Security and Privacy Challenge in CBDC

John Tsz Hon Yuen

The University of Hong Kong,

Hong Kong

HKU FinTech Day 2021
2021/11/2

Security

- **The CBDC ecosystem will be a high-value target once deployed**.
  - The central bank would have to put suitable controls and processes in place to mitigate the risk of large-scale attacks from these advanced persistent threats

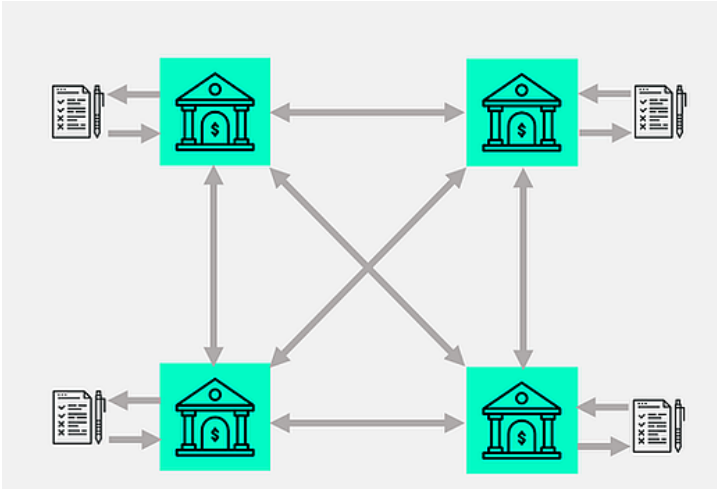
- **Security is a primary attribute for a CBDC**.
  - Confidentiality, integrity and availability.
  - Operational security: continuous testing, authentication safeguards, adherence to best practices and periodic external audits of key system components.

Security of Different CBDC Design

- **Potential CBDC designs offer differing levels of security**.
  - Solutions that rely on centralized or distributed designs maximize integrity and availability, at the risk of confidentiality.
  - Solutions built around dedicated devices that embed a store of value eliminate system-wide risk at the expense of integrity.
  - A hybrid solution maximizes usability but increases risk and cost.

Security of Different CBDC Design

- **Distributed ledger technology (DLT)**
  - Public DLTs do not fit the risk profile for a CBDC system.
  - Private/permissioned DLTs offer redundancy and payment authenticity (non-repudiation) by design but increase operational complexity and points of vulnerability.



- **Local store-of-value devices**.
  - Devices incur an integrity risk and can be damaged or stolen.
  - Dedicated single-purpose devices that store value locally are robust against network-level attacks or acts of nature.

Privacy Requirement

- Privacy is a more challenging task due to its complexity
  - Should all transactions be routinely disclosed to the government, or only some (e.g., by dollar threshold)?
  - Should law enforcement be able to determine a person's holdings, even if only approximately?
  - Should a payer's identity be hidden from a merchant?
  - What transaction details should be shown to a payer's MSB?
  - Should users be able to transact outside of KYC regulations to some extent?

A Wide Range of Privacy

- What is technologically feasible for privacy in a CBDC system?
  - goes beyond binary choices of anonymity or full disclosure

Table 1: Privacy profiles of payment technologies

Solution	Government					Payer MSB					Payee MSB					Payee	Payment providers					Public (other users)				
	H		T			H		T			H		T			T	H		T			H		T		
	O	B	Pr	Pe	A	O	B	Pr	Pe	A	O	B	Pr	Pe	A	Pr	O	B	Pr	Pe	A	O	B	Pr	Pe	A
Credit card (stripe)	3	3	1	1	0	0	0	0	0	0	2	3	2	0	0	0	1	3	1	0	0	3	3	3	3	3
Credit card (EMV)	3	3	1	1	0	0	0	0	0	0	2	3	2	0	0	2	1	3	1	1	0	3	3	3	3	3
E-transfer	3	3	1	1	0	0	0	0	1	0	1	3	1	0	0	2	1	3	1	1	0	3	3	3	3	3
Debit card	3	3	1	1	0	0	0	0	0	0	1	3	1	0	0	1	1	3	1	1	0	3	3	3	3	3
Permissioned DLT	1	0	1	1	0	0	0	0	1	0	1	3	1	0	0	1	1	0	1	1	0	3	3	3	3	3
Bitcoin custodial	2	3	2	2	0	0	0	0	2	0	2	3	2	0	0	2	2	3	2	2	0	2	3	2	2	0
Bitcoin pro	3	3	2	2	0	3	3	2	2	0	3	3	2	2	0	2	3	3	2	2	0	3	3	2	2	0
Tiered ledgers	1	0	1	1	0	0	0	0	1	0	2	3	2	0	0	1	3	3	3	3	3	3	3	3	3	3
Device-based (KYC, non-transferable)	0	2	2	0	2	0	2	2	0	2	0	2	2	0	2	1	2	3	3	3	3	3	3	3	3	3
Device-based (non-KYC, transferable)	3	3	2	0	2	3	3	2	0	2	3	3	2	0	2	1	2	3	3	3	3	3	3	3	3	3
Cash	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3

Note: Higher/darker values indicate more privacy.

Holding (H) has an owner (O) and a balance (B)
Transaction (T) has a payer (Pr), payee (Pe) and amount (A)

https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/

Privacy-Enhancing Technologies

- 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.
  - **Group signatures** (Chaum and van Heyst 1991)
  - **Secret sharing** (Shamir 1979)
  - **Zero-knowledge proofs** (Blum, Feldman and Micali 1988)
  - **Homomorphic encryption** (Rivest, Adleman and Dertouzos 1978)
  - **Multi-party computation** (Yao 1982)
  - **Differential privacy** (Dwork and Roth 2014)

Privacy by Design

- The central bank could engineer a CBDC system with higher levels of privacy than commercial products can offer—but with trade-offs.
- Some combinations of requirements will not be feasible or may lead to high operational costs and excessive complexity and risk.
- The user's overall privacy will depend on factors such as user behaviour and the privacy policies of other entities in the CBDC ecosystem.

Challenge for Privacy in CBDC

- Maintaining privacy and complying with regulations (requires disclosure of information) for a CBDC is challenging. This is further complicated by the need for proactive disclosure to prevent fraud.
  - Techniques to achieve cash-like privacy are immature, have limited deployments, and difficult to comply with KYC and AML regulations.

- A designer could build a system with hybrid privacy levels.
  - Unregulated holdings and transactions (offering maximum privacy to users) would be permitted within limits (e.g., a maximum amount) alongside regulated ones without limits.

Trust

- Public trust in the privacy design could be enhanced through third-party reviews of CBDC architecture and operations.

Conclusion

- The CBDC ecosystem will be a high-value target once deployed, and hence security is essential.
- Privacy is a challenging task due to its complexity, and it is difficult to achieve cash-like privacy.
- Hybrid solutions are possible for fine-grained control in security and privacy.

Thank you!