US House of Representatives Committee on
Financial Services
Task Force on Financial Technology

"*Digitizing the Dollar: Investigating the Technological Infrastructure, Privacy, and Financial Inclusion Implications of Central Bank Digital Currencies"*

June 15th, 2021
Written testimony of
Dr. Neha Narula

Thank you Chairman Lynch, Ranking Member Davidson, and members of the task force, for the opportunity to testify today.

My name is Neha Narula and I am the Director of the Digital Currency Initiative at the Massachusetts Institute of Technology. We are a research group based within the MIT Media Lab focusing on cryptocurrency and digital currency design, including development of the open source software behind Bitcoin. I have taught five graduate cryptocurrency courses across departments at MIT and during the course of my PhD I conducted research in MIT's Computer Science and Artificial Intelligence Laboratory on databases and distributed systems. In August 2020 the DCI began a multi-year research collaboration with the Federal Reserve Bank of Boston on Project Hamilton, to understand the technology tradeoffs involved in a hypothetical digital currency. We will be releasing a paper and open source software this summer. I'd like to note that my views are my own, and not the views of MIT, the Board of Governors, or the Federal Reserve Bank of Boston, nor am I offering any insight into Federal Reserve policy or perspectives.

The problem and opportunity

Traditional electronic transaction systems today have high fees and limited access. These systems have simply not evolved fast enough to keep pace with the demand for online digital payments. Our legacy payment rails require expensive delays because they were created at a time when the technology did not support settling every transaction in real time. The pace of updates has been slow due, in part, to structural problems in the payment ecosystem making it difficult to coordinate large-scale change.

At the same time, we are seeing experimentation in the realm of cryptocurrencies built on open networks that do not require a traditional financial intermediary. This area serves as a laboratory showing what innovation and functionality might be possible if we were not constrained by legacy financial rules and systems. However, this area is still developing and comes with many risks, not least of which is the immaturity of the technology and its ability to provide widely available, highly secure, and scalable payment transactions. Figuring out how to address these limitations is an active area of research where my group spends much of its time.

In response, central banks across the world are considering issuing digital forms of their currency to the public. A Bank for International Settlements survey of 65 central banks found that 86% are actively engaging in some sort of work on Central Bank Digital Currency (CBDC), to improve payment efficiency and robustness, facilitate financial inclusion, and maintain financial stability, among other reasons.[1]

It is important to note that a CBDC might not be the only way to address some of these problems. For example, in the US we might improve financial inclusion by requiring commercial banks to provide free, no-minimum accounts to users, or by limiting or eliminating fees. (These would address some reasons people offer for not having bank accounts.[2]) More research is needed to determine how a CBDC might compare to other approaches to solving financial inclusion issues, and how exactly to build a CBDC to address these challenges. At MIT, we are beginning to investigate the possibilities of CBDC as a vehicle for increased financial inclusion, but as of yet, the promise is unverified in either a US or global context.

The potential promise of a CBDC goes beyond payment efficiency and financial inclusion. Digital currency is an opportunity for a ground-up redesign of our current payment systems. If designed in the right way, a system to create and support a digital dollar might increase competition and standardize disparate data models, leading to more interoperability and creating a platform for innovation in payments, much as the Internet created a platform for innovation by facilitating the transfer of information. In undertaking such a redesign, additional opportunities for increasing financial inclusion and solving challenges in the legacy financial system might also be uncovered.

Though promising, the way forward is not entirely clear. There are many remaining open questions regarding how a US CBDC should operate, how users might access it, and how consumer privacy would be protected. In what follows I offer a few of the choices that would need to be made if the United States decided to issue a digital dollar.

It would be irresponsible to launch a digital dollar until we can make progress on these questions -- but addressing them requires investment now, and extensive collaboration between academic researchers and the public and private sectors.

International exploration of CBDC

Some countries have issued a CBDC, and others are considering issuing one, or are exploring CBDC viability. For example, in October 2020 the Central Bank of the Bahamas issued the Sand Dollar to promote financial inclusion and access. Sweden is exploring an e-krona because of the decline in the use of cash in payments, and its Riksbank wants to continue its mandate of providing a public option for payments. The People's Bank of China is engaging in late stage

[1] Boar, Codruta, and Andreas Wehrli. "Ready, steady, go? Results of the third BIS survey on central bank digital currency." (2021).
[2] FDIC. "How America Banks: Household Use of Banking and Financial Services." FDIC Survey (2019).

digital currency pilots and might launch the eCNY[3] to, in part, bring China's massive fintech industry back under the umbrella of the central bank after the enormous success of payment platforms like Alipay and WeChat Pay. Those platforms together comprise 93% of mobile payments in China.[4] Each of these countries is using a different technology stack and has made different initial choices about how to involve commercial banks and about how the CBDC might be accessed by users.

Currencies compete; it is certainly possible that consumers might be attracted to a digital currency which is easy to use, has no or low fees, and comes with interesting features. But the concerns of the United States are unique in that the dollar plays a critical role in the global economy as the world's reserve currency. The once-in-a-century opportunity to redesign the US dollar should not be rushed. It is important to carefully consider how we might want a US digital dollar to operate and what effect different technical and policy choices will have on accessibility, overall financial stability, and the potential for a US digital dollar to be a platform for innovation.

What is a CBDC?

A general purpose, or retail, CBDC is defined as a digital liability of a nation's central bank that is broadly accessible and usable by the general public. It is distinguished from commercial bank money, credit cards, and mobile payment application balances in that it is a liability of the central bank; it is different from cash in that it is entirely digital; and it is different from central bank reserves in that users might hold it directly. This is in contrast to what is known as wholesale CBDC, which is a digital liability of the central bank which is limited to certain financial institutions and is not available to the general public.

Beyond those basics, definitions start to vary widely. Some experts argue that a CBDC must be built on distributed ledger technology (DLT). I believe that is putting the cart before the horse. We should first determine how a CBDC should operate before choosing an implementation technology. Also, it is important to distinguish between the underlying datastore of a CBDC implementation, and the interface to the CBDC and how it is intermediated and accessed. These different aspects are often conflated under the general term "distributed ledger technology." For example, a CBDC could act as a legal bearer instrument with a programmable interface even if it is built on top of traditional database technology.

CBDC and cryptocurrency will coexist

[3] In China there have been mixed messages as to whether the eCNY even is a CBDC: Former PBOC Governor Zhou Xiaochuan said in December 2020 that eCNY would not be a liability of the PBoC, contradicting statements by Mu Changchun, Director-General of the Digital Currency Institute at the PBoC, and Fan Yifei, Deputy Governor at the PBoC.

[4] Zhang, M. "China moves further towards cashless society as payment giants Alipay, WeChat Pay gain ground." *Retrieved from South China Morning Post: www.scmp.com/business/companies/article/2130400/ china-movesfurther-towards-cashless-society-payment-giants.* (2018).

Cryptocurrency and central bank digital currency are not mutually exclusive and will coexist. One prominent reason people use cryptocurrency is *because* its issuance is determined by software and a decentralized network, instead of a central bank. A central bank digital currency would not replace this preference.

Another reason people use cryptocurrencies today is for the innovative applications and flexibility they increasingly provide. Cryptocurrencies serve as a platform for rapid financial innovation, while a nation's monetary system benefits from long-term stability. The experimentation enabled and incentivized by cryptocurrencies has been productive. We can highlight two examples: programmability and innovation in cryptography. Much of the excitement about DLT is actually about programmability and automation.[5] This comes directly from developments in cryptocurrency. For example, the atomic swaps used in the Bank of Canada and the Monetary Authority of Singapore's Project Jasper/Ubin could reduce economic rents and increase stability in wholesale settlement.[6] Similarly, protecting consumer privacy is a requirement for a hypothetical CBDC and privacy-protecting designs directly benefit from innovation in cryptography driven by privacy-focused cryptocurrencies. Innovations such as these would not exist without pioneering work done in cryptocurrencies in general and Bitcoin in particular.

Accessibility: How is the CBDC accessed and managed?

In order to achieve goals of financial inclusion, a CBDC should be broadly accessible and usable. Every point of intermediation involved in a user obtaining and using CBDC is another potential friction that could inhibit access.

For example, international studies on financial inclusion have shown that requiring strong forms of identification deters the poor from accessing financial services.[7] One of the benefits of cash is that it can be used by anyone without requiring identification or signing up for an account, which is, in part, what makes it the payment system of choice for the poor. However, at the same time, policymakers would like to limit the potential use of CBDC for illicit activity. One way to address this tension is by creating tiers of access that would require different levels of identification. In the Bahamas, there is a low-value tier of access to the Sand Dollar that requires only an email address or mobile number to sign up, but limits balances to $500 and transaction volume to $1,500 per month.[8]

---

[5] Bundesbank, Deutsche. "Money in programmable applications: Cross-sector perspectives from the German economy." (2020).
[6] Bank of Canada and Monetary Authority of Singapore. "Jasper Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies." 2016.
[7] Demirguc-Kunt, Asli, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution. The World Bank, 2018.
[8] Central Bank of the Bahamas. "Consumer-Centric Aspects of the Proposed Regulations for the Bahamian Digital Currency." (2021).

It is important to consider users who might not be able to use mobile payment applications. For example, 36% of those in the US who lack bank accounts also do not have smartphones.[9] Many Americans do not have reliable internet connectivity. Such people could not use a digital currency that requires a mobile app or constant connection to the Internet. To help with financial inclusion, a US CBDC could be available via smart cards, which could limit certain aspects of its design. At MIT we are investigating designs that would enable forms of secure offline transactions.

Data protection: What data is visible to whom, and under what circumstances?

Transaction data can vary widely; at a minimum it includes sender and recipient, amounts, and the time of the transaction. Some transaction systems collect user data like name, date of birth, social security number, and address, or other passive information like a user's IP address, GPS location, browser, or mobile operator. All of this information can then be used to track users and build profiles of their habits and behavior across websites and applications.

Financial transactions reveal sensitive data about our lives and protecting privacy is essential for human dignity and a democratic society. Consumer privacy is a requirement for a US CBDC as well as a potential competitive advantage. In addition, collecting and storing personally identifying user data at all makes that data vulnerable to accidental leaks or malicious hacking attempts, so the design of a US CBDC should strive to limit data collection to only what is critically necessary to safely process transactions.

The private sector has an incentive to collect and monetize all these different forms of data. Whether through regulation or by providing a public option, CBDC designers must consider how to protect user data. In particular, it should not be the case that those who can afford it can pay for services which protect their data while the poor are left to services that monetize their data and exploit their digital footprints for financial gain.

A CBDC which is in some part run by the central bank does not necessarily require the central bank to have visibility into fine-grained transaction data. Legitimate public policy goals relating to combating criminal activity can be fulfilled while preserving the privacy of the public and preventing a central bank being drawn into the commercial surveillance models which are now prevalent in the private sector.[10]

Seven architectures to implement a CBDC and adjacent designs

[9] FDIC survey.

[10] Ali, Robleh, and Neha Narula. "Redesigning digital money: What can we learn from a decade of cryptocurrencies." Digital Currency Initiative, MIT Media Lab (2020).

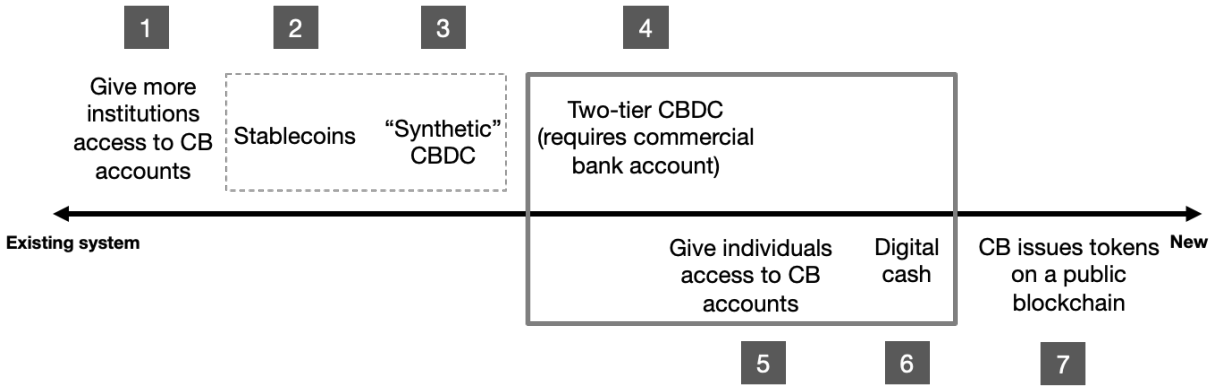

Figure 1. Collection of seven different architectures we describe that directly implement or are adjacent to a general purpose central bank digital currency. The dotted box contains architectures that do not fit the definition of CBDC given above, in that they are not liabilities of the central bank. The solid box contains the most common architectures proposed for retail CBDC. CB is "Central Bank". Architecture 6 "digital cash" is where the Digital Currency Initiative at MIT is currently spending its time.

Figure 1 shows seven different architectures to consider in CBDC design, ranging from those closer to our existing system to entirely new models for accessing central bank currency. For each architecture I describe its potential to improve financial inclusion and to serve as a platform for innovation.

Under the basic definition given earlier, wholesale CBDC already exists since financial institutions hold electronic balances with the Federal Reserve. Architecture 1 would simply expand access to the Federal Reserve balance sheet to a larger set of institutions, for example by extending access to mobile payment application providers. This might reduce settlement costs and improve competition, and through that, improve access and innovation. However, it would also require increased regulatory scrutiny of these new participants, which might limit their ability to provide accounts to those currently left out. It is not clear it will help promote interoperability and standards, leading to a platform for innovation.

The next two architectures shown in Figure 1 do not fit under the definition of CBDC provided above in that they are not direct liabilities of the central bank. One option is to expand support and regulatory clarity for so-called stablecoin providers (Architecture 2 above). Stablecoin providers issue dollar-pegged tokens on public (so-called permissionless) or non-public (so called permissioned) blockchains. These then fall into two categories: Those that are one-to-one backed by commercial bank deposits or other relatively stable, liquid assets like US Treasuries, and algorithmic stablecoins, that operate in a smart contract on a public blockchain, and are usually heavily overcollateralized using cryptocurrency assets or other stablecoins, with the peg managed by a software algorithm running in the smart contract. To date, US dollar-denominated stablecoins have a market capitalization of over $100B, with the vast majority of that value in the first category.[11] They appear to be primarily used as a mechanism for facilitating cryptocurrency trading, and I am not aware of any rigorous evidence that stablecoins help improve financial inclusion, though this is an area deserving more research. Architecture 3 is what the

[11] https://coinmarketcap.com/view/stablecoin/

International Monetary Fund deems “synthetic” CBDC, in that it is issued by commercial banks and not actually a liability of the central bank, but is backed entirely by central bank reserves.[12] It is also unclear exactly how this architecture might help promote access and financial inclusion beyond our existing system, or how it could become a platform for innovation.

Architectures 4, 5, and 6 (contained in the solid box) are the most discussed designs for retail CBDC, though there are still many choices and variations within the proposals. Architecture 4 is deemed “two-tier” CBDC in that it is expected that the CBDC would be accessible only through commercial banks.[13] This implies that a user will need to obtain an account with a commercial bank in order to receive and transact in the CBDC. This design is appealing because it preserves the current structure of electronic payments, but at the same time, it is unclear how this design alone would help promote financial inclusion in the US because it does not appear to address the main reasons why the unbanked do not use banks. Figure 2 (below) is copied from Figure ES.3 from the FDIC’s 2019 survey on “How America Banks: Household Use of Banking and Financial Services” and shows survey responses for why unbanked households do not have bank accounts. The success of this architecture in addressing financial inclusion will depend on exactly how commercial banks would administer CBDC accounts; if it is not different from how they administer traditional checking accounts, they would be unlikely to address any of the unbanked’s concerns.

How successful this design would be in providing a platform for innovation also depends on whether commercial banks cooperate to provide compatible APIs (Application Program Interfaces) to facilitate building new applications that transfer CBDC. Under the status quo it is unlikely a two-tier CBDC would help promote innovation in payments, since commercial banks currently do not provide these interfaces widely and do not interoperate.

[12] Adrian, Tobias, and Tommaso Mancini-Griffoli. "The rise of digital money." Annual Review of Financial Economics 13 (2019).

[13] The CBDC might also be available through additional regulated financial service providers. We should compare and contrast this type of two-tier model with the benefits and risks of the first architecture, which is expanding the set of institutions that can access the central bank’s balance sheet, without issuing a new form of CBDC.

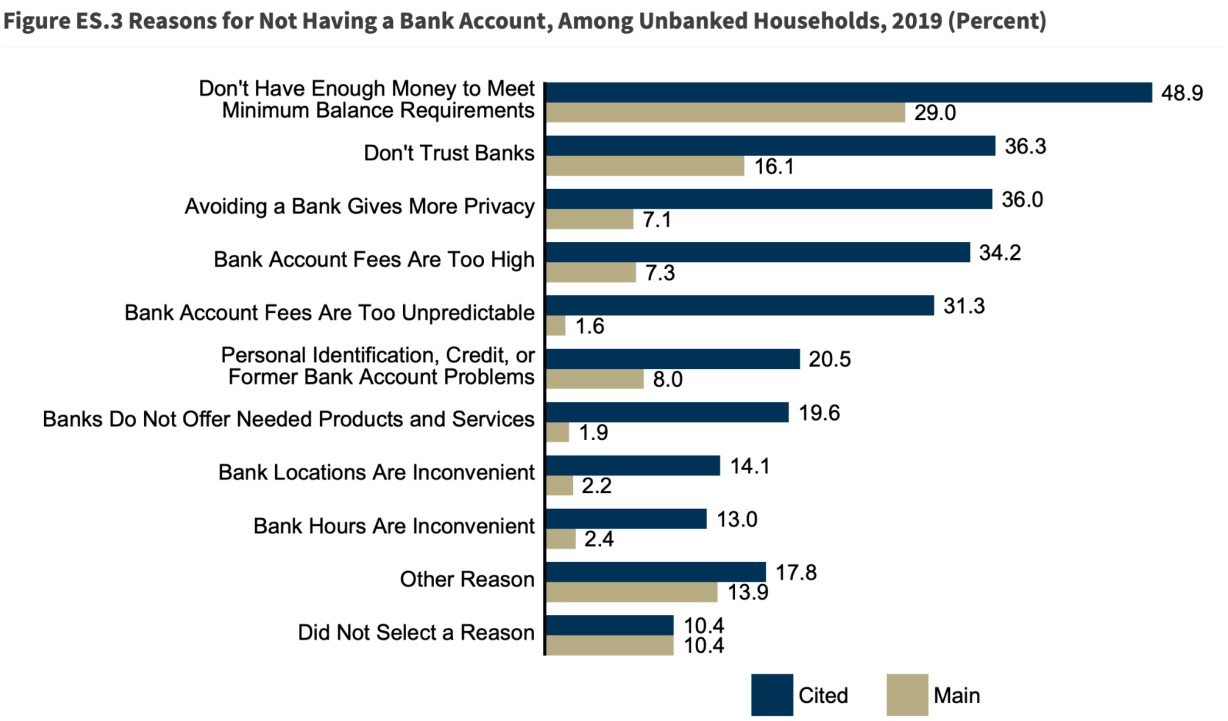

Figure 2. Source: FDIC survey on How America Banks: Household Use of Banking and Financial Services[14]

Architecture 5 is also known as FedAccounts. It would give retail users the option of holding an account directly with the Federal Reserve, a privilege currently limited to regulated financial institutions. The authors of the FedAccounts proposal have written extensively on how the proposal might help with financial inclusion.[15] We have not independently verified those reports. It is to be determined if the FedAccounts proposal would promote innovation in payments beyond improving competition.

Architecture 6 is “digital cash,” which is a CBDC that can be held directly by users without requiring an intermediary commercial bank account. It is important to note that a digital currency cannot be entirely peer-to-peer as is cash; digital information, unlikely physical objects, can be easily copied, so at some point a recipient needs to check that the payment they are receiving has not already been previously spent (this is called a “double spend”). One option for doing this is to employ secure hardware, which would prevent the double spend in the first place. This, however, requires relying on the correctness and integrity of secure hardware implementations, which might have bugs. The more common way is to reconcile with a ledger managing the issuance of the digital currency. There is a lot of leeway in the design of how exactly that ledger is accessed and when, and what controls that ledger has in terms of permitting, denying, or reversing transactions. In a CBDC designed to look more like digital cash, the ledger could simply prevent double spends.

---

[14] FDIC survey.

[15] Ricks, Morgan, John Crawford, and Lev Menand. "Central banking for all: A public option for bank accounts." The Great Democracy Initiative Report (2018).

This architecture could improve financial inclusion if it were easy to use and implemented in a way that is widely accessible, because it would not necessarily require users to sign up for accounts to receive payments,[16] and users would have an already existing mental model (cash) for how it works and how to use it. Note that banks or other third-party providers could custody digital cash for users, if desired. This architecture could also provide a standard to use as a layer of interoperability among payment providers, promoting a platform for innovation. At MIT, we are currently actively researching how to design safe, efficient, and useful digital cash.

Architecture 7 is proposed by some private-sector actors as well as some blockchain technology and cryptocurrency advocates; they suggest that a central bank issue digital currency on an existing blockchain system. This might be a permissionless smart-contract platform like Ethereum or a permissioned blockchain like Facebook's Diem. Under this type of architecture, a central bank could control issuance of the digital currency, but would give up all other control to the governance of the underlying blockchain. For example, the participants in the blockchain network might decide to reverse a transaction, as happened in Ethereum after one of its smart contracts, the DAO, was hacked. Ethereum developers, miners, and community members cooperated to reverse the hack and restore funds.[17] It is extremely unlikely that any central bank would want to put this level of control in the hands of blockchain participants. Blockchain networks are open and accessible and have high levels of innovation, though there has not necessarily been a concerted effort to research how to effectively add features that reliably support financial inclusion through blockchain networks. This is also an area that deserves further investigation as it might help inform CBDC design features and possibilities for advancing financial inclusion.

All of these architectures need to be carefully evaluated for their potential to improve financial inclusion, risks and complexity of implementation, monetary and economic implications, and the potential to affect the cost of credit and financial stability.

Conclusion

Extensive collaboration between academic researchers and the public and private sectors, as well as research funding, is needed to make progress on these key questions.

The first step is to obtain agreement on goals. In parallel, the Treasury Department and the Federal Reserve should be investing more in research and development, not to build "the" digital dollar but to fully understand its possibilities and implications as well as spur technology development.

---

[16] Identity checks could be done depending on the amount transacted, as described earlier.

[17] DuPont, Quinn. "Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization." Bitcoin and beyond (2017): 157-177.

To build consensus across varied stakeholders and create a neutral environment where the best ideas can flourish, we should rely on the principles of open source software development. The government's typical way of building systems -- outsourcing to a third party vendor -- will not, in my opinion, work here. What is possible in terms of policy is inextricably linked to the technical implementation. The US cannot outsource monetary policy to a vendor. As a first step I recommend expanding the type of work MIT is currently doing with the Federal Reserve Bank of Boston and other collaborations between academia and the public sector.

In conclusion, we have a once-in-a-century opportunity to redesign the dollar. Central bank digital currency might have the potential to increase financial inclusion, reduce transaction costs, and become a platform for innovation in payments, if designed and implemented well.

I commend this task force for raising this important issue and encouraging this critical dialogue. Thank you and I look forward to your questions.