Paths Toward an Acceptable Public Digital Currency

By Jay Stanley
March 3, 2023

Serious discussions are underway inside the U.S. Federal Reserve and other central banks around the world on creating a new form of government-issued digital money. The Fed has already issued a policy paper and research report evaluating the idea, and in March, President Biden issued an executive order directing that the executive branch place "the highest priority on research and development" of such a "digital dollar."

There are good reasons to embrace the idea of a digital dollar (often called a "Central Bank Digital Currency," or CBDC, though such a currency could also be issued by the Treasury Department). There is clearly a high demand for digital monetary transactions in today's world, yet all the options for carrying out such transactions rely on private companies that have troubling records on privacy, freedom of expression, and accessibility — especially compared to the government currency that we already have: cash. Cash has a set of qualities that are good for freedom: It is universally accessible, universally accepted, relatively stable in value, and can be exchanged for goods and services without transaction fees. It can be used offline, and it lends itself to privacy, anonymity, free expression, and user control.

The companies that currently provide our electronic money, including the credit card oligopoly as well as payment networks such as Paypal and Venmo, spy on their customers' transactions. They frequently block transactions that they don't like, such as those related to sex or to political causes that are unpopular with the public — or with the government. And they are terrible when it comes to accessibility for people who are low-income or marginalized from the bureaucratic and technological structures that one must navigate to participate in digital transactions. The often exploitative fees they charge pose more barriers and suck dollars out of the economy for providing functions that could easily be provided for free by a true digital dollar.

Is cryptocurrency the answer? We share the values of those cryptocurrency and blockchain enthusiasts who embrace the technology because they believe money should be private and permissionless. But despite its enormous expansion as a speculative instrument, cryptocurrency has not become fully functional as an actual currency. While it has proven useful for some purposes such as making anonymous charitable contributions, vanishingly few retail purchases

are being made with cryptocurrency. Built on the ideals of decentralization and disintermediation of legacy financial institutions, it has become centralized and institutionalized. It requires some tech savvy and can't be used without an internet connection, which doesn't work for people who lack consistent quality access. And cryptocurrency has not lived up to the hopes it would protect privacy.

We can't predict how these technologies will evolve and what implications such evolution may have for civil liberties. Tools have been developed that can make cryptocurrencies more "cash-like" in their privacy, and the government should accept those tools insofar as they apply to ordinary people and transactions and otherwise conform to the principles we lay out here for a CBDC. But whatever uses cryptocurrencies come to serve in our society, we don't believe that they will become a functional digital dollar anytime soon.

That brings us back to a CBDC as a possible means of achieving a better digital payment system. The biggest problem with a government digital dollar is the prospect that it would be even worse for privacy than the companies we have now. There is little doubt that law enforcement and national security interests within the government will push for a system design that gives them sweeping powers to monitor and investigate even the smallest financial transactions. Some are skeptical that our government will ever allow a privacy-protective CBDC to come into effect.

On the other hand, it's safe to say that most Americans would not want a currency system that creates a government record every time they give a friend money for beer or pay a kid to mow their lawn. There are good reasons to think that libertarians, civil libertarians, liberals, conservatives, and populists would all for their own reasons oppose such a system and insist that any CBDC offer robust privacy protections.

A menu of options

The balance that will be struck between the government's ability to oversee financial transactions and the civil liberties interests in a free and private currency will be worked out through the design choices that are made in the creation of a public digital currency. So those design choices — whether made by the Fed, the executive branch, or Congress — have enormous importance.

In September 2022, the White House issued a report outlining various policy and technical options for how a public digital currency might be designed. That report provides an excellent framework for analyzing the range of options in how a CBDC could be designed, and we make use of its framework in this report.

The paper, which was produced by the White House's Office of Science and Technology Policy (OSTP), doesn't make recommendations for how a government digital currency should be structured; instead it offers a kind of menu of technical options that policymakers will need to choose from. Many of the options described in the report would spark fierce opposition from the ACLU and other privacy and civil liberties groups — and probably from Americans across the political spectrum. But among the "menu" listings there are also the makings of a digital currency system that would be entirely acceptable, and indeed could be an affirmative good for our nation and its people.

The White House paper does make *policy* recommendations, including three that address the biggest civil liberties concerns with a government digital currency:

1. **Preserving cash.** The report declares, "Use of the CBDC system should not be mandated. Offline capability should be incorporated, and the role of cash should be preserved." At the ACLU, we regard the preservation of physical cash as the starting point of any discussion of how currency and payments should work in the future.
2. **Privacy:** The report says that a CBDC "should maintain privacy and protect against arbitrary or unlawful surveillance." That's awfully weak, because surveillance doesn't have to be arbitrary or unlawful to be deeply problematic. More promisingly, the paper says that a CBDC should incorporate "privacy engineering best practices," including "privacy by design" and "dissociability," which means minimizing the links between data and identifiable people or devices. We also view this as vital — that anonymity of transactions, at least below a certain limit that meets the needs of regular people, should be built into the technological design of the system using the best available privacy technologies.
3. **Accessibility.** "All should be able to use the CBDC system," OSTP says, and it "should expand equitable access to the financial system." This is also a crucial policy goal for any public digital currency. Fixing the inaccessibility of the current financial system would be a major reason to implement a CBDC. It's also important to note that accessibility and privacy are linked; as the White House points out, a 2020 government study found that concern about privacy is one of the top reasons that unbanked households cite for why they don't have a bank account.

At the same time, however, the paper declares as a policy goal that a CBDC should "protect national security," "promote compliance" with Anti-Money Laundering (AML) and anti-terrorist financial-surveillance laws, and "mitigate illicit finance risks."

The trillion-dollar question is how the tensions and conflicts among the goals cited in this paper will be resolved in the design of a CBDC system. To what extent will the security agencies be permitted to use the transition from physical to digital dollars to expand their already too-broad visibility into Americans' financial lives? Physical cash allows for a great deal of privacy, a certain amount of which is used for illicit activity. The security agencies already have plentiful and overbroad powers to investigate people's finances — but would no doubt love to have new surveillance superpowers to try to reduce that illicit activity. The question is whether policymakers will bake surveillance into our digital financial system and toss out what remains of Americans' financial privacy in pursuit of that aim.

We recognize that the government has a legitimate interest in monitoring the transfers of large sums of money. Wealthy tax evaders or other criminals should not be offered new ways to send millions of dollars around the world undetected. What is needed is a system that protects the privacy of ordinary people while not hiding large transactions by wealthy people and companies. As far as we're concerned, the problem of how to build a CBDC *is* the problem of how to build that kind of a system.

Privacy-protecting cryptographic innovations must be at center of a CBDC

And privacy protections based on *policy* are not good enough. No one should support a CBDC system that generates centrally held usage data about every transaction and then purports to protect that data through a warrant requirement, as the OSTP paper seems to contemplate. Nor is the protection afforded by having data held by third-party intermediaries sufficient. Given uncertainties around how the courts will interpret the Fourth Amendment and the unreliability of lawmakers in protecting privacy, Americans need to be able to trust that the privacy of their past and future transactions won't be stripped away by some crisis, panic, or bad court ruling. We want a system that uses new and existing cryptographic techniques to make it, to the greatest extent possible, *technologically* impossible for the government (or any other party) to record ordinary transactions.

As we have discussed, one solution proposed in Congress would be a digital bearer instrument in which money is stored on a device with no party keeping track of balances on a centralized (or public) ledger. That would be the best, most cash-like option for digital money if the security questions around such a system could be addressed — not necessarily perfectly, but at least to the degree that would be reasonable given the privacy advantages such an architecture would bring.

In its menu of technology options, the OSTP paper does contemplate some limited offline options. And it discusses how transactions could be "tiered" to protect privacy, "with lower tiers facilitating a higher level of privacy in transactions than higher tiers." And, as the paper points out, transactions "could be limited to the lower tier with temporal restrictions on cumulative transfer amounts." That would stop somebody from trying to hide a million-dollar transfer simply by making a million one-dollar transfers, for example.

Even in a system not based on a pure bearer instrument, there are already a number of promising cryptographic technologies that could be used to protect people's privacy. For example, untraceable e-cash is an idea introduced 40 years ago by computer scientist and cryptographer David Chaum that by now has many well-developed realizations. It could allow the Fed to keep a central accounting of people's balances as they transact, while making it impossible for the central bank to see how much each transaction is worth and who the parties are. Other techniques include those used by privacy-protecting cryptocurrencies such as Zcash, Monero, and MobileCoin that use zero-knowledge proofs to ensure that each transaction is valid, even while hiding the details.

Another technique that cryptographers have developed would make it mathematically impossible for the Fed to see data about transactions below a certain size, but allow the agency to see the details of larger ones, or even groups of transactions that reach a certain size within a certain period of time. These kinds of limits should be baked into the technology so they can't be changed on anybody's whim. As the White House says in its report, "This could help increase consumer trust that the CBDC system's rules will not be changed haphazardly, and this could also help protect the CBDC system from being abused during periods of high political volatility."

Overall, the field of privacy-protecting cryptography is advancing quickly with a great deal of creative research that promises to allow us to "have our cake and eat it too" when it comes to privacy and security. As a result, there is absolutely no justification for a CBDC system not to make maximal use of all the latest and greatest privacy-protecting technologies.

It's true that not all of the available techniques may yet be sufficiently stress-tested for security and for practicality in actual implementation — but such testing does not happen by itself, and the federal government is in an excellent position to make sure it happens by promoting public and transparent research in cooperation with academia and other stakeholders. Indeed, the White House paper declares that "It is important that the U.S. Government direct resources and the research community toward solving" open questions about CBDC design, and that it will be "vital to bring an all-of-government approach to bear on a digital assets R&D agenda." The White House moved toward such an approach in January when it announced the creation of a government committee pursuing a "National Digital Assets Research and Development Agenda" and solicited public comments on what the research priorities should be.

Other policy choices

As we and our allies have stated before, we should aim for a digital dollar that is as close to physical cash as possible in its accessibility and protection of privacy. That has implications for a number of the other items on the CBDC design-choice menu laid out by the White House in its report. Among them are:

- **Intermediaries.** Some visions for a CBDC involve the government spinning off various functions to private companies. This may make sense in some narrow areas, but the whole point of a CBDC is to extend the role of money as a *public good* into the digital arena, not to put big banks or other financial players at the center of a system. That would allow them to continue to suck fees out of the financial system to the detriment of economic efficiency and accessibility for low-income people, and undercut much of the very rationale for a CBDC. Putting private, profit-oriented financial players at the center of a CBDC system also risks replicating the terrible privacy regime that we have now with digital transactions. As with physical cash, transacting with digital dollars should not incur fees; it should be created and run as a public good.
- **Offline transactions.** It's vital that offline and peer-to-peer transactions be enabled to the greatest extent feasible. A fully offline digital bearer instrument would be the ideal, but if that does not prove feasible, then the greatest possible degree of offline functionality should be enabled. The less frequently an internet connection is required to settle balances, the better, because the United States is a big country, and many places and people have poor to non-existent internet connectivity. Nor is it a good idea to create a payment system that stops working when there's an Internet outage due to natural disaster or other causes.
- **Fungible vs. non-fungible units.** Fungible dollars are basically all the same, while non-fungible dollars could be differentiated from each other. That means, for example, that non-fungible digital dollars could be marked or categorized in ways that make them more controllable than cash. For example, the White House points out that "non-fungible units could enable the limiting of certain CBDC to be used toward more economically-beneficial uses, especially during times of recession," and certain digital dollars "could be

marked as 'tainted' if they are used in illicit activity." This would allow the authorities granular control over how dollars are spent — blocking entities from accepting certain dollars, or providing that they can only be used to buy certain things, for example. Building non-fungible units is a bad idea. It's something that could never be done with cash, and (as the OSTP paper acknowledges) opens up wide avenues for centralized control and abuse.

- **Identification requirements.** Identification requirements should be minimized. If I'm buying and selling goods at a flea market or garage sale, I don't have to register with the government to accept cash. Unless someone is engaging in transfers of large amounts of money or the like, there is no reason to require every participant in a digital currency eco-system to rigorously identify themselves to a central ledger keeper. Where identification requirements are imposed, they should also make use of cryptographic privacy-protecting ID techniques that can satisfy some of the more reasonable administrative and security needs while protecting privacy to the greatest extent possible.
- **Transparency.** It's important that the software and hardware infrastructure behind a CBDC be transparent and subject to external, independent audits. As OSTP notes, an open-source approach "increases trust, security, reproducibility, and collaboration" and could reduce barriers to adoption, while "a degree of auditability will be important" as well as "the publication of data about the CBDC system using appropriate privacy-preserving approaches." Overall, as OSTP declares, transparency "is vital for people to believe the system is sufficiently safe, effective, and private for them to use."
- **Anti-money laundering rules**. A CBDC should be subject to the rules that apply to physical cash, and not the rules that apply to bank accounts. Under current law, cash transactions of $10,000 or more must be reported to the government by anyone "engaged in a trade or business," but cash is not otherwise generally subject to surveillance. Banks, however, are required to act like proxy police officers by "proactively monitoring and investigating suspicious activity" in their customers' accounts. And currently, "regulators are putting more pressure on financial institutions to know their customers in depth." Banks are also required to keep records of their customers' transactions in case the government wants to see them — and to carry out searches of that data for the government about any individual that any law enforcement agency claims is engaged in terrorism or money laundering.

Conclusion

CBDC policymakers and architects need a clear and early vision of what a good government digital currency system would look like. That vision should center around creating a system that replicates, to the greatest extent possible, the advantages of cash when it comes to privacy and accessibility for ordinary people. The construction of a digital dollar could, if done right, significantly advance financial inclusion and privacy. But it would be an unprecedented and historic task, potentially shaping the U.S. financial system for decades or even centuries to come. As such, its design needs to very carefully balance the government's legitimate interest in stopping large-scale tax evasion and other financial crimes against the need to keep the tentacles of its surveillance powers out of the lives of ordinary people and ordinary transactions. Such a system should reach that balance by making maximal use of the latest cryptographic innovations for protecting privacy.