Testimony before the

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
Subcommittee on Digital Assets, Financial Technology and Inclusion

Regarding

"Digital Dollar Dilemma: The Implications of a Central Bank Digital Currency and Private Sector Alternatives"

September 14, 2023

Raúl Carrillo, Esq.

Academic Fellow, Lecturer in Law
Columbia Law School

Background & Summary

Chair Hill, Ranking Member Lynch, and distinguished Members of the Subcommittee, thank you for inviting me to testify. I offer my testimony as an Academic Fellow and Lecturer in Law at Columbia Law School, where my research focuses on financial technology and innovation. My scholarship draws on my experiences as an attorney providing legal services to low-income consumers and community groups in New York City and my upbringing in the U.S.-Mexico borderlands, a landscape defined by both financial deserts and omnipresent surveillance by federal law enforcement. I have also served as Special Counsel to the Enforcement Director of the Consumer Financial Protection Bureau (CFPB).

In my previous testimony before the House Financial Services Committee and its subcommittees and task forces, I have called for policymakers to consider the more profound impacts of nascent financial technologies on our society and our aspirations toward democracy. In a recent law review article, I join the call for a Digital Dollar system, while taking up the challenge of privacy and data governance within that system.[1] Today, I draw on that work, with a particular focus on finding common ground.

To frame our conversation more constructively, I will focus on two critical, faulty assumptions that dominate Digital Dollar discourse and limit innovation.

The first is a matter of legal and technological design. The myopic concentration on Central Bank Digital Currency (CBDC) as the only possible format for digital fiat currency and the attendant focus on the Federal Reserve System as the only set of institutions that might issue digital fiat currency or establish Digital Dollar infrastructure limits our vision. Although debates focused on the Fed may make for convenient political fodder, we do a disservice to the public when we restrict conversation to the Fed alone. We miss the forest for the trees. At a minimum, this conversation should include a discussion of the Treasury and its many bureaus already involved in daily money creation and deployment of financial technology.

The second is a matter of baseline privacy analysis. There is a profoundly mistaken assumption that we do not already live in a financial surveillance state. Background laws allow the government to evade data collection constraints by acquiring data from private sector entities. As a result, financial institutions, technology companies (including blockchain

[1] Raúl Carrillo, *Seeing Through Money: Democracy, Data Governance, and the Digital Dollar*, 57 Georgia Law Review 1207 (2023).

companies), and U.S. government agencies collectively enjoy virtually unfettered access to our financial records and regularly share data, information, and knowledge. We should be forcefully moving in the other direction.

Although counterintuitive to some CBDC critics, substantively reigning in government financial surveillance means limiting public-private partnerships, as direct relationships between the government and members of the public are more likely to engender constitutional protections, including protection under the Fourth Amendment. While I share fundamental commitments to privacy with many CBDC opponents, crude opposition to CBDC based on surveillance grounds is "throwing the baby out with the bathwater."

I conclude with ideas for moving forward with a new "public fintech" system. Most importantly, I respond to concerns regarding CBDC surveillance by advocating for the inclusion of "digital cash" within the Digital Dollar System to help mitigate data collection and preserve privacy. As such, I strongly support the Electronic Cash and Secured Hardware (ECASH) Act, reintroduced today.[2]

We can expand financial inclusion and access, help consumers and small businesses, and still preserve our hard-won civil rights in our exciting digital future.

CBDC and Beyond

Governments are now designing "digital fiat currency" (DFC)—public money native to government computers. The Biden Administration has mandated the exploration of a "Digital Dollar."[3] Governments could use a retail Digital Dollar system to distribute funds directly to individuals, households, and businesses, bypassing the commercial banking system. They could also deputize commercial banks to distribute DFC in some form. Some policymakers argue the U.S. government should limit the Digital Dollar system to wholesale "back-of-the-house" operations between banks and the central bank. Still, others see a role for public-private partnerships with fintech companies, including blockchain companies.

Thus far, the Federal Reserve System (Fed) has driven the policy conversation and argues any new infrastructure using "central bank digital currency" (CBDC) should still maintain banks

[2] For the previous iteration, see H.R. 7231, 117th Cong. *See also* Automatic Boost to Communities Act, H.R. 6553, 116th Cong. § 3 (establishing digital cash wallets as well as "FedAccounts").
[3] *See* Exec. Order on Ensuring Responsible Development of Digital Assets, Exec. Order No. 14,067, 87 Fed. Reg. 14, 143 (Mar. 9, 2022).

as intermediaries between the government and the public.[4] Herein, I echo many of the remarks made by my colleague, Prof. Rohan Grey of Willamette Law School, before the Financial Technology Task Force on June 15, 2021.[5]

First, I agree with his points about financial stability and macroeconomic risk, but do not repeat them here.

Second, and more importantly for this hearing, I strongly agree that properly designed and administered, a digital dollar system could improve financial access and equity, revitalize the direct public provisioning of payments and banking services, and ensure the United States meets the evolving challenges of the 21st-century digital economy. I believe the Federal Reserve should and will play a central role in any future digital dollar regime introduced in the United States. I also strongly endorse proposals for offering a public option for banking through FedAccounts, especially via partnerships with the U.S. Postal Service.[3] However, equating and reducing the Digital Dollar to CBDC is a mistake. The former category encompasses various designs, architectures, and arrangements. The latter category refers only to a narrow segment of that set of designs, in which central banks are the exclusive issuers and administrators.

The Fed is not and has never been the only federal entity responsible for issuing currency or administering public payments infrastructure. The Treasury operates several bureaus and components concerned with public finance and financial technology. The Mint, which issues coins, is the oldest monetary institution in the U.S. government, preceding the founding of the Fed by over a hundred years.[6] The Bureau of Engraving and Printing, also housed in the Treasury, is responsible for printing Federal Reserve Notes ("FRNs") on behalf of the Federal Reserve. Indeed, modern FRNs are themselves modeled on earlier Treasury Notes known as Greenbacks, which circulated concurrently with FRNs until 1971.[7]

---

[4] *See* Fed Board, Money and Payments: The U.S. Dollar in the Age of Digital Transformation (Jan. 20, 2022), https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf, [https://perma.cc/HZS5-999Z]. The Boston Fed is collaborating with MIT to explore CBDC. *See Project Hamilton Phase 1*, Fed. Res. Bank of Boston (Feb. 3, 2022), www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx. The New York Fed is exploring blockchain-based CBDC along with partnering banks. *Facilitating Wholesale Digital Asset Settlement*, Fed. Res. Bank of N.Y., https://www.newyorkfed.org/aboutthefed/nyic/facilitating-wholesale-digital-asset-settlement.

[5] *Digitizing the Dollar: Investigating the Technological Infrastructure, Privacy, and Financial Inclusion Implications of Central Bank Digital Currencies, Hearing Before the Task Force on Fin. Tech. of the H. Comm. on Fin. Serv.*, 117th Cong. (2021) (statement of Prof. Rohan Grey, Willamette Univ. College of Law).

[6] Curiously, a recently introduced anti-CBDC bill (H.R. 3402), called the "Power of the Mint Act," does not empower the Mint. It does not even mention the Mint.

[7] United States Treasury, *Legal Tender Status*, Frequently Asked Questions (Jan 1., 2011), https://www.treasury.gov/resource-center/faqs/Currency/Pages/legal-tender.aspx.

Another Treasury agency, the Bureau of the Fiscal Service, partners with commercial banks to issue prepaid debit cards to millions of benefit recipients, as well as military servicemembers overseas.[9] It also operates the TreasuryDirect program, through which individuals can acquire and hold digital book-entry securities directly at the Treasury without any involvement from the Federal Reserve or private intermediaries.[10]

Beyond the Treasury, the U.S. Postal Service provided postal banking services from 1910-1967 until Congress shut it down due to pressure from banking interests who saw it as a growing threat to their business model.[11] Today, the Department of Education is responsible for issuing, processing, and securitizing millions of student loans annually. GSEs trillions of dollars of U.S. government-backed financial assets that circulate in the capital markets as a form of near-money alongside Treasuries and Mortgage-Backed Securities issued by Freddie, Fannie, and Ginnie.[12]

The Surveillance Status Quo

Commercial Data Collection

Some policymakers have suggested that the U.S. government partner with fintech companies to build the Digital Dollar system. While there are surface-level advantages to such an approach, the visions often betray ignorance of (or ambivalence toward) the expansion of financial surveillance over the past decade, spurred by the evolution of the fintech industry.

Like other technology companies, fintech firms reconstitute people into "data doubles," which can then be sorted, stored, scored, shared, and sold. In doing so, fintech companies often partner with "data brokers"—underregulated conglomerates operating platforms that analyze and share data in a more sophisticated fashion. These companies and their champions claim that mass data collection makes financial services faster and easier, but also more automated, sophisticated, objective, predictive, accurate, and neutral, yielding more comprehensive assessments of human behavior. Allegedly, surveillance improves customer insights and the quality and pricing of algorithmic products and services.

While data brokers monitor our activity constantly, the public knows very little about them. In a December 2021 survey, The Clearinghouse—a payments company collectively owned by the largest U.S. commercial banks—found that 80% of consumer respondents were largely

unaware that fintech app providers partner with brokers to collect other financial data; 76% did not know brokers can sell that data to other parties; and 78% did not know brokers regularly access personal data even when the app is closed or deleted.[8]

Companies are especially interested in payments data because it is granular, ubiquitous, and necessary.[9] If social media activity says what we "like," payments data provides a clearer picture of what we do. Payments data provides information about how consumers actually spend money, which suggests patterns of future spending.[10]

Legally, we have very few data protections in this environment. The problem begins at the level of contract law, which is to say, at the user's fingertips. At their core, U.S. privacy laws hinge on a shallow theory of contractual consent. I want to be very explicit: This consent is a fiction. When users sign up for a mobile banking app, digital wallet, or even a standard credit card, they agree to privacy policies affirming the company's right to share data according to its terms. These contracts, known as "click-through contracts" are usually upheld via a "notice-and-choice" regime. As long as the company notifies us about potential data sharing and we click "I agree" to privacy terms we cannot modulate, courts consider companies to have met the standard of consent. Moreover, many of these contracts contain mandatory arbitration provisions, which courts do not review.

Leading scholars have concluded privacy laws on the books are insufficiently protective of people's data when private technology companies collect it.[11] There is no overarching substantive federal privacy law. Statutory law is industry-specific and primarily protects against data misuse rather than collection. The common law focuses on reputational injuries rather than the material consequences of privacy violations.

Statutes governing commercial collection offer little protection. The Financial Services Modernization Act of 1999 (the Gramm-Leach-Bliley Act, or "GLBA") requires financial institutions to notify their customers as to their privacy apologies and inform customers of their right to opt out of data sharing.[12] In practice, consumers do not do this because data sharing is an

---

[8] The Clearing House, 2021 Consumer Survey: Data Privacy and Financial App Usage 3 (Dec. 2021), https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2021-TCH-ConsumerSurveyReport_Final [https://perma.cc/M8D6-WYPW].

[9] Carrillo, *supra* note 1, at 1222-23.

[10] *See, e.g.,* Adam J. Levitin, *Pandora's Digital Box: The Promise and Perils of Digital Wallets*, 166 U. Pa. L. Rev. 305, 333 (2018) (arguing that "if general consumer information is digital gold, payment information is digital platinum…").

[11] For a discussion of this scholarship, see Carrillo, *supra* note 1, at 1226-38.

[12] *See* Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified and amended in various parts of 12 and 15 U.S.C.).

unavoidable term of service. The Fair Credit Reporting Act of 1970 (FCRA) nominally restricts data collection to credit, insurance, and employment purposes.[13] Yet courts have reduced FCRA to individual rights to correct inaccurate information and receive notices of negative judgment. Moreover, they often refrain from applying FCRA to data brokers.

Government Data Collection

As a general matter, so long as we consent to share *any* data with a private party, we have few claims against subsequent government use of that data. While there are no meaningful collection limits on the private sector, there are also no substantive legal constraints preventing the government from obtaining data collected by those businesses.

In my recent scholarship, I survey many harms that flow from public-private financial data sharing, including exacerbated identity fraud, erroneous disqualification from public benefits and infrastructure, and the increased punishment of people sending remittances to family members, people seeking reproductive healthcare services, and people attempting to land on their feet after release from carceral institutions.[14]

Most importantly, so long as the government purchases or otherwise procures data from financial institutions and service providers, the Fourth Amendment prohibition against unreasonable search and seizure does not apply. In 1976, in *U.S. v. Miller,*[15] the Court held that government access to third-party banking records was not a "search" for purposes of the Fourth Amendment, as there is no "reasonable expectation of privacy" in records shared with a third party. This principle, known as the *third-party doctrine,* now shapes all U.S. privacy laws and enables mass surveillance generally.

In the wake of *Miller*, Congress passed statutes that failed to restore constitutional protections, most notably the Privacy Act of 1974[16] and the Right to Financial Privacy Act of 1978.[17] Like GLBA, these statutes focus on individual harms concerning proper notice-and-disclosure and individualized remedies, such as rights or private action for limited

[13] There are also explicit exceptions for government benefits, law enforcement, and other purposes. *See* 15 U.S.C. § 1681b.
[14] Carrillo, *supra* note 1.
[15] 425 U.S. 435, 442-43 (1976).
[16] *See* 5 U.S.C. § 552a.
[17] *See* 12 U.S.C. §§ 3401-3422.

damages. Moreover, surveillance statutes override many of the essential provisions of these privacy statutes.

Most importantly, the BSA/AML regime authorizes the Treasury Secretary to require financial institutions to pre-emptively report any transaction *potentially relevant to any possible violation of law*.[18] Many legal scholars argue the U.S. Treasury, entrusted with executing these laws, is failing its criminal mandate. Others argue the Treasury burdens financial institutions with nothing to show for it. Still, other scholars criticize the Treasury for engaging in harmful mass surveillance along lines of race and class and facilitating inequitable criminal punishment.

When discussing Digital Dollar surveillance capabilities, policymakers must honestly confront financial surveillance as it operates today.

Design Options

We need public infrastructure for digital finance that is inclusive, safe, accountable, and thus more democratic. Legally, because of the way privacy and data governance laws operate in the U.S., the Fed Board's vision of an intermediated Digital Dollar and other visions featuring private-public partnership would leave little room for privacy at a general level.

Of course, we must also consider data sharing between government agencies. There are examples of successful legal firewalls between administrative data collection and law enforcement.[19] Yet, for every instance of a legal firewall working, there is an equally significant chance of a legal firewall failing.[20]

To truly minimize abusive data collection within the Digital Dollar system, we should also engage in "privacy by design."[21] We should hardwire principles and values into components of the Digital Dollar system. If the devices and infrastructure we use cannot generate the desired data in the first place, institutions cannot abuse or lose that data.

---

[18] *See* 31 U.S.C. § 5318.

[19] For instance, the IRS does not share data with the Department of Homeland Security, arguing it would decrease tax compliance. *See, e.g.,* Jennifer Chang Newell, *Will Immigration Authorities Use Our Taxes to Go After Immigrants?*, ACLU (Apr. 23, 2018), https://www.aclu.org/blog/immigrants-rights/deportation-and-due-process/will-immigration-authorities-use-our-taxes-go.

[20] *See, e.g.,* Demand Progress, "Institutional Lack of Candor" A Primer on Recent Unauthorized Activity by the Intelligence Community (Sept. 27, 2017), https://s3.amazonaws.com/demandprogress/reports/FISA_Violations.pdf [https://perma.cc/F99Y-7R7D].

[21] Ann Cavoukian, a former Ontario Privacy Commissioner, coined the term "privacy by design." *See* Ann Cavoukian, Privacy by Design: The Seven Foundational Principles (2009), https://iapp.org/media/pdf/resource_center/Privacy%20by%CC20Design%20-%207%20Foundational%20Principles.pdf [https://perma.cc/U7FH-BPED].

Most policymakers (and scholars) envisioning the Digital Dollar system tend to imagine a design choice between two money types: *account money* and *token money*.[22] According to this view, account money, such as a bank deposit, functions as "points" within controlled institutional systems. When we pay for something at a store with a bank-issued debit or credit card, we transfer those points from our bank to a merchant's bank. Bank money travels on interbank *payment rails*—physical and virtual channels through which data travels to settle a transaction. On the other hand, digital token monies (such as new cryptocurrencies) travel on separate payment rails (blockchain systems) built with different software. However, users can take token money "off the rails" or "off-chain" for circulation. For this reason, many people wrongly assume cryptocurrency is better for privacy than bank money.

However, the account vs. token focus elides deeper systems design questions. It tends to narrow the Digital Dollar design debate to a single question: Should the Digital Dollar system connect to the banking system's current rails, perhaps improving them? Or should the Digital Dollar system incorporate a new, separate, blockchain-based system?

We can approach data governance with a more helpful design menu. Payment instruments do not generate data solely according to the properties of instruments but also the configuration of broader communications infrastructure. Most importantly, bank card and blockchain transactions operate "online." Whether users pay for things on the rails or off the rails, other actors on the internet may still record them.

A more fundamental, anterior distinction is at play: the difference between *ledger money* and *bearer money.* Bank deposits and cryptocurrency are both types of *ledger money.* Ledger money moves "on the rails" and records transactions "on the books"—it leaves an imprint of what we own and owe, when, and where. By contrast, *bearer money* can live "off the rails" and "off the books." Paper cash and metal coins do not require an intermediary operator or recordkeeper. When we transact with each other in cash, one party might decide to report the transaction, and cameras may record our exchange, etc., but cash payments do not generate data like bank and blockchain payments. Subject to certain conditions, "digital cash" devices that store money on hardware rather than software mimic the functions of paper cash.

The choice between ledger money and bearer money entails significant tradeoffs. When we use cash instead of bank deposits or cryptocurrency to make payments, firms and government

[22] For citations for the ensuing adopted text, see Carrillo, *supra* note 1, at 1238-51.

agencies cannot see through money as widely or deeply. However, cash offers fewer conduits to the rest of the financial system. Ultimately, both forms of financial technology are necessary in a democratic system.

Banking[23]

Centralized ledgers make our economy possible. Within an accountable legal regime, centralized ledgers offer obvious upsides for financial inclusion: precisely because of the way they record data, ledger systems are gateways into formal credit, insurance, and investment. Cash transactions only help build a credit file if tracked through vigorous effort. Only some insurance or investment companies accept cash payments (at least not without extensive recordkeeping). Although blockchain companies attempt to offer gateways into lending and investment, they rely on interfaces with the centralized ledger technology of banks and other financial institutions. People without bank accounts save at a much lower rate. Low savings increases the likelihood that these households will need to use the expensive alternative, "fringe financial services," and the unbanked bear tens of billions of dollars in annual costs for these services.

Ledger money transactions trigger fundamental consumer protections that do not cover blockchain or cash payments. People can use established payment records to defend against discrimination, unfairness, deception, and abuse by creditors and landlords. For example, when employers pay employees with cash rather than bank money or other traceable money, employees may be unable to point to a payment record to prove theft or fraud. The federal government insures deposits up to $250,000 per depositor, per bank. A bank will often replace funds following robbery, fraud, or loss of access to the bank account. By contrast, if you lose your bitcoin or paper cash, that money is likely gone forever.

However, there are severe downsides to over-reliance on ledger money without an accountable legal regime. Ledger money produces the data collected by platforms discussed in the previous section of this testimony. Moreover, banks themselves are collecting more and more data. They collect data to charge fees, freeze and block transactions, collect debts, garnish wages, and intercept tax refunds. Companies like Early Warning Services (owned by commercial banks in a consortium) now monitor payments activity and share data with other reporting agencies,

[23] For citations accompanying this adopted text, see Carrillo, *supra* note 1, at 1240-42.

often locking out legitimate customers in poor neighborhoods based on unsubstantiated fraud charges.

New partnerships also raise new concerns. Fintech companies that provide apps are filling the vacuum left by banks retreating from customer services. Indeed, many banks now partner with fintech firms, outsourcing the user experience, while the fintech companies evade banking regulations, including usury rates, deposit insurance, and other critical protections. Developers build *digital wallets* (predominantly mobile software apps like ApplePay, Venmo, and PayPal) on top of existing interbank payment rails. Wallet providers are now racing to build "super apps"—one-stop shops for data organization. Because super apps combine troves of account information, credit card numbers, PINs, and cryptographic keys *as a feature,* they increase fraud and breach risks for retailers and users alike.

Any vision for public banking must take data governance into account. As a starting point, government agencies can set strict regulatory limits on how bank account data can be used. If mobile phone applications connect to other accounts, they should do so via secure APIs. We can also separate the management of account data from the issuance of the currency. For instance, in the FedAccounts example, the Postal Service could serve as a custodian of user financial data to mitigate the central bank's potential abuse of power. A network of legally autonomous "sectoral and place-based data trusts" could give citizens access and democratic control over data that can improve their lives. These autonomous legal bodies would act as custodians and stewards of a specific data set, making sure that the data is stored safely.[24]

Blockchain[25]

Users make cryptocurrency payments using *distributed ledger technology (DLT).* Blockchain is the most popular type of DLT. Succinctly, blockchain shares the rights and responsibilities of a centralized ledger—including the power to see through money—among multiple participants.

Several policymakers and scholars have argued that the Digital Dollar should run on a blockchain. Yet there is no proof of a blockchain-based currency system reliably serving the

[24] Thomas M. Hanna, Mathew Lawrence, and Nils Peters, *A Common Platform: Reimagining Data and Platforms | Report*, Common Wealth (2020), https://www.common-wealth.org/publications/a-common-platform-reimagining-data-and-platforms.
[25] For citations accompanying this adopted text, see Carrillo, *supra* note 1, at 1242-44.

payment functions of bank accounts or cash. There is also no example of it providing the privacy features of cash. Far from hiding payments, blockchain systems share records with multiple, potentially millions of parties (some of whom have more power over the ledger system than others).

Although advocates of blockchain-based technologies notoriously tend to explain its essential functions in complicated ways, we can easily grasp the basic principles of data governance. When debating the origins of money, scholars often refer to the Micronesian island of Yap. However, the Yapese system is also unique in data governance. Arguably, the people of Yap have used distributed ledger technology for half a millennium. As part of their monetary system, communities place giant rocks, known as Rai stones, in specific places. However, to reduce the need to move the stones, the people of Yap have created a shared oral history regarding placement, value, and ownership. Each time stone ownership transfers, community members change their memory based on a collective consensus, trusting in communal transparency (not privacy) to maintain integrity. Although the Rai system can make counterfeiting and fraud difficult, individuals and groups can still collaborate to change the common oral history, assert an alternative account, or integrate false or malicious narratives.

The most popular distributed ledger technology, the Bitcoin blockchain, resembles the Rai system but relies on an internet ledger rather than oral history. It also depends on trust between strangers rather than within a community. Essentially, "miners" around the world solve challenging mathematical puzzles on computers to initiate payments and create an encrypted record of transactions. When miners achieve "consensus" about the transactions that have occurred and should occur, they "sync" their ledgers as if creating a single database. Although the blockchain shields transactions with complex cryptographic or semi-cryptographic mechanisms, it shares the transaction records with multiple parties.

The second most popular blockchain system, Ethereum, is more data-intensive than bitcoin and operates via more advanced *smart contracts* (software programs), which automate the transfer of coins. Smart contracts pull data from *off the chain* (information regarding other moves in stock prices, interest rates, exchange rates, etc.) using third-party *oracles* (software programs). In essence, Ethereum will make X payment on the chain if Y happens off the chain. Companies can use the Ethereum platform to conduct more complex financial transactions but also keep a record of non-monetary transactions on the blockchain.

Most importantly, for today's purposes, the Ethereum protocol also supports the "stablecoin" industry, which aims to avoid Bitcoin's volatility but also increases data governance concerns. Stablecoins are privately-issued digital financial instruments, denominated or pegged to fiat currency ($USD, etc.), held out as being just as valuable and reliable as government money—as stable as the dollar bill in your pocket. The stablecoin industry is now the backbone of the entire cryptocurrency industry, supplying "safe money" used in more significant trades, skyrocketing to over $119 billion in value in 2021 before crashing multiple times in 2022 and 2023. Although most stablecoin holders purchase the coins for investment purposes, issuers market them as payment tools. Moreover, many technology companies, most famously Meta (formerly Facebook), are interested in stablecoins due to their potential payments use cases.

Proponents argue blockchain is simultaneously (a) decentralized, (b) immutable, (c) transparent, and (d) anonymous, promoting inclusion and integrity. Yet these promises do not withstand scrutiny. As CFTC Commissioner Kristin Johnson has argued in her academic work, digital asset systems increasingly rely on powerful intermediaries.[26] Typically, a majority of recordkeepers (node validators) can collaborate to change the ledger and can even re-identify participants. The average user has little to no idea how these processes function, undermining claims of transparency.

Aspirationally, blockchain hides sensitive data about users, but in practice, blockchain systems necessarily interface with the surveilled infrastructure of the rest of the internet. Internet service providers can link pseudonyms and accounts. Although blockchain enables users to host their digital wallets, most people register with and use digital exchanges (third-party apps) to manage coins, and most people pay for coins with bank deposits or digital wallet balances that identify the customer.[27]

Some cryptocurrency advocates argue blockchain can protect vulnerable populations from law enforcement overreach. However, blockchain is an exceptional tracing tool.[28] While a blockchain's historical ledger will not list the names of parties to transactions, law enforcement authorities can download a copy of the ledger with the public key history and determine how

[26] Kristin N. Johnson, *Decentralized Finance: Regulating Cryptocurrency Exchanges,* 62 Wm. & Mary L. Rev. 1911 (2021).
[27] Pro-privacy companies are careful to note that transactions are not truly anonymous, because accounts on the Ethereum network are pseudonymous. *See, e.g.*, *Blockchain wallet FAQs*, MetaMask, https://metamask.io/faqs/.
[28] *See, e.g.,* Neal B. Christiansen & Julia E. Jarrett, *Forfeiting Cryptocurrency: Decrypting the Challenges of A Modern Asset*, 67 DOJ J. Fed. L. & Prac. 155, 166 (2019).

individual users have transferred cryptocurrency.[29] Legally speaking, this data is "publicly available," and agencies do not need to obtain subpoenas or warrants. Blockchain operators actively collude with law enforcement agencies to monitor payments and unmask identities.

Digital Cash[30]

Most money we use in the United States is ledger money (usually bank deposits). But cash is still the most common form of payment in the world. Unfortunately, governments are increasingly banning paper cash and metal coins, associating the most popular payment tool of poor people (and the most private payment tool for everyone) with underdevelopment and criminality. It is more appropriate to think of cash as entailing tradeoffs, like bank accounts and blockchain wallets.

Cash is the only genuine peer-to-peer legal tender: a public good and public infrastructure. For governments, cash is a cheap, generic technology that enables people to engage with each other, even in informal economies or during political crises. Cash of all kinds makes many businesses possible. For instance, the availability of an anonymous source of transactions is especially critical for companies that are legal in sub-federal but not federal jurisdictions. For example, cannabis shops now legally conduct business in most states, but federal law largely excludes them from the formal banking system. Mastercard and Visa would impose even heavier fees on retailers if they did not have to compete with cash.

The Digital Dollar system should include online bank accounts (and potentially digital wallets). Yet, we should be able to pay for things in our daily lives while avoiding targeted advertising, credit scoring, screen scraping, and extraneous data-sharing with law enforcement. This means uploading paper cash into the 21st Century.

Ultimately, the only surefire way to protect privacy is for policymakers to provide devices that enable offline transactions. Government-issued bearer money like paper cash and metal coins can enable payments beyond the sight of powerful institutions. Digital bearer money can achieve the same goal.

---

[29] *See Terrorism and Cryptocurrency: Industry Perspectives: Hearing Before U.S. House Comm. on Homeland Security, Subcomm. on Intelligence and Counterterrorism*, 117th Cong. (2022) (Statement of John Kothanek, VP of Global Intel. Coinbase), (testifying to the superior utility of blockchain technology in fighting illicit flows).

[30] For citations for this section, see Carrillo, *supra* note 1, at 1244-51, 1278-99.

For example, stored-value cards (a type of "smartcard") store money on the cards themselves, facilitating transactions that do not generate data for online systems to collect, store, share, or score. We already use relevant technology that functions offline, connecting devices to each other rather than a network. Devices using Bluetooth, near-field communication (NFC), or QR codes could enable payments while avoiding internet surveillance. Subject to network design, phone-based SIM cards can accomplish the same function.

These are principles embodied in the E-CASH Act, reintroduced today.[31] In some senses, the proposal is conservative. It helps preserve cash—a technology humans have used for thousands of years—in the digital era. The proposal also reduces harm: a shield against surveillance that materially punishes vulnerable populations, especially in the informal economy. Yet the proposal is also progressive, striving for public infrastructure and innovation.

Deepening the Debate

Some policymakers cast the digital fiat currency development as an arms race. I urge this subcommittee to instead focus on collaboration, shared research, and open standards as much as competition. In particular, we have much to learn from many governments around the world that are much further in terms of innovation and have much knowledge to share, especially concerning financial inclusion.[32] DFC discourse in the United States is comparatively impoverished and unimaginative. For example, many governments are already exploring offline payments.[33] In large part, this is because policymakers outside of the U.S. recognize that

[31] In my academic work, I offer just one modular proposal. The Treasury can issue a Digital Dollar, while the U.S. Postal Service can provide the infrastructure and devices to make it work. Other government institutions may be able to provide some or all of the devices. In any case, the plan would limit private-sector partnerships to research, development, and procurement, generally eschewing the delegation of data governance. Carrillo, *supra* note 1.

[32] *Id.* at 1278-99.

[33] *CBDCs in Emerging Market Economies*, (BIS Paper No. 123, Apr. 2022), https://www.bis.org/publ/bppdf/bispap123.pdf (finding emerging market economies ranks offline use as the most important feature to promote financial access). *See also CBDC Proof of Concept and Research Offline payments,* Digital Marketplace, https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/18203; John Kiff, *Taking Digital Currencies Offline*, IMF (Sept. 27, 2022), www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline; Fabio Panetta, *A digital euro that serves the needs of the public: striking the right balance*, Eur. Central Bank (Mar. 30, 2022), www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220330_1~f9fa9a6137.en.html; Gilad Edelman, *The Future of Digital Cash Is Not on the Blockchain*, Wired (Mar. 28, 2022), www.wired.com/story/digital-cash-ecash-act/.

unbanked and underbanked users often lack the smartphones and high-speed internet access necessary to use mobile apps.[34]

We are not properly funding the future of public money. With appropriate resources and administration, however, many talented people now working in the fintech and crypto industries could instead help build public infrastructure, including by upgrading cold, hard American cash.

More broadly, the design and marketing of public digital money should be a matter of widespread consultation among many groups and stakeholders. Simple polling of the public will not suffice. Individual users may think the benefits of payment data maximization outweigh the harms, which seem remote. However, individuals are not in a position to fully assess or evaluate the possibility of social harm. As more users relinquish privacy, institutions aggregate more data, and we increase the risk of privacy violations and consequent material harm for each user, specific populations, and the public as a whole.[35]

Should we choose to build the Digital Dollar system, it will impact everyone, just like any other major national infrastructure project, with significant political consequences. The development process must be more democratic so that private actors and obscure public bureaucrats from any agency do not inadvertently become the only official stakeholders and set the terms of the debate for everyone else.

Policymakers should support an array of Digital Dollar pilot programs and develop a steady rhythm of innovation, aiming to build a safe and secure financial system for all.

---

[34] 33% of adults lack high-speed internet access in their homes. Between 41% and 44% of adults in low-income communities lack high-speed internet access in their homes. Smartphones required for fintech outside the home are often prohibitively expensive. Terri Friedline, Banking on a Revolution 131-48 (2020).

[35] *See* Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World 265-80 (2016) (underscoring the conflict between individual and collective interests).