Risks involved with CBDCs: On Cash, Privacy, and Information Centralization

Presentation · November 2019

DOI: 10.13140/RG.2.2.30645.22248

1 author:

Linda Schilling
Olin Business School Washington University in St. Louis
30 PUBLICATIONS **434** CITATIONS

Risks involved with CBDCs:
On Cash, Privacy, and Information Centralization

Prepared for the 'Reinventing Bretton Woods Committee': Dialogue of the Continents, Oct 29-30, 2019, Hamburg

Linda M. Schilling - Ecole Polytechnique CREST

A central bank digital currency (CBDC) is planned to be a direct deposit a citizen has in the central bank. CBDC is supposed to be backed by central bank assets, to be purely digital, it can be private or non-private, it may or may not replace cash and can compete with bank deposits. CBDC is the central banks' digital answer to cryptocurrencies. To put it in the words of Christine Lagarde, let me read the following quotes taken from the 'Winds of change' IMF staff paper:

'[...] the fintech revolution questions the two forms of money [...] - coins and commercial bank deposits. And it questions the role of the state in providing money.'
'Should central banks issue a new digital form of money? True, your deposits in commercial banks are already digital. But a digital currency would be a liability of the state, like cash today, not of a private firm.'
'Would central banks jump to the rescue and offer a fully anonymous digital currency? Certainly not. Doing so would be a bonanza for criminals.'

I take away from this article that the way the ECB envisions the implementation of CBDC is in its non-private form. As a consequence, all citizens' transactions via CBDC will be transparent to the central bank. The comments I would like to make in the following, therefore, discuss the resilience and privacy of a CBDC based system. In particular, I would like to address the role of CBDC in comparison to the current central bank system involving cash and deposits on the one hand and to cryptocurrencies such as Bitcoin on the other. Altogether, I would like to make three points.

My first point is, I believe that giving up cash in favour of a purely electronic CBDC means giving up a major strategic advantage of the current system over cryptocurrencies. Citizens may opt-out of the CB system and start transacting via crypto only.

What do decentralized cryptocurrencies such as Bitcoin have to offer? Bitcoin obtains truthful reporting of payment transactions in an anonymous way, in a non-trusted, potentially hostile environment. Bitcoin tries to be a digital form of cash. What does the current CB system have to counteroffer? It has to offer cash. Cash allows truthful transactions in a non-trusted environment through immediate settlement if the two transacting parties directly meet each other and trust in the physical token, the Euro coin or bill. If I meet a stranger in the street in the middle of the night and I would like to purchase a banana, I can do this with a Euro coin since the stranger trusts in the coin. This is not the case for bank deposits where settlement requires transacting via a third party, the bank. Transacting via deposits requires trust in the bank that she does not report a 5 Euro banana purchase in my bank statement instead of the true transaction value of 1 Euro.

Cash not only offers immediate settlement, but it also offers wide adoption as a medium of exchange in the Eurozone. Most people and businesses in the Euro area accept Euro coins and bills as a means of payment. We take a wide adoption of the Euro as granted. But 100% adoption is, for instance, not accomplished in the case of Bitcoin. In addition, the cash-deposit-reserve combination of the current CB system offers a proven track record of stability (inflation levels around and below 4%), and continuity, i.e., absence of uncertainty on the Euro being 'a' medium of exchange and store of value not only today but also in the near future. The absence of uncertainty is the strategic advantage of the current CB system over cryptocurrencies.

What does switching to a CBDC mean? CBDC is fully electronic and therefore, may create uncertainty about its usage for certain, elder generations of the population. If uncertainty on CBDC transactions reaches a level close to uncertainty on how to transact via cryptocurrency, its adoption as a payment method becomes uncertain and may lead citizens to opt-out of the Euro currency system.

In contrast, while CBDC wants to be less like cash, Bitcoin wants to be more like cash. Let me introduce you to the Lightning Network. The Lightning Network is a layer-two system which runs on top of the Bitcoin protocol. While every Bitcoin transaction is written in the public Bitcoin blockchain, transactions via the Lightning Network can be conducted off-chain, by this remaining unrecorded in the public ledger. Therefore, the Lighting network on Bitcoin not only achieves higher speed and number of transactions per time unit (scalability) than Bitcoin does, but it, in particular, allows a higher degree of anonymity, by this moving further towards the goal of becoming 'digital cash'.

To conclude my first point, giving up cash as a non-digital payment method may create uncertainty. But lack of uncertainty is the strategic advantage of the current CB system over cryptocurrencies.

The second point I would like to make is that a CBDC based structure is more centralized than the structure of the current CB system. As a consequence, the central bank becomes more prone to cyber-attacks. Further, the amount of data collected will make the central bank itself the subject of supervision .

The CBDC implied system is more centralized than the current cash-deposit CB structure. Currently, there coexist several private and public deposit making banks. Citizens have their deposits in these banks, and the banks in return hold reserves in the central bank. There are no direct deposits in the central bank, yet, the central bank is the central node.

With a CBDC system, citizens have direct deposits in the central bank, potentially replacing their deposits in private banks.

Why can more centralization harm?

A centralized structure requires reliance on the central node, the central bank, in terms of its full functionality. To explain, if the CBDC system is account-based (non-private) all transactions of citizens will be visible by the central bank. Centralization via CBDC causes the accumulation of large amounts of sensitive information. The number of deposit accounts at the central bank level is likely to grow larger than the number of accounts at the average private bank. Thus, also the information aggregation on the level of the CB can exceed the

information gathered by the average deposit making bank. In contrast, in the current system, information aggregation through payments is segmented. It takes place at the level of *multiple* private banks that collect *complementary* information on customers.

The sensitivity of information can reach or exceed that of facebook's and Amazon's collected data. We talk about salaries, shopping behavior, payments by public figures such as politicians and CEOs of companies. As a consequence, the CB may itself become a target for cyber-attacks. We remember the Equifax data breach in 2017, where around 143 million customers' accounts were hacked or the 2014 data breach regarding JP Morgan Chase, where 83 million accounts were hacked.

In addition, if we impose privacy and data regulation on data collecting firms such as facebook and amazon, we have to impose the same kind of regulation on the CB according to the principle 'same business, same risk, same regulation'. Who will supervise and regulate the CB? Have we thought the possibility that an attack on CBDC accounts may undermine trust in the system and exactly create the demand for anonymity which the CBDC based system then can no longer serve? As citizens opt-out, the impact of central bank monetary policy vanishes.

These arguments so far concern attacks from the outside, but what about attacks from the inside? The data accumulation of payment information makes CBs also prone to political influencing. But central banks should aim for and protect their political independence. Altogether, the transition to CBDC makes the central bank a more interesting target for attacks. This is critical for centralized systems. Bitcoin achieves to be trusted even in nontrusted environments, i.e., when nodes act selfish or are hostile. It achieves this goal through decentralization, free entry, and mutually independent operating nodes. Our banking system should try to mimic this structure, and the current private banking system comes closer to it than the CBDC based one.

To summarize, the switch to CBDC implies the aggregation and centralization of highly sensitive data on payment streams. This makes the CB prone to attacks from the inside and the outside. Questions we will have to deal with is what is the amount of public money we are willing to spend on hiring (the best) cyber security experts. Potentially, the separation of the provision of money by the CB and the processing of payments by banks should remain.

The last point I would like to make is that the introduction of CBDC may lead to conflicts of interest with the CB's stability mandate. In order to stabilize currency and target inflation, CBs use the tool to 'print money' through open market operations. With a CBDC based system, however, printing money may serve a second purpose. In case of rumors on the CB's assets, customers can directly run at the central bank to save their deposit. Since there is no lender of last resort (LoLR) for the LoLR, the CB may have to stop the run by printing money, by this loosening monetary policy and affecting the price level of the currency even if not wanted. If the run occurs during economic boom times due to an idiosyncratic shock to the CBs assets, the CB is in a situation where she would want to tighten monetary policy to stabilize prices but has to print money to fend off the run. There is a conflict of interest.
In the current CB system, on the other hand, there can be runs on multiple private deposit making banks. But idiosyncratic shocks do not affect all private banks simultaneously.
Since the private banks are small in comparison to the CB, the CB can intervene as the LoLR and provide liquidity. The private banks provide a cushion layer between the CB and demand-deposits. With centralization via CBDC, the CB is directly exposed to depositor runs.

References

Agur, Ari, Dell'Ariccia (2019): Designing Central Bank Digital Currencies

Fernandez-Villaverde, Jesus; Sanchez, Daniel; Schilling, Linda; Uhlig, Harald: 'CBDCs and the reorganization of the banking system' [coming soon]

Lagarde, Christine; IMF staff paper: 'Winds of Change: The Case for New Digital Currency'

Mancini-Griffoli, Martinez, Agur, Ari, Kiff, Popescu, Rochon (2019): Casting Light on Central Bank Digital Currency, IMF staff note