Central bank digital currencies: system design and interoperability

September 2021

Report no 2
in a series of
collaborations from a
group of central banks

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

This publication is available on the BIS website (www.bis.org).

ISBN: 978-92-9259-510-4 (online)

Contents

1. Introduction and general overview 1

2. System design 2

2.1 Elements outlined 2

"Accounts" and "tokens" in CBDC systems 4

2.2 Possible roles 4

2.3 Considerations 5

2.3.1 Additional access to central bank money 5

2.3.2 Resilience 6

2.3.3 Increased payments diversity 6

2.3.4 Financial inclusion 6

2.3.5 Improving cross-border payments 7

2.3.6 Supporting privacy 7

Privacy and data in CBDC systems 8

2.3.7 Facilitating fiscal transfers 8

3 Interoperability 9

3.1 Interoperability explained 9

3.2 Options 10

3.3 Considerations 10

Interoperability benefits and barriers in CBDC systems 11

4 Concluding thoughts and next steps 12

Glossary 13

References 13

Annex: Expert group members 15

CBDCs would exist in interoperable systems where the multiple roles and responsibilities would need to be coherent and support policy goals. This report outlines the considerations for central banks in designing systems that benefit from private-public collaboration and interoperability. Doing so highlights the importance of payment data and privacy in driving choices on infrastructure architecture, messaging standards and the role of a central bank. The next steps for this work will be to review the impact of financial stability safeguards and user requirements on system designs.

1. Introduction and general overview

This report explores central banks' considerations for designing a potential general purpose (retail) central bank digital currency (CBDC) system. This includes an overview of the potential functions in a broad ecosystem, the different possible roles in a private-public collaboration, how interoperability could be a core feature and a central bank's options in how an interoperable CBDC system could be implemented.

Key messages:

- **The central banks contributing to this report anticipate any CBDC ecosystems would involve the public and private sectors in a balance to deliver the desired policy outcomes and enable innovation that meets users' evolving payment needs**. Depending on the priority motivations for a CBDC, there would be multiple considerations involved in allocating roles individually and collectively, requiring extensive dialogue with users and stakeholders. Yet a theme that cuts through almost every consideration is interoperability. Domestic interoperability would be key to ensuring a CBDC system coexists with other national payment systems and contributes to broader accessibility, resilience and diversity.
- **For CBDC systems, domestic interoperability would need to be sufficient to achieve an easy flow of funds to and from other payment systems and arrangements**. Central banks would have options in how they achieve interoperability, from use of established messaging, data and other technical standards to building technical interfaces to communicate with other systems. Yet barriers to interoperability would likely exist, covering technical, commercial and legal aspects. Dialogue with stakeholders would be key in addressing these.
- **Regardless of the design, developing and running a CBDC system would be a major undertaking for a central bank**. Operating CBDC ecosystem functions would be a significant undertaking and any outsourced functions would need to be carefully managed to deliver public trust in a CBDC system. Likewise, individual and collective oversight of those functions and services provided or operated by private intermediaries would be required.
- **Access to and treatment of payment data would play a significant role in any ecosystem design**. Privacy considerations could create a series of other design and interoperability challenges, ranging from the messaging standards used, how to create incentives for diverse intermediaries to offer services and how to interoperate with traditional systems that require detailed account and transaction information.
- Further exploration will further review the practicalities of interoperability with existing payment systems; while also considering how financial stability safeguards and user requirements (including privacy) might influence the design of a CBDC system that enhances monetary and financial stability, co-exists with robust private money and offers users an innovative and efficient means of payment.

Section 2 sketches the elements, functions and possible roles in CBDC systems as well as considerations for central banks. Section 3 then narrows its focus to interoperability, including a technical introduction, options and considerations. Section 4 concludes and outlines possible next steps.

2. System design

- A CBDC ecosystem would comprise multiple elements and functions. A core ledger with supporting infrastructure and rules would underpin a broader ecosystem of processing infrastructure, processing providers and user services with business and technical rules.
- The central banks contributing to this report anticipate ecosystem functions divided among the public and private sectors in a balance that delivers the desired policy outcome.
- To deliver that outcome, a central bank would have to consider the motivations or goals driving the implementation of CBDC. Yet, in any CBDC system, the central bank would face additional operational or oversight tasks and accompanying challenges regardless of the division of responsibilities among the various actors.

2.1 Elements outlined

A CBDC system would likely comprise similar elements and underlying functions as traditional payment systems, with central banks facing many of the practical policy questions around access, services and structure that they do today (CPSS (2003)). Payment systems comprise an operator and participants as well as the instruments, procedures, and rules for transferring funds (CPMI-IOSCO (2012)). Beyond this "core" system, a broader ecosystem includes end users and technical processing and supporting infrastructure providers as well as contextual legal, supervisory and contractual arrangements exist. These elements and functions are set out in Table 1.

At the centre of any CBDC ecosystem would be a CBDC core rulebook outlining the legal basis, governance, risk management, access and other requirements of participants in the CBDC system. Supporting these rules would be a core technical infrastructure operating a core ledger allowing a central bank to issue, redeem and settle CBDC as well as potential other activities.[1]

Participants in the CBDC system would act as intermediaries between the central bank and end users. Intermediaries could include banks, payment service providers, mobile operators and fintech or big tech companies depending on the access policies set out in the core rulebook. Each use case would follow its own business and technical rules depending on the participants and processing infrastructure involved. These rules would determine how different use cases work, including (eg) initiation, processing, fees and compensations, use of data and data protection. These could include how offline payments are processed and corresponding risks are managed outside the CBDC ledger (all within the scope of any broader requirements set out in the CBDC scheme rules).

Intermediaries would use one or several processing infrastructures enabling payment messages to be processed, reconciled and to access and communicate with the core infrastructure.[2] The intermediaries could be responsible for payment services including: (i) pre-transaction (eg on-boarding, providing access devices and channels); (ii) transactions (eg customer service and support); and (iii) post-transaction (eg advice, statements and billing).[3] Intermediaries would also include the operators of the processing infrastructures as well as the providers of processing services. This broader ecosystem would

[1] For example, monitoring or implementing remuneration and centralised controls and safeguards.

[2] A processing infrastructure could be owned and operated by the intermediary itself or another entity (eg a payment processor). The processing infrastructure could perform (eg) pre-checks (limit checks, funds availability), authentication, authorisation, verification or validation (manage exceptions, restore and correct incorrect transactions, handle offline authorisation limits, biometrics), screening (security and regulatory checks), interaction between intermediaries and between intermediaries/CB, reporting and statistics.

[3] An access device or channel provider could be someone other than an intermediary, eg a point-of-sale terminal provider or a software provider.

be complemented by a legal and supervisory framework and contractual arrangements between end users and their intermediaries. For users and intermediaries to understand this broad ecosystem, a central bank would need to communicate clearly (Box 1).

Elements, functions and roles in a CBDC ecosystem Table 1

Element	Possible functions	Role considerations
Core system		
Core rulebook	The core principles of CBDC transactions/use, outlining the legal basis, governance, risk management, access and other requirements of participants.	The central bank could be a sole operator and/or a broader governance arrangement could include public or industry governance bodies.
Core infrastructure	Issuing, redeeming and settling CBDC on the CBDC ledger and potentially monitoring, safeguard or remuneration implementation.	Issuing and redeeming CBDC would be a core central bank function. Yet some activities could be outsourced and supervised by the central bank.
Broader ecosystem		
Processing Infrastructure	Message preparation, processing and reconciliation Communication with core infrastructure Connectivity with enabling functions (eg digital identity systems, underlying telecoms networks)	A variety of processing infrastructure options could add choice and competition for users but also create complexity. A single processing infrastructure run by the central bank or outsourced to a third party could provide a level playing field for payment and processing service providers.
Processing Services	Payment pre-checks (eg limit checks, funds availability) Authorisation, verification or validation (eg managing exceptions, restoring and correcting transactions, handling offline authorisation limits) Screening (eg security and regulatory checks) Data and analytical services	To encourage innovation and efficiency, a variety and combination of private providers (eg banks, payment service providers, non-bank processors, technology companies, and other entities) could run processing services enabling their own payment services, or those of others.
Payment Services (interaction with end users)	Pre-transaction (eg access device or channel, on-boarding of users) Transaction (eg payment instruction, authentication, customer service and support) Post-transaction (eg payment advice statements and billing)	To encourage innovation and efficiency, a variety and combination of private providers (eg banks, payment service providers) could run payments services and provide user support.
Use case arrangements	A set of business and technical rules determining how a use case works	Responsibilities could fall with the central bank and/or industry governance bodies.

Box 1

"Accounts" and "tokens" in CBDC systems

Many CBDC system design discussions initially drew a distinction between "account-based" and "token-based" CBDCs in the context of how it would be used as a means of payment (CPMI-MC (2018)). However, since the terms "token" and "account" can be used to demarcate different concepts across different fields, there has subsequently been differing usage and interpretations of these terms. For example, "token" is sometimes used in economic literature as shorthand for designs where CBDC has one or more cash-like features (such as representing a bearer instrument and supporting offline or anonymous payments). Elsewhere, in computer science literature, "token" can instead refer to digital access keys or to representations of assets on blockchains.

Central banks engaging in public dialogue and consultation on CBDC would want to avoid confusion, so the terms "token" and "account" may therefore require additional explanation in any communications. For example, "account-based" might be used to refer to a CBDC system where payment involves updating payer and payee balances whereas "token-based" could be used to refer to a system where a record is updated for who holds a particular CBDC representation. Yet as digital systems, these would both require a ledger ie neither would replicate cash-like transfers. Both CBDC systems could also use various means to identify users ie in either approach, payments could be anonymous, pseudonymous or fully identifiable. Finally, these two approaches are technology-agnostic ie they could be implemented based on traditional technology or a distributed-ledger.

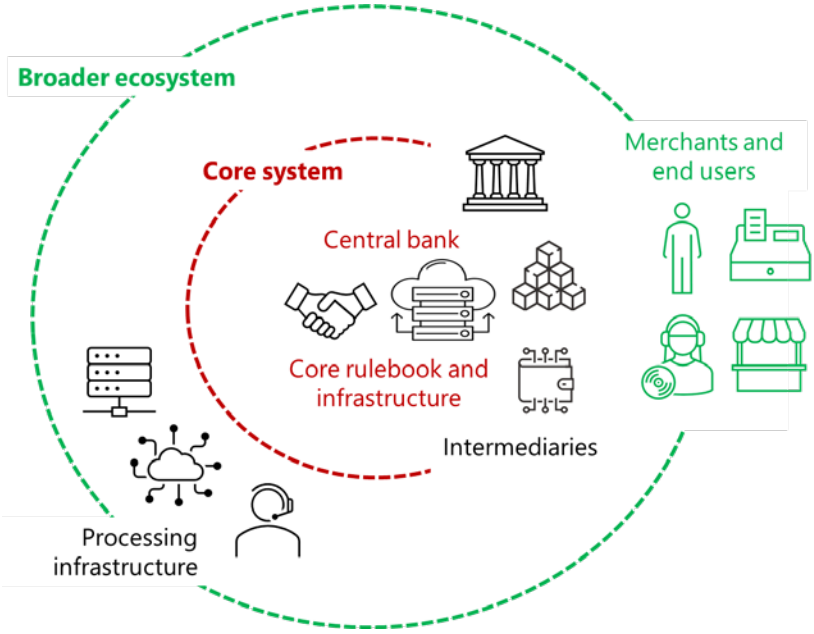
2.2 Possible roles

The functions outlined above could (in most cases) be carried out by different actors of the public or private sector. Central banks would be the only entities entitled to issue and redeem a CBDC and would bear the ultimate responsibility for the design of the CBDC system and the operation/oversight of the core ledger. Therefore, assigning the roles within a CBDC system would likely be the prerogative of a central bank – including the roles it would play as an operator (running a function internally), outsourcer (maintaining responsibility for a function but contracting a specialist provider) or overseer (not performing the function but ensuring that it was carried out effectively and diligently).

Theoretically, a central bank could perform all the functions in an ecosystem, either through directly operating or outsourcing certain functions. For example, a "direct" CBDC system (Auer and Böhme (2020)) could resemble government or post office banking services (Grym (2020)). However, central banks lack experience in customer service and established networks of physical and digital contact points for customers. In the case of a CBDC purely operated by a central bank (potentially with some outsourced elements), everything would need to be set up and (arguably more importantly) maintained and updated, to support users' developing digital payment needs. Although likely unsuitable for the central banks contributing to this report, for jurisdictions lacking adequate private payment provision for the public, a direct system could be appropriate.

The central banks contributing to this report envisage CBDC ecosystems based on a broad public-private collaboration, ie a "tiered" system where some roles would be carried out by the public sector and others by private entities. In an effective system, each actor would collaboratively play the role they are best suited for. Public entities have public policy goals, private entities have shareholders and market-driven goals. A natural split in any tiered CBDC system would be for the central bank to be responsible for the core of the system to the extent that they could steer the system to deliver policy goals and a safe and efficient payment system. Multiple private entities would then act as intermediaries, competing and offering choice within an ecosystem to drive innovation and efficiency (Uchida (2021)). The functions and possible roles are outlined in Table 1 and illustrated in Graph 1.

Illustrated elements, functions and roles in a CBDC ecosystem Graph 1



2.3 Considerations

A central bank would face a significant number of considerations in assigning the functions within an ecosystem. Each function would bring its own unique considerations (eg the entities best placed to carry it out given their incentives and/or technical ability) and fit into a broader consideration (eg how choices fit together to meet the policy objectives for the system).

System designs would likely differ between jurisdictions as central banks make choices that best suit their circumstances. These include motivations previously outlined by central banks, including: (i) continued access to central bank money, (ii) resilience, (iii) increased payments diversity, (iv) encouraging financial inclusion, (v) improving cross-border payments (vi) supporting privacy and (vii) facilitating fiscal transfers (Group of central banks (2020)). Different elements and functions differ in importance across each motivation and bring different broader considerations for a central bank allocating roles.

2.3.1 Additional access to central bank money

To provide additional access to central bank money for the public, a CBDC ecosystem would need to closely define the payment use cases it wants to support (Group of Central Banks (2021b)), including elements applicable to financial inclusion (discussed in 2.3.4 below).

Depending on how broad the use cases in a CBDC ecosystem were, a larger public sector and central bank role in providing services to end users may be required to achieve universal access to central bank money (these considerations are similar to those for financial inclusion, discussed in 2.3.4 below). For some use cases, a central bank could play an operational role beyond the core system, eg through providing processing infrastructure, services and services to end users. Where there were a lack of interest or incentive for private participation in roles beyond the core system, or certain use cases, a central bank or other public body could also consider providing these themselves.

If the central bank were to play too operational or dominant a role in the ecosystem, private intermediary participation could be curtailed with a reduction in the diversity, innovation and efficiency of the system (potentially also giving rise to legal or constitutional questions). To avoid negative outcomes while still maintaining access to central bank money, interoperability with other systems and convertibility with other types of robust private money would be necessary.

2.3.2 Resilience

Enhancing a jurisdiction's broader operational resilience could be achieved through a CBDC system acting as an additional payment method. A CBDC system itself would need to be resilient to technical failure, counterfeiting and cyber risks. And such a system, operated solely by the central bank, with elements independent of pre-existing payment infrastructure, could continue to operate if those other systems fail. Designing a system in this way would, however, be a significant undertaking and the resilience benefits would need to be assessed against the costs in the broader context of the resilience of existing domestic payment systems.

All technical elements of a CBDC ecosystem would need a high level of operational and cyber resilience. And depending on technical designs, the core infrastructure may have to have an even higher standard. Beyond the core system, the broader ecosystem could share processing infrastructure with other payment systems. Yet if this failed or was compromised, it could undermine both system's availability at the same time. Building parallel processing infrastructure to duplicate functionality could add resilience but also costs to users, merchants and intermediaries (potentially even undermining convertibility between a CBDC and other types of money). And finally, to act as an additional payment method if another system failed, a CBDC system would need to be interoperable or substitutable for that system and use cases.

Beyond incorporating stand-alone elements, a CBDC system could also introduce a higher standard of business continuity or cyber resilience for intermediaries providing payment or processing services. However, private intermediaries may not internalise all broader negative impacts from an operational incident (ie they may be likely to invest less in business continuity than is systemically optimal) (CPMI (2018b)). Requirements would need to be set and overseen to ensure high standards. Yet high requirements may also raise costs for intermediaries, reducing competition and innovation.

2.3.3 Increased payments diversity

Payment systems, like other infrastructure, benefit from strong network effects, potentially leading to concentration and/or fragmentation. A CBDC system could avoid these private "winner takes all" networks achieving a monopoly through providing/demanding interoperability between them (Cœuré, (2020)).

In a tiered CBDC ecosystem, the more diverse the private intermediaries were, the more likely there would be overlapping system or network memberships, creating competition, choice for users and efficiency in the system. This would be true for intermediaries in payment services but also potentially for payment processing too (eg where competition between private payment processors were limited, this could erode the opportunities for payment service intermediaries who rely on them).

However, a broad range of intermediaries may also lead to unclear responsibilities, a higher likelihood of failures (operational or financial) and user disruption. Approval processes for new intermediaries or certain services and strong oversight could help mitigate this (although the costs of oversight would increase with the number and diversity of intermediaries).

2.3.4 Financial inclusion

Increasing digitalisation could create financial inclusion issues as barriers around trust, digital literacy, access to IT and data privacy concerns create a digital divide (barriers also applicable to continuing to provide access to central bank money, discussed in 2.3.1 above).

Private payment services intermediaries naturally have an incentive to cater to users likely to generate the most profit. Therefore, an ecosystem in which the public could only access CBDC through private intermediaries might struggle to achieve universal access or services for all relevant use cases. To overcome this, a central bank or other public body (eg a post office or government bank) could offer services, legislation requiring basic access could be proposed and/or incentives for private intermediaries to supply otherwise underserved end users could be introduced.[4]

However, as for any financial inclusion initiative, a broader strategy to tackle the causes of exclusion may be required to realise results. For example, a CBDC would be unlikely to represent a "complete package" of financial services, therefore interoperability with other private savings products, government services or digital identification may be beneficial.

2.3.5 Improving cross-border payments

CBDC systems, through starting with a "clean slate", could reduce some of the frictions in current cross-border payments through interoperating across borders (CPMI (2021)). However, a CBDC would be no different to a traditional payment system in that broader compatibility requirements like consistent technical standards, oversight frameworks, private and public laws and requirements for anti-money laundering and counter terrorism financing, would still be necessary for effective interoperability (Auer et al (2021)). Yet international collaboration, specifically through the G20 "roadmap" to enhance cross-border payments, is actively working on these issues to improve existing payments and CBDC systems of the future (FSB (2020)).

2.3.6 Supporting privacy

Supporting privacy could be a key motivation for CBDC issuance (Box 2). Yet full anonymity is not plausible, as central banks would design CBDC systems to meet anti-money laundering and combating the financing of terrorism requirements (along with any other regulatory expectations or disclosure laws) (Group of central banks (2020)).

The CBDC system design would determine which actors have access to what information. This would include models where a central bank outsources the operation of parts of the core or processing infrastructure. The central bank would have no commercial interest in end-user data and may be better placed than a commercial entity to commit to a minimal use of such data outside payment processing, eg the use of anonymised and consolidated data for macro-economic policy related analysis or use for a system backup.[5] Yet concentration of end-user data may nonetheless raise concerns among the public, even if privacy safeguards were in place. Beyond the central bank, end-user identities could be stored by intermediaries, subject to the rules imposed in the system. These rules would need to be transparent, understood across the ecosystem and flexible enough to respond to developing data regulation in jurisdictions.

Considerations for a central bank regarding privacy include intermediaries' business models and innovation, interoperability and other motivations. Data is rapidly becoming an important part of private sector business models. Higher levels of privacy and restrictions beyond those required by the jurisdiction's data regulation may negatively impact intermediaries' revenue streams and their ability to add new innovative products, potentially reducing the diversity of participants in the system. For interoperability, where other systems require personal information to settle payments, there could be challenges in implementation. Finally, other motivations like use for fiscal transfers or integration in wider governmental systems would require users to share their "CBDC address" with public authorities other than the central

[4] In Europe, legislation has been introduced to create general access to transaction accounts with basic payment functions at banks. An equivalent approach for CBDC services could also be considered.

[5] For example, Auer and Böhme (2021) envisage a CBDC with "hybrid architecture" where the central bank would retain a copy of all user CBDC holdings, allowing it to act as technical backstop to the system.

bank. Digital identity systems could play an important role, yet financial inclusion and universal access to central bank money motivations (including the possibility for use by foreign travellers) could require other identification means even where a digital identity was in place.

Box 2

Privacy and data in CBDC systems

Privacy is an acknowledged fundamental human right in most international instruments, such as the United Nations Declaration of Human Rights (Article 12). In payment systems, privacy requirements can protect against business models that abuse individual data, resulting in unfair business practices like exclusion or discrimination. Requirements can also protect against malfeasance or negligence by counterparties or the operator of a system and against unsubstantiated or unreasonable government surveillance. The ECB's recent public consultation on the requirements of a digital euro shows that privacy was considered the most important feature, subject to restrictions to avoid illicit activities (ECB (2021)).

Restrictions to avoid illicit activities would require the design of a CBDC to consider anti-money laundering and counter financing of terrorism risks (AML and CFT). Financial Action Task Force (FATF) recommendations covering cash or electronic payments could apply to CBDC yet could also bring hurdles in protecting privacy for users. For example, the so-called "travel rule" (FATF (2021)) requires participants' transaction data to be collected and shared along a payment chain (hence "travel"). Outside these requirements, collecting and processing personal data is also subject to country-specific data protection regulations.

In this context, central banks would face three questions regarding privacy: (i) what data is to be protected; (ii) from whom is it to be protected, and (iii) to what degree is it to be protected? Data to be protected could include personal information about the payer or payee or information about the payment itself. Information about the payment could reveal personal information about the payee (eg wealth when buying luxury items or health issues when buying medicine), their relationships or business. This would likely be especially revealing when combined with corroborating data sets. Privacy could be protected from the payment parties (at least with respect to their identities), against the issuer of the money, the payment/network providers/processors, the regulator/supervisor, the government, or other third parties. Regarding the degree of data protection, information could be kept anonymous, pseudonymous, or confidential. For example, anonymous payments would contain no data to identify parties,① pseudonymous payments would contain data that cannot be linked to the identities of the parties and confidential payments would identify the parties but only to a narrow set of recipients. The transparency of the data to these recipients could also be defined further.

Existing retail payment system designs (eg those supporting cards or credit transfers) exchanging originator and beneficiary information at every step in the payment chain could struggle to offer the level of privacy required for a CBDC system without redesign. Central banks face two challenges in this context: (i) building a system with potentially different architecture to support privacy and then (ii) interoperating with existing systems that require personal information to settle payments.

However, new developments in cryptography such as "zero-knowledge proofs", blind signatures, private decentralized networks, offline smartcards and the use of "layered" data management in payment systems are promising and could offer ways to enable a high degree of privacy whilst complying with existing AML and CFT standards. However, not all of them have been subjected to due cryptographic auditing, let alone stood the test of time. Implementing these techniques in CBDC may therefore require a significantly longer timeline.

① Although for a CBDC, full anonymity is not plausible (Group of central banks (2020)).

2.3.7 Facilitating fiscal transfers

A central bank motivated to build a system to better enable fiscal transfers (eg the government assistance payments from some governments seen in the recent Covid-19 pandemic) would need to overcome identifying the recipients of any payments. A system in which the central bank (eg) operated some of the payment processing infrastructure and had complete information about user identities, accounts and balances would make this simple. Yet it would also raise significant privacy concerns (outlined above).

Interoperability with a digital identity system could allay some of these concerns and accommodate a broader tiered system.

3 Interoperability

- Interoperability is a broad term. For a CBDC system, it would encompass characteristics sufficient to achieve an easy flow of funds to and from other payment systems. This would help ensure the coexistence of a CBDC system within a wider payment ecosystem.
- Central banks have options in how they could achieve interoperability, from use of established messaging standards, data and other technical standards, to building technical interfaces to communicate with other systems.
- Significant domestic and international consultation and dialogue to understand the practical impact of any choices would likely be required, both prior to launch and during the life of any CBDC system.

3.1 Interoperability explained

Interoperability is a broad term, potentially incorporating any characteristic of systems that enable payment systems to exchange information.[6] For a CBDC system, sufficient interoperability to ensure an easy flow of funds between payment systems would be a "core feature" and would contribute to the coexistence of a CBDC within a wider payment system (Group of central banks (2020)). This would include a range of characteristics from accommodative technical infrastructure to common legal and regulatory frameworks and data and messaging standards. The essential foundation of interoperability would be "standardisation", which would allow compatibility (Bank of Japan (2021)).

Interoperability between payment systems contributes to achieving adoption, co-existence, innovation and efficiency for end users.[7] It would be key to integrating a CBDC into the broader payments landscape of a jurisdiction and thereby drive end user adoption (both for the public and merchants). Where payment systems fail to interoperate, there is a risk of fragmentation and "closed loop systems" that create risks and user costs from a lack of competition (CPMI (2018a)). As outlined in the considerations for system design above, interoperability would directly or indirectly support most payment motivations for CBDC issuance.

Cross-border and cross-currency payments are inherently more complex than domestic ones (CPMI (2018a)). Interoperability between cross-border CBDC systems would likely face additional challenges and a broader range of considerations than those explored here. However, significant international work is currently underway to improve current and future cross-border payments (CPMI (2021)). The main frictions identified to cross-border payments are high costs, limited access, low speed and limited transparency (CPMI (2020)) and interoperability could help to address these frictions. The central banks contributing to this report are also active participants in this work.

[6] The International Organization for Standardization (ISO) defines interoperability as the "capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units" (ISO (2015)).

[7] Also referred to as "horizontal" interoperability compared to "vertical" interoperability, which is concerned with characteristics that aid integration within a single system.

3.2 Options

Interoperability would be a core feature of any CBDC system and central banks would have options in how it was achieved.

At a basic level, interoperability would involve standards. For payment systems, these would include a range of technical specifications, operational requirements and legal or supervisory accreditation. Standards would include messaging and data (ie how a payment message and the data it includes would be formatted and structured), security (ie the cyber and endpoint security requirements) and others (eg operational processing and opening hour requirements or supervisory obligations). Common standards would allow a reduction of frictions and barriers, arguably necessary for the success of any infrastructure interoperability measure such as an interlinkage or technical interface (Bech et al (2020)). Potential options for CBDC infrastructure interoperability include sharing functions (eg using the same authorisation and clearing providers or using the same digital identity scheme), incorporating settlement (eg one system settling in another) or completely shared processing infrastructure and services outside the CBDC core system.

In all likely CBDC system designs, payments would involve multiple stages, as outlined in the functions described in the previous section. Across stages, including the initiating, authorising, processing and settling payments, different characteristics would be more relevant. Common standards could enhance interoperability across these functions. For example, consistent data standards could reduce costs for intermediaries and enable simpler and more effective implementation of technical interfaces (eg common digital identity schemes could enable more efficient initiation and authorisation and consistent messaging standards could allow simpler clearing and settlement). Likewise, consistent encryption and security standards between systems would allow for greater technical integration.

3.3 Considerations

Deciding on the best way to make a system interoperable would bring a significant number of considerations. As system designs and use cases would differ across jurisdictions, the manner, and degree of interoperability would also differ.

In a domestic context, the characteristics of pre-existing payment systems would likely play a significant role in a CBDC's interoperability. For example, if common technical interfaces and data or messaging standards already existed, adopting these could reduce costs. Yet a CBDC could also be introduced with an explicit policy goal to catalyse a migration of national standards to (eg) an internationally promoted standard. To understand the practical implications of any choices, central banks would likely undertake public and technical consultation, with end-users and providers of payments services. Central banks might also need to consider potential barriers to interoperability in their jurisdictions arising from legal or regulatory issues, technological compatibility and commercial interests (Box 3).

Box 3

Interoperability benefits and barriers in CBDC systems

The Great Baltimore Fire in 1904 destroyed buildings across 140 acres of the city. Fire engines from nearby rushed to help extinguish the blaze but were unable to help, as their fire hose couplings did not fit Baltimore's fire hydrants. In response, national standards in firefighting equipment, ensuring interoperability between hoses and hydrants, were put in place (Cochrane (1966)). Payment system interoperability is arguably less dramatic but is based on the same conceptual foundation – the basis of interoperability is common standards.

Interoperability would be a core feature of a CBDC and would be necessary for integrating into a broader payments landscape and achieving public policy objectives. Interoperability could promote competition between payment service providers, create the conditions for innovation and enhance the operational resilience of a broader national payment ecosystem. Failing to achieve interoperability would risk fragmentation of the payment landscape into closed loops, leading to users and merchants facing costs from multiple memberships of systems with frictions impairing the speed and cost of payments. This would be inconvenient for end-users and socially inefficient.

Effective interoperability would also be key to ensure that CBDC would be an appealing proposition for end-users. It could enable smoother user on-boarding, cashing in and out of CBDC, making payments across systems, "sweeping" (eg where businesses would invest their funds overnight) and integration of CBDC wallets with other devices, services and technology. Without achieving interoperability, CBDCs may struggle to achieve the adoption required to be effective (discussed in Group of central banks (2020b)).

Although interoperability would bring significant benefits, its practical implementation could be difficult and may involve trade-offs and compromise. Barriers would relate to technical, commercial and legal issues. Technical barriers could include: inconsistent standards for message formats, data elements, numbering and coding systems, security protocols, scalability or throughput capacity and opening hours. Avoiding these barriers could involve, respectively: using of common (international) technical standards and/or application programming interfaces; requiring minimally viable security standards or encouraging other systems to adopt stronger security; engaging in early and frequent communication with other systems to estimate volumes and throughput; and establishing rules for CBDC payments initiated during the closing hours of other systems. A broad forum of relevant stakeholders could agree a CBDC's technical specifications and coordinate interoperability issues.

Commercial barriers could include an unwillingness of other systems and/or participants to use the CBDC to protect revenues from existing systems. In response a central bank could incentivise participation in the CBDC ecosystem and engage in early outreach. Lowering costs by avoiding the technical interoperability barriers above could also help.

Legal/regulatory domestic barriers could include differences arising from participant supervisory regimes and compliance requirements as well as settlement finality and consumer protection rules in payment systems. Specifically, if there were different supervisory requirements between a CBDC and other payment systems then there could be insufficient overlap to ensure a smooth flow of funds (assuming a more technical interface were not implemented). Similarly, if know-your-customer, anti-money laundering and counter terrorism financing requirements were higher or differed from existing payment systems, this could add costs to participants. For payment systems, rules on the finality of settlement and consumer protection could differ (eg where one system was net settlement and another was gross settlement and procedures in the event of transaction errors, delays, fraud, theft, or insolvency differed). As for other barriers, early engagement and dialogue would be essential to avoiding issues, in this context, with other public authorities tasked with bank and/or payment service provider supervision, the providers themselves and other payment systems.

4 Concluding thoughts and next steps

Designing an interoperable CBDC system, allocating roles and striking the right balance between the responsibilities of the central bank, the public sector and the private sector would be complex. Many of these complexities would arise from coexisting with a jurisdiction's current payments systems while providing a novel, innovative and efficient service for users. Both would be necessary conditions for the success of a CBDC and would likely change with time. The pace of change in private payments arrangements is increasing (BIS (2021)) and consumer expectations for what constitutes innovative, efficient and convenient payments are not static either.

Any CBDC ecosystem would need to be flexible to accommodate future user demands and interoperate with new and existing systems and arrangements while at the same time safeguarding policy goals and system resilience. Therefore, when allocating roles across a system, a central bank would need the power to change the system, either through how it operates or through using oversight powers. In any CBDC system the central bank would play an important role and would have to allocate resource accordingly. Operating any ecosystem functions would be a significant undertaking and any outsourced functions would need to be carefully managed to ensure resilience and public trust in CBDC as a public good.

To keep up with these changes in a highly technical and practical capacity, central banks issuing CBDCs may need to broaden their skills (Carstens (2020)). And supporting these efforts, a central bank's involvement in private-public payments fora may need to significantly increase. The fora themselves may also need to adapt to incorporate a broader range of issues. For example, personal data governance, with its potentially significant impact on interoperability, user confidence and participant business models, may require central banks to engage in extensive dialogue with a broader set of stakeholders outside the traditional payment ecosystem.

Interoperable system designs would be significantly influenced by idiosyncratic domestic circumstances. This would also be true for the user demands and necessary safeguards that would drive the desirability and policy viability of a CBDC (Group of central banks (2021a and 2021b)). The next steps for this work will include reviewing the practicalities of interoperability with existing payment systems. It will also consider how financial stability safeguards and user requirements (including privacy) might influence the design of a CBDC system that enhances monetary and financial stability, co-exists with robust private money and offers users an innovative and efficient means of payment.

Glossary

Central bank digital currency is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts ie a digital payment instrument, denominated in the national unit of account (Group of central banks (2020)).

Payment systems are sets of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement. A payment system is a financial market infrastructure (CPMI-IOSCO (2012)).

Payment arrangements refer to any network of participants who collaborate to send and receive payments. These can include payment systems but also networks without a formal operator, overarching agreement or a rulebook (eg correspondent banking arrangements or multi-CBDC arrangements (Auer et al (2021)).

Interoperability is the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units (ISO (2015)) and the technical or legal compatibility that enables a system or mechanism to be used in conjunction with other systems or mechanisms without imposing unnecessary costs on the users (CPSS (2007)).

References

Auer, R and R Böhme (2020): "The technology of retail central bank digital currency", *BIS Quarterly Review*, March, pp 85-100.

Auer, R and R Böhme (2021): "Central bank digital currency: the quest for minimally invasive technology", BIS Working Papers, no 948, June.

Auer, R, P Haene and H Holden (2020): "Multi CBDC arrangements and the future of cross-border payments", *BIS papers*, March.

Bank of Japan (2021): "Standardization in Information Technology related to Digital Currencies" *Payment and Settlement Systems Report*, Annex, June.

Bech, M, U Faruqui and T Shirakami (2020): "Payments without borders", *BIS Quarterly Review*, March 2020, pp 53–65.

BIS (2021): "CBDCs: an opportunity for the monetary system", *Annual Economic Report*, Chapter 3, June.

Carstens, A (2020): "Central bankers of the future", Speech at the Deutsche Bundesbank's internal discussion series on "Digitalisation and central banking – Is there a fundamental change under way?" December.

Cœuré, B (2020): "CBDCs Mean Evolution, Not Revolution", Op-ed for *CoinDesk* as part of the DC Fintech Week, October.

Cochrane, R C (1966): Measures for Progress – A History of the National Bureau of Standards, January.

Committee on Payments and Market Infrastructures (2018a): *Cross-border retail payments*, February.

Committee on Payments and Market Infrastructures (2018b): *Reducing the risk of wholesale payments fraud related to endpoint security*, May.

Committee on Payments and Market Infrastructures (2020): *Enhancing cross-border payments: building blocks of a global roadmap – Stage 2 report to the G20,* July.

Committee on Payments and Market Infrastructures (2021): *Central bank digital currencies for cross-border payments*, July.

Committee on Payments and Market Infrastructures and Markets Committee (2018): *Central bank digital currencies*, March.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions (2012): *Principles for financial market infrastructures*, April

Committee on Payment and Settlement Systems (2003): *The role of central bank money in payment systems*, August.

Committee on Payment and Settlement Systems (2007): *New developments in clearing and settlement arrangements for OTC derivatives*, March.

European Central Bank (2021): *Eurosystem report on the public consultation on a digital euro*, April.

Financial Action Task Force (2021): *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation – The FATF Recommendations*, June.

Financial Stability Board (2020): *Enhancing Cross-border Payments: Stage 3 roadmap*, October.

Group of Central Banks (2020): *Central bank digital currencies: foundational principles and core features*, October.

Group of Central Banks (2021a): *Central bank digital currencies: financial stability implications*, September.

Group of Central Banks (2021b): *Central bank digital currencies: user needs and adoption*, September.

Grym, A (2020): "Lessons learned from the world's first CBDC", *Bank of Finland Economics Review*, August.

International Organization for Standardization (2015): ISO/IEC 2382:2015: *Information technology – Vocabulary*

Uchida, S (2021): "Opening Remarks at the First Meeting of the Liaison and Coordination Committee on Central Bank Digital Currency", March.

Annex: Expert group members

Chair	Cecilia Skingsley (Sveriges Riksbank)
Bank of Canada	Rakesh Arora Ram Darbh Sriram Darbha Scott Hendry Francisco Rivadeneyra Dinesh Shah Jeff Stewart
European Central Bank	Maria Tereza Cavaco (Portugal) Eric Faber (Netherlands) Aleksi Grym (Finland) Hannes Hermanky (Austria) Manuel Marques (Spain) Sergio Gorjon Rivas (Spain) Giorgia Rocco (Italy)
Bank of Japan	Masaki Bessho Junichiro Hatogai Masashi Hojo Masahiro Katsuragi Yutaka Soejima Keiko Sumida
Sveriges Riksbank	Carl Andreas Claussen Anders Mölgaard Pedersen Björn Segendorf Ian Vitek
Swiss National Bank	Petra Gerlach Basil Guggenheim Christina Kessler Thomas Moser
Bank of England	Paul Bedford Rachel Greener Richard Lewis Tom Mutton Laurie Roberts Simon Scorer
Board of Governors of the Federal Reserve System	Jillian Butecalli Jim Cunha (Boston) Jorge Herrada Alex Lee (New York) Paul Wong
Bank for International Settlements	Raphael Auer Codruta Boar Henry Holden Ayu Kinanti