Central Bank Digital Currencies (CBDCs) and democratic values

Please cite as: OECD (2023), *Central Bank Digital Currencies (CBDCs) and democratic values,* OECD Business and Finance Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/f3e70f1f-en.

Discussions on Central Bank Digital Currencies (CBDCs) have so far mostly focused on the potential risks that these currencies could represent for financial intermediation and financial stability. It is important, however, to also consider how they could contribute to the welfare of citizens, and how they can be leveraged to help uphold certain democratic values. This paper explores how the design and implementation of CBDCs can help countries mitigate threats to individual liberties and human rights, as well as promote the equitable treatment of citizens, the protection of privacy, and citizens' trust in central banks. The sound governance architecture of CBDC systems at the national and international level can further support these objectives.

Table of contents

FIGURES

TABLES

Acknowledgements

This report has been prepared by Iota Kaousar Nassr under the supervision of Fatos Koc and with oversight from Serdar Çelik of the Capital Markets and Financial Institutions Division of the OECD Directorate for Financial and Enterprise Affairs. Liv Gudmundson and Eva Abbott provided editorial and communication support.

The report supports the work of the OECD Committee on Financial Markets chaired by Aerdt Houben. The report was discussed by the Committee on Financial Markets in April 2023 and has been declassified on 16 June 2023.

The authors gratefully acknowledge valuable input and constructive feedback provided by the following individuals and organisations: Béranger Butruille, Banque de France; María Antonieta Campa Rojas, Banco de México; Bilgen Cebir Benli, Ministry of Treasury and Finance of Türkiye; Lia Cruz, European Central Bank; Jean Dalbard and Arthur Frappereau, Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique (Direction Générale du Trésor), France; Juan Fernando Gongora Sabogal, Superintendencia Financiera, Colombia; Eleftheria Kostika, Bank of Greece; Nadia Linciano, Commissione Nazionale per le Societa e la Borsa (CONSOB); Adam Głogowski, National Bank of Poland; Giuseppe Grande, Silvia Vori, Ilaria Supino and Giuseppe Ferrero, Banca d'Italia; Tetsuro Hanajiri, Bank of Japan; Irina Mnohogheitne, Bank of England; Josef Mládek Ing., Ministry of Finance of the Czech Republic; Borut Poljšak, Bank of Slovenia; Paull Randt and Peter Grills, US Treasury; Isabel Torre Rodríguez, Banco de España; Gian Paolo Ruggiero, Ministry of the Economy and Finance of Italy; Mai Santamaria, Department of Finance, Ireland; Yoav Soffer, Amir Moshe and Merav Shemesh, Bank of Israel; John Kiff and Josiah Hernandez; as well as Giuseppe Bianco, Francesca Casalini, Miles Larbey, Rob Patalano, Nayana Satpathy, Matthew Soursourian and Seohyun Kim from the OECD.

1 Introduction

Central Bank Digital Currencies (CBDCs) are digital representations of sovereign currency that is issued by a jurisdiction's monetary authority and appears on the liability side of the monetary authority's balance sheet.[1] CBDCs can be broken down into retail CBDCs, which are broadly available to the public for general-purpose use, and wholesale CBDCs, which are limited to a set of pre-defined user groups, typically financial institutions to settle large value transactions.[2] **This report focuses primarily on retail CBDCs and, unless otherwise specified, any reference to CBDCs corresponds to retail CBDCs.[3]**

Today, 94 central banks are exploring CBDCs, and more than a quarter of them are developing or running concrete pilots or other technological experiments of retail and/or wholesale CBDC issuance, with different motivations underpinning such experimentation. CBDCs have been fully launched in three countries, while pilots of CBDCs are running, or have been run, in five jurisdictions. Sixteen jurisdictions have started or completed technical proof-of-concept (PoC) work.[4] In advanced economies (AE), central banks mainly focus on ensuring continuing central bank money access in light of a significant decrease in the retail cash usage, and monetary sovereignty, against a backdrop of increasing competition from private sector digital payment platforms, and the emergence of stablecoins and other crypto-assets. In emerging market and developing economies (EMDE), central bank CBDC exploration tends to be driven by financial inclusion motivations, reducing costs associated with physical cash, increasing payment system efficiency, and strengthening financial integrity. Wholesale CBDC exploration by both AE and EMDE central banks is predominantly focused on cross-border payments efficiency, while in the case of AE it is also focused on facilitating cross-border wholesale digital asset settlement. Cross-border functionalities have recently been explored for retail CBDC as well (BISIH, 2023[1]).

The discussions around CBDCs are intensifying and the feasibility of issuing digital public money is increasing. Given the central role that a possible CBDC arrangement would play in the structure and functioning of the financial system, it is increasingly important to consider how the design choices of such instruments could contribute to citizens' welfare and abide by democratic values and principles.

CBDC design and/or implementation choices can guard economies against threats to the following four democratic values discussed in this paper: civil liberties and human rights protection; equitable treatment of citizens (which in this case involves availability, accessibility and affordability of CBDCs); protection of

[1] According to the Bank for International Settlements (BIS), a CBDC refers to a digital payment instrument, denominated in the national unit of account, which is a direct liability of the central bank, like cash (Group of Central Banks, 2020[55]).

[2] It should be noted that both retail and wholesale CBDCs are being tested for cross-border use cases.

[3] Wholesale CBDCs may not be available directly to citizens, depending on the design. However, there are still implications comparable to the ones discussed here for retail CBDCs, for example around affordability; accessibility, level playing field and open competition; security and operational resilience; and overall trust of users.

[4] CBDCs have been fully launched in three countries: the Bahamas (the Sand Dollar), Jamaica (Jam-Dex) and Nigeria (e-Naira). Pilots of CBDCs are running, or have been run, in five jurisdictions: China (e-CNY), Eastern Caribbean Economic and Currency Union (DCash), Ghana, India, and Uruguay. Sixteen jurisdictions have started or completed technical experimentation, including the Euro Area (Digital Euro), Japan, Korea, Russia, Sweden, and the United States.

privacy; and protection of citizens' trust in central banks/government (through security and operational resilience of CBDC systems, but also overall, by protecting the abovementioned values). Sound governance architectures of CBDC systems at the national and cross-border level could support these objectives so that CBDCs continue to abide by these democratic values, while balancing possible trade-offs with other core policy objectives, such as transparency and the need to defend the financial system from abuse and preserve its integrity.[5]

Box 1.1. Scenarios under which CBDCs could undermine democratic values

Several scenarios of possible negative effects of a CBDCs issuance on democratic values have been considered for the elaboration of this report and have motivated the analysis therein.

Under such scenarios, CBDCs could enable governments to abridge civil liberties and human rights, using CBDC rails as a means to censor individuals and exert control over CBDC users; or as a way to exert control over individuals' transactions in what is described in the report as 'digital authoritarianism'. Authorities could censor users and transactions without due process or recourse. Such risks could be exacerbated in times of heightened political volatility, when governments may try to use CBDCs to enforce domestic political discipline.

The equitable access of citizens to central bank money could be undermined by a decreasing availability of cash given the possible inability or unwillingness of some parts of the population to use digital forms of central bank money. Similar risks would arise in a scenario whereby CBDCs are not affordable by citizens leading to exclusion, or equally where a level playing field and open competition among service providers is not preserved.

Such scenarios also involve the possible use of CBDCs as a surveillance tool, given that they give access to heightened levels of information about users, including transaction and account level data. At the extreme, CBDCs could give governments the ability to monitor and track all transaction and other financial activity details of users, and also the possibility to exert greater control over private transactions. Under such scenario, and depending on the design, banks, Payment Service Providers (PSPs) and other intermediaries that are part of the CBDC ecosystem could also have this monitoring ability.

Overall, any lack of trust by users could stimulate part of the population to opt out of formal financial systems under such scenarios. Inadequate security and/or operational resilience of a CBDC could damage user trust in this system, especially given the importance of technological infrastructure in this form of public money. Risks includes, for example, cyber-attacks, electronic counterfeiting and fraud. Lack of trust for any of the abovementioned reasons under all scenarios examined could undermine the reputation of the central bank issuer, with widespread repercussions.

The use of technological innovation could facilitate the incorporation of democratic principles in the design of CBDCs. The technology alternatives available and so far considered to underpin CBDCs do not preclude any of the democratic value objectives. Ultimately, it is the policy decisions around CBDC design and governance that will allow for democratic values to be respected and incorporated precisely 'by design'. Indeed, technological advances can actually enable the alleviation of some of the characteristics that may appear to be constraining the respect of such values, while they can also offer solutions to possible trade-

[5] Similar human-centric values are embedded in the OECD Recommendation of the Council on Artificial Intelligence (OECD, 2019[70]). The Recommendation prescribes that AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.

offs between policy objectives (e.g., privacy and financial integrity). FinTech innovation could drive progress in financial inclusion, particularly in EMDEs, by enhancing competition through the entry of new types of providers or business models. In essence, some innovation could benefit the integration of democratic principles into CBDC, while at the same time some tech innovations may erode or harm democratic principles, and for this reason design and governance of CBDCs will be critical.

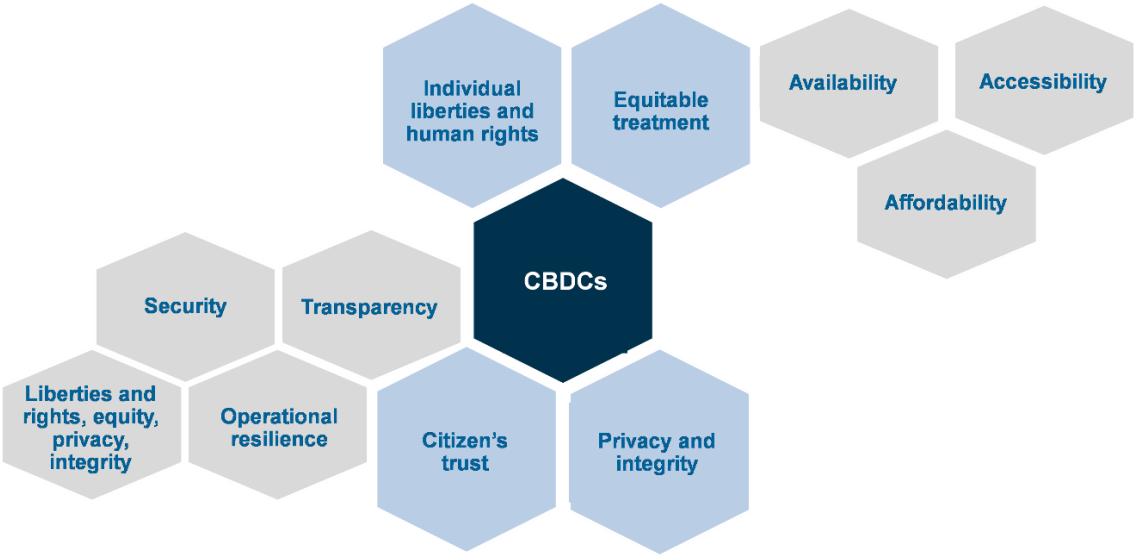
Perhaps the most important decision that will allow a CBDC to abide by democratic principles is the fundamental decision about issuing a CBDC. Any such policy decision would need to make sense for the citizens who will rely on it in the first place, which includes citizens' trust in the instrument. A CBDC would need to be carefully designed and implemented to reflect the core values of the citizens it will serve, avoid unintended or unexpected societal consequences and ensure that trust in it is earned, secured and maintained.

2 Democratic values in CBDC design and implementation

As part of the monetary system, CBDCs represent public goods. The widespread adoption of CBDCs, should it happen, could represent a significant change in the way societies engage with, circulate, and exchange money. In light of efforts at many central banks to develop CBDCs, attention needs to be drawn to the major design and implementation characteristics that will promote CBDCs that abide by democratic values. Such common values include individual liberty, the values of democracy, the rule of law and the defence of human rights (OECD, 2021[2]). In particular when it comes to the digitalisation of our societies and economies, the OECD Council in its Declaration on a Trusted, Sustainable and Inclusive Digital Future recognised both the immense potential of digitalisation to contribute to inclusive economic and social prosperity and well-being, and the significant challenges, risks and potential harms that may emerge as a consequence, with OECD Members reaffirming their commitment to advance a human-centric and rights-oriented digital transformation (OECD, 2022[3]).

This report describes major design attributes and policy-related choices that could help support democratic values are reflected in the design and implementation of CBDCs. These are grouped into four main areas of focus: (i) civil liberties and human rights; (ii) equitable treatment: availability, accessibility and affordability; (iii) privacy and integrity; (iv) trust: including security, transparency, operational resilience, as well as the protection of the abovementioned values (Figure 2.1). The chapter also discusses trade-offs between some of these principles and other policy objectives, for example enhanced privacy protection against objectives of financial integrity (including AML/CFT).

Figure 2.1. Democratic values for the design and implementation of CBDCs as defined in the report



2.1. Civil liberties and human rights

CBDCs design and usage could be considered in accordance with civil liberties and human rights, such as those protected by OECD member constitutions, and outlined in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (United Nations, 1948[4]; 1976[5]). CBDC design could be supportive of human rights protection, provided it does not give room to governments to abridge civil liberties and human rights, for example by using CBDC rails as a surveillance tool; as a means to unjustly censor individuals and exert control over CBDC users; or as a way to exert greater control over individuals' transactions. Such risks could be exacerbated in times of heightened political volatility in case of authoritarian regimes that deviate from the democratic values outlined in this paper, where governments may try to use CBDCs to enforce domestic political discipline. Depending on the design of the CBDC model, private financial institutions, payment service providers (PSPs) and other intermediaries that are part of the CBDC ecosystem could also have this ability to exert control.

CBDC designs could consider ways to support the protection against inappropriate surveillance and coercion or other forms of 'digital authoritarianism'. The latter involves the use of digital technology to enable the repression of citizens and/or to suppress the rights of specific groups or individuals (OECD, 2021[4]). Protection against digital authoritarianism could be achieved *inter alia* by incorporating privacy by design (see Section 2.3) and by considering limits to the programmability of money.

One of the risks posed by CBDCs for society is their potential use as surveillance tools, given potential access to heightened levels of information about users, including transaction and account level information. At the extreme, CBDCs could give governments the ability to monitor and track all transaction and other financial activity details of users, and also the possibility to exert greater control over private transactions. Authorities could unjustly censor users and transactions without due process or recourse. Depending on the design, banks, PSPs and other intermediaries that are part of the CBDC ecosystem could also have this monitoring ability (European Commission, 2022[5]). The collection and storing of personal and transaction information increases reputational and cybersecurity risk, as in the case of a hack. The leakage of personal information could lead, in the most extreme case, to financial losses that the central bank and/or its agents may be obliged to cover. Moreover, in a scenario in which CBDCs are used for large-scale control of monetary transactions, CBDCs could become an instrument of control and social profiling, biased and discriminatory treatment of users and possible human rights abuse.

Democratic nations may wish to avoid arbitrary blocking or control over private transactions and protect the rights of their citizens using CBDCs, while allowing for policy objectives such as AML/CFT controls to be achieved. This raises the issue of programmability of money, including conditionality of money, built into CBDC design by the central bank (and/or the government), and the possible limits of these, to prevent the issuer from controlling payments going to certain specific individuals on political, social or arbitrary grounds. In contrast, programmability that involves due process and the appropriate legal exercise of state power would need to be subject to the same democratic limitations and obligations that apply to other coercive functions (e.g., for financial integrity purposes in case of illicit finance).

Additionally, a differentiation may be useful between programmability of money (which corresponds, for example, to the imposition of limits on how money can be used, for how long etc.) and programmability of payments (which corresponds to automated payments triggered by defined events, which is useful for example for micropayments cases). In particular, arbitrary control over private transactions or other power over citizens using CBDCs as a means of payment may need to be avoided. Examples of such control may include *inter alia* limitations set by the CBDC issuer on where, when or to whom citizens can pay with a CBDC, with a view to avoid the potential use of programmability to yield punitive control power over users, unless such limitations are of payments that are in breach of illicit finance controls. Users, on the other hand, can decide to authorise payments where pre-defined conditions of their own choosing are met (Panetta, 2023[6]). However, there are clear cases where programmability is identified as a positive design choice, such as in AML/CFT controls (e.g., programmable illicit finance controls).

Although programmability could enable government or central bank-initiated programmable money that works only in certain ways, this would work against policy objectives of providing uniform CBDCs to citizens and promoting user trust. Payments programmability on the other hand, controlled by the users, could provide enhanced functionality for users to set rules on their payments. In some cases, it is envisaged that Payment Interface Providers and External Service Interface Providers could implement such programmable functionalities themselves, but they would require user consent and not be at the issuer's direction (Bank of England and HM Treasury, 2023[7]).

In terms of implementation, governance arrangements of CBDC systems would need to be considered, incorporating appropriate oversight and accountability mechanisms so as to promote the safeguarding of civil and human rights. CBDCs can maintain privacy through central banks not having access to CBDC users' personal data, which would instead be managed by private-sector wallet providers (subject to appropriate data protection – and, as is the case today with private forms of digital money such as bank accounts, law enforcement agencies and other competent authorities could only access the personal data held by wallet providers where there is a fair and lawful basis). Technical protections could be incorporated as one of the ways to prevent the use of CBDC in ways that violate civil or human rights, primarily through the protection of personal data. Clear assignment of accountability for the protection of users' data as well as transparency on what kind of information will be accessed, how it will be used and secured, are some of the possible governance safeguards with regards to privacy protection (see Section 4.3). Appropriate limitations to the level of programmability features of CBDCs could help prevent these instruments from being used to exert punitive control power over the end-user for political or other reasons.

The negative environmental impact of some CBDCs may also infringe the rights of citizens in many jurisdictions. As such, the choice of the underlying technology could have implications for the environmental footprint of users and could be examined also through the sustainability lens. For example, the consensus mechanisms that some distributed ledger technology networks use to validate transactions are inefficient from an environmental point of view, as they require a large amount of energy (Panetta, 2022[8]; OECD, 2022[9]).

2.2. Equitable treatment: availability, accessibility and affordability

Central bank money serves as the foundation of the financial system and the overall economy (Board of Governors of the Federal Reserve System, 2022[10]). Global continued availability by the issuing institution and universal equal accessibility for all citizens to a digital version of sovereign currency are both prerequisites for a CBDC to promote the equitable treatment and protect the rights of all individuals. For this to happen, no undue restrictions should be imposed related to user profiles and/or conditions to the use of CBDCs by any and all citizens.

When introducing CBDCs, issuance and availability of physical cash would need to be protected as one of the ways to support that those not able to use CBDCs can still enjoy the benefits of access to physical form of public money. Authorities would need to avoid negative implications associated with a decreasing availability of public money to all citizens, including those who may not be able to use a digital form of currency or those who do not trust the use of digital means for payments. The parallel continuation of physical cash availability to the general public, even in economies where cash usage popularity is in decline, could safeguard the availability of central bank money of some form for all citizens. Indeed, CBDCs would need to be considered a means to expand safe payment options, not to reduce or replace them (Board of Governors of the Federal Reserve System, 2022[10]). It should be also noted that physical cash remains a major vector of financial inclusion, including in the most advanced economies, as it is still widely used for peer-to-peer (P2P) and point of sale (POS) transactions. More generally, if a CBDC is issued, there should be no policy discrimination against any other legitimate payment form.

Difficulties in accessibility can be more prominent in certain segments of the population who already face barriers to digital financial inclusion, such as the elderly or people with disabilities. Continuous availability of physical cash in parallel to a CBDC could be one of the ways to support accessibility for parts of the population with low level of trust for digital payments and where technical upskilling would be more challenging if the design involves the use of smartphones or other digital interfaces (e.g. the elderly).[6] This could include, for example, the implementation of offline functionalities that can allow some payments to be made without internet access, although with limitations both at the technical and at the regulatory levels (see Box 2.1). Offline functionalities may also play a greater role in ensuring that a CBDC can be used in remote geographical environments with poor connectivity. The digital divide also applies to disabled people, and the design of CBDCs could incorporate alternatives and features that will make their access equally easy for people with disabilities such as reduced mobility, intellectual disabilities or auditory or visual impairments.

Equity vis-à-vis public goods means that, to the extent possible, all citizens receive equitable treatment with regards to their CBDC experience, and this concerns gender disparities; digital access divides; vulnerable parts of the population likely to face exclusion (e.g., elderly); or those without formal proof of identity. Lack of a basic technical proficiency or financial literacy skills may also restrain individuals' ability to use CBDCs, particularly within the above parts of the population. Policies and strategies promoting financial education for digital financial products are therefore of paramount importance as a way to mitigate such impediments to accessibility of CBDCs by all citizens (OECD, 2018[11]). Identification is foundational to all AML/CFT controls and KYC is expected to be a pre-requisite to onboarding users to any CBDC system. When it comes to citizens lacking formal proof of identification, a mix of technical and policy solutions could support access to identification, digital or otherwise, to enhance access to CBDC systems.

Universal accessibility would also need to be safeguarded at the level of third-party participants or digital providers or operators participating in two-tier CBDC models[7] (see Annex A). Central banks that have launched, piloted, or are in the advanced stages of research have focused on two-tier CBDC models (see Annex A). Given the central role of third-party private sector participants in two-tier CBDC architectures, it is important that such parties provide for equal and universal accessibility of central bank money to all citizens, potentially through a relevant commitment in their obligations for participation in the CBDC system which, for example, ensure they do not cause undue risks to financial stability.

In parallel to universal accessibility, CBDCs should also maintain a level playing field and open competition among service providers. Any CBDC services provider, subject to appropriate qualifications, should be allowed to compete on a level playing field vis-à-vis the CBDC issuer. The equitable treatment of intermediaries, whether domestic or foreign, should be promoted alongside the equitable treatment of end-users.

[6] Similar considerations apply to non-CBDC digital payments.

[7] Two tier models involve private-sector partners - payment service providers (PSPs) - and can be hybrid models or intermediated models. In hybrid models, the private sector PSPs would provide user facing services, while the central bank would be responsible for recording individual users' balances (potentially pseudonymously). In intermediated models, the central bank would only record wholesale balances, with PSPs recording individual user balances (Auer and Böhme, 2021[66]).

Box 2.1. Offline accessibility of CBDCs

In many regions, internet or even mobile connectivity cannot be taken for granted, so offline functionalities may be necessary for a resilient CBDC system, complementing other initiatives as an additional option for financially excluded groups. While challenging to implement, this could be valuable in remote areas or for users with limited internet access (Bank of England and HM Treasury, 2023[7]). The World Bank Findex Database shows that 75% of the world's low-income population does not have internet access. In some cases, non-internet-enabled mobile phones may still allow for the use of a CBDC that requires connectivity (Sarmiento, 2022[12]). However, if financial inclusion is a motive for issuing CBDC, even a CBDC based on a basic mobile phone could be inaccessible to many.

A number of offline technology options are already available and allow for the verification of the availability of funds and the validation of transactions without the need to check in with an online ledger (Kiff, 2022[13]). Existing applications tested include offline platforms that piggyback on text-based, non-internet-enabled mobile phones, known as "feature phones," and costing as little as USD 5. Some systems, for example, involve low-cost devices attached to the phone's SIM card, noting that even in low-income countries, 66 percent of adults own at least such a phone. In 2017–18 the Central Bank of Uruguay conducted a successful six-month test of a CBDC that users could access using feature phones.

The Central Bank of Ghana has been testing a card-based CBDC platform that allows for unlimited consecutive offline transactions using an (offline) intermediary device like a smartphone (Bank of Ghana, 2019[14]). This stored-value card (eCedi) is configured to allow for unlimited consecutive offline transactions but uses an intermediary device. eCedi can be used by anyone with either a digital wallet app or a contactless smart card that can be used offline. It should be noted, however, that offline payments, where transactions occur with both parties disconnected from the network, come with an increased risk of double spend. Such risk of double spend might be reduced by a combination of policy (e.g., limits for consecutive offline payments, local recording and online reconciliation of offline payments) and technology controls (secure hardware and potential cryptography mechanisms). These approaches require further analysis and experimentation to determine their viability and appropriateness (Bank of England, 2023[15]).

Providing offline functionalities would be consistent with democratic values in the context of facilitating financial inclusion and equitable access. Offline functionalities at the implementation of CBDCs could be one of the tools to address digital access divides mentioned above, by allowing access to citizens without smartphones or use of advanced technology means and while being device agnostic. The use of accessible POS devices is another example of ways to ease transactions with near-field communication connections (NFC) (AFI, 2022[16]). Low-cost, non-internet enabled 'feature phones' could be another way to address these parts of the population and have indeed been used in CBDC experimentations (see Box 2.1 for other examples).

Offline capabilities could also reduce CBDC dependence on the quality and availability of mobile and broadband networks, and round-the-clock availability of electricity (Auer et al., 2022[17]). Offline accessibility would likely be indispensable when CBDCs are meant to serve in times of crisis such as natural disaster or war, which may cause widespread disruption in the payment infrastructure, such as in the event of an earthquake or tsunami. It has to be noted, however, that in the case of offline payments, it is difficult to design a solution that would allow one to carry out an unlimited number of consecutive offline transactions[8], while at the same time promoting the security of the system (e.g., ensuring spending does

[8] Offline solutions require a periodic connection with the CBDC infrastructure in online mode.

not exceed available funds and that AML/CFT controls are not compromised). In addition, offline payments significantly increase the risk of stability and integrity of the CBDC system (e.g., risk of double spending, see Box 2.1).

There are many parameters involved in the objective of equal treatment, and affordability of public goods, is one of the most difficult ones to weigh up. Although central banks operate on a cost recovery basis and do not apply mark-ups, the affordability of CBDCs cannot be taken for granted, because most experimentations of CBDCs rely on an intermediated architecture, which involves private third-party service providers. On the one hand, it could be conceivable that a lower cost system based on CBDCs and digital wallets could provide lower cost access, particularly to the benefit of the unbanked parts of the population. The primary technical and operational costs involved in a CBDC include *inter alia* the costs involved in developing the CBDC architecture and the costs of managing the circulation of a CBDC, including human resources, infrastructure and information system costs, security and property for each of the issuer and user. On the other hand, whether CBDCs ultimately prove to be lower cost than current payment solutions will depend on design, distribution, and other policy choices (Box 2.2).

Box 2.2. CBDCs and financial inclusion

Financial inclusion is often cited as one of the main objectives of CBDC exploration, particularly in EMDEs or other countries with underdeveloped financial systems, low financial system penetration, or low access to high quality affordable financial products and services that fit user needs. Central banks see CBDC as a potential tool to promote financial inclusion if this goal features prominently in the design from the get-go (Auer et al., 2022[17]). CBDC introduction in such cases has the potential to improve financial inclusion and ultimately promote economic and social prosperity and well-being. Financial inclusion barriers can include high costs of being banked (fees and minimum balance and financial history requirements), a lack of affordable and/or reliable electrical and/or digital connectivity infrastructure, limited access to mobile phones and/or banks, distrust of financial service providers, lack of personal identity documentation, digital and financial illiteracy, accessibility challenges, and social or cultural barriers.

CBDC design can address some but not all accessibility constraints related to digital financial services. CBDCs are likely to remain limited by poor electricity coverage, access to CBDC-enabled devices and limited cash-in and cash-out infrastructure, a key prerequisite for driving the adoption of digital payment instruments (AFI, 2022[16]). CBDC issuance would also not itself directly address the challenges faced by people with low levels of digital literacy.

Lack of formal proof of identity is a barrier to the financial inclusion benefits of CBDCs, as KYC is expected to be a pre-requisite to onboarding users to CBDC systems. A mix of technological advances and policy solutions could help make CBDCs available to people without formal identification (e.g., Digital IDs). Regulatory provisions and policy objectives related to customer due diligence will play an important role in determining the impact that CBDCs could have on financial inclusion.

2.3. Privacy

As early as 1980, OECD Members established that citizens' privacy is a key element that underpins safety, dignity, freedom of thought and expression (OECD, 1980[18]). Different forms of money differ in terms of their degree of privacy. Cash, found on the one extreme of the spectrum, is the most private form of money. Digital payments, like debit and credit cards, bank account transfers, and mobile money, are significantly less private. To mitigate illicit finance risks, KYC measures are necessary to open bank accounts and,

ultimately, to conduct transactions. Confidential KYC and transaction data is shared with banks, credit card companies and other intermediaries involved in the transaction process of digitally enabled payments.

While CBDCs could be used for extensive data collection around private transactions, their design could incorporate privacy and disassociability. Disassociability is an important safeguard in the design of CBDCs and refers to the processing of data or events without association to individuals or devices beyond the operational requirements of the system (Nadeau, 2020[19]). In terms of privacy, the design could consider allowing only for the collection of data that is strictly necessary for advancing CBDC system policy objectives. This includes information necessary to promote AML/CFT compliance obligations and mitigate illicit finance risks. The design of CBDC could consider offering at least the same data privacy safeguards currently required of debit and credit card issuers without compromising AML/CFT compliance (see, for example, data privacy obligations for PSPs and other intermediaries in data-sharing frameworks in OECD countries (OECD, 2023[20]).

Authorities will need to consider the dependencies of potential tensions between access to user information to meet important public policy objectives like AML/CFT compliance, preventing tax evasion or guaranteeing sanctions compliance, and supporting user privacy (Panetta, 2023[6]). In addition to rigorous standards of privacy, accountability for the protection of users' data and transparency of how information will be secured and used are essential for CBDCs to command trust and confidence (G7, 2021[21]). Privacy options and design alternatives are being debated in many economies, in order to protect users' right to privacy, while preserving compliance with regulations – in particular around AML/CFT checks. A risk-based approach could be considered, whereby small transactions could require the collection of less data.

The Bank of England in its CBDC consultation paper notes the Bank would not have access to users' personal data, intermediaries' access to users' personal data would be subject to the existing data protection regime, and law enforcement agencies and competent authorities could only access digital pound data where there is a fair and lawful basis (Bank of England and HM Treasury, 2023[7]).

In terms of privacy options, the lowest degree of privacy would involve a design wherein all onboarding/KYC and transaction data are visible to the central bank. The second lowest degree of privacy would involve transparency and visibility of the above data to the intermediary only. On the other end of the spectrum, no data is visible to any third party or the central bank itself, i.e., full anonymity, which is not a desirable feature, as this would make it impossible to control circulation and to prevent money laundering. It would also impede regulation and enforcement activities. Instead, a model of 'selective privacy' involves a higher degree of privacy for low-value / low-risk payments, involving simplified checks (e.g., specific wallet with lower requirements during onboarding). Under this model, higher-value transactions would remain subject to standard controls (ECB, 2022[22]).

Built-in protections and design choices could ensure that a degree of privacy protection is included by design and by default. Privacy by design involves taking privacy into account from the conception of a product or service. Privacy by default involves having the settings on the maximum permissible level of privacy protection, without the user needing to make a choice (Information and Privacy Commissioner of Ontario, 2009[23]; EU, 2016[24]; ISO, 2023[25]). An example of privacy by design and by default is providing that data collection conforms to reasonable expectations and only data that is strictly necessary for advancing CBDC system policy objectives is collected. Although a less intermediated CBDC model (similar to P2P transactions) could improve the privacy of sensitive financial data, it may limit the ability of the CBDC to improve the payment system.

A permissioned[9] CBDC system, where participation is managed by a trusted entity or set of trusted entities, could yield better results in terms of privacy protection of sensitive financial data: transaction history is

[9] In contrast, in a permissionless CBDC system, participation in the system would not be managed by a central, trusted entity. This design choice does not assume the use of distributed ledger technology, but rather focuses on the governance structure of the system regardless of the technology used.

generally only viewable by a small number of trusted entities and kept private with respect to others (The White House, 2022[26]). Such governance design may also help mitigate other risks for consumers, investors, and businesses, such as lack of transaction remediation or migration of CBDC to non-compliant trading venues or actors engaged in misconduct or fraud.

The design of some of the CBDCs that have been fully rolled-out or are in pilot mode include access by the central bank only to pseudonymous data, but in some cases also de-anonymised data where they can show a legitimate cause, such as with a court order (Table 2.1). In other cases, central banks have access to all data and can link these to users' registered phone number or full identification and banking information, depending on transaction size limits.

Table 2.1. Transaction data access by central banks in live or pilot CBDCs, as reported by issuing authorities

CBDC	Central Bank CBDC Transaction Data Access
Central Bank of the Bahamas Sand Dollar	Transaction transparency to enable central bank (CB) to monitor suspicious transactions and stop accounts. Use of pseudonyms for users. CB maintains ledger and server is encrypted.
Eastern Caribbean Central Bank DCash	CB can see anonymized transaction data and outstanding CBDC in each digital wallet. Registered financial institutions can fully observe the identity of payers and payees and the purpose of transactions.
Central Bank of Uruguay e-Peso	User data is segregated across different databases. Transaction data per (anonymous) digital wallet can be decrypted to reveal the user's identity under very restrictive conditions – e.g., a competent authority prosecuting someone that has probable cause to access the transaction data.
Central Bank of Nigeria eNaira	CB has adopted an account based CBDC, will be able to identify users on the platform using identify frameworks. CB will retain control over the eNaira payment system and will be responsible for issuing the digital currency, managing the wallet, and maintaining a central ledger of all transactions. Privacy and confidentiality of transactions and data pertaining to business transactions.
People's Bank of China eCNY	"Controllable anonymity": The CB is privy to the identity of its users as they are required to provide their real identities when they first sign up.
Bank of Jamaica Jam-Dex	The CB does not maintain data on users. Wallet providers maintain the identities of their respective users and transactions in line with AML/CFT/CFP regulations.
Reserve Bank of India e-Rupee	n/a

Source: As reported by issuing authorities: SandDollar (2020[27]), Individual Sand Dollar – Bahamas, https://www.sanddollar.bs/individual; ECCB (2021[28]), Frequently Asked Questions, https://www.eccb-centralbank.org/p/frequently-asked-questions; SUERF and Bocconi (2018[29]), Do We Need Central Bank Digital Currency?, https://iris.unibocconi.it/retrieve/handle/11565/4014058/92065/Masciandaro%20SUERF%20book%20%2B%20SUERF%20book%20chapter.pdf; PBOC (2021[30]), Progress of Research and Development of E-CNY in China, http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.

Examples of technological advancement and experimentation that could support the objective of preserving privacy include, for example, the employment of privacy-enhancing technologies (PETs) and techniques such as zero-knowledge proofs (ZKPs)[10], private information retrieval (PIR)[11], aggregated or

[10] ZKPs refer to cryptographic protocols in which a prover can convince a verifier about a mathematical statement, for example, that the prover knows a piece of data that has specific properties. This statement may refer to the knowledge of a pre-image of a publicly known value under a hash function or about properties of the result of a publicly known algorithm that was executed on public or private data. In this setting, with a ZKP, the prover can convince the verifier without disclosing any information beyond the statement under consideration. ZKPs are "proofs that convey no additional knowledge other than the correctness of the proposition in question" (Goldwasser, Micali and Rackoff, 1989[69]).

[11] Private information retrieval allows a client to retrieve an element of a database without the owner of that database being able to determine which element was selected.

distributed data analysis, or homomorphic encryption[12], to name a few. Indicatively, these could allow for cash-like privacy in a compliant manner from a KYC perspective. In the case of CBDCs, the use of blind proofs or other PETs could possibly be an example of technology that addresses regulatory requirements without disclosing any transaction details to third parties. Such technological tools could theoretically allow for both privacy preserving and AML/CFT compliant digital currency (Gross, Sedlmeir and Seiter, 2023[31]). Recent work by the Bank of Japan provides a deep-dive on the different privacy enhancing technologies that could be relevant to payment and financial services applications, as well as CBDC experimentations (Bank of Japan, 2023[32]) (see Box 2.3).[13] Nevertheless, the robustness of the technology and its performance may need additional testing to reach maturity for use cases such as CBDCs.

Box 2.3. Privacy enhancing technologies for payments and digital financial services

The Bank of Japan has published an analysis of the different technologies that are being developed to contribute to the protection of users' privacy while using their data for business creation and soundness of transactions.

Specifically, the analysis highlights the concepts of *anonymization*, in which data is altered so that individuals cannot be identified, and *differential privacy*, in which the possibility of identification from analysis results is suppressed by adding noise or by other means.

Other methods include *secure computation*, in which analysis is performed while data is kept secret, and *trusted execution environment*, in which hardware technology is used to perform computational processing in a secure area where confidentiality is maintained.

In addition, *federated learning (privacy aware machine learning)*, in which users' information contained in each party's data is kept secret from other parties while collaborating with them to perform machine learning, is also being studied and deployed by some businesses (e.g., (Altana Atlas, 2023[33])).

As a privacy-related concept, *self-sovereign identity (SSI)* is also attracting attention. The concept of SSI is that an individual controls their identity without the intervention of an administrative organisation.

Many of these technologies are only at the experimental stage, and they are still in the process of being researched. Even if privacy enhancing technology progresses to a level where it can be implemented in society, technology alone cannot solve all problems. It is important to consider that effective privacy enhancing mechanisms can only be achieved by applying technologies in conjunction with various mechanisms, such as strong privacy and information security policies, governance, and operational frameworks. Having a sound legal framework that acknowledges and underpins privacy can further be essential for achieving the ultimate goals pursued in this field.

Source: Bank of Japan (2023[32]), Privacy Enhancing Technologies: Payments and Financial Services in a Digital Society, https://www.boj.or.jp/en/research/brp/psr/data/psrb230120.pdf.

Potential options to support the preservation of user privacy include, for example, the introduction of transaction limits. These could enable cash-like private CBDC transactions up to specific monetary limits, potentially balancing the privacy/integrity trade-off. If these limits are reached, transactions above the limit have similar degrees of privacy as existing digital payment platforms. Limits could be specified in terms of transaction size, holdings and/or turnover. High privacy guarantees and compliance with limits could be

[12] Homomorphic encryption is a form of encryption that allows computations to be performed on encrypted data without having to compromise the encryption (de-crypt them).

[13] Section 3.1 of the Bank of England's 'The digital pound: Technology Working Paper' also contains a discussion of zero knowledge proofs and other privacy-enhancing technologies (Bank of England, 2023[15]).

supported via the use of technological solutions. One example of possible solutions being explored is cryptographic zero-knowledge proofs.

Most central banks with live CBDCs or pilots underway are opting for a risk-based approach by allowing the collection of less information for lower risk transactions in line with global AML/CFT standards. Such models have tiers or limits for transactions that can be executed with enhanced privacy, enabling greater privacy for low-value transactions (see Table 2.2). Limits on holdings or transactions as well as tiered remuneration-based tools could also be embedded in the design of CBDCs as an example of one way to possibly avoid excessive use of CBDCs as a form of investment/interest-bearing deposit and minimise the risks from disintermediation of a CBDC introduction.[14] Such tiers are already used in AML/CFT regulation in some jurisdictions as a way to support financial inclusion (FATF, 2017[34]).

Table 2.2. Holding/Transaction limits in the design of live or pilot CBDCs

CBDC	Holding/Transaction limits in the design of live or pilot CBDCs
Central Bank of the Bahamas Sand Dollar	Physical/email address, phone number and photo for low-limit access (BSD 500 holding and BSD 1,500/month transaction). Plus, government-issued photo ID for higher limits (BSD 8,000 holding and BSD 10,000/month).
Eastern Caribbean Central Bank DCash	Physical/email address, phone number, photo and birth date/place for low limit access (XCD 1,000 to XCD 2,700/month transaction depending on risk profile). Plus, full name and bank account for higher limits (XCD 3,000 to XCD 20,000/day).
Central Bank of Uruguay e-Peso	Physical/email address, SIM card and national ID for low limit access (UYU 30,000). No higher limits except for businesses (UYU 200,000).
Central Bank of Nigeria eNaira	Physical/email address, phone number, passport photo and birth date/place for low limit access (NGN 120,000 holding and NGN 20,000/day). Plus, National Identity Number and bank account for higher limits (NGN 50,000 – NGN 1,000,000/day and NGN 300,000 – NGN 5,000,000 holding). No limits on businesses.
People's Bank of China eCNY	SIM card for low limit access (CNY 10,000 holding, CNY 2,000/transaction and CNY 5,000/day). Plus, full name, address, phone number and bank account for higher limits (CNY 500,000 holding, CNY 50,000/transaction and CNY 100,000/day).
Bank of Jamaica Jam-Dex (via Lynk wallet)	Government-issued ID to activate a Lynk wallet but no holding limits. Person-to-person limit is JMD 100,000/day. Cash-out limit is JMD 100,000/day, cash-ins are limited to JMD 50,000/day from a bank account, JMD 50,000/month from a debit/credit card.
Reserve Bank of India e-Rupee	e-Rupee concept note considers limits on individuals' CBDC holdings or transactions and CBDC remuneration.

Source: SandDollar (2020[27]), Individual Sand Dollar – Bahamas, https://www.sanddollar.bs/individual; ECCB (2021[28]), Frequently Asked Questions, https://www.eccb-centralbank.org/p/frequently-asked-questions; SUERF and Bocconi (2018[29]), Do We Need Central Bank Digital Currency?, https://iris.unibocconi.it/retrieve/handle/11565/4014058/92065/Masciandaro%20SUERF%20book%20%2B%20SUERF%20book%20chapter.pdf; Lynk (2022[35]), Lynk FAQs, https://www.lynk.us/faqs; Reserve Bank of India (2022[36]), Concept note on Central Bank Digital Currency, https://rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=1218; eNaira (2023[37]), eNaira Design Paper | Same Naira. More Possibilities, https://enaira.gov.ng/about/design.

In Europe, the Eurosystem is exploring options that could allow a digital euro to replicate some cash-like features and enable greater privacy for low-value transactions, while consideration is also being given to incorporating limit-based[15] tools[16] in the design of a digital euro to curb its use as a form of investment

[14] Imposing quantitative limits on the holdings of individual users or limits on transactions reduces the individual take-up or the speed of deposit conversion. Tiered remuneration-based tools could be calibrated to make large CBDC holdings above a certain threshold unattractive compared with other highly liquid and low-risk assets. In the euro-area, the ECB is also considering "waterfall" functionalities in the design of a digital euro, under which funds in excess of holding limits would be transferred automatically to a linked commercial bank account, for the same purposes.

[15] As well as remuneration-based tools.

[16] A given CBDC could have two sets of thresholds if deemed necessary. On the one hand, those that aim to address financial stability issues and, on the other hand, potentially lower ones to allow for low-risk transactions taking place with less points of friction.

(ECB, 2022[38]) (see Box 2.4). A 'selective privacy' option would allow greater privacy for low-value/low-risk payments, while transactions beyond that limit would provide a level of privacy equal to that of current private sector digital payment platforms.

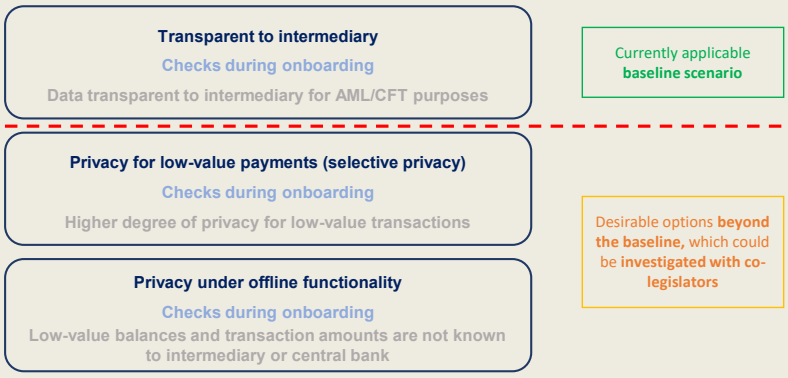
Box 2.4. Digital Euro privacy considerations: alternative scenarios

In a baseline scenario, compatible with the current regulatory framework, a digital euro would provide a level of privacy equal to that of current private sector digital solutions. Users would need to identify themselves when they start using the digital euro, and intermediaries would perform customer checks during onboarding. Personal and transaction data would only be accessible to intermediaries for AML/CFT purposes. User data obtained by intermediaries during the onboarding process would remain with the respective intermediary.

The Eurosystem will also explore two options that go beyond this baseline scenario. These could allow the digital euro to replicate some cash-like features and enable greater privacy for low-value/low-risk payments:

- The 'selective privacy' option would allow greater privacy for low-value/low risk payments. Users would need to identify themselves when first starting to use the digital euro, but simplified due diligence checks could apply, enabling a higher degree of privacy for low-value/low-risk payments. At the same time, higher-value transactions would remain subject to standard controls.
- The 'offline functionality' option would enable greater privacy for low-value offline payments in close physical proximity, also promoting financial inclusion.

Figure 2.2. Digital euro: privacy options from the user perspective



Source: ECB (2022[38]), Progress on the investigation phase of a digital euro, https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf.

It should also be noted that two-tier models for CBDCs have the distinct advantage of involving private-sector partners with established operations as one of the ways to help support compliance with AML/CFT rules. Such models, where users access CBDC services through financial intermediaries, could best balance trade-offs between privacy and preventing illicit activity (Board of Governors of the Federal Reserve System, 2022[10]).

OECD members have comprehensive and systematic frameworks of legal and regulatory measures in place that balance individual rights of privacy and authorities' legitimate needs for transparency. Policy choices and frameworks around CBDCs are therefore expected to align with such frameworks.

2.4. Trust: Security, transparency, operational resilience and protection of civil liberties and human rights

A democratic debate on the possible issuance of CBDCs could support broad acceptance of CBDCs given economic, political but also sociological dimensions at stake. Consultations with stakeholders and experiments with market players are some of the examples of possible outreach activities that could promote the establishment of a climate of trust. Transparency of operations, technology, and governance is another facet of trust that could be considered to support this objective.

To support democratic values in CBDCs, citizens will ultimately need to trust CBDCs and their issuing institutions in the same way that they have trusted cash as a public good. Trust relies on closely intertwined notions of independence, mandate and accountability of central banks and are the result of a long historical progress (Villeroy de Galhau, 2022[39]). Independence of the issuing institution from political power or other influence, explicit accountability and clear mandate are conducive to the development of trust. On the contrary, a lack of trust in the CBDC instrument and its underlying issuing authority could stimulate larger part of the populations to opt out of formal financial systems. Inadequate security and/or operational resilience of a CBDC could damage user trust in this system, especially given the importance of technological infrastructure in this form of public money. Similarly, privacy breaches, inadequate affordability or any other risks in the areas mentioned in this report could undermine user trust with possible reputational damage for CBDC issuers.

In terms of operational resilience, CBDC ecosystems should consider ways to enforce the security and resilience to cyber, fraud and other operational risks (G7, 2021[21]). The episode of prolonged unavailability of the ECCB's DCash in early 2022 is a notable illustration of the bounded potential of CBDC due to outages (AFI, 2022[16]). Other operational challenges include electronic counterfeiting and quantum computing-related threats related to cyber security. The potential ability of ability of quantum computing technology to break current encryption methods could compromise sensitive financial data (BIS Innovation Hub, 2023[40]). Technical disruptions in a CBDC's implementation or functioning would harm users' trust in the issuing central bank, with subsequent reputational repercussions. Designing appropriate defences for CBDC could be particularly difficult because a CBDC network could potentially have more entry points than existing payment services. (Board of Governors of the Federal Reserve System, 2022[10]). At the same time, it should be highlighted that a CBDC could enhance the operational resilience of the payment system if it were designed with offline capability, allowing payments to be made without internet access. Many digital payments today cannot be executed during natural disasters or other large disruptions and affected areas must rely on in-person cash transactions (Board of Governors of the Federal Reserve System, 2022[10]).

3 Policy considerations

The discussions around CBDCs are intensifying and issuing digital public money is becoming increasingly achievable. Given the central role that a possible CBDC arrangement would have on the structure and functioning of the financial system, it is increasingly important to consider ways to design CBDCs as instruments that can support citizens' welfare and abide by democratic values and principles.

CBDC design and/or implementation choices (including with regard to either or both governance and technology) could guard economies against threats to democratic values, protecting civil liberties and human rights. Design and implementation choices can support the policy objectives of providing equitable treatment of what is universally acknowledged as public good to citizens, involving availability, accessibility and affordability of CBDCs. When it comes to protection of users' privacy, this would allows to promote their safety, dignity, freedom of thought and expression. Also, the promotion of users' trust particularly through security and operational resilience of CBDC systems could be a cornerstone to the success of a CBDC development. Sound governance architectures of CBDC systems at the national and cross-border level could support the objective that CBDCs continue to abide by those democratic values, while balancing trade-offs with other core policy objectives, such as transparency and the ways to defend the financial system from abuse and preserve its integrity. Any CBDC system may be considered critical infrastructure and could therefore be subject to appropriate monitoring and adequate resilience and recovery plans.

The above objectives could be met using a variety of CBDC technology models. Ultimately, it is the policy decisions around CBDC design that will allow for democratic values to be respected and incorporated precisely 'by design'. On the contrary, technological advances can actually enable the alleviation of some of the characteristics that may appear to be constraining the respect of such values, while they can also offer solutions to some of the trade-offs between policy objectives (e.g., privacy and financial integrity).

CBDC design and implementation choices need to consider ways to support the protection of civil and human rights protected by OECD member constitutions, including protection against any kind of privacy-intrusive unlawful surveillance or 'digital authoritarianism'. This concerns both privacy protection as well as limits to the programmability of money and/or conditionality built in CBDC design, so as to avoid CBDCs being used arbitrarily to unjustly censor individuals and/or exert control over users without due process or recourse; or as a way to unjustly exert greater control over individuals' transactions. Built-in privacy protections, disassociability and other design choices are some examples of ways to ensure that privacy is included by default and by design in a potential CBDC.

The right balance needs to be struck between an acceptable level of privacy and other important public policy objectives of protecting financial integrity of financial markets (incl. AML/CFT). In addition to technical-level protections, governance arrangements of CBDC systems could also support the above policy objectives, incorporating appropriate oversight and accountability mechanisms that can support the safeguarding of civil and human rights. Having a sound legal framework that acknowledges and underpins these objectives can be essential for achieving the CBDC's intended goals. At the same time, a convincing value proposition is critical for the success of CBDCs – so, for example, CBDCs could enable users themselves to initiate programmable payments or to allow private-sector wallet providers to

offer tailored services based on users' personal data (subject to appropriate data protection and consumer consent).

Universal continuous access to central bank money would need to be maintained when introducing a CBDC. To that end, continuous availability and widespread acceptability of physical cash would need to be protected in jurisdictions where CBDCs are issued, as one of the ways to support those not able or not willing to use CBDCs so that they can still enjoy the benefits of access to physical form of public money. In addition, the physical infrastructure that allows people to access cash (cash-in/cash-out) may need to also be preserved for this to be accomplished.

All citizens would need to receive equitable treatment with regards to their CBDC experience. This concerns gender disparities; digital access divides; or parts of the population more likely to face inclusion barriers, such as the elderly, people with disabilities or those without a formal proof of identity. Policies and strategies promoting financial education for digital financial products can promote accessibility and usability of CBDCs, while technical advances can alleviate identity gaps. Offline functionalities at the implementation level could be one of the ways to address digital divides, while also protecting against interruption of transactions in case of infrastructure failure or widespread disruption in the payment infrastructure. The latter is however limited to short-term interruptions, as existing offline solutions require a periodic connection with the CBDC infrastructure in online mode. At the same time, offline functionalities have limitations (e.g., double spending or loss of funds if the device is damaged, misplaced or stolen) and offline environments may not be comprehensively monitored, exposing the system to increased security risks. Countries planning to introduce a CBDC with offline functionality may need to further investigate the security of such functionalities. What is more, costs related to devices supporting a safe and efficient CBDC system with offline functionalities may have a positive impact on the affordability of CBDCs and may require further research.

Built-in privacy protections, disassociability and other design choices are some of the ways that could help support privacy objectives that could be included by default and by design in a potential CBDC. Given that they give access to heightened levels of information about users (e.g., transaction and account level data), CBDCs could risk being used as a surveillance tool and as a way to exert greater control over private transactions (e.g., censorship purposes). At the same time, CBDC systems would need to support important public policy objectives of protecting financial integrity of financial markets (incl. AML/CFT). A number of alternative technological and design solutions are being put forward as some examples of solutions that can support the achievement of such balance. CBDCs can maintain privacy through central banks not having access to CBDC users' personal data, which would instead be managed by private-sector wallet providers (subject to appropriate data protection). Also, as is the case today with private forms of digital money such as bank accounts, law enforcement agencies and other competent authorities could only access the personal data held by wallet providers where there is a fair and lawful basis (Bank of England and HM Treasury, 2023[7]).

The success of a possible CBDC may depend to a large extent on its ability to build sufficient trust with citizens. While trust on public money relies on closely intertwined notions of independence, mandate and accountability of central banks, it could be undermined by inadequate security or operational failures, especially given the importance of technological infrastructure for digital forms of money. CBDC ecosystems would need to be secure and resilient to cyber, fraud and other operational risks, and safeguarded also when these ecosystems allow for offline and cross-border functionalities. With the backing of the central bank and strengthening through security protocols, CBDCs could potentially offer users a more secure and trustworthy payment instrument.

Perhaps the most important decision that could allow a CBDC to abide by democratic principles is the fundamental decision about issuing a CBDC. Any such policy decision would need to make sense for the citizens who will rely on it in the first place, which includes citizens' trust in the instrument. Such CBDC would then need to be carefully designed and implemented to reflect the core values of the citizens it will

serve and avoid unintended or unexpected societal consequences. As CBDCs progress from concept to pilot to reality, more work is needed to carefully consider how design, technology, functionality choices ensure that democratic values are considered and embedded in the outcomes, to support ensuing benefits that rest on democratic principles and trust.

Annex A. The current state of global CBDC experimentation and development

The debate on whether to allow any individual to hold electronic central bank liabilities began decades ago, but recent developments have intensified it. In the 1980s, it was proposed that central banks make available to the public a medium of exchange/payment with the convenience of deposits and the safety of currency (essentially currency on deposit), transferable in any amount by check or other order (Tobin 1985, 1987). Falling use of cash for payments (accelerated by the COVID-19 pandemic) and the emergence of crypto-assets, especially stablecoins, have accelerated the work on CBDCs.

Today, most central banks are exploring CBDCs, and more than a quarter of them are developing or running concrete pilots of retail and/or wholesale CBDC issuance (Kosse and Mattei, 2022[41]). According to the 2021 BIS survey, 90% of the 81 central banks surveyed at the end of 2021 were exploring retail and/or wholesale CBDC issuance, and two thirds of them are likely to issue a retail CBDC in the short or medium term (Kosse and Mattei, 2022[41]). Eight CBDCs have been launched or piloted at significant scale and 23 are in the very advanced exploration stages.

CBDCs have been fully launched in three countries: the Bahamas (the Sand Dollar), Jamaica (Jam-Dex) and Nigeria (e-Naira). Pilots of CBDCs are running, or have been run, in five jurisdictions: China (e-CNY), Eastern Caribbean Economic and Currency Union (DCash), Ghana, India, and Uruguay. Sixteen jurisdictions have started or completed technical experimentation, including the Euro Area (Digital Euro), Japan, Korea, Russia, Sweden, and the United States.

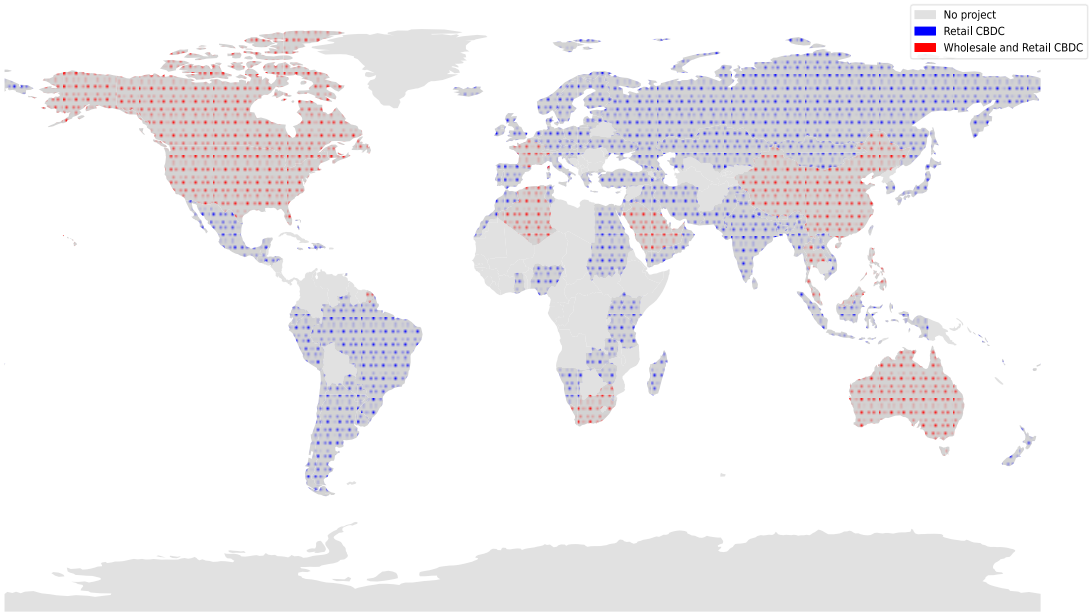
Pilots engage real end-users, even if in a limited scale relative to the entire user base of the respective countries, while Proof-of-Concept (PoC) projects involve - at most - central bank staff. As of October 2021, the People's Republic of China announced that about 140 million people had opened digital wallets for China's digital yuan and used it for transactions totalling about 62 billion yuan, the equivalent of c. USD 10 billion (Reuters, 2021[42]). It is estimated that about one-fifth of China's population has installed the central bank's digital yuan wallet (Congressional Research Service, 2022[43]).

As of the time of writing of this report, 94 central banks are exploring retail CBDCs across the globe. The motivations for CBDC exploration are diverse and are very much linked to the underlying degree of financial infrastructure development in each jurisdiction and to the needs of the respective economies (OECD, 2021[44]). For that reason, stated motivations for CBDC exploration differ between advanced economy (AE) and emerging market and developing economy (EMDE) central banks.

AE central banks focus on ensuring continuing central bank money access due to significant decrease in the cash usage for retail payments (particularly in the post COVID19 era), and monetary sovereignty, against a backdrop of increasing competition from private sector digital payment platforms, some of which threaten to exercise monopoly powers (Gabriel Soderberg et al., 2022[45]). AE central banks have indicated that the emergence of stablecoins and other crypto-assets has accelerated their CBDC experimentation (Kosse and Mattei, 2022[41]). CBDC introduction could encourage greater competition and innovation by allowing for equal access to a more efficient, consumer-friendly, convenient and safe payment option on the basis of which financial service innovation can flourish while safeguarding stability and security (BIS, 2022[46]). Another motivation in some AEs is to support the tokenisation of assets and limit settlement risks of wholesale transactions.

Figure A A.1. CBDC experimentation gaining momentum

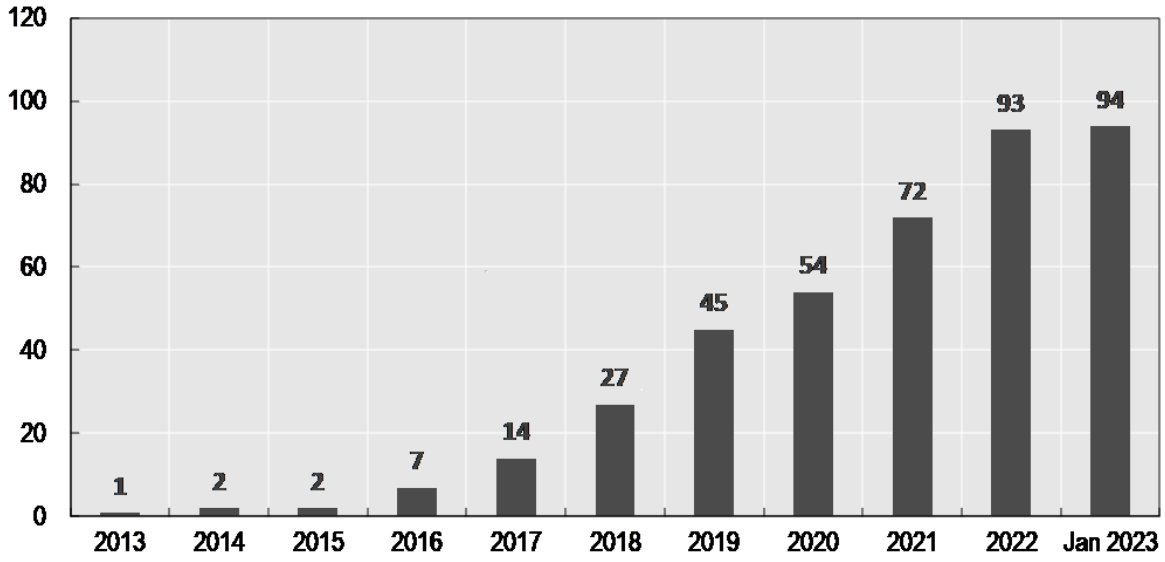
As of 31 January 2023



Note: Includes research, proof-of-concept and pilots of CBDCs, as well as cancelled experimentation and launched CBDCs. Countries shown in grey colour have not released any public information about any CBDC projects as of yet. Wholesale CBDC projects refer to central bank money only in the form of digital tokens.
Source: OECD based on database compiled by John Kiff and Josiah Hernandez, as of January 2023.

Figure A A.2. Retail CBDCs experimentation by launch year

In absolute number of experimentation projects, based on publicly available information



Source: Database compiled by John Kiff and Josiah Hernandez, as of January 2023. Includes live CBDCs in the Bahamas, Jamaica and Nigeria.

EMDE central bank CBDC exploration tends to be driven by financial inclusion motivations, reducing costs associated with physical cash, increasing payment system efficiency, and strengthening financial integrity. Interoperable CBDCs may increase the efficiency and speed of international payments (especially remittances), while lowering their cost, which has significant relevance for lower income parts of the population in EMDEs (OECD, 2021[44]). EMDEs also seek to protect themselves from the risk of monetary substitution and thus to defend their monetary sovereignty in the same way as advanced economies.

Table A A.1. Wholesale CBDCs experiments focusing on domestic payments systems

Central Bank	Project	Year	Description
Reserve Bank of Australia	Interbank payments	2020	Proof-of-concept of a wholesale settlement system for interbank payments running on a private, permissioned Ethereum network
Bank of Canada	Project Jasper (Phase 1 and 2)	2017	Use of DLT for the settlement of high-value interbank payments.
New York Fed	Technical experimentation	2022	Technical experimentation facilitating wholesale digital asset settlement
Republic of the Philippines	Project CBDCPh	2022	Use of CBDCs for large-value financial transactions on a 24/7 basis across a limited number of financial institutions.
Monetary Authority of Singapore (MAS)	Project Ubin (Phase 1 and 2)	2017	Inter-bank payments using DLT and tokenised form of the Singapore Dollar (SGD) on a DLT
South Africa Reserve Bank (SARB)	Project Khokha	2018	Use of DLT for interbank payments settlement
Bank of Thailand	Project Inthanon Phase 1	2019	Decentralised real time gross settlement system using wholesale CBDC

Note: Non exhaustive list.
Source: RBA (2020[47]), Settlement token for interbank payments, https://www.rba.gov.au/information/foi/disclosure-log/rbafoi-192024.html; Bank of Canada (n.d.[48]), Digital currencies and fintech: projects, https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/; Federal Reserve Bank of New York (2022[49]), Facilitating Wholesale Digital Asset Settlement, https://www.newyorkfed.org/aboutthefed/nyic/facilitating-wholesale-digital-asset-settlement; Bangko Sentral ng Pilipinas (2022[50]), Project CBDCPh to Further Strengthen PH Payment System, https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=6252; MAS and Deloitte (2017[51]), The future is here Project Ubin: SGD on Distributed Ledger, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-project-ubin-report.pdf; South African Reserve Bank (2022[52]), Project Khokha 2 - Report Release, https://www.resbank.co.za/en/home/publications/publication-detail-pages/media-releases/2022/Project-Khokha-2-Report-Release; Bank of Thailand (2019[53]), Ithanon Phase I, https://www.bot.or.th/English/FinancialMarkets/ProjectInthanon/Documents/Inthanon_Phase1_Report.pdf.

Wholesale CBDC exploration by both AE and EMDE central banks is predominantly focused on cross-border payments efficiency and facilitating cross-border wholesale digital asset settlement (Table A A.1 and Table A A.2).[17] Most central banks' view wholesale CBDC as a way to address cross-border frictions (and more efficiently so than retail CBDCs) (Kosse and Mattei, 2022[41]). Frictions include fragmented data

[17] Wholesale CBDC is a broad concept, not necessarily linked to any specific digital technology, as it encompasses all forms of settlement of interbank and related wholesale transactions in central bank reserves (see, e.g., (Panetta, 2022[8])). In practice, two main macro-models of wholesale CBDC can be distinguished: (i) the "Bridge" solutions (also known as "Trigger"), which envisage the implementation of a hybrid model, in which the settlement of wholesale transactions in central bank money takes place on infrastructures based on non-DLT technology that are linked to external systems, based on DLT technology, for the settlement of digital assets; (ii) the "Full DLT" solutions, which envisage that both the settlement in central bank money (issued as "native digital assets") and the settlement of digital assets take place on platforms based on DLT technology. This option would thus provide for the creation of a wholesale settlement system based on DLT technology, in which settlement in central bank money would take place in "DLT-based" central bank money. Two examples of bridge solutions are the experiments of delivery versus payment in euro via a 'bridge' between DLT platforms and the large-value payment system TARGET2 (see Deutsche Bundesbank's press release of 24 March 2021 on "DLT-based securities settlement in central bank money successfully tested") or the instant payments system TIPS (see (Rocca et al., 2022[71])).

formats, complexity of compliance checks, limited operating hours and unclear foreign exchange rates, as well as legacy technologies, long transaction chains, funding costs and weak competition. Indeed, wholesale CBDC can potentially enhance cross-border payments efficiency, if countries work together to ensure interoperability between CBDCs and mitigate undesired macro-financial consequences (CPMI, 2021[54]). Recently, Project Icebreaker has been looking at retail CBDCs as well as a platform for cross-border payments (BISIH, 2023[1]).

Depending on the motivation and the policy objectives, there are different design choices for CBDC instruments and for the underlying CBDC systems (Group of Central Banks, 2020[55]). Design features include introduction of interest; imposition of caps or limits to holdings; design of the ledger; and incentive structures. Such design features are not discrete, and all have some bearing on one another, increasing the importance of a coherent set of design choices (Group of Central Banks, 2020[55]).

Table A A.2. Wholesale CBDCs experiments focusing on cross-border payments

Central Bank	Project	Year	Description
Bank of Canada, Monetary Authority of Singapore	Project Jasper-Ubin	2019	Cross-Border High Value Transfer Using Distributed Ledger Technologies
Banque de France	Project Mariana (Cross-Border Payments)	2022	Cross-Border Payments experimentation
Hong Kong Monetary Authority (HKMA) & Bank of Thailand (BOT)	Project Inthanon-LionRock 1 & 2	2019 2020	Real-time transfers and atomic payment-versus-payment settlement
Monetary Authority of Singapore (MAS)	Project Ubin+	2022	Cross-border foreign exchange (FX) settlement using wholesale CBDC
New York Fed	Project Cedar	2022	DLT-enabled wholesale CBDC cross-border payment experimentation
New York Fed and MAS	Project Cedar Phase II x Ubin+	2022	Cross-border cross-currency transaction experiment, leveraging wCBDCs
Saudi Arabian Monetary Authority (SAMA) and the CBUAE	Project Aber	2020	wCBDC for cross-border commercial bank transactions
Bank for International Settlements Innovation Hub (BISIH) and: Swiss National Bank and Banque de France RBA, Bank Negara Malaysia (BNM), MAS, and SARB HKMA, BOT; the People's Bank of China (PBOC), and CBUAE Banque de France, MAS, and Swiss National Bank (SNB)	Project Jura Project Dunbar Multiple CBDC (mCBDC) Bridge	2021	Cross-border international settlements using digital currencies issued by multiple central banks

Note: Non-exhaustive list. Source: Bank of Canada and Mas (Bank of Canada and MAS, 2019[56]), Jasper–Ubin Design Paper, https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf; Villeroy de Galhau (2022[39]), Central bank digital currency (CBDC) and bank intermediation in the digital age, https://www.banque-france.fr/en/intervention/cbdc-and-bank-intermediation-digital-age; Bank of Thailand and HKMA (Bank of Thailand and HKMA, 2019[57]), Inthanon-LionRock, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf; HKMA (2020[58]), Hong Kong Monetary Authority - Hong Kong FinTech Week 2020, https://www.hkma.gov.hk/eng/news-and-media/press-releases/2020/11/20201102-3/, MAS (2022[59]), MAS Launches Expanded Initiative to Advance Cross-Border Connectivity in Wholesale CBDCs, https://www.mas.gov.sg/news/media-releases/2022/mas-launches-expanded-initiative-to-advance-cross-border-connectivity-in-wholesale-cbdcs; Federal Reserve Bank of New York (Federal Reserve Bank of New York, 2022[60]), Project Cedar: Improving Cross-Border Payments With Blockchain Technology, https://www.newyorkfed.org/aboutthefed/nyic/project-cedar; Federal Reserve Bank of New York (Federal Reserve Bank of New York, 2022[61]), New York Fed and Monetary Authority of Singapore Collaborate to Explore Potential Enhancements to Cross-Border Payments Using Wholesale CBDCs, https://www.newyorkfed.org/newsevents/news/financial-services-and-infrastructure/2022/20221110; SAMA (2020[62]), SAMA and CBUAE Issue Report on Results of Joint Digital Currency Project "Aber", https://www.sama.gov.sa/en-US/News/Pages/news-630.aspx; BIS (2021[63]), Project Jura: cross-border settlement using wholesale CBDC, https://www.bis.org/about/bisih/topics/cbdc/jura.htm; BIS (BIS, 2022[64]), Project Dunbar: international settlements using multi-CBDCs, https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm; BIS (2022[65]), Project mBridge: Connecting economies through CBDC, https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

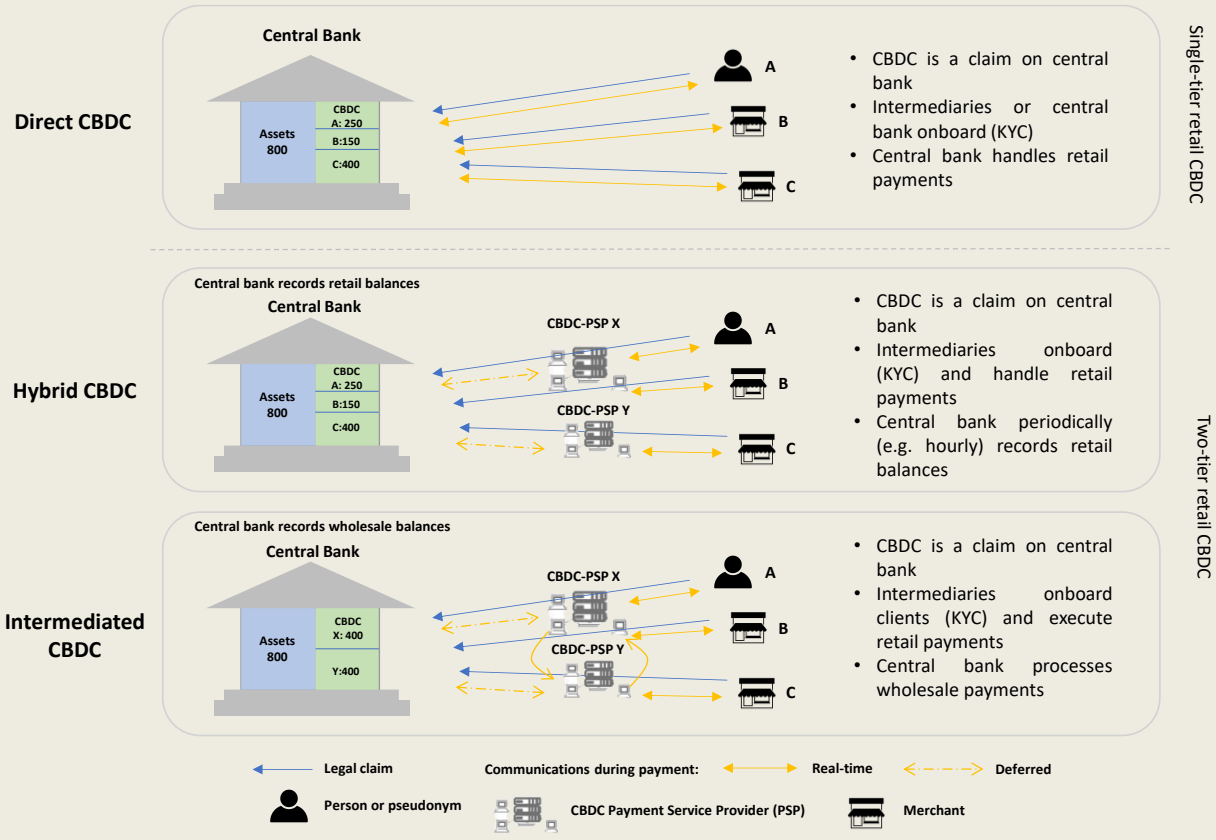
Box A A.1. CBDC design architectures and the intermediated model

CBDC design choices depend on policy objectives and country specifics, but among those CBDCs that have been launched, and different market infrastructure models for CBDCs have different possible effects on financial stability. Among central banks that are in the advanced stages of CBDC research, there is a high degree of high-level commonality towards two tier models.

In hybrid models, the private sector payment service providers (PSPs) would provide user facing services, while the central bank would be responsible for recording individual users' balances (potentially pseudonymously). In intermediated models, the central bank would only record wholesale balances, with PSPs recording individual user balances (Auer and Böhme, 2021[66]) (Figure A A.3).

Both of these two-tier models allow for CBDC co-existence with existing means of payment and for financial institutions to play their traditional payment service roles. It also supports the ability for third parties to build on top of the core, which could broaden choice and diversity in payment options.

Figure A A.3. Retail CBDC architectures



Source: Based on Auer and Böhme (2021[66]), Central bank digital currency: the quest for minimally invasive technology, https://www.bis.org/publ/work948.pdf.

References

AFI (2022), *Central Bank Digital Currency – an opportunity for financial inclusion in developing and emerging economies? | Alliance for Financial Inclusion*, https://www.afi-global.org/publications/central-bank-digital-currency-special-report/ (accessed on 2 February 2023). [16]

Altana Atlas (2023), *Altana Atlas*, https://altana.ai/atlas (accessed on 9 May 2023). [33]

Auer, R. et al. (2022), "Central bank digital currencies: a new tool in the financial inclusion toolkit?", https://www.bis.org/fsi/publ/insights41.htm (accessed on 2 February 2023). [17]

Auer, R. and R. Böhme (2021), "BIS Working Papers No 948 Central bank digital currency: the quest for minimally invasive technology", http://www.bis.org (accessed on 6 February 2023). [66]

Bangko Sentral ng Pilipinas (2022), *Project CBDCPh to Further Strengthen PH Payment System*, https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=6252 (accessed on 1 February 2023). [50]

Bank of Canada (n.d.), *Digital currencies and fintech: projects - Bank of Canada*, 2017, https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/ (accessed on 1 February 2023). [48]

Bank of Canada and MAS (2019), *Jasper–Ubin Design Paper*, https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf (accessed on 1 February 2023). [56]

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?la=en&hash=A97A5C2056FF5CD4D494B1E6A2EED7B8271ACA54 (accessed on 14 March 2023). [15]

Bank of England and HM Treasury (2023), *The digital pound: a new form of money for households and businesses? Consultation Paper*. [7]

Bank of Ghana (2019), *Design paper of the digital Cedi (eCedi)*, https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf (accessed on 2 February 2023). [14]

Bank of Japan (2023), "Privacy Enhancing Technologies: Payments and Financial Services in a Digital Society". [32]

Bank of Thailand (2019), *Ithanon Phase I*, https://www.bot.or.th/English/FinancialMarkets/ProjectInthanon/Documents/Inthanon_Phase1_Report.pdf (accessed on 1 February 2023). [53]

Bank of Thailand and HKMA (2019), *Inthanon-LionRock*, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf (accessed on 1 February 2023). [57]

BIS (2022), *Press release: The BIS presents a vision for the future monetary system*, https://www.bis.org/press/p220621.htm (accessed on 1 February 2023). [46]

BIS (2022), "Project Dunbar: international settlements using multi-CBDCs", https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm (accessed on 1 February 2023). [64]

BIS (2022), *Project mBridge: Connecting economies through CBDC*, https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm (accessed on 1 February 2023). [65]

BIS (2021), *Project Jura: cross-border settlement using wholesale CBDC*, https://www.bis.org/about/bisih/topics/cbdc/jura.htm (accessed on 1 February 2023). [63]

BIS Innovation Hub (2023), *Project Leap: Quantum-proofing the financial system*, https://www.bis.org/about/bisih/topics/cyber_security/leap.htm (accessed on 9 May 2023). [40]

BISIH (2023), *Breaking new paths in cross-border retail CBDC payments Project Icebreaker-Breaking new paths in cross border retail CBDC payments 2 Content*. [1]

Board of Governors of the Federal Reserve System (2022), "Money and Payments: The U.S. Dollar in the Age of Digital Transformation", http://www.federalreserve.gov/aboutthefed.htm. (accessed on 1 February 2023). [10]

Congressional Research Service (2022), *Central Bank Digital Currencies: Policy Issues*, https://crsreports.congress.gov/product/pdf/R/R46850 (accessed on 1 February 2023). [43]

CPMI (2021), *Central bank digital currencies for cross-border payments*, https://www.bis.org/publ/othp38.htm (accessed on 1 February 2023). [54]

ECB (2022), *Digital euro Privacy options Eurogroup ECB-PUBLIC*, http://www.ecb.europa.eu© (accessed on 6 February 2023). [22]

ECB (2022), "Progress on the investigation phase of a digital euro". [38]

ECCB (2021), *Frequently Asked Questions | Eastern Caribbean Central Bank*, https://www.eccb-centralbank.org/p/frequently-asked-questions (accessed on 6 February 2023). [28]

eNaira (2023), *eNaira Design Paper | Same Naira. More Possibilities*, https://enaira.gov.ng/about/design (accessed on 30 May 2023). [37]

EU (2016), *GDPR*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3063-1-1 (accessed on 11 May 2023). [24]

European Commission (2022), *Targeted consultation on a digital euro - responses finance-2022-digital-euro*, https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-digital-euro_en (accessed on 6 February 2023). [5]

FATF (2017), *FATF Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence*, https://www.fatf-gafi.org/en/publications/Fatfgeneral/Financial-inclusion-cdd-2017.html (accessed on 16 February 2023). [34]

Federal Reserve Bank of New York (2022), *Facilitating Wholesale Digital Asset Settlement - FEDERAL RESERVE BANK of NEW YORK*, https://www.newyorkfed.org/aboutthefed/nyic/facilitating-wholesale-digital-asset-settlement (accessed on 1 February 2023). [49]

Federal Reserve Bank of New York (2022), *New York Fed and Monetary Authority of Singapore Collaborate to Explore Potential Enhancements to Cross-Border Payments Using Wholesale CBDCs - FEDERAL RESERVE BANK of NEW YORK*, https://www.newyorkfed.org/newsevents/news/financial-services-and-infrastructure/2022/20221110 (accessed on 1 February 2023). [61]

Federal Reserve Bank of New York (2022), *Project Cedar: Improving Cross-Border Payments With Blockchain Technology - FEDERAL RESERVE BANK of NEW YORK*, https://www.newyorkfed.org/aboutthefed/nyic/project-cedar (accessed on 1 February 2023). [60]

G7 (2021), "Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)". [21]

Gabriel Soderberg et al. (2022), *Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons*, https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174 (accessed on 1 February 2023). [45]

Goldwasser, S., S. Micali and C. Rackoff (1989), "The knowledge complexity of interactive proof systems", https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf (accessed on 6 February 2023). [69]

Gross, J., J. Sedlmeir and S. Seiter (2023), *How to Design a Compliant, Privacy-Preserving Fiat Stablecoin via Zero-Knowledge Proofs*, https://www.etonec.com/post/how-to-design-a-compliant-privacy-preserving-fiat-stablecoin-via-zero-knowledge-proofs (accessed on 6 February 2023). [31]

Group of Central Banks (2020), "Central bank digital currencies: foundational principles and core features - 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", http://www.bis.org (accessed on 16 February 2023). [55]

HKMA (2020), *Hong Kong Monetary Authority - Hong Kong FinTech Week 2020*, https://www.hkma.gov.hk/eng/news-and-media/press-releases/2020/11/20201102-3/ (accessed on 1 February 2023). [58]

Information and Privacy Commissioner of Ontario (2009), *Privacy by Design: the 7 foundational principles*. [23]

ISO (2023), *ISO 31700-1:2023 - Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements*, https://www.iso.org/standard/84977.html (accessed on 11 May 2023). [25]

Kiff, J. (2022), *Taking Digital Currencies Offline*, https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline (accessed on 6 February 2023). [13]

Kosse, A. and I. Mattei (2022), "Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies", https://www.bis.org/publ/bppdf/bispap125.htm (accessed on [41]

31 January 2023).

Lynk (2022), *Lynk FAQs*, https://www.lynk.us/faqs (accessed on 6 February 2023). [35]

MAS (2022), *MAS Launches Expanded Initiative to Advance Cross-Border Connectivity in Wholesale CBDCs*, https://www.mas.gov.sg/news/media-releases/2022/mas-launches-expanded-initiative-to-advance-cross-border-connectivity-in-wholesale-cbdcs (accessed on 1 February 2023). [59]

MAS and Deloitte (2017), "The future is here Project Ubin: SGD on Distributed Ledger". [51]

Nadeau, E. (2020), "NIST privacy framework: a tool for improving privacy through enterprise risk management", https://www.nist.gov/privacy-framework. (accessed on 6 February 2023). [19]

OECD (2023), *Shifting from open banking to open finance: Results from the 2022 OECD survey on data sharing frameworks | en | OECD*, https://www.oecd.org/finance/shifting-from-open-banking-to-open-finance-9f881c0c-en.htm (accessed on 21 May 2023). [20]

OECD (2022), *Environmental impact of digital assets: Crypto-asset mining and distributed ledger technology consensus mechanisms | en | OECD*, https://www.oecd.org/publications/environmental-impact-of-digital-assets-8d834684-en.htm (accessed on 14 March 2023). [9]

OECD (2022), *OECD Council Declaration on a Trusted, Sustainable and Inclusive Digital Future*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488 (accessed on 31 January 2023). [3]

OECD (2021), *Development Co-operation Report 2021: Shaping a Just Digital Transformation*, OECD Publishing, Paris, https://doi.org/10.1787/ce08832f-en. [4]

OECD (2021), *Digitalisation and Finance in Asia - OECD*, https://www.oecd.org/finance/financial-markets/digitalisation-and-finance-in-asia.htm (accessed on 1 February 2023). [44]

OECD (2021), "Meeting of the OECD Council at Ministerial Level: Trust in Global Cooperation - The vision for the OECD for the next decade", http://www.oecd.orgTel.:+33 (accessed on 31 January 2023). [2]

OECD (2019), *Artificial Intelligence in Society*, OECD Publishing, Paris, https://doi.org/10.1787/eedfee77-en. [70]

OECD (2018), "G20/OECD INFE Policy Guidance Digitalisation and Financial Literacy", http://www.oecd.org/going-digital. (accessed on 19 December 2022). [11]

OECD (1980), *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (accessed on 16 February 2023). [18]

Panetta, F. (2023), *The digital euro: our money wherever, whenever we need it*, https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230123~2f8271ed76.en.html (accessed on 1 February 2023). [6]

Panetta, F. (2022), *Demystifying wholesale central bank digital currency*, https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220926~5f9b85685a.en.html [8]

(accessed on 14 March 2023).

PBOC (2021), “Progress of Research and Development of E-CNY in China”. [30]

RBA (2020), *Settlement token for interbank payments*, https://www.rba.gov.au/information/foi/disclosure-log/rbafoi-192024.html (accessed on 1 February 2023). [47]

Reserve Bank of India (2022), *Concept note on Central Bank Digital Currency*, https://rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=1218 (accessed on 6 February 2023). [36]

Reuters (2021), *$9.5 billion spent using Chinese central bank’s digital currency - official | Reuters*, https://www.reuters.com/article/fintech-cbdc-china-idCAKBN2HO0WP (accessed on 1 February 2023). [42]

Rocca, R. et al. (2022), “Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms”, http://www.bancaditalia.it. (accessed on 17 June 2023). [71]

SAMA (2020), *SAMA and CBUAE Issue Report on Results of Joint Digital Currency Project “Aber”*, https://www.sama.gov.sa/en-US/News/Pages/news-630.aspx (accessed on 1 February 2023). [62]

SandDollar (2020), *Individual Sand Dollar - Bahamas*, https://www.sanddollar.bs/individual (accessed on 6 February 2023). [27]

Sarmiento, A. (2022), “Seven lessons from the e-Peso pilot plan: The possibility of a Central Bank Digital Currency”, *Latin American Journal of Central Banking*, Vol. 3/2, p. 100062, https://doi.org/10.1016/J.LATCB.2022.100062. [12]

South African Reserve Bank (2022), *Project Khokha 2 - Report Release*, https://www.resbank.co.za/en/home/publications/publication-detail-pages/media-releases/2022/Project-Khokha-2-Report-Release (accessed on 1 February 2023). [52]

SUERF and Bocconi (2018), *Do We Need Central Bank Digital Currency?*, https://iris.unibocconi.it/retrieve/handle/11565/4014058/92065/Masciandaro%20SUERF%20book%20%2B%20SUERF%20book%20chapter.pdf (accessed on 6 February 2023). [29]

The White House (2022), “Technical evaluation for a U.S. central bank digital currency system”, http://www.whitehouse.gov/ostp. (accessed on 6 February 2023). [26]

United Nations (1976), *International Covenant on Civil and Political Rights | OHCHR*, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed on 1 February 2023). [68]

United Nations (1948), “Universal Declaration of Human Rights | United Nations”, https://www.un.org/en/about-us/universal-declaration-of-human-rights (accessed on 1 February 2023). [67]

Villeroy de Galhau, F. (2022), *Central bank digital currency (CBDC) and bank intermediation in the digital age | Banque de France*, https://www.banque-france.fr/en/intervention/cbdc-and-bank-intermediation-digital-age (accessed on 1 February 2023). [39]