BANK OF CANADA
BANQUE DU CANADA

Staff Analytical Note/Note analytique du personnel — 2020-21

Last updated: October 5, 2020

Security and convenience of a central bank digital currency

by Charles M. Kahn[1] and Francisco Rivadeneyra[2]

[1] Department of Finance and Department of Economics
University of Illinois, Champaign, Illinois, United States of America 61820

[2] Funds Management and Banking Department
Bank of Canada, Ottawa, Ontario, Canada K1A 0G9

cmkahn@illinois.edu, frivadeneyra@bankofcanada.ca

ISSN 2369-9639

Acknowledgements

This paper is based on "Eggs in One Basket: Security and Convenience of Digital Currencies," by Charles M. Kahn, Francisco Rivadeneyra and Tsz-Nga Wong (2020).

We thank James Chapman, Scott Hendry, Cyrus Minwalla and Dinesh Shah for valuable comments.

Abstract

An anonymous token-based central bank digital currency (CBDC) would pose certain security risks to users. These risks arise from how balances are aggregated, from their transactional use and from the competition between suppliers of aggregation solutions. The central bank could mitigate these risks in the design of the CBDC by limiting balances or transfers, modifying liability rules or imposing security protocols on storage providers.

Topics: Central bank research; Digital currencies and fintech; Financial system regulation and policies; Payment clearing and settlement systems
JEL codes: E, E4, E42, G, G2, G21

Résumé

Une monnaie numérique de banque centrale (MNBC) anonyme sous forme de jetons présenterait certains risques de sécurité pour les utilisateurs. Ces risques tiennent aux méthodes d'agrégation, au rôle des jetons comme intermédiaire des échanges et à la concurrence entre les fournisseurs de solutions d'agrégation. En limitant les soldes ou les transferts, en modifiant les règles de partage de la responsabilité ou en imposant des protocoles de sécurité aux fournisseurs de dispositifs de stockage, la banque centrale peut atténuer ces risques lors de la conception de la MNBC.

Sujets : Recherches menées par les banques centrales; Monnaies numériques et technologies financières; Réglementation et politiques relatives au système financier; Systèmes de compensation et de règlement des paiements
Codes JEL : E, E4, E42, G, G2, G21

Introduction

An anonymous token-based central bank digital currency (CBDC) would pose particular security risks. These risks arise from how balances are aggregated and stored, how CBDC is used for transactions, and how various solutions such as e-wallets, crypto exchanges and banks compete to attract users. Potential security risks include the following:

- Digital currencies allow users to aggregate balances in anonymous addresses on a scale not possible with cash. This creates trade-offs between security and convenience that do not exist for cash and traditional bank accounts.
- Users of anonymous digital currencies will economize on the costs of security management of these addresess balancing them with the risk of loss. Depending on the arrangement, storage solutions for digital currencies will pose different security threats; because users are unlikely to fully bear potential losses, they are unlikely to exercise enough care.
- The safety of CBDC will also depend on the competition between providers of aggregation solutions and the interaction of individual security protocols chosen by each supplier. Externalities from competition will be present because suppliers will not internalize the risks to their users that result from their security standards.
- To mitigate these risks, the central bank can:
    - design the CBDC to limit balances or transfers,
    - modify liability rules, and
    - direct the security protocols chosen by the suppliers of aggregation solutions.

CBDC form, security and convenience

If the Bank of Canada were to issue a CBDC, it would likely be token-based.[1] Token-based digital currencies are secured by private keys. Managing private keys can be inconvenient for individuals, and this could stimulate demand for convenience solutions for managing keys and carrying out transactions. In response to this demand, a CBDC ecosystem will likely emerge, with public and private components.

To ensure that CBDC is a safe and efficient means of payment, the Bank needs to carefully consider how CBDC will be aggregated and used, and what externalities will arise from it.

Aggregation

Anonymous digital currencies store balances of tokens in addresses that do not associate the account balance with the identity of the account owner. These addresses can, in principle, store an arbitrarily large

[1] The Bank of Canada is unlikely to issue an account-based CBDC because it would require the Bank to bear the responsibility of verifying and maintaining the identity of the users in the system (see Kahn, Rivadeneyra and Wong 2008).

balance of tokens. The account balance in each address is secured by a private key that is virtually impossible to guess but inconvenient to manage directly.

To use any token in a given address, the private key belonging to that address must be used during the transaction. Losing the private key of an address implies the permanent loss of the *entire* balance of tokens in that address.

To reduce the risk associated with losing their key, which arises from storing and managing private keys directly, users rely instead on e-wallets and account providers. An e-wallet is software, secured with a password, designed to manage multiple private keys. When users of e-wallets forget their password, they risk losing all their private keys managed by the e-wallet. Thus, the user's risks associated with losing each private key are combined with the use of an e-wallet. Developers of e-wallets do not typically bear liability in case of loss, regardless of whether the loss results from vulnerabilities in their code or carelessness of the user.

Another way to store a digital currency is by using account providers (such as crypto exchanges) that manage users' private keys and essentially take possession of their tokens. In exchange, users receive an account associated with their identity. This could help users recover their balances in case of forgotten passwords and protect them against fraudulent transactions.

Managing balances of digital currencies presents the users with a trade-off between the security of their balances and the convenience of using them for transactions. This is different from the trade-off between cash and traditional bank accounts because:

- directly storing large amounts of cash is more inconvenient than directly managing digital currencies; and
- because the aggregation solutions of digital currencies and traditional bank accounts have different liability standards, for example traditional bank accounts have deposit insurance.

Table 1 summarizes the main forms of aggregation of digital currencies and their trade-offs between security and convenience.

Table 1: Forms of aggregation, key and transaction management in digital currencies. Tokens are the basic store of value that are aggregated in addresses, wallets and accounts

Aggregation method:	Address	→	E-wallet	→	Account
Provided by:	Digital currency		Developers		Crypto exchanges, banks
Secured by:	Private key		E-wallet password		Account password
Key management:	User controls and manages private keys directly		Software manages keys, but user maintains control		Account provider controls keys
Risks:	Forgetting/losing keys; key theft	+	Code vulnerabilities of e-wallet	+	Account provider fraud
Benefits:	Privacy		Key and transaction management	+	Alternative recovery mechanisms with identity; protection against fraudulent transactions
Liability for loss:	With the user		With the user		Potentially shared depending on contract

Security risks

Users face the following risks from storing and using digital currency balances in anonymous addresses:

- forgetting or losing their private keys;
- code vulnerabilities in e-wallets and account providers, which can result in theft of the keys or hacking of the account providers; and
- falling victim to fraud and wrongdoing conducted by the account providers.

In equilibrium, these risks will be shared between users and providers. Users will economize on the costs of key and transaction management, balancing these costs against the risks of theft and malfeasance from the account providers. Evidence shows that theft of private digital currencies and wrongdoing by account providers are quite common (Ciphertrace 2019). This is not related to the cryptographic protocols of digital currencies, which are extremely secure, but rather to how users store and use their balances (either directly, with e-wallets or with account providers).

If the Bank were to issue an anonymous token-based CBDC, it should expect similar risks to arise.

Externalities

A CBDC ecosystem would face three main security externalities. First, a typical balance holder faces increased risk from hackers attempting to break into large accounts held by account providers. Because hackers cannot identify the sizes of individual accounts, an account provider with larger total balances will provide more incentives to hackers, leading to additional risk for all account holders using that account provider.

Second, account providers might have a competitive incentive to absorb some of the losses, and regulations might limit the losses account providers can pass on to users. Therefore, users who store their digital currencies with account providers typically use enough caution to secure their balances.

Third, account providers will not internalize their costs by lowering security standards when competing to attract users. Externalities will exist unless users fully bear losses and authorities intervene in directing the security protocols that account providers establish.

Implications

If central banks establish liability rules for the loss of CBDC similar to those that exist for bank notes and traditional bank accounts, users will have the incentive to exert a greater level of care when managing their balances of CBDC. Enforcing these rules, however, might not be straightforward because determining responsibility for the loss of digital currencies can be difficult.

Enforcement of liability rules would be further complicated if the design of the CBDC allows any individual or firm to directly hold the digital tokens. If this is possible, it is likely that some users to store their balances in accounts at third parties that might be out of reach of domestic authorities.

Designing a CBDC that is universally accessible but that can be stored only at approved intermediaries is a technological challenge that should be investigated.

References

Ciphertrace Cryptocurrency Intelligence. 2019. *Cryptocurrency Anti-Money Laundering Report, 2018-Q4*.

Kahn, C. M., F. Rivadeneyra and T.-N. Wong. 2018. "Should the Central Bank Issue E-money?" Bank of Canada Staff Working Paper No. 2018-58.

Kahn, C. M., F. Rivadeneyra and T.-N. Wong. 2020. "Eggs in One Basket: Security and Convenience of Digital Currencies." Working Paper No. 2020-032A.