3

# Decoding Privacy Design Options of CBDCs

## Balancing Confidentiality, Security, and Regulatory Requirements (Fraunhofer FIT)



Atomium of Brussels I Brussels, Belgium

As central banks worldwide move closer to implementing CBDCs, privacy has become one of the most decisive factors for public acceptance, particularly in Western economies. Balancing user confidentiality with regulatory compliance and system security forms a central trade-off in CBDC design. Unlike cash and existing forms of e-money, CBDCs can generate more traceable data for public and private actors. Consequently, decisions on how this data is stored, protected, and shared strongly shape trust, adoption, and transaction and holding limits, ensuring that the amounts transacted or held do not exceed thresholds that would require enhanced regulatory checks.

The digital renminbi (e-CNY) exemplifies this approach by offering multiple KYC tiers, representing an initial design choice that partially shields user data by reducing disclosure requirements for lower-value transactions.[2]

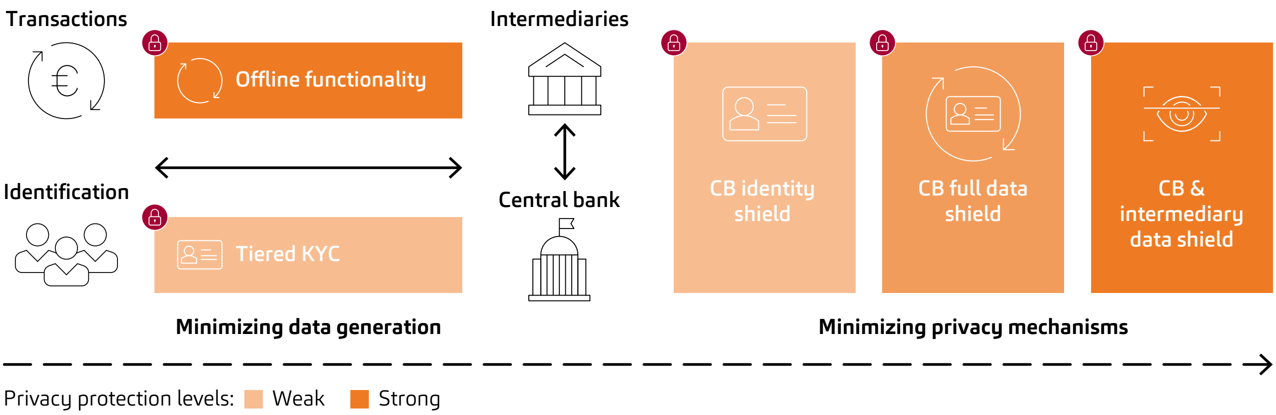


Figure 5: Overview of CBDC Privacy Design Approaches

legitimacy. Current initiatives such as the digital euro, the Sand Dollar, and the e-CNY illustrate different approaches, ranging from centralized architectures to intermediary-based models with various forms of privacy protection.[1] As illustrated in Figure 5, CBDC privacy approaches largely fall into two categories: those that aim to minimize data at the point of generation and those that apply additional privacy-enhancing mechanisms afterward.

Onboarding and transaction execution are the main data-generation points, after which the information is recorded on the data layer. First, because CBDCs operate under a strict regulatory framework, onboarding always requires a Know Your Customer (KYC) process to generate the identification data needed for anti-money-laundering (AML) compliance. In addition to the regular full KYC process, central banks have also developed **tiered KYC** models that allow users to choose how much personal data they wish to disclose, ranging from minimal details such as a phone number to full identification information. These tiers are linked to

Second, transactional data is generated during payment when users authenticate themselves and submit transaction details, generating additional privacy-relevant information. A key design question here is how much of this processing should occur offline on the user's device versus online through a central system. Offline processing within secure hardware elements keeps sensitive information local, enhancing privacy and reducing unnecessary data transmission. However, longer periods without synchronization introduce additional risks, such as undetected misuse or double spending. Online processing, by contrast, continuously synchronizes transactions with a central authority, offering stronger security and ensuring ledger consistency, but increasing data exposure. Consequently, central banks typically follow one of two approaches: They either rely entirely on online verification, as seen in the Bahamian Sand Dollar, or they complement the online system with an **offline functionality**, as planned for the digital euro.[3]

In the latter case, offline payments provide greater privacy for smallvalue transactions, while periodic synchronization with the central ledger restores security guarantees.

These two design choices primarily determine how early-stage data can be minimized during onboarding and payment, allowing users to decide which information will enter the system. Not all CBDCs, however, prioritize privacy; the Sand Dollar and the Nigerian eNaira, for instance, use relatively simple approaches that grant broad data access to central banks and intermediaries, reflecting goals such as financial inclusion and economic monitoring. In Western economies, by contrast, privacy plays a more central role, as trust and democratic legitimacy are key motivations for CBDC adoption.[4]

Analyses indicate that this leads to three privacy-enhancing models: the central bank (CB) identity shield, the CB full data shield, and the CB & intermediary data shield.


The **CB identity shield** refers to designs in which intermediaries process user data for regulatory purposes but apply privacy-enhancing technologies such as blind signatures or encryption to hide identities before forwarding transaction information to central banks for settlement. This limits concealment to identity data: The settlement authority cannot link transactions to individuals, while intermediaries retain the information needed for compliance, similar to current interbank models. The online digital euro appears to follow this structure, as ECB documentation states that user identities will be encrypted and pseudonymized before settlement and stored in a form that cannot be resolved.[5]

This preserves security and enables compliance checks for higher-value transactions while still protecting user identities. The Bahamas central bank has also begun to incorporate elements of this model into its Sand Dollar design.

The **CB full data shield** extends this approach by protecting both user identities and transaction details, often through homomorphic encryption. Intermediaries continue to store the underlying identification and transaction data and remain responsible for AML checks and customer relationships, while the settlement authority that receives this data does not access the raw information. Homomorphic encryption allows compliance and consistency checks to be performed directly on encrypted data, enabling the detection of suspicious patterns or threshold breaches without revealing identities or amounts to central banks. Only designated intermediaries or regulators may access unencrypted information, and even then, only upon lawful request. This privacy-preserving model has been explored extensively in Canada and Sweden, where encrypted computations were evaluated as a way to support oversight while sharply limiting data visibility.[6]

European Court of Justice, Parliament and Philharmonic Hall I Kirchberg, Luxembourg

The **CB & intermediary data shield** is the most privacy-oriented model because it can prevent both the central bank and intermediaries from seeing sensitive information about users and their transactions.

There are several ways this can be achieved, often in combination. For example, users can gain more control over their own payment data through self-custody wallets, payments can be grouped into larger pools so that individual transactions cannot be identified, and privacy-enhancing technologies such as zero-knowledge proofs can verify compliance without revealing identities or amounts.[7]

Although these combinations can provide very strong privacy, they also introduce greater operational and oversight risks, such as making it harder to detect misuse, ensure system integrity, or intervene when suspicious activity occurs. Another challenge is that some approaches, such as self-custody, may require a higher level of technical understanding from users, which can limit accessibility. For these reasons, this model appears mainly in academic research rather than in central bank design projects.

Finally, with only a few CBDCs live, the landscape remains highly experimental. Approaches vary widely, and it is still unclear which privacy model will prove viable at scale. It is, however, beyond dispute that the privacy decisions central banks make today will be central to shaping the future of digital public money.

Fraunhofer
FIT

**Valeriya Arnold**
Researcher at Fraunhofer FIT
valeriya.arnold@fit.fraunhofer.de

**Prof. Dr. Nils Urbach**
Director at Fraunhofer FIT
nils.urbach@fit.fraunhofer.de

1. Schumacher, L. V. (2024): CBDC Examples. In: Decoding Digital Assets, pp. 159–206.
2. Li, S. Y. & Huang, Y. P. (2021): The genesis, design and implications of China's central bank digital currency. In: China Economic Journal, 14(1), pp. 67–77.
3. European Central Bank (2023): A stocktake on the Digital Euro: Summary report on the investigation phase and outlook on the next phase.
4. Schumacher, L. V. (2024): CBDC Examples. In: Decoding Digital Assets, pp. 159–206.
5. European Central Bank (2023): A stocktake on the Digital Euro: Summary report on the investigation phase and outlook on the next phase.
6. A. Veneris, A. Park, F. Long, and P. Puri (2021): Central Bank Digital Loonie: Canadian cash for a new global, pp. 1–76.
7. J. Gross, J. Sedlmeir, M. Babel, A. Bechtel, and B. Schellinger (2022): Designing a Central Bank Digital Currency with support for cash-like privacy, pp. 1–44.