



► Central bank digital currencies:

System design

November 2024

Bank of Canada
European Central Bank
Bank of Japan
Sveriges Riksbank

Swiss National Bank
Bank of England
Board of Governors Federal Reserve System
Bank for International Settlements

Bank for International Settlements (BIS)

ISBN 978-92-9259-806-8 (online)

Central bank digital currencies: system design

1. Introduction and general overview

Since 2020, a group of central banks, together with the Bank for International Settlements, have been exploring selected aspects of central bank digital currencies (CBDCs).¹ As part of this joint work, the group shares insights and perspectives gained from the central banks' individual analysis and experiments on a range of CBDC-themes, including those more broadly related to payments modernization.² This report summarises the group's discussion on several topics in relation to the system design of retail (also called general-purpose) CBDC arrangements.³ These may likely become relevant should a central bank consider developing a retail CBDC arrangement.

The report first provides some perspectives on overall system design and then focuses on four key issues essential for designing a well-functioning retail CBDC system: privacy, cyber security (including quantum computing), offline functionality⁴ and point of sale considerations. These issues are multi-dimensional and often interconnected.

Technical experimentation frequently highlights complementary policy choices that a jurisdiction may need to determine when it is designing or modernizing a payments system. Jurisdictions each have their own existing policy, legal, and regulatory frameworks, as well as their own policy objectives. For a given jurisdiction, addressing legal and public policy requirements as well as interactions and interconnectedness both within and beyond the system may be essential to ensure a coherent system design. The work of the group over the last 18 months has discussed those areas alongside technical capabilities to better understand the associated trade-offs, without drawing specific policy conclusions. Despite progress to better understand the practicalities around these issues, challenges and open questions remain. In addition, for the purpose of developing a well-functioning retail CBDC system, there are other issues which should be addressed.

The main takeaways are:

- In a two-tier CBDC system centralised versus decentralised options may not have to be two mutually exclusive and incompatible design choices. A jurisdiction's optimal architecture may consist of many different modular components, each supporting a specific set of requirements.
- Privacy may be a key consideration for central banks when designing a CBDC system and involves navigating numerous trade-offs. Privacy enhancing techniques (PETs) may provide both opportunities and challenges within a retail

¹ Participating central banks are: the Bank of Canada, the Bank of England, the Bank of Japan, the European Central Bank, the Board of Governors of the Federal Reserve System, Sveriges Riksbank and the Swiss National Bank. Since publishing [a report in October 2020](#) setting out the common foundational principles and core features of a CBDC, and an [executive summary](#) and three detailed reports on [system design and interoperability](#), [user needs and adoption](#) and [financial stability implications](#) in September 2021, the group has continued to share ideas and perspectives on similar themes published in [2023](#).

² While sharing lessons learned and finding commonalities, the group is not conducting joint experimentation.

³ The discussions focus on a two-tiered model for retail CBDC.

⁴ Offline functionality is being explored as a potential feature and it is not necessarily agreed that it would be desirable in every jurisdiction.

CBDC system and trade-offs should be examined when considering PETs versus more traditional methods to deliver privacy. The system should also be designed in a way to ensure that the implementation of privacy still allows for robust protection of end-users and issuers against fraud and forgery.

- PET may allow extraction of information from encrypted data without revealing personal information and would add an extra layer of protection and design flexibility. However, experimental work conducted by some of the central banks contributing to this report suggests that some of these PETs may not yet be feasible to use in real-time, are complicated, introduce additional latency and raise reliability concerns. However, the field is evolving, and more investigation might be required.
- Most security risks are not unique to CBDC. However, traditional risks may be amplified for CBDC because there may be greater incentives for malicious actors to attack the system. Existing cyber defence practices and frameworks may be applicable to CBDC, but the choice of a two-tier model, which may allow external parties to innovate in the ecosystem in jurisdictions that allow them to do so, can introduce new challenges.
- Quantum computers of the future may have the potential to challenge the integrity of the current ('classical') cryptography methods, albeit over an uncertain period. A path to utilising post-quantum cryptography (PQC), or avoiding the vulnerabilities of classical cryptography, likely needs to be formulated. The question of quantum safety may also apply to conventional payment systems but, being greenfield, central banks, if issuing CBDC, may be well placed to adopt transition strategies to PQC and make relevant trade-offs proactively.
- Security may also be interconnected with the ability to deliver offline services ensuring funds cannot be double spent, minted outside the central bank, or compliance circumvented. There is cautious optimism that a practical solution for offline functionality may be found, though jurisdictions may choose to have additional controls such as holding limits in place to mitigate residual risks.
- Central banks may also consider how to use existing technology and standards in accordance with their strategies for adoption. For example, according to the [proof-of-concept](#) by a central bank, overall modern Point of Sale (PoS) terminals may be ubiquitous and flexible enough to accommodate CBDC, though there may likely still be several technical considerations.

The report is organised as follows. Section 2 shares perspectives on the overall system design of retail CBDC platforms. Section 3 then discusses the system design considerations in more detail, focussing on privacy and privacy enhancing techniques, cyber security, offline CBDC and PoS considerations. Section 4 concludes.

2. Perspectives on the overall system design

The central banks contributing to this report explored, as part of an [earlier report](#), considerations for designing a potential retail CBDC, including an overview of functions in a broad ecosystem, the different roles in a private-public collaboration,

and how an interoperable CBDC system could be implemented.⁵ Central banks are focusing their exploration on the two-tier system (where some roles would be carried out by the public sector and other by private institutions), and within this system there are different architectural design options. As work has progressed and more experience has been gained, discussions around how the division of responsibility between central banks and intermediaries in a centralised versus decentralised model have matured.⁶ In particular, the group focused on the division of data ownership from the authority to update the data.

For the purpose of this report, architectures may be categorized into two approaches: centralised and decentralised. In a centralised model, one entity owns the data and has authority over updates, ie to execute functions. In a decentralised model, data is spread across the system, regardless of controlling entities.⁷ Decentralised models may either take the form of (i) *hub-and-spoke* in which data is owned by multiple entities while authority over updates is in one entity's control; or (ii) *peer-to-peer* in which data ownership and authority over updates are both shared across multiple entities.

Each model may bring opportunities and challenges. While a hub-and-spoke configuration has formed the basis of several proofs-of-concept and pilots for CBDC, it may present challenges of weak resilience if a data store is lost. It may also introduce critical dependencies on the infrastructure operated by a central authority which could result in a single point of failure and if improperly designed, bottlenecks to processing. However, designed suitably, decentralised architectures of this type may be more trustworthy from a privacy perspective by restricting consumers' information to private entities outside the central bank's visibility.

On the other side, delegating authority as in a peer-to-peer configuration might not be suitable for the core settlement of a CBDC system. For example, jurisdictions likely believe that it is inappropriate to delegate authority in a manner that potentially introduces scenarios that runs counter to the central banks' goals. However, the peer-to-peer model may theoretically be appropriate in scenarios where no single entity has end-to-end authority, such as cross-border transfers that span multiple jurisdictions.⁸

A more nuanced assessment of the system design in the context of CBDC may also be considered: centralised versus decentralised options may not have to be two mutually exclusive and incompatible design choices for building a CBDC platform. An optimal design may consist of many different, modular components, each supporting a specific set of requirements. For example, some components may likely

⁵ CBDC Group (2021) available at [CBDC - System design and interoperability \(bis.org\)](#) and [CBDC Group \(2023\) available at Central bank digital currencies: ongoing policy perspectives \(bis.org\)](#).

⁶ The terms centralised and decentralised refer to the allocation of responsibilities to different entities in the CBDC arrangement, for example to perform functions and for data and its storage. Despite these distinct categories, the group agreed that decentralisation should be thought of as a spectrum rather than as binary.

⁷ Distribution means the decomposition of a system into functional blocks that could be operated by one or several entities. Every decentralised system is distributed but the reverse is not necessarily true. While blockchain or DLT platforms are examples of decentralised systems, decentralisation does not necessarily imply their use.

⁸ The appropriateness of the scenario may also likely depend on existing laws, regulations, and policies for data in each jurisdiction.

be better suited to a centralised architecture, such as a core settlement engine that can support high throughput and low-latency transaction processing. Such an arrangement would present a straightforward governance model, with the ownership of data, code, and the authority to update within the purview of a central authority. If properly risk managed, other components may benefit from a decentralised approach, such as those supporting identity and attestations, management of cryptographic keys or reconciliation and auditing of transactions. However, the governance models of such platforms may potentially become more complex.

Against this background, a two-tier system may likely be a mix of centralised and decentralised architectures. Specific design choices will likely be jurisdiction specific and may stem from the nature of trust the public has in certain private and public institutions.

3. In-depth system design considerations

3a. Privacy/privacy enhancing technologies

Supporting privacy may be a key motivation for CBDC issuance. However, this Group has acknowledged that the requirements on privacy must also enable CBDC systems to meet anti-money laundering (AML) and combating the financing of terrorism requirements (CFT) (along with any other regulatory expectations or disclosure laws).⁹

Privacy is a multi-dimensional issue encompassing evolving law, politics, public sentiment, institutional arrangements, and technology. The approach to ensuring privacy would likely require a combination of system design (“privacy by design”) and regulation (“privacy by policy”).¹⁰ Privacy by design may likely include technological (eg the use of cryptography), ecosystem (eg which entity will hold which data and how), and operational (eg what are the safeguards that ensure the safe release of information under judicial warrant) elements. Privacy by policy may require a deliberate and precise formulation of the privacy – and its limits – that is to be designed. It may be informed by law, political and public sentiment, technological possibilities and constraints, trade-offs to create a viable ecosystem, and other considerations. Communicating these considerations to the public and stakeholders will likely be essential. Several considerations and trade-offs may need to be resolved for a final privacy policy and system design (Table 1).

Existing technologies and processes may be used to provide privacy in the CBDC system. However, users would likely need to trust the entities in the CBDC system to protect personally identifiable information (PII). Privacy enhancing technologies (PETs) (eg homomorphic encryption, differential privacy, secure multi-party computation, confidential computing¹¹), along with existing privacy

⁹ See Group of central banks (2020) available at [Central bank digital currencies: foundational principles and core features \(bis.org\)](https://www.bis.org/publ/ncg/ncg03.htm)

¹⁰ See, for example, Mascelli (2023) <https://www.federalreserve.gov/econres/feds/data-privacy-for-digital-asset-systems.htm>

¹¹ *Homomorphic encryption* is a cryptographic technique that allows data to be encrypted and shared while still being usable for computations. *Differential privacy* is a technique that adds a controlled amount of noise or randomness to data to protect privacy. *Secure multi-party computation* is a cryptographic

technologies (eg encryption, access control), may offer ways to enable a high degree of privacy while complying with existing AML/CFT standards and help maintain a balance between privacy and compliance. See Box 1 for an overview of compliance related considerations in the context of the CBDC system architecture and design and Box 2 for an overview on central banks' experiments with PETs.

Experimental work conducted by several central banks suggests that some of the privacy enhancing techniques may not be feasible to use in real-time or are very complicated, introduce additional latency and raise reliability concerns. The field is evolving, and more investigation would be required. Privacy in CBDC is not dependent on PETs or any single PET - more traditional technical and operational methods can be used. However, it is possible that PETs may add an extra layer of protection and design flexibility. An understanding of central banks' risk tolerance may be needed to inform the necessity for PETs. Moreover, the system should also be designed in a way to ensure that the implementation of privacy still allows for robust protection of end-users and issuers against fraud and forgery.

Box 1: Compliance and system architecture and design

Several key aspects of AML/CFT framework that currently apply to financial institutions are likely to impact the architecture design of a CBDC: Know Your Customer (KYC)¹², Record Keeping¹³ and Monitoring and reporting¹⁴.

System architecture and design could be impacted in the following areas:

- Ecosystem Design - In the design of the CBDC system, particularly a two-tiered system, clear delineations of roles and responsibilities would need to be established to govern various aspects of its operation, including compliance. This would ensure accountability and effective coordination among stakeholders within the ecosystem, ultimately impacting the efficacy of AML/CFT measures.
- Data collection and management - A CBDC system may likely be required to collect and maintain accurate, up-to-date, and relevant data throughout the customer lifecycle to support AML/CFT compliance.
- User onboarding - If appropriate for meeting a jurisdiction's policy goals, a CBDC system may encompass several onboarding processes tailored to meet diverse user needs and business objectives. A series of technical design considerations may be considered for optimizing the efficiency and effectiveness of these onboarding services, while ensuring compliance with KYC

technique that allows multiple parties to jointly perform computations on their private data. (See Table 1 in [III. Blueprint for the future monetary system: improving the old, enabling the new \(bis.org\)](#))

¹² Generally, KYC procedures are a fundamental component of AML/CFT law. Typically under AML/ATF law, financial institutions and other regulated entities verify the identities of their customers and keep a record of the relevant information.

¹³ Generally, under AML/CFT law, covered entities keep comprehensive records that must be readily available to the appropriate authorities in authorized circumstances, such as for investigative purposes and regulatory oversight. Covered entities must maintain these records for a minimum period (eg five years).

¹⁴ Generally, under AML/CFT, the covered entities establish a regime to monitor transactions and report certain transactions, such as suspicious transactions or transactions that surpass a certain threshold, to the appropriate authority.

regulations. These include rule-based¹⁵ and principle-based compliance¹⁶, two approaches used in regulatory frameworks to guide behaviour and ensure adherence to laws, regulations, and industry standards.

- **Reporting & Investigations** – A CBDC system would likely need to provide the ability to report suspicious transactions to regulatory authorities and aid law-enforcement authorities in investigations related to financial crimes.

Box 2: Experimental work on PETs by central banks

Bank of Canada has tested a *Secure Multi-Party Computation* (SMPC) protocol. SMPC is a cryptographic protocol that distributes a computation process across multiple parties, where no single party can view the data of others. This can provide a high level of privacy where no single party in the CBDC ecosystem has the visibility to the private data of end users (eg, account balance, transaction history). The challenge with SMPC lies in its complexity and insufficiently developed and tested code, requiring specialist competence.

Riksbank has investigated *Zero Knowledge Proofs* (ZKP). ZKP provides technical solutions that allow information to be kept anonymously, but trusted parties can verify that the information is correct. This technology is based on advanced mathematical algorithms and relies on cryptography. ZKP is computationally demanding, very complex and requires specialist competence to implement and maintain.

Some of the BISIH retail CBDC experiments explored how to embed privacy elements in a retail CBDC arrangement. One example is [Project Tourbillon](#), which explored privacy, security, and scalability for rCBDC. The project (i) demonstrated cash-like anonymity for retail CBDC and, (ii) proved that implementing quantum-safe cryptography is possible, but requires specialised expertise, and severely limits transaction processing. [Project Hertha](#) is exploring how network analytics could help identify financial crime patterns while preserving user privacy within a real-time payment system. Project [Aurum](#) is studying the privacy of payments in retail CBDCs, leveraging expertise from academia and privacy regulators.

3b. Cyber security

A CBDC system would need to be resilient to technical failure and cyber risks.¹⁷ Cyber security threats may span across several dimensions, eg offline payments, blockchain/smart contract security, data privacy, ecosystem complexity, machine-to-machine payments, quantum computing, etc.

Central banks' existing cyber defence practices are wholly applicable to CBDC. Most threats are not unique to CBDC, and span eg data breaches and denial of service. Cyber defence practices in existing payment systems range from using risk-management frameworks to understand threats, developing policies, building partnerships and governance, and running effective operations. Cyber security for CBDC would likely build on these practices and extend as appropriate. See Table 1 for an overview of considerations and trade-offs that would need to be resolved.

¹⁵ Rule-based compliance, also known as prescriptive or specific compliance, relies on a set of explicit, detailed rules, guidelines, and regulations that dictate specific behaviours and actions that must be followed.

¹⁶ Principle-based compliance, also known as outcome-based compliance, focuses on overarching objectives that guide behaviour and decision-making without describing specific processes or procedures.

¹⁷ See Group of central banks (2020) available at [Central bank digital currencies: foundational principles and core features \(bis.org\)](https://www.bis.org/cbdc/foundational-principles-and-core-features)

While not unique to CBDC, the division of responsibilities between entities in a CBDC ecosystem requires interfaces at their boundaries that may create vulnerabilities - an incident at one entity may have negative effects on the wider system. This may be mitigated through close cooperation of the ecosystem during design and operations, where effective governance will be important.

Another security issue relates to double spending.¹⁸ While this risk is present in non-CBDC systems, a CBDC ecosystem will likely have multiple actors and thus presents a larger attack surface. The issue may be effectively dealt with by the application of a risk framework to understand the threat, and to consider the various system design options, and how well these could identify and mitigate double spending. The group's preliminary analysis of some design options concluded that an actor would need to take over a system to execute double spending and the preferred design options differ based on the type of attack. Having settlement occur in the system operated solely by the central bank may eliminate or minimise the risk of double spending. If the settlement occurs outside the central ledger for an offline CBDC, this may present a double spending risk that would need to be solved and this is an area for further work (See section 3c).

Looking forward, quantum computers could have the potential to break current ('classical') cryptography methods. A path to mitigating these new vulnerabilities would need to be formulated. A new generation of post-quantum cryptography (PQC) is emerging, and all central bank systems, including potential CBDC, would eventually need to use them. However, this is not a simple swap from old to new. Some – but not all – PQC constructs are highly computationally demanding, as the group has found in their respective experimental work (see Box 3).

Since CBDC is greenfield, PQCs are maturing, and transition strategies are being developed early, central banks would be able to chart a course to post-quantum safety and address the relevant trade-offs. Some PQC algorithms incur minimal overhead, indicating that a set of algorithms could be practically used in CBDC. Using a combination of pre- and post-quantum cryptography could maximise cryptographic agility, allowing legacy and new systems to coexist. Some PQC algorithms are feasible on smartphones. However, they may still be too demanding for low-power chips found on internet-of-things devices and cards.

¹⁸ Double spending is the ability of a malicious actor to spend the same funds in two different transactions. At scale this can lead to, effectively, an inflation of the currency and serious reputational damage undermining confidence of the system.

Box 3: Post-quantum cryptography experiments

[Project Tourbillon](#) of the BSIH Swiss Centre explored privacy, security and scalability for CBDCs. The project introduced PQC into a CBDC solution. Measuring the results between the classical and PQC based systems showed dramatically lower performance with PQC, including an unacceptably slow user experience. The project also found that the change from classical cryptography to PQC is not a simple substitution of cryptographic constructs and this transition effort will require relevant expertise.

Bank of Canada has experimented with PQC and a transition strategy, assuming it is likely that quantum computers become practical during the lifetime of a CBDC system. A real-world scenario of an operational CBDC ecosystem with entities and components of differing capabilities exchanging information was assumed. The work paid specific attention to channel security and digital signatures, which are the core cryptographic elements under threat, and will be required in any CBDC solution, regardless of the system architecture. These elements form the backbone of the Secure Software Layer (SSL) standard and library, which currently underpins secure communications between devices, commonly seen by consumers in connecting to banking and shopping applications. To assess the impact of upgrading classical cryptographic algorithms to PQC variants in an operational context, the project developed a quantum safe version of a secure channel library, titled OpenSSL, for communications between desktops, servers, smartphones, PoS terminals and smartcards. Experimental work tested and measured the performance of a hybrid approach with classical and quantum-safe key exchange mechanisms and signature configurations.

3c. Offline CBDC

For the purposes of this report, offline CBDC is defined as (i) a CBDC that can be exchanged even in the absence of a network connection, and (ii) a CBDC arrangement in which a transaction can be established without a third party acting as an arbitrator.¹⁹ Based on this definition, two operating modes would be possible: immediate, where there is immediate settlement between devices in a transaction; and deferred, where the settlement takes place after a device connects to the network.

Security is a fundamental consideration when it comes to offline CBDC. Central banks need to ensure that funds cannot be double spent, minted outside the central bank, and that compliance cannot be circumvented. There is cautious optimism that a practical solution can be found, though jurisdictions may choose to have additional controls such as holding limits in place to mitigate residual risks. New security technologies are emerging that may help, but the timelines for their maturity and availability are difficult to predict.

Alongside careful system design, limits on holdings, numbers of forward transactions and duration of funds kept offline may mitigate residual risks. Limits may also be relevant for non-security risks. For example, if a non-zero interest rate would be paid on CBDC, it may be difficult to implement for offline CBDC.

Despite progress achieved by several central banks in this space,²⁰ more aspects would need to be considered, eg understanding risks related to the illicit usage of

¹⁹ Abrazhevich (2004)

²⁰ For example, Bank of England tested four commercial solutions for offline CBDC. Riksbank has incorporated offline into the overall e-krona project. Bank of Japan has reviewed multiple past and present offline solutions. [Bank of Canada](#) has focused on secure hardware and certification and co-invented the Physical

offline CBDC. See Table 1 for an overview of offline considerations and trade-offs that will need to be resolved.

3d. CBDC point of sale considerations

Central banks may want to consider how to use existing technology and standards in accordance with their strategies for adoption at the point of sale (PoS). Enabling CBDC to work at the PoS may be an important requirement for CBDC since consumers may want to be able to spend their CBDC to purchase goods and services in store. Merchants may not want to acquire new hardware to accept CBDC, which may limit adoption and CBDC acceptance. Therefore, exploring compatibility with existing PoS terminals may be worthwhile.

How existing terminals are used is likely jurisdiction dependent. Broadly, PoS terminals may use EMVCo protocols²¹ to enable contactless transactions for funds to be transferred from the consumer's account to the merchant's account. PoS terminals typically contain software, the contactless kernel, which provides functions and processes that implement the business logic of a contactless transaction.

Several technical design questions for how CBDC could work with existing PoS systems may be explored. Central banks may need to consider the contactless kernel that should be used to perform the transaction at the merchant terminals, the transaction flow (such as push, pull, or peer-to-peer), the customer verification method (such as online PIN or Face ID), and how consumer wallet balances are updated (value actually transferred at PoS or authorised instruction sent to ledger to update the balance).

Modern PoS terminals may be ubiquitous and are flexible enough to accommodate CBDC. [Proof of concept work](#) by the Bank of England demonstrated that existing PoS terminals could, in principle, be used to initiate CBDC payments and do not appear to require modification in order to do so.

Unclonable Function (PUF) Cash offline protocol. The BISIH, through [Project Polaris](#), has developed a high-level design guide for offline payments.

²¹ EMV originally stood for Europay, Mastercard and Visa, the three companies that created the standard. The standard is now managed by EMVCo, a consortium with control split equally among Visa, Mastercard, JCB, American Express, UnionPay and Discover.

Element	Considerations and trade-offs
Privacy	
Laws, norms, and trust in institutions	These elements may vary in different jurisdictions. Therefore, the details of solutions will likely need to be tailored to local situations and needs even though the set of design options is common.
PETs	PETs are complex and differ in terms of their degree of privacy protection, computational burden and ease of implementation. For example, using computationally demanding PETs may increase transaction times and degrade the user experience.
Intermediaries	In jurisdictions that may choose to allow the behaviour, intermediaries may be incentivised to participate by being able to monetise users' information, such as the case in existing payment solutions. ² Balancing the incentivisation of a viable ecosystem with the need for privacy would need to be considered. While a two-tier model of private sector intermediaries is generally preferred, there may be reasons and benefits for a jurisdiction to have a public sector intermediary (not necessarily the central bank). In this arrangement a public intermediary may need to be held to a different data privacy standard than a private intermediary.
Cost	Minimising data held at the central bank may raise the maintenance cost on intermediaries, potentially reducing their incentive to participate.
Financial inclusion	For jurisdictions whose policy goals include being inclusive for people without sufficient identity for Know Your Customer (KYC), one potential solution may be to offer a non-registered CBDC. This may likely be constrained with holding and or transaction limits to reduce AML risks. Another consideration is the type of device (eg if mobile phones would be required this may exclude some parts of the population (young kids, elderly)).
Offline	One potential aspect of extended offline CBDC – where users can transfer funds offline for longer time periods (such as weeks or months) – is that these transactions are inherently not visible and therefore may not be traceable for compliance purposes. As with non-registered CBDC, limits to manage AML risk may need to be imposed.
Users	Allowing each user to determine the degree of privacy they would like – perhaps for benefits such as rewards by intermediaries – may be desirable in some jurisdictions. However, different levels of privacy may lead to engineering complexity, disputes with users who may claim they did not consent to reduced privacy, and the reduction of the value of privacy as a public good (which requires all users to retain privacy).
Cyber security	
Two-tier model	The two-tier model may create vulnerabilities, and central banks may have to strike a balance between imposing constraints for safety, while ensuring that intermediaries have the space to create value for themselves as well as their clients.
Standards	While the general assumption is that the standards for cyber security are expected to be extremely high, a more precise articulation by policy makers and risk managers would be required to make policy and system design choices. ³
Intermediaries	The contractual and oversight relationships with intermediaries, and technical controls placed on them to ensure security, may need to be coherent and balanced (trade-offs could arise between technical controls and oversight).
Quantum threat	The question of quantum safety is broader than CBDC, concerning the financial system at large. Risk and cyber security groups in many central banks are developing strategies for a post-quantum world, and some financial entities are collaborating with standard setting bodies. The investigation of the quantum threat by members in the context of CBDC would be applicable to other systems.
Offline	

Utility / security	A key choice around managing risk may be whether funds will be settled offline and will be available for immediate forward use, or settled only when one of the parties eventually goes online.
Operational aspects	For example, updating devices in the field (older devices become vulnerable over time). The option of adding offline functionality separate to the main system may be considered.
Rules	Due to the possibility of loss of funds (from losing a device), rules around who bears the loss may have to be made clear.
Use cases	As demand for offline CBDC is unclear, it is difficult to solve for all possible use cases. As such, each jurisdiction may have to prioritize specific use cases for offline CBDC.
Point of Sale	
Compatibility with existing system	Design aspects that should be considered may include the contactless kernel (software which provides functions and processes that implement the business logic of a contactless transaction) to be used, transaction flow (such as push, pull, or peer-to-peer), the customer verification method (eg online PIN or Face ID), and the method to update wallet balances.

¹ This is a non-exhaustive list. ² This trade-off should not be read to imply that central banks are considering letting the private sector monetize CBDC transactions. It is merely illustrative. ³ Some work is already underway. See for example [CBDC information security and operational risks to central banks](#).

4. Concluding thoughts

As many central banks continue to explore and investigate retail CBDC, the range of issues that need to be considered cannot be tackled in isolation. Given the scale of interconnectedness, both within and beyond the system, central banks may likely need to draw on expertise from both across their institutions, as well as from the private sector, to ensure a holistic approach. Reflecting this, the Group of central banks and BIS have worked closely across different topics, for example sharing insights on legal aspects of retail CBDC relevant to system design considerations²².

Many of these issues are not unique or new for retail CBDC and, where possible, central banks may wish to consider utilising existing technology, standards and practices. At the same time, central banks may choose to explore new technologies and strategies in CBDC design (for example utilising post-quantum cryptography that might be needed to address challenges in the system), although some of the emerging technology, such as PETs, may not yet be feasible to use.

²² See Group of central banks (2024), Legal aspects of retail CBDCs.

Annex: Expert group members

Chair	Aino Bunge (Sveriges Riksbank)
	Paul Chilcott (Bank of Canada)
Bank of Canada	Roger Hatch
	Scott Hendry
	Dinesh Shah
European Central Bank	Holger Thiemann
	Heike Winter
Bank of Japan	Tomohiro Usui
	Daisuke Terayama
Sveriges Riksbank	Veljko Andrijasevic
	Johan Schmalholz
Swiss National Bank	Philipp Haene
	Severin Bernhard
Bank of England	William Lovell
	Danny Russell
Board of Governors of the Federal Reserve System	Jesse Maniff
Bank for International Settlements	William Zhang

The work has also benefited from the contributions provided by Jeremy Brotherton, Christopher Desch, Eric Thompson (Federal Reserve System), Ram Darbha, Rakesh Arora, and Cyrus Minwalla (Bank of Canada). Thanks also go to Codruta Boar (Bank for International Settlements) and Marianne Schneider-Petsinger and Lizzie Peck (Bank of England) for secretariat assistance.