Taguette highlights: problem statement

Generally, achieving high levels of privacy while complying with regulations is complicated.

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

---

Is it possible to enable full privacy whilst also achieving the resiliency benefits of distribution?

Document: BoE Open Problems.pdf **Tags:** problem statement

Privacy considerations could create a series of other design and interoperability challenges, ranging from the messaging standards used, how to create incentives for diverse intermediaries to offer services, and how to interoperate with traditional systems that require detailed account and transaction information.

Document: CBDC - Executive Summary .pdf **Tags:** problem statement

---

Privacy considerations could create a series of other design and interoperability chal enges, ranging from the messaging standards used, how to create incentives for diverse intermediaries to offer services and how to interoperate with traditional systems that require detailed account and transaction information.

Document: CBDC - System design and interoperability .pdf **Tags:** problem statement

---

What is the appropriate privacy model for CBDC? Is it necessary, or feasible, to replicate any of the privacy aspects of cash?

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

---

With respect to safety, there are still many unanswered questions regarding the risks of cyber attacks and the protection of the privacy of users.

Document: Kahn - Should the Central Bank Issue E-money.pdf **Tags:** problem statement

---

But the greater the anonymity, the harder it is to reverse fraudulent transactions (risk of theft) and claim ownership (risk of loss).

Document: Mancini-Griffoli et al. - 2019 - Casting Light on **Tags:** problem 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).

20 INTERNATIONAL MONETARY FUND

CASTING LIGHT ON CENTRAL BANK DIGITAL CURRENCY

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

---

Generally, achieving high levels of privacy while complying with regulations is complicated.

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

---

Enabling both privacy for users and controlled disclosure (to comply with anti-money-laundering and other laws and regulations) is chal enging.

Document: Shah et al. - Technology Approach for a CBDC.pdf **Tags:** problem statement