

**Ann E. Misback
Secretary
Board of Governors of the Federal Reserve
230 S LaSalle Street
Chicago, IL 60604**

Sent via electronic mail to digital-innovations@frb.gov

May 20, 2022

**Request for Information – Federal Reserve White Paper - Money and Payments: The U.S. Dollar
in the Age of Digital Transformation**

**Submission from Americans for Financial Reform Education Fund and Demand Progress
Education Fund**

CBDC Benefits, Risks, and Policy Considerations

1. What additional potential benefits, policy considerations, or risks of a CBDC may exist that have not been raised in this paper?

The Fed white paper assumes that a central bank digital currency, issued by the Federal Reserve and promulgated using distributed ledger technology (DLT, e.g., a blockchain), would be the primary and/or preferred means by which a federally issued or ‘public’ digital currency might be issued. This paper also assumes that such technology and its associated institutional architecture may be able to address key financial inclusion issues, such as lack of access to bank accounts, the need for faster, more secure, and reliable payment systems, etc., and can do so while offering sufficient privacy and consumer protections for CBDC holders and users.

For reasons related to efficiency, privacy concerns, consumer protections, and financial inclusion, we urge the Fed to reconsider this fundamental premise and work with other financial regulators to make room for a more polycentric institutional and technological architecture, which may or may not incorporate blockchain-based tokens, if they prove to be as or more effective than other option and do not present comparatively higher risks.

Indeed, that structure could incorporate both existing Fed systems and new innovative approaches that are not dependent on DLT technology. For example, we would support the acceleration of the Fed Now program, with consumer fraud protections incorporated, which would expand the availability of real-time payments as a first step. We would additionally see promise in the deployment of a privacy-protecting Fed Accounts system that would expand the capacity of the Fed to provide account-based deposit and payment systems, with low or no fee services, beyond commercial banking institutions to retail customers. Such a system could be coupled with proposals to implement a postal banking program where the post office, which already provides payments-based services such as money orders, could serve as a front-end point of contact for retail users.

Finally, we support proposals to create “e-cash” – offline, hardware-based digital cash, built using existing technology, and issued by the Fed, Treasury or some combination of agencies – that could serve the same function as physical cash, without the risks to privacy, consumer fraud and structural imbalances that a Fed-issued, blockchain based digital currency may present. Indeed, such systems already exist outside the US, where payment systems using SIM-card based hardware tied to mobile phone platforms are a popular means of making payments. Card and chip-based hardware already in use for commercial smartcards and U.S. military payments technology¹ could be modified or altered to serve as digital cash, and there are many measures that could be employed to ensure the safety, security and authenticity of such digital cash using existing or modified technology to make such e-cash comparable to paper cash by these measures.

There is precedent for such a diversified approach to providing different forms of money via varied technology or systems. Currently, account-based systems of money and token-based systems of money (e.g., cash) already coexist, are distributed in tandem, and converted from one system to the other effectively, with known and understood points of friction. This is also true for other public service systems that not only deal with cash but have unique payment systems for that service - such as transit systems that allow customers to pay fares using both stored value ‘cash’ cards, as well as account-linked cards, to serve diverse needs of its users (e.g., short-term riders vs. long-term commuters). The same can and should be true for digital currencies and payment systems.

Additionally, while the Federal Reserve plays a key role in managing monetary policy both historically and currently, the Fed is not the only federal agency with the capacity, expertise, and mandate to offer payment system services and issue currency. The Mint, the Bureau of Engraving and Printing, Treasury and the Postal Service have all played this role or continue to do so. Indeed, situating a US digital currency outside of the Fed may help address concerns regarding credit allocation, run risk, and other structural issues that could arise with having the Fed become the issuer of a US digital currency. It might also distribute responsibility for monetary policy more evenly between the Treasury and the Federal Reserve, such that the Fed would have comparatively more capacity to focus on oversight of the banking system.

By expanding the scope of options beyond solely blockchain-based currency vehicles and payment approaches issued by the Federal Reserve (with the risks and limitations such an approach is likely to bring) the Administration would be better able to ensure individuals, commercial entities and other parties have access to a diverse array of publicly issued digital financial instruments and tools, each offering unique properties with respect to efficacy, reliability, speed, security, and privacy.

2. Could some or all of the potential benefits of a CBDC be better achieved in a different way

The Fed could accelerate implementation of Fed Now - with measures to protect Fed Now users against real-time payments or ‘inducement’ fraud - thereby increasing the speed of the current payments system in ways that could directly benefit consumers – particularly low-income consumers who are more likely to be negatively impacted by slow rates of payment processing. Fed Now not only has the potential to increase real-time payments, but, if deployed using the ISO 20022 standard, could increase the utility of the system to contain

¹ <https://fiscal.treasury.gov/eaglecash/>

more information, and offer options for more sophisticated payment activities (such as encoding invoices within a payment), without the need for DLT-based system.

The Fed could also pursue a “Fed Accounts” program that extends the account-based money services it provides to commercial banks to retail consumers. Such an accounts-system – which will need to balance AML compliance with robust privacy protections for consumers – need not rely on a CBDC as the ‘fuel’ for such transactions but could use the current form of money issued by the Federal Reserve. Doing so would avoid a costly and time-consuming effort to generate a new form of digital, DLT-dependent currency that could meet robust privacy and security standards.

Critically, the Fed should seriously consider how the roll-out of this program could address longstanding distrust of both government and financial institutions. One way we believe this could be accomplished is by renewing the Postal Service’s capacity to provide low or no-cost banking services as well as other financial services, including access to and management of Fed Accounts. The Postal Service played this role in the past, until such activities were largely phased out or scaled back in the 1970s. The Postal Service is a familiar, accessible agency for many that operates as a public service for all, regardless of wealth or income levels. The service is not without its challenges and has faced malign political interference from various angles in recent years. However, the Postal Service’s role in providing vital services during the pandemic despite these challenges showcases how the agency can offer essential infrastructure in times of crisis. Additionally, the recent passage of the bipartisan Postal Service Reform Act of 2022 will provide much needed funding and financial stability for the service, which could set the stage for further expansion of postal banking services to facilitate Fed Accounts. A form of public banking service relying on Fed Accounts and a lead agency could also coordinate or partner with similar public banking proposals being considered or developed at the state level, such as in California. Doing so could provide a broader array of accessible, low or no cost financial services to underserved populations while leveraging both the state/national banking infrastructure and oversight mechanisms.

Finally, as described above, other agencies could produce a non-blockchain, non-ledger, truly peer-to-peer form of digital fiat currency, that would replace the functionality of physical cash as it is currently used, ensuring that individuals and communities unlikely to fully embrace or be integrated into account-based systems (public or private) still have a method of payment that is secure, reliable, private, easy to use and is backed by the government.

It is worth noting that these services could work not only on their own, but in tandem to provide some of the services that CBDCs are intended to provide. For example, future proposals to directly deposit or issue government assistance in the form of tax credits or direct payments could be distributed either by Fed Accounts, e-cash, or combination of the two, with the postal service playing an intermediary role where needed.

Outside of these public innovations, the Fed could require commercial banks to offer Bank On accounts, which have low or no monthly fees, as a condition of receiving Fed Master accounts. Additionally, the Fed and other financial regulatory agencies could make sure existing remittance rules and infrastructure are adapted to streamline payments hurdles, and address hidden costs, without the use of CBDC as a payment infrastructure. And, beyond the Fed’s remit, the CFPB could adopt rules to prevent the abuse of overdraft and insufficient funds fees, which have significant negative impacts on low-income banking consumers.

Lastly, while beyond the scope of this paper, we would strongly urge the Fed to resist arguments that privately created and circulated cryptocurrencies are a viable alternative to a CBDC. Digital assets have flaws and

vulnerabilities too numerous to name in full, but the concerns we and many others have about these assets' security, reliability, volatility, stability, and viability as payment systems should be enough to move the Fed to keep digital assets largely 'off the table' as a realistic solution for financial inclusion.

3. Could a CBDC affect financial inclusion? Would the net effect be positive or negative for inclusion?

Regarding potential negative effects, a CBDC (in general, or a poorly designed/deployed one) might: 1) Expose users to undue violations of privacy; 2) Undermine access to and availability of physical cash; 3) Push the Fed to take more of a role in the economy and financial markets than may be wise, either by buying more assets to offset CBDC liabilities, or by exercising more control over bank's debt and credit decisions, constraining banks' and consumers' access to credit; 4) Impact funding or support for the community reinvestment act program, negatively impacting access to banking services for low income communities; and 5) Be used or abused to unfairly restrict people's use of public benefits, or to garnish wages to serve private or government debts.

Regarding positive effects, it is difficult to determine how to enumerate the potential positives without a clearer understanding of and more detail regarding which CBDC approach the Fed intends to put forth. However, as a starting point, a CBDC would need to demonstrate some of the following attributes (as well as others to be determined) for it to be equipped to address financial inclusion challenges properly.

Firstly, a CBDC would need to establish principles, systems, and standards of trust. For example, CBDC users would need to have confidence in the safety of the credit being used and issued via a CBDC. Users would also need to have confidence that the CBDC issuer would minimize the generation, collection and retention of data produced by the use or holding of a CBDC. Users would also need confidence that the issuer, related government agencies or infrastructure would be treated as a public utility under 'common carrier' standards - meaning all users would have equal access and use of the CBDC and would not be subject to tiered access based on cost or other criteria. Similarly, users would need to have assurances that a CBDC would not be used as a means of political censorship.

Second, a CBDC would need to be well-designed from a user interface (UI) and user experience (UX) perspective. Prospective users already have experience using digital tools and apps that are designed with UI and UX in mind. The best of these apps is clear and easy to use, reliable, accessible for different users, and enjoyable to use. A CBDC should strive to meet this same standard, both to provide its users with a similar level of service as private sector tools, and to ensure uptake and mainstream use of a CBDC.

Thirdly, a well-implemented CBDC should be widely accessible and interoperable. Anywhere a consumer might be able to use a private payment system (e.g., credit cards such as Visa, Mastercard; payment apps such as Venmo or PayPal), CBDC users should be able to use a CBDC with comparable levels of ease. This has implications for both how the CBDC would be issued to users as well as how vendors would need to be engaged to ensure this standard is met. Doing so would not only address equitable access concerns, but would also ensure CBDC use becomes mainstream, a critical measure of viability for a CBDC.

However, as expressed elsewhere in these comments, alternative measures could also promote inclusion and avoid or more easily address some of the challenges to doing so than a digital currency based on distributed

ledger technology, and we are concerned that a CBDC using an intermediated model would more likely fail to achieve the assumed financial inclusion goals from the start.

Using a CBDC to increase financial inclusion might run afoul of problems with digital inclusion; many people still do not have widespread access to reliable, affordable high-speed internet. Surveys indicate this digital divide persists across racial, class and ethnic lines today. For example, a 2021 Pew Research Survey found that while eight-in-ten white adults report having a broadband connection at home, smaller shares of Black and Hispanic adults reported the same – 71% and 65% respectively.² Meanwhile, adults living in low-income households (making less than \$30,000 a year report having significantly less access to smartphones, desktop or laptop computers, tablets, or home broadband than more affluent households.³ Low income broadband users also report more trouble paying for their high-speed internet service, in particular during the height of the COVID-10 pandemic.⁴ This lack of access to internet service and computing technology could mean that low-income, African-American or Hispanic households would have less reliable or affordable access to digital currencies or payment systems, relative to more affluent, white households. While calls for expanding broadband access have been long standing, there is no clear path for extending universal coverage of which we are aware. Hence, relying primarily on a digital currency that is distributed online and on-chain under current digital access conditions could perpetuate or exacerbate efforts to increase financial inclusion.

4. How might a U.S. CBDC affect the Federal Reserve’s ability to effectively implement monetary policy in the pursuit of its maximum-employment and price-stability goals?

(No answer submitted)

5. How could a CBDC affect financial stability? Would the net effect be positive or negative for stability?

(No answer submitted)

6. Could a CBDC adversely affect the financial sector? How might a CBDC affect the financial sector differently from stable coins or other non-bank money?

(No answer submitted)

7. What tools could be considered to mitigate any adverse impact of CBDC on the financial sector? Would some of these tools diminish the potential benefits of a CBDC?

(No answer submitted)

8. If cash usage declines, is it important to preserve the general public’s access to a form of central bank money that can be used widely for payments?

² <https://www.pewresearch.org/fact-tank/2021/07/16/home-broadband-adoption-computer-ownership-vary-by-race-ethnicity-in-the-u-s/>

³ <https://www.pewresearch.org/fact-tank/2021/06/22/digital-divide-persists-even-as-americans-with-lower-incomes-make-gains-in-tech-adoption/>

⁴ <https://www.pewresearch.org/fact-tank/2021/06/03/34-of-lower-income-home-broadband-users-have-had-trouble-paying-for-their-service-amid-covid-19/>

If and as the use of physical cash declines, it is important that people have access to a form of digital fiat currency that can be widely used for payments which provides the same features of physical cash – in particular, the ability to conduct transactions ‘offline’ with a reasonable expectation of privacy, no transaction costs, no need to have access to special purpose equipment, and reduced chance of public authorities unduly ‘censoring’ individuals by constricting their financial activity. Physical cash has been in existence and has coexisted with the use of ledger-based accounting systems for thousands of years. Even today, the use of physical cash is a necessity for tens of millions of individuals in the US and abroad, many of whom are unbanked or underbanked, and use cash to conduct financial transactions, purchase goods or services, or engage in peer-to-peer exchanges of value in a low or no cost manner, with some reasonable expectation of privacy.

Account-based money uses ledger systems that record payments which represent contractual obligations between the account holder and account manager to be settled on demand. This system has attributes that, properly administered, can provide benefits to account holders, including fraud prevention and consumer protection. However, relying on account-based money also involves trade-offs. An individual's account deposits can be exposed to risk should the firm holding those funds become insolvent. Additionally, accounts held with financial institutions are subject to AML/KYC monitoring and compliance, which necessarily reduces an account holder's expectation of privacy, even in situations where a ledger records transaction or other identifying information, without an account manager involved. As such, some people may have legitimate reasons for wanting to use a means of transaction that is less dependent on financial intermediaries, ensures some measure of privacy and allows people to take direct custody of the assets they own.

Physical cash, or token-based forms of money, differs from account-based money in that such tokens are transferable bearer instruments. The legal ownership of such tokens resides with the person who currently possesses them - either as a stack of physical cash under a bed, in someone's wallet, or existing in digital form on a server or in a piece of offline hardware. This distinction means an individual does not need to rely on a third party to claim this asset, nor refer to a historically continuous ledger of ownership transfer. They do not receive the protections that account-based money might provide, but neither do they incur the potential liabilities involved. Additionally, two individuals can use token-based cash to transact in goods or services without a financial intermediary, and without generating a default record of the transaction that persists beyond the two parties involved.

Reliance on physical cash is not merely an adherence to more ‘traditional’ means of payment but is rooted in long-standing economic inequities and institutional racism which have fostered distrust of commercial banking institutions and related government entities. Unbanked individuals often lack the income, identification documents or credit worthiness that private financial institutions often require for even basic checking or savings accounts. There is also a long history of exploitation of marginalized populations by private financial institutions. This has come in many forms - discriminatory lending policies; exclusion from traditional financial advisory services; predation by firms offering sub-par alternatives, such as payday lending, and more. Finally, low-income, and marginalized communities have experienced decades of unequal and unfair surveillance, harassment, and policing by law enforcement agencies. Finance itself has been used to facilitate such discriminatory policing via practices such as civil or criminal asset forfeiture, bail requirements and other exorbitant fees and punitive measures levied by the criminal justice system.

These practices have fostered within these communities and individuals a deep distrust of both private financial institutions as well as government efforts to extend the financial services franchise to them unless or until profound measures are taken to restore trust, reduce barriers to access, and protect individuals' privacy. Thus, access to physical cash and cash-based transactions without use of intermediaries is already highly desired by many and perceived by some to be a necessity. Furthermore, should more aspects of the financial services sector become digitized and subject to either private or government surveillance without transformational changes in privacy law, such need or demand may grow.

9. How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?

(No answer submitted)

10. How should decisions by other large economy nations to issue CBDCs influence the decision whether the United States should do so?

(No answer submitted)

11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?

(No answer submitted)

12. How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?

A DLT-based government issued digital currency presents a conundrum for anyone who holds the following positions: 1) Illicit finance is a critical global problem that harms untold numbers of people and must be addressed by regulators, law enforcement, and governments using a range of effective and fair tools; 2) The suite of laws and regulations that constitute the US AML/CFT regime has serious flaws and has been misused or abused by law enforcement and national security authorities in ways that have disproportionately harmed low-income and BIPOC communities, many of whom are often victims of the crimes facilitated by illicit finance in the first place. This includes the selective application of the AML/CFT regime, such that often, major financial institutions or wealthy individuals have easy access to financial services while avoiding full prosecution or penalties, while ordinary individuals - say, immigrants seeking to send remittances home - face disproportionate restrictions, scrutiny and penalties; and 3) The US lacks comprehensive laws that protect individuals' digital privacy and has a history of regulation and judicial jurisprudence that has greatly undermined individuals' right to privacy as understood under the Fourth Amendment.

It is certainly possible that technological approaches exist for developing DLT systems that could provide a measure of privacy for those individuals using a CBDC. However, we believe these technological fixes are unlikely to be sufficient to address how intrusions into CBDC users' privacy would unfold.

One use case for a DLT-based digital currency is that the ledger itself provides both transparency (regarding transaction activity and holdings) and anonymity (with respect to the identity of holders of tokens and/or

wallets). There is some validity to this insofar as, at least under some scenarios, law enforcement has been able to directly gather data on-chain, or via intermediaries (exchanges) in order to investigate illicit finance, while at the same time, wallet holders who hold their tokens off-chain in private non-custodial wallets may achieve some degree of privacy (though most individuals still purchase crypto assets with bank deposits, and regulators are asserting some jurisdiction over wallets and wallet issuers).

With a publicly issued DLT-based digital currency, in theory such a balance could still hold. Transaction information about digital tokens would exist on a government created chain; tokens themselves would be held in private wallets, issued either by private entities (banks, or non-bank payment providers) or by government entities (say, for example, by the post office).

However, it is unclear how regulators and the courts would differentiate or distinguish between the privacy protections that exist for an account-based payment system (either through a private institution or government entity) and a DLT-system where individuals hold digital tokens in digital wallets which may or may not be linked to accounts held by private or public entities.

In theory, an individual has more assurances of privacy regarding their physical wallet versus what is held in their bank account (though as mentioned elsewhere, privacy rights for one's physical assets are also not secure under current law). However, it doesn't take much imagination to envision how, when all these elements are connected by one stream of data, such distinctions might be eroded, either explicitly (through court rulings or new statutes) or implicitly, through suspension of privacy restrictions in the name of national security; via information sharing agreements between agencies after initial use of the data for a specified purpose; or the deanonymization of flows from digital wallets by cross-referencing such information with other data.

The situation also becomes murkier when third party digital service providers play a role either on the back end or front end of such a system. Major digital service providers have business models that harvest data from individuals' online activities. Securing access to an individual's financial transaction data record as well would be hard for such companies to resist. As such, we are concerned that legislative or regulatory attempts to bar access to such data would be insufficient or subject to regulatory capture by the industry. Lastly, in the past, such service providers have either offered or have been compelled by law enforcement to disclose data previously deemed private. It is reasonable to assume the same would hold true for CBDC data collected and stored by such digital service providers as well.

In sum, unless there are fundamental reforms to data privacy and financial privacy laws, it will be difficult to ensure that a CBDC, regardless of its structure and concept, can provide sufficient privacy for consumers that is well-balanced with respect to the competing need for access to financial information for AML/KYC purposes.

13. How could a CBDC be designed to foster operational and cyber resiliency? What operational or cyber risks might be unavoidable?

(Not intending to answer)

14. Should a CBDC be legal tender?

(No answer submitted)

CBDC Design

15. Should a CBDC pay interest? If so, why and how? If not, why not?

(No answer submitted)

16. Should the amount of CBDC held by a single end-user be subject to quantity limits?

(No answer submitted)

17. What types of firms should serve as intermediaries for CBDC? What should be the role and regulatory structure for these intermediaries?

While we have foundational concerns about the use of an intermediated model overall, one key concern we have is the possibility of non-depository institutions serving as intermediaries. Non-banks (and ILCs) are not held to the same supervisory and oversight standards and have had problematic records - allowing fraudulent accounts to be opened while also unduly freezing or shutting down legitimate accounts in overreaction, KYC compliance, and other issues. At a minimum, only insured depositories whose parent companies are subject to the Bank Holding Company Act should be eligible to be intermediaries.

Even so, relying on intermediaries, as mentioned above, could create problems with credit allocation, expand the Fed's balance sheet, and, ironically, could end up excluding individuals using traditional banking accounts and systems from greater access to preferred financial services.

We would also note that one argument for introduction of a CBDC is to bring government issued money – a public good - into the digital age. Yet, pursuing an intermediated CBDC model could in some scenarios bring about a backdoor privatization of that good, with commercial banks continuing to play an outsized role in determining how financial services are operationalized. Embedding that dynamic within a CBDC system could simply perpetuate some of the existing inequities in our current system.

Given these risks, as discussed earlier in this comment, we would prefer a system that relies more on public institutions or agencies, such as the Postal Service, the Mint, Treasury, or other appropriate agencies, to play an intermediary role if needed. This could help address privacy concerns and conflicts of interest that may be present when private entities play a custodial role, and could also ensure there is a viable public option for a digital currency and payment system that can provide vital public services and good directly to people without intermediaries - an arrangement that can offer resilience in times of crisis when private sector supply chains and production processes founder.

18. Should a CBDC have "offline" capabilities? If so, how might that be achieved?

(No answer submitted)

19. Should a CBDC be designed to maximize ease of use and acceptance at the point of sale? If so, how?

20. How could a CBDC be designed to achieve transferability across multiple payment platforms? Would new technology or technical standards be needed?

(No answer submitted)

21. How might future technological innovations affect design and policy choices related to CBDC?

(No answer submitted)

22. Are there additional design principles that should be considered? Are there tradeoffs around any of the identified design principles, especially in trying to achieve the potential benefits of a CBDC?

(No answer submitted)

For any questions or comments about this submission,

Please contact Mark Hays with AFREF/DPEF, markhays@ourfinancialsecurity.org