Taguette highlights: solution statement

Privacy in a CBDC goes beyond binary choices of anonymity or full disclosure.

Document: bankofcanada.ca-Privacy in CBDC technology.pdf **Tags:** solution statement

---

There are many cryptographic techniques and operational arrangements for a fine-grained privacy design. These demand knowledge of the detailed requirements around privacy and disclosure.

Document: bankofcanada.ca-Privacy in CBDC technology.pdf **Tags:** solution statement

---

Security of a CBDC

bankofcanada.ca/2020/06/staff-analytical-note-2020-11

Document: bankofcanada.ca-Security of a CBDC.pdf **Tags:** solution statement

---

This includes the possibility that a CBDC could be fully anonymous for small value payments but not for large payments.

Document: cbdc- user needs and adoption.pdf **Tags:** solution statement

---

Cash-like. The technology would need to enable person-to-person transfers with immediate settlement, offer a great deal of privacy (not anonymity),

have very high resilience in the event of infrastructure failure and be universal y accessible.

Document: Contingency Planning for a Central Bank Digital Cu **Tags:** solution statement

---

The Bank wil continue to investigate both centralized and decentralized options for implementing a CBDC. For the core system, the Bank wil draw on cutting-edge techniques, such as new cryptographic schemes, tamper-resistant hardware and hardware security modules to ensure privacy, security and resilience.

Document: Contingency Planning for a Central Bank Digital Cu **Tags:** solution statement

---

The appropriate degree of anonymity in a CBDC system is a political and social question, rather than a narrow technical question. As discussed above, CBDC would need to be compliant with AML regulations, which rules out truly anonymous payments. However, CBDC could be designed to protect privacy and give users control over who they share data with, even if CBDC payments are not truly anonymous (or secret). For example, a user may legitimately want to make a payment to a supermarket without sharing their identity with the supermarket, as this would allow the supermarket to build a picture of their shopping habits. In most cases, the payer should be able to pay without revealing their identity to the payee. In this sense, they could have anonymity with regards to other users, without having anonymity with regards to law enforcement.

Document: Discussion Paper - Central Bank Digital Currency . **Tags:** solution statement, dataholder

---

Data privacy: involving third parties in the processing of transactions (‘transaction validators’) may require the sharing of private data with them. There are approaches to mitigate this, but these come with their own challenges.(1) One approach involves segregating the data so that each

individual transaction validator only has visibility of a subset of the ledger. Alternative approaches involve using advanced cryptographic techniques (for example those based on zero-knowledge proofs)(2) to hide details, such as the counterparties or the value of the transaction, from the transaction validators. However, these are currently computationally intensive and currently have a negative impact on performance.

Document: Discussion Paper - Central Bank Digital Currency . **Tags:** solution statement

---

As a result of these considerations, the benchmark CBDC would provide for some increased contestability with other electronic payment methods, possibly in terms of reduced costs, and, in particular, in terms of enhanced privacy.

Document: Engert and Fung - Central Bank Digital Currency Mo **Tags:** solution statement

---

Alternatively, CBDC transactions in excess of a threshold value could be required to satisfy user identification requirements; this would eliminate anonymity for such transactions.

Document: Engert and Fung - Central Bank Digital Currency Mo **Tags:** solution statement

---

For example, online transactions may be foregone because of the following frictions:15

• Security and privacy concerns: Users may worry about how their payment information is stored and transferred. However, there are some market solutions that address these concerns.

Document: Fung and Halaburda - 2016 - Central Bank Digital C **Tags:** solution statement

---

A number of privacy-preserving techniques are based on cryptography (e.g., encryption of user data) and operational arrangement (e.g., distribution of decryption key fragments among multiple agents who do not have the incentive to col ude).

Document: Jiang - CBDC adoption and usage some insights from **Tags:** solution statement

---

And central banks may be prepared to offer full anonymity only with strict and low limits on CBDC holdings, thus undermining scalability.

Document: Mancini-Griffoli et al. - 2019 - Casting Light on **Tags:** solution statement

---

37. **Depending on its design, CBDC can strengthen or undermine financial integrity.**

Financial integrity could be strengthened if authorities impose strict limits on the size of transactions. Alternatively, CBDC can be designed to facilitate effective identity authentication and tracking of payments and transfers. Identities would be authenticated through customer due diligence procedures, and transactions recorded. But unless required by law, users' information could be protected from disclosure to third parties and governments, while criminals could be deterred by the risk of investigation and prosecution. Although promising on paper, these solutions would have to be further evaluated, and questions answered. For instance, Would users trust the safeguards established to protect their privacy? Would central banks be held responsible for 27 Judson (2017); sample includes Australia, Brazil, Canada, the euro area, Hong Kong SAR, India, Japan, Mexico, Singapore, South Arabia, South Korea, Sweden, Switzerland, Turkey, Russia, the United Kingdom, and the United States.

See also Europol (2015).

compliance failures, even if customer due diligence procedures were outsourced? And to what extent could authorities benefit from the ability to scrutinize transaction information for il icit activity in real time? On the other hand, CBDC offering full anonymity and large-value transactions would undermine financial integrity relative to cash and current noncash fund transfer systems. Whatever design is chosen, it should accommodate the implementation of effective AML/CFT measures.

Document: Mancini-Griffoli et al. - 2019 - Casting Light on **Tags:** solution statement, problem statement

---

There are many cryptographic techniques and operational arrangements for a fine-grained privacy design. These demand knowledge of the detailed requirements around privacy and disclosure.

Document: Privacy in CBDC technology.pdf **Tags:** solution statement

---

The proof of concept drawn up by the ESCB demonstrates that it is possible to construct a simplified CBDC payment system that allows users some degree of privacy for lower-value transactions, while still ensuring that higher-value transactions are subject to mandatory AML/CFT checks.

That proof of concept boasts several novel features developed by the ESCB’s EUROchain research network (with the support of Accenture and R3) using distributed ledger technology (DLT). It provides a digitalisation solution for AML/CFT

compliance procedures whereby a user’s identity and transaction history cannot be seen by the central bank or intermediaries other than that chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional checks are delegated to an AML authority. This is achieved using

“anonymity vouchers”, which allow users to anonymously transfer a limited amount of CBDC over a defined period of time.

Document: ecb.mipinfocus191217.en.pdf **Tags:** solution statement

---

Anonymity vouchers

In order to enforce AML/CTF limits on the amount that a user can spend without the AML authority seeing transaction data, a novel new concept – “anonymity vouchers”

– has been devised. The AML authority issues these additional, time-limited states to every CBDC user at regular intervals.7 If users want to transfer CBDC without revealing information to the AML authority, they need to spend these vouchers (at a ratio of one voucher per CBDC unit transferred). Thus, the amount of CBDC that can be spent anonymously is limited by the number of vouchers that the AML authority provides to each user.

Although vouchers are technically “spent”, they are issued free of charge and are not transferrable among users. They are simply a technical tool used to limit the amount of CBDC that can be transferred anonymously. This means that limits on anonymous CBDC transfers can be enforced without recording the amount of CBDC that a user has spent, thereby protecting users’ privacy.

Document: ecb.mipinfocus191217.en.pdf **Tags:** solution statement

---

Adding privacy-enhancing techniques: privacy could be further enhanced by using mechanisms such as rotating public keys, zero-knowledge proof and enclave computing. Using rotating keys, which would involve users generating new pseudonyms on a regular basis, would limit nodes’ ability to link transactions to individual users, since users would be using various different pseudonyms over time.

Document: ecb.mipinfocus191217.en.pdf **Tags:** solution statement