BANK OF CANADA
BANQUE DU CANADA

Technology Approach for a CBDC

Staff Analytical Note 2020-6 (English)
Dinesh Shah, **Rakesh Arora**, **Han Du**, **Sriram Darbha**, **John Miedema**, **Cyrus Minwalla**
February 2020

While no decision has been made to pursue the issuance of a central bank digital currency (CBDC), this paper explores the technological approach to constructing a CBDC system for contingency planning purposes. Any design needs to be determined by policy choices about the attributes of the CBDC (e.g., privacy, resilience); the business model (considering, e.g., partners, end-user channels and the cost model); and the qualities the system supports (e.g., user experience, security). This note explores these options and describes the potential limits that the underlying technology may impose on the mix of policy objectives.

Key messages

- The capability of currently available technologies means that developing and deploying a Canada-wide retail CBDC system is possible. In addition, newer technologies are capable of supporting policy nuances, especially around privacy and universal access.
- Enabling both privacy for users *and* controlled disclosure (to comply with anti-money-laundering and other laws and regulations) is challenging. However, it is achievable using advanced cryptographic techniques and operational arrangements.
- Universal access can be realized through compact dedicated devices or stored-value cards, or a combination of these. This would allow for a cash-like experience that includes direct person-to-person transfers.
- We have investigated two broad categories of core technologies—centralized and decentralized (blockchain). The case for a blockchain approach is not clear since its value is most evident in situations where there is no commonly trusted party, whereas in the case of a CBDC, the Bank of Canada would be a trusted party. However, additional research is needed.

Considerations in system design

A CBDC system for Canada

While additional clarity and refinement of requirements are needed, the Bank of Canada would be able to develop a system that supports the ability to:

- store a claim in Canadian dollars against the Bank of Canada
- make payments person to person, at points of sale and online
- purchase and sell a CBDC with commercial bank money or cash

Transaction rates of around 1,000 payments per second are achievable. This is roughly equal to 25 million people making 2 payments per day spread evenly over 12 hours. The architecture could be designed for scaling. High security standards could also be achieved, albeit by possibly trading off other features, such as the openness of the system to third-party extensions.

The availability of cloud computing and other services means we would not have to invest in large infrastructure during research and development, in this way deferring the highest costs until the system is put into operation. Thus, a contingent CBDC system could be developed, with a choice of states of readiness, without incurring inordinate capital costs.

Integration with the retail payment system and banking ecosystem

To buy and sell a CBDC, the system would need to integrate with Interac and, in the future, Real-Time Rail[1] (where the CBDC system would act like a commercial bank). Payment at point of sale and online would require either integrating with existing networks or creating a network specifically for the CBDC.

Existing networks would provide the benefit of an established infrastructure, but using them would tie a CBDC to network fees. On the other hand, a new dedicated network would need to be built from scratch. However, it could leverage the newest technology to mitigate costs.

For users without bank accounts, the system would need to provide access points (like that of the m-pesa[2] mobile payment system in Kenya) that allow cash-to-CBDC purchases and redemption.

Core technology and architecture

The primary determinants of the system architecture of a CDBC are privacy, resilience, universal access and security. The Bank's research has created a deep body of knowledge on these. The precise requirements across these public policy objectives would need to be defined before architecture design could be completed.

Blockchain has been discussed extensively. However, other approaches, including quite conventional centralized systems, also have merits. Because the Bank of Canada is a trusted third party, the rationale for a blockchain approach would not entirely apply. However, some properties of blockchain systems, such as immutable data and smart contracts, support functions like conditional payments (e.g., where a payment would be made on receipt of goods).

A mixture of technologies would likely be needed to achieve public policy objectives and meet user requirements. The Bank can monitor the evolution of these technologies to take advantage of the benefits they bring as they mature.

No distinctions between accounts and tokens

Research on CBDC often draws a fundamental distinction between account-based and token-based architecture. At the end-user, functional level, the distinction is not as clear. Furthermore, there is no universally accepted definition of a token. It may therefore be preferable to avoid framing the scope of a CBDC in terms of notions of accounts and tokens. To maximize flexibility, any policy or legislative definitions should be technology-neutral (e.g., by using terms like “value in electronic form”).

A layered platform approach

A platform approach is flexible in that it supports three business models:

- the Bank provides the entire system
- the Bank only issues and redeems the digital currency, with third parties providing all end-user services
- a mixed model in which the Bank supplies a minimal viable service (supporting public-policy goals) that can be supplemented with value-added services from third parties for end-users (e.g., targeted to small businesses)

A well-designed system would separate the core system from the front-end user experience. Clearly designed interfaces between system components would help make deployment, vendor selection and the business model more flexible. For example, as new types of consumer electronics devices became available, they would be integrated into the system, perhaps by third parties, without the need to alter the core of the system.

This approach could support smartphones, universal access devices (UADs) and integrated points of sale. In the future, the platform could extend to new-use cases, such as payments between automated systems (e.g., rideshare apps that use autonomous vehicles). Furthermore, layering supports the ability for third parties to build on top of the core, if needed.

Attributes of a central bank digital currency

Access

Universal access could be engineered to distinguish a CBDC from conventional payment offerings. Apps for smartphones could be designed to be accessible to users who have sight, dexterity or cognitive impairments. For users without a bank account or smartphone, stored-value cards and small, portable UADs could allow cash-like, person-to-person transfers. UADs support goals for financial, digital and accessibility inclusion. A small user-base may find operating a smartphone or UAD difficult; the Bank would need to find a solution to this challenge.

Privacy

Enabling both privacy and regulatory compliance will be challenging, but new technologies provide options. Privacy is not the sole purview of the Bank, and we will need to clarify the exact level of privacy to consider by consulting with external institutions (e.g., the Privacy Commissioner of Canada, civil liberties advocates, law enforcement and the Financial Transactions and Reports Analysis Centre of Canada). While not every possible requirement will be practical, new cryptographic techniques may allow the Bank to satisfy the need for privacy as well as controlled disclosure (e.g., disclosure required to comply with anti-money laundering regulations).

Payment of interest

Currently, our studies are considering only non-interest-bearing CBDCs. Enabling the payment of interest may be challenging. In systems where transaction time stamps and interest rates are known, calculating interest to be paid is straightforward. But using a UAD in a de-networked way (directly from one device to another) would be more complex since this information may not be readily available. It may be possible to determine the time by using an onboard clock or the interest rate when connecting to a network.

In a positive-rate environment, a UAD user who did not connect to the network would forego interest; but this would also allow the user to avoid paying interest in a negative-rate environment. One policy remedy would be to simply cap the maximum allowable amount on a UAD and not calculate interest. Another would be to require occasional connection to a network, perhaps every 50 transactions or so. Further research is needed in this area.

Resilience

Payment systems are in general built to be very robust, using techniques such as multiple geographically dispersed data centres. In this way, even if one or two data centres were to fail, the system as a whole would continue to function, albeit with some degradation in services.

The current state of computer and software engineering would allow for a highly resilient CBDC system. A system that incorporates UADs could function without continual power or network access, adding to the resilience. However, such a system would have reduced functionality (e.g., it would not be able to add more CBDC from the Bank since this requires network connectivity).

Settlement finality and irrevocability

Most technological choices would allow the completion of transactions at a clear point in time. The point of settlement finality, defined as the point at which the transaction is irrevocable, would need to be clear to users.

While a CBDC-to-CBDC transaction may have immediate settlement finality, the point in time of settlement in a purchase and sale of a CBDC using commercial bank money would depend on the national clearing and settlement system. A cash-like immediate settlement would simplify the engineering of a CBDC system. Transaction revocation would both complicate the engineering and require operational support (customer requests for revocation).

On this issue, system designers will require policy guidance, and end-users will require clear communication.

Distribution channel

The digital nature of a CBDC may enable firms other than financial institutions to act as distribution channels. If an end-user purchase of a CBDC from a distributer settled instantly, then the distributor would not need to maintain a stock of CBDC. This would reduce barriers to entry for a distributor. The question of distribution will be addressed by the business model.

In summary

A CBDC system would need to have cash-like properties that are not typically present in other money and payment systems—in particular, privacy, universal access and resilience to infrastructure outages. Beyond these cash-like properties, a CBDC system should strive to enhance financial and digital inclusion, for example, by allowing purchases from online merchants. These are challenging to design and build and will require further research.

An approach to design that supports these core properties but allows for additional services could create an innovative ecosystem of products and services, if desired.

Designing and building a contingent CBDC system for Canada is a challenging enterprise. While there is no commitment to issuing a CBDC, the Bank could achieve a contingent state of readiness. This will provide the confidence that, should it be decided in the future that a CBDC is necessary, the Bank could deploy one within a reasonable time frame.

Endnotes

Footnotes

1. As part of Payments Canada's payment system modernization program, Real-Time Rail is designed to enable fast, convenient payments and funds transfers.[←]

2. The m-pesa system makes use of thousands of agents (e.g., cellular airtime sellers) around the country, where people can buy and sell m-pesa mobile money with cash. [←]

Disclaimer

Content Type(s): **Staff research**, **Staff analytical notes**
Topic(s): **Central bank research**, **Digital currencies and fintech**
JEL Code(s): **E**, **E4**, **E42**, **E5**, **E51**, **O**, **O3**, **O31**
DOI: https://doi.org/10.34989/san-2020-6