work>.

⁵³ Jens Weidmann. “Exploring a digital euro.” September 14, 2021.

<https://www.bundesbank.de/en/press/speeches/exploring-a-digital-euro-875408>.

⁵⁴ Bank for International Settlements. “III. CBDCs: an opportunity for the monetary system.” *BIS Annual Economic Report*, Jun. 23, 2021. <https://www.bis.org/publ/arpdf/ar2021e3.htm>.

⁵⁵ Federal Reserve Bank of Kansas City. “Assessing the Case for Retail CBDCs: central banks’ Considerations.” *Payments System Research Briefing*, May 26, 2022. <https://www.kansascityfed.org/research/payments-system-research-briefings/assessing-the-case-for-retail-cbdcs-central-banks-considerations/>.

Proponents of CBDCs emphasize their benefits for end users: now cash transactions can take place digitally, instantly, and at very low cost.⁵⁶ ⁵⁷ Intermediaries who today steward cash transactions—particularly across borders—are in effect removed, dramatically lowering friction and costs for consumers. CBDCs would also enable governments to send stimulus payments directly to citizens—even the unbanked—without the security and fraud risks of mailing paper checks.⁵⁸ But the same benefits are already available with cryptocurrencies not issued by governments—for example, with bitcoin,⁵⁹ a stateless currency whose value floats freely in a 24-hour market, or with stablecoins, privately-issued currencies whose value is pegged to that of a fiat currency (similar to the eurodollar system, which has been in operation globally since the late 1950s⁶⁰). Indeed, the rationales stated by central banks themselves for implementing CBDCs⁶¹ are already well covered by bitcoin and stablecoins, as we shall see below.

If alternatives that achieve the same objectives are already available, why are so many governments interested in the creation of CBDCs? This paper argues that there are two main reasons: First, CBDCs grant governments complete surveillance and control over the last remaining sphere of financial transactions that has eluded them: cash transactions. Second, governments are deeply in debt, and they need money to pay down that debt. Since raising taxes is politically unpalatable, central banks are turning to their control over monetary policy to generate revenue for the state. CBDCs afford a new technological avenue to achieve this objective. We will first discuss this second reason governments are pursuing CBDCs, before moving on to the first.

Central banks took on unprecedented levels of debt during the COVID-19 pandemic—a crisis that only accelerated the general trend of rising sovereign debt that has been ongoing since the mid-20th

⁵⁶ Board of Governors of the Federal Reserve System, “Money and Payments.”

⁵⁷ Himes, “Winning the Future of Money.”

⁵⁸ Prasad, Eswar. “Cash Will Soon Be Obsolete. Will America Be Ready?” *The New York Times*, Jul. 22, 2021. <https://www.nytimes.com/2021/07/22/opinion/cash-digital-currency-central-bank.html>.

⁵⁹ Bitcoin is both a network for final settlement and a digital currency. When referred to primarily as a network or protocol, Bitcoin will be capitalized. When referred to primarily as a currency, bitcoin will be lowercase.

⁶⁰ Schenk, Catherine R. “The Origins of the Eurodollar Market in London: 1955–1963.” *Explorations in Economic History*, Vol. 35, pp. 221-238. 1998. https://www.sfu.ca/~poitras/EEH_Eurodollar_98.pdf.

⁶¹ Federal Reserve Bank of Kansas City. “Assessing the Case for Retail CBDCs: Central Banks’ Considerations.” *Payments System Research Briefing*, May 26, 2022. <https://www.kansascityfed.org/research/payments-system-research-briefings/assessing-the-case-for-retail-cbdcs-central-banks-considerations/>.

century.⁶² ⁶³ Global debt-to-GDP ratio had risen to an extraordinary 356% by the end of 2021, with 30% of the increase occurring since 2016.⁶⁴ As of mid-2021, rapid increases in sovereign debt had already driven several countries into sovereign default and placed dozens of others on the brink.⁶⁵ Even countries that are structurally more solvent because their debt is denominated in their own currencies, like the United States, the United Kingdom, Japan, and China, are concerned about the negative economic effects of ballooning debt. These include distorted supply and demand balances that indirectly undermine growth; defensive measures taken by industry to protect itself from having to absorb the costs of sovereign debt (which also negatively impacts growth); the creation of fictional growth via asset bubbles; and looming financial and political crises.⁶⁶

In short, governments need money, fast. As we will see, CBDCs represent an opportunity to extract it from private cash holdings. Once the technological infrastructure is put in place to realize this purpose of a CBDC, however, governments can use the same technology for another purpose: to dramatically increase surveillance and control of everyday behavior at population scale. Surveillance can be used to micromanage human behavior by tying government services and other benefits to “pro-social” behavior (as defined by the state) while penalizing “anti-social” behavior. Such programs have already been implemented in China and are collectively referred to as the “social credit system.”⁶⁷ But China’s example is only the most explicit of a much broader worldwide trend crossing both public and private sectors: surveillance capitalism, a term describing a political economy in which profits for private actors and compliance for governments are generated by monitoring and influencing human behavior both at the individual level and at the level of human collectives.⁶⁸

⁶² M. Ayhan Kose, Peter Nagle, Franziska Ohnsorge, and Naotaka Sugawara, “Debt tsunami of the pandemic.” *The Brookings Institute*. December 17, 2021. <https://www.brookings.edu/blog/future-development/2021/12/17/debt-tsunami-of-the-pandemic/>.

⁶³ See remarks by Kristalina Georgieva, Managing Director of the International Monetary Fund, in “IMF Seminar: Debate on the Global Economy.” *International Monetary Fund and World Bank Group Spring Meetings 2022*. April 21, 2022. <https://meetings.imf.org/en/2022/spring/schedule/2022/04/21/imf-seminar-debate-on-the-global-economy>.

⁶⁴ Pettis, Michael. “How Does Excessive Debt Hurt an Economy?” *Carnegie Endowment for International Peace*, Feb. 8, 2022. <https://carnegieendowment.org/chinafinancialmarkets/86397>.

⁶⁵ The Congressional Research Service, “Sovereign Debt and the COVID-19 Pandemic.” July 16, 2021. <https://sgp.fas.org/crs/row/IF11880.pdf>.

⁶⁶ Pettis, “How Does Excessive Debt Hurt an Economy?”

⁶⁷ Kobie, Nicole. “The complicated truth about China’s social credit system.” *Wired UK*, Jul. 6, 2019. <https://www.wired.co.uk/article/china-social-credit-system-explained>.

⁶⁸ Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs, 2019.

Programmable Cash

CBDCs are digital cash. Unlike traditional (physical) cash, which can be transacted anonymously, digital cash is fully programmable. This means that CBDCs enable central banks to have direct insight into the identities of transacting parties and can block or censor any transaction. Central banks argue that they need this power in order to combat money laundering, fraud, terrorist financing, and other criminal activities.^{69 70} But as we will see below, the ability of governments to meaningfully combat financial crimes using existing anti-money laundering and know your customer laws (“AML/KYC”) has proven woefully inadequate, at best, while effectively eliminating financial privacy for billions of people.

The ability to block and censor transactions also implies its opposite: the ability to require or incentivize transactions. A CBDC could be programmed to only be spendable at certain retailers or service providers, at certain times, by certain people. The government could maintain lists of “preferred providers” to encourage spending with certain companies over others and “discouraged providers” to punish spending with others. In other words, with a CBDC, cash effectively becomes a state-issued token, like a food stamp, that can only be spent under predefined conditions. Means testing could be built into every transaction.

But censoring, discouraging, and incentivizing transactions are not the only powers available to central banks with programmable cash. Banks can also disincentivize saving—holding digital cash—by capping cash balances (as the Bahamas have already done for their CBDC)⁷¹ or by imposing “penalty” (negative) interest rates on balances over a certain amount.^{72 73} This can be used to prevent consumers from converting too much of their M1 or M2 bank balances—credit money issued to them by commercial banks—into cash (M0). After all, if too many people rush to demand cash (hard money) at once, commercial banks will be deprived of funding and may dramatically reduce their lending if they can’t find other sources of capital. Central banks understandably wish to prevent these “credit crunches,” which often result in economic recessions or depressions. However, their policy interventions also deprive people of access to M0 currency—the hardest and safest form of money

⁶⁹ Gertjan Vlieghe, “Running out of room: revisiting the 3D perspective on low interest rates.” *Bank of England*. Speech delivered at the London School of Economics, Jul. 26, 2021.

<https://www.bankofengland.co.uk/speech/2021/july/gertjan-vlieghe-speech-at-the-london-school-of-economics?sf148018825=1>.

⁷⁰ Weidmann, “Exploring a digital euro.”

⁷¹ Central Bank of The Bahamas, “Project Sand Dollar: A Bahamas Payments System Modernisation Initiative.” Dec. 24, 2019. <https://www.centralbankbahamas.com/viewPDF/documents/2019-12-25-02-18-11-Project-Sanddollar.pdf>.

⁷² Vlieghe, “Running out of room.”

⁷³ Weidmann, “Exploring a digital euro.”

under a fiat currency regime—leaving billions of people, especially the poorest, without recourse in the event of monetary crises.

Of course, negative interest rates can be imposed by central banks on *all* cash holdings, not only balances over a certain amount.⁷⁴ While the objective of imposing negative interest rates is, again, to prevent recessions by stimulating near-term consumer spending, this objective is achieved at the cost of accelerating the destruction of private wealth. We can take the world’s current economic situation as an example. Central banks intervened during the COVID-19 pandemic to prevent recession by monetizing growing levels of sovereign debt, which flooded markets with fiat money. This has resulted in more money chasing fewer assets, a reliable recipe for inflation. The world is therefore seeing the highest sustained global rates of inflation in 20 years, with some countries experiencing rates much higher than the global average.⁷⁵ Inflation already incentivizes spending, because people understand that their money is worth more today than it will be tomorrow. By implementing negative interest rates, central banks further erode the value of people’s savings, creating a perverse incentive for them to spend their already-dwindling resources even faster. This vicious cycle does not end in economic prosperity, but in a collapse of the currency.

While penalty and generalized negative interest rates are both methods central banks can use to incrementally confiscate money from individuals and private organizations, these are not the only methods available to them. Once CBDCs are implemented, there is nothing technically or legally preventing central banks from imposing direct haircuts on, or repossessions of, anyone’s cash holdings, anywhere in the world. Central banks could directly confiscate private digital cash to pay down their sovereign debt, to discourage the use of digital cash, to decrease the money supply, or for any other reason. Although this possibility has not been openly discussed, it is built into the political and technical architectures of CBDCs.

Finally, central banks can programmatically require tax payments for every CBDC transaction. Some economists have argued that this measure is necessary to recover tax revenue that is sometimes avoided when physical cash is used, and then rather optimistically note that governments could take advantage of the recovered tax revenue to lower effective tax rates.⁷⁶ However, there is no indication that revenue-strapped governments already incentivized to harvest private wealth would take any measures to lower

⁷⁴ James Mackintosh. “Digital Currencies Pave Way for Deeply Negative Interest Rates.” *Wall Street Journal*. Sep. 8, 2021. <https://www.wsj.com/articles/digital-currencies-pave-way-for-deeply-negative-interest-rates-11631091581>.

⁷⁵ Carmen Reinhart and Clemens Graf von Luckner, “The Return of Global Inflation.” *World Bank Blogs*. Feb. 14, 2022. <https://blogs.worldbank.org/voices/return-global-inflation>.

⁷⁶ Leigh Beeson, “Eliminating cash could benefit average U.S. families.” *UGA Today*, September 7, 2021. <https://news.uga.edu/eliminating-cash-could-benefit-average-u-s-families/>.

taxes. Instead, CBDCs will most likely be used to generate additional tax revenue for the state at onerous cost to individuals.

Imagine: with mandatory taxation on every CBDC transaction, you would be taxed for giving your neighbor \$20, or giving your children an allowance, or for every item you sell at a yard sale. A person paying their friend \$50 to change a tire or \$100 to look after their home while they are away would be taxed for these activities. This “informal” economy is not only a necessary mode of intimate interpersonal relating, but a lifeblood for millions of people who rely on it to survive day to day. It is morally unfathomable to imagine a homeless person selling flowers on the street being taxed for every transaction.

Summary

- Retail CBDCs are programmable cash.
- Programmable cash gives central banks direct relationships with consumers.
- Direct relationships between central banks and consumers enable central banks to:
 - Surveil all financial transactions
 - Flag, block or reverse any transaction at any time
 - Determine how much cash anyone can hold and transact with
 - Determine what products and services cash can be used to buy, and by whom
 - Directly implement monetary policy (like negative interest rates) at the level of private cash holdings
 - Confiscate privately held cash
 - Enforce tax collection on every cash transaction, no matter how small

Elimination of Physical Cash

At this point, one might ask: if such measures are enacted, wouldn't people simply hoard physical cash? Governments have anticipated this possibility, which is why a growing number of central banks are openly working toward the elimination of physical cash.⁷⁷ The publicly stated rationale for eliminating cash is prevention of fraud and money laundering—the same reason central banks have given for tying the identities of real people and organizations to every financial transaction. This process, referred to under the umbrella term “anti-money laundering and know your customer” (AML/KYC), would extend to every holder of cash laws that currently force banks to identify their customers.

⁷⁷ Adam Hayes, “Why Governments Want to Eliminate Cash.” *Investopedia*. July 21, 2021.
<https://www.investopedia.com/articles/investing/021816/why-governments-want-eliminate-cash.asp>.

In other words, with both the imposition of CBDCs and the elimination of physical cash, the ability to anonymously transact will also be eliminated. This destruction of the last remnants of financial privacy is touted by governments as necessary to prevent financial crimes. But the world's experience implementing AML/KYC laws suggests that identifying parties to a transaction has almost no effect on preventing crime, for a number of reasons. First, wealthy criminals are lucrative customers for banks, who are therefore incentivized to keep them; second, wealthy criminals are able to threaten or otherwise coerce governments. Most importantly, however, corporate privacy laws make it easy to create shell companies through which to launder money in a manner which can be virtually impossible to trace. AML/KYC does nothing to change these laws.

AML/KYC does, however, dramatically increase compliance costs and makes transacting harder for the vast majority of people who lack the wealth and influence to ensure their transactions remain uninterrupted. It is these, generally low-value, transactions that are most likely to be flagged, prevented, or reversed by banks today. Recent studies suggest that anywhere between 30% and 65% of all e-commerce transactions that are declined globally are in fact legitimate, representing up to \$640 billion in lost revenue, a figure that grows higher when lost customers and their customer lifetime revenue are taken into account.⁷⁸ But declining transactions not only results in a loss of revenue; first and foremost, it represents an unprecedented infringement on economic liberty. The call centers of credit card companies and banks around the world are inundated with calls from irate customers demanding to know why they are being blocked from using their own money; however, this anger has not yet turned into meaningful political opposition to AML/KYC policies.

Ronald F. Pol, writing in 2018, observed: “anti-money laundering policy intervention has less than 0.1 percent impact on criminal finances, compliance costs exceed recovered criminal funds more than a hundred times over, and banks, taxpayers and ordinary citizens are penalized more than criminal enterprises.”⁷⁹ ⁸⁰ That same year, Rob Wainwright, outgoing director of Europol, said: “Professional money launderers — and we have identified 400 at the top, top level in Europe — are running billions

⁷⁸ Montero, Andrea. “Preventing Fraud and Minimizing False Declines is Possible for Retailers...Here’s How.” *PaymentsJournal*, Nov. 11, 2021. <https://www.paymentsjournal.com/preventing-fraud-and-minimizing-false-declines-is-possible-for-retailers-heres-how/>.

⁷⁹ Ronald F. Pol, “Uncomfortable truths? ML=BS and AML= BS2.” *Journal of Financial Crime*, Vol. 25 No. 2 (2018). pp. 294-308. <https://www.emerald.com/insight/content/doi/10.1108/JFC-08-2017-0071/full/html>.

⁸⁰ Ronald F. Pol, “Anti-money laundering: The world's least effective policy experiment? Together, we can fix it.” *Policy Design and Practice*, Vol. 3, No. 1 (2018). pp. 73-94. <https://www.tandfonline.com/doi/full/10.1080/25741292.2020.1725366>.

of illegal drug and other criminal profits through the banking system with a 99 percent success rate.”⁸¹ A 2020 report by the International Consortium of Investigative Journalists similarly concluded, “The records show that five global banks — JPMorgan, HSBC, Standard Chartered Bank, Deutsche Bank and Bank of New York Mellon — kept profiting from powerful and dangerous players even after U.S. authorities fined these financial institutions for earlier failures to stem flows of dirty money.”⁸² “The Economist” notes why this is likely the case: “it is not much more difficult today than it was 20 years ago to rinse dirty money by setting up a shell company, disguising the loot flowing through it as legitimate revenue and persuading an established bank to process it.”⁸³ Again, tying legal identities to financial transactions does not foreclose this path for concealing the sources of earnings.

What is clear, then, is that governments are incrementally imposing the requirement of full financial transparency on entire populations while either refusing to or being unable to target the powerful individuals and institutions engaged in the most egregious criminal behavior. This not only erodes individual liberty by eliminating financial privacy and making the government a third party to every transaction; it erodes trust in government institutions and creates extraordinary costs and points of friction throughout the value chain. These collectively have resulted in an anti-competitive environment for small and medium-sized businesses, who struggle to afford the increasingly onerous costs of compliance with AML/KYC regulations, while excluding 1.7 billion people (about a fourth of the world’s population) from the global financial system either because they cannot prove legal identity or because they are simply unprofitable to bank.⁸⁴

For these reasons, central bank statements about efforts to protect consumer “privacy” when designing CBDCs⁸⁵ must be understood very precisely: “privacy” in these statements does not mean privacy from the state. Rather, the state is presumed to be an essentially good and trustworthy overseer of markets at every scale, including at the level of individual transactions—and a desire for privacy from the state is implicitly equated to criminal intent.

⁸¹ Giulia Paravicini, “Europe is losing the fight against dirty money.” *Politico*. Apr. 2, 2018.

<https://www.politico.eu/article/europe-money-laundering-is-losing-the-fight-against-dirty-money-europol-crime-rob-wainwright/>.

⁸² International Consortium of Investigative Journalists, “Global banks defy U.S. crackdowns by serving oligarchs, criminals and terrorists.” Sep. 20, 2020. <https://www.icij.org/investigations/fincen-files/global-banks-defy-u-s-crackdowns-by-serving-oligarchs-criminals-and-terrorists/>.

⁸³ N.A. “The war against money-laundering is being lost.” *The Economist*. April 12, 2021.

<https://www.economist.com/finance-and-economics/2021/04/12/the-war-against-money-laundering-is-being-lost>.

⁸⁴ The World Bank, “Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows.” Press Release. April 19, 2018. <https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows>.

⁸⁵ Weidmann, “Exploring a digital euro.”

Structural Problems with CBDCs

In addition to the escalated authoritarianism that CBDCs would usher into the world's financial system, they also present a number of structural problems that must be addressed.

Contraction of Commercial Banking

Retail CBDCs would enable central banks to cannibalize a significant portion of the commercial banking system. As we discussed above, the more money consumers place in an account with the central bank, the less money commercial banks have to attract depositors and offer loans, mortgages, and other banking services. JP Morgan strategist Josh Younger estimates that up to 30% of commercial banks' funding base could leave from checking accounts to CBDC accounts.⁸⁶ For this reason, he recommends keeping a low-cap limit on American CBDC accounts—approximately \$2,500—in order to minimize the impact of this transition. (As we saw above, the Bahamas have already implemented their own limits on cash accounts.)

Penalization of Low-Income Households

Since most U.S. households have less than \$1,000 in their checking accounts, Younger argues that such limits would not result in financial exclusion for lower-income households. However, it is bizarre that a central bank would aim to disincentivize any household, but particularly lower-income households, from saving more than \$2,500 in cash. Such seemingly arbitrary limitations on savings and spending erode trust in banks, which suggests why a quarter of lower-income Americans have no interest in opening bank accounts at all.⁸⁷ The *main* reason many of the unbanked do not want bank accounts, however, is their inability or unwillingness to pay bank service fees.⁸⁸ Negative interest rates implemented on central bank cash accounts are in effect bank fees, despite central bank accounts being marketed as supposedly “fee-free” accounts. It is morally unconscionable to imagine central banks harvesting wealth from households with less than \$1,000 in their bank accounts via negative interest rates—a virtual certainty should CBDCs be implemented.

⁸⁶ Ossinger, Joanna. “JPMorgan Says Digital Currencies Must Balance Inclusion, Banks.” *Bloomberg*, Aug. 6, 2021. <https://www.bloomberg.com/news/articles/2021-08-06/jpmorgan-says-digital-currencies-must-balance-inclusion-banks?sref=3REHEaVI>.

⁸⁷ Pathe, Simone. “U.S. ‘underbanked’ population increasingly using mobile banking.” *PBS NewsHour*, Mar. 27, 2014. <https://www.pbs.org/newshour/nation/us-underbanked-population-increasingly-using-mobile-banking>.

⁸⁸ The Pew Charitable Trusts, “What Do Consumers Without Bank Accounts Think About Mobile Payments?” *Issue Brief*, Jun. 22, 2016. <https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2016/06/what-do-consumers-without-bank-accounts-think-about-mobile-payments>.

Governments Are Not Technology Service Providers

A CBDC requires a robust, highly secure, extremely reliable, and regularly-updated technical infrastructure to implement and maintain. To date, governments—even in the software-forward countries of the United States and the United Kingdom—have demonstrated that the design, delivery, and maintenance of software is not their strength.^{89 90 91} As a result, governments typically rely on the private sector to design and implement IT projects. CBDCs are no different; over the past several years, companies like Amazon and Accenture have been pitching governments on their capabilities to implement CBDCs.^{92 93}

The limitations of government-led software projects became starkly visible in early 2022, when the Eastern Caribbean Central Bank’s CBDC, DCash, went offline for nearly two months. The root cause appeared to be trivial: “a certificate on the version of the Hyperledger Fabric that hosted the DCash ledger expired.”⁹⁴ Replacing an expired certificate is a process that typically takes only a few minutes, but it took the ECCB nearly two months. During this time, DCash was unusable.

By contrast, the Bank for International Settlement and the Swiss National Bank have relied on SIX⁹⁵, a private financial services infrastructure provider, to issue its CBDC and settle transactions with it during early-stage pilots.⁹⁶ To build its platform, SDX, SIX leveraged R3 Corda, a private, permissioned blockchain built by a financial services industry consortium.⁹⁷ While the system has not been tested in-market yet, it promises to map CBDCs to existing central bank ledgers and serve as a

⁸⁹ Yaraghi, Niam. “Doomed: Challenges and solutions to government IT projects.” *Brookings Institute*, Aug. 25, 2015. <https://www.brookings.edu/blog/techtank/2015/08/25/doomed-challenges-and-solutions-to-government-it-projects/>.

⁹⁰ Grothaus, Michael. “Why Exactly Does The Government Suck So Badly At Software?” *Fast Company*, May 27, 2014. <https://www.fastcompany.com/3031108/why-exactly-does-the-government-suck-so-badly-at-software>.

⁹¹ Evenstad, Lis. “Government has poor track record in delivering major projects, says NAO.” *Computer Weekly*, Jan. 6, 2016. <https://www.computerweekly.com/news/4500269842/Government-has-poor-track-record-in-delivering-major-projects-says-NAO>.

⁹² “CBDC technology: interest intensifies in digital currency ‘innovation catalysts’.” *Global Government: Fintech*, Apr. 27, 2021. <https://www.globalgovernmentfintech.com/cbdc-technology-interest-intensifies-in-digital-currency-innovation-catalysts/>.

⁹³ Oliver Wyman Forum and AWS. “Retail Central Bank Digital Currency: From Vision to Design.” Mar. 2022. <https://www.oliverwymanforum.com/content/dam/oliver-wyman/ow-forum/future-of-money/Retail-Central-Bank-Digital-Currency-From-Vision-to-Design.pdf>.

⁹⁴ Vold, Fredrik. “Caribbean CBDC Functional Again After Two-Month Outage.” <https://cryptonews.com/news/caribbean-cbdc-functional-again-after-two-month-outage.htm>.

⁹⁵ SIX. <https://www.six-group.com/en/home.html>.

⁹⁶ SIX. “BIS, SNB and SIX Complete Test of Wholesale CBDC Settlement.” *Markets Media Group*, Jan. 14, 2022. <https://www.marketsmedia.com/bis-snb-and-six-complete-test-of-wholesale-cbdc-settlement/>.

⁹⁷ R3. “The Power of 3.” <https://www.r3.com/the-power-of-3/>.

new infrastructure that provides “central bank control over wholesale CBDC.”⁹⁸ Among other things, SDX, combined with the other solution components, enables central banks to “collect all relevant transaction data” and allow “monitoring of wholesale CBDC settlements and holdings.”⁹⁹ Once in place, this wholesale CBDC solution will be easily extensible to a retail CBDC.

In effect, where governments lead the implementation of CBDCs, serious stability and reliability issues will arise. Alternatively, where the private sector designs and implements the solution, a public good–money–will become a software service that is only operable as long as it generates profit for private infrastructure providers. In the United States, rolling out a CBDC would effectively privatize the U.S. Bureau of Engraving and Printing and the U.S. Mint, both currently bureaus of the U.S. Department of the Treasury. Even Microsoft, a global leader in cloud computing, has expressed reservations about outsourcing a key function of sovereign governments to the private sector, arguing that it would remove the public accountability mandate from the issuance and management of fiat currency.¹⁰⁰

Security Risk

Government IT infrastructure worldwide is the target of constant and escalating cyberattacks as the digital realm has become a primary theater of war and espionage.¹⁰¹ Intelligence agencies are in an ongoing race to defend against security vulnerabilities, many of which are created by their own teams to compromise the software of rival countries but are quickly leaked and turned against their creators.¹⁰² Moreover, government agencies and regulatory bodies store troves of sensitive personal data that may be hacked or leaked by internal actors, whether for personal benefit, as part of a whistleblowing endeavor, or for other reasons (i.e., as a result of a social engineering attack). For example, a 2020 leak of data from FinCEN (U.S. Department of the Treasury’s Financial Crimes Enforcement Network) exposed the identities of suspected financial criminals around the world and of the businesses and specific AML/KYC compliance staffers who reported them.¹⁰³ This made both

⁹⁸ Bank for International Settlements. “Project Helvetia: Phase II Overview.” *YouTube*, Jan. 13, 2022. <https://www.youtube.com/watch?v=R5TF3xB5J88&t=1s>.

⁹⁹ Bank for International Settlements. “Project Helvetia: Phase II Overview.” *YouTube*, Jan. 13, 2022. <https://www.youtube.com/watch?v=R5TF3xB5J88&t=1s>.

¹⁰⁰ Catherine Bosley. “Microsoft President Smith Is No Fan of Private Digital Currency.” *Bloomberg*, Mar. 24, 2021. <https://www.bloomberg.com/news/articles/2021-03-24/microsoft-president-smith-is-no-fan-of-private-digital-currency>.

¹⁰¹ N.A. “Significant Cyber Incidents.” *Center for Strategic and International Studies*, March 2022. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.

¹⁰² Greenberg, Andy. “China Hijacked an NSA Hacking Tool in 2014—and Used It for Years.” *Wired*, Feb. 22, 2021. <https://www.wired.com/story/china-nsa-hacking-tool-epme-hijack/>.

¹⁰³ Lynch, Nathan and Brett Wolf. “U.S. FinCEN leaks to have ‘chilling effect’ on fight against financial crime, say AML experts.” *Thomson Reuters*, Sep. 18, 2020. <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/fincen-leaks-aml/>.

businesses and staffers vulnerable to threats and violence while further eroding the efficacy of financial law enforcement. In 2022, one of the largest publicly-known data breaches in history occurred when a Shanghai police database was hacked, revealing the data of over 1 billion Chinese citizens.¹⁰⁴

Any data a government collects is vulnerable to exploits. CBDC infrastructure would collect data about every transaction conducted with digital cash by every person everywhere in the world and record it on a permanent ledger—likely one maintained by a private corporation or corporations, as discussed in the previous section. This structure would give both the involved corporations and the state full visibility into the ledger and create a giant honeypot of personal data that would inevitably be compromised and exposed to other state and criminal actors.

Centralized Blockchains: An Oxymoron?

This leads us to a discussion of the technology underpinning CBDCs: digital ledgers. Any CBDC implementation would require the use of a centralized ledger maintained by and/or fully visible to the central bank. One such digital ledger implementation is a blockchain, a data structure that appends new transactions to previous transactions in a time-sequenced manner. These transactions are then recorded in so-called “blocks” (transaction groupings). Transactions are validated by members of the blockchain network (“nodes” or “validators”, depending on the consensus model) according to consensus rules established at the protocol level, then recorded in the ledger and broadcast to all other nodes. This creates a shared record of transactions that verifiably demonstrates how much digital currency is owned by every address on the network at any point in time.


Bitcoin: The First “Blockchain”

Bitcoin, the first “blockchain,” was introduced in 2009, during the Great Financial Crisis, by an individual or group writing under the pseudonym “Satoshi Nakamoto.”¹⁰⁵ Bitcoin pioneered the use of a blockchain data structure (which Nakamoto called a “timechain”) to prevent the “double spending” of cryptocurrency. In other words, the Bitcoin protocol prevents cryptocurrency holders from spending their money more than once by validating and updating address balances against a shared ledger once every ten minutes. In addition, the protocol has a fixed monetary policy which specifies that only 21,000,000 bitcoin will ever be issued. In this way, Nakamoto created *scarce* digital money, solving a major problem in computer science that had motivated many of its brightest minds for decades. For this reason, Bitcoin has been called “the internet of value.”

¹⁰⁴ Ni, Vincent. “Hacker claims to have obtained data on 1 billion Chinese citizens.” *The Guardian*. July 4, 2022.

<https://www.theguardian.com/technology/2022/jul/04/hacker-claims-access-data-billion-chinese-citizens>.

¹⁰⁵ Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” <https://bitcoin.org/bitcoin.pdf>.



Bitcoin was designed to be a stateless cryptocurrency, not issued by any government or pegged to any government-issued currency. Its network is maintained by a loose coalition of volunteer software developers and so-called “miners” (computers running the Bitcoin protocol to mint new bitcoin by validating transactions). Since Bitcoin is a public network, like the internet, anyone can run the Bitcoin protocol to validate transactions, and anyone can transact on the network. This openness means that the Bitcoin protocol must assume that all parties using the network are potentially enemies incentivized to game the network to maximize their own bitcoin holdings. This gives its protocol a robust game-theoretic set of incentives to ensure good behavior without good actors. For this reason, bitcoin is often called “enemy money.”

Bitcoin’s bottom-up design and adoption model means that it operates independently of state funding and from the policy interventions of central banks. It enables direct peer-to-peer transacting of money without any third-party intermediaries. Bitcoin’s release during the GFC was motivated by the desire to create a digital store of value and medium of exchange that people could use, as fiat currencies became increasingly devalued in response to central bank policies like quantitative easing and sovereign debt monetization.

For evident reasons, central banks have been ambivalent—at best—about Bitcoin. They sense in some of its functions a potential existential threat: Bitcoin has automated the issuance and transaction of hard money, calling into question the role of central banks in economic life. Yet central banks are also aware that digital cash is the future, and they want to ride this wave of innovation. How can they participate in this technological advancement without abdicating their roles as creators and managers of sovereign (fiat) currencies?

Centralized Blockchains

One popular answer: centralized blockchains. Because Bitcoin’s code is open source, it could easily be copied and used to create new blockchains. In the early years, many of these blockchains were simply versions of Bitcoin, though they never came to enjoy the network effects of adoption that characterize the original chain. In the years that followed, however, many software developers and companies drew inspiration from the Bitcoin code to build very different blockchain infrastructures that afforded more direct control of validation and transaction by specific “trusted” nodes. This enabled the creation of private or permissioned blockchains, where—in principle—only trusted parties can view or validate transactions or transact on the ledger.

Since members of these restricted blockchain networks must be trusted to some degree, the chains no longer create “enemy money” --instead, they create “friendly money” that is in need of a human administrative layer to manage its usage. Moreover, because private blockchains assume that only “trusted” users will access the network, many of their architectures enable the encoding of personal transaction data directly on-chain. This makes private blockchains honey pots of personal data waiting to be exploited by malicious actors.

In addition to being huge, hackable databases of personal financial data, private blockchains also suffer from other security shortcomings. Although little information about the level of decentralization of most private blockchains is available to the public, anecdotal evidence suggests that a significant percentage of these networks are not Byzantine fault-tolerant, meaning they have too few nodes to provide basic blockchain network security. This is why some companies have created “consensus-as-a-service” offerings; these companies are finding initial market traction by securing centralized blockchain projects that cannot establish consensus on the state of the ledger on their own.¹⁰⁶ One wonders what value blockchains provide for these private network use cases that cannot be handled more efficiently and effectively by private databases.

The answer may be as simple as this: central banks are seeking to compete with Bitcoin, so they believe they must implement their own versions of blockchain technology. In this way, they hope to stem the adoption of Bitcoin and the threat it represents to their influence over private economic life. However, as noted above, the more a blockchain network relies on trust, the more centralized—or controlled by a few “trusted” actors—it must be. For this reason, we might reasonably ask what functions can be performed by private blockchains that could not be performed by, say, a shared database. In the context of payments, the Visa or Mastercard payment networks are already well-functioning examples. Indeed, some CBDC proponents have explicitly argued against using blockchains or distributed ledgers for digital fiat currencies and instead to simply use centralized databases.¹⁰⁷ Why do CBDCs need blockchains at all?

The takeaway here is that any government and central bank rhetoric that CBDCs are “distributed” or “decentralized” is simply not the case. Whether they use blockchains or not, CBDCs are centralized implementations of digital money that afford the state full transparency into every economic

¹⁰⁶ Hedera Consensus Service. Accessed May 2, 2022. <https://hedera.com/consensus-service>.

¹⁰⁷ Rohan Grey, quoted in “Rep. Lynch Introduces Legislation to Develop Electronic Version of U.S. Dollar.” *Newsroom of Congressman Stephen F. Lynch*. Mar. 28, 2022. <https://lynch.house.gov/press-releases?ID=5A0DA9DE-8884-4E06-AC0A-BCA08850F05E>.

transaction. And of course, CBDCs are unnecessary. The value of natively digital currencies for individual users can be fully realized with a combination of bitcoin and privately issued stablecoins.

Alternatives to CBDCs

The U.S. Dollar is Already Digital

The U.S. dollar, like other fiat currencies, is already digital.¹⁰⁸ Digital dollars and other fiat currencies are created and used today through the commercial banking system. People deposit their fiat-denominated holdings at a commercial bank (for example, Bank of America) and then transact electronically using a variety of digital payment rails like ACH, FedWire, and Swift. Commercial banks, in turn, use digital record keeping to track their ledger balances with central banks.

These digital dollar transactions are already highly surveilled. Banks require full identity verification to both open accounts and transact. Any transaction can be flagged as suspicious and blocked. Banks impose limits on the amount of money individuals can withdraw in one day, in one week, or in one month. Individuals must specify the purpose of transactions above a certain amount. All of this constitutes not only a substantial invasion of privacy by the state, but erodes individual economic liberty. People today can only transact at the pleasure of the state via banks who deploy police power as quasi-state institutions.

The status quo reasonably leads many to ask what the value of CBDCs is for end users. Central banks might reply that the speed of transactions can now be substantially reduced: for example, the average ACH transaction takes three business days, while a CBDC transaction might be virtually instant. Similarly, they may say that CBDCs will also dramatically lower the cost of transacting, particularly internationally. Fees to wire money typically range from \$0-\$50, but high-value transfers often charge on a percentage basis, which can make transfer fees climb steeply. Money transfer firms also charge very high percentage fees to move physical cash from one location to another; these services are used frequently by the unbanked.

But while people in principle wouldn't need bank accounts to transact with CBDCs, in practice they would need mobile phones (usually smartphones). About 60% of the unbanked worldwide have

¹⁰⁸ Quarles, Randal. "Parachute Pants and Central Bank Money." *Speech at the 113th Annual Utah Bankers Association Convention, Sun Valley, Idaho*, Jun. 28, 2021. <https://www.federalreserve.gov/newsevents/speech/quarles20210628a.htm>.

smartphones¹⁰⁹, but they also rely on cash for its immediate access and anonymity. Meanwhile, for the banked, payment networks like Visa and Mastercard are already used widely and effectively. Indeed, in China, WeChat Pay and Alipay are ubiquitous and extremely convenient.¹¹⁰ This has somewhat stalled the adoption of the e-CNY, as end users aren't sure what value it provides over and above their existing digital payment services.

Bitcoin

The highly surveilled and controlled world of digital money suggests that a meaningful alternative must be private, uncensorable, and free. These are characteristics of bitcoin: a global cryptocurrency issued by a protocol rather than by a bank.

Bitcoin was launched to preserve a space for individual economic freedom in a world where economic life increasingly takes place on the world wide web—and where surveillance and censorship are easy to implement. Bitcoin provides all of the purported benefits of CBDCs for end users (instant, low-cost or even free transactions, domestically and across borders; final settlement) but without built-in surveillance and transaction control, and without the ability to control Bitcoin's monetary policy. For these reasons, it presents an important alternative to both CBDCs and digital dollars.

Privacy

Privacy is a critical component of economic liberty, which is in turn the key value motivating the Bitcoin project. Economic liberty means that individuals are free to transact with anyone they choose, without having to disclose their holdings or their identities. Bitcoin privacy is continually evolving to better protect these rights.

Before discussing how Bitcoin protects privacy, it is worth asking: why does freedom depend on privacy? Here it is worth quoting at length Edward Snowden, former contractor for the U.S. National Security Agency, who in 2013 exposed the unconstrained surveillance conducted by U.S. intelligence

¹⁰⁹ Bruchert, Philipp. "New mobile money propositions have the potential to reduce the world's unbanked population by more than a third." *Mastercard*, March 28, 2019. <https://www.mastercard.com/news/europe/en-uk/newsroom/press-releases/en-gb/2019/march/new-mobile-money-propositions-have-the-potential-to-reduce-the-world-s-unbanked-population-by-more-than-a-third/>.

¹¹⁰ Benzmilller, Theodore. "China's Progress Towards a Central Bank Digital Currency." *Center for Strategic and International Studies: New Perspectives on Asia*, Apr. 19, 2022. <https://www.csis.org/blogs/new-perspectives-asia/chinas-progress-towards-central-bank-digital-currency>.

agencies against American citizens without regard for constitutional protections.^{111 112 113} In a 2016 panel discussion, Snowden said:

"Privacy isn't about something to hide. Privacy is about something to protect. That's who you are. That's what you believe in. Privacy is the right to a self. Privacy is what gives you the ability to share with the world who you are on your own terms. For them to understand what you're trying to be and to protect for yourself the parts of you you're not sure about, that you're still experimenting with.

"If we don't have privacy, what we're losing is the ability to make mistakes, we're losing the ability to be ourselves. Privacy is the fountainhead of all other rights. Freedom of speech doesn't have a lot of meaning if you can't have a quiet space, a space within yourself, your mind, your community, your friends, your family, to decide what it is you actually want to say.

"Freedom of religion doesn't mean that much if you can't figure out what you actually believe without being influenced by the criticisms of outside direction and peer pressure. And it goes on and on.

"Privacy is baked into our language, our core concepts of government and self in every way. It's why we call it 'private property.' Without privacy you don't have anything for yourself.

"So when people say that to me ["if you have nothing to hide, you have nothing to fear"] I say back, arguing that you don't care about privacy because you have nothing to hide is like arguing that you don't care about free speech because you have nothing to say."¹¹⁴

Snowden's eloquent defense of privacy as critical for the formation of an independent moral self stands in stark contrast to the now-famous statement by Scott McNealy, then-CEO of Sun

¹¹¹ N.A., "Snowden Revelations." *Lawfare Blog*, N.D. Accessed May 16, 2022. <https://www.lawfareblog.com/snowden-revelations>.

¹¹² MacAskill, Ewen and Gabriel Dance. "NSA Files: Decoded." *The Guardian*, Nov. 1, 2013. <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>.

¹¹³ Franceschi-Bicchierai, Lorenzo. "The 10 Biggest Revelations from Edward Snowden's Leaks." *Mashable*, Jun. 5, 2014. http://sjo.pwr.edu.pl/fcp/2GBUKOQtTKlQhbx08SlkTUgRCUWRuHQwFDBoIVURNWHVRBFhnRIUuWTISTnoYDxMe/_users/code_cE14VPxYXPVI8ShEqTVcBE0MAXS0oGEMSBQ/pasaz/angielski/science/180409_the_10_biggest_revelations_from_edward_snowden_s_leaks-1.pdf.

¹¹⁴ Schrodt, Paul. "Edward Snowden just made an impassioned argument for why privacy is the most important right." *Business Insider*, Sep. 15, 2016. <https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9>.

Microsystems, in 1999: “You have zero privacy anyway. Get over it.”¹¹⁵ While McNealy’s comments generated an outcry, he had stated a truth that many did not want to believe: by the end of the 1990s, surveillance capitalism was already firmly established as a revenue model for an entire generation of U.S. software companies. In effect, McNealy was saying to the world: *There is no alternative.*

In many ways, McNealy was not wrong. In his time, the technical architectures that could protect individual privacy in a world of interconnected digital devices were rudimentary, and commercial software was designed intentionally to maximize data sharing between corporations and governments in ways that both drove revenue and increased state control. Because so few people understood the rarefied world of software development, and because this macro-trend was rarely reported on by the press (whose own advertising-based business models incentivized them to support the sharing of personal data at scale), few Americans noticed that anything untoward was happening. Moreover, the commercial success of the U.S. software industry became another incentive not to “mess with success”: privacy advocates were seen by some as idealistic curmudgeons willing to crash the economy to preserve an illusion of personal inviolability.^{116 117} And after 9/11, a political rationale was added to the destruction of privacy: Americans rushed to authorize sweeping new government powers in the name of protecting the homeland, setting the stage for Edward Snowden’s revelations more than a decade later.¹¹⁸

During the late 1970s and 1980s, a small group of cryptographers and software engineers anticipated that neither the U.S. government nor the private sector could be relied upon to effectively preserve individual privacy in the digital age. This loosely-affiliated group became known as the cypherpunks, a portmanteau of the words “cypher” and “cyberpunks.” The cypherpunk movement can be traced back using various genealogies and periodizations,^{119 120} but a few moments stand out in its emergence: the publication of David Chaum’s “Security Without Identification” in 1985;¹²¹ the creation of the

¹¹⁵ Sprenger, Polly. “Sun on Privacy: ‘Get Over It’.” *Wired*, Jan. 26, 1999. <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/>.

¹¹⁶ EPIC, “Public Opinion on Privacy.” *Electronic Privacy Information Center*. N.D. <https://archive.epic.org/privacy/survey/>.

¹¹⁷ Castro, Daniel. “Trust Us, We Know Best: The Steady Rise of Privacy Paternalism.” *Information Technology & Innovation Foundation*, Jun. 24, 2021. <https://itif.org/publications/2021/06/24/trust-us-we-know-best-steady-rise-privacy-paternalism>.

¹¹⁸ Franklin, Sharon Bradford. “Rethinking Surveillance on the 20th Anniversary of the Patriot Act.” *Just Security*, Oct. 6, 2021. <https://www.justsecurity.org/78753/rethinking-surveillance-on-the-20th-anniversary-of-the-patriot-act/>.

¹¹⁹ Lopp, Jameson. “Bitcoin and the Rise of the Cypherpunks.” *CoinDesk*, Apr. 9, 2016. <https://www.coindesk.com/markets/2016/04/09/bitcoin-and-the-rise-of-the-cypherpunks/>.

¹²⁰ Qureshi, Haseeb. “The Cypherpunks.” *Nakamoto.com*, Dec. 29, 2019. <https://nakamoto.com/the-cypherpunks/>.

¹²¹ Chaum, David. “Security without identification: transaction systems to make big brother obsolete.” *Communications of the ACM*, Vol. 28, No. 10, Oct. 1985, pp. 1030–1044. <https://dl.acm.org/doi/10.1145/4372.4373>.

Cypherpunks mailing list in 1992;¹²² and the publication of “A Cypherpunk’s Manifesto” online by Eric Hughes in 1993.¹²³

Cypherpunks foresaw that the rise of the internet would create a surveillance society and began building cryptographic standards that could be deployed to protect money and identity on the web. They played a critical role in “The Crypto Wars” of the 1990s, which kicked off when the White House introduced the Clipper Chip in 1993.¹²⁴ This microchip created an unencrypted “back door” in consumer hardware telephones, giving the government full access to all the data produced by the devices. The White House was forced to pull the Clipper Chip after cypherpunk Matt Blaze demonstrated that a brute force attack could disable its key escrow capability, effectively rendering it useless.¹²⁵

Although the cypherpunks won the first Crypto Wars, U.S. government agencies have not stopped pushing for encryption back doors. Over the past decade, two federal bills have been introduced by members of both parties to mandate the creation of encryption back doors for law enforcement.^{126 127} High-ranking members of the executive branch, like Attorney General William Barr,¹²⁸ have explicitly called for encryption back doors. Neither bill passed, and Attorney General Barr’s pronouncements didn’t go much farther than words. Despite this temporary preservation of encryption, however, data sharing between software companies and the U.S. government has been a well-established practice for decades, blurring or eliminating the lines between public and private communication.^{129 130 131}

¹²² Qureshi, “The Cypherpunks.”

¹²³ Hughes, Eric. “A Cypherpunk’s Manifesto.” <https://www.activism.net/cypherpunk/manifesto.html>.

¹²⁴ Thompson, Andi Wilson, Danielle Kehl, and Kevin Bankston. “Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s.” *New America*. Jun. 17, 2015. <https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/>.

¹²⁵ Blaze, Matt. “Protocol Failure in the Escrowed Encryption Standard.” Aug. 20, 1994. <https://www.mattblaze.org/papers/eesproto.pdf>.

¹²⁶ Whittaker, Zack. “Senate’s encryption backdoor bill is ‘dangerous for Americans,’ says Rep. Lofgren.” *TechCrunch*, Sep. 20, 2020. <https://techcrunch.com/2020/09/20/encryption-backdoor-bill-dangerous-lofgren/>.

¹²⁷ Farivar, Cyrus and Kevin Collier. “‘Lawful access’ bill would allow feds to legally bust into encrypted devices.” *NBC News*, Jun. 24, 2020. <https://www.nbcnews.com/tech/security/lawful-access-bill-would-allow-feds-legally-bust-encrypted-devices-n1232071>.

¹²⁸ Farivar, Cyrus. “AG Barr rails against encryption — but security experts have heard it before.” *NBC News*, Jul. 26, 2019. <https://www.nbcnews.com/tech/tech-news/ag-barr-rails-against-encryption-security-experts-have-heard-it-n1035196>.

¹²⁹ EPIC, “Public Opinion on Privacy.”

¹³⁰ Greenwald, Glenn and Ewen MacAskill. “NSA Prism program taps in to user data of Apple, Google and others.” *The Guardian*, Jun. 7, 2013. <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

¹³¹ Wamsley, Laurel. “Library Of Congress Will No Longer Archive Every Tweet.” *National Public Radio*, Dec. 26, 2017. <https://www.npr.org/sections/thetwo-way/2017/12/26/573609499/library-of-congress-will-no-longer-archive-every-tweet>.

This suggests that there are multiple fronts in what should perhaps be more appropriately called the Privacy Wars, and encryption is only one of them.

Cypherpunks were not the only advocates for internet privacy during the 1990s. With the rise of the web, it soon became apparent that any kind of e-commerce would be impossible without effective protections for payments and identity. Accordingly, companies like Netscape pioneered the development of SSL and HTTPS privacy standards, which enabled the “Web 2.0” era of commercial software platforms.¹³² (Since that time, SSL has evolved into TLS, a more advanced cryptographic protocol.) On the policy side, as of mid-2022, over 70% of governments worldwide have passed internet privacy laws to prevent the most egregious abuses of user data.¹³³

Yet as indicated above, encryption standards and privacy laws have failed to prevent the continued intensification of the surveillance economy. Indeed, they can be said to enable it by giving technical and legal cover to the routine exploitation of user data. As Web 2.0 evolved and the mobile computing revolution took root, surveillance began to skyrocket as well. By mid-2022, smartphone penetration had surpassed 80% of the world’s population.¹³⁴ ¹³⁵ Common smartphone apps like Twitter, Facebook, and dating apps sell user data (for example, location data) to advertisers, who in turn resell it to organizations in the public or private sector.¹³⁶ This personal data economy has enabled government agencies to track the movements and online activities of billions of people around the world in real time with near-perfect accuracy.¹³⁷

In a world where every user’s digital identity and identifiers are constantly broadcast to virtually anyone with a telecommunications capability,¹³⁸ the separation of money from identity arguably

¹³² Matthews, Tim. “The Origins of Web Security and the Birth of Security Socket Layer (SSL) Protocol.” *Exabeam*, Feb. 6, 2019. <https://www.exabeam.com/information-security/web-security-security-socket-layer-protocol-ssl/>.

¹³³ UNCTAD, “Data Protection and Privacy Legislation Worldwide.” Accessed May 8, 2022. <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

¹³⁴ Statista, “Number of smartphone subscriptions worldwide from 2016 to 2027.” Accessed May 8, 2022. <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>.

¹³⁵ BankMyCell, “May 2022 Mobile User Statistics: Discover the Number of Phones in The World & Smartphone Penetration by Country or Region.” Accessed May 8, 2022. <https://www.bankmycell.com/blog/how-many-phones-are-in-the-world#:~:text=In%202022%2C%20the%20number%20of,91.54%25%20of%20the%20world's%20population..>

¹³⁶ Tau, Byron and Georgia Wells. “Grindr User Data Was Sold Through Ad Networks.” *The Wall Street Journal*, May 2, 2022. <https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800>.

¹³⁷ Biddle, Sam and Jack Poulson. “American Phone-Tracking Firm Demo’d Surveillance Powers by Spying on CIA and NSA.” *The Intercept*, April 22, 2022. <https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-signal-surveillance-cia-nsa/>.

¹³⁸ McCullough, Austin. “Stingray Searches and the Fourth Amendment: Implications of Modern Cellular Surveillance.” *American Criminal Law Review Online*, Vol. 53, No. 41. pp. 41-46. <https://www.law.georgetown.edu/american->

becomes a pressing issue of basic human rights. The most violent, repressive, and authoritarian governments of the past had only a tiny fraction of the surveillance capability now available to not only governments, but anyone willing to pay for it.

For these reasons, the Bitcoin project is centrally concerned with the separation of money from identity. As Satoshi Nakamoto wrote in the Bitcoin white paper:

"The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the 'tape', is made public, but without telling who the parties were."¹³⁹

While bitcoin addresses (cryptographic public keys) can currently be tied to known identities, and the bitcoin holdings of specific addresses can be made public, various privacy-enhancing proposals have been and are being developed that would make transactions more private over time.¹⁴⁰ The most recently-implemented privacy-enhancing software upgrade was called Taproot, which changed Bitcoin's signature scheme from the Elliptic Curve Digital Signature algorithm to Schnorr signatures to mask transactions involving multiple wallets.¹⁴¹ This makes multisignature transactions appear indistinguishable from single-signature transactions on the blockchain. Taproot was initially proposed in 2018, then went through years of iteration and testing. It was formally approved in June 2021 when

[criminal-law-review/wp-content/uploads/sites/15/2021/10/53-0_McCullough_-_STINGRAY_SEARCHES_AND_THE_FOURTH_AMENDMENT_IMPLICATIONS_OF_MODERN_CELLULAR_SURVEILLANCE.pdf](#).

¹³⁹ Nakamoto, "Bitcoin", p. 6.

¹⁴⁰ Lopp, "Bitcoin and the Rise of the Cypherpunks."

¹⁴¹ Ikeda, Scott. "New Privacy Update to Bitcoin Network Approved, "Taproot" Upgrade Will Improve Digital Signatures & Clears Path for Smart Contracts." *CPO Magazine*, Jun. 23, 2021. <https://www.cpomagazine.com/data-privacy/new-privacy-update-to-bitcoin-network-approved-taproot-upgrade-will-improve-digital-signatures-clears-path-for-smart-contracts/>.

90% of miners signaled support for it, and then implemented in production on November 14, 2021.¹⁴²

¹⁴³

Many other privacy-enhancing projects are in development, a number of which do not involve changes to the Bitcoin protocol itself. One example is the creation of Federated Chaumian Mints.¹⁴⁴ These mints are in effect pools of bitcoin where ownership of any particular amount is obscured. Federated Chaumian Mints enable more private bitcoin custody solutions than the centralized exchanges and wallets most frequently used today. By doing so, proponents argue, the mints will spur adoption among Bitcoin's less technical users who cannot or do not wish to manage their own keys.

Another noteworthy initiative is the development of decentralized exchanges (for example, TBD) which use advanced cryptographic identity standards to protect the identities of users from network observers while allowing disclosure to counterparties in specific transactions.¹⁴⁵ This enables trust while preventing surveillance.

In short, transaction privacy is a central aim of the Bitcoin project. The Bitcoin developer community embraces the established principle within U.S. law that building and releasing open-source software constitutes free speech, which cannot be constitutionally abridged.¹⁴⁶ In this way, Bitcoin aims to create a meaningful alternative to the surveillance economy without relying on support from either the public or the private sector, neither of which is incentivized to disrupt a status quo that both generates profits and facilitates population control.

Censorship Resistance

The Bitcoin network itself does not afford the ability to censor (prohibit) or reverse transactions. Any Bitcoin address can send any of its holdings to any other address at any time, and once the transaction has been finalized on-chain, there is no reversing it. This is what makes Bitcoin a “peer-to-peer”

¹⁴² Hertig, Alyssa. “Taproot, Bitcoin’s Long-Anticipated Upgrade, Has Activated.” *CoinDesk*, Nov. 12, 2021.

<https://www.coindesk.com/tech/2021/11/13/taproot-bitcoins-long-anticipated-upgrade-activates-this-weekend/>.

¹⁴³ As a decentralized network, Bitcoin requires broad consensus to approve any changes to its underlying protocol.

Typically the miner approval threshold is 95%, but it was expedited with Taproot through a process known as “Speedy Trial”.

¹⁴⁴ Namcios, “Federated Chaumian Mints: The Future of Bitcoin Privacy?” *Bitcoin Magazine*, Apr. 8, 2022.

<https://bitcoinmagazine.com/technical/what-is-the-future-of-bitcoin-privacy>.

¹⁴⁵ TBD Developer, “introducing tbDEX.” Nov. 19, 2021. <https://tbd54566975.ghost.io/introducing-tbdex/>.

¹⁴⁶ Brito, Jerry and Peter Van Valkenburgh. “Writing and publishing code alone cannot be a crime.” *Coin Center*, Oct. 29, 2018. <https://www.coincenter.org/writing-and-publishing-code-alone-cannot-be-a-crime/>.

network: users can interact with each other directly, without depending on any third party or centralized intermediary.

This does not mean that there can be no provisionality in transacting on the Bitcoin network. Since 2015, a growing part of the Bitcoin developer ecosystem has been building “the Lightning Network,” a protocol suite that enables the creation of peer-to-peer payment channels that eventually settle to the Bitcoin blockchain.¹⁴⁷ The blockchain itself is referred to as “Layer 1,” while the Lightning Network is referred to as “Layer 2.” Each layer is optimized for its specific function: final settlement for Layer 1, payment processing for Layer 2. Only the final Lightning channel balance gets settled to the Bitcoin blockchain, preserving the privacy of parties to the transaction and dramatically increasing the network’s overall throughput. As more Lightning nodes come online, the transaction throughput of the network as a whole increases dramatically.

In this way, the Lightning Network enables not only the scalability of Bitcoin transactions far beyond existing digital payments networks (i.e., Visa, Mastercard, SWIFT), but a broad suite of financial and commercial services that benefit from the finality of settlement ensured by the base layer (Bitcoin). This makes the Lightning Network an innovation as economically consequential as SSL and HTTPS, discussed above, by facilitating mass access to the “internet of value.” Before Bitcoin, finality of settlement in the U.S. could only be ensured through the FedWire system, which settles transaction balances for U.S. Reserve Banks. (Before the FedWire System, often the only recourse to determine final settlement was often physical violence—or the threat of it.) In this way, Bitcoin has brought the trust technology behind central banking—and the state—to the individual user via peaceful, open-source code.

There is some concern, however, that the Lightning Network may introduce vectors of centralization that could result in transaction censorship.¹⁴⁸ This is an important consideration that must be addressed as the network develops. Despite this potential threat, however, the Lightning Network continues to be—as of mid-2022—the most promising framework for ensuring the decentralized scalability of Bitcoin. It is this virtually limitless scalability which opens the door to Bitcoin’s use as an everyday medium of exchange.

Along those lines, arguably the most important frontier for ensuring Bitcoin’s continued censorship resistance lies in custody solutions. As we mentioned in the discussion of Federated Chaumian Mints

¹⁴⁷ Alden, Lyn. “A Look at the Lightning Network.” *LynAlden.com*, August 2022. <https://www.lyalden.com/lightning-network/>.

¹⁴⁸ Frankenfield, “Lightning Network.”

above, most users currently access both the Bitcoin network and the Lightning Network through centralized third parties: digital exchanges and wallet providers. These platforms typically implement full AML/KYC along with withdrawal limits and transaction policing. In other words, exchanges and wallet providers operate like typical banks, which means using bitcoin via these services is often not very different from using digital fiat currency. This is a trade-off many today make for the convenience of having a trusted third party custody their bitcoin. However, this is a dangerous trade, as it eliminates many of the unique benefits of using the Bitcoin network and opens user assets to confiscation. Full censorship resistance will therefore only be realized if the software used to custody bitcoin is itself censorship resistant.

Freedom

Ultimately, transaction privacy and censorship resistance are prerequisites for economic freedom. Economic freedom is a critical element of human freedom as such. A free person is able to enter into mutually beneficial relationships with whomever they choose and to negotiate the terms of those relationships without undue pressure or external influence. Freedom is the value at the root of the Bitcoin network. It is also—we argue—the value at the root of the American project. Freedom hinges on a foundational prior right, discussed above: the right to privacy. Without privacy, freedom is impossible.

As the discussion of CBDCs above shows, expansion of government power is frequently justified by ostensibly urgent police action: the need to prevent terrorism, human trafficking, money laundering, illegal border crossings, etc. In the United States, both 9/11 and the January 6 insurrection became reasons to greatly step up the policing of both economic activity and speech by the government—with the private sector serving as a willing enabler and (often pre-emptive) enforcer.^{149 150} In the intelligence community, such public crises are often referred to as “covers for action”: they offer a publicly-acceptable rationale for the expansion of government power.¹⁵¹

Such covers for action have done extraordinary work to make Americans willing participants in the erosion of their own freedoms. Surveillance of U.S. citizens by federal intelligence agencies has been

¹⁴⁹ Feingold, Russ. “In the Wake of the January 6 Attacks, Will Congress and the Administration Heed the Lessons of 9/11?” *Just Security*, Sep. 20, 2021. <https://www.justsecurity.org/78290/in-the-wake-of-the-january-6-attacks-will-congress-and-the-administration-heed-the-lessons-of-9-11/>.

¹⁵⁰ Levin, Sam. “US Capitol attack: is the government’s expanded online surveillance effective?” *The Guardian*, Jan. 7, 2022. <https://www.theguardian.com/us-news/2022/jan/07/us-capitol-attack-government-online-surveillance>.

¹⁵¹ Snowden, Edward. “Here’s how we take back the Internet.” *TED*, Mar. 2014. https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet?language=en.

ubiquitous for years,^{152 153} and U.S. police at municipal, state, and federal levels increasingly use facial recognition software, location tracking, and data mining to produce detailed maps of the predilections and behaviors of anyone on U.S. territory and beyond.^{154 155 156} Predictive policing is known to exacerbate racial prejudices while calling into question a fundamental premise of the U.S. justice system: that people are innocent until proven guilty.^{157 158}

Meanwhile, the “technologies of the border”--increased surveillance and suspension of certain rights typically reserved for border crossings--have become generalized to two-thirds of the American population via the encroachment of Customs and Border Patrol jurisdiction up to 100 miles inland.¹⁵⁹ The CPB incorrectly, but routinely, interprets their enhanced powers within this zone as effectively suspending the constitutional rights of U.S. citizens--particularly the First and Fourth Amendments.¹⁶⁰ While some have brought suit against the CPB for violations of their civil rights,¹⁶¹ these initiatives have not received widespread attention either from the public or from U.S. federal or state legislatures. If anything, the agency’s power appears to be expanding. In April 2022, the Department of Homeland Security (the umbrella organization that oversees CPB) generated an outcry when it announced the creation of a Disinformation Governance Board to police online speech in the name of national security.¹⁶²

¹⁵² EFF, “NSA Timeline 1791–2015.” *Electronic Frontier Foundation*. N.D. <https://www.eff.org/nsa-spying/timeline>.

¹⁵³ Goitein, Elizabeth. “How the CIA Is Acting Outside the Law to Spy on Americans.” *The Brennan Center for Justice*, Feb. 15, 2022. <https://www.brennancenter.org/our-work/analysis-opinion/how-cia-acting-outside-law-spy-americans>.

¹⁵⁴ Turner Lee, Nicol and Caitlin Chin. “Police surveillance and facial recognition: Why data privacy is imperative for communities of color.” *Brookings*, Apr. 12, 2022. <https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>.

¹⁵⁵ Valentino-DeVries, Jennifer. “Tracking Phones, Google Is a Dragnet for the Police.” *The New York Times*, Apr. 13, 2019. <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html>.

¹⁵⁶ Harris, Mark. “How Peter Thiel’s Secretive Data Company Pushed Into Policing.” *Wired*, Aug. 9, 2017. <https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/>.

¹⁵⁷ Hvistendahl, Mara. “How the LAPD and Palantir Use Data to Justify Racist Policing.” *The Intercept*, Jan. 30, 2021. <https://theintercept.com/2021/01/30/lapd-palantir-data-driven-policing/>.

¹⁵⁸ Lau, “Predictive Policing Explained.”

¹⁵⁹ Misra, Tanvi. “Inside the Massive U.S. ‘Border Zone’.” *Bloomberg*, May 14, 2018.

<https://www.bloomberg.com/news/articles/2018-05-14/mapping-who-lives-in-border-patrol-s-100-mile-zone>.

¹⁶⁰ ACLU, “The Constitution in the 100-mile Border Zone.” *The American Civil Liberties Union*, N.D. <https://www.aclu.org/other/constitution-100-mile-border-zone>.

¹⁶¹ N.A., “Hold CPB Accountable.” N.D. <https://holdcbpaccountable.org/about-us/>.

¹⁶² Woodruff Swan, Betsy and Daniel Lippman. “Small group, big headache: Inside DHS’ messy Disinformation Governance Board launch.” *Politico*, May 5, 2022. <https://www.politico.com/news/2022/05/05/dhs-disinformation-board-mayorkas-00030123>.

In short, the sphere of privacy in America has been systematically contracting.¹⁶³ The U.S. government is now an observer of, and at times participant in, the day-to-day economic transactions of hundreds of millions of people, from ordering groceries to wiring money to paying a friend back for dinner.¹⁶⁴ This activity produces a rich trail of data that e-commerce providers and payment processors often sell to data brokers, who in turn resell it to companies and the government.¹⁶⁵ Police cameras and drones monitor how often Americans leave their apartments or neighborhoods, where they go, and who they spend time with.¹⁶⁶ ¹⁶⁷ ¹⁶⁸ Advertisers buy ads on social media sites, which enables them to collect user data that they can, in turn, sell to other companies and the government.¹⁶⁹

This process has not faced meaningful pushback from American civil society; indeed, it has often been accelerated by broad and enthusiastic popular support. Political candidates who implement or demand increased surveillance are often rewarded—not punished—electorally.¹⁷⁰ ¹⁷¹ This suggests that, over the long term, the electoral process cannot be meaningfully relied upon to protect basic human rights, including the right to privacy and the right to freely transact. This has significant implications for the future of the form of democratic governance practiced in the United States.

¹⁶³ Bode, Karl. “The Decade We Learned There’s No Such Thing as Privacy Online.” *Vice: Motherboard*, Dec. 31, 2019. <https://www.vice.com/en/article/epgdvz/the-decade-we-learned-theres-no-such-thing-as-privacy-online>.

¹⁶⁴ Fitzsimons, Tim. “Venmo, PayPal, Cash App must report \$600+ in business transactions to IRS.” *NBC News*, Jan. 6, 2022. <https://www.nbcnews.com/news/venmo-paypal-zelle-must-report-600-transactions-irs-rcna11260>.

¹⁶⁵ Knowledge at Wharton Staff, “Your Data Is Shared and Sold... What’s Being Done About It?” *Knowledge at Wharton*, Oct. 28, 2019. <https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/>.

¹⁶⁶ Lapientytė, Jurgita. “This is the most heavily surveilled city in the US: 50 CCTV cameras per 1,000 citizens.” *cybernews*, Feb. 22, 2021. <https://cybernews.com/editorial/this-is-the-most-heavily-surveilled-city-in-the-us-50-cctv-cameras-per-1000-citizens/>.

¹⁶⁷ Koebler, Jason, Emanuel Maiberg, and Joseph Cox. “This Small Company Is Turning Utah Into a Surveillance Panopticon.” *Vice: Motherboard*, Mar. 4, 2020. <https://www.vice.com/en/article/k7exem/banjo-ai-company-utah-surveillance-panopticon>.

¹⁶⁸ Richards, Sam. “This Is Footage From a Spy Plane That Flew Above George Floyd Protests in Minneapolis.” *Vice: Motherboard*, Jul. 29, 2020. <https://www.vice.com/en/article/qj4end/this-is-footage-from-a-spy-plane-that-flew-above-george-floyd-protests-in-minneapolis>.

¹⁶⁹ Ng, Alfred. “What Does It Actually Mean When a Company Says, ‘We Do Not Sell Your Data?’” *The Markup*, Sep. 2, 2021. <https://themarkup.org/ask-the-markup/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data#:~:text=Even%20though%20companies%20like%20Facebook,your%20personal%20information%20in%20return..>

¹⁷⁰ Zorabedian, John. “Where do US presidential candidates stand on privacy and surveillance?” *Naked Security by Sophos*, Feb. 2, 2016. <https://nakedsecurity.sophos.com/2016/02/02/where-do-us-presidential-candidates-stand-on-privacy-and-surveillance/>.

¹⁷¹ Malone, Scott. “Massachusetts Senate candidates spar on surveillance programs.” *Reuters*, Jun. 18, 2013. <https://www.reuters.com/article/us-usa-congress-massachusetts/massachusetts-senate-candidates-spar-on-u-s-surveillance-programs-idUKBRE95H10P20130619>.

As political avenues to protect civil liberties become increasingly ineffective, today's cypherpunks turn to a-jurisdictional open-source code.

Stablecoins

Stablecoins are Private Bank-Created Dollars

If CBDCs are programmable cash, or M0 money supply, then stablecoins are programmable money—M1 or M2 money supply, akin to the dollars created by commercial banks as part of their ongoing lending operations. But stablecoins are not “digital dollars”—digital representations of M2 money supply—as described above. Instead, they are “cryptographic tokens which circulate on public blockchains and aim to track the return of sovereign currencies.”¹⁷² The underlying blockchain used to track the circulation of different stablecoins varies, but the stablecoin token is always pegged to the value of the fiat currency it represents. Ownership of stablecoins is proved by ownership of a private key, which allows a user to spend from a blockchain address. Stablecoins are usually backed 1:1 by the fiat currency they mirror (its M1 or M2 money supply), though they may also be backed by other assets, like gold or bitcoin.¹⁷³

Because stablecoins are privately issued money used worldwide to achieve final settlement across financial institutions and platforms, they closely resemble eurodollars. Eurodollars, which have been in existence since 1954, are fiat currencies issued by private banks outside the fiat currency's country of origin.¹⁷⁴ Eurodollars are mostly denominated in U.S. dollars, but can be used to track other fiat currencies as well. For this reason, some refer to stablecoins as “cryptodollars.”¹⁷⁵ However, eurodollars are typically not backed by U.S. dollars or Treasuries; for this reason, they have at most an indirect effect on the U.S. money supply.¹⁷⁶ Many cryptodollars, by contrast, are backed by U.S. currency. For this reason, backed cryptodollars could serve as a powerful new source of demand for U.S. dollars and Treasuries worldwide in an era when their status as a reserve currency is increasingly in question.¹⁷⁷

¹⁷² Castle Island Ventures, “Cryptodollars: The Story So Far.” Jul. 7, 2020.

https://cdn.b12.io/client_media/2nMpL8WQ/2b43d97c-c061-11ea-a23f-0242ac110002-Cryptodollars_Castle_Island_Ventures_2020-07-07.pdf.

¹⁷³ Castle Island Ventures, “Cryptodollars.”

¹⁷⁴ Schenk, “The Origins of the Eurodollar Market in London.”

¹⁷⁵ Castle Island Ventures, “Cryptodollars.”

¹⁷⁶ Balbach, Anatol B. and David H. Resler. “Eurodollars and the U.S. Money Supply.” *Federal Reserve Bank of St. Louis*, June/July 1980. https://files.stlouisfed.org/files/htdocs/publications/review/80/06/Eurodollars_Jun_Jul1980.pdf.

¹⁷⁷ Alden, Lyn. “The Fraying of the US Global Currency Reserve System.” *Lyn Alden Investment Strategy*, Dec. 2, 2020. <https://www.lynalden.com/fraying-petrodollar-system/>.

Stablecoins enable fast, low-cost transacting and settlement in fiat currencies by bypassing many of the frictions and fees of the global banking system. They also enable users to hold cryptocurrencies in a less volatile format that can be easily exchanged for other, non-fiat cryptocurrencies. The vast majority of stablecoin transactions take place on cryptocurrency exchanges, many of which also issue their own stablecoins. Exchanges must comply with the identity verification requirements of AML/KYC in order to operate in many countries, which has been driving compliance worldwide.¹⁷⁸

Stablecoin usage has exploded since they were first introduced in 2017; their market capitalization reached nearly \$150 billion by the end of 2021.¹⁷⁹ In 2021 alone, the market capitalizations of the leading stablecoins grew between 500%-1,300%, and stablecoins had come to represent nearly two-thirds of total cryptocurrency trading volume by January 2022.¹⁸⁰ By far the most popular stablecoins worldwide are pegged to the U.S. dollar; these represent over 99% of all stablecoins in circulation as of Q2 2022.¹⁸¹

The Push for Regulation

Some government officials perceive stablecoins as a threat to central banks' control over money supply and capital markets. Jerome Powell, chairman of the U.S. Federal Reserve, has said, "You wouldn't need stablecoins, you wouldn't need cryptocurrencies if you had a digital U.S. currency [CBDC]."¹⁸² In 2021, U.S. Treasury Secretary Janet Yellen chaired the President's Working Group on Financial Markets, which produced a report outlining the risks stablecoins might pose to the U.S. banking system.¹⁸³ ¹⁸⁴ Chairman of the U.S. Securities and Exchange Commission, Gary Gensler, has stated outright that the SEC has regulatory authority over stablecoins: "Make no mistake: It doesn't matter whether it's a stock token, a stable value token backed by securities, or any other virtual product that

¹⁷⁸ George, Benedict. "What Is KYC and Why Does It Matter For Crypto?" *CoinDesk*, Mar. 25, 2022.

<https://www.coindesk.com/learn/what-is-kyc-and-why-does-it-matter-for-crypto/>.

¹⁷⁹ Cecchetti, Stephen G. and Kermit L. Schoenholtz, "Stablecoin: The Regulation Debate." *Money & Banking*, Dec. 13, 2021. <https://www.moneyandbanking.com/commentary/2021/12/13/stablecoin-the-regulation-debate>.

¹⁸⁰ Redman, Jamie. "Expanding Crypto Market Caps by 500% to 1,300%: Stablecoin Issuance Saw Significant Growth Last Year." *Bitcoin.com*, Jan. 11, 2022. <https://news.bitcoin.com/expanding-crypto-market-caps-by-500-to-1300-stablecoin-issuance-saw-significant-growth-last-year/>.

¹⁸¹ "Share of Fiat-Backed Stablecoin Supply (in USD) by Currency." *The Block*, May 16, 2022.

<https://www.theblockcrypto.com/data/decentralized-finance/stablecoins/share-of-fiat-backed-stablecoin-supply-in-usd-by-currency>.

¹⁸² MacKenzie Sigalos, "Why the Fed hates cryptocurrencies and especially stablecoins." *CNBC*, Jul. 16, 2021.

<https://www.cnbc.com/2021/07/16/jerome-powell-promotes-cbdc-digital-dollar-warns-against-stablecoins.html>.

¹⁸³ Vigna, Paul. "Risks of Crypto Stablecoins Attract Attention of Yellen, Fed and SEC." *The Wall Street Journal*, Jul. 17, 2021. <https://www.wsj.com/articles/risks-of-crypto-stablecoins-attract-attention-of-yellen-fed-and-sec-11626537601>.

¹⁸⁴ President's Working Group on Financial Markets, "Report on Stablecoins." *U.S. Department of the Treasury*, Nov. 1, 2021. https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

provides synthetic exposure to underlying securities. These platforms – whether in the decentralized or centralized finance space – are implicated by the securities laws and must work within our securities regime.”¹⁸⁵

Indeed, regulatory scrutiny of stablecoins has intensified significantly after the Terra/LUNA/UST debacle of 2022. A bit of historical context: In 2018, a venture-backed startup called Terraform Labs¹⁸⁶ launched with a new public blockchain, Terra, ostensibly built specifically for decentralized finance (“DeFi”) use cases. In 2020, Terraform Labs introduced a new stablecoin, UST, on its blockchain. Unlike most stablecoins, however, UST was not backed by collateral (although a nonprofit foundation, the Luna Foundation Guard, eventually began raising billions of dollars in forex reserves to one day back the currency—mostly in bitcoin). Instead of backing its assets, UST relied on an algorithm, the Terra protocol, that supposedly created market-based incentives to maintain its peg with the U.S. dollar using a Terra-native token called LUNA.^{187 188}

UST did very well in the bull-run climate of 2021; however, on May 7, 2022, large amounts of UST selling began.¹⁸⁹ This sent the protocol into a “death spiral”: within a week, UST plunged from \$1 to 12 cents, while the LUNA token became effectively valueless, going from around \$85 to zero.^{190 191} Terra(LUNA)’s market capitalization dropped from \$40 billion to just over \$500 million, wiping out many investors.¹⁹²

¹⁸⁵ De, Nikhilesh. “SEC Chair Hints Some Stablecoins Are Securities.” *CoinDesk*, Jul. 21, 2021.

<https://www.coindesk.com/markets/2021/07/21/sec-chair-hints-some-stablecoins-are-securities/>.

¹⁸⁶ Terraform Labs. <https://www.terra.money/>.

¹⁸⁷ Orcutt, Mike and MK Manoylov. “Terra, Luna and UST: How we got here.” *The Block*, May 11, 2022.

<https://www.theblockcrypto.com/post/146444/terra-luna-and-ust-how-we-got-here>.

¹⁸⁸ Kelly, Liam J. and Robert Stevens. “What Is Terra? The Algorithmic Stablecoin Protocol Explained.” *Decrypt*, May 11, 2022. <https://decrypt.co/resources/what-is-terra-algorithmic-stablecoin-protocol-explained>.

¹⁸⁹ Gola, Yashu. “LUNA drops 20% in a day as whale dumps Terra’s UST stablecoin — Sell-off risks ahead?” *CoinTelegraph*, May 8, 2022. <https://cointelegraph.com/news/luna-drops-20-in-a-day-as-whale-dumps-terra-s-ust-stablecoin-selloff-risks-ahead>.

¹⁹⁰ Karpal, Arjun. “Cryptocurrency luna now almost worthless after controversial stablecoin it is linked to loses peg.” *CNBC*, May 12, 2022. <https://www.cnbc.com/2022/05/12/cryptocurrency-luna-now-almost-worthless-after-ust-falls-below-peg.html>.

¹⁹¹ Karpal, Arjun, and Ryan Browne. “Cryptocurrency luna crashes to \$0 as UST falls further from dollar peg.” *CNBC*, May 13, 2022. <https://www.cnbc.com/2022/05/13/cryptocurrency-luna-crashes-to-0-as-ust-falls-from-peg-bitcoin-rises.html>.

¹⁹² IANS, “Terra Luna cryptocurrency collapses 98%, investors lose life savings.” *Business Standard*, May 12, 2022. https://www.business-standard.com/article/finance/terra-luna-cryptocurrency-collapses-98-investors-lose-life-savings-122051200809_1.html.

This vulnerability to “death spirals” has been described as a key characteristic of algorithmic stablecoins by a number of authors, perhaps most succinctly by Dr. Ryan Clements, assistant professor at the University of Calgary.¹⁹³ In short, when an algorithmic stablecoin slips below its peg, the algorithm will automatically start minting more of its paired token (in this case, LUNA). This creates downward price pressure on the token, incentivizing token holders to sell it immediately rather than hold it and wait for the price to recover (which, as they know, is unlikely to happen).¹⁹⁴

The UST fiasco quickly prompted new calls for regulation of stablecoins: U.S. Treasury Secretary Janet Yellen renewed her request that Congress pass legislation regulating stablecoins by the end of 2022.¹⁹⁵ The same request was made several times in 2021, most explicitly in the report published by the President’s Working Group on Financial Markets, which Yellen Chaired.¹⁹⁶ ¹⁹⁷ The report advised Congress to pass a law limiting stablecoin issuance to insured depository institutions, which would in effect make the traditional financial system the sole issuer of stablecoins. So far, this proposal has met with bipartisan resistance,¹⁹⁸ but there is little doubt that additional regulatory scrutiny of stablecoins is on the horizon.

Tether, the most popular and highly capitalized stablecoin worldwide, has also drawn the concern of regulators both in the U.S. and beyond. Tether’s reserve asset composition has been difficult to determine at various periods throughout its history. Its parent company, Tether Holdings Ltd., settled with the New York Attorney General in February 2021 for \$18.5 million after a protracted lawsuit claiming that it had lied about its reserves and hid losses of funds.¹⁹⁹ ²⁰⁰ As a result of the settlement, Tether Holdings committed to publishing quarterly reports for the NYAG outlining its reserves; these

¹⁹³ Clements, Ryan. “Built to Fail: The Inherent Fragility of Algorithmic Stablecoins.” *The Wake Forest Law Review*, Oct. 25, 2021. <http://www.wakeforestlawreview.com/wp-content/uploads/2021/10/11WakeForestLRevOnline131.pdf>.

¹⁹⁴ Hayes, Arthur. “Luna Brothers, Inc.” *Entrepreneur’s Handbook*, May 12, 2022. <https://entrepreneurshandbook.co/luna-brothers-inc-712ec5abe199>.

¹⁹⁵ Post, Kollen. “US Treasury Secretary Yellen points to UST slip, asks for new stablecoin legislation by the end of 2022.” *The Block*, May 10, 2022. <https://www.theblockcrypto.com/linked/146048/us-treasury-secretary-yellen-points-to-ust-slip-asks-for-new-stablecoin-legislation-by-the-end-of-2022>.

¹⁹⁶ Post, Kollen. “House and Senate hearings on stablecoins will spotlight official behind Treasury report: sources.” *The Block*, Feb. 2, 2022. <https://www.theblockcrypto.com/post/132827/house-and-senate-hearings-on-stablecoins-will-spotlight-official-behind-treasury-report-sources>.

¹⁹⁷ President’s Working Group on Financial Markets, “Report on Stablecoins.”

¹⁹⁸ Post, “House and Senate hearings on stablecoins.”

¹⁹⁹ Yang, Yueqi. “Tether Fails to Dispel Mystery on Stablecoin’s Crucial Reserves.” *Bloomberg*, Dec. 3, 2021.

²⁰⁰ Ostroff, Caitlin. “Tether’s Peg Slips Below \$1 as Pressure Builds on Stablecoins.” *The Wall Street Journal*, May 12, 2022. <https://www.wsj.com/livecoverage/stock-market-today-inflation-05-11-2022/card/tether-s-peg-slips-below-1-as-pressure-builds-on-stablecoins-WFmrWXcUCrd87vgYQgig>.

are now known to include a number of potentially insecure assets, like loans, commercial paper from unknown sources, and reverse repo notes.²⁰¹ After the UST/LUNA collapse, investors concerned about Tether’s solvency began a sell-off that also caused it to briefly slip below its peg with the U.S. dollar.

In August of 2022, Scott Beck, CEO of United Texas Bank, testified before the Texas State Work Group on Blockchain Matters, an expert group established by Texas statute to make policy recommendations for the state of Texas.²⁰² Beck stated that stablecoin issuers were “effectively sucking deposits out of the banking industry.”²⁰³ He argued that because stablecoin issuers cannot hold deposits at the Federal Reserve, and because stablecoins are not insured by the U.S. Federal Deposit Insurance Corporation (aka “FDIC insured”), they introduce systemic risk into the global financial system.

However, this argument is somewhat circular, as many stablecoin issuers are in fact seeking to become fully-reserved, federally-chartered commercial banks,²⁰⁴ but are unable to hold deposits at the Federal Reserve until they receive those bank charters. For its part, the Federal Reserve has so far refused to approve master accounts for many banks that custody cryptocurrency assets. One such bank, Custodia, filed suit against the Federal Reserve in June of 2022, alleging that the agency is unlawfully delaying its application process.²⁰⁵

This tension results from the questions that bitcoin and stablecoins necessarily raise about the future role of banks—including central banks—in human societies. We argue here that the core value proposition of banks—providing trusted custodianship of valuable assets and creating credit—are enduring social functions that will not go away. These functions can easily accommodate new form factors for money, like stablecoins and bitcoin.

²⁰¹ Adachi, Mitsutoshi, Alexandra Born, Isabella Gschossmann, and Anton van der Kraaij. “The expanding functions and uses of stablecoins.” *European Central Bank*, Nov. 2021. https://www.ecb.europa.eu/pub/financial-stability/fsr/focus/2021/html/ecb.fsrbox202111_04~45293c08fc.en.html.

²⁰² Texas Work Group on Blockchain Matters. <https://texas-scg5.demo.socrata.com/stories/s/fxdd-vpwt>.

²⁰³ Turner Wright. “United Texas Bank CEO wants to ‘limit the issuance of US dollar-backed stablecoins to banks’.” *Coin Telegraph*, Aug. 19, 2022. <https://cointelegraph.com/news/united-texas-ceo-wants-to-limit-the-issuance-of-us-dollar-backed-stablecoins-to-banks>.

²⁰⁴ Jeremy Allaire. “Our Journey to Become a National Digital Currency Bank.” *Circle Blog*. Aug. 9, 2021. <https://www.circle.com/blog/our-journey-to-become-a-national-digital-currency-bank>.

²⁰⁵ James Rubin. “Crypto Bank Custodia Sues Federal Reserve.” *CoinDesk*, Jun. 7, 2022. <https://www.coindesk.com/policy/2022/06/07/crypto-bank-custodia-sues-federal-reserve/>.

The Future of Stablecoins: 1:1 Collateralization at Banks

In light of both the general characteristics of stablecoins and the risks posed by algorithmic and under-collateralized stablecoins discussed above, it is the argument of this paper that stablecoins would create the most value for the U.S.--and global--economy if they were issued by private banks, defined broadly to also include new financial institutions like cryptocurrency exchanges and neobanks, so long as they meet the objective requirements outlined for chartered banks. Stablecoins should be fully backed--1:1--with U.S. dollars, Treasuries, gold, bitcoin, or other hard assets. This would require some regulatory oversight, but not a monopoly over stablecoins by either central banks or existing financial institutions. Indeed, as Vice Chair for Supervision of the U.S. Federal Reserve, Randal Quarles, stated in 2021: “the concern that stablecoins represent the unprecedented creation of private money and thus challenge our monetary sovereignty is puzzling, given that our existing system involves—indeed depends on—private firms creating money every day.”²⁰⁶

It is such privately issued, well-collateralized cryptodollars that represent genuine innovation in the already highly digital dollar economy. Private stablecoins would dramatically increase the speed and reduce the costs of cross-border, cross-platform transactions and settlement while entrenching the U.S. dollar’s status as the world’s reserve currency. Perhaps most importantly, privately issued stablecoins could preclude the worst violations of individual privacy and currency control that are virtually certain with the imposition of state-managed CBDCs.

²⁰⁶ Quarles, “Parachute Pants and Central Bank Money.”

Conclusion

We live in a world characterized by the systematic erosion of individual privacy, which leads inexorably to the extinction of freedom. While the United States remains a liberal democracy for now, all indicators show that we are on path to the kind of authoritarianism characteristic of strong states like China. The rise of the internet and the global software industry has provided new tools for both governments and corporations to maximize their influence over large populations for control and profit. These digital tools have made it difficult for individuals to exercise ownership of their property, as economic transacting increasingly occurs only with the permission of the state. In this way, an important vector of resistance to state power by civil society is being fundamentally eroded.

Central bank digital currencies (CBDCs) represent an extension of this state control over economic life. CBDCs provide governments with direct access to every transaction in that currency conducted by any individual anywhere in the world. As governments worldwide routinely share data with one another,²⁰⁷ ²⁰⁸ individual transaction data will quickly become known to any government in a data-sharing arrangement. Given the frequency with which government databases are compromised, this arrangement virtually ensures that anyone's transaction data will eventually become available for global perusal. CBDCs also enable governments to prohibit, require, disincentivize, incentivize, or reverse transactions, making them tools of financial censorship and control. Moreover, as a direct liability of central banks, CBDCs become a new vanguard for the imposition of monetary policy directly on consumers: such policies include, but are not limited to, negative interest rates, penalties for saving, tax increases, and currency confiscation. In these ways, governments will unsuccessfully attempt to pay down ballooning national debts using private capital from individuals—about half of whom (worldwide) live on less than \$5.50 per day.²⁰⁹

Clearly, individuals and organizations need to transact digitally with fiat currencies, and the current global banking system often makes those transactions slow and expensive. To solve this problem, cryptographic stablecoins pegged to fiat currencies and backed 1:1 with hard collateral can be issued by private banks worldwide. This would provide all of the purported benefits of CBDCs for end users while precluding the levels of surveillance and control that CBDCs offer the state. In this way,

²⁰⁷ N.A., "Which countries could have access to your data?" *Amnesty International*, N.D.

<https://www.amnesty.org.uk/which-countries-access-your-data-nsa-gchq-five-eyes-snowden-surveillance#:~:text=The%20top%20table%20of%20intelligence,countries%20across%20Asia%20and%20beyond>.

²⁰⁸ N.A., "Five Eyes." *Privacy International*, N.D. <https://privacyinternational.org/learn/five-eyes>.

²⁰⁹ Lugo, Maria Ana and Dean Mitchell Jolliffe. "Why the World Bank is adding new ways to measure poverty." *The World Bank*, Oct. 17, 2018. <https://blogs.worldbank.org/developmenttalk/why-world-bank-adding-new-ways-measure-poverty>.

stablecoins could also preclude the elimination of physical cash—which the United States should continue to issue out of respect for the values of individual privacy and liberty.

Finally, Bitcoin will endure as a monetary tool for those who wish to preserve a sphere of individual self-determination on the internet. While humans have always inhabited a multi-currency world, today that reality takes on a new meaning as bitcoin—an a-jurisdictional, stateless cryptocurrency—gains adoption alongside sovereign fiat currencies. No government can “regulate bitcoin out of existence,” as it has no headquarters, no leader, no legally incorporated organization, and no jurisdiction. Jurisdictional arbitrage between nation-states will facilitate the availability of bitcoin for the world. The Bitcoin protocol’s commitment to privacy, censorship resistance, and freedom make it a bulwark of individual protection in the face of technologically augmented institutional power. And as a natively digital currency, bitcoin has not only enabled the creation of stablecoins, but continues to underpin their utility, as a number of stablecoins use the Bitcoin blockchain for final settlement.

For most people, a combination of physical cash, bitcoin, digital dollars, and privately issued, well-collateralized stablecoins will cover virtually all monetary use cases. Physical cash and bitcoin will preserve a realm of individual financial privacy, while private stablecoins will place at least some checks on the surveillance and censorial powers of governments. Both bitcoin and private stablecoins will enable instant, low-cost digital transacting both domestically and across borders. Digital dollars and stablecoins will continue to be subject to AML/KYC compliance by the platforms that facilitate transacting with them. In this currency ecosystem—which is with us already—the creation of CBDCs is, quite simply, unnecessary.

It is a truism that technological innovation cannot be slowed down. One of the characteristics of technology is that it amplifies power—both for those previously disempowered, and for well-entrenched institutions. The competitive dynamics created by technological innovation, in which everyone races to stay ahead of their rivals, often create unwanted second-order effects. We should think carefully about what kinds of “innovation” we want the U.S. government to embrace, so that we do not unexpectedly find ourselves without rights—and without recourse.

The assumption that leaders we empower with technology will always work in the public interest and for the public good is one of the myths dispelled by the political theorists of the Enlightenment. The principle that power corrupts gave rise to the separation of powers and to the highly federated form of government that has characterized the United States since its foundation. As Professor Andrew

Ferguson at the American University Washington College of Law has succinctly stated, “Assume the tyrant.”²¹⁰

This does not mean that we call for the U.S. government to remain weak in the face of threats by other national governments. Rather, we invite policymakers, but first and foremost the American people to whom they are accountable, to *preserve a meaningful distinction* between the political economy of the United States and that of other countries. As the world goes the way of China in the 21st century, the United States should stand for something different: it should stand for freedom. For this reason, the United States should reject central bank digital currencies.

²¹⁰ Andavolu, Krishna. “State of Surveillance & Killing Dissent.” *Vice*, Season 2, Episode 2, Dec. 5, 2021. <https://www.sho.com/vice/season/2/episode/12/state-of-surveillance-and-killing-dissent>.