Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)

Foreword

The UK's Presidency of the G7 comes at a pivotal time for the future of money and payments, with rapid innovation bringing fresh opportunities and considerations for public policy.

Central Bank Digital Currencies (CBDCs), a potential digital form of money that could be used alongside physical notes and coins, are part of this wider story of digital innovation. CBDCs might offer businesses and consumers new ways to pay in the future and could support inclusion and innovation in an increasingly digital and dynamic economy. But they also raise important questions about the reshaping of our economy, financial systems, and the way in which people interact with money and payments.

No G7 authority has yet decided whether they will issue a CBDC and this is a sovereign matter for each jurisdiction. This report, Public Policy Principles for Retail CBDCs, sets out a common set of considerations on the public policy implications of CBDC, reflecting the shared and enduring values of the G7 on transparency, the rule of law, and sound economic governance.

These Public Policy Principles for Retail CBDCs should support and inform policy deliberations as we respond to a new wave of innovation in money and payments; and will be useful to jurisdictions and international organisations considering CBDC, in the G7 and beyond.

Rt Hon Rishi Sunak MP
Chancellor of the Exchequer

Andrew Bailey
Governor of the Bank of England

Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)

Introduction

Money and payments are fundamental to our societies and economies. Innovation is rapidly reshaping domestic and international financial infrastructure, with new forms of private and public money emerging. Safe and efficient transactions are critical to support a thriving economy, ensure monetary and financial stability, and safeguard trust in the financial system. The rapid rise in the use of digital payments is transforming the way people and businesses transact, and their impacts are now wide-ranging, with implications for broader public policy objectives. These trends have been further accelerated by the Covid-19 pandemic.

Harnessing the opportunities and addressing the risks of these developments is a priority. In response, G7 central banks and finance ministries are exploring how digital innovation can maintain access to, and promote the utility of, central bank money in the form of retail Central Bank Digital Currencies (CBDCs). A retail CBDC would be a digital form of central bank money, denominated in the national unit of account, distinct from electronic reserves (which cannot currently be accessed by individuals), and physical cash. As a direct liability of the central bank CBDCs would also be distinct from commercial bank money. If issued, CBDCs, as a form of central bank money, could act as both a liquid, safe settlement asset and as an anchor for the payments system.

CBDCs are not 'cryptoassets'. Cryptoassets are not issued by a central bank, can be highly volatile, and are not currently widely used for payments. CBDCs are fundamentally different from privately issued digital currencies such as stablecoins, which are a liability of private entities that seek to maintain stability in their price (typically in relation to stable assets such as fiat currency). CBDC can be considered in two parts: the CBDC itself, an instrument issued by the central bank that can be transferred as a means of payment or held as a store of value, and the wider 'ecosystem' in which a CBDC operates, including the supporting infrastructure that allows CBDC balances to be managed and payments made. This wider infrastructure could involve both public and private participants (such as banks, digital wallet providers or other payment entities).

In recent years G7 central banks, together with the Sveriges Riksbank and the Swiss National Bank, have worked collaboratively, including in a group jointly chaired by the Bank for International Settlements (BIS) and the Bank of England, to explore considerations related to retail CBDCs.[1] In

[1] Central banks and the BIS explore what a retail CBDC might look like

a joint report published in October 2020, they outlined foundational principles for, and core features of, a potential CBDC. These principles emphasise that any CBDC must not compromise financial and monetary stability; should coexist with, and complement existing forms of money, and promote innovation and efficiency in payments.[2] In meeting these principles, this group have determined that CBDCs could be an important instrument for central banks in the future and that the design of any CBDC must be capable of accommodating future payments needs. At the same time, it is clear that CBDCs, if launched, would have important public policy implications, beyond the central bank's remit alone, which any jurisdiction considering CBDC issuance must consider from the outset.

The G7 announced in its communiqué issued on 5 June 2021[3] that its finance ministries and central banks are working together to explore these wider public policy implications and to develop a common set of principles for retail CBDCs. These principles are intended to guide and inform the exploration and potential development of national retail CBDCs with respect to these wider public policy considerations. They reflect shared values, and do not presuppose decisions on the issuance of domestic CBDC, which is a sovereign matter for each jurisdiction. These principles have been developed by the G7, but have relevance to other countries as they explore CBDC in their own jurisdiction. Whilst these principles focus on considerations for a retail CBDC, there may be aspects with relevance to other potential projects looking into the issuance of wholesale CBDC which may be explored by G7 jurisdictions.

As set out in the June 2021 communiqué, the G7's objective is to ensure that any CBDC is grounded in long-standing commitments to transparency, the rule of law, and sound economic governance.[4] The G7 also considers this should be underpinned by a firm commitment to ongoing collaboration and knowledge sharing.

The international use of CBDC, including for cross-border payments, could bring important benefits, but if CBDC design is not carefully calibrated, might also pose unintended consequences. The G7 commits, where possible, to avoid such unintended consequences. Reflecting this, the G7 supports ongoing international work underway on aspects of CBDC by the BIS,[5] Committee on Payments and Market Infrastructure (CPMI), International Monetary Fund (IMF),[6] the World Bank and Financial Stability Board (FSB),[7] as well as the Financial Action Task Force (FATF). This report also complements the work under building block 19[8] (led by CPMI and BIS Innovation Hub) of the G20's cross-border payments roadmap on the international dimension of CBDCs.

The principles explored in this report are divided into two categories and placed in no order of importance. The first category, *foundational issues*, covers monetary and financial stability; legal

[2] Central bank digital currencies: foundational principles and core features
[3] G7 Finance Ministers and Central Bank Governors Communiqué
[4] The communiqué also said: "CBDCs should be resilient and energy-efficient; support innovation, competition, inclusion, and could enhance cross-border payments; they should operate within appropriate privacy frameworks and minimise spillovers."
[5] III. CBDCs: an opportunity for the monetary system; BIS Innovation Hub work on central bank digital currency
[6] Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law considerations; New Forms of Digital Money: Implications for Monetary and Financial Stability
[7] Enhancing Cross-border Payments: Stage 3 Roadmap
[8] Central bank digital currencies for cross-border payments: Report to the G20

and governance frameworks; data privacy; competition; operational resilience and cybersecurity; illicit finance; spillovers; and energy and environment. The second category, *opportunities*, focuses on supporting the digital economy and innovation; financial inclusion; payments to and from the public sector; cross-border functionality; and international development. The final section discusses the concept of dependencies that may be encountered in designing a retail CBDC ecosystem, for example, interactions between protecting users' privacy and countering illicit finance. The report seeks to highlight some of the design choices that these dependencies might imply and offers some considerations on how to approach these complex issues, whilst recognising that it is for national authorities to consider how best to balance them.

Principle 1.

Monetary and financial stability

Principle 1: Any CBDC should be designed such that it supports the fulfillment of public policy objectives, does not impede the central bank's ability to fulfill its mandate and 'does no harm' to monetary and financial stability.

- The G7 endorses the work on CBDC of the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and BIS. We welcome the conclusions both of their first report in October 2020 setting out common foundational principles and core features of a CBDC and of their second set of reports in September 2021 further analysing policy options and practical design questions.[9]

- That group has emphasised the role of central bank money in a monetary system in anchoring public trust in money and supporting public welfare. In meeting their foundational principles, CBDCs could be important instruments for central banks in the future to enhance financial stability, harness new technologies and continue serving the public.[10]

- Whilst recognising CBDCs would have implications for financial intermediation that would need careful design and implementation, the group's recent analysis[11] suggests the impacts on bank disintermediation and lending could be manageable for the banking sector. They note that the financial system is dynamic and evolving and has successfully navigated episodes of structural change over many years. Irrespective of CBDCs, private sector developments may generate similar deposit substitution risks, and the introduction of CBDC may generate additional innovative opportunities for banks and other financial intermediaries. Nevertheless, central banks will have to carefully consider how they would manage these impacts, particularly through any transition phase for CBDC.

- Central banks may need to explore safeguards that could be built into any CBDC to address financial stability risks, although such measures may need careful consideration before they were used. Such measures could be valuable in managing risks in any transition were a CBDC to be introduced and could potentially have a longer-term role in some jurisdictions. The design of any measures would likely need to balance moderating the risks from high and/or

[9] Central bank digital currencies: foundational principles and core features
[10] Central bank digital currencies – executive summary
[11] Central bank digital currencies: financial stability implications

rapid adoption of CBDC with other policy objectives and benefits associated with a meaningful level of CBDC use.

Principle 2.
Legal and governance frameworks

Principle 2: G7 values for the International Monetary and Financial System should guide the design and operation of any CBDC, namely observance of the rule of law, sound economic governance and appropriate transparency.

- G7 Finance Ministers and Central Bank Governors set out these expectations in their Statement on Digital Payments in 2020.[12]

- Appropriate national legal, regulatory, supervisory and oversight frameworks are essential to ensure trust, resilience, security and confidence in any CBDC.

- CBDC might involve new responsibilities for authorities, enable new policy opportunities, and potentially bring entities in a CBDC ecosystem into contact with personal data. Appropriate transparency and accountability frameworks, for both public and private sector participants, are crucial.

Principle 3.
Data privacy

Principle 3: Rigorous standards of privacy, accountability for the protection of users' data, and transparency on how information will be secured and used is essential for any CBDC to command trust and confidence. The rule of law in each jurisdiction establishes and underpins such considerations.

- CBDC must protect the privacy of users, including by requiring that the processing of their personal data is subject to laws governing privacy and the collection, storage, safeguarding, disposal and use of personal data that are enforceable in the jurisdiction. Existing laws and regulations differ across jurisdictions, but general principles regarding data collection and processing include: (i) legality, (ii) purpose limitation, (iii) data minimisation, (iv) transparency and accountability and (v) user consent.

[12] G7 Finance Ministers and Central Bank Governors' Statement on Digital Payments

- Public and private-sector entities in any CBDC ecosystem should only access, hold, process or share users' personal data where this data is necessary to achieve clear, open and legal purposes, for example, to mitigate money laundering or terrorist financing (ML/TF) risks.

- Users of any CBDC should have a high degree of transparency regarding the use of their personal data, centred around the principles of data minimisation and control for the user (wherever possible). Access to individual users' data beyond the minimum required should be supported by a strong consent framework where entities (public and private) should clearly and transparently lay out those additional requirements that are necessary to providing a viable and functional service. As part of this, CBDC ecosystems should consider how they will offer robust protection and safeguards against misuse of data by any involved parties, and be aligned to the progress being made towards international standards. The G7 has recently published the Roadmap for Cooperation on Data Free Flow with Trust,[13] which may be relevant, and includes sections on data localisation, regulatory cooperation, government access to data and data sharing approaches for priority sectors.

Principle 4.
Operational Resilience and Cyber Security

Principle 4: To achieve trusted, durable, and adaptable digital payments; any CBDC ecosystem must be secure and resilient to cyber, fraud and other operational risks.

- Achieving a secure and resilient CBDC ecosystem requires careful decision-making in the design and configuration of any CBDC as well as in its ongoing operation, maintenance and evolution. Countries may wish to utilise different technologies to reach these objectives.

- All entities in a CBDC ecosystem (both public sector and any private sector) should have operational resilience, data security and cybersecurity strategies and operating frameworks consistent with national and international standards, such as the high-level Fundamental Elements of Cybersecurity for the Financial Sector set out by the G7 in 2016[14] and relevant aspects of CPMI-IOSCO's guidance on cyber resilience for financial market infrastructures.[15] Entities participating in a CBDC ecosystem may be required to coordinate their approaches to operational resilience and cybersecurity in order to ensure the resilience of the overall ecosystem.

- Capacity planning, business continuity and disaster recovery planning, crisis simulation and playbook development, and other sound response and recovery practices, are critical to maintaining the resilience of any CBDC infrastructure.

[13] Annex 2: G7 Roadmap for cooperation on Data Free Flow with Trust

[14] Including subsequent *G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (2017), G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector (2018), G7 Fundamental Elements for Threat-Led Penetration Testing (2018),* and *G7 Fundamental Elements of Cyber Exercise Programmes (2020).*

[15] The CPMI-IOSCO Cyber Guidance supplements CPMI-IOSCO's Principles for Financial Market Infrastructures.

- Motivations for any CBDC will determine some of the key operational requirements and risk profile. For example, where countries envisage CBDC as a means of enhancing the resilience of the overall payments landscape by providing an additional way to make payments, consideration could be given to the degree and nature of reliance on infrastructure shared with the broader payments landscape.

Principle 5.
Competition

Principle 5: CBDCs should coexist with existing means of payment and should operate in an open, secure, resilient, transparent and competitive environment that promotes choice and diversity in payment options.

- Payment services and ecosystems are subject to dynamics that can lead to market concentration, including strong network effects. Carefully tailored policies can promote fair and effective competition, diversity and choice in payments markets, which in turn support innovation and ensure strong levels of competition in the market. The introduction of CBDCs themselves may contribute positively to the overall level of competition in the payments landscape through provision of an additional means of payment for consumers. Standards to ensure (two-way) interoperability of other payment methods with CBDC are particularly important.

- The respective roles and responsibilities of the central bank and private sector service providers in the CBDC ecosystem should reflect, among other things, a consideration of their comparative advantages in providing the various necessary services. Many CBDC proposals envisage a prominent role for the private sector, for example in providing 'payments interfaces' (or 'digital wallets'). The provision of these services should be in an open, transparent and competitive environment and subject to regulatory and resilience requirements to ensure consumers have the required protections.

- Additionally, measures may be needed to ensure that users can easily switch between different types of money such as between CBDCs, bank deposits and cash, and also between payments interfaces, such as wallets, within any CBDC ecosystem.

- Any CBDC must be underpinned by a competitive and innovative environment capable of meeting consumer and business demand and support competition, choice and diversity in payment services. Therefore, consideration should be given to the applicable policy, regulatory and operational standards that apply to both CBDC and to other forms of digital payments. This is to ensure a common baseline expectation of resilience, integrity and user protection.

Principle 6.
Illicit finance

Principle 6: Any CBDC needs to carefully integrate the need for faster, more accessible, safer and cheaper payments with a commitment to mitigate their use in facilitating crime.

- CBDCs and accompanying regulatory frameworks should commit to countering their use in facilitating crime and be designed to comply with anti-money laundering (AML), counter-terrorist financing (CTF), and counter-proliferation of weapons of mass destruction obligations. They should also mitigate the risk of evasion of financial sanctions and comply with Financial Action Task Force (FATF) Standards.

- CBDCs can potentially contribute to the safe and efficient use and/or sharing of information in order to make existing processes, such as real-time monitoring and ex post facto investigation of payments and value transfer, more efficient and effective. Governments should identify and assess potential money laundering and terrorist financing (ML/TF) risks posed by CBDCs and prevent or mitigate those risks from the outset.

- Clearly defined roles and responsibilities with respect to AML/CFT regulations and obligations for all entities in a CBDC ecosystem will enable jurisdictions to counter illicit finance effectively and efficiently, and to ensure that CBDC ecosystems uphold rigorous standards of privacy and command users' trust and confidence. Where private-sector entities provide relevant services, or otherwise meet the FATF definition of a financial institution or another covered entity, they should be designated as obliged entities under the FATF Recommendations and hold responsibility for countering illicit finance in the CBDC ecosystem.

- When designing CBDCs, public authorities should look to build in ways of countering fraud and other forms of illicit finance by looking to incorporate advancements in technology and/or innovative solutions that may improve the authentication and verification of transactions.

- Public authorities' powers and use of data in any CBDC ecosystem to counter their use for illicit finance should be set out transparently in national legislative frameworks (see Principle 2) and those powers should not be used for other purposes.

Principle 7.
Spillovers

Principle 7: CBDCs should be designed to avoid risks of harm to the international monetary and financial system, including the monetary sovereignty and financial stability of other countries.

- When considering the level of access to CBDCs, some access by non-residents could be desirable, for example, for cross-border payments, trade and financial flows, as well as for 'retail' use, such as for remittances and use by foreign visitors. However, in the extreme, significant use of any CBDC by residents of a foreign country could lead to currency substitution and loss of monetary sovereignty in both the issuing and foreign country, which in turn might impede the ability of authorities to achieve their own policy objectives, including monetary and financial stability, and the countering of illicit finance.

- Where overseas access to a jurisdiction's CBDC could leave other countries vulnerable to currency substitution or other spillovers, collaborative work to design and implement safeguards, particularly through relevant international organisations, can help mitigate negative effects.

- Relevant International Financial Institutions (IFIs) and standard setting bodies should continue to analyse the implications of CBDCs and their potential cross-border use for the international monetary and financial system. This includes ongoing multilateral cooperation to ensure the safety and integrity of all CBDCs. Implications for the nature and scale of cross-border capital flows, the potential for higher capital flow volatility to amplify spillovers and cause spillbacks, the role of capital flow management measures, the supply and demand of global reserve assets, the configurations of international reserve currencies and the design of the global financial safety net are important topics. Countries will continue to reflect this work in their domestic explorations of CBDCs, engaging closely in the first instance with the ongoing work at CPMI, the BIS Innovation Hub, the IMF and the World Bank under Building Block 19 of the G20's roadmap for enhancing cross-border payments.

Principle 8.
Energy and Environment

Principle 8: The energy usage of any CBDC infrastructure should be as efficient as possible to support the international community's shared commitments to transition to a 'net zero' economy.

- With increasing digitalisation, IT infrastructures facilitating the storage, processing and transfer of information and value are becoming an important global user of energy. CBDCs

present the opportunity to set a marker for how future payment and settlement ecosystems are designed for optimal energy efficiency, including through utilising carbon-neutral and sustainable energy sources, whilst achieving necessary functional, performance and resilience aims.

- Energy usage should be factored into the design and implementation of any CBDC from the outset.

- Those central banks which publish climate-related disclosures (for example disclosures consistent with the Task Force on Climate-related Financial Disclosure (TCFD) framework) should consider disclosure of the environmental impact of CBDC operations in their reporting.

Opportunities

Principle 9.

Digital economy and innovation

Principle 9: CBDCs should support and be a catalyst for responsible innovation in the digital economy and ensure interoperability with existing and future payments solutions.

- The benefits of CBDC will in part depend on, and be enhanced by, wider public digital infrastructure and enabling digital economy strategies. As a digital complement to existing means of payment, including cash (with which CBDCs will coexist), CBDCs should contribute to the development of faster, cheaper, more inclusive, convenient and efficient payment solutions including in support of wider trends and innovations (such as 'open finance'). In this way, CBDCs might bridge fragmentation among regulated 'end-user' payment services, alongside adding diversity to, and easing concerns around, concentration within the payments landscape. The design of CBDC may also support interoperability with existing and future regulated payment solutions on both a domestic and cross-border basis.

- Clearly and appropriately allocated roles for the public and private sectors in a CBDC ecosystem can support innovation, including by minimising policy uncertainty that might, for instance, diminish investment in the wider payments landscape.

- CBDC might also support new innovative financial activities by facilitating new capabilities for payments such as programmability[16] and micro-payments. To take account of current and likely future needs, any CBDC should be developed in consultation with end-users, financial institutions, technology and other service providers and merchants.

[16] The CPMI defines programmability as the ability to automate processes by pre-programming actions to be taken if a specific event occurs (Wholesale digital tokens).

Principle 10.
Financial inclusion

Principle 10: Authorities should consider the role of CBDCs in contributing to financial inclusion. CBDC should not impede, and where possible should enhance, access to payment services for those excluded from or underserved by the existing financial system, while also complementing the important role that will continue to be played by cash.

- Barriers to accessing payment services vary across and within jurisdictions. They include cost, geographic factors (e.g. remote or sparsely populated areas), connectivity, demographics, low levels of economic development, access to verifiable identification and low levels of financial and digital literacy. CBDCs, as part of public infrastructure for digital payments, should be designed to take account of these challenges and encourage private sector innovation in order to address these gaps. Ancillary developments such as digital identity or other improvements to identity verification or authentication systems, if judged appropriate for use in a CBDC ecosystem, might also offer benefits for inclusion.

- CBDC ecosystems should avoid reinforcing barriers to financial access and should not introduce any unintended sources of exclusion.

- Countries, in collaboration with international organisations, should work towards developing a wider set of enabling policies, particularly on financial literacy, digital literacy and open and affordable access to digital infrastructure.[17]

Principle 11.
Payments to and from the public sector

Principle 11: Any CBDC, where used to support payments between authorities and the public, should do so in a fast, inexpensive, transparent, inclusive and safe manner, both in normal times and in times of crisis.

- The introduction of a CBDC could potentially enhance the efficiency of payments between authorities and the public, through benefits such as real-time settlement, a more resilient payments ecosystem through provision of an additional payment infrastructure, (potentially) improved coverage of unbanked populations, improved identity verification and the possibility of efficiency-enhancing capabilities of CBDCs. Achieving some of these benefits may require CBDCs to be adopted at scale within a jurisdiction.

[17] Payment Aspects of Financial Inclusion (PAFI)

- Where CBDC ecosystems are used for such transfers, public authorities should commit to use them in a transparent, legally defined manner that protects individual rights and social values.

Principle 12.
Cross-border functionality

Principle 12: Jurisdictions considering issuing CBDCs should explore how they might enhance cross-border payments, including through central banks and other organisations working openly and collaboratively to consider the international dimensions of CBDC design.

- Cross-border payments often face challenges of high costs, low speed, limited access and insufficient transparency.[18] Jurisdictions exploring CBDCs have the opportunity to learn from frictions in current cross-border payments. Through cooperation to consider the potential for cross-border and cross-currency interoperability, central banks could develop complementary CBDCs that might help ease frictions in international payments.

- International use of any CBDC at scale may bring additional considerations for the safe functioning of the international monetary and financial system as outlined in Principle 7. While there are challenges in allowing access for non-residents to CBDCs, an appropriate level and a phased, synchronised approach, of overseas access and use, or the definition of appropriate standards for cross-currency payments, might strengthen the efficiency of international transactions, including remittances and cross-border trade in goods and services.

- Facilitating international payments with CBDCs might be achieved through different degrees of integration and cooperation. In the first instance, countries should engage closely with work at CPMI, the BIS Innovation Hub, the FSB the IMF and the World Bank under Building Block 19 of the G20's roadmap for enhancing cross-border payments adopted in 2020, and factor this work into domestic explorations and design.

Principle 13.
International development

Principle 13: Any CBDC deployed for the provision of international development assistance should safeguard key public policies of the issuing and recipient countries, while providing sufficient transparency about the nature of the CBDC's design features.

[18] FSB delivers a roadmap to enhance cross-border payments

- The G7 supports efforts to achieve the Sustainable Development Goals (SDGs) through development finance, leveraging their own international development institutions and supporting international development efforts through membership of International Financial Institutions (e.g. World Bank, IMF). As the G7 considers CBDC design and use-cases, the risks and opportunities for development assistance are important considerations. Their use should be aligned to the principles of aid effectiveness and effective development cooperation.[19]

- There are certain use-cases where CBDC may be beneficial in the near-term, such as in humanitarian and disaster scenarios. However, there are constraints to using any CBDC for international development, including legal, regulatory and other policy considerations of issuing and recipient countries, including the monetary sovereignty and financial stability of the recipient country. Issuing authorities and development agencies should be transparent on CBDC design, key features and their motivation for use of CBDC in development assistance.

- Relevant IFIs and development institutions should support research and capacity development on CBDCs, in line with the principles laid out in this paper, in addition to drawing on relevant guidance from international standard-setting bodies and member experiences.

[19] Including Paris Declaration and Accra Agenda for Action

Considering CBDC Dependencies

National authorities are carefully considering CBDC objectives and design choices – including understanding where their implications may need to be carefully balanced.

CBDC could offer a range of benefits, particularly the opportunity for more resilient, efficient and inclusive payment services. Given the significant implications of CBDC for our economies and the broader public policy landscape, it is essential that CBDC objectives and design choices are thoroughly evaluated and tested before any launch.

This group has explored the wide-ranging considerations around retail CBDC and the possible implications for public policy. The principles set out in this paper acknowledge that there are a number of policy and design choices which will determine whether a CBDC achieves its desired outcomes. Those principles can help inform national explorations of CBDC, whilst recognising that any decision to launch a CBDC, the objectives it seeks to address, and the particular design choices made, will be sovereign decisions for authorities and legislators in those territories based on their own circumstances and preferences.

The objectives for CBDC and its policy implications will often intersect, and there will be numerous linkages and connections between aspects of CBDC. This could take the form of *'dependencies'*, where decisions made on one aspect of CBDC could have implications for, or be necessary to support the fulfilment of, other goals of CBDC.

Equally, and more challenging, there may be areas where CBDC objectives need to be carefully balanced against each other which may entail choices on how to prioritise certain issues, sometimes referred to as '*trade-offs'*. Therefore, thorough exploration of the implications of these Public Policy Principles and striking a careful balance between them in the design and implementation of any CBDC, will be essential.

The annex to this report discusses these areas further and proposes some high-level approaches that could help navigate them.

Conclusion

No G7 authority has yet decided to implement a CBDC, but it is a topic of strategic importance for G7 central banks and finance ministries who have worked together to explore, and articulate, principles related to public policy implications of CBDC. Decisions on whether CBDC is needed, and the form it might take, are for national authorities and legislators, taking account of their jurisdictions' circumstances, objectives and preferences. However, by setting out a common set of principles, and underscoring the fundamental importance of shared values such as transparency, rule of law and sound economic governance, these principles can guide and inform exploration of retail CBDC in the G7 and beyond.

The principles articulate 'foundational issues' that a CBDC must demonstrate, if it is to command the confidence and trust of users. These includethe preservation of monetary and financial stability, protection of users' privacy, strong standards of operational and cyber resilience, the avoidance of financial crime and sanctions evasion, and environmental sustainability. CBDC also offers a number of opportunities to advance public policy goals, including in respect of innovation and digital economy, financial inclusion, and reducing frictions in cross-border payments.

The design of any CBDC will involve complex decisions, including a need to find a balance between the public policy objectives for CBDC. Whilst the approach to CBDC design may well differ between countries, this report proposes some high-level approaches that could help navigate those dependencies and trade-offs.

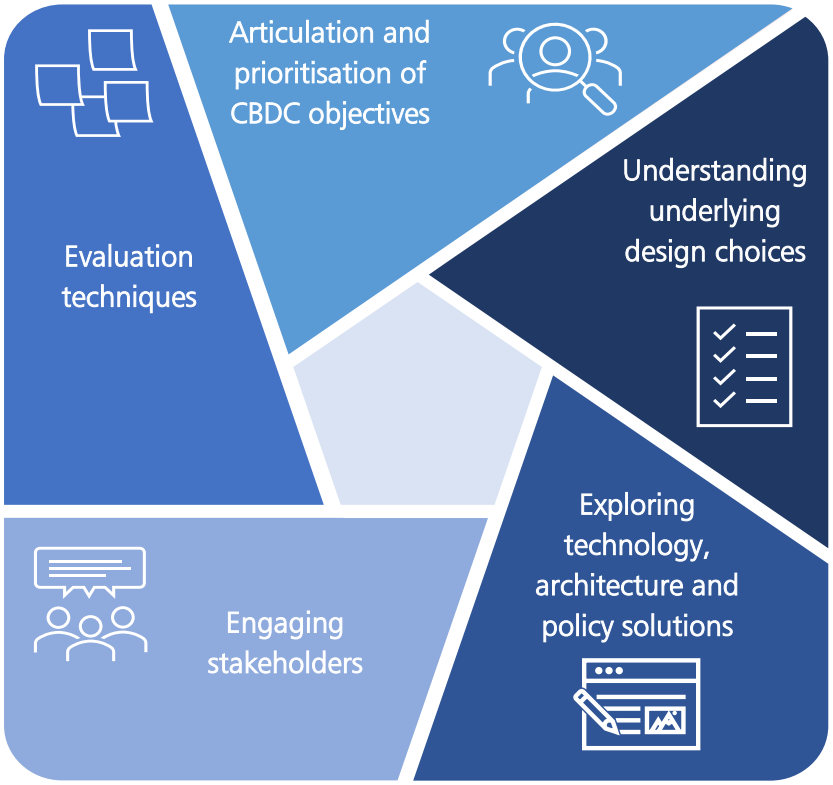
These principles represent an initial articulation of the G7's views on CBDC, but will require ongoing research and analysis, both domestically and collaboratively with international peers. G7 members' domestic exploration and that of other jurisdictions going forward can be supported by the important work ongoing in the international community including international organisations and standard-setting bodies. Through international collaboration, there is a chance to share insights and lessons learned in order to make meaningful progress and realise the potential range of powerful benefits a CBDC may have, particularly the opportunity to harness innovation to deliver resilient, efficient and inclusive payments.

Annex A: CBDC Dependencies

Possible approach to 'dependencies' between Public Policy Principles.

Deciding how to navigate 'dependencies' and striking the right balance between priorities is one of the most challenging, but also critical, aspects of CBDC exploration. Given the complex and delicate nature of the issues involved, and the range of national circumstances, a 'one size fits all' framework would be impossible. Nevertheless, there are some high-level approaches that can be helpful.

Figure 1 Possible approach to dependencies between Public Policy Principles



- Articulation and prioritisation of CBDC objectives: Dependencies generally stem from connections, and sometimes, possible tensions between CBDC objectives. A clear articulation, and where possible a structured prioritisation of those objectives, provides the foundation for successfully understanding the relative balance between objectives. To manage dependencies and trade-offs in particular, a realistic assessment of priorities between CBDC objectives is essential.

- Understanding underlying design choices: CBDC objectives are implemented through design choices (e.g. who can access the CBDC, what data is used). As such the decisions made on design choices will determine how interdependencies are addressed. An example may be determining the level of identity verification to require, to access a CBDC system;

the choice here will also have an effect on who can access the system generally and therefore wider objectives for financial inclusion. Judgements on "where to set the dial" on a particular design choice will have a critical bearing and making well considered decisions on design can help optimise for the best outcomes where objectives may need to be balanced.

- Evaluation techniques: There are techniques which may help explicitly evaluate the implications ahead of deciding how to balance dependencies in CBDC objectives and design, rather than making decisions implicitly or as a by-product of some other choice (e.g. due to a preference for a particular technology). Many of these techniques will be qualitative, but quantitative methods and cost benefit analysis approaches could add value. It is also imperative that evaluation of dependencies looks at CBDC 'holistically' and recognises the process of determining dependencies is a multiple attribute decision making process.

- Exploring technology, architecture and policy solutions: Addressing dependencies and, in particular, balancing trade-offs can require difficult policy choices to be made. However, opportunities around CBDC architectures (e.g. data restriction and segregation, use of public key infrastructure technology for security and data protection), new technologies (e.g. privacy enhancing technologies, tracing technologies) and policy interventions (e.g. reiteration of risk-based approaches to aspects of financial crime compliance) might help to optimise outcomes.

- Engaging stakeholders: A wide range of stakeholders will have views on, and interest in, how dependencies are managed. The views of stakeholders should be sought and accounted for in an open and transparent manner. In addition, CBDC ecosystems are usually expected to include a mixture of public and private actors; the approach to balancing trade-offs will need to take into account the interaction with consumers, merchants and providers, each of whom might make choices which influence how interdependencies play out.

Our discussions revealed a large number of areas of dependence, and the need to consider Public Policy Principles holistically.

Through exploration of the principles we put forward, we identified that there are a wide ranging series of areas where dependencies are likely to exist. Those areas and dependencies are likely not homogeneous and there will be a need for jurisdictions to consider such issues holistically. Those principles we considered as 'foundational' may have the strongest bearing on other policy objectives. Principles for monetary policy and financial stability, legal and governance frameworks and important commitments to data privacy, resilience and the countering of financial crime are likely to be strongly linked to other objectives for CBDC. Equally, for many of the principles identified as 'opportunities' there are many interdependencies present where objectives will need to be balanced. This emphasises that optimising for one, or a small number of, CBDC objectives

or design features is unlikely to produce the best overall outcome given the range of considerations and interactions in play.

Carefully balancing CBDC design options with respect to Public Policy Principles is essential, given it may be challenging to realise a CBDC design which can simultaneously optimise outcomes across all the principles identified.

The principles in Section One of this paper outline important implications of potential CBDCs for public policy objectives, and considerations that can help guide exploration of CBDC. National choices will determine how any CBDC might adopt and implement these principles; but all are highly relevant considerations for CBDC design. Beyond considerations around monetary and financial stability and legal frameworks, the CBDC design choices that have a bearing on resilience, security and integrity will be fundamental to trust and confidence in the CBDC ecosystem. These are fundamental criteria that must be satisfied to the fullest degree. Given that CBDC would likely be critical infrastructure, there would be very little room for flexibility on objectives like operational resilience and cyber security, data privacy or tackling illicit finance.

However, delivering the highest of standards in those 'fundamental' areas might present difficult decisions with regard to other important objectives such as supporting innovation, competition and financial inclusion. Authorities should be mindful of the need for appropriate balance within these trade-offs as they explore CBDC. These effects might occur, for example, were security or resilience requirements to act as a barrier to smaller businesses, perhaps with less operational and technology resources, from acting as intermediaries in a CBDC ecosystem. Alternatively, were financial crime compliance requirements or privacy concerns to limit the ability (or indeed motivation) of certain prospective user groups to access CBDC (and the basic payments services it could provide them), that may impact objectives around utility and financial inclusion. A snapshot of some of these considerations, both between objectives but also with critical factors such as adoption, are set out in Figure 2.

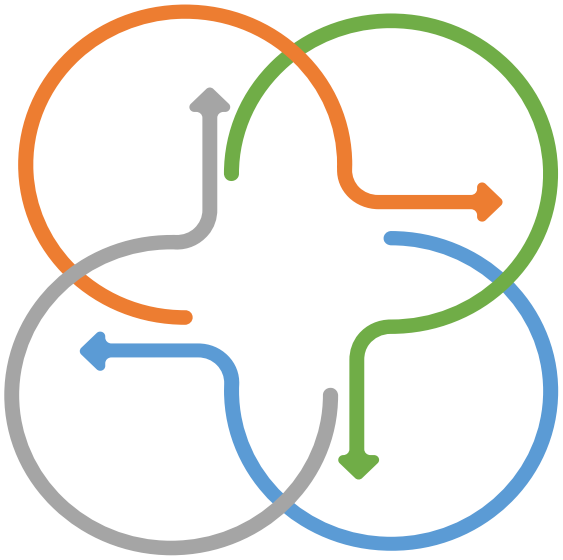
Figure 2 High level considerations related to dependencies between some principles

OPERATIONAL RESILIENCE VS DIVERSITY AND COMPETITION

CBDC will be critical infrastructure, so operational resilience is of upmost importance. But compliance requirements to deliver this resilience may risk excluding smaller firms with fewer resources from participating and may limit diversity and competition.

CYBER SECURITY VS SYSTEM PERFORMANCE, UTILITY AND ADOPTION

Cyber resilience and system security is fundamental to trust and confidence – a system at risk of breach will not be used. But any requirements may have knock-on implications for system performance (speed, range of functions including the potential applications of programmability). This, in turn, may impact CBDC adoption and utility, particularly in how far such CBDCs can support innovation.



REDUCING ILLICIT FINANCE VS PRIVACY AND INCLUSION

CBDC systems might enable enhanced transparency and rigorous standards of documentation and verification which are not possible with cash. This could help reduce illicit finance and ensure sanctions compliance. But this could have implications for users' privacy and the ability of those without documentation to access the CBDC system.

PRIVACY VS DIVERSITY IN BUSINESS MODELS AND FINANCIAL INCLUSION

Strong standards of privacy support inclusion by giving confidence to use CBDC. But strict restrictions on data use could serve to reduce the range of possible business models in a CBDC system, and increase costs to users, which could deter use or encourage the use of less private alternatives.

In developing CBDCs, jurisdictions should take a rounded view of the Public Policy Principles and it could be important to consider how to calibrate this prioritisation of the principles (where some are relatively fixed, versus others where there may be more flexibility in approaching how to balance the principles). It is essential to consider whether mitigating actions could be taken via parallel policy interventions, or technology opportunities.

Diving deeper into specific dependencies:

Whilst it is not possible to explore all dependencies in detail in this report, the group have dived deeper into three specific areas to provide a greater insight into their analysis.

1 Protecting Users' Privacy Whilst Reducing Opportunities for Illicit Finance:

What is the possible dependency: CBDC may offer opportunities for greater transparency in payments including potentially better standards of identification and verification of transactions. However, depending on design choices, this may involve some reduction in user privacy. In making this comparison, it is essential to note that privacy does not require full anonymity in payments.

What is the design choice: Which entities in a CBDC ecosystem will have access to what data for what purpose?

Relevant considerations: Determining the level of access to information for specific purposes is not a new debate – and indeed is something existing payment systems have to manage. Access to and use of data is core to the function of all electronic payments, including CBDC. Data is needed to process, authorise and validate transactions; it is important to have data accompanying a payment both to allow the right payment to be transferred and for security reasons. Increasingly users are conscious about the data generated in their daily activities including payments.[20] Firms would like to harness data to learn more about their customers and payments habits, and payments operators need this information for critical security functions and know-your-customer protocols to avoid money being used for illicit uses. There are a number of other potential uses for data in a payment but, when considering the design of a CBDC, jurisdictions must consider how to balance user trust and security with the need to counter illicit finance (such as the financing of terrorism and money-laundering and respect targeted financial sanctions).

Possible policy and technology solutions: CBDCs, like existing digital payments, must comply with AML/CFT regulations and requirements and are subject to international standards established by the FATF. The identity of a CBDC user would need to be verified/authorised by at least some regulated entity in the CBDC ecosystem, but not necessarily all. Optimal solutions are likely to be different for differing models of CBDC. For example, for one possible model a jurisdiction may take a core ledger operated by the central bank and might only store pseudonymous CBDC balances, but a user's private service provider (e.g. their digital wallet) would know/verify the user's identity. That private sector provider would likely be responsible for applying AML/CFT checks to users and reporting suspicious transactions, among other obligations, to the authorities in this case. This is just one possible model that an individual jurisdiction might choose. An alternative might involve dedicated (private) verification entities who could verify users' identity and harness new techniques to identify and report suspicious activity.

[20] In a recent survey (Whom do consumers trust with their data? US survey evidence), US households say they are more likely to trust traditional financial institutions than government agencies or fintechs to safeguard their personal data. They have far less trust in big techs.

2 Operational Resilience and Cyber Security vs Performance and functionality:

What is the possible dependency: To be adopted widely, a payment instrument must maintain the trust of its users (that it can successfully be used and transferred to others) and be as fast, convenient, and easy to use as other successful payment methods. As such, both the operational resilience and cyber security of any CBDC ecosystem and the convenience and functionality provided itself will have important implications on CBDC's ability to achieve its wider objectives. If specific resilience specifications for CBDC proved onerous and began to affect performance or speed of the infrastructure, this might reduce the functionality or usefulness of CBDC and deter adoption or holding of such CBDC.

What is the design choice: Does the preferred level of resilience and security affect the performance of CBDC infrastructure?

Relevant considerations: Given recent developments in cybersecurity technology and research, one way to enhance the resilience of payments may be duplication of data and processes across multiple data centres and locations (distribution). Using decentralisation may go even further in involving multiple entities in the process.[21] Adding diversity to the ecosystem could be beneficial in ensuring that problems that arise in one type of technology or location (possibly from a malicious attack) do not compromise the whole network. Conversely, these additional nodes create more targets for attackers (for example those looking to steal data or disrupt operational activities of a CBDC). Additionally, infrastructures which are decentralised and require communication between multiple data centres for the processing of each transaction are likely to be relatively slow,[22] and may encounter challenges with scalability and responsiveness. This would ultimately detract from the objective to support an innovative digital economy through providing convenient and efficient payments to users.

Operational resilience goes to the heart of central banks role in payments and is essential in maintaining financial stability within the wider financial system. It would be untenable for any of our jurisdictions to make compromises on security and resilience within any CBDC infrastructure. As such, we recognise that jurisdictions will have to carefully assess the appropriate technology and respective implications for resilience and functionality. Research into new technologies may therefore be a vital part of any jurisdiction's exploration of CBDC.

Possible policy and technology solutions: G7 authorities have comprehensive approaches to operational resilience and cyber security management, and central banks have extensive experience of safeguarding the essential financial infrastructure they operate. In the case of CBDC, this will require close engagement and collaboration with the private sector given their likely role in possible CBDC ecosystems. It may be that certain technical choices can optimise resilience and security whilst also improving functionality. A recent experiment by the Bank of Italy[23] provides

[21] Resilience considerations of CBDC infrastructure were also explored by the Group of Central Banks with the BIS in Oct 2020: Central bank digital currencies: foundational principles and core features

[22] Advancements in computing are improving speeds.

[23] A digital Euro: a contribution to the discussion on technical design choices

an example of potential mitigation measures (for example, the use of a decentralized solution like TIPS, possibly replicated on multiple nodes, could overcome this trade-off, combining the resilience of decentralized architectures with very high performance, such as 40,000 transactions per second). Frameworks such as the G7 fundamental elements for cybersecurity, threat-led penetration testing, expectations for business continuity, as well as ongoing engagement with national cyber security agencies can also help to ensure the resilience of the ecosystem from the perspective of both private and public participants.

3 Cross-Border Access vs Minimising Spillovers:

What is the possible dependency: Supporting effective cross-border payments could require foreign nationals or overseas residents to have access to a jurisdiction's CBDC. Whilst this could have many benefits it could also run the risk of currency substitution should adoption occur at scale.

What is the design choice: What level of access (if any) should non-residents have to a jurisdiction's CBDC?

Relevant considerations: Today, central bank money is only available to consumers in the form of physical cash. Cash can be exchanged hand to hand between people of a sovereign nation and can be generally held by those who live outside the country, particularly tourists and business travellers. In issuing a CBDC, there is an overarching question about which individuals or entities can access and transact in any CBDC.

CBDCs could enhance cross-border payments through interoperability between different CBDCs and/or an appropriate degree of non-resident access to a given CBDC. Access by non-residents would enable visitors to spend in CBDC and could thereby also be an important factor in how attractive it might be for merchants to accept CBDC payments. However, significant use or holdings of any particular CBDC by residents of a foreign country could lead to currency substitution and loss of monetary sovereignty in that foreign country. Interoperability between CBDCs may subsequently enable greater cross-border financial flows, which could also have macro-financial consequences. These risks, commonly identified as spillovers, are impacts a central bank will want to minimise. However, without tangible insights into a widely used CBDC, it is hard to estimate their full impacts and central banks continue to explore these effects. Another area to consider is the role of cross-currency payments in respective CBDCs, which may not require individuals to directly access different CBDCs but require back-end interoperability. Careful consideration and close international coordination for CBDCs is imperative to ensure good compliance with AML/CTF requirements as well as the stability of the international monetary system.

Possible policy and technology solutions: The 2021 BIS survey on cross-border CBDC[24] suggested most central banks exploring a form of CBDC are yet to make a decision around both access and potential controls to mitigate spillovers. The joint report to the G20 on CBDC for cross-border payments[25] concluded that CBDCs could help to enhance cross-border payments when authorities coordinate internationally. Facilitating international payments with CBDCs can leverage different degrees of integration and cooperation, ranging from basic compatibility with common standards to the establishment of international payment infrastructures. The analysis highlighted both the need for multilateral collaboration on macrofinancial consequences as well as the importance of interoperability between CBDCs.

[24] CBDCs beyond borders: results from a survey of central banks

[25] Central bank digital currencies for cross-border payments: Report to the G20

Annex B: Acknowledgements

This report was compiled by the CBDC drafting group which brought together experts on CBDC and digital payments from respective finance ministries, central banks of the G7 alongside invited contributors from other central banks and international organisations who have lent their expertise and perspective to this report. We would like to thank those experts for their contributions to the report. Alongside these members we would like to thank the Financial Services Agency Japan, Sveriges Riksbank, Swiss National Bank, IMF, WBG, BIS Innovation Hub and the OECD for their valuable contributions to the discussion.

Organisation	Representative(s)
Bank of Canada	Scott Hendry *Senior Director, Financial Technology*
Department of Finance Canada	Nicolas Moreau *Director General, Funds Management Division*
Banque de France	Anne-Catherine Bohnert *Deputy Head of the Digital Currency and Innovation Department*
French Ministry of Finance	Pierre-Olivier Chotard *Head of Unit Banking Services and Means of Payment*
Bundesbank	Dr Heike Winter *Head of Section, Digitalisation in Payments*
BMF/German Ministry of Finance	Matthias Mueller *Global Economy Lead*
European Commission	Peter Kerstens *Advisor – Digitalisation, Technological Innovation and Security, DG FISMA*
European Central Bank	Naisa Tussi and Kalina Tylko-Tylczynska *Market Infrastructure Specialist and Economist*
Banca d'Italia	Giuseppe Ferrero *Research Department*
Italian Ministry of Finance	Mattia Suardi *Policy Officer*
Bank of Japan	Masaki Bessho and Takeshi Yamada *Payment and Settlement Systems Department*
Ministry of Finance Japan	Kohei Asao *Deputy Director, International Bureau*

Financial Services Agency Japan	Yuji Kawada *Deputy Director*
Sveriges Riksbank	Gabriela Guibourg *Head of Analysis and Policy, Payments*
Swiss National Bank	Thomas Moser *Alternate Member of the Governing Board*
Bank of England	Tom Mutton (co-Chair) *Director of CBDC*
HM Treasury	Laura Mountford (co-Chair) *Deputy Director, Payments and Fintech*
Federal Reserve Board	Ruth Judson and Jean Flemming *Senior Economic Project Manager and Economist*
US Treasury	Julia Smearman *Deputy Director*
BIS Innovation Hub	Codruta Boar *Adviser*
IMF	Tommaso Mancini-Griffoli
OECD	Oliver Garrett-Jones *Counsellor to the Director of Financial and Enterprise Affairs*
World Bank Group	Ahmed Faragallah and Tatiana Alonso Gispert *Senior Financial Sector Specialists*
Joint secretariat by Bank of England and HM Treasury: Alisdair McDade, Priya Mistry, Manisha Patel, David Song, Sasha Spyrou, Michael Yoganayagam	