Technology Development of Digital Currency

Neha Narula

We often spend a lot of time talking about the regulatory aspects of what a digital currency might look like, or the economic aspects. But if we take a look at the largest companies, the most influential on our ways of life, they're tech companies. Technology is incredibly important and influences what we can do with policy and what kinds of functionality we can even enable. So, what I hope to tell you today is a little bit about how I'm seeing the technology development of digital currency.

Digital Payments Today

To start, let's recap where digital payments are today. Digital payments are really, at their essence, just the transfer of information. It should be extraordinarily cheap, easy, and universal to make a digital payment. Yet retail transaction costs are anywhere from 0.5 percent to 0.9 percent of a country's GDP, depending on the country (Hayashi and Keaton 2012). This is a huge amount. About seven million American households don't have bank accounts, so that means they don't have access to digital payments (FDIC 2019). And our existing payment systems are, I would argue, woefully behind. Think about how easy it is for you to send a photo to a friend in another country. It's trivial: you get an email address or an

---

Cato Journal, Vol. 41, No. 2 (Spring/Summer 2021). DOI:10.36009/CJ.41.2.3.

Neha Narula is Director of the Digital Currency Initiative at the MIT Media Lab. This article is based on her remarks at the Cato Institute's 38th Annual Monetary Conference, November 19, 2020.

SMS phone number; and you know that you're going to be able to send that photo. But think about sending a small payment: you both have to agree on a service; you have to think about exchange costs; and you have to think about fees. It can be really difficult and slow to do this type of thing.

I don't think that this is going to be very easy to fix if we leave things the way they are because, unfortunately, large-scale change requires coordination among many different stakeholders. The way the system works today is the way that it's worked for decades. The system was built at a time when it was unfeasible to think about settling hundreds of millions of transactions instantly. It was built at a time when the technology wasn't there, so we had to think about things like netting and batching. The technology has advanced, but the architecture of the system—the structure—has not advanced with it.

I would argue we have a very good payment instrument right now that we should go back to and take a look at some of its features. A lot of people, when thinking about central bank digital currency (CBDC), approach it from the perspective that we have digital money in the form of central bank reserves and perhaps we should give more people access to the reserves. I would argue that another really interesting framework and approach is that we have coins and dollar bills—$2 trillion worth—and they're very useful. Can we think about digitizing these things?

Cash is universally accepted and very easy to use. Almost no matter who you are, you don't have to be an expert with technology: cash preserves privacy. When I pay someone $20, there's no one else eavesdropping on that transaction, and it doesn't require an intermediary, an internet connection, or complex new software in order to make cash payments. But unfortunately, cash isn't digital. However, I think it's really good for us to approach the potential for digital currency from the perspective of a universal digital protocol for value transfer. If we look back to the internet, the internet enabled us to standardize the transfer of information into addressable packets.

Many decades ago, we created these layers of protocol, and at the very bottom layer, ultimately, it's very simple. The bottom layer doesn't know if you're streaming a YouTube video, if you're sending a photo, if you're doing a Zoom call, if you're transferring really important sensitive information. The bottom layer has no idea, it's just standardized addressable packets and all of the functionality that we take

for granted that's been built on top of the internet comes on top of that. The system was simple, open, and accessible with useful interfaces and APIs (application programming interfaces), so we were able to build these really rich, amazing applications on top of it by first defining this basic standard.

Cryptocurrencies are a very interesting example of what a universal protocol for value transfer could look like. But digital cash is quite different. If we look back to the internet, we remember that it was a partnership between industry, academia, and government. It was very important to have all three of those sectors present at the beginning in defining these standards. Yet it's very hard once standards are defined and once the technology moves very fast. We're still using the internet protocols from 60 years ago, because we were very careful in designing them in such a layered way. They are still working quite well. We can innovate and move forward at the higher layers.

Central Bank Digital Currency

So how does this apply to CBDC? Well, what I'd like to articulate here are what we see as some of the core requirements for a CBDC. First of all, like dollar bills and coins, CBDC is a liability of the central bank. It means that the central bank controls issuance and final transaction validation, and I think it's very important to consider it from this perspective to maintain the mandate of financial stability. This is critical infrastructure, so security and resilience are the most important features. Moreover, if this becomes a national retail payment system, we must make sure that it's accessible and can't be attacked.

Obviously, a central bank digital currency needs to comply with all laws and regulations, and I would hope that it can support these diverse interfaces to encourage competition and innovation. Now, if we think about a retail CBDC, which individuals have direct access to, then we have some additional requirements. We need a retail CBDC to be very high throughput and low latency, to be broadly accessible and usable, and to consider user privacy. The last two requirements are a little bit in tension. I would hope that we can create a system that preserves fine-grained user privacy. But the challenge is in complying with laws and regulations and preventing illicit activity. This is something that is really fundamentally difficult to do.

CBDC Technical Design

I would argue CBDC technical design doesn't just require building in the private sector, it actually requires fundamental research. The existing private-sector digital currency platforms and protocols were not actually built with a CBDC use case in mind. Many of them were built for decentralized cryptocurrencies, or as an interchange between banks, or for more broad data like supply chains or provenance for other types of things. So, we don't actually have a system right now that was built with purely a CBDC use case in mind, and I think that that introduces a different set of requirements. CBDC research today is generally quite limited, mainly focusing on high-level policy questions or overly simplified proofs of concept that are not really getting at the true challenges of what it would take to create and launch a CBDC. Neutral rigorous CBDC technical research is still needed in order to prove real-world feasibility—in order to get to the point where we can actually uncover important tradeoffs and opportunities in both the technical and policy areas.

Building Central Banks' Capability for CBDC

Unfortunately, central banks at the moment lack the capabilities to rigorously build and test CBDC designs. There are, quite simply, very few expert digital currency engineers globally. Central banks have traditionally not had technical expertise in distributed systems and cryptography, with good reason—they haven't had to. And there is a cultural and knowledge divide right now between engineers and central bankers. So, central banks will need to partner and collaborate with experts in these arenas, because there are so many challenging research questions that we still have to address.

First of all, we need to figure out how to provide universal access for critical infrastructure with security and resilience. So, we want something that is broadly accessible, usable by large parts of the population, and incredibly secure. So how can we do that? Security is usually handled by limiting access to the system.

We also want to think about offline access. If we're thinking about digital cash, we can't presume that the users of the system have access to the internet at all points in time. We want this to be something that is usable in case of a natural disaster, for example. We also

can't assume that the users will have access to the latest smartphone devices, so we want to think about how to access CBDC at the base level for people who might not be very technically literate.

Drawing the Line between the Public and Private Sectors

A very important issue is how to think about designing architectures to best enable competition and innovation in the private sector. A key issue is where is the line between the public and the private sector (see Adrian and Mancini-Griffoli 2021). I don't think we have the answer to that question yet, and we need to build and test different architectures in order to understand what is possible at different levels, at different breaks in the design, between what part of the rails the public sector runs and what part of the rails the private sector runs.

The Biggest Challenge

Our most important challenge that we need to address is to figure out how to preserve user privacy while preventing illicit activity. It's very interesting because there is a lot to learn from the realm of cryptocurrencies. There have been major advances in using cryptography to provide privacy while at the same time making it publicly verifiable that a transaction preserves certain invariants, such as the user actually has the money to spend, money is not being created out of nowhere, and transactions are valid (i.e., authorized by the owner of the funds being spent). These things can be proven without actually being able to see the amount of the transaction or even the people involved. Therefore, I think what is essential is to engage in research to extend what we can prove using cryptography in CBDCs to have the ability to comply with laws and regulations.

The right to privacy is a critical part of our values as Americans. Different central banks will think about digital currency in different ways and they will build different systems. But as Americans, we need to think about what types of values we want to embed in our system, and I would argue that privacy is essential.

We are going to need to have a very involved conversation about how to manage illicit activity while at the same time preserving the privacy of individual transactions (see Narula and White 2020). It shouldn't be the case that every transaction I make (e.g., buying

coffee) is recorded somewhere and readable in some big database. I don't think that the government wants that, and I don't think that we want that. So we have to think about how to do this.

Conclusion

Central banks are realizing that though they might not know yet whether they actually want to issue a digital currency, they need to be prepared to do so. They need to actually engage in this research to figure out what it might look like and what the different approaches are. Research needs to be neutral. We need independent trustworthy results. We can't rely on the private sector to provide results that are trustworthy if they're being driven by a profit motive or promoting a specific token or technology. This should be technology first, but at the same time we need to incorporate policy requirements and user research at each stage, so we need to do these things in tandem.

It can't be that we go and figure out all of the policy and then find the technology that works, nor can we build a design and then layer the policy on top. These things have to be done together because they influence each other. And ideally, the work that we do would be flexible enough so that even though central banks are going to build different systems and incorporate different values, we have enough commonality and enough standards that the systems can work together.

References

Adrian, T., and Mancini-Griffoli, T. (2021) "Public and Private Money Can Coexist in the Digital Age." *Cato Journal* 41 (2): 225–29.

Federal Deposit Insurance Corporation (2019) "How America Banks." Available at www.fdic.gov/analysis/household-survey/index.html.

Hayashi, F., and Keeton, W. R. (2012) "Measuring the Costs of Retail Payment Methods." Federal Reserve Bank of Kansas City *Economic Review* (Second Quarter): 37–77.

Narula, N., and White, L. H. (2020) "Does the U.S. Need a National Digital Currency?" *Wall Street Journal* (February 23).