


► 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)

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/ncg030.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 \(bis.org\)](#)

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 Tourbillion](#) of the BISIH 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.

Considerations and trade-offs¹

Table 1

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.

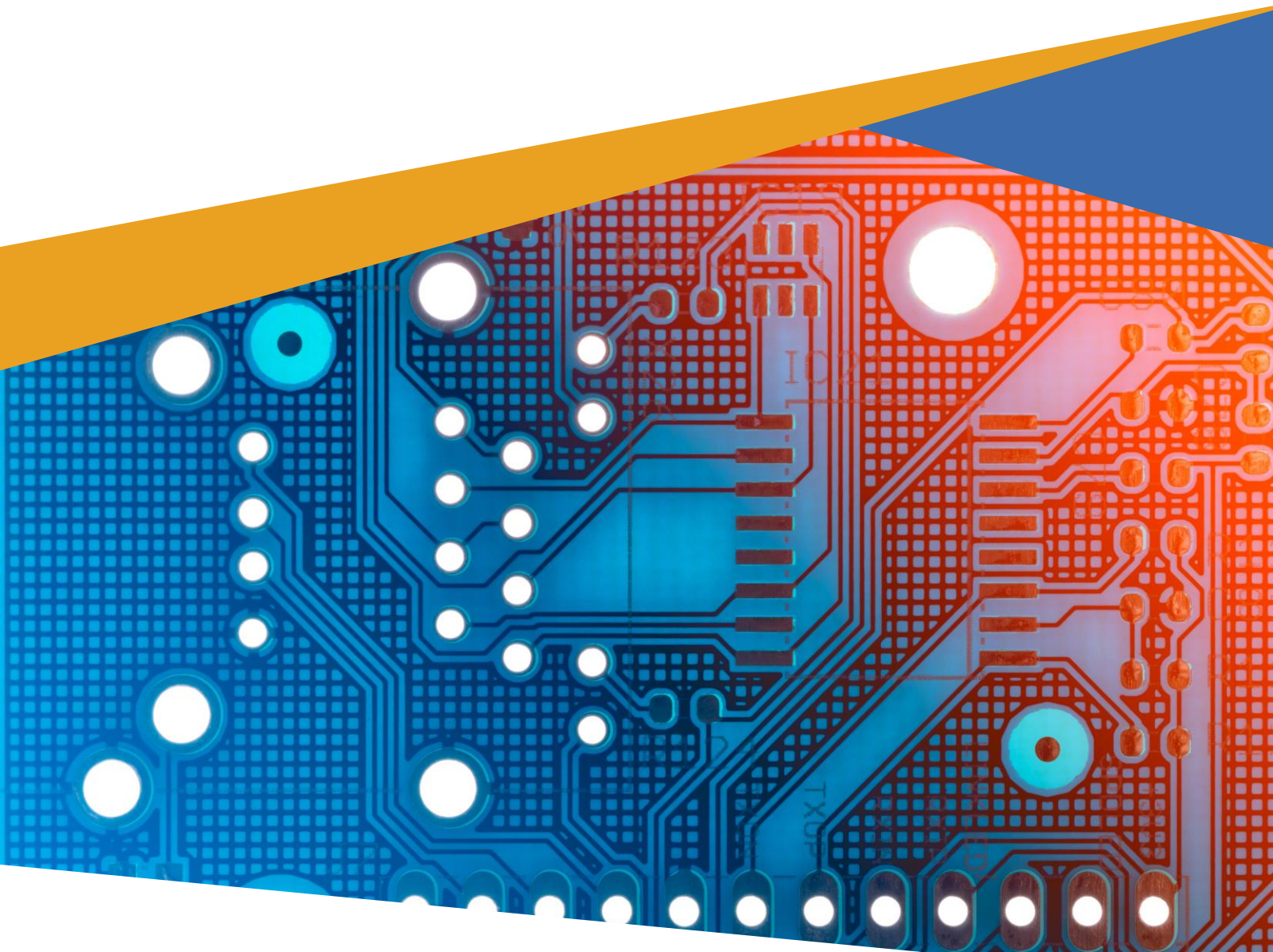
Many of these issues are not unique or new for retail CBDC and, where possible, central banks may wish to consider utilising existing technology, standards and practices. At the same time, central banks may choose to explore new technologies and strategies in CBDC design (for example utilising post-quantum 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.




► Central bank digital currencies:

Legal aspects of retail CBDCs

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 978-92-9259-805-1 (online)

Executive summary

This paper examines some key legal questions that may need to be addressed by any jurisdiction considering issuing a retail CBDC (“rCBDC”) but does not attempt to provide definitive answers to those questions. It focuses on four areas: the legal classification of rCBDC; the obligations and liabilities of participants in the rCBDC ecosystem; privacy and financial crime; and cross-border issues.

- The legal frameworks governing money, payments and central banking were not drafted with digital central bank money for the public in mind. Jurisdictions may need to consider creating a new legal object/asset for rCBDC with a bespoke monetary and private law framework to accommodate it.
- The rights, obligations and potential liabilities of stakeholders within the rCBDC ecosystem will need to be clearly addressed in the legal framework. Pursuant to policy goals, each risk that could arise in the system might be clearly and unambiguously allocated through that framework to the party that is most appropriate to bear it or best able to mitigate it.
- The legal framework will likely need to draw an appropriate balance between the need to protect the privacy of users, and the need to guard against the criminal misuse of the financial system. While the protection of privacy is an important policy objective, the efforts of the authorities to combat money laundering and terrorist financing may require access to and the sharing of personal data with certain parties. In balancing privacy protection and AML/CFT enforcement in the legal framework for rCBDC, policy makers could draw on the rules that apply in the conventional banking system.
- Policy makers may need to decide whether to allow for access to their rCBDC system by non-resident/non-domiciled end-users or intermediaries. If non-resident access is permitted, rules might need to be developed to determine which jurisdiction’s law will apply to disputes as standard conflicts of laws rules may not function well for digital assets. Relevant jurisdictions may wish to consider establishing a bilateral or multilateral framework for determining the applicable law.
- CBDC systems that facilitate the cross-border exchange of CBDCs may be categorised as: (i) compatible CBDC systems, (ii) interlinked CBDC systems, and (iii) a single system. Each model poses separate legal challenges.

A jurisdiction considering issuing rCBDC might need to decide on the appropriate legislative, regulatory and contractual rules for its rCBDC, having regard to its own legal framework, and its CBDC design and policy aims.

Considerable legal work might be needed in each jurisdiction to identify and address the range of legal issues.

Introduction

1. This paper examines some key legal questions that may need to be addressed by any jurisdiction considering issuing a retail CBDC (“rCBDC”).
2. It does not attempt to provide definitive answers to those questions. It recognises that the answers will depend on, among other things: the legal traditions and legal system of the relevant jurisdiction; the degree of central bank independence in the jurisdiction; the design of the rCBDC; and the legal classification of the rCBDC in the relevant jurisdiction.
3. The paper does not recommend any particular policy or design choices^{1,2} but adopts the following design assumptions to guide the legal discussion:
 - 3.1. The rCBDC system is two-tier,³ and available to retail users.
 - 3.2. The central bank issues the rCBDC and oversees the rCBDC system.
 - 3.3. The central bank ledger has data related to end-user holdings but does not hold data that would enable the central bank to identify end-users. Information on the identity of end-users is held elsewhere in the system.
 - 3.4. The central bank is not the anti-money laundering authority.
 - 3.5. Private sector firms may be involved in building the rCBDC system and in writing the code.
 - 3.6. Banks and fintech firms provide wallet-related services for customers built on software provided by third party software developers.
 - 3.7. Intermediaries do not hold an end-user’s rCBDC on their balance sheets.
4. The paper begins by examining the legal classification of rCBDC, and the treatment of an rCBDC in private law. The paper then considers the legal relationships between parties within the rCBDC system and the risks within the system that could give rise to obligations or liabilities for such parties. The paper subsequently discusses the manner in which the legal framework may need to draw a balance between the protection of the privacy of end-users while also guarding against the criminal misuse of rCBDC. In the final section the paper considers the use of rCBDC across international borders.

¹ Some CBDC discussions have drawn a distinction between “account-based” and “token-based” CBDC system designs. However, these terms are not used consistently across different fields and are avoided here. See further [CBDC - System design and interoperability BIS, September 2021 at Box 1](#).

² Legal issues relating to the offline provision of rCBDC are out of scope. The many different definitions of “offline” CBDC (See the BSIH Project Polaris *Handbook for Offline Payments with CBDC* at 3.2) would each raise different legal issues.

³ For the purposes of this paper, in a two-tier rCBDC system, the ledger is maintained by the central bank (or the central bank oversees an operator for this purpose) while client-facing services are provided by various types of service providers, such as banks.

Legal nature of CBDC

5. A fundamental question underlying the legal framework is the legal nature of the rCBDC.
From a legal perspective, what is it? Is it a form of money and if so, what kind of money?

CBDCs as money

6. Whether something is “money” or not determines, to some degree, how it will be treated within a legal system.⁴ For this reason, it may be important to ensure that rCBDC’s status as a form of money (or not) is clear.
7. Economists generally agree that, for something to be money, it must fulfil three functions: it must act as a unit of account, a store of value, and a medium of exchange. Money, which represents a *store of value*, may be distinguished from a payment instrument such as a credit card or cheque that is used to *transfer value*. However, the concepts of money and payment instruments are not mutually exclusive. While some forms of money such as banknotes and coins may also be considered to be a payment instrument, some other payment instruments are not considered to be a form of money. For example, cheques, money orders, or debit and credit cards are payment instruments but are not generally considered to be money.⁵
8. While the economic definition is relatively settled, the legal definition of money remains unclear. A jurisdiction’s legal system may have several different definitions of “money” that are used for different purposes. In any event, a discussion of a legal definition of money needs to be premised on an understanding of several key legal concepts including currency, and legal tender.⁶
9. Currency is a form of money. It refers to the unit of account and medium of exchange denominated by reference to that unit of account prescribed by law. Currency is typically issued by the State (ie the central bank) and is thought to be negotiable and passes without any adverse legal or equitable interest. This characteristic of currency may be considered an exception to the general rule that a person who does not have adequate ownership of goods or property cannot transfer good ownership to someone else.⁷ A payee who in good faith receives currency as a means of payment is usually protected against a claim from a fraudulently-deprived owner.⁸ Such exceptions are designed to foster the rapid turnover of assets without the need for the recipient to check the legal title.

⁴ For example, the laws concerning sale of goods, negligence claims involving economic loss vs physical loss, or criminal laws relating to fraud and theft may all apply differently if money is involved.

⁵ Banque de France, “Payments and market infrastructures in the digital era”, 2018, p. 18.

⁶ Other relevant concepts include convertibility and seigniorage.

⁷ This is often known as the *nemo dat* rule, from the Latin *nemo dat quod non habet* “no one can give what they do not have”.

⁸ The exception may also apply in other situations, for example the good faith acquisition of securities.

10. In many jurisdictions, the law restricts the legal concept of currency to state-issued banknotes and coins.⁹ As such, the legal concept of currency is typically narrower than the concept of money. As a legal matter, banknotes and coins are a form of money but not all forms of money are a form of currency. For example, a demand deposit (which is convertible into currency) is, in many jurisdictions, considered to be a form of money but not a form of currency.
11. Legal tender status is closely related to the concepts of money and currency. The legal implications of a form of money being granted legal tender status vary from jurisdiction to jurisdiction. Legal tender is generally considered to be anything recognised by law as a means to settle debts or meet financial obligations.¹⁰ In some jurisdictions, legal tender is merely the “default” means of payment, meaning that a tender of currency has the effect of discharging a debt to a creditor without the need for the parties to agree to that form of settlement.¹¹ In other jurisdictions, acceptance of legal tender in payment for the discharge of a debt is mandatory. While a means of payment may only be granted legal tender status if it is a form of money, not all forms of money are granted legal tender status.¹² In most jurisdictions, only state-issued currency in the form of banknotes and coins is given legal tender status.
12. Publicly-issued currency acts as the monetary anchor for an economy. It “anchors” privately issued money through which holders of private money can convert that money into public money at par value.¹³
13. rCBDC would constitute a new form of public money.¹⁴ Moreover, designating rCBDC as both currency and as legal tender¹⁵ may assist with strengthening its monetary anchor function.

What kind of money is CBDC?

14. While rCBDC would be considered to be a form of money, the question then arises, what kind of money is it? Could it be considered to fall within an existing monetary asset class, or would it be something entirely new? Common monetary asset classes such as cash, deposits and e-money all benefit from well-defined legal rules that govern their use. Classifying rCBDC as part of an existing asset class would mean it would be subject to the legal rules that apply to that class including, for example, whether it is a form of currency and has legal tender status, whether the central bank has a mandate to issue it, and how the asset is

⁹ Bossu, W, et al “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations” WP/20/254, *IMF Working Paper* November 2020.

¹⁰ Lastra, R *Monetary Law*, chapter 1.

¹¹ In these jurisdictions, private businesses are not required to accept legal tender as payment.

¹² Geva and Geva “Non-State community currencies” in D Fox and S Green (eds) *Cryptocurrencies in Public and Private Law* OUP, 2019 at 11:09.

¹³ See Zellweger-Gutknecht, C, “CBDC and Monetary Sovereignty” in ECB (ed.) *Treading Softly: How central banks are addressing current global challenges*, ECB Legal Conference 2023, December 2023, p.,165.

¹⁴ Commenters have pointed out that CBDC holding limits could impact its monetary anchor function. See eg Niepelt, D, “A Macroeconomic Perspective on Retail CBDC and the Digital Euro,” EIZ, 2023 In Christos V. Gortsos and Rolf Sethe, editors: *Central Bank Digital Currencies*, EIZ Publishing, ch. 3, Zurich, October 2023.

¹⁵ Jurisdictions where acceptance of legal tender is mandatory may need to consider whether any technological requirements may constitute barriers to persons’ ability to receive rCBDC and thus whether legal tender status is appropriate for rCBDC.

transferred between holders. The following section examines the legal characteristics of each of these monetary asset classes and discusses to what degree an rCBDC might fit into each.¹⁶ The section then also considers the pros and cons of an alternative approach of creating a new monetary asset class for rCBDC subject to a bespoke legal regime.

CBDC as cash

15. rCBDC is sometimes compared to cash, that is, banknotes and coins, or is said to be “cash-like”. Cash is, in most jurisdictions, easily exchangeable for goods and services and is widely accepted. It is a form of currency and is legal tender. It is the only central bank money available to the public. It can be used anonymously without transactions being traceable and does not require a contractual relationship between a central bank or any intermediary or its users. Legally, payment using cash is effected by the transfer of possession of the banknote or coin from the payer to the payee. Cash offers a theoretically unlimited store of value¹⁷ and allows peer-to-peer transactions without the need for any infrastructure or third-party involvement.¹⁸
16. Some of cash’s characteristics may also be relevant for an rCBDC. It could be classified as legal tender and would constitute a form of central bank money available to the public. In some CBDC system designs, peer to peer (P2P) payments may be possible via a mobile app or similar means and could even be anonymous, for example, in an offline scenario.
17. On the other hand, an rCBDC differs from cash in important ways, not least in its intangibility. Regardless of the intentions of policy makers, a digital asset could never be a perfect replica of a physical asset. An rCBDC would rely on a dedicated technical system to be transferred. Potential design choices such as holding limits, programmability, the payment of interest or a possible contractual relationship between the issuing central bank and the user could widen the differences. Accordingly, there may be challenges in treating an rCBDC as the legal equivalent of cash or in subjecting it to the entire system of rules that apply to cash in most jurisdictions. At most, it may be that only some such rules could be made to apply.

CBDC as a deposit

18. The second main form of money circulating in a jurisdiction is commercial bank money in the form of deposits. Deposits are rarely considered to be “currency”. They are unlikely to be legal tender.
19. A person with a credit balance on a deposit account with a commercial bank has a claim on that bank and the bank has a liability to the depositor.¹⁹ The credit balance represents a debt owed by the bank to the depositor and arises in the

¹⁶ Securities are not typically considered to be a means of payment and may not be “money”. However, jurisdictions may separately need to consider whether an rCBDC could or should be a security under securities legislation.

¹⁷ Cash’s function as a store of value is limited only by physical storage constraints.

¹⁸ The issuance and distribution of cash does require an extensive network of financial institution intermediaries.

¹⁹ Another form of deposit is that held by financial institutions with their central bank. These accounts are a form of public money but function in a similar way to commercial bank deposits.

context of a contractual relationship between the bank and the depositor. The depositor is, in substance, lending funds to the bank, usually in return for interest on the debt.²⁰ The bank does not store or safeguard units of currency for the depositor and the depositor has no claim for the return of any specific units. Rather, the depositor's claim consists of the right to payment of the credit balance in central bank money (cash).²¹

20. The transfer of money in the form of bank deposits operates according to a bespoke regime.²² The legal effect of payments from a deposit account is the destruction, or alternatively, the discharge, of (part of) the original claim held by the depositor and the creation of a new claim held by the payee.²³ There is no assignment of the original claim from the depositor to the payee and no transfer of property, tangible or intangible.
21. rCBDC may be expected to share certain core features with deposit accounts. Central banks would create a liability on their balance sheet by issuing rCBDC. The holder of rCBDC could be understood as having a claim on the central bank for payment of the value of their rCBDC holdings, much like the debtor/creditor relationship that exists between a depositor and commercial bank.
22. However, there are also areas where the rCBDC and deposit models may differ. Central banks may book rCBDC as a liability for accounting purposes, but characterising the relationship between the rCBDC holder and the central bank as one involving a debt claim may be difficult. If the central bank owes a debt to the holders of rCBDC, what would a payment of that debt require of the central bank? Is it the replacement of the rCBDC with other central bank money of equivalent value? Or for payment in banknotes or coins? If so, would this presuppose that cash must continue to exist alongside rCBDC?
23. For these reasons, rCBDCs, depending on their design, are not necessarily a comfortable fit in the "deposit" class. If a legal characterisation of CBDC as a deposit with the central bank is desirable in a particular jurisdiction, amendments to, at a minimum, the definition of currency and of legal tender (if CBDC is to be legal tender) may be required.

²⁰ Deposits are also created by the bank making a loan to a customer while simultaneously creating a matching deposit in the borrower's bank account. See McLeay, M, A Radia and R Thomas, "Money creation in the modern economy", Quarterly Bulletin 2014 Q1.

²¹ In many jurisdictions, the government insures certain types and amounts of commercial bank deposits in the event of bank failure.

²² The transfer of other types of personal claims typically requires assignment of the claim.

²³ On receiving a payment instruction from the depositor, the bank removes (destroys) credit from the depositor's account and, where the payee account is also held at the same bank, adds (creates) credit in the account belonging to the third party. If the payee account is with another institution, the bank instructs that institution to credit the account and compensates it for doing so by making a payment from its central bank reserve account to the reserve account of the other institution. See Fox, D, *Property Rights in Money*, OUP, 2008, at 5.23.

CBDC as electronic/e-money

24. Electronic money or “e-money” has been introduced in a number of jurisdictions in recent years. E-money is generally treated differently from deposits and cash. In some jurisdictions consideration has been given to issuing rCBDC as e-money.²⁴
25. It is difficult to describe the key legal features of e-money with complete certainty, since there is no universal definition of the term and the understanding of what e-money is may differ from country to country. However, e-money is often understood as electronically stored monetary value that represents a claim on the issuer. E-money can be issued by banks, as well as by non-deposit-taking providers, such as e-money institutions, and it is usually not granted legal tender status.²⁵
26. A key difficulty with characterising rCBDC as e-money is that e-money is issued on receipt of funds for the purpose of making payment transactions, that is, it is pre-paid and is understood largely as a payments instrument. Its utility as a store of value is limited, Customers buy e-money using cash or commercial bank money, It is primarily issued by private actors as opposed to public sector entities like central banks.²⁶
27. E-money is a “new” asset class, benefiting from relatively recent legislative consideration and clearly defined rules.²⁷ This may mean it would be easier to adapt relevant e-money legislation to allow for the usage of rCBDC as a payment instrument, should rCBDC be classified as e-money. But the key characteristics of e-money discussed above differ from those envisaged for rCBDC in many jurisdictions. Accordingly, policy makers would have to consider whether it would be appropriate to conflate the two concepts.

Should CBDC slot into an existing asset class?

28. All the above asset classes could be potential options for the legal classification of an rCBDC. There could be both legal and policy reasons for using an existing asset class, possibly with modifications. It could make rCBDC easier to comprehend both for the public and lawyers and would mean that rCBDC, at least to some extent, would benefit from an existing private law structure. The rules on, for example, ownership interests and transfer mechanisms for rCBDC would follow the clearly defined frameworks that have been developed for the asset class to which rCBDC is assigned. Further, there might be monetary law advantages if an

²⁴ The Bahamas has issued rCBDC as e-money, with the Central Bank Act 2020 (Bahamas) authorising the central bank to issue electronic money as defined in the Payments Systems Act 2012 (Bahamas). The Bahamian Dollar Digital Currency Regulations 2021 (Bahamas) provide that the Bahamian Dollar Digital Currency is an electronic version of the Bahamian Dollar issued by the Central Bank pursuant to the authority conferred upon it by the Central Bank Act.

²⁵ Compare with CPMI's *A glossary of terms used in payments and settlement systems*; CPMI, *Digital Currencies (2015)*; [CPMI, Payment aspects of financial inclusion, 2016](#) (p. 14), and the European Commission's proposed Payment Services Directive 3 (PSD3).

²⁶ For example, the European Commission's PSD3 proposal draws a distinction between central bank money issued for retail use and e-money.

²⁷ Albeit these rules are primarily focused on financial market regulation, rather than on questions of monetary law and private law.

rCBDC were classified as cash, as a central bank's mandate to issue rCBDC and its legal tender status may follow automatically.

29. There may also be downsides to using an existing asset class. rCBDC may not slot easily into existing legal structures developed for assets that differ from rCBDC in important ways. This could lead to unintended consequences. If an existing asset class were used, it would likely need legislative modification to ensure that it functions effectively for rCBDC.
30. Should none of the monetary asset classes (even if modified) that currently exist in a jurisdiction be considered suitable for rCBDC, a new legal object/asset may need to be created. If this route were taken, there would be a new form of money and payment instrument in the jurisdiction and new legal rules would need to be created. Creating a new asset class would allow policymakers the freedom to design an rCBDC without the need to take account of restrictions that apply in respect of existing assets. Questions such as the desirability of holding and transaction limits, remuneration, legal tender status and whether rCBDC can be used as a monetary policy instrument could be considered afresh.
31. This approach would require more extensive new legislation to establish the legal framework for the new asset, as well as the review and amendment of the corpus of existing legislation. The need for the development of new case law could cause uncertainty, which may potentially impact the public uptake of the rCBDC.
32. Legislators and policymakers in each jurisdiction may need to consider which approach makes the most sense in their particular context.

CBDCs in private law

33. Regardless of which monetary asset class an rCBDC is assigned to, jurisdictions will need to consider the rCBDC's treatment in private law. The nature of the legal interest that an individual holds in units of rCBDC, as well as issues such as how rCBDC can be disposed of, are difficult questions. They may need careful consideration by policy makers in the design of the legal framework for the rCBDC.
34. The legal framework for an rCBDC system would consist of rules found in many different sources, including legislation, regulation and possibly a "rulebook" governing the system's operation. The CBDC system rulebook could take the form of the contractual terms and conditions governing the relationship between the central bank as issuer of CBDC, and the intermediaries who provide end-users with access to the system. In this model, certain terms from the central bank/intermediary contract may also need to be reflected in the contracts that are concluded between intermediaries and end-users to ensure the system functions as intended. Other models could include rulebooks with the status of regulation, applying to all participants in the system.²⁸

²⁸ See further the discussion in the Obligations and Liabilities section of this paper.

The nature of the legal interest in CBDC

35. A key legal question that would need to be determined is whether an rCBDC could be the subject of a property right that, for example, would impact key legal questions such as the ability to pledge the asset as collateral.²⁹ Many legal systems divide property rights into strict categories of rights to tangible things and intangible rights. The former category may be limited to physical objects that are capable of being possessed while the latter covers rights against another person that depend on the ability to enforce them through the courts. Rights to tangible things are generally enforceable against the world (real rights) while rights to intangibles may only represent a right enforceable against a particular person (personal rights).³⁰
36. New forms of asset like an rCBDC³¹ do not fit neatly into either of these categories. They are intangible and will likely constitute a claim on the central bank. But, unlike an intangible asset, an rCBDC will consist of more than a legal right or claim and may exist factually in a manner that is similar to a tangible asset. Moreover, it may be desirable that rCBDC be transferable without an obligation to inform an obligor.
37. In many technical system designs envisaged for rCBDC, payments in CBDC operate in a way that is conceptually similar to the way in which payments are made from a deposit account. That is, a payment instruction is made by the holder which results in the extinguishment of an existing claim, attributed to the payer, and the creation of a new one, attributed to the payee. This is also true for certain crypto-assets.
38. Even though an rCBDC may not fit within existing categories of property, they may still be treated as the subject of property rights in certain jurisdictions. The law governing digital assets is evolving rapidly in some jurisdictions. In particular, courts in certain common law jurisdictions are showing an increasing willingness to recognise digital assets as being things to which personal property rights can relate, even though they do not fit into existing categories of property.³² For example, crypto-assets have been found to be capable of being objects of property rights in cases from across the common law world,³³ suggesting that common law courts may find the same applies to rCBDC.³⁴ Civil law or mixed jurisdictions may be more constrained in their ability to depart from traditional notions of property. In all cases, legislative intervention may be required to

²⁹ The question of whether a holder's interest in rCBDC is proprietary may also have an international dimension. See the discussion in the Cross-border Considerations section, below.

³⁰ An example of a real right (right in rem) is ownership of a house. The owner can assert their ownership against any other person. By contrast, the right to be paid a sum of money under a contract is a personal right (right in personam). The right holder can only assert the right against the other party to the contract.

³¹ See also crypto assets, quotas, intellectual property rights, carbon emission allowances and waste management licences.

³² UK Law Commission *Digital Assets: Final Report*, June 2023 <https://www.lawcom.gov.uk/project/digital-assets/> at 3.38 ff.

³³ Including cases from the UK, Australia, Canada, New Zealand, Singapore, Hong Kong and the US. UK Law Commission at 3.43.

³⁴ However, relying on judicial interpretation may not provide the necessary degree of legal certainty for users of CBDC.

confirm the legal nature of digital assets and whether they are capable of being objects of proprietary rights.³⁵

39. The 2023 UNIDROIT³⁶ Principles on Digital Assets and Private Law recognise that digital assets can be the subject of property rights and suggest that de facto control of digital assets could substitute for traditional concepts of possession of tangible things. The Principles might provide useful guidance as jurisdictions consider these issues in the context of rCBDC.³⁷
40. The nature of the legal interest that a holder has in their rCBDC could impact how competing claims to rCBDC might be dealt with in the context of a legal dispute. The rules for resolving such situations often depend on whether a claimant is considered to have a proprietary right in the asset in question or not.

Transfer of CBDC and its potential use as collateral

41. In most cases, a key policy objective for rCBDC is that it should function effectively as a means of payment. To achieve this, the rCBDC system rulebook and potentially the legal framework more broadly will need clear rules on the transfer of rCBDC.
42. Central to the question of transfer is the legal regime for settlement finality. The point in time at which the transfer legally becomes irrevocable and unconditional will need to be specified. This will likely be specific to the system's technical design. In a non-distributed system where the central bank is the sole validator, this point may be easy to identify. More consideration may be needed for DLT-based infrastructures where responsibility for the validation of transactions is distributed.³⁸ Once the point of legal finality is reached, the rules would provide that the payer can no longer revoke the transaction and payer and payee holdings will be updated.
43. To fulfil its function as money, an rCBDC may need to fit into the existing financial system and be able to be used in the same way as other types of money. This includes its potential use as collateral. Bank deposits are regularly used as collateral, both for banks but also for third party arrangements. Cash can also be pledged.³⁹ The mechanism by which an rCBDC might be pledged may need

³⁵ Some civil law jurisdictions have already introduced legislation allowing for proprietary rights to attach to things that do not fall into the traditional categories. For example, the Swiss Distributed Ledger Technology Act (2020) allows for proprietary rights to exist in respect of tokenised securities. Proposals for legislative reform have also been made in common law jurisdictions, for example, the UK Law Commission Final Report on Digital Assets.

³⁶ The International Institute for the Unification of Private Law (UNIDROIT) is an independent intergovernmental organisation that studies needs and methods for modernising, harmonising and co-ordinating private and commercial law.

³⁷ If the concept of control as a determinant of proprietary rights is to be adopted in respect of rCBDC, consideration should be given as to how control of the asset would be established. In a two-tiered CBDC model, this would not necessarily be analogous to commercial bank accounts which are held by the debtor (the bank) itself.

³⁸ In all cases, settlement finality is a legal point in time. For CBDC designs with a probabilistic settlement DLT-based infrastructure, finality could be defined as a minimum percentage of validators or certain number of blocks post transaction on chain to consider the transaction final. For deterministic DLT-based systems, this point could perhaps be defined as the point at which consensus is reached amongst the validators on the specific block containing the transaction.

³⁹ Although it is not clear to the authors how frequently this happens in practice.

consideration. For physical property like banknotes, physical control (the delivery of possession) is typically required. For claims, it is usually the notice of assignment of the claim that perfects the pledge. The requirements for a valid pledge of CBDC may need to be specified in legislation.⁴⁰

Obligations and liabilities of parties within the CBDC ecosystem

44. A well-functioning payments system requires clearly defined roles and responsibilities for its participants.
45. Although rCBDC systems may be designed in many ways, participants in the system could include: (i) a central bank to issue the asset; (ii) an operator to run the system; (iii) intermediaries to act as a gateway to the system for users;⁴¹ (iv) providers of access devices that allow users to make payments or manage their rCBDC balances;⁴² and (v) entities or individuals that use the rCBDC for transactions (end-users). Within such a system, a number of questions arise. What should the obligations of each of these parties be? And who should be responsible for any issues that might arise?
46. This section looks first at the types of risks that may exist within the system. It then considers how those risks can be allocated through the legal relationships between the parties in an rCBDC system.

Risks in an rCBDC system

47. In identifying and allocating the risks that can arise within an rCBDC system, policy makers can draw on the detailed guidance that has already been developed in the context of Financial Market Infrastructures (FMIs) and, in particular, the Principles for Financial Market Infrastructures (PFMIs) that have been developed by CPMI-IOSCO. While it would need to be determined if and how the PFMI would apply to an rCBDC system, policy makers might choose to draw from this existing learning in designing an rCBDC system. In this way, they can incorporate techniques that have already been considered and tested. However, the operation of an rCBDC may give rise to heightened risks (or public concerns about risks),

⁴⁰ The UNIDROIT principles may also be of assistance here.

⁴¹ These intermediaries would vary by jurisdiction, but may include commercial banks, non-bank payment service providers, and regulated nonbank financial service providers. These entities would offer accounts or digital wallets and would be responsible for managing the relationship with end-users.

⁴² It is possible that providers of these devices may specialise in the device and not be a full-service intermediary. Including access devices as a separate category from intermediaries is meant to highlight the difference between a hardware form factor that is provided by a non-financial services company and a smartphone app provided by a traditional financial intermediary. It is possible that the obligations of these access device providers to end users may differ from those of the intermediaries in certain instances, such as fraud.

particularly in relation to cybersecurity and privacy. These challenges would need to be addressed in the legal framework.

48. Broad categories of risk associated with the design and operation of an rCBDC system include operational risk, legal risk, and reputational risk.^{43,44} The definitions of these concepts set out in the PFMI provide a useful foundation upon which to consider how they can be identified and addressed within an rCBDC system.

Operational risk

49. Under the PFMI, operational risk is “the risk that deficiencies in information systems or internal processes, human errors, management failures or disruptions from external events will result in the reduction, deterioration or breakdown of services provided by an FMI”.⁴⁵ This type of risk includes process-related risk, technology risk, third-party risk (including fraud), business continuity risk, and cyber risk.⁴⁶
50. In the context of an rCBDC, process-related risks are the risks associated with operating the rCBDC system. rCBDC, like existing payment systems, would require specific processes to effectively transfer rCBDC. Operational mistakes could affect the efficiency and security of the system. Operational risks for rCBDC could materialize through human error, inadequate definitions, or incomplete planning.⁴⁷
51. Technology risks associated with rCBDC may include technological failure or maintenance issues. Technology failures may affect the operation of the transfer mechanism and the availability of the rCBDC leading to delayed settlement or double spending. Maintenance issues could result in errors in the recording of rCBDC holdings or missed payments.
52. Risks may also arise with a third-party service provider who, in the context of an FMI, is “an unaffiliated entity that provides services to an FMI”. Within an rCBDC system, risks associated with these providers may include technology failures, cyber-attacks, fraud or error, business disruptions, dependencies on a fourth party, or different operational risk standards. For example, access device providers may be considered third-party service providers and there are risks that these devices may become corrupted and unable to process payments.
53. Business continuity refers to “all of the organizational, technical and staffing measures used to ensure the continuation of operations following a disruption to

⁴³ Credit and liquidity risks are outside the scope of this note. Should such risks be identified in a particular system (for example, credit risk in a system in which - contrary to this paper’s assumption - intermediaries hold CBDC on-balance sheet) then these risks would also need to be addressed through one or more of the means discussed in this paper, or otherwise.

⁴⁴ A CBDC system could also create other risks which would be borne by society as a whole. These could include risks to financial stability (including through disintermediation of the banking sector) or to the environment (including through the energy demands of the system).

⁴⁵ [Committee on Payments and Market Infrastructures Glossary](https://www.bis.org/cpmi/publ/d00b.htm): <https://www.bis.org/cpmi/publ/d00b.htm>.

⁴⁶ Bank for International Settlements (2023): *Central bank digital currency (CBDC) information security and operational risks to central banks: An operational lifecycle risk management framework*, November <https://www.bis.org/publ/othp81.htm>

⁴⁷ Bank for International Settlements (2023): *Central bank digital currency (CBDC) information security and operational risks to central banks: An operational lifecycle risk management framework*, November <https://www.bis.org/publ/othp81.htm>

a service, including in the event of a wide-scale or major disruption”.⁴⁸ Business continuity risks to the uninterrupted functioning of an rCBDC system include natural disasters affecting infrastructure, supply chain disruptions, and an issue with certain access devices impacting their ability to properly reconcile offline transactions with a functioning general ledger.⁴⁹

54. In the context of an FMI, cyber risk refers to the “risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorised access, use, disclosure, disruption, modification, or destruction of the manufacturing system”.⁵⁰ Many cyber risks associated with an rCBDC system are the same as those associated with traditional FMIs. But, depending on the design of the rCBDC system, there may also be new areas for cyber risk, such as increased data centralisation, increased difficulty reversing fraudulent or erroneous transactions, challenges in payment credential management and key custody, susceptibility to malicious transactions enabled by automated financial applications, and increased reliance on non-banks.⁵¹
55. Liability for operational risks emerging within an rCBDC system will need to be distributed across the relevant parties involved. If each participant in the CBDC system is subject to clear obligations in relation to its participation, it would have the appropriate incentive to ensure that it mitigates operational risks, where possible. Liability for failure to perform those obligations would follow accordingly. The appropriate assignment of liability for operational issues may come down to whether the policy goal is to prevent the incident from happening or to limit potential losses if the incident happens.

Legal risk

56. Under the PFMI, legal risk is “the risk of the unexpected application of a law or regulation, usually resulting in a loss”.⁵² The operation of an rCBDC system would give rise to a number of legal risks. There are legal risks associated with incomplete legislative or regulatory frameworks for rCBDC.⁵³ Any uncertainty as to the obligations and responsibilities of parties in the rCBDC system may result in the uneven application of existing laws across all parties. Such ambiguity likely would result in all parties taking on some form of legal risk.⁵⁴

⁴⁸ Committee on Payments and Market Infrastructures Glossary: <https://www.bis.org/cpmi/publ/d00b.htm>.

⁴⁹ Bank for International Settlements (2023): *Central bank digital currency (CBDC) information security and operational risks to central banks: An operational lifecycle risk management framework*, November <https://www.bis.org/publ/othp81.htm>

⁵⁰ National Institute of Standards and Technology, US Department of Commerce: *Computer Security Resource Center Glossary*, <https://csrc.nist.gov/glossary>.

⁵¹ Fanti, G et al (2022): *Missing Key: The challenge of cybersecurity and central bank digital currency*, Atlantic Council, June, <https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/>.

⁵² Committee on Payments and Market Infrastructures Glossary: <https://www.bis.org/cpmi/publ/d00b.htm>.

⁵³ Bank for International Settlements (2023): *Central bank digital currency (CBDC) information security and operational risks to central banks: An operational lifecycle risk management framework*, November <https://www.bis.org/publ/othp81.htm>.

⁵⁴ Central banks may have statutory immunity from suit for actions taken in the exercise of their public functions. The issuance of CBDC, as the issuance of public money for a public purpose, could fall within the scope of this immunity. The limits of any statutory immunity in a particular jurisdiction may also impact the question of the appropriate form (contractual or regulatory) of the rulebook.

57. Even if the legal regime applicable to rCBDC is clear and well-understood, other legal risks may arise. For example, intermediaries and other participants may incur compliance risk through their participation in the rCBDC system. This is the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a participant may suffer as a result of its failure to comply with relevant laws, regulations, rules, related self-regulatory organisation standards, or codes of conduct.⁵⁵ Participants also may be subject to litigation for failure to comply with applicable laws and regulations.
58. Legal risk for all parties arising from the operation of rCBDC may be minimised by ensuring that (i) the legislative framework for the rCBDC is clear, particularly in relation to the legal nature of the rCBDC and the rights of its holders; and (ii) the relevant contractual framework is comprehensive and unambiguous.⁵⁶

Reputational risk

59. In the context of an rCBDC system, reputational risk is the risk arising from any negative publicity a central bank, intermediary, or other participant faces for its participation in the rCBDC system, including when something goes wrong in the system.
60. As the issuer of rCBDC, the central bank may face significant reputational risk in relation to any issues arising within the system, regardless of whether it is itself responsible for the particular issue. Reputational risk is harder to allocate through a legal framework than is the case for other risks. Even if a central bank issuing an rCBDC is not responsible for an operational incident, it may be expected to fix it or to provide compensation. A clear communication strategy regarding liabilities within the system may go some way to mitigating this risk.

Legal mechanisms for allocating liability

61. The principal mechanisms for assigning obligations and liabilities across multiple parties within a payments system are law (that is, legislation and regulation) and contractual arrangements. Legislation and regulation may advance public policy goals, allocate risk to the parties most appropriate to bear it, and generally set forth the legal framework for the CBDC ecosystem. Contractual arrangements, meanwhile, may allow for more bespoke and flexible arrangements between certain parties that operate within boundaries set by law.

Legislation and regulation

62. Central bank authority is often derived from legislation, and it is likely that any roles the central bank would play within the CBDC system would need to be codified in law. Legislation and regulation outlining the obligations and liabilities

⁵⁵ Basel Committee on Banking Supervision (2008): Implementation of the Compliance Principles: A survey, August <https://www.bis.org/publ/bcbs142.pdf>.

⁵⁶ The legislative and contractual frameworks should be consistent with the Principles for Financial Market Infrastructures, where appropriate, even though those may not be directly applicable.

of a central bank in these roles would help to mitigate legal risk and to clarify the extent (if any) of the central bank's responsibility for operational issues.⁵⁷

63. The obligations and liabilities of intermediaries may be determined by a combination of legislation, regulation, and contractual agreements. It is important to note that an rCBDC will be issued against a background of legislation and regulations that are applicable to payments generally. Certain intermediaries and their activities may already fall within an existing legislative or regulatory framework. Each jurisdiction would therefore need to determine to what degree existing rules would remain appropriate in the context of the rCBDC system and whether they appropriately allocate liability for CBDC risks.

Contractual relationships between parties

64. The central bank, as issuer of the asset, is likely to have a contractual relationship with both the operator of the system (if the central bank contracts out this function)⁵⁸ and with each of the intermediaries who provide rCBDC services to end users.
65. Like existing central bank operated payment systems, the contractual arrangements⁵⁹ concluded between the central bank and the intermediaries would be based on a standardised set of terms and conditions governing the constitution and administration of the system. Terms and conditions that a jurisdiction may incorporate into its rulebook would, in particular, define the rights and obligations of the participants and provide authoritative information to stakeholders respecting: the operation of the system,⁶⁰ compliance; participant management;⁶¹ cost allocation;⁶² and technology.⁶³
66. In a two-tiered system, end-users may not have a direct contractual relationship with the central bank. Rather, they would likely have a contractual relationship

⁵⁷ For example, a central bank may wish to consider (potentially with other stakeholders) whether it would indemnify third parties for certain risks, or otherwise reduce their liabilities. Decision-makers may also consider whether the central bank itself would need to be indemnified, for example by the government.

⁵⁸ Jurisdictions may take different approaches with respect to whether the central bank or a private sector entity would own and operate the core CBDC ledger that tracks outstanding balances. Certain jurisdictions, such as the United Kingdom, propose that the central bank should be responsible for the CBDC ledger (Bank of England (2023): The digital pound: Technology Working Paper <https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-technology-working-paper.pdf>) Other projects, such as Project Helvetia (a wholesale CBDC project), envision a private sector operator (a fully licensed and supervised Swiss central securities depository) that is subject to strict control and monitoring by the central bank (Bank for International Settlements, SIX Group, Swiss National Bank (2022) "Project Heletia Phase II Settling tokenised assets in wholesale CBDC" <https://www.bis.org/publ/othp45.pdf>) In both approaches, the operator would have to consider the legal obligations of any party that provides hardware or software for the CBDC system.

⁵⁹ Intermediaries wishing to provide services to end users in relation to CBDC would likely have to agree to the rulebook as a condition of their participation in the system. However, the rulebook also has the potential to affect the rights and obligations of end users, who would not be party to the contract. Jurisdictions may therefore have to consider the trade-offs between the rulebook being private in nature and taking the form of regulation or legislation.

⁶⁰ Including purchase and redemption of CBDC, reconciliation, settlement finality, transfer mechanics, charge definition and registration, choice of law and dispute management – including end-customer transactional disputes and monitoring.

⁶¹ Including onboarding, eligibility, rights and duties, suspension and termination.

⁶² Including fees, charges and penalties.

⁶³ Including potential interoperability with other systems, messaging, security including identity and other validation, infrastructure and contingency standards.

with the intermediaries whose services they use. Important end-user obligations, particularly in relation to privacy and payments fraud, could be contained in these contracts. The contract between the central bank and the intermediary may limit or dictate the content of the contract between the end user and the intermediary, as could the legislative framework.

67. It is likely that providers of access devices would also need to have in place contractual relationships with the users of the devices (who may be end users or intermediaries).⁶⁴

Protection of privacy and AML/CFT compliance

68. Privacy considerations are critical to the design of rCBDC systems, as privacy is one of the public's central concerns about rCBDC. An rCBDC system must therefore be designed keeping existing data protection laws in mind.

Privacy

69. Privacy is an important concept that is found in the legal frameworks of many jurisdictions. In the realm of payments, privacy often refers to the ability of each party to a transaction to exercise control over the personal data necessary to process the payment, and to decide who can access that data and for what purpose. This general concept finds expression in a multitude of laws and policies that differ considerably by region and country, as well as by subject matter and context. Understanding how privacy is expressed as a right, or law, can help in comprehending its possible relationship with an rCBDC system.
70. Privacy may be differentiated from anonymity. Anonymity is generally understood to refer to circumstances where the identity of a party to a transaction is not known to others.⁶⁵ Although anonymity may enable privacy – in the sense that attributing a transaction to an anonymous party can be challenging or impossible – it is not the same as privacy.⁶⁶

Privacy as a right

71. In many jurisdictions, although by no means all, privacy is a fundamental right.⁶⁷ In some common law countries, privacy is recognised as a “constitutional right”,

⁶⁴ The central bank may wish to consider whether it will require providers of access devices to also contract directly with the central bank. The need for this will be driven by the design and functions of the devices.

⁶⁵ Anonymity itself must be differentiated from pseudo-anonymity (or pseudonymity) which describes circumstances in which an individual's identity is unknown, but where (trans)actions can be assigned to that individual.

⁶⁶ For example, a person spying on a family having lunch with binoculars could be in violation of privacy laws, regardless whether the person spying knows the identity of the individuals observed.

⁶⁷ Jurisdictions differ in their terminology for these provisions. Intended are any rules that are guaranteed by a constitution (or similar), that override ordinary legislation, and that are usually in place to safeguard individuals' rights.

eg, as a “right to be let alone”. In others, the right to privacy is instead contained in sector-specific laws.⁶⁸

72. In many civil law jurisdictions, privacy is implicitly or explicitly contained in the constitution to protect individuals from state interference. It often takes the form of a right to “informational self-determination”,⁶⁹ which gives individuals the right to determine which information about them may be disclosed and how it can be used.
73. Privacy is also recognised as a universal human right in several supra-national instruments. The Universal Declaration of Human Rights refers to a person’s right to protection from arbitrary interference with their privacy. The European Convention on Human Rights and the EU Charter of Fundamental Rights both refer to a “right to respect for (...) private (...) life”.
74. Beyond the realm of constitutional and fundamental rights, many jurisdictions have sought to protect the privacy of parties in certain circumstances by putting in place comprehensive data protection regimes. Generally, data protection laws encompass any information relating to an identified or identifiable natural person.⁷⁰ These regimes generally emphasise the need to obtain informed consent from individuals, limit the purposes for which data can be collected and used, and require organisations to implement robust security measures to safeguard personal data.
75. The precise scope and content of these laws varies between jurisdictions. Examples can range from specific regulatory target areas like medical records, data concerning children, or consumers’ financial information to general acts that target personal information and data as a whole.
76. Most data protection regimes establish rules specifying how financial intermediaries may process the data that they hold about their customers. Financial intermediaries are typically required to put in place processes through which such intermediaries can effectively protect the privacy of individuals and the confidentiality of their data. Although the right to privacy is not absolute, legal regimes in many jurisdictions establish strict rules against the disclosure of personal information.

Current payment systems and privacy

77. Existing payment instruments enable varying levels of privacy. Cash is at the high end of the spectrum while other electronic payment instruments score lower.
78. Cash, as a bearer-instrument, can be directly passed from payor to payee and leaves no trace of identity. No validation of the transfer or the identity of the parties involved is required. It is sufficient that the payee can verify the cash

⁶⁸ Eg, in the UK the most central one of these laws is the Human Rights Act of 1998 that safeguards individuals’ right to live a private life without government interference.

⁶⁹ Eg, Germany.

⁷⁰ See, eg, the Data Protection Regulation (GDPR) of the European Union, which regulating personal data as “any information relating to an identified or identifiable natural person”, Art. 4 (1).

instrument's authenticity for the payor's debt to be extinguished through the act of tendering that instrument in settlement.

79. Payments made with physical cash can therefore protect the privacy, and potentially anonymity, of users. However, to limit the scope for the use of physical cash for illicit activities, many jurisdictions impose limits on the maximum value of cash transactions or impose mandatory reporting requirements if payments exceed a certain value.⁷¹
80. Private (and anonymous) payment transactions may also be possible – typically up to certain limits – with the use of e-money. And some crypto-assets may protect the privacy (and anonymity) of their users to a standard comparable to that of physical cash, because of their use of cryptography or other anonymity-protection mechanisms.⁷²
81. At the other end of the spectrum, payments made through bank account transfers or with credit cards require entire data troves for processing. These payment instruments are tied to a transaction history that identifies their holder. Because knowledge of these transactions is limited to the processing institutions, these transfers can be described as private, although the level of privacy may be diminished as more (intermediary) parties are involved.⁷³

Privacy in an rCBDC system

82. It is, to some degree, a policy decision as to how much privacy the designers of an rCBDC system would afford to users.⁷⁴ As noted above, the design assumptions underlying this paper provide that the central bank will have no information that would enable it to identify holders of the rCBDC. Under such a system, the central bank could be required to authenticate the validity of the rCBDC units (where relevant) used in a particular transaction (to avert the risk of digital counterfeits) but without the user's identity being disclosed.
83. A complicating factor is the recognition of rCBDC as a liability of its issuing central bank. Regardless of other design choices, the need for the issuing central bank to authenticate claims against it from CBDC unit holders may require a mechanism

⁷¹ For an account of the limits applicable in several EU Member State jurisdictions see N Pocher and A Veneris (2021), "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme", p 5. In Canada, financial institutions and other reporting entities are required to report cash transactions exceeding CAD 10,000 to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) pursuant to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (S.C. 2000, c. 17) (the PCMLTF Act) and its regulations.

⁷² What determines the traceability of crypto-assets is how they are accessed. Monero and zcash are less easily traceable compared to, say, bitcoin, which, however, also offers a high level of privacy (see A Kaushik, J Wyatt and T Xi (2019-2020)), "Central Bank Digital Currency (CBDC) and Privacy", Massachusetts Institute of Technology, *Working Groups Cycle*, p 20.

⁷³ The level of privacy afforded by different (non-cash) payment instruments will also depend on the terms of the contract between payment instrument providers and the users of payment instruments: users may (and routinely do), authorise payment instrument providers to process (track, aggregate, etc.) as well as use (disseminate) their transaction data and other personal data for marketing purposes, and for convenience or cost-saving reasons.

⁷⁴ It has aptly been observed that, "CBDC design choices are not merely technical in nature; they can also be used to operationalize policy objectives ... As a result, policy objectives can and should guide the design of a CBDC" (R. Mahari, T Hardjono and A Pentland (2022), "AML by design: Designing a central bank digital currency to stifle money laundering", *MIT Science Policy Review*, vol 3, p 58).

for ascertaining the identity of claimholders in certain circumstances - for example, in the insolvency of an intermediary. Such cases could be addressed through a mechanism allowing for an insolvency administrator of an intermediary to submit block requests to the central bank without disclosing the identities of the intermediary's customers.

AML/CFT

The current AML/CFT landscape

84. Competing with the policy objective of preserving privacy is the need to detect and combat money laundering and terrorist financing, which requires access to personal data regarding the parties to a (suspicious) transaction and the transaction itself. In this context, privacy cannot be understood as an absolute right but rather a right that needs to be reconciled with jurisdictions' obligation to combat financial crime.
85. It is against this background that jurisdictions have put in place comprehensive anti-money laundering and countering the financing of terrorism (AML/CFT) regimes that aim to prevent illicit financial activities and protect the integrity of the financial system. AML/CFT rules are set out in law and regulation that differ between jurisdictions.
86. On a global level, the Financial Action Task Force (FATF) has issued recommendations that serve as guidance for the design and implementation of AML/CFT regimes. AML/CFT regimes typically require financial intermediaries such as banks and payment service providers to engage in know-your-customer (KYC) procedures, conduct customer due diligence, and identify and report suspicious activities and transactions to the relevant AML/CFT authorities. These disclosures are mandatory if certain conditions are met, and do not require customer consent. In some jurisdictions, an entity's AML/CFT duties qualify as public interest duties, enabling the lawful processing of personal data for these purposes.

AML/CFT for rCBDC systems

87. In balancing privacy protection and AML/CFT enforcement in the legal framework for an rCBDC system, policy makers may choose to draw on the rules that apply in the conventional banking system. Potential tensions between the two objectives have been carefully considered and addressed by many jurisdictions in the context of the traditional financial system. Financial intermediaries must generally protect the privacy of customer-related information but may be required to disclose it with relevant parties (eg, law enforcement authorities) in certain circumstances. Moreover, AML/CFT regimes generally recognize the need to protect customers' privacy except when necessary to preserve financial integrity. Indeed, the FATF recommendations touch on the topic of privacy in the context of national cooperation and coordination and require relevant competent authorities to ensure the compatibility of AML/CFT requirements with data

protection and privacy rules and other similar provisions.⁷⁵ For international cooperation, the FATF recommendations require that exchanged information is consistent with institutions' obligations concerning privacy and data protection.⁷⁶

88. Following the approach taken in the traditional financial system, intermediaries in an rCBDC system could be required to comply with broadly the same due diligence and disclosure requirements that apply to existing means of payment. This would include conducting KYC processes and customer due diligence, and identifying and reporting suspicious activities and transactions to the competent AML/CFT authorities.
89. At the same time, the legal framework for an rCBDC system may need to address certain issues that are specific to rCBDC. For example, it would need to be determined whether anonymous payments using rCBDC would be permitted for small amounts. By permitting the making of anonymous payments up to specified limits, policy makers could replicate some features of physical cash without necessarily exacerbating money laundering risks.

Cross-border issues

Cross-border access to CBDCs

90. A fundamental question for jurisdictions that are considering issuing a CBDC is whether to permit non-resident/non-domiciled end-users⁷⁷ or intermediaries to have access to their CBDC.⁷⁸ This is primarily a policy question.⁷⁹ However, the question may also entail legal consequences.

Non-resident/non-domiciled end-users

91. Relevant policy issues for jurisdictions considering non-resident access could include the need to protect their balance of payments and guard against the risk of destabilising capital outflows. In granting non-resident access, jurisdictions may need to consider whether the rules that would apply to non-residents should differ from those that apply to residents. Rules specific to non-resident use may include exchange control measures or AML/CFT controls needed to address heightened money laundering risks associated with non-resident transactions.
92. For example, opening an account with a bank or nonbank payment service provider from outside the jurisdiction is often more difficult than doing so from the inside. This is partly because transacting with non-residents can require financial institutions and nonbank payment service providers to follow special

⁷⁵ FATF recommendation A.2.

⁷⁶ FATF Interpretative note to recommendation 40, A.4.

⁷⁷ This could include tourists or e-commerce consumers but also those who simply prefer to hold another currency.

⁷⁸ Such access can be direct (where a market actor itself participates in the system) or indirect (where access is only possible through a direct participant in the system).

⁷⁹ Unless required by a bilateral or multilateral treaty.

(and often more stringent) AML/CFT rules. Non-resident customers are generally considered to carry a higher financial crime risk.⁸⁰

93. Tiered user identification (eg, limited identification requirements allowing access to a type of rCBDC with limited functionality, such as a lower holding limit) might be one way to balance heightened financial crime risks with making an rCBDC available to non-residents.⁸¹ Lower holding limits may also be an option for jurisdictions concerned about destabilising capital flows.

Non-domiciled intermediaries

94. In deciding whether to allow non-domiciled intermediaries to provide services in respect of their rCBDC, jurisdictions may need to consider how such intermediaries should be regulated/supervised/overseen.⁸² In particular, they may need to decide what regulatory rules non-domiciled intermediaries should be subject to and whether (and how) such regulatory rules would be enforced.⁸³
95. It is possible that the rCBDC-issuing jurisdiction would wish to regulate/supervise/oversee domiciled and non-domiciled intermediaries according to the same or similar standards as domiciled companies to avoid distorting the competitive environment. This could give rise to certain legal challenges respecting the enforceability of regulatory measures across borders, and the need to put in place cooperation arrangements with the supervisors in which such intermediaries are based.

Conflict of laws issue

96. A significant issue when considering cross-border use of rCBDC is how the applicable law should be determined in particular cases.⁸⁴ For example, if a company located in Jurisdiction X accesses a CBDC issued by Jurisdiction Y through an intermediary located in Jurisdiction X and the CBDC system malfunctions causing the transaction to fail, should the law of Jurisdiction X or the law of Jurisdiction Y apply to the resulting dispute?⁸⁵

A conventional approach

97. A conventional approach to the determination of the governing law in many jurisdictions is to focus on the subject and nature of the legal issues in question. As a starting point, it should be noted that money has a special conflict of laws rule in many jurisdictions: the *lex monetae* which provides that the government

⁸⁰ Para. 15 of [The FATF Recommendations](#) lists “Non-resident customers” as one of the customer risk factors.

⁸¹ The proposal for the digital euro regulation provides that visitors to the euro area shall be subject to limits as regards the use of the euro as a store of value that are not higher than the ones effectively implemented in the euro area for natural and legal persons residing or established in Member States whose currency is the euro (Article 16.5).

⁸² The requirements of existing RTGS systems or central counterparties that allow non-resident institutions access may be a useful starting point.

⁸³ The jurisdiction in which the intermediary is domiciled will also have its own supervisory requirements.

⁸⁴ The Hague Conference on Private International Law is currently considering these issues, as is the UK Law Commission.

⁸⁵ Another significant area of cross-border legal risk is the insolvency of intermediaries, where an insolvency administrator may need to resolve issues relating to the CBDC of other jurisdictions.

that creates the monetary unit has the authority to take actions in respect of it, including revaluing it, and that these actions have extraterritorial effect. However, the scope of this rule is generally limited to the monetary units themselves and would not apply to a dispute between two parties involving the use of an rCBDC. The contractual relationship between end-users and intermediaries would be governed by the *lex contractus* (the law of the place the contract was formed, or the choice of law specified in the contract). Proprietary aspects of an rCBDC would be governed by the *lex situs* (the law of the place where the property is situated),⁸⁶ while other disputes outside of any relevant contract such as a tort claim based on the negligence of a party might be governed by law of the place of the tort.

98. While these conventional approaches may prove sufficient for some cases involving rCBDC, challenges may, in some instances, arise because of the digital (intangible) nature of CBDC.⁸⁷ For example, the *situs* of an rCBDC might be unclear especially where distributed ledgers are used.⁸⁸
99. To address such uncertainties, different approaches may be envisaged. Some of these would follow traditional approaches while others would not.

Approaches focusing on the intermediary

100. For cases involving intermediaries and end-users, the applicable law could be specified in the agreements that are put in place between them. Article 4(1) of the Hague Securities Convention⁸⁹ takes this approach. This method may be particularly beneficial for non-resident end-users who access an rCBDC through an intermediary in their own jurisdiction. Under this approach, non-resident end-users in such circumstances may avoid the possibility that they might be subject to the law of the CBDC-issuing jurisdiction. For example, a company established in Jurisdiction X may want to access an rCBDC issued by Jurisdiction Y, but it may not want any disputes to be subject to Jurisdiction Y's laws. The company could access Jurisdiction Y's rCBDC while avoiding Jurisdiction Y law if "Jurisdiction X law"⁹⁰ were designated as the applicable law under the agreement with its intermediary (eg, in the terms and conditions for the CBDC wallet service).⁹¹
101. Determining the applicable law based on the location of the relevant intermediary (Place of the Relevant Intermediary Approach, PRIMA) could be an

⁸⁶ William Blair: "Monetary Obligations, Governing Law and Jurisdiction" presentation at a meeting of the Committee on International Monetary Law of the International Law Association (MOCOMILA) in Tokyo on 1 April 2004. [The minutes of the meeting](#) (available only in Japanese).

⁸⁷ Commentary of Principle 5 of [UNIDROIT Principles on Digital Assets and Private Law](#) "recognises that the usual connecting factors for choice-of-law rules (eg the location of persons, offices, activity, or assets) usually have no useful role to play in the context of the law applicable to proprietary issues relating to digital assets".

⁸⁸ It is also possible to imagine issues arising if the property law classification of CBDC (see above) differs across jurisdictions.

⁸⁹ To date, Switzerland, Mauritius and the United States have ratified the convention.

⁹⁰ Article 4(1) of Hague Securities Convention does not allow designating a completely unrelated third country law; the intermediary must have a certain relation (eg, having an office) to the designated jurisdiction.

⁹¹ In practice, choice of law by the intermediary may be constrained by the terms of the intermediary's relationship with the CBDC-issuing central bank.

alternative.⁹² In the example described above, the PRIMA approach would allow the company to access to Jurisdiction Y's CBDC while avoiding Jurisdiction Y law because the applicable law is determined based on the place of the relevant intermediary (that is, Jurisdiction X).

Specification in the system

102. An approach that applies the law specified in the CBDC system itself as the governing law could also be a possible solution. This is what is proposed by Principle 5 of UNIDROIT Principles on Digital Assets and Private Law.

103. If this approach is in place, the applicable law in the example described above would be determined by the specification in Jurisdiction Y's CBDC system, regardless of factors such as the choice of law clause in the agreement between the company (as the user) and its intermediary, or the location of such intermediary.⁹³

Possibility of an international framework

104. Given the specific features of rCBDC and digital assets more generally, jurisdictions may wish to consider developing special rules to be used by courts in determining the applicable law in relevant disputes. Such an approach could promote greater legal certainty that would encourage the cross-border use of CBDC. Such rules could also be set out in bilateral or multilateral agreements between jurisdictions who wish to promote the cross-border use and exchange of their respective rCBDCs.⁹⁴

Exchange of CBDCs from different jurisdictions

105. In addition to decisions as to whether to permit non-resident/non-domiciled access by end-users and intermediaries, some jurisdictions could consider CBDC system models that facilitate the cross-border exchange of CBDCs.⁹⁵ Such models can be categorised into three types: (i) compatible CBDC systems, (ii) interlinked CBDC systems, and (iii) a single system.⁹⁶ While some of these models are particularly relevant for wholesale CBDC, they can also be used to promote interoperability between rCBDC issued by different jurisdictions.

⁹² Article 9(2) of the European Union's Settlement Finality Directive ([DIRECTIVE 98/26/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 May 1998 on settlement finality in payment and securities settlement systems](#)) is said to have introduced this approach.

⁹³ A related approach would be for Jurisdiction Y's CBDC rulebook to specify that the CBDC was situated in Jurisdiction Y for the purposes of the lex situs rule. All parties to the system would agree that, as between themselves, they would operate on that basis. Contracts between intermediaries and end users would need to contain an equivalent provision.

⁹⁴ Any such framework could also address how courts in each jurisdiction enforce judgements of courts in the other jurisdiction/s to enhance the framework's effectiveness.

⁹⁵ The legal issues arising from a digital currency area, as discussed in Markus K Brunnermeier, Harold James and Jean-Pierre Landau, The digitalization of money, BIS Working Papers No 941, May 2021, are out of scope for this paper.

⁹⁶ Auer, R, et al (2021): Multi-CBDC arrangements and the future of cross- border payments. <https://www.bis.org/publ/bppdf/bispap115.pdf>.

106. Interoperability, in a general sense, refers to the technical, semantic, legal and business compatibility that enables a system to be used in conjunction with other systems. In the context of CBDC, interoperability allows payment service providers from different CBDC systems to seamlessly make payments across systems without participating in multiple systems.⁹⁷
107. Cross-border interoperability of payment systems is not a new or CBDC-specific topic. Many existing payment systems do not fare well in terms of cross-border interoperability whether from a technical or from a legal perspective.⁹⁸
108. CBDC systems could be set-up with cross-border interoperability taken into account from the outset. The design of a CBDC, including decisions about the legal classification of the CBDC, may have a considerable impact on its suitability for interoperability solutions.

Model 1: Compatible CBDC systems

109. The key idea of Model 1 is to enable and facilitate interaction between distinct systems by agreeing on the use of common technical standards and harmonising legal and regulatory rules and requirements. Ideally, compatible systems reduce inefficiencies in the interaction between systems and facilitate the implementation of correspondent and clearing services.
110. Besides technical standardisation (eg, data standards and message formats, user interfaces, operating hours), legal and regulatory harmonisation is an important element for compatibility. In fact, legal and regulatory compatibility is sometimes cited as the greatest source of friction for cross-border payments by banks and payment service providers.^{99 100}
111. Harmonisation of legal and regulatory rules and requirements typically occurs within a federal framework (such as the EU), through the adoption of rules agreed at a multilateral level (such as conventions adopted within the OECD or UN) or through the unilateral adoption by one sovereign state of another sovereign state's legal system.¹⁰¹ Experience from existing settlement systems shows that improving compatibility takes time and can require coordinated policy action.¹⁰²
112. Areas where legal harmonisation might potentially have a positive impact on cross-border interoperability include AML/CFT and data protection rules and requirements. Applying different compliance standards can be challenging and inefficient, though may ultimately be necessary to achieve individual jurisdictions' policy goals. In addition, cross-border activities may mean intermediaries are

⁹⁷ See CPMI, BIS Innovation Hub, IMF and World Bank, [Options for access to and interoperability of CBDCs for cross-border payments](#), (Report to the G20, July 2022), p.5.

⁹⁸ Lack of interoperability has been identified by the Financial Stability Board as one of main frictions to be addressed in the context of the ongoing G20 project aiming to enhance cross-border payments by making them faster, cheaper, more transparent and more inclusive. [FSB reports on its work to develop a roadmap to enhance global cross-border payments - Financial Stability Board](#).

⁹⁹ Auer et al (2021).

¹⁰⁰ Yet this friction may be difficult to overcome, as jurisdictions frequently have and should choose legislation and regulation that best fit their policy goals.

¹⁰¹ E Baffi, P Santella, ["The Economics of Legal Harmonization"](#), Encyclopaedia of Law and Economics, Second Edition, Vol. 7, 2011.

¹⁰² Auer et al (2021).

subject to supervision by the authorities of multiple jurisdictions, which may be an additional source of friction.

Model 2: Interlinked CBDC systems

113. Model 2 expands on the idea of distinct settlement systems, but it goes one step further in bringing them together, typically either by adding (i) a shared technical interface (supported by contractual arrangements between systems), or (ii) a common clearing mechanism, linking systems through designated settlement accounts. This may offer the opportunity to implement improved settlement mechanisms, such as improved versions of payment-versus-payment (PvP), ensuring that a final transfer of one CBDC occurs only if a final transfer of the other CBDC also takes place.¹⁰³

114. Harmonised legal and regulatory frameworks tend to facilitate interlinking of systems, so Model 2 (interlinking) often builds on Model 1 (compatible systems).

Model 3: Single CBDC system

115. In Model 3, the CBDCs of different jurisdictions are issued on a single multi-currency system. The single system has an independent rulebook and bespoke access criteria¹⁰⁴. This deeper integration may allow for more functionality and efficiency but increases governance and control complexity. A single rulebook with a single governing law¹⁰⁵ would necessitate acceptance by (at least some of) the participating central banks of the applicability of a foreign governing law to issues affecting their own currency¹⁰⁶.

116. From a governance and legal perspective, single platforms raise several issues. Many of these issues increase in complexity with each additional CBDC issued on the single platform.

116.1. *Legal basis:* Each central bank considering issuing its CBDC on a single platform will have to consider, in addition to whether it has authority to issue CBDC, whether it is in conformity with its mandate and related powers/instruments to issue a CBDC on a single platform (potentially outside of its own jurisdiction).

116.2. *Access to central bank money:* Central banks must be able to determine access to central bank money independently in the exercise of their monetary policy powers.

116.3. *Governing law:* A single platform would need a rulebook or similar legal document governing the platform's operations including, for example, transfers of CBDCs. This may require that (at least some

¹⁰³ Auer et al (2021).

¹⁰⁴ This contrasts with "interlinking" where participants typically connect to their respective home systems.

¹⁰⁵ Potentially the law of the jurisdiction in which the system is situated.

¹⁰⁶ Auer et al (2021).

of) the participating central banks accept the applicability of a foreign governing law.¹⁰⁷

116.4. *Central bank controls:* The nature and extent of the necessary control over a central bank's CBDC would primarily be a policy decision for that central bank. In some jurisdictions, a degree of central bank control may be required for the CBDC to legally qualify as central bank money.¹⁰⁸ Such controls would be more difficult to exercise and enforce with a foreign platform and a rulebook governed by a foreign law.

116.5. *Settlement finality:* It is likely that a goal of a single platform would be to settle transactions with finality on the platform. To achieve this, the respective requirements of each participating jurisdiction would have to be considered.¹⁰⁹

116.6. *Compliance duties (AML/CFT, sanctions, data protection, foreign exchange controls, bank secrecy etc.):* In principle, the platform would have to comply with the rules of each of the legal systems involved.¹¹⁰ For example, in the case of different applicable regimes, this could be achieved by cumulatively performing such duties or by applying and complying with the most stringent rules.

Conclusion

117. A jurisdiction considering issuing an rCBDC may need to ensure its legal system is appropriately updated to, at a minimum: (i) provide a coherent legal framework for the issuance of the rCBDC and its subsequent use by the public; (ii) manage risk; (iii) deliver on privacy and AML/CFT expectations and obligations; and (iv) if a policy objective, promote its orderly cross-border use.

118. Each jurisdiction would need to decide on the appropriate legislative, regulatory and contractual rules for its rCBDC, having regard to its own legal framework and its rCBDC design and policy aims.

¹⁰⁷ This issue is relevant for not only the participating central banks but also other participants (eg, intermediaries, if any, and end-users). For how to address conflict of laws issues which might arise in a single platform, see above.

¹⁰⁸ For example, in Project Helvetia Phase II (2022), the Swiss National Bank issued a (wholesale) CBDC on a platform operated by a third party (a fully licensed and supervised Swiss central securities depository). From a legal perspective, the wCBDC was not set-up as a new type of central bank money, but rather an alternative representation of traditional reserve balances. Under applicable central banking laws, for such wCBDC to qualify as central bank money and legal tender, the Swiss National Bank was required to retain certain control and monitoring functions over the wCBDC equivalent to those over traditional reserve balances through technical functionalities and contractual arrangements with the platform operator. These included for instance the unilateral legal right and technical ability to order at any time an individual (one participant) or global (all participants) wCBDC settlement stop.

¹⁰⁹ For example, in Project mBridge (2022), settlement finality was achieved through specially developed legal agreements between each central bank and its respective commercial banks, further supplemented by operating terms of the platform tailored on a per-jurisdiction basis.

¹¹⁰ It would have to be decided whether to take a platform view (all involved jurisdictions are relevant) or a transaction view (only jurisdictions involved in the specific transaction are relevant).

119. While this note has focused on some of the most pressing legal issues with rCBDC, it does not cover all potential legal considerations. Considerable further legal work will be needed in each jurisdiction to identify and then address the range of legal issues.

Annex: Expert group members

Chair	Ross Leckow (Bank for International Settlements)
Bank of Canada	Jeanelle Dundas Andrew Kidd Alain Laplante
European Central Bank	Phoebus Athanassiou
Bank of Japan	Masaki Bessho (until Jun 2024) Takahiro Kawakami Shigeru Shimizu (from Jun 2024) Akihiro Yoshinaga
Sveriges Riksbank	Susanne Bohman (as of June 2024) Eric Frieberg (until Feb 2024) Monika Johansson Elsa Themner
Swiss National Bank	Milena Di Cioccio Andreas Josuran
Bank of England	Randip Bains Amy Cheung David Geen Temitayo Shittu
Board of Governors of the Federal Reserve System	Jesse Maniff Andrew Ruben Gavin Smith
Bank for International Settlements	Susanne Bohman (until May 2024) Vincent Carl Jacobsen Jennifer Devlin

This paper has also benefitted from comments received from Simon Gleeson, Rosa Lastra, and Corinne Zellweger.