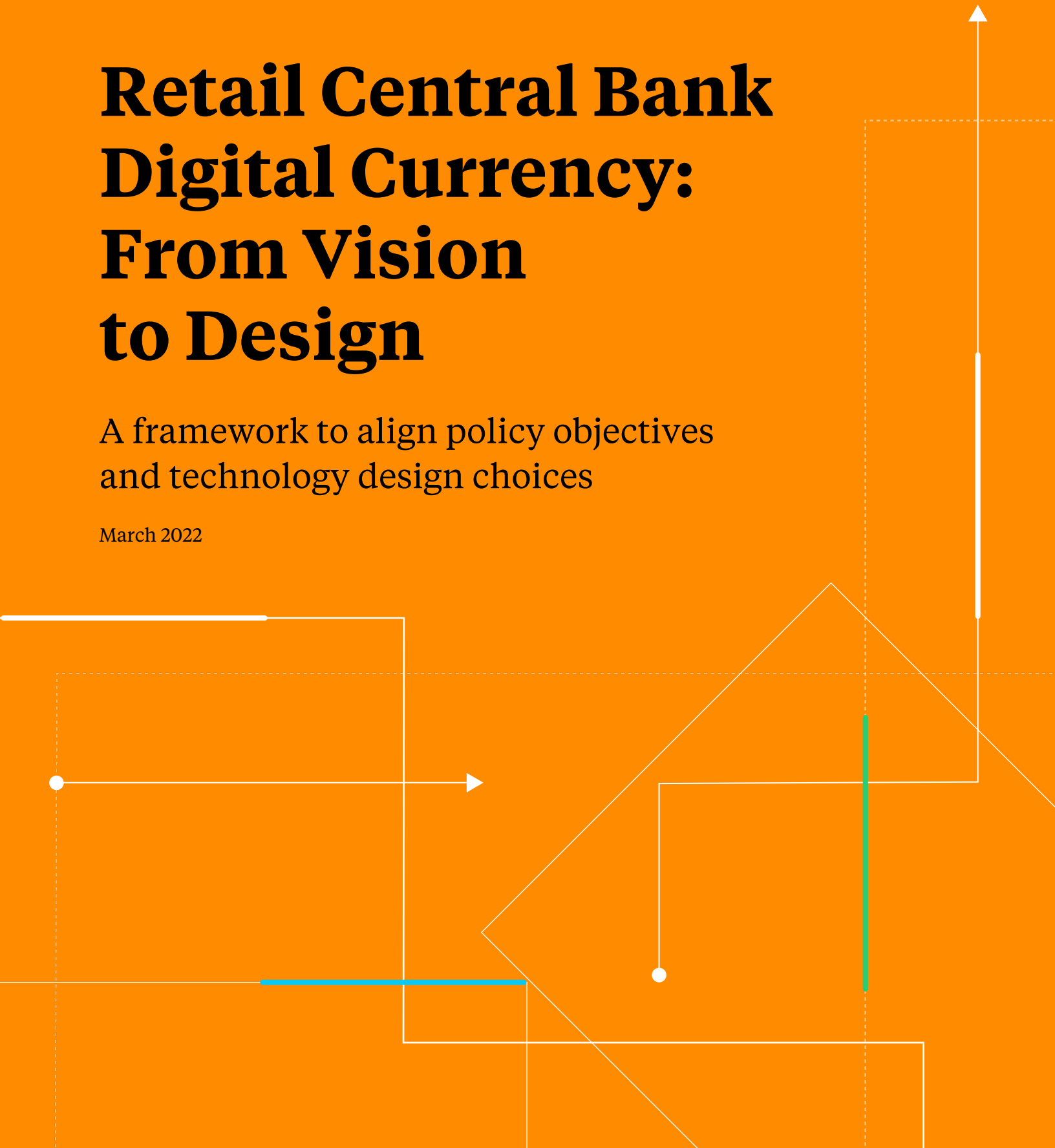
OliverWyman Forum | aws

Retail Central Bank Digital Currency: From Vision to Design

A framework to align policy objectives and technology design choices

March 2022



Why read this report

Over 80 countries[1] worldwide are currently researching the possibility of launching a central bank digital currency (CBDC). Proponents of CBDCs believe they have the potential to build a more efficient, secure, and inclusive monetary system, while others often question how this would be achieved. Many studies[2] on this topic tend to fall into two categories: some cover what policy objectives a CBDC may help deliver and its implications on the financial system and the general public, while others cover the different technology (for example, network protocols, transaction processing logic) and architecture (for example, direct, two-tier, synthetic) options for designing a CBDC.

However, the literature on the relationship *between* policy objectives, technology design choices and competitive dynamics is still relatively limited. Understanding these relationships is critical not only for evaluating and determining whether to launch a CBDC, but also for developing a tailored design. Beyond core technology decisions, system design configurations are impactful in shaping a solution to build in desired system attributes, such as privacy and data sovereignty. For this reason, the Oliver Wyman Forum and Amazon Web Services (AWS) have decided to collaborate to:

- Highlight policy choices and trade-offs that should be considered early in the design process,
- Assess what technology design choices are particularly sensitive to policy drivers,
- Detail how policy and technology design choices may impact competitive dynamics depending on the available roles for the private sector in the delivery of a CBDC,
- Illustrate how different jurisdictions may opt for different design configurations.

We provide a framework for central bankers, technologists, and impacted stakeholders to discuss together whether and how a CBDC solution can be designed and evolve to fit their policy goals.

[1] See Atlantic Council CBDC Tracker
[2] See literature review in Appendix B

Lead Authors

Larissa de Lima
Senior Fellow, Future of Money Initiative
Oliver Wyman Forum

Erica M Salinas
Principal, Digital Assets
Amazon Web Services

Contributing Authors

Douglas J Elliott
Partner, Financial Services & Public Policy
Oliver Wyman

Jean-Baptiste Lepetit
Principal, Financial Services & Digital Transformation
Oliver Wyman

Ramiro de la Rosa
Director of Strategic Partnerships
Oliver Wyman

David MacKeith
Principal, EMEA Federal Financials
Amazon Web Services

Paul Cauchon
Solutions Architect, Federal Financials
Amazon Web Services

Acknowledgments

We would like to thank Tom Buerkle, John Cann, Paul Cantwell, James Emmett, Alenka Grealish, Michael Gurock, Shamarah Hernandez, Dustin Irwin, The Kiffmeister, Ugur Koyluoglu, Filidausi Mbatudde, Francine Minadeo, Layla Mosadegh, Ben Power, Marcelo Prates, Tracy Raissis, Rob Robinson, Ayo Roque, Adrien Slimani, Michael Wagner and Xiaochen Zhang for their invaluable contributions.

We also thank the many excellent early reviewers of the paper who have been helpful to us at central banks, government agencies and regulatory bodies who prefer to remain anonymous.

Disclaimer

Policy perspectives and competitor considerations in the report reflect research and interviews conducted by the Oliver Wyman Forum. AWS provided technology guidance and CBDC considerations based on work with its public sector customers.

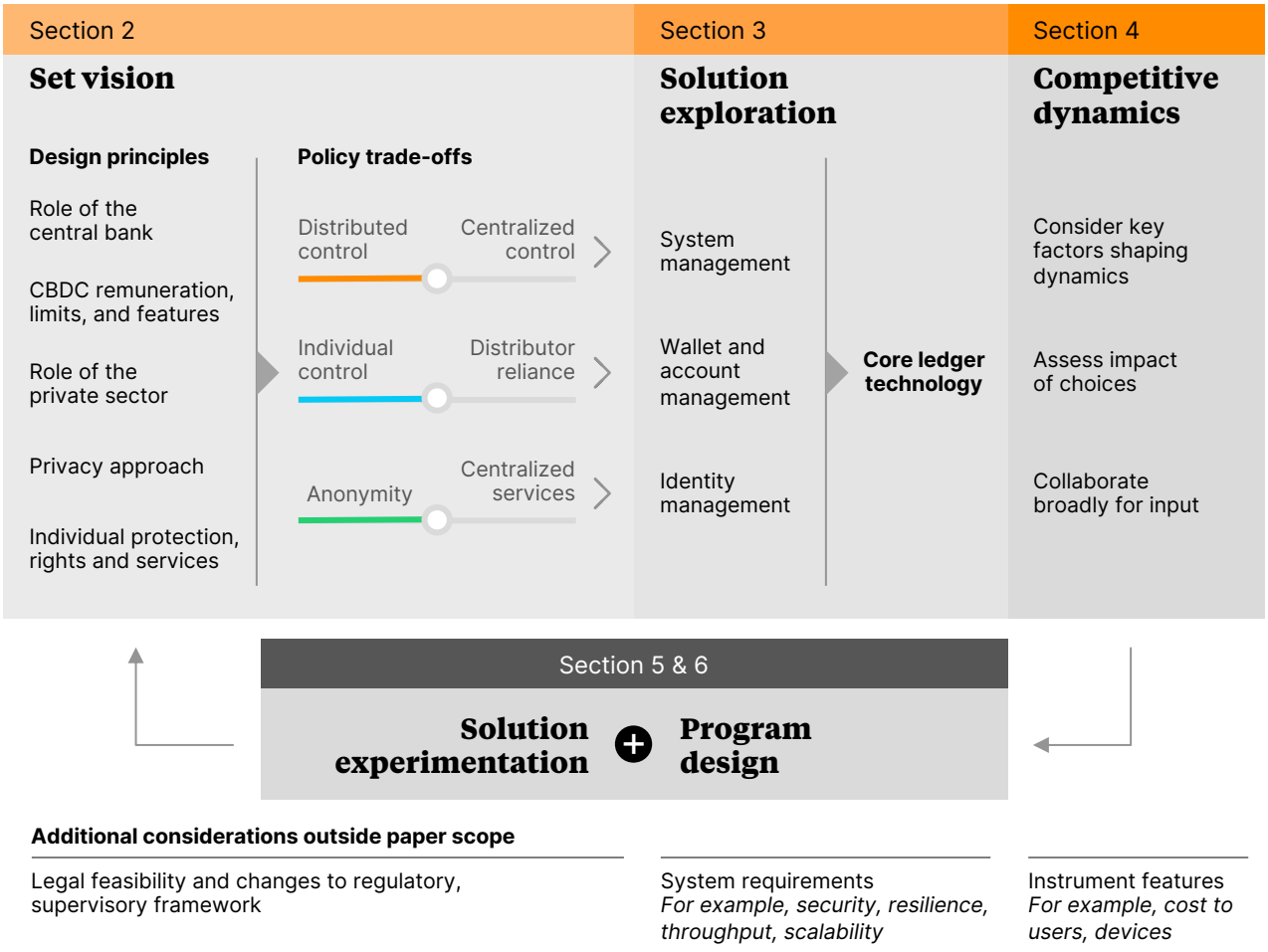
Table of contents

Executive summary

The advent of private sector digital currencies, and their growing usage, combined with the reduction in everyday use of physical cash in parts of the world opens up new opportunities and risks for central banks. In response, many countries are researching the possibility of launching a retail central bank digital currency (CBDC). However, many different approaches and designs are being considered given the different needs and situations of each country. The wrong design could lead to an inadequate system or even have an unintended negative impact on the financial services industry.

Developing a CBDC is a complex undertaking, given the interdependencies between policy and technology choices, as well as potential market impacts. This paper does not make any recommendation as to whether a central bank should introduce a CBDC or on which solution choice to adopt if they do. Rather, we propose a framework to support policy makers in evaluating these interdependencies as they develop their research programs and consider technical experiments. Given time and length constraints, we could not cover all relevant policy and technology choices. Therefore, we cover decisions that are highly interconnected or are currently underdiscussed. Additional factors will matter to policy makers and stakeholders, but are outside the scope of this paper. Figure 1 below summarizes our CBDC strategy design framework, which highlights those design principles most likely to impact design choices, and vice versa.

Figure 1. From vision to design: a CBDC strategy framework



Source: Oliver Wyman Forum and AWS Analysis

First, central banks should **set a clear vision** for what a CBDC would be designed to achieve. Clear high-level objectives, with at least broad prioritization, should underpin all exploratory efforts. These objectives for a CBDC must be considered in the context of the full range of issues related to payments, stablecoins, other types of digital assets/currencies, and surrounding economic and social circumstances. At each step of the journey in exploring whether or not to launch a CBDC, central banks should return to their vision and assess whether the system being designed fulfills that vision.

This vision should be further detailed through **high-level design principles**. A CBDC design requires trade-offs, as all objectives may not be fully achievable with a given technical solution and CBDCs may need to compete with other solutions in the market. Clear design principles, informed by a clear vision, can guide these trade-offs and avoid the need to backtrack on initial decisions. Key design principles discussed here include the approach to privacy and individual protections, mechanisms to manage CBDC adoption, and the division of roles and responsibilities between the public and private sector.

Next, policy makers should strive to **understand technology design choices**. Literature to date has discussed choices around ledger technology (distributed ledger technology (DLT) versus conventional databases) and their associated data structure (which either captures individual CBDC units or maintains a combined balance for an individual's account). We find that these decisions are overstated in significance. For many policy decisions, any combination of these two choices can meet a wide variety of policy needs. In contrast, architecture and design choices (for example, roles and information flow between participants) are more sensitive to policy decisions and require specification early in the design process. Creating technical solutions that are both flexible enough to accommodate unclear or changing policy objectives and still produce sufficiently optimized results is difficult. However, policy makers can build degrees of flexibility into architectural design that will help enable experimentation and iteration.

Policy makers should also **evaluate market incentives and dynamics** embedded in these design choices. Many central banks are collaborating with financial institutions and other stakeholders in considering the role of the private sector in delivering CBDCs. Policy and technology choices will drive what functions various actors can perform, how information flows, and how service providers gain access to the CBDC system. As a result, different technical solutions will produce different competitive dynamics and data-driven network effects. Thus, when evaluating CBDC design choices, the private sector should be a critical participant in analyzing what incentives and business models will create the conditions for innovation and competition in financial services while best enabling the system's maintenance, resilience, and continued enhancement.

Engaging with a cross-section of stakeholders to make design choices depends on having a shared understanding of the central bank's policy vision and any required trade-offs. To illustrate how different policy visions may translate to different technological solution choices, **we present four archetypes** of central bank policy goals, covering a broad range of commonly stated motivations. For each archetype, we illustrate what design choices could be made to meet policy objectives and the extent to which compromises are necessary. Policy makers could benefit from building their own archetypes of possible design choices to promote public debate and understanding.

The **Path Forward** for policy makers, as they decide whether or not to pursue a CBDC, is long and includes considering a wide range of issues not covered in this report, spanning legal considerations, system requirements, and instrument features. Ensuring clear policy goals to drive the CBDC vision requires significant societal input, while the complexities require significant collaboration between policy makers, technologists, and impacted stakeholders. Competitive structures are necessarily dynamic, so while it is critical to have an initial hypothesis and high-level objectives, it is also important to plan for learning and allow for the ability to change course.

BOX A. Getting it right: aligning technical design choices with policy goals

Do

- ✓ Ensure clear policy goals, with a preliminary prioritization, are established early in the design and research process
- ✓ Decide where to stand across three key policy trade-offs: providing anonymity versus centralized identity-based services, allowing more individual self-reliance versus a reliance on distributors, and maintaining distributed versus centralized control
- ✓ Bring technologists into the CBDC design discussions early
- ✓ Align technology design decisions to policy objectives, while diving into configuration options within the CBDC core system
- ✓ Engage early and frequently with a broad set of constituents
- ✓ Clearly define the business cases for adoption and maintenance of the infrastructure
- ✓ Prioritize decision making about how identity will be managed, with understanding of downstream impacts
- ✓ Be mindful of how access to data impacts competition, developing clear hypotheses of where network effects will likely emerge and how they might be captured

Don't

- × Assume a CBDC is the right solution for any given set of policy goals without investigating its fit to your jurisdiction, as well as comparing it to alternative solutions
- × Fixate on the choice of ledger technology, but look instead at key solution dimensions such as the degree of centralization of transaction processing and the way CBDC accounts and wallets are managed
- × Consider policy issues in isolation from one another or try to solve for everything simultaneously: instead, frequently revisit the policy vision and priorities to determine how to manage trade-offs
- × Hold off on scenario building, economic modeling, and technical experiments, as these can help make policy principles more tangible and surface new trade-offs
- × Make assumptions about the role of distributors without including them in the design and testing process
- × Ignore the impact of policy choices on competitive dynamics
- × Assume building a CBDC system is a "one and done" at launch as it will require ongoing monitoring, maintenance, and evolution to keep pace with innovation

Source: Oliver Wyman Forum and AWS Analysis

Section 1. Focus and assumptions

As defined by the Bank for International Settlements (BIS),[3] a CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank. CBDCs span wholesale and retail CBDC or national versus cross-border use cases. For this analysis, **we focus on CBDCs within national borders** and **accessible to individuals**, known as "retail CBDCs."

In a few of the solution configurations explored, access for retail use is entirely in the domain of the private sector, with end-user data including identity and transactions also managed by the private sector. However, individuals (or merchants) would still be able to access and claim liabilities of the central bank balance sheet, with payments made and settled in CBDCs. This is in contrast to "wholesale CBDCs", which are central bank liabilities accessible exclusively to institutions and meant to provide a final means of settlement for high value payments made with deposits or other types of private sector monies.[4]

We further refine our focus by assuming a "two-tier" CBDC in which the central bank relies on private sector participants to act as intermediaries, serving as the gateway between individual users of CBDC and the CBDC system itself. In this paper we refer to the providers of gateway services as "distributors." As we will explore in detail in this paper, these distributors serve a critical role and can fulfill a range of other functions, from operating CBDC core system infrastructure to providing tailored end-user services. Defining the role of the distributor is at the heart of solution design choices.

The launch of a CBDC would require adapting existing money movement rails, and/or building entirely new ones, and thus requires a series of difficult choices. This endeavor presents countries with an opportunity (among others) to reimagine their payment systems to fulfill a clear policy vision. Success will require being amenable to change as well as reconciling policy, technology and market impact.

Many central banks are at a stage in their explorations where the structure of a future CBDC system should be outlined with sufficient clarity so as to launch targeted technical experiments, while maintaining maximum flexibility to tailor the final system in line with public consultation, changing policy priorities, and the outcomes of technical trials.

Our contribution in this paper is to support central banks as they seek out how best to meet their policy goals by providing a framework in which to evaluate the interrelation of desired design principles with available solution design decisions. In Appendix B, we expand on how our paper connects to the broader literature.

Given time and length constraints, we could not cover all relevant policy and technology choices. We therefore highlight decisions that should be considered early as they are highly interconnected or are currently underdiscussed. There are many additional factors that will matter to policy makers and stakeholders within the financial system that are important to recognize but are outside the scope of this paper. For example, on the policy side, central banks are exploring connectivity between retail, wholesale and cross-border CBDC projects. Policy choices may also be constrained by legal considerations. As policy makers refine their choices, impact on regulatory and supervisory frameworks are likely to come into consideration.

[3] See the Glossary of BIS (2020): Central banks and payments in the digital era, Annual Economic Report, Chapter III.
[4] See for example the "Money Flower" first introduced in Bech, Morten L. and Garratt, Rodney (2017): Central Bank Cryptocurrencies, BIS Quarterly Review September. Wholesale CBDCs may be analogous to reserve systems, but could differ from existing real-time gross settlement solutions by making central bank balance sheet available 24/7 and exploring technologies that enable programmability or direct peer-to-peer payments between institutions.

Central banks that move forward with a CBDC will universally want the system to meet several key technical requirements, such as security, resilience, and scalability. For these characteristics central banks are likely to build on their experience, if applicable, with existing fast payment systems[5] and to leverage best practices developed by leading cloud services providers.[6] The technological solution design decisions discussed here are possible across a spectrum of ledger types, data structures, and infrastructure types. Thus, these technical requirements must first be met by the underlying platform and then extended to ensure that they are also supported through the implementation of the described solution design decisions.

[5] M Bech, J Hancock and W Zhang (2020): Fast retail payment systems, BIS Quarterly Review, March.
[6] One example is AWS Well-Architected framework, which helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads.

Section 2. Defining a CBDC vision

2.1. Purpose statement

2.2. Design principles

2.3 Trade-offs

CBDCs have been proposed as one solution to a wide range of distinct policy challenges, from a declining use of cash to financial exclusion and distribution of humanitarian aid to a perceived need for faster payment processes to challenges arising from the increasing popularity of private currencies. No system will be the best possible means of addressing all potential goals. For example, a central bank that primarily aims to introduce a digital asset closely analogous to cash will adopt a different system design from one that primarily seeks to improve cross-border payments.

As central banks begin researching the technical implementation of a CBDC, they will face a number of design decisions that will shape the high-level architecture of the system. These questions can be satisfactorily answered only by taking a clear view of the problems that a central bank is trying to solve, and therefore the type of tool it seeks to build. Setting a vision is thus a critical step in dictating the technical and operational parameters within which a CBDC must operate.

Defining a vision will require continual engagement with the government, the public, the various institutions that may play a role in the new CBDC system, and the various entities that are likely to be impacted by the implementation of a CBDC.

In Section 2.1 we recommend that central banks start by creating a concise summary (or "purpose statement") to provide clarity about the primary objectives a CBDC would be designed to achieve. Additionally, we introduce policy choices in Section 2.2 and trade-offs in Section 2.3 that are important to make early on, as they help align vision with implementation and determine what technical experiments will help to ensure an optimal design.

Key takeaways from this section:

- Investigation into whether to launch a CBDC, and if so, how to design it, must start with clear high-level objectives, which need at least broad prioritization.
- Key policy choices include the approach to privacy and individual protections and rights, CBDC remuneration, and the division of roles and responsibilities between the public and private sector.
- Policy makers should encourage public debate and stakeholder input to decide where to stand across three key trade-offs: providing anonymity versus centralized identity-based services, allowing more individual self-reliance versus a reliance on distributors, and maintaining centralized versus distributed control.

Policy and technical options often fall along a spectrum. Understanding how those options are interrelated can support a solution configured to optimize any required trade-off.

2.1. Purpose statement

In evaluating the purpose of a CBDC system, central banks should begin with the specific local context. What are the most pressing societal objectives that a retail CBDC might achieve, and are there equally important goals that a CBDC must not undermine? Other relevant questions for central banks to consider at this stage include:

- Do current payment systems provide sufficiently wide coverage of services to meet the needs of all citizens and businesses?
- Do current financial service providers face healthy competition to encourage continual innovation and competitive pricing?
- Should a CBDC system be designed to integrate with a digital identity system for citizens? And if yes, how?
- Is innovation in financial services a priority and how would a CBDC complement (or undermine) any existing initiatives such as open banking programs or new real-time payment systems?
- How would a CBDC system fit in with and/or support existing government plans for a digital economy? What are adjacent and supporting policies?
- Does the existing financial system infrastructure have weaknesses in terms of resilience and/or over-reliance on a limited number of existing digital platforms?

CBDCs have the potential to serve as either a complement to or replacement of each of the different existing and emerging payment instruments: cash, deposits, stablecoins, etc. Central banks should determine where they want adoption to be focused on a limited number of specific use cases or widespread to bring about more significant transformation. Figure 2, below, includes some potential roles for a CBDC system, which are illustrative rather than comprehensive. The desired role of a CBDC may evolve with policy objectives but starting with a clear unifying goal will help align other policy decisions.

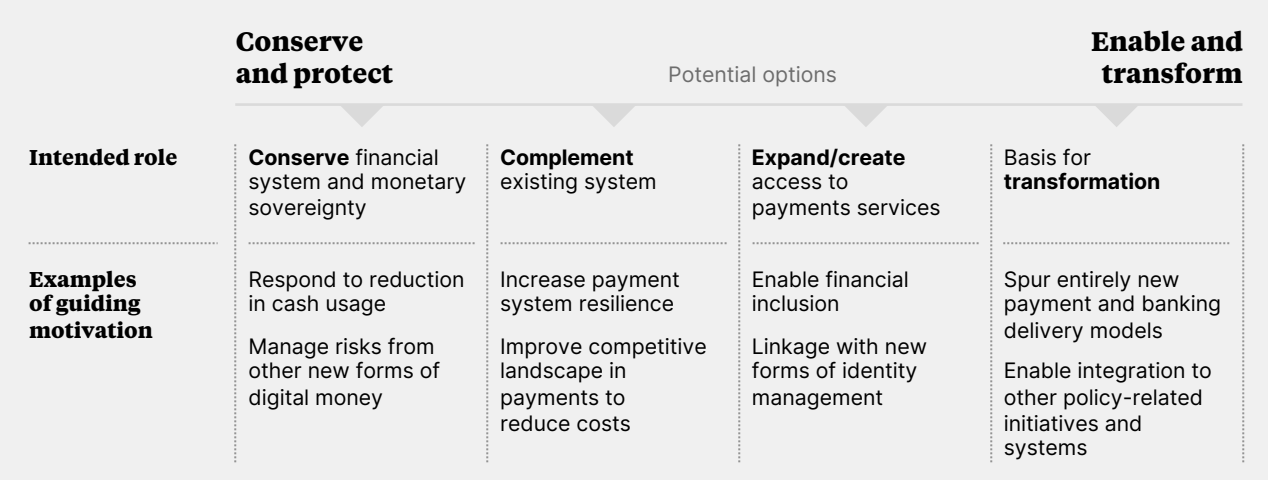
The decision to implement a CBDC must also be informed by a careful consideration of associated risks. Many different types of risks can emerge with the implementation of a CBDC system. These include individual risks like loss of privacy and difficulty of use; operational risks such as operational failure, data breaches, or novel cyber-attacks; and financial system risks like credit disintermediation, among others. A more extensive discussion of these potential risks is available across the CBDC literature.[7]

Central banks will also want to consider their overall appetite for adopting new technologies. For example, some countries[8] are exploring ways to encourage adoption of CBDCs and the development of features such as programmability in order to be on the cutting edge of payments infrastructure and innovation. Other countries may take a more conservative approach, minimizing potential risks to financial system stability by limiting CBDC use cases and utility to control adoption.

[7] See for example BIS (2020): Central banks and payments in the digital era, Annual Economic Report, Chapter III. Reports and consultation papers published by central banks also typically include a discussion on risks. For global examples, see Bank of Thailand (2021): The Way Forward for Retail Central Bank Digital Currency in Thailand; Central Bank of Nigeria (2021): Design Paper for the eNaira, and Group of Central Banks (2020): Central bank digital currencies: foundational principles and core features, Joint Report, no 1.

[8] See as an example recent press release from Banco Central do Brasil, the Brazilian central bank.

Figure 2. Potential role for CBDC



Source: Oliver Wyman Forum and AWS Analysis

2.2. Design principles

Once policy makers have a clear sense of what a CBDC would be designed to achieve, there are additional policy choices that will help guide solution choices. The policy choices presented here are not intended to be a comprehensive list, but rather those that a central bank should consider early to best inform technological design choices.

Defining the central bank role

A desire to have robust and clear control over the operation of the CBDC system may motivate a central bank to design and build the whole of the infrastructure and operate it themselves. However, managing a CBDC is a highly complex task requiring a wide array of sophisticated skills.

While some central banks may build on their experience in managing payment infrastructures like real-time gross settlement (RTGS) and fast payment systems, managing a CBDC system will also involve an increase in transaction volumes and a step-change in the proximity to the retail users of financial services. The latter will require building a new retail payment scheme. This set of rules and standards for the execution of payment transactions, will likely include rules around management of chargebacks, litigation, and guarantee issuance for merchants. Building such a scheme is critical to generate the necessary trust between payers and payees and to enable merchant payment use cases. Participating in building a new retail payment scheme requires capabilities and skills that have not typically been required by central banks. This is likely true regardless of whether the central bank is leading, coordinating, participating in, or supervising such a scheme.

Further, depending on the technology chosen for the CBDC platform, central banks may need to develop new forms of technical expertise, particularly given the consequences for economic activity, financial stability and public trust in case of any failure. These concerns could be partially addressed by outsourcing or partnering with technology providers to support the delivery of a CBDC solution. However, managing new third-party vendors and partners may still require increasing technical capacity.

An alternative approach for involving the private sector is to adopt a hybrid or federated model where distributors themselves participate in operating parts of the CBDC system. This could reduce the overall technical burden on the central bank as well as increase the potential for innovation as private solutions co-exist and compete. Simultaneously, as highlighted by the BIS,[9] relying on the private sector to build and manage the system will require a higher degree of supervision, as well as robust contingency planning in case of failure. There are also concerns that delegating responsibility for operating parts of the CBDC ledger and processing transactions could impair the core feature of the CBDC as a direct liability of the central bank and introduce counterparty risk.

Building a CBDC system that is aligned to the central bank's policy vision will require developing new capabilities beyond supervision and technology, such as the payment scheme described. Achieving a desired level of CBDC adoption requires understanding individual preferences and payment behaviors, as well as the incentives, rules, and business models that shape them. It is also worth noting that building a retail CBDC system is not a one-time endeavor. Its continued relevance will require significant effort including ongoing monitoring of market signals, scheme enforcement and updating, appropriate supervision and controls, and technical maintenance.

CBDC remuneration, limits, and features

Policy goals will be critical in defining how central banks choose to manage the extent of CBDC adoption. On the one hand, if central banks want to maximize adoption, they will aim to make their CBDCs as attractive as possible. This could include paying interest and minimizing constraints on CBDC holdings and usage, as well as integrating the new digital currency with other payment systems. This could also mean including features such as programmability that could promote its adoption by the private sector.

On the other hand, financial stability is a key concern.[10] Central banks may focus on minimized or targeted adoption if they are concerned that CBDCs will be too attractive as a substitute for bank deposits and other existing financial products and services. Those central banks may choose instead to impose quantity limits on holdings and take other actions to limit CBDC utility. In any case, managing financial stability concerns will require ongoing monitoring of not just CBDC systems but also deposits and private monies.

Central banks will also need to decide whether a CBDC should support the expansion of their existing monetary policy toolkits. Options to be considered include the ability to impose negative interest rates on CBDC deposits, restrict the type of goods or services that can be purchased with CBDCs, or distribute stimulus payments encoded with an expiration date. All desired features should be considered during the design of a CBDC system, even if they are not to be immediately implemented.

[9] See Auer et al (2021) Central bank digital currency: the quest for minimally invasive technology, BIS Working Paper No 948.
[10] See Group of Central Banks (2021): Central bank digital currencies: financial stability implications, BIS Other Publications, Report no. 4.

Defining the private sector role

A common theme throughout the CBDC literature is the need for public-private partnership in the creation of a successful CBDC system. In this paper, we assume that the private sector will play a critical role in the distribution of a CBDC to the public and provide a gateway for access to the CBDC system (given a two-tiered architecture). There are a variety of private sector entities that may consider participating as a distributor. These may include commercial banks, payment processors, fintechs, telcos, and large merchants. Regardless of distributor type, the central bank will maintain control of CBDC issuance (that is, be responsible for minting and issuing CBDCs and any remuneration).

We highlight three types of functions within a CBDC system. A central bank may choose to collaborate with the private sector to provide some of the activities within these functions.

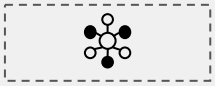
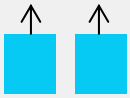
- **CBDC system management** is defined by how the core ledger and processing infrastructure is run. At a minimum the private sector, acting as CBDC distributors, could play a role in connecting individuals to the CBDC system by providing gateway access. However, if a more expansive role is desired, CBDC distributors may also operate parts of the CBDC infrastructure, by processing transactions (for example, validating that transactions are correct, posting transactions, and producing the necessary messaging) or by storing relevant data.
- **CBDC account management** is defined as the creation of end-user accounts and processing of corresponding transactions. At one end of the spectrum, policy makers may want end users to have a CBDC distributor (potentially through a third party) play an expansive role in delivery: managing access, authenticating identity, and possibly even processing granular-level transactions so the CBDC system only has to process distributor-level transactions. On the other hand, policy makers may want to minimize reliance on intermediaries and provide mechanisms for individuals to access the infrastructure more directly (for example, through a non-custodial wallet). Even in this case, the private sector could still play a critical role in authenticating identity and performing know-your-customer (KYC) checks as part of CBDC account creation for end users, if desired.
- **CBDC-based payment services** are all additional customer-facing services that include user interfaces (mobile app, web widget), value-added functionality, customer support, merchant services, payment gateways, and potentially other forms of programmability. These are not services that a central bank will likely consider delivering itself,[11] but are critical to a country's payment system. Distributors can play a large role in end-user services. However, non-distributors may also be active in the space by leveraging system access provided by a distributor. Policy makers should work to ensure that non-distributor access to the system has low barriers of entry. This can then incentivize actors in these areas to adapt their services to support the delivery of the CBDC and to encourage the evolution of a competitive and innovative market.

[11] Preferred approach across multiple geographies and types of countries, for example: Group of Central Banks (2021): "Central bank digital currencies: system design and interoperability", BIS Other Publications, Report no 2, and Hong Kong Monetary Authority (2021): e-HKD: A technical perspective, as well as Dcash and Sand Dollar live projects.

CBDC governance defines the processes by which decisions over the structure, capabilities, and technical features of a CBDC system are made. Policy makers will need to consider not only what role the private sector plays in the functions above but what role they play in how those functions evolve. We go into more detail on governance considerations in Box C: "Governance of a CBDC system" on page 28.

Central banks cannot assume the private sector will want to serve in the role of distributor as defined in this paper. They may seek an alternate role or to not have one at all. Thus, it is critical that the central bank provides clarity around expected investment costs, risks, and potential business models of this key role. The types of incentives that might be appealing are also likely to evolve over time, which requires considering viable business models at time of launch and at future points. Developing hypotheses and scenarios for how these business models may evolve over time can support continued engagement and participation of the private sector. We expand on potential competitive dynamics in Section 4.

Figure 3. CBDC roles

	Category	What
	**System management**	Running of core ledger and infrastructure Communication with core infrastructure and its enabling functions
	**Wallet and account management**	Processing services and managing accounts in the core system
	**Broader ecosystem**	Wider range of financial services, for example, merchant services, payments gateways, and programmable or individualized services
	**Governance**	Processes by which decisions over the structure, capabilities, and technical features of a CBDC systems are made

Source: Oliver Wyman Forum and AWS Analysis

Privacy approach

Privacy of financial transactions is critical for many individuals, with privacy protection consistently ranking in public surveys as one of the top priorities for payment systems.[12] However, privacy is a multifaceted concept, not a binary choice. Individuals typically are sensitive not just to what information is shared and collected, but also with whom it is shared and for what purpose. While privacy relates to the ability of individuals to control what, when, and with whom personal information is shared, anonymity relates to the ability to not have one's identity captured. Cash is anonymous as it doesn't require individuals to prove or even provide their identity to make use of it, and individuals in some jurisdiction may have strong preferences for maintaining that anonymity in digital payment systems.

[12] See for example, Official Monetary and Financial Institutions Forum (2021): Digital currencies: A question of trust.

Central banks will need to make decisions about user privacy in any CBDC system along numerous dimensions, starting with whether the identities of transaction participants remain anonymous. Different participants may be granted different levels of visibility into user information, such as CBDC distributors, payment services providers (PSPs), and central banks themselves. Governments will also need to establish the conditions under which public entities can access both data and metadata[13] from the CBDC system (for law enforcement or national security investigations, for example), and how such data may be shared with the private sector.

To achieve a desired approach to privacy, policy makers will rely on a mix of technology, such as cryptographic techniques that mask identity, and data governance policies, such as regulations that limit usage and access. Implementation through technology reduces the chances that the desired privacy approach is undermined by institutions violating regulations, or skirting them, or by a change in political direction. On the other hand, implementation through policy provides more flexibility to adapt to changing societal expectations and desires.

Individual protections, rights and services

A retail CBDC has the potential to impact individuals in many ways beyond privacy. Additional considerations may include how to ensure additional individual protections and rights. Which individual protections and rights are considered will vary across jurisdictions as will the approaches and philosophies used in securing them, whether that involves policy, law, the market, or a combination of mechanisms. We highlight some individual rights and protections that will have a greater influence on technology design: the ready access of data collected about individuals, and redress in case of mistakes (such as lost authentication), fraud, and systemic failures.

In regard to individual protections and rights around data, beyond privacy, some jurisdictions may also want to provide individuals with access to their own data as well as the ability to easily port their data and switch providers. Some policy makers may want to provide even further means of individual autonomy and provide individuals with the ability to interact directly with the CBDC system through distributor-managed software. Another important protection is ensuring individuals have access to their claim over the central bank should a distributor have an insolvency event or attack. Operational resilience will have to meet or exceed current payment system standards.

Policy makers may also be interested in leveraging the CBDC system to proactively expand or improve the efficiency of government services. For example, some policy makers might be interested in supporting automated tax collection and reporting or the digitized payout of government services. The need for a mechanism to address the latter issue was clear across many countries during the COVID-19 pandemic, as they struggled to quickly distribute stimulus payments.

Implementation of a CBDC has the potential to exacerbate risks to individuals, but also provide tools for better managing these risks. CBDC architectures can be designed to incorporate sophisticated anti-money laundering (AML) detection features and anti-fraud protections.

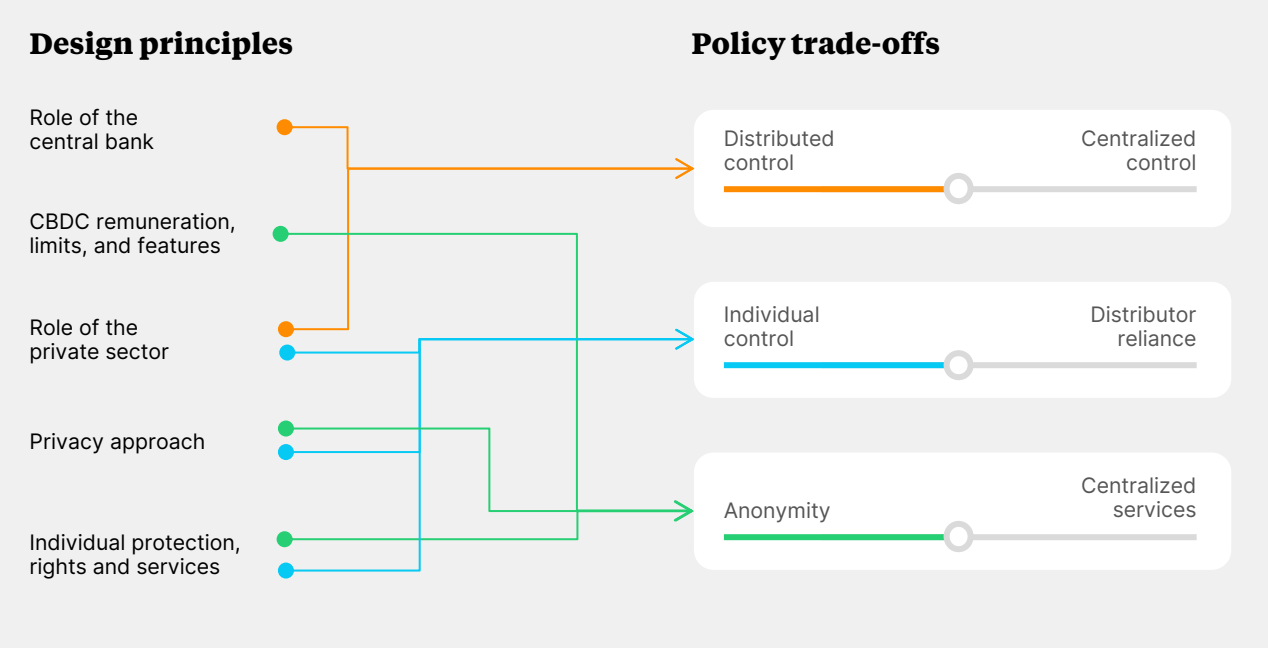
[13] Metadata is data about data. For example, a file's metadata could include author, file size, date created, data modified, etc.

Policy makers have different approaches they may take to secure individual rights and services. One option is to limit their remit over the CBDC system to the "payment rails" and leave individual rights to be secured through a combination of consumer standards and market competition, as firms compete to provide customer value. Alternatively, a second option is to have a more expansive role in ensuring value-added services. In this case, the central bank or some other government authority could build, or coordinate the creation of, a full payment scheme along with the CBDC payment rail.

2.3. Trade-offs

Many of the policy choices highlighted in the prior section are in tension with one another. This tension means one policy choice could lead down a path toward a technological solution that then precludes the fulfillment of other policy choices. In this section, we highlight three key areas to help policy makers prioritize their policy goals given the interdependence between goals and implementation options, which are described in Section 3.

Figure 4. Policy trade-offs



Source: Oliver Wyman Forum and AWS Analysis

Distributed vs. centralized control

Depending on central bank capacity and the desired level of public-private partnership, policy makers can design a CBDC system to have more or less centralized control over the core system. Policy makers will always have control over the regulatory environment; the question is about the extent to which there is distributed control over transaction processing and storage of core ledger data.

Control of the CBDC system may be reserved entirely for the central bank or decentralized to incorporate a large number of trusted private-sector entities. Fully centralizing control over the system limits the need to negotiate with a collection of governing entities, affording central banks more control over system design and potentially speeding decision-making. However, a completely centralized structure means the central bank bears all operational risks and could reduce opportunities for innovation.

Sharing the burden of operating and managing the system necessarily raises questions about how wide the circle of governing entities should be, given the potential to encourage the participation of non-traditional players or, conversely, to bolster existing financial service providers.

The desired role of the private sector will depend in part on the nature of existing institutions and their relative levels of maturity. For example, the central bank of a country with a less developed financial system may opt for more centralized control, while the central bank of a country with a diversity of firms ready and engaged in the payment system may opt for a more distributed model. We further expand on how policy makers may think about market dynamics in Section 4.

Individual control vs. distributor reliance

Policy makers may decide on a system where individuals bear more of the responsibility and risks related to CBDC delivery, or one where more responsibility is borne by distributors. This decision will be shaped by policy makers' approach to individual rights, privacy, and the role agreed upon with the private sector.

The approach to individual protections and rights needs to be carefully aligned with the role of the private sector. On the one hand, policy makers may envision individual protections being guaranteed through distributors. For example, the system could be designed to have distributors manage individual data and provide recourse in case of user errors, such as lost access to their CBDC wallet.

Alternatively, a society may conceive of individual rights and innovation as driven by providing more autonomy, choice, and responsibility to individuals. Consequently, distributor roles may be narrower, allowing more varied services to emerge in the broader market based on demand. This approach would favor providing individuals with more autonomy in managing their own accounts and the custody of their holdings, and more freedom to move between distributors. In some ways, this may be closer to a cash system, where individuals fully control the use and movement of their funds but are also responsible, with limited recourse, for any losses.

The approach to privacy may also impact policy maker’s ability to increase individual self-reliance. For example, if integration to a national or federated identity system is tolerated or desirable, that can open up more options around easing movement between distributors and PSPs, as well as designing in individual access and control of their personal data.

Anonymity vs. central, identity-based services

As noted earlier, privacy is a multifaceted concept, not a binary choice. Policy makers may have competing goals in providing anonymity to individuals, allowing the central bank or the private sector to provide identity-based services, and designing services to reduce illicit activities. From a solution perspective, these trade-offs will be reflected in choices about how identity is managed by the CBDC system.

On one end of the spectrum, policy makers may want to provide as much anonymity as possible, with identity information hard to access by the public or private sectors. On the other end of the spectrum, policy makers may want to facilitate the provision of identity-based centralized services, such as extending emergency aid. This trade-off depends on a country's broader approach to data protection and digital identity management. The existence of an independent national ID system outside of the perimeter of the central bank could allow for centralized identity-based systems without meaningfully changing a country's approach to privacy.

There is also a tension between providing anonymity and ensuring end-user protections. For example, if a CBDC system allows for a level of privacy protection similar to coins or paper money, then it may be very difficult to unwind theft, fraud, or other criminal activities without manual intervention. All else being equal, an ideal CBDC system would offer robust, automated protections to users in case of system failure or technical hack. At a system-wide level, this includes the ability to restore the entire CBDC ledger if it ever goes down. However, if a society desires the central bank to provide this back-up, then the central bank would need access to at least some individual level information.

Another key design principle impacting this trade-off is the approach to CBDC limits. Imposing restrictions on the amount of CBDC an individual may hold requires information sharing. As individuals may hold accounts across multiple institutions, there will need to be an entity, either the central bank or another party, that knows how much is in each individual's accounts across all their providers. If that information sharing is undesirable from a policy perspective, the policy approach could be to limit an individual to only a single CBDC wallet from a single provider. Or if lesser control is acceptable, limits on each account could mitigate the total amount of CBDC an individual could hold across accounts.

Section 3. Understanding design choices

3.1. System design configuration

3.2. Core ledger technology

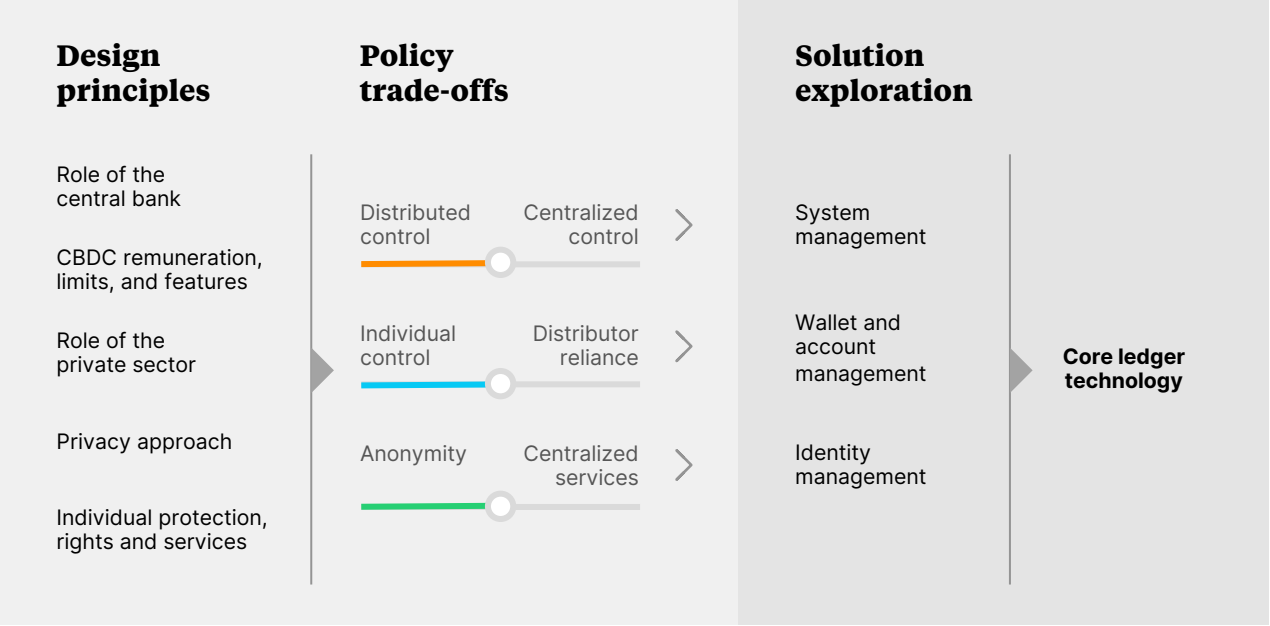
After identifying the underlying policy goals of CBDC exploration, technology solutions should be evaluated by how well suited they are to achieve these ends. We define technology solutions as a set of functional design choices that specify how the CBDC core system works and how it is accessed by participants in the space. Specifying these design choices is a key step toward launching technical experiments.

In this section, we discuss options for (1) configuring system design and (2) core ledger technology. These options are interconnected, but decisions about system design configuration should drive the choice of core ledger technology, rather than the other way around.

Key takeaways from this section:

- The solution decisions key to meeting policy drivers are generally not about ledger technology but rather primarily about system design.
- All technology choices don't have to be made immediately, but knowing which choices provide the flexibility to change later allows for a more adaptable system.
- Collaborating with distributors in operating a CBDC system is not a binary decision. There are a range of options available with different degrees of distributed control.
- There is a spectrum of options for how wallets and accounts can be managed, which will impact the level of reliance users have on a particular distributor.
- Identity management drives the degree of privacy from distributors and from the CBDC system itself, and whether central banks can provide centralized, identity-based services, controls, and protections for users.

Figure 5. Translating principles into design



Source: Oliver Wyman Forum and AWS Analysis

BOX B. CBDC technology stack

A technology stack is the set of hardware and software tools/frameworks leveraged to provide the complete set of functionalities needed for an application or system. There are many ways to represent the layers of a CBDC technology stack, which will inevitably differ across implementations.

Here, we generalize this stack into four layers, which serve to represent functionality that would exist in both DLT and conventional database architectures.

The **network layer** controls the mechanism through which participants[14] in the CBDC system will be discovered, validated, and have information propagated to them. A well-functioning network layer can be supported through high-speed network connections, such as a cloud network's internal backbone.[15] Redundancy in these connections also supports a resilient system across participants.

The **transaction layer** defines the CBDC data and transaction structure. This layer's design depends on choices made about how transactions are to be processed and approved. Basic transaction posting and advanced payments logic can be supported at this level to support multiple transaction types and validation structures. Event-driven architectures[16] can support scalable transaction processing and be designed to optimize the per transaction cost structure.

The **data layer** defines what and how much is stored of transaction data, current global state, and system event logging. This layer's design depends on choices made around data management, access, and storage. High availability datastores[17] with synchronous data replication will underpin data storage for both centralized and decentralized architectures. Additional data access controls will also support data privacy.

The final layer is the **application layer**, where end-user functionality and business logic can be implemented. This logic, whether built into or built on the core CBDC stack, can be implemented through cloud native or containerized solutions.[18] Additionally, the interface to distributor software can be supported through private links or a high-capacity API gateway.

The design configuration options presented in this section will impact functionality within each of these layers, with policy-guided system management design decisions impacting if/how participants operate in each layer.

[14] Here participants in the CBDC network are likely to be synonymous with distributors. However, from a technical architecture perspective, it is any secured endpoint that is approved to participate in the functioning of the CBDC system.

[15] Amazon CloudFront is a content delivery network (CDN) service built for high performance, security, and developer convenience..

[16] See this link for more on Amazon Event Driven Architecture.

[17] Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora. Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale. They are both serverless database options with automatic scaling and data replication.

[18] AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers.

3.1. System design configuration

Beyond architectural options, which determine the overall role of participants and transaction flows, and beyond core technology selections such as ledger type, a system's design configuration implements the desired logical interrelationship between a CBDC system's critical roles and functions. A system's design configuration will fundamentally shape how the CBDC system operates and thus its ability to support different policy objectives.

There are three key technology decisions that can be thought of as levers that move a CBDC solution across policy trade-offs identified in Section 2.3:

1. **System management** defines how the core ledger and processing infrastructure is run. This moves along a spectrum from highly distributed control of the CBDC system across a set of distributors to highly centralized control of the system by the central bank.
2. **Wallet and account management** defines how end-user accounts are created and how end users interact with their funds. This moves along a spectrum from high individual control of personal funds to high reliance on a distributor for control of those funds.
3. **Identity management** defines what information about individuals is collected and made available, and to whom**.** This relates to the level of privacy and moves along a spectrum from high individual privacy to high provision of centralized identity-based services

Placement of a CBDC solution at the high or low ends of any spectrum is descriptive rather than normative as intermediate options exist. The type of solution adopted should be guided, as noted previously, by a country's policy objectives.

3.1.1. System management

System management defines how the CBDC core ledger and processing infrastructure is scoped and maintained. The core ledger holds the immutable list of all CBDC issuance and transaction events. Central banks can play a central role in maintaining the core ledger and its associated supporting infrastructure.

A CBDC system is likely to be complex, with different players assuming different roles in the management of the system. Solution decisions must take into account which roles the central bank wishes to maintain, which to share, and which to delegate. Thus, the combination of choices for system management can move a design from one fully centralized within the control of the central bank to one with shared governance and the participation of multiple entities.

This core architecture will underpin a broader "CBDC ecosystem" as defined by the BIS and a group of central banks[19] to encompass processing infrastructure, processing services and payment services. The central bank must also decide how to exercise oversight over this broader CBDC ecosystem with business and technical rules.

[19] See page 2 of Group of Central Banks (2021): Central Bank Digital Currencies: System Design and Interoperability, BIS Other Publications: "A core ledger with supporting infrastructure and rules would underpin a broader ecosystem of processing infrastructure, processing providers and user services with business and technical rules."

Key decisions

We define CBDC distributors as firms that provide access points, or gateways, to the core ledger. Distributors ensure all transactions are correctly formatted prior to submission to the core ledger and track corresponding response messages received from the ledger. Distributors are thus responsible for operating any infrastructure needed by users as well as non-distributor payment service providers to communicate with the CBDC system.

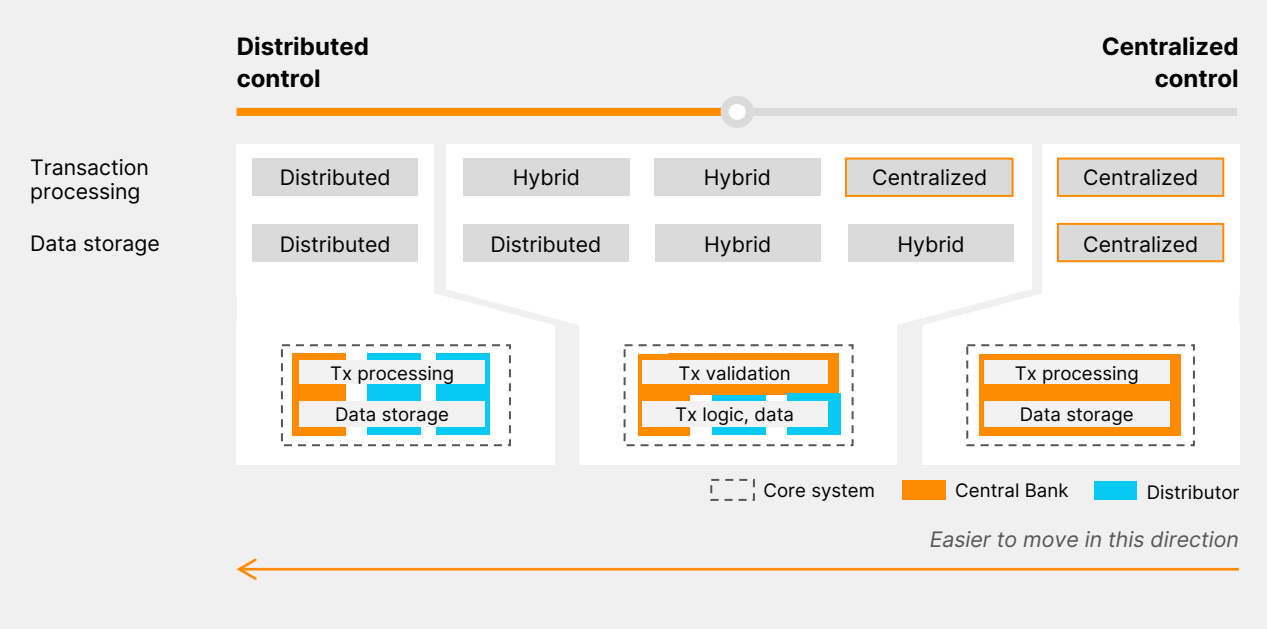
Additionally, central banks have two interrelated system management functions that they can choose to manage themselves, or delegate to distributors in full or part:

- **Transaction Processing**: A core function of the CBDC system will be the processing of transactions. This involves performing two steps: (1) validation and (2) transaction logic. Validation involves ensuring that the funds have not already been spent (a double-spend) and that they are not counterfeit (were not issued by the central bank). Transaction logic involves checking that signature(s) are valid and that sufficient funds are available, as well as executing any other advanced processing logic (for example, imposition of transaction limits) programmed into the system. In systems with unspent transaction outputs (UTXO) data structure,[20] these two functions can be performed separately by different parties.[21] With an account-based data structure, they are performed together.
- **Data Storage**: Determining where data is housed is a key consideration for a CBDC system. Central banks will need to set policies governing access to both transaction data and transaction metadata. Transaction data includes only the data needed to process a transaction (for example. sender ID, recipient ID, and amount), while metadata contains other information about a transaction, which may include counterparty information and additional text fields with transaction notes.

[20] See Box F "Tokens and accounts" for more on the distinction between UTXO and account-based data structures.

[21] In Federal Reserve Bank of Boston and Massachusetts Institute of Technology Digital Currency Initiative (2022) Project Hamilton Phase 1: A High Performance Payment Processing System Designed for Central Bank Digital Currencies, transaction processing is divided into three functions, which differs from the model here. However, those functions are performed by the same entity on differing functional components.

Figure 6. System management decision spectrum



Source: Oliver Wyman Forum and AWS Analysis

Decision spectrum

The decisions regarding processing and data storage are interrelated. At the two ends of the spectrum, is a fully distributed system management and fully centralized system management. Additionally, at least three variations between these two extremes exist and are also described in this section:

Distributed system management

- With **distributed transaction processing**, certain distributors are permitted to fully handle transaction verification and transaction processing logic. In this case the central bank may still have visibility into the overall state of the ledger, but it is not required to directly validate individual transactions. This offers individual CBDC users' greater privacy from the central bank, eases throughput requirements for any individual distributor, and provides shared responsibility for system uptime. However, even in fully distributed transaction processing, the central bank maintains exclusive authority to issue CBDC.

- With transaction processing distributed, it is likely that data storage will be distributed as well. **Distributed data storage** allows for each system participant to hold only the data relevant to transactions in which they are involved or to which they have been given explicit access. This provides the most privacy for individuals and could lead to more control of how data is shared with others. Unless configured to send a copy of all transactions, the central bank would have access only to data related to transactions for which the central bank is either a sender or a recipient of CBDC. Thus, they would either hold only a subset of the full CBDC ledger, because the data was not sent to them, or they would hold a complete encrypted ledger with visibility only into the transactions to which they were a participant.

Centralized System Management

- In **centralized transaction processing,** the central bank manages all validation checks and performs any advanced transaction logic that may be programmed into the core system. This minimizes reliance on third-party distributors for validation authority as well as reliance on private-sector managed transaction logic. However, it creates a potential bottleneck with all transactions being processed by central-bank controlled infrastructure and increases the technical burden on the central bank. It may also require providing technical support to participating distributors and/or end users. Depending on the configuration, it may also require the central bank to assume financial risks associated with fraud or transaction errors.
- With centralized transaction processing, data storage may also be centralized. With **centralized data storage**, all data for a transaction is processed by the CBDC system. This option provides greatest visibility into individual financial activities, though data may be encrypted in such a way as to limit access absent exceptional circumstances. Although metadata passes through the CBDC system, in order to address privacy concerns the transaction processing rules may dictate that no copies of metadata are retained after the completion of a transaction. Even with centralized data storage, distributors are likely to keep data related to their end users, however, that data is not maintained as part of the CBDC system.

System Management Variations

- In addition to centralized and distributed transaction processing, **hybrid transaction processing**[22] is also possible. In this case, the central bank performs only transaction validation. This typically includes validating the CBDC transaction inputs to ensure they are legitimate, ensuring no double spend or counterfeit funds. Distributors then handle all other processing of transaction logic. This allows for the central bank to have visibility into all transactions, but not necessarily into transaction participants. Splitting responsibility for each form of validation reduces technical and operational burdens on the central bank but increases the need for supervision of distributors who process transactions.
- With hybrid transaction processing, **hybrid data storage** is likely. In this case only necessary transaction data is received and stored by the CBDC system.[23] Other transaction data including metadata is likely to be communicated in peer-to-peer messaging and stored only by relevant parties,

[22] Hybrid transaction processing is most common with a UTXO data structure.

[23] Necessary data typically included sender, recipient, and amount for an account-based structure and input UTXOs for a UTXO-based structure.

such as distributors used by each participant and on individual wallets. The central bank retains a copy of the ledger that includes CBDC ownership details and transaction history.[24] Distributors hold transaction metadata only for the transactions they are a party to.[25] This option is most similar to existing mechanisms of transferring commercial bank money.

- **Centralized transaction processing** can also support **hybrid data storage** where only necessary transaction data is received and stored by the CBDC system. This assumes bilateral communication channels between distributors for the sending and receiving of additional transactions data. Thus, while the central bank maintains control of ensuring all transaction validation and common transaction logic, pre-processing and other data exchanges between distributors is also enabled.
- Finally, **hybrid transaction processing** can also support **distributed data storage** where both central banks and distributors hold transaction data necessary for transaction processing. Thus, while the central bank maintains control of validating all transactions, distributors can also validate transaction inputs that could support a future move to distributed transaction processing.[26]

Decisions about transaction processing and data storage necessarily entail centralization of control within central banks, or delegation of authority to other system participants. While not all combinations are feasible, the more centralized the option, the more technical capacity is needed by the central bank.[27] Conversely, the more decentralized the option, the more governance is needed to ensure alignment among all participants. A central bank's relative comfort with assuming technical versus supervisory responsibilities will weigh heavily in its choice of system design features.

Flexibility

If distributed control is desired either in the short or long term, a solution can be designed to ease movement from centralized system management to distributed system management. As new systems are developed, they typically start as smaller centralized proofs-of-concept. As these systems grow and additional participants join the network, shared responsibility may grow organically along with expanded system functionality.

Starting with distributed system management requires much pre-launch planning to ensure all participants are ready to perform their requisite roles. Moving from a distributed to a centralized system, requires the off-boarding of participants that may have invested significant time and acquired dedicated technology to support this system. Additionally, the now centralized system has to reevaluate its implementation to ensure it can support increased usage, while still meeting requirements of security, scalability, and resilience. For these reasons it is likely to be much more difficult to move from a decentralized to a centralized system.

[24] In a UTXO-model there is an additional possibility that the central bank has a transaction list but does not capture ownership of each UTXO.
[25] A complementary design choice not addressed here is determining whether the distributor also has access to the full CBDC core ledger.
[26] This may also support future offline transactions depending on system design.
[27] In situations where the central bank maintains control, but outsources full management of a CBDC system, it is likely that both more governance and technical capacity may be required, as we discuss in Section 2.2.

An approach, where the system moves along the spectrum from centralized to decentralized through time, can also allow for governance mechanisms to mature with the system. The addition of both number and type of participants can create a robust system if done thoughtfully. In the case that distributed governance is a desired end state, a slow and thoughtful increase of participants as part of a DLT-based solution should be highly considered.

BOX C. Governance of a CBDC system

Governance is a complex issue that could sustain a paper by itself. Central banks will need to consider organizational governance of participants in the CBDC system through mechanisms such as a governing charter, as well as technical governance of the CBDC system. Though governance mechanisms are required at the organizational level, technical governance mechanisms can optionally be coded into a CBDC system.

At an organizational level, governance could include topics such as processes for addressing technical issues, communication or messaging standards, methods of proposing the addition of new functionality, development of redress processes, and more. This level of governance is critical, regardless of which technical solution design is chosen, and is accordingly beyond the scope of this paper.

At a technical level, governance can be incorporated into a DLT-based CBDC system's protocol in two ways. The first is a consensus mechanism regulating how the system validates and stores an accepted transaction (typically a block of transactions) to the ledger. High-energy consensus mechanisms are a common issue with some public blockchains. However, there are many energy-efficient consensus mechanisms that could be leveraged in a permissioned DLT system.

The second technical governance mechanism regulates acceptance of new participants to operate part of the CBDC system infrastructure. These decisions can be made exclusively by a central bank, or in a decentralized model, these may be shared decisions requiring approval from a set number of system participants.

Fully centralized governance of a CBDC system enables the central bank to fully control the operation of the system, potentially speeding decision-making and ensuring that the key policy objectives are enabled. However, a shared governance model may have advantages in encouraging innovation and ensuring that the interests of the private sector are represented.

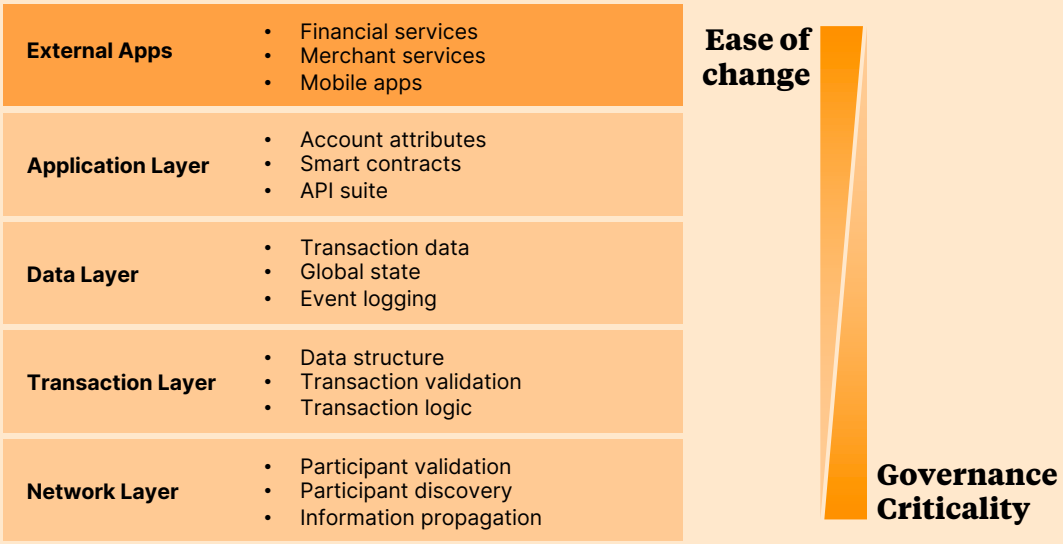
Any decentralized governance system necessarily raises questions about how wide the circle of governing entities should be, given the potential to entrench existing financial incumbents or create new privileged competitors. It can also be an opportunity to broaden access to new entity types like telecom operators or fintech providers. Decisions like these are inherently political and require thoughtful consideration to ensure alignment with CBDC policy goals.

BOX D. Programmability

Programmability is often discussed in the context of CBDCs, and programmability is also often equated to smart contracts that run on distributed ledger technology (DLT) networks. However, programmable business logic that could be adapted to support CBDCs has existed in some form for many years, and is not exclusive to DLT networks. The novel type of programmability brought by DLT is embedding business logic into the payment instrument such that users are guaranteed consistent outcomes regardless of which distributor they use.

Programmability can exist at different layers of a technology stack, as seen in Figure 7.

Figure 7. Implementing programmability across the technology stack



Source: Oliver Wyman Forum and AWS Analysis, adapted from Ethereum technical stack in Chen et al (2019)

Programmability at the **network layer** can provide central banks with controls for network participants. For example, governance can be programmed to be limited to a subset of participants, which could uniquely perform functions like adding a new participant. Or each participant can be given a different weight in approving updates to network protocols. Change management at this layer is critical as any modification can have a high impact on the system and its participants. Regardless, decisions at this layer are difficult to change unless the ability to expand functionality in the future is built in.

Programmability at the **transaction layer** could support transaction validation or advanced transaction logic. For example, existence of a consensus mechanism to support distributed transaction processing would be set at the transaction layer. Programmability here could also implement transaction logic, such as setting limits to transaction amounts or recipient balances, which could be relevant, for example, in building thresholds for users who did not provide KYC information. Changes at this layer can also be difficult to implement, although flexibility to adjust parameters can be designed into the system.

Programmability at the **data layer** can be used to impact the location and type of data stored across participants. For example, data can be segmented with only authorized participants allowed to read and/or write to a particular section of the ledger. This provides the ability to create read-only participants and segment data access, which could support privacy. Similar to the

network layer, structure at this layer is highly dependent on defined participant types. Though changes at this layer are easier to make, governance is critical as data privacy can be highly impacted.

The final layer is the **application layer**. Programmability can be enabled here in two ways. First, custom application logic can be implemented within the CBDC system itself through smart contracts, for example. Performing that logic within the CBDC system stack will leverage network resources. Thus, any implementation of this type of programmability should be tightly governed to ensure system performance is optimized. Additionally, in this approach security audits are highly recommended since smart contract code is stored and run by all network participants and directly sets network functionality. Second, custom application logic can be enabled within the CBDC system but created through an open system for third-party innovation. Creating a suite of open APIs accessible to external parties within this layer can support a vibrant market of third-party applications and enable payment service providers to provide programmable money functionality as overlay services outside of the CBDC system. For example, programmable application logic can be used to create a delivery-versus-payment (DvP) system for integration with government securities.

Governance bodies should include input from a wide array of organizations to ensure services are being developed that address the wide spectrum of needs across a country's population, as well as to ensure interoperability with other related systems. And while the application layer is the top layer of the CBDC system, external applications are likely to be the primary source of programmable functionality. Governance here is likely to be seen more in the form of regulating the organizations and services developed.

3.1.2. Wallet and account management

We define wallet as the mechanism through which an individual or distributor interacts with their funds, while account refers to an individual or distributor's holding of CBDC. Thus, the combination of wallet and account types can move a design from one where an individual has complete control of funds to one where they rely on a distributor to control funds on their behalf.

Key decisions

Wallet and account types can be determined by leveraging three separate design decisions, based on the responsibilities of distributors in the delivery of CBDCs.

Who bears responsibility for the custody of funds?

- **Custodial:** A custodial wallet is one in which a third party holds all information necessary to sign and submit a transaction on behalf of the user, thus assuming custody over these assets on behalf of the user. In a token-based access system, this typically means that the custodian is holding the private keys[28] needed to sign a valid transaction. In an identity-based access system, this typically means that the custodian maintains the link between identity and CBDC account required for authentication to request movement of funds.
- **Non-custodial:** A non-custodial wallet is one where an individual holds all information necessary to sign and submit a transaction on their own. In a token-based access system, this means that the user manages their own private keys. In an identity-based access system, non-custodial implies the user is able to prove their ownership of CBDC independently of any specific distributor, such as through a national ID system.

Will transactions be processed at the distributor level or both the individual and distributor level?

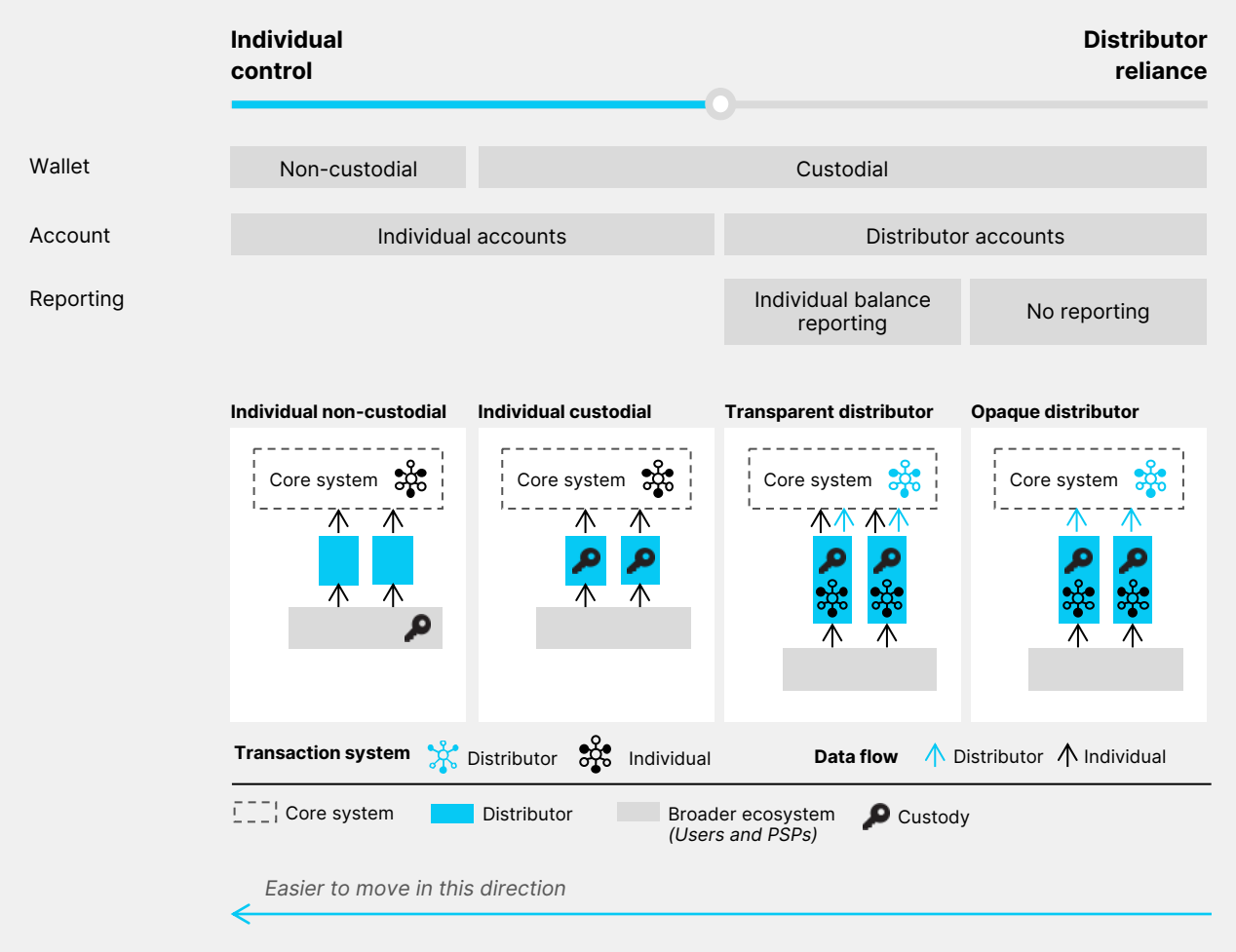
- **Individual accounts:** Every user has their CBDC holdings recorded directly on the core CBDC ledger. Transactions directly update balance or UTXO ownership within the core ledger.
- **Distributor accounts:** Individual users access the CBDC system exclusively through a selected distributor, with the core CBDC ledger recording only the total CBDC holdings of each distributor. Transactions at the individual level are processed by distributors, either locally within a distributor system or as part of a dedicated retail system. Distributors maintain records of an individual's CBDC holdings, which remain a liability of the central bank.

[28] Public-private key pairs are a sophisticated form of cryptography that identifies a digital wallet and allows the owner to access their digital currency.

Will the system hold individual balance information?

- **Reporting:** Use of distributor-level accounts creates the risk of individual balances being lost in case of distributor failure. To mitigate this risk, individual balances can be maintained by a single distributor but reported to the CBDC system at regular intervals, even if individual accounts and transactions are not directly managed by the system.

Figure 8. Account and wallet management decision spectrum



Source: Oliver Wyman Forum and AWS Analysis

Decision spectrum

The combination of these three decisions creates a spectrum of intermediation at the distributor level, along which lie four options:

- **Individual-level account with non-custodial wallet:** This account and wallet type combination gives full control of funds to individuals. In an identity-based access model,[29] an individual would be able to control their funds by simply proving their identity. In a token-based access system, individuals are able to have exclusive control of their private keys. Both allow an individual to transact without dependence on any specific distributor, and ownership of their CBDC is recorded directly on the CBDC ledger. Given a two-tier architecture, distributors would still play a role in onboarding of new users, KYC checks, and wallet creation, as well as acquisition or redemption of CBDC for cash or commercial bank money. While individual control is increased, individual risk is also increased, particularly for a token-based access model. Loss of the private key or a storage device like a cell phone could result in irrecoverable loss of funds.
- **Individual-level account with custodial wallet:** This account and wallet type combination requires a distributor, serving as a custodian, to sign and submit all transactions on behalf of the individual. In a token-based access model, the distributor would custody the private keys associated with each individual's CBDC; in an identity-based access model, the distributor would be responsible for authenticating that individual's identity. Reliance on a particular distributor is increased but recording of individual CBDC balances on the CBDC ledger may allow for easier movement between distributors and provide protection in case of distributor failure.
- **Distributor-level account with reporting:** Accounts at the distributor level afford an additional level of privacy from the central bank to individual users holding custodial wallets. Transactions at the individual level are not recorded on the CBDC ledger, and the central bank is only aware of distributor level balances and transactions. However, with reporting, the risk of a user losing the information necessary to secure claim of their CBDC holdings is reduced. In cases of distributor error or malfeasance, ownership of CBDC claims is still maintained by the central banks as they are reported by distributors on a regular basis.
- **Distributor-level account without reporting:** This approach is akin to wholesale CBDC. Distributors intermediate all individual functionality and are responsible for providing all individual-level services. However, in this case there may be limited means for users to gain protection if their distributors fail. This system is akin to the contemporary commercial money system, where only deposit insurance is provided in case of distributor failure. This approach may also require regulatory interventions such as open banking requirements to enable users to freely move between distributors.

Flexibility

More than one option along this spectrum could be included in a single CBDC solution. For example, the core ledger may allow for both individual-level accounts and distributor-level accounts, enabling a combination of transaction processing approaches. CBDC solutions could also accommodate a mixture of both custodial and non-custodial wallet options to serve the differing needs across user segments.

[29] See Box F: "Tokens and accounts" for how identity-based access models differ from alternatives.

3.1.3. Identity management

Identity management will be integral to implementing a central bank's desired privacy approach, as well as determining how data flows across actors and the resulting business incentives. The choice of identity management solution accordingly shapes whether CBDC systems optimize for high levels of individual privacy or for easier expansion of public services.

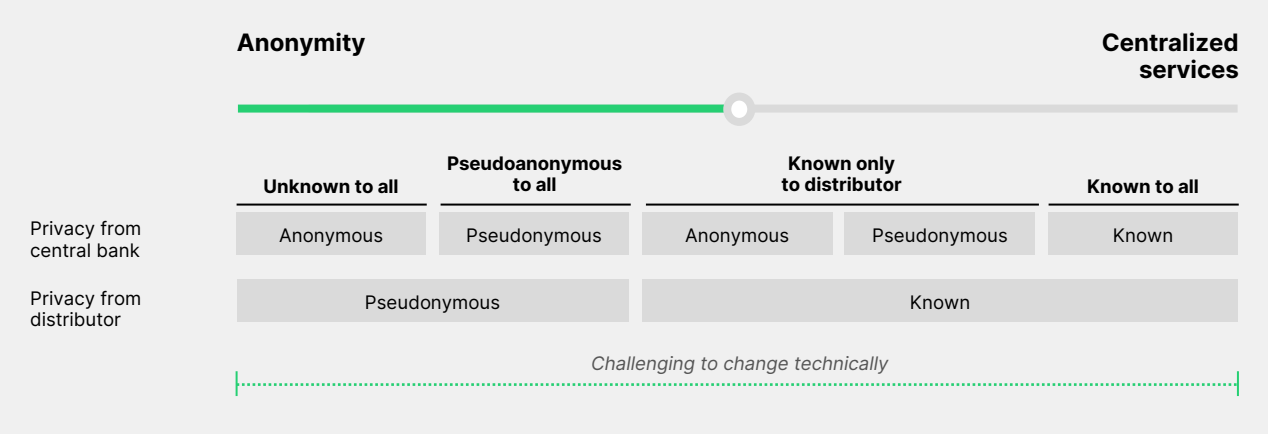
Key decisions

The relationship of individual identities to a CBDC system can be separated into three broad categories:

- **Anonymous:** The individual is not known to the central bank, distributors, or any counterparties, and it would be extremely difficult for true identities to be determined solely from data accessible to the system.[30]
- **Pseudonymous:** The individual's true identity is not directly recorded in the system, but an identifier unique to each individual is linked to each of their transactions. Though true identities are not immediately available, account activity can be monitored by authorized parties and identities may be determined if needed, for example as part of a law enforcement investigation.
- **Knowable:** The individual's identity is known to the central bank and/or distributor, and is linked to any accounts they own or transactions they perform.

With these three broad categories, individual privacy can be assessed in relation to the central bank (taken here to include a centralized CBDC system), and to the distributor(s) involved in processing a transaction.

Figure 9. Identity management decision spectrum



Source: Oliver Wyman Forum and AWS Analysis

[30] One implementation option is dynamic public keys as described in the e-HKD paper

Decision spectrum

As with each key design decision, privacy trade-offs are rarely binary "this-or-that" decisions but more akin to "more-of-this, less-of-that." Here, the salient decision spectrum ranges from greater ability to maintain anonymity to greater ability to provide centralized, identity-based services. Individuals are likely to vary significantly in their willingness to give up some level of privacy to gain access to such services.

There are different levels of user privacy possible within a CBDC system. At one end of the spectrum, the highest level of privacy is one with only a system identifier assigned by a distributor. This identifier is not tied to the individual's identity and the identifier is obscured from its transactions, providing complete anonymity. While this is a possible configuration, it is unlikely to be a preferred option due to KYC considerations and ensuring anonymity is much more technically complex than pseudonymity.

The three likely options are:

Identity is pseudonymous to all.

- In the two options below, identity is assumed to be captured by a distributor. However, in certain cases identity may not be required and no user identity recorded. This is likely to be most common in countries where lack of identity documents is widespread and already contributing to financial exclusion, or where governments wish to permit individuals to maintain anonymity for low-value transactions.
- Where there is a need to allow ownership of CBDC without identification, pseudonymity is likely to be a favored option. Distributors would be able to create CBDC accounts without requiring identification. To minimize fraud and criminality, these accounts are likely to have limits on the amount of CBDC that can be held and the value of the transactions a user can perform. With identity unknown to the distributor, it would also be unknown to the central system.[31] This structure allows for those either lacking identification or seeking additional privacy to still participate in the CBDC system. If an individual wants to unlock additional services that require identity verification, identification can always be provided at a later time. This allows for individuals to have more control over the context in which they are willing to share their information and for what it will be exchanged.
- Drawbacks of this structure generally involve concerns about illegal activity perpetrated through the use of multiple wallets. Money laundering and other financial crimes may be easier to conceal if funds are circulated through many pseudonymous wallets, while investigations into fraud and other financial crimes are hindered by the difficulty of tracing beneficial ownership of illicit gains. The ability to hold multiple wallets without detection also makes it difficult to impose limits on CBDC holdings by any one individual.

[31] The desire for some type of common identifier within the CBDC system would prevent adoption of a fully anonymous system, leaving pseudoanonymity as the most private potential option given this constraint.

Identity is known to an individual's distributor but not the CBDC system.

- This option most closely mimics existing commercial money systems. Distributors perform all KYC procedures, thus capturing and holding the identity of their customers. With pseudonymity from the central bank, a CBDC system identifier is used to process transactions, but this identifier is not directly tied to an individual's identity within the system. However, should an investigation be required, the distributor could provide information regarding the owner of those funds. Privacy from a central authority is maintained, while law enforcement is still able to request identifying information from a distributor in case of individualized suspicion.
- In the case where true anonymity from the central bank is desired, technology exists to rotate identifiers or employ multiple identifiers for a single account. This can minimize the ability to monitor an individual's transactions over time. However, again with identity known to the distributor, information can be provided when criminal activity is suspected. Both structures are nevertheless limited in their ability to facilitate direct government assistance to individuals or enforce limits on CBDC ownership across multiple accounts. Administration of public benefits through the CBDC system would continue to require information on an individual's chosen financial services provider, which must be explicitly shared with the state and may limit advantages of pseudonymity.

Identity is known to both the central bank and an individual's distributor.

- A typical option considered would employ a national identity system in conjunction with the CBDC system, where the national ID is harnessed as the CBDC system identifier.[32] A user's national ID is contained in all transactions, making it trivial for the central bank to tie transactions back to a particular individual.
- The benefits of known identity are many. First, it expands options for the provision of public services. Stimulus payments can be credited to recipients without concern for duplication, welfare benefits can be distributed directly to qualifying individuals, and tax refunds can be processed straight to account holders. Additionally, access to identity information supports central coordination of anti-money laundering and fraud detection activities. Tying identity to CBDC ownership also supports the enforcement of CBDC limits, as aggregate balances of a single user can be calculated across multiple accounts. Finally, should illegal activity be discovered, the owner of tainted funds can quickly be identified by law enforcement.
- Drawbacks of known-identity systems have already been voiced by privacy advocates. Tying identities to financial activity would provide access to private financial data to anyone permitted to access transaction data – particularly if CBDCs largely replace the use of physical cash. If shared with or sold to third parties, identifiable transaction data could also be exploited for targeted marketing campaigns or lead to greater discrimination in the products offered to the less wealthy.

[32] It is likely that the national ID would be linked to a system ID. Instead of the national ID being embedded in transactions, the corresponding system ID would be used, and that system ID would be made available to both distributor and the CBDC system.

Flexibility

Central banks could potentially incorporate multiple privacy options, such as anonymous or pseudonymous transactions that are limited to carrying low balances in conjunction with identity compliant wallets that can hold higher balances. However, while additional options can be added over time to move along the privacy spectrum, it is generally difficult to change the privacy level of existing wallets.

Finally, and in addition to technological design, privacy options can be set through other mechanisms such as regulatory constraints. These policy choices are easier to change than technological design choices, allowing the system to evolve over time. However, robust oversight mechanisms are required to ensure compliance with regulatory strictures.[33]

BOX E. Know your customer (KYC) and financial crime prevention

The implications of different CBDC privacy configurations vary across the different types of financial crime from anti-money laundering (AML) to financial fraud to terrorism financing.

It is assumed that distributors will capture user identity through KYC checks when a CBDC account is created, though certain low-value accounts may be permitted without KYC. Thus, for most accounts, ownership can be ascertained from the distributor when legally permitted. To prevent fraud, other measures can be taken, such as continual authentication throughout a CBDC transaction flow. Step-up authentication[34] can also be performed optionally given the risk-level of the transaction. For these measures, there is no necessity to make identity information available to the central bank.

Constraining central collation of identity information poses a greater challenge to AML and countering the financing of terrorism (CFT) protections. Detection of these crimes may be greatly assisted by the availability of identity information to the CBDC system. Nevertheless, the capture of transaction data with pseudonymous identities in a single system alone is likely to increase the ability to identify patterns of activity across multiple distributors by eliminating the need to reconcile information across financial institutions. With recent advances in the use of artificial intelligence and machine learning (AI/ML) to create and share suspicious activity alerts, central collection of identity information can be minimized in support of AML and CFT.

[33] See Auer et al (2021) Central bank digital currency: the quest for minimally invasive technology, BIS Working Paper No 948.

[34] Step-up authentication means requiring additional authentication measures depending on presumed risk. This approach can balance security and user interface complexity, as it ensures users can access some functionality with basic credentials (for example, user name and password), but will prompt them for additional authentication (for example, one-time code or biometrics) when they want to perform a higher risk activity.

3.2. Core ledger technology

Many CBDC technology solutions are being investigated and piloted across the globe, with multiple live large-scale pilots.[35] However, the conversation is often simplified to whether distributed ledger technology or conventional databases are best suited for meeting technical requirements. This ignores the need for the ledger technology selected to support the system design configurations chosen to meet policy goals.

The choice of ledger technology is important, but that choice should follow rather than drive decisions around system design. While DLT-based solutions are available, there are also a range of alternative technologies for storing and processing a CBDC. Conventional databases and cryptographically verifiable ledgers[36] are also capable of supporting CBDC systems. Solutions also exist that are a mix of the two approaches.[37] In general, several options may be suitable given a particular set of policy objectives.

One of the most important system design choices previously described is whether system management should be centralized or distributed. While a deep dive into the pros and cons of these core ledger technologies and how they support system management design choices is beyond the scope of this paper, there are specific circumstances that might lead central banks to prefer one over another.

For example, if a country is seeking to distribute governance of its CBDC system to include private sector participants, a DLT architecture may be most appropriate. Features of DLT solutions include immutable data storage and increased transparency into system usage, greater programmability options, and platform-native support of tokenized assets. However, the distributed nature of DLT systems simultaneously adds complexity in managing additional participants in the network, requires increased technical sophistication of those operating the system, and potentially introduces new threat vectors that may reduce system security. In addition, there remain concerns that DLT technologies have yet to demonstrate the throughput required by a CBDC system. However recent scalability and performance tests are now demonstrating high throughput with distributed ledger systems.[38]

For countries seeking a centralized governance model or that prefer technology proven to meet the needs of large-scale payment systems, conventional database systems may be most appropriate. Benefits attributed to DLT architectures, such as cryptographically verifiable append-only ledgers and high levels of programmability throughout the tech stack, can often be achieved with centralized solutions. However, the centralized nature of the system may cause concern regarding control of end-user and transaction data.

[35] As of January 2022, these include the central banks of the Bahamas, China, the Eastern Caribbean Currency Union, and Nigeria.
[36] Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log."
[37] See for example the opensource architecture recently published in Federal Reserve Bank of Boston and Massachusetts Institute of Technology Digital Currency Initiative (2022): Project Hamilton Phase 1: A High Performance Payment Processing System Designed for Central Bank Digital Currencies.
[38] See SETL (2021): The Regulated Liability Network: Whitepaper on Scalability and Performance.

An additional technical dimension to consider is adoption of a UTXO-based or account-based data structure (see Box below). While UTXO-based structures are typically associated with DLT solutions and account-based structures with conventional databases, these relationships are not exclusive. In fact, Ethereum[39] is an account-based system, while most DLT solutions leverage a database in the backend. And while account-based systems are aligned with the structure of today's financial systems, central banks may be attracted to unique properties of UTXO-based systems, such as the ability to separate transaction validation from counterparty information. Both data structures can be adapted to support the functionality required to meet the potential policy objectives discussed in this paper.

BOX F. Tokens and accounts

A **UTXO-based system** uses UTXOs (unspent transaction outputs) to represent specific amounts of CBDC. To conduct a transaction, one or more UTXOs are selected as inputs, validated as unspent, and then marked as spent to never be used again. The outputs of a transaction are new UTXOs, whose values are derived from the transaction itself, and which can carry the history of the UTXOs that were used to create them. UTXO-based systems are often referred to as token-based.

By contrast, with an **account-based data structure**, transactions directly reduce the balance of the sender's account and increase the balance of the recipient's account by the value transferred. While the amount sent has a particular unit (for example, $1), these units do not exist independently or uniquely from each other or the account in which they are held.

In earlier CBDC literature, the term "account-based" was used to reference solutions where a user must prove their identity to transact using CBDCs – an "I am, therefore I own" model.[40] To avoid this potential double-meaning of the term "account-based," we use the additional term **"identity-based" access** to reference this "I am, therefore I own" structure.

The term "token-based" is used in other ways, not just to refer to UTXO-based systems. This term has been used to reference a CBDC system where a user need only provide a digital token to transact with their CBDC – an "I know, therefore I own" model. Here, we keep the term **"token-based" access** to reference this "I know, therefore I own" structure. Some refer to this type of access as a **bearer model**.

It should be noted that within the DLT space, a token is no more than the digital representation of an asset. Tokens are not unique to UTXO-based systems (like Bitcoin) but can be used to describe assets in account-based systems (like Ethereum). The term could therefore also apply to a CBDC hosted by a centralized system and any other central bank asset with a digital representation.

[39] Ethereum is the second largest blockchain project. It is a single, decentralized system that runs a computer called the Ethereum Virtual Machine. Each node holds a copy of that computer and all interactions are verified, with all ledger copies updated.

[40] Although the BIS has since updated its terminology from Auer, R and R Boehme (2021): Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers, no 948, the "I am" versus "I know" is still of relevance.

BOX G. Offline systems

A commonly stated requirement for future CBDC systems is the ability to perform offline transactions. The reasons for this are many, including to ensure access to funds in case of natural disaster and in areas of poor electrical or internet connectivity, which are critical to financial inclusion goals, and to ensure resiliency in the case of lost network connectivity.

While the technical details of potential solutions are out of the scope of this paper, central banks will need to bear in mind a set of high-level considerations regarding the system design and challenges of offline transactions.

A primary concern is security. Online transactions are validated in real time to ensure funds are not spent more than once and that the funds themselves were in fact issued by the central bank. In an offline setting, validation is dependent on the hardware and software of the devices[41] used to complete the transaction – whether these are smartphones,[42] dedicated electronic devices, or smartcards. A highly secure design to mitigate compromise of these devices is paramount.

Thus, while competition between service providers can be facilitated through defined standards and protocols for distributors issuing and managing offline devices, strong security requirements must be enforced for these service providers. Distributors seeking to offer offline services may be accountable for ensuring device security in accordance with defined standards, enforcing any limits and other controls, and safely managing movement of funds and associated data between the online and offline system.

Harmonization of online and offline systems must balance the competing policy drivers of privacy and ability to trace offline transactions. If a more cash-like system is desired for financial inclusion or privacy objectives, anonymous offline transactions may be permitted subject to limits such as total transaction size. However, if full insight into offline transactions is desired, the ability to store and trace transaction history is also possible.

Given the fundamental differences between online and offline transactions, they can in some ways be treated as parallel systems. Offline capability may accordingly be added to a CBDC system after implementation of online operations. However, both systems must be designed to ensure the security of the other, with robust integration and reconciliation points.

[41] Beyond security, devices have additional limitations such as storage limits, cultural acceptance, or access by end users.

[42] See for example research by Visa, Christodorescu et al (2020): Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies, and Huawei's Mate 40 Phone designed to support China's pilot CBDC, the e-CNY.

Section 4. Understanding competitive dynamics

4.1. Consider factors influencing competitive dynamics

4.2. Assess how system design shapes competitive dynamics

4.3. Next steps in evaluating competitive dynamics

Many central banks are designing a CBDC system with the assumption that the private sector plays a significant role. Certain decisions on technology solutions impact available roles for the private sector in the management, operation, and delivery of CBDCs. As policy makers are evaluating these options, they should also understand the competitive dynamics created by these roles and how they may impact private sector incentives.

An understanding of potential impact on competitive dynamics should be included while deciding what solution designs to experiment with and whether to launch a CBDC in the first place. Early in the design process, policy makers will want to develop hypotheses on this impact through scenario analysis, deep engagement with the private sector, and economic modeling. Throughout development and deployment phases, policy makers will want to monitor how these dynamics play out, as well as continue to keep a watch as solutions are developed. These dynamics may cause a revisiting of what solution design is best suited.

In Section 4.1, we describe a number of factors that shape competitive dynamics. In Section 4.2, we discuss how these factors may play out differently across the solution design choices described in Section 3, in ways that could support or hinder a central bank's policy objectives. Finally, in Section 4.3, we make recommendations on what policy makers should do to deepen their understanding of competitive dynamics as they continue to build and develop their CBDC programs.

Key take-aways from this section:

- Understand that a CBDC system may be prone to network effects, so it's important to hypothesize where those are likely to emerge and how they may impact competition and innovation in the private sector.
- Barriers to participate as a distributor can arise from design decisions that require operating parts of the CBDC system itself. Design decisions can also hinder new entrants by increasing the difficulty for end users and PSPs to change distributors.
- Maintaining a modern CBDC system requires responding to market signals and having the ability to adapt. Governance mechanisms and system participation can support this process.
- Solution design can encourage innovation at various levels – either by empowering distributors or by creating the conditions for new services to emerge through open competition.
- Privileged access to data could limit competition. The right balance between privacy and the ability to provide individualized services and user protections is needed.
- While distributors are highlighted in this paper, PSPs also serve as intermediators between the core CBDC system and individuals. New tiers may emerge, which could impact the ability to achieve policy goals.

4.1. Factors influencing competitive dynamics

CBDC policy and system design choices will impact competitive dynamics in the financial system either directly, such as by authorizing what types of institutions can and cannot connect to the core system, or indirectly, by providing certain players with an informational edge that becomes a barrier to entry, for example. Direct and indirect effects are important considerations for policy makers when assessing if and how these dynamics will help promote overall policy objectives.

Competitive dynamics are inherently multifaceted and highly dependent on local context. What works to foster private sector collaboration in one country may cause concerns around increasing barriers to entry in another. Market dynamics may also evolve in unpredictable ways, and the same holds true within the CBDC space. Policy analysis and decisions can take months or even years, given the need for caution and stakeholder engagement. However, a digital context allows for rapid scaling and adoption, making this a more complex and pressing topic for policy makers to watch.

While predicting outcomes can be difficult, it is still critical for policy makers to be thoughtful about the questions they are asking, hypothesize answers early in the design process with substantial stakeholder input, and then continually learn and adapt over time. We highlight three factors here that have the potential to have both direct and indirect effects on competitive dynamics:

- Who can become a distributor? How can sound competition be enabled between them?
- How can innovation be fostered through incentives and system mechanisms?
- How can data access be managed in line with policy goals, for example, to both respect the privacy of citizens and simultaneously favor open innovation?

Barriers to entry: Who can become a distributor?

Distributors, as defined in this paper, play a special role in a CBDC system by providing the connection between the core system and the broader set of system participants. In some CBDC solutions distributors may also have a role in operating part of the CBDC system itself. We highlight three areas where policy decisions impact barriers to entry: distributor requirements, competition with non-distributors, and portability across distributors.

Distributor requirements can pose barriers to entry because they demand resources or expertise. The need for would-be distributors to invest in technology and meet regulatory requirements around operational resiliency, data protection, and cybersecurity make these barriers potentially hard to reverse. This is especially the case if investments in infrastructure were high.

Given the connectivity to the core CBDC system, central banks will naturally want to be mindful of who can be a distributor. Policy makers can shape this by defining licensing and regulatory requirements, as often occurs today. Some policy makers may leverage this option to preserve a special role for financial institutions. Requirements can also be adjusted over time if there is a desire to expand the role to include non-traditional players.

If these and any other barriers to entry to become a distributor are too high, then this may limit competition. Policy makers will therefore want to keep a close watch on emerging business models and what types of firms can sustainably perform the distributor role. In some current payment systems for example, it is hard to remain compliant with network rules unless you are an owner bank with greater influence on the implementation of new network requirements and timing.

Next, dynamics between distributors and non-distributors are also important as distributors control access to the CBDC system. Policy makers may aim to keep barriers low for non-distributors to access the system in order to encourage innovation, inclusive finance, and integration with other payment systems. The distributor's role will help shape this dynamic, but the impact may be complex, requiring ongoing monitoring and policy adjustments.

Understanding how non-distributor PSPs will fit is important as they too will impact future competitive dynamics. Central banks interested in creating a level playing field between PSPs and distributors should take into account any inherent privileges that distributors have, especially if they have a role in governing or operating parts of the CBDC solution. Without understanding potential roles for non-distributors, unintended specialization may occur and drive the creation of additional layers of intermediation. Layers that exist outside the scope of policy makers can provide an opportunity for closed systems to develop, which may undermine policy objectives.

Finally, barriers to entry are also shaped by policy decisions made in the trade-off between individual self-reliance and distributor reliance, as described in Sections 2.3 and 3.2. A CBDC solution designed for greater individual control may make it easier for users to move between distributors. Ease of movement increases the chance that a new entrant, either distributor or non-distributor, will more easily grow their own share of the market through providing innovative and competitive services.

Continual innovation: How to put the incentives and mechanisms in place to foster innovation?

While central banks may desire tight control of the core system, innovation is expected to come from in the broader market. Many policy makers not only expect this but have it as a policy objective. However, a common argument against a public-sector led CBDC system is that the public sector is not able to innovate as quickly as the private sector and the technology choices made at the outset will freeze the system in a moment in time.

While this may be true in some instances, the public sector in many countries is now leading innovative research. There are two areas that policy makers should addressed: how to incentivize the private sector to innovate within the system, and how to ensure the capacity to adapt to change.

Incentivizing distributors and non-distributor PSPs to innovate within the system matters because otherwise they may innovate "outside" the system, leading to new layers of intermediation that silo market growth into privately owned closed systems. While this may result in similarly innovative services, it can also limit the ability of the central bank to meet its policy objectives. Siloed services can introduce frictions to the flow of funds and data and decrease interoperability across CBDC service providers. This could exacerbate "winner takes all" dynamics and create barriers to systemic innovation.

One option to encourage innovation within the CBDC system is provide distributors with a clear ownership stake in the core system. Distributors may then work to ensure the core system adapts by investing in changes demanded by the market. This approach however has a flip side where distributors foster self-serving changes or create frictions for PSPs looking to access the core system.

Governance mechanisms are also an important channel for understanding and evaluating opportunities for innovation. Convening stakeholders on an ongoing basis can help create consensus around what changes or new functionalities in the core system are required or desirable. This can also help address the second challenge around capacity building. Consider a case where market demand exists for the creation of CBDC accounts for children to buy school lunch, for example. Creation of this new account type may be implemented in the transaction layer or through development of a smart contract. Such change is technically feasible but also potentially complex. Governance mechanisms may provide the convening power to bring together policy makers and the private sector to discuss and implement changes being demanded by the market. Ultimately, modernizing the core system requires capturing the right market signals and having the know-how to respond to them. This includes the technical sophistication to implement a new capability, as well as the regulatory framework to ensure its intended usage.

Planning for these potential challenges can help policy makers ensure the CBDC system evolves at a balanced pace. Ideally, the system should evolve quickly enough to keep the private sector incentivized to innovate within the CBDC system, instead of apart from it. At the same time, new functionality must be introduced responsibly and in a way that ensures risks are properly understood and managed.

Access to data: How to manage it in line with policy priorities?

As discussed throughout this paper, securing the right approach to individual privacy is a primary concern among policy makers. Yet they face additional and often conflicting pressures in terms of deciding who has access to what data.

The achievement of "open banking" and "open finance" is increasingly an objective globally. These innovations aim to provide individuals with greater control over who can access their data, as well as drive competition among financial services providers. It will be important to align CBDC data decisions with those being made in the realm of open finance.

Common standards and interoperability are useful not only to foster competition among similar services but also to promote innovation in what services are provided. Data is unlike other commodities in that it can be used by multiple firms without being exhausted, with value unlocked through data sharing. Additionally, the creation of system-wide standards and exchange is valuable to promote innovation in system-wide services. For example, anti-money laundering (AML) efforts can make significant progress if the need to reconcile information across multiple financial institutions is eliminated. Similarly, creating linkages between the CBDC system and identity-based systems can support additional use cases. It will be important to find the right mechanisms for sharing data in aggregate, without breaching individual privacy, as well as to identify ways to enable individuals to decide how their data is shared.

On the other hand, exclusive access to data provides a competitive advantage. Some limitations to data sharing and access may be desirable not only for privacy concerns but also to make certain business models viable. However, excessive limitations and frictions to data sharing may enable significant returns for exclusive data control, enabling what the BIS has called the "DNA loop:" a self-reinforcing dynamic whereby data with strong network effects elicits user activity that generates more data, creating a powerful barrier to entry.[43] Because this dynamic does not emerge overnight, policy makers should watch for potential signs as digitization enables rapid scaling of business models.

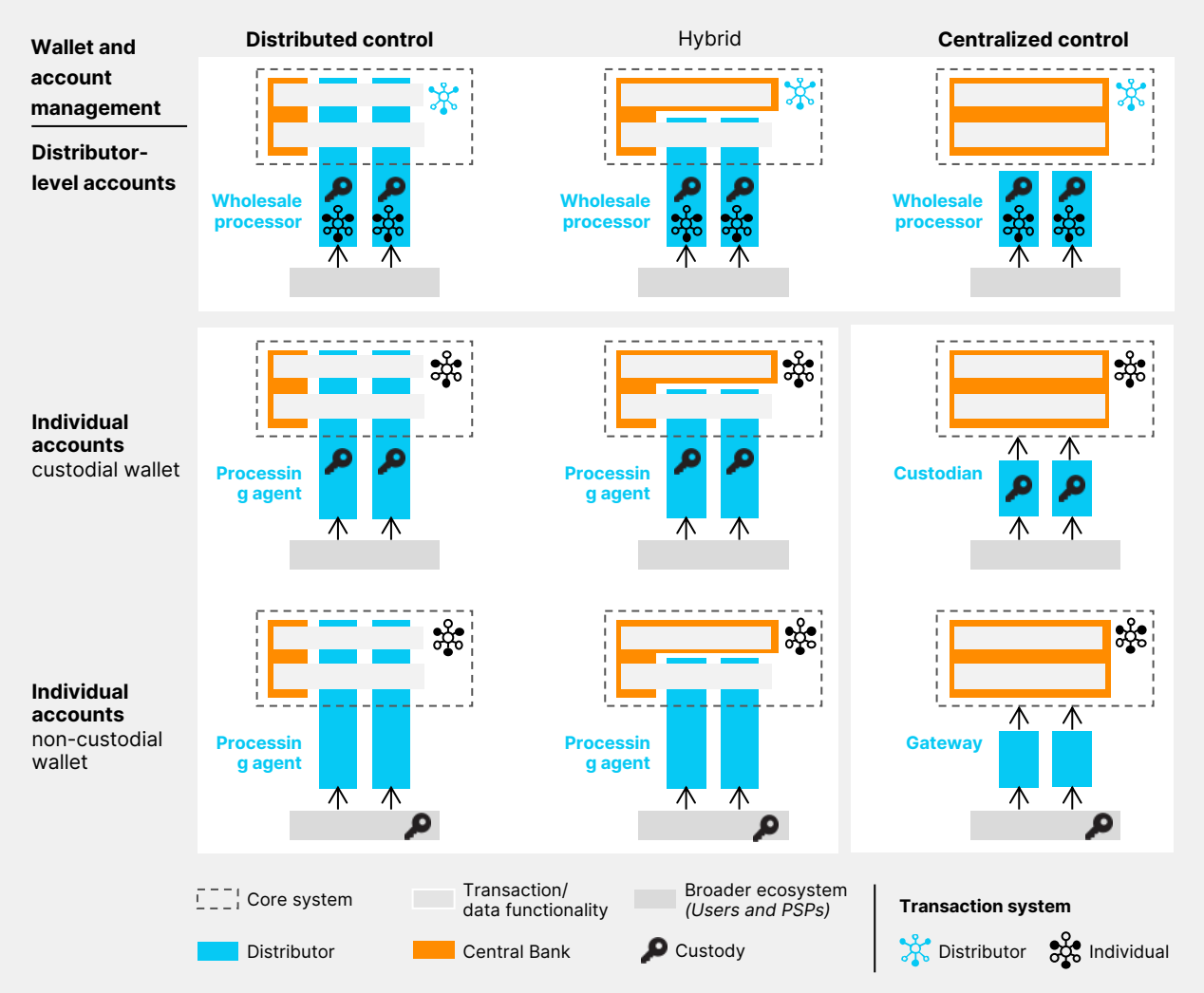
Data access may also impact credit provisioning. Traditionally, deposits have played a dual role as a credit funding source for financial institutions and a means of payment for individuals, resulting in bank access to payments information. A CBDC system has the potential to disconnect this dual role for deposits and decrease bank visibility into payment data. Efficient allocation of credit depends on data both about individuals and about populations, especially as transaction-based credit modeling has shown promise for financial inclusion and promotion of small businesses. Thus, enabling individuals and merchants to easily share their CBDC related histories with credit-creating institutions may be critical in increasing financial inclusion and participation in the formal financial sector.

[43] Bank for International Settlements (BIS) (2019), "Big techs in finance: opportunities and risks", Annual Economic Report 2019, Chapter III.

4.2. Assessing how system design shapes competitive dynamics

The scope of distributors' role can impact competitive dynamics in several ways: facilitating non-distributor access to the system, shaping data flows, and influencing how firms respond to innovation. The solution choices discussed in Section 3 will heavily shape the scope of the distributor role. We discuss a simplified set of options in the figure below to illustrate the relationship between distributor role and competitive dynamics, although we recognize policy makers may choose more complex solution designs.[44]

Figure 10. Spectrum of roles for CBDC distributor



Source: Oliver Wyman Forum and AWS Analysis

[44] As noted in Section 3, policy makers may choose a combination of different options for system or account management, such as allowing both individual-level accounts and distributor-level accounts to exist simultaneously. This means there could be distributors with different scopes, with some distributors playing a role only in processing the core infrastructure while others might also process transactions at a more granular level for their own clients.

Distributor-level accounts: Distributors as wholesale processors

A retail CBDC system based on distributor-level accounts will have some structural similarities to a wholesale CBDC system, with each distributor processing their own set of individual or more granular transactions. This type of system has barriers to entry that protect distributors and creates risk of silos emerging in data flows and innovation.

Barriers to entry

This type of system creates a sharp differentiation between distributors who are involved in the management of user accounts and have direct access to the CBDC system, and other private sector competitors who would only be able to provide services to users by employing distributor gateway services.

There will be technological barriers as distributors will be responsible for processing more granular transactions. Given the importance of distributors to processing transactions, there will also likely be a number of regulatory requirements regarding operational resiliency and end-user protections.

Policy makers may choose to rely only on larger, established operators such as commercial banks, which are able to meet the high regulatory and technical standards that would be required to act as an operator of infrastructure that essentially forms part of the CBDC system. Commercial banks would potentially have a further advantage in gaining market share in the provision of CBDC services through their privileged role as distributors of CBDC.

Some expect CBDCs to initially be distributed through the conversion of commercial bank deposits, which means deposit-taking institutions would serve as catalysts for CBDC adoption. In this case, deposit-taking institutions may then be in a privileged position as first movers in providing CBDC services such as wallet management as well as through their continued visibility into market activity. This could help mitigate the risk of bank disintermediation.

In this design there is another barrier to entry caused by the reliance on a specific distributor. This makes it more burdensome for new entrants to entice users, whether PSPs or individuals, to move to a new distributor. Regulators could overcome this barrier by regulating portability for both individuals and PSPs. Given the structural advantages to distributors in this system, policy makers may consider ways to balance the market power between distributors and other market participants. They could do so by supporting specialized distributors aimed at serving as gateways to PSPs and setting standards regarding open-API access.

Support for continual innovation

Distributors will follow rules agreed to with the central bank for distributor-to-distributor transactions. However, depending on the governance system or regulated structure of retail transactions, they may have significantly more discretion in how they process more granular transactions. They could, for example, automate certain types of payments or differentiate how they batch and order payments for certain providers. It's possible these distributor-based systems could start to diverge in their capabilities.

Distributors will have insight into what innovations are gaining traction in the market. With each distributor responsible for managing their own end-user offerings, they may adjust the way they process individual-level transactions accordingly, such as by incorporating programmability, or look to coordinate changes across all distributors.

In a distributed system, distributors may be more incentivized to coordinate with each other to make changes to the core system consistent with innovations demanded by the market, as they also play a role in processing transactions. However, this may be preferable only in instances where their ability to process transactions is impacted. The ability for innovation to occur in the external application layer, independent of core system processing, is critical with distributor level-accounts.

Access to data

By processing individual-level transactions, distributors have a major advantage as the management of individual user accounts brings with it benefits in terms of access to data and ability to provide additional value-added services, either directly to individuals or to other PSPs. A distributor may also act as an intermediary for a large number of CBDC accounts on behalf of a network of non-distributor PSPs and therefore gain insights from aggregate data across that broader customer base. These insights can provide a significant competitive advantage in payment and other financial services.

As each distributor makes their own technical choices in how they process more granular transactions, it is possible that the distributor-based systems each grow and evolve in ways that reduce portability and interoperability across distributors, as well as the innovation of system-wide services. If there are multiple layers of intermediation, it may be desirable to have standards not just for the exchange of individual data but also PSP data. Additionally, as standards are set, they should be seen as evolving with the market to support continued innovation.

A concern with relying on distributors as wholesale processors is ensuring individuals have a tangible claim to their central bank liability. This is the reason why reporting may be desirable and required, so in case of a malfunction or crisis at the distributor level, the central bank has a back-up to validate user claims, even if such a back-up may come with some timing lag. However, it's possible there will be multiple layers of firms between the individual and the core system. The more layers of intermediation, the more potential risks to individual ownership claims and the more required layers of reporting.

Distributed/ hybrid system management: Distributors as processing agents

A distributed CBDC system will have distributors as key participants/operators of the core system, with advantages in transaction processing, data insights, as well as influence over system functionality. Such a system produces barriers to entry protective of distributors, with potential for data flows that encourage data sharing and flexibility to adapt to innovation.

Barriers to entry

The greater the role distributors perform in system management, the greater the differentiation between distributors and other participants in the CBDC delivery system. With distributed system management, distributors may perform one or both roles: (a) processing transactions and managing CBDC data on behalf of their own customers (and those of their affiliated companies or business partners) and (b) providing access via APIs to the CBDC system to other PSPs who are not directly involved in the operation of the CBDC system.

The type of entity able to fulfil the distributor role in this kind of solution will tend to be larger, established service providers who have the operational and financial resources to invest in participating. Distributors will then be able to perform a dual role – both directly processing their own customer transactions and providing CBDC services to third-party service providers. This dual role provides advantages. For example, they may be able to have improved technical performance in comparison with non-distributors by virtue of not having the latency of the connection from an external system, navigating an API gateway, etc. They may also have benefits in terms of early visibility of changes to the CBDC system and economies of scale in operating multiple systems in the same location. They may also have an advantage in providing overlay services such as programmability, and therefore expand potential business models that advantage them in provision of end services.

Support for continual innovation

Distributors who perform this role will also have outsized influence in how the core system evolves. The specifics will depend on overall governance arrangements. This influence may be a positive: they may use it to promote innovation demanded by the market or promote interoperability with other services or infrastructure they leverage for add-on services. Conversely, they may use influence for their own advantage by pushing updates to the system that favor, for example, specific functionality they have developed. While this could provide incentive to get to market quickly, policy makers should be careful about the possibility of anti-competitive behavior.

Access to data

Access to transaction meta-data can provide distributors with further advantages, as metadata provides valuable insights into user personal profile and buying patterns. This access will depend on decisions made on identity management and data storage. If end-user identity is known and their transaction data available, targeted and personalized services are possible, while otherwise only higher-level aggregate data may be accessible.

Permissioned access to this data could be extremely valuable in creating alternative credit scoring models. The ability to accurately assess customer risk can result in a decrease in service provision costs and open up segments of the population that can be profitable but were previously deemed as too risky.

These additional data-related advantages depend on the extent to which distributors are permitted to make commercial use of information about transactions that do not involve their own customers. If this is not considered acceptable from a policy perspective, then use of encryption and other privacy-preserving technology plus data protection regulation could be used to limit distributor access or the commercialization of granular or personal data. However, policy makers may allow or encourage the usage of aggregate data by distributors, as it could support valuable services such as AML or even innovation in brand new services. For example, there could be the option to provide industry specific data sets to support the development of new products based on macroeconomic trends, such as insurance risk models).

Centralized system management: Distributors as custodians and gateways

If policy makers choose a CBDC system with centralized system management and individual-level accounts, distributors will perform a limited set of functions. Policy makers may choose such an approach for a number of reasons, for example, to maintain more control over the system, provide individuals with more autonomy, or enable a more level playing field between distributors and other payment service providers. However, this type of system might be more prone to multi-layered intermediation, which could impact competitive dynamics, data flows, and innovation in unexpected ways.

Barriers to entry

In a system where distributors perform a limited role as a gateway (see Figure 10), they would serve to open accounts, allow customers to purchase or redeem CBDC for traditional fiat, and submit and process all transactions to the central CBDC system. This type of system has low barriers to entry among distributors, as individuals have full control of their funds and thus greater freedom to move between distributors. This may also result in lower barriers for non-distributors if access to transaction gateway services can be affordably obtained. However, it also implies that there would be fewer competitive advantages to having a distributor role.

If desirable, barriers to entry can be designed to be similarly low in cases where the distributor serves as custodian for end-user accounts. If identity is known to the central bank, portability between distributors could be designed that allows an end user to request custody of their funds be transferred to a new custodian without the authorization of the original custodian. Identity could be proven through a national identity system or federated identity system. This would break a CBDC user's reliance on the custodian who manages the link between their identity and their CBDC account. Proof of identity would then be sufficient to allow a user to transition custody of their CBDC. This would be a further catalyst for competition in services using CBDC, if that is the desired policy goal.

Support for continual innovation

With a centralized system, system performance characteristics could become a limiting factor for innovation. For example, if the core system is constrained in its ability to process transactions in a timely fashion, the implementation of real-time services leveraging the network may be constrained, leading to additional processes like pre-processing or batch transactions. This then creates secondary systems of records that may undermine the policy objectives of a centralized system.

However, a centralized system design also has the ability to encourage innovation in two ways. First, with control of the infrastructure, the ability to implement new functionality can occur rapidly. Second, through equal access to a set of open APIs, new participants and low barriers to entry may result in rapid innovation as an overlay to the system.

Beyond the design of the CBDC system, protocols could be put in place similar to open banking regimes today that would compel a distributor to facilitate movement of services to another distributor and ensure common data sharing standards across the system.

Access to data

A distributor that is strictly a gateway has a smaller informational edge over non-distributors, relative to the other options discussed. Beyond protocols and interoperability standards, it could be desirable to balance data exchange through the provision of shared utilities. For example, as noted above, storing identity centrally could support automatic data exchange through the system.

4.3. Next steps in evaluating competitive dynamics

This section aimed to demonstrate how competitive dynamics may evolve in complex ways. While an overview of high-level factors was provided, the specifics will depend on many factors, such as system requirements, costs, and business models. Just as payment systems have evolved over time in a complex manner, the CBDC space too will not evolve in a single way. This evolution will take place over time, and be dependent on decisions made post-launch.

Our recommendations include:

- Build scenarios and economic models to help anticipate and understand dynamics. We recommend that policy makers work proactively with industry, technologists, and civil society to build potential scenarios to help assess likely dynamics. While it is impossible to be exhaustive in scenario analysis, a collaborative approach may surface new factors that can impact competitive dynamics and the overall vision. Scenarios and models can start out broad, but it will also be useful to add increasing detail that goes beyond the scope of this paper. For example, key components to evaluate will include network connections to merchants, gateways between different payment rails, and the provision of value-added services such as fraud detection.
- Deepen understanding of business models, incentives and user demands. Competitive dynamics will be shaped by what individuals want, what business models are able to meet these end-user demands, and whether those business models are sustainable. Demands from end users will differ by country, but it is important to note that within a single country, multiple end-user groups are likely to emerge with different preferences.
- Use the development and deployment phases to experiment with collaboration models. We also recommend broad experimentation in collaboration with private sector participants to create and test different market structures. Many central banks are requesting feedback on CBDC papers or holding hackathons[45] to inform their research and design process. These same mechanisms could continue to provide value and fresh ideas to mature the system and ensure continued innovation. Success depends not only on governance mechanisms like rules, processes, and standards, but getting the right norms, know-how, and participants. This will take time and iteration. Policy makers would be wise to think ahead as the input gathering process itself may have valuable lessons on what types of forums, participants, and engagement may be most helpful in the long run.

Policy makers should be considering competitive dynamics early on in the process and also continuously. As the space matures, new areas of competitive dynamics will emerge and must be considered. This continual evolution of the system requires that broad stakeholder input be sought not only when designing a CBDC system, but regularly after launch.

[45] See for example Monetary Authority of Singapore (2021): Global CBDC Challenge.

Section 5. Illustrating design trade-offs

As discussed above, central banks may adopt different system design choices based on their specific goals and policy preferences. To further illustrate, we present four different policy archetypes, each with a different vision for their CBDC system and with different positions across the policy trade-offs highlighted in Section 2. For the sake of discussion, we assume each archetype has made the decision to go ahead with launching a CBDC. We then exemplify what these archetypes might choose as a potential solution, given their policy goals.

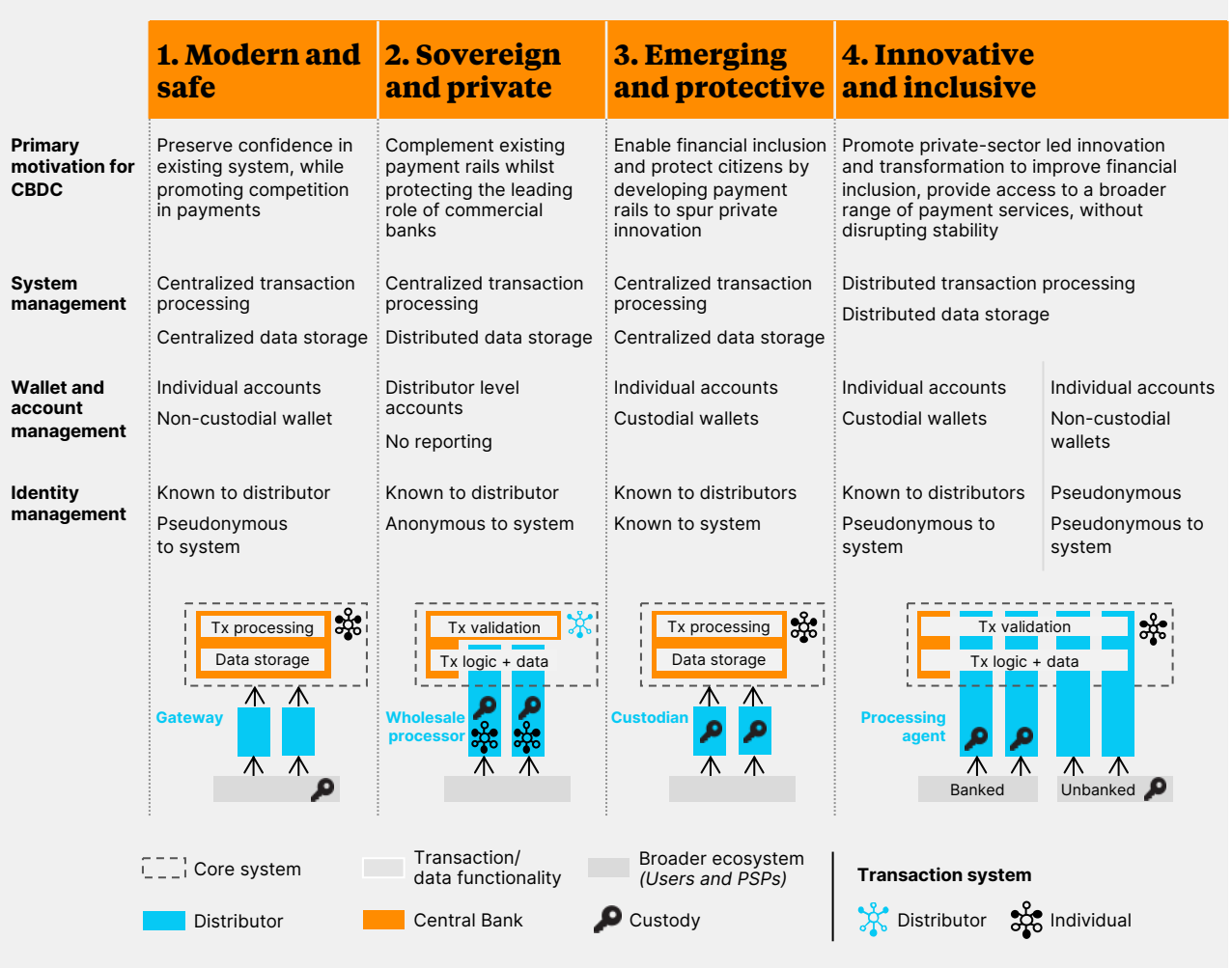
These policy archetypes were chosen to represent a range of potential policy motivations and contexts, spanning developed and emerging markets. While the archetypes are not meant as exact replicas of any specific country, they were inspired by commonly stated policy motivations. For purposes of illustration, we assumed the decision was made to pursue a CBDC in each case to exemplify potential solution choices. However, the right decision for some countries may be to not launch a CBDC at all.

While this paper builds out four very different archetypes, policy makers may benefit from developing their own archetypes to illustrate the trade-offs inherent in different solution choices. Archetypes can be a useful tool for engaging with stakeholders to illustrate the connection between policy and system design choices, and drive a concrete discussion on market impacts.

Key takeaways from this section:

- Similar designs could work for a variety of CBDC visions as long as they are fine-tuned for specific local objectives.
- Pursuing a solution that spans multiple options across wallet and account management can add complexity, but may be the appropriate choice when policy objectives demand it.
- Integration with other facets of a country's payment and data systems can help policy makers reach decisions. For example, the existence of national ID system provides more options as to how identity can be managed.

Figure 11. Overview of archetypes



Source: Oliver Wyman Forum and AWS Analysis

Archetype 1: Modern and safe

High-level purpose: Preserve financial stability and confidence in the existing financial system while promoting competition in payments and protecting monetary sovereignty. Additional goals:

- Modernize payment systems to ensure public infrastructure is attractive to the private sector and not displaced by privately run alternatives.
- Likewise, provide citizens with autonomy and choice in providers while reducing need to experiment with private currencies such as stablecoins.

Assumptions about policy priorities

Distributed vs. Centralized control	• This central bank has high technical and organizational capacity but relatively low appetite for technological risk, while the private sector has high capacity. • Policy makers have low to medium appetite for disruption of the existing banking sector but want to enable financial innovation.
Individual control vs. Distributor reliance	• Individuals tolerate risks, with government willing and able to provide additional resilience, and a strong desire to ease movement across providers. • Policy makers desire to include non-bank PSPs and digital asset providers in the CBDC system, possibly – though not necessarily – as distributors.
Anonymity vs. Centralized services	• This country has a national digital ID system at a level of privacy individuals are comfortable with. Policy makers want to integrate the CBDC system with the national ID system, but individuals are highly sensitive to privacy concerns. • Provision of centralized identity-based services, such as direct transfer of government benefits or tax refunds, may be a lower priority due to the maturity of existing public sector and financial services infrastructure.

Solution design choices

CBDC system management: **Centralized transaction processing and data storage**

- Given the low appetite for technological risk, a centralized CBDC system may be preferred as it leverages proven technologies and minimizes governance complexity. It also enables the central bank to exert leverage over the entire system to enact measures that promote innovation and competition.
- If the central bank would rather broaden the role of distributors, it may prefer a distributed approach with hybrid transaction processing and distributed data storage. Such an approach should be carefully designed to ensure the chosen distributors are not granted undue influence over the CBDC system.

Wallet and account management: **Individual accounts stored on ledger; non-custodial wallet**

- Non-custodial individual accounts would provide the highest degree of freedom of movement between distributors, lowering barriers to competition and helping drive innovation.

***Level of privacy*: ID known to distributor, pseudonymous to system**

- As having sufficient level of individual privacy would be critical for uptake, pseudonymity could help balance that with the need to monitor for illegal activity.
- Continued reliance on distributors for account management and KYC would require identity to be known to the distributor.
- Integration with a National ID system would support the standardization of onboarding processes for distributors and allow the provisioning of ID to receive centralized services should an end user choose to do so.

Archetype 2: Sovereign and private

High-level purpose: Complement existing payment rails while protecting the leading role of commercial banks. Additional goals:

- Protect the current financial system by creating a privacy-preserving retail payment system while ensuring banks retain a leading role in the payment system.
- Counter the declining use of cash and maintain CBDC as a payment mechanism, not as a store of value.

Assumptions about policy priorities

Distributed vs. Centralized control	• This central bank has high capacity and appetite for experimentation. • The private sector also has high capacity, with commercial banks playing an important role in the economy that policy makers want to preserve.
Individual control vs. Distributor reliance	• Individuals are digitally literate, with a core group of individuals being sophisticated and desiring more control of their funds. Individuals are willing to take on more risk in the case of user-error in exchange for autonomy. • Policy makers want to prioritize individual self-reliance over other consumer protections. • To avoid CBDCs being used as a store of value and to avoid adverse impact on banks, policy makers are interested in exploring limits to either transaction size or individual holdings.
Anonymity vs. Centralized services	• The population desires a very high level of privacy, especially privacy from government. Given this preference, privacy is prioritized over the ability of central banks to ascertain individual holdings. • Integration of identity-based government functions is not a policy priority, but personalized services could serve as a differentiator for distributors.

Solution design choices

CBDC system management: **Hybrid with centralized transaction processing and distributed data storage**

- A hybrid infrastructure may be preferred as it allows the central bank to supervise all transactions while limiting its access to data.
- This system design would also support a continued vital role for commercial banks in the new system if they choose to serve as designated distributors.

Wallet and account management: **Distributor level accounts with no reporting**

- Distributor level accounts, combined with distributed data storage, may be preferred to keep individual data with the distributor and accordingly provide individuals an extra layer of privacy protection from government.
- Distributor level accounts would enable similar functioning to a wholesale CBDC system, and would not be dissimilar to existing commercial bank accounts and RTGS payment systems. Distributors would continue to handle individual level transactions and account servicing via internal infrastructure and services.
- Privacy concerns may also lead to policy makers limiting individual-level reporting. Policy makers should then plan for solutions that are actioned in the unlikely event of distributor failure, such as mechanisms for citizen-prompted recovery of lost CBDC or back-up data made accessible to the central bank under these limited circumstances. To minimize risk in case of distributor failure, a link between individual-held CBDC and its associated distributor-held CBDC can be built in to the system to ensure that information is available apart from any distributor's internal systems.[46]

Level of Privacy**: Known to distributor, anonymous to system**

- Given the priority placed on privacy from government, maintaining an anonymous system is likely to be preferred. In this case, there will be a tension between the desire to limit CBDC holdings and this emphasis on privacy. Capping an individual's CBDC balance across multiple accounts requires capacity to track wallets held by multiple distributors, which is not possible in an anonymous system. However, a softer cap can be implemented by imposing limits on CBDC holdings and transaction sizes at each individual distributor.
- Just like current payment systems, KYC processes require distributors to obtain identity information prior to an individual obtaining a CBDC account. Distributors would also continue to support individual level customer support, fraud monitoring, AML reporting, etc.

[46] In the e-HKD paper, a cryptographic link between CBDC issued to a distributor and that held by a retail user is proposed.

Archetype 3: Emerging and protective

High-level vision: Expand access to financial services by developing mature payment rails to spur private innovation, enable financial inclusion, and protect citizens. Additional goals:

- Spur growth and development of the financial system while safeguarding customer protection for a population that may be wary of the formal financial system.
- Enable payments within country (domestic remittances) and possibly across geographic borders (international remittances).

Assumptions about policy priorities

Distributed vs. Centralized control	• This central bank has limited capacity and desire to manage a complex CBDC system but high willingness to experiment with new delivery forms to incentivize adoption. • Local private sector participants have limited technical capacity; developing and building capacity within the financial sector is a driving motivation.
Individual control vs. Distributor reliance	• Financial inclusion is a top priority, along with providing strong protections to individual CBDC users. • Policy makers may want to ensure low barriers to entry to encourage innovation and ensure payment rails are highly efficient and low cost.
Anonymity vs. Centralized services	• There is a willingness to tolerate lower levels of privacy in exchange for increased consumer protection and services. • Policy makers may also be interested in integrating a CBDC system with a national ID system to support public benefits administration and aid distribution.

Solution design choices

CBDC system management: **Centralized transaction processing and data storage**

- A central bank without strong local partners may choose to own system management, potentially collaborating with trusted private-sector partners on system design and training of participants.
- Central banks may begin with a centralized approach while planning to increase distribution of governance and technical responsibility as the financial system matures. Increasingly sophisticated participants in the CBDC system will be able to perform a larger role over time in system management if desired.

Wallet and account management: **Individual accounts stored on ledger, custodial wallets**

- In order to promote resilience in case of private sector failure as well as limit risks of financial loss borne by a potentially vulnerable population, storing and processing of individual balances and transactions by a centralized operator may be preferred.
- Public-private partnerships may enable custodial services built on provision of digital identities, potentially including public campaigns to increase digital literacy of custodians and citizens alike.

***Level of privacy*: Known to distributors and system**

- Tying identity to CBDC accounts may be preferred in this context to support new financial products, such as alternative credit scoring built on digital financial histories. New or existing digital identity systems may be integrated with the CBDC system to promote accessibility to those previously excluded from the formal financial sector.
- Centralized identity management would also facilitate provision of direct fiscal transfers to citizens, and protects CBDC assets against failure of any individual distributor.

Archetype 4: Innovative and inclusive

High-level purpose: Promote increasing financial inclusion by providing wider access to a broader range of payment services and enabling innovation without disrupting stability. Additional goals:

- Ensure wider access to a range of payment services for both retail end users and small to medium- sized enterprises (SMEs).
- Enable new forms of financial innovation without necessarily disrupting existing financial or technology incumbents.

Assumptions about policy priorities

Distributed vs. Centralized control	• The central bank has high willingness to experiment with new forms of delivery and incentivize wide adoption. • Policy makers may also value enabling cross-border payments and integration with the global financial system, including interoperability with other digital assets such as private stablecoins to facilitate innovation and encourage growth.
Individual control vs. Distributor reliance	• There is a sizeable unbanked population, motivating a strong desire to protect individuals by ensuring risk is primarily borne by the private or public sector. • Policy makers want to ensure low barriers to entry for PSPs to encourage experimentation with inclusive models, as well as a desire to leverage non-traditional actors like telcos and social media firms to expand reach of distribution.
Anonymity vs. Centralized services	• Society has a willingness to tolerate lower levels of privacy in exchange for individual risk mitigation and greater consumer protection and services. • Policy makers may want to provide services for individuals currently excluded from the financial system due to lack of government identification by offering low-value accounts.

Solution design choices

A mixed solution model is best suited to the policy goals of this archetype. While system management is common across solution designs, levels of privacy and extent of intermediation will vary between solutions designed for currently banked populations and for unbanked populations.[47]

- Providing non-custodial wallets to low-income individuals can limit customer protection mechanisms and increase risk of fraud and financial crimes. These wallets may be treated as short-term solutions until individuals are provided with appropriate identification and moved to a custodial wallet with advanced consumer protection. CBDC system roll-out may include programs to support those operating with low-value, non-KYC wallets to obtain the necessary documents to verify their identity and move into the formal financial sector.
- Nevertheless, a limited number of individuals may prefer to accept these risks in order to maintain privacy for low-value transactions

CBDC system management: **Federated with shared governance (distributed transaction processing and distributed data storage)**

- A distributed model may be chosen to support integration with a wide variety of financial firms and partnerships with non-traditional financial players that could promote financial inclusion. Incorporating non-traditional actors in the CBDC network promotes innovative services, including interoperability with other digital asset platforms.
- Shared governance could build private sector buy-in and ensures the central bank is participating in the issuance of CBDC while not appropriating any of the services private sector players may provide. However, governance of a distributed system would increase complexity and necessitate close public-private collaboration on system management.

For those currently banked

Wallet and account management: **Individual-level accounts with custodial wallets**

- Central bank capacity and willingness to experiment could motivate the decision to support individual accounts within the CBDC core system. This would facilitate the provision of additional government services, especially if connected to digital identity.
- Custodial wallets are desirable to minimize risks borne by individuals and ensure distributors bear responsibility for the risk of lost funds.

Identity management**: Known to distributor and pseudonymous or known to system**

- Those with an existing banking relationship will already be known to their financial institution. Unique identifiers are likely linked to a central ID if such a system exists; otherwise, individuals remain pseudonymous to the central bank.

[47] For example, the ECCB currently offers two ways to access DCash depending on whether the end user has an account at a participating financial institution or not.

- Optional sharing of identity with central bank may also be offered to acquire government services. Citizen's may also opt in to sharing their financial data to acquire additional financial services.

For those currently unbanked

***Wallet and account management*: Individual-level accounts with non-custodial wallets**

- The use of non-custodial web wallets is high in countries with large proportions of unbanked customers,[48] and in case of high mobile adoption, policy makers may opt for non-custodial wallets with keys stored on a mobile device.
- Storing keys on mobile devices could increase the risk of lost funds. Policy makers could cap both CBDC holdings as well as transaction size to mitigate large losses. Initial provision of these limited capacity wallets could serve as a bridge to eventual inclusion in the formal financial sector.

***Identity management*: Pseudonymous to distributor and system**

- In the absence of any other accepted forms of identity, an account number could be assigned to unbanked individuals as an interim form of identification.
- If pseudonymous identities are all that would be available to the distributor, then that is all that would be available to the central system as well.

[48] See Chainalysis Global Crypto Adoption Index.

Section 6. Path forward

The complete journey from CBDC discovery through launch is a multi-year effort that requires close collaboration between policy makers, technology teams, and all impacted stakeholders. Throughout this journey, there will likely be many points at which various countries decide to continue, or not, toward a CBDC launch. Research, experimentation, and collaboration along the way can ensure that if a central bank makes it to launch, they will have a well-designed policy-driven CBDC system.

To support the development of policy-driven CBDC solutions, we summarized common policy goals driving central banks to consider implementing a CBDC. Those policy drivers were then analyzed to determine which were likely to be particularly sensitive to technology choice. The result was a framework that central banks can use to evaluate the interrelation of desired design principles with available solution design decisions as they seek how best to meet their policy goals.

As policy should guide technology choices and there are many choices to be made, public engagement is critical. Any CBDC system will have required many choices that will continue to have a dynamic effect over time.

We recommend that central banks:

- **Set clear policy priorities from the outset and continue to revisit them.** Policy priorities should be agreed upon and examined to determine if a CBDC is the right solution. As discussed in this paper, many aspects of design are interconnected and will require trade-offs based on those priorities. Clarity will help ensure that solution design and thus the program fulfills expectations.
- **Learn about key technological aspects of CBDCs, and likewise, have technologists learn about potential policy impacts of their design choices.** Throughout a multi-year program, new technology considerations will likely emerge and have an impact on policy. Policy makers should stay on top of developments in order to refine their policy choices. Those closest to the technology are positioned to understand it. There could potentially be second-order effects that are best understood when there is clarity on policy objectives. As the iterative process progresses, every decision needs to be evaluated both for its technical ability to meet functional requirements and for its impact on the ability to meet today's – and tomorrow's – policy objectives.
- **Launch technical experiments.** Experimentation does not require a final decision about whether or not to launch a CBDC. Many countries are awaiting the results from their own and other's experiments before finalizing their decision. CBDC systems will need rigorous technical experimentation around system requirements for resilience, throughput, and scalability, for example, before determining if the system can achieve policy goals. Flexibility in these experiments will then guide final design decisions and CBDC system development. A growing body of technical trials provide a foundation on which new CBDC projects can be built. Nevertheless, each central bank has a distinct hierarchy of goals and faces a unique set of implementation constraints. Experiments are required to identify the most appropriate system design and verify its operational integrity.

- **Develop your own scenarios, as a way to engage with stakeholders.** Building out scenarios has three benefits: First, it can sharpen policy makers' understanding of potential dynamics, risks and second order effects of a particular set of design choices. Second, scenario analysis can provide input into design deliberations and potential mitigants to various challenges and risks. Finally, it can also play a role in helping refine policy priorities as scenarios help both policy makers and constituents better understand policy trade-offs.
- **Track industry developments.** There is significant innovation happening in payments and digital assets across both technology and business models. Financial institutions are innovating quickly in the realm of tokenized assets. Large international merchants have extensive experience in developing and maintaining sophisticated payment systems. And leading cloud providers can provide the infrastructure to support CBDC development from design through launch. Central banks should keep their fingers on the pulse of that innovation as it may unlock new possibilities and risks that were not yet considered in their CBDC program.
- **Differentiate between near-term, long-term, and evolving goals.** There remain many unknowns and the effectiveness of a CBDC system will depend on the dynamic evolution of public and private collaboration. Understanding "must-haves" can help policy makers clarify which goals they want to meet through technology as opposed to policy.[49]
- **Continue to learn and experiment throughout the process.** Continued experimentation, combined with public engagement, will provide additional information that will inform policy changes to the system. Rolling out such systems at scale is also likely to reveal unanticipated issues. Pre-emptive communication with the public will increase confidence that discovered issues do not threaten the fundamental integrity of the system. Policy makers will also need to consider their own specific policy context, including issues like data strategy and open banking, and devise a process for potentially integrating CBDC systems with other digital services such as national identity and delivery of social programs, whether they are public or private.

[49] For example, data privacy can be controlled by technology through cryptographic means or through governance standards that limit data access.

Appendix A. Glossary

- **Account-based system:** System where digital assets are recorded as a balance amount held by an entity, with transactions increasing or decreasing the balance.
- **Anonymous**: The individual is not known to the central bank, distributors, or any counterparties.
- **Central bank digital currency (CBDC):** A digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank.
- **CBDC account**: An individual or distributor's holding of CBDC, whether stored as a single balance or collection of unique unspent transaction outputs (UTXOs).
- **CBDC governance:** The processes by which decisions over the structure, capabilities, and technical features of a CBDC system are made.
- **CBDC distributor:** A private sector participant that provides gateway services between individual users of CBDC and the CBDC system itself.
- **CBDC wallet:** The mechanism through which an individual or distributor interacts with their funds.
- **Centralized transaction processing:** A central entity manages all validation checks and performs any advanced transaction logic that may be programmed into the core system.
- **Centralized data storage:** A central entity holds all data for a transaction as it is processed by the core system.
- **Consensus mechanism**: A fault-tolerant computational mechanism used to reach an agreement on a single global state among distributed network participants.
- **Core CBDC ledger:** The primary ledger of the CBDC system that holds an immutable list of all state updates. The core ledger can exist within a single datastore or across multiple datastores.
- **Core CBDC system:** The set of technologies, participants, procedures, and rules in place to maintain the issuing and settling of CBDCs. We assume the central bank is issuing/minting CBDCs.
- **Core ledger technology:** The underlying ledger and data choices that define how the CBDC core ledger processes and stores issuance and transaction events. This can include conventional database technology such as SQL and NoSQL, distributed ledger technologies like Ethereum, Corda, and Hyperledger, or custom technologies such as Taler and eCurrency.
- **Custodial wallet:** One in which a third party holds all information necessary to sign and submit a transaction on behalf of the user, thus assuming custody over these assets on behalf of the user.
- **Custodian:** A third party that manages assets on behalf of the asset owner.
- **Digital currency:** A means of payment and store of value that does not have physical attributes and is available only in digital form.
- **Distributed data storage:** A system in which each distributor holds only the data relevant to the transactions in which they are involved or to which they have been given explicit access.
- **Distributed ledger technology (DLT):** The technological infrastructure and protocols that allow simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations.

- **Distributed transaction processing:** A system in which distributors are permitted to fully handle transaction verification and transaction processing logic.
- **Distributor-level accounts**: Accounts in the core CBDC ledger that record only the total CBDC holdings of each distributor.
- **Double spend:** When a digital asset is spent more than once, creating a discrepancy between the spending record and the amount of currency available.
- **Global state:** The current distribution of digital assets among owners at any point in time.
- **Federated system:** A model in which several distinct systems exist, while allowing for interoperability and authentication across systems and external applications.
- **Gateway:** Distributor role that serves to open accounts, allow customers to purchase or redeem CBDC for traditional fiat currency, and submit and process all transactions to the CBDC core system.
- **Hybrid transaction processing:** A system in which the central bank performs only part of transaction validation, typically including validating CBDC inputs into a transaction to ensure they are legitimate, ensuring no double spend or counterfeit funds. Distributors then handle all other validations of the transaction itself and the processing of transaction logic. Most common in UTXO-based systems.
- **Hybrid data storage:** Only necessary transaction data is received and stored by the CBDC system. Transaction metadata is likely to be communicated in peer-to-peer messaging and stored only by relevant parties**.**
- **Identity-based access:** Access solutions in which a user must prove their identity, through a username and password, for example, to transact with their CBDC holdings.
- **Identity-based service:** Any service that requires the owner of an account be known such that funds are provided to that exact individual. Examples include stimulus payments, tax refunds, and emergency aid.
- **Individual-level account:** An account for which CBDC holdings are recorded directly on the core CBDC ledger and transactions directly update the core CBDC ledger.
- **Intermediary:** An entity that sits between two or more parties in a financial transaction to ensure the transaction completes as agreed upon.
- **Non-custodial Wallet** – One in which an individual holds all information necessary to sign and submit a transaction on their own.
- **Payment Service Provider (PSP):** An entity that does not serve as a distributor but provides additional customer-facing services that include user interfaces like mobile apps and web widgets, value-added functionality, customer support, merchant services, payment gateways, and potentially other forms of programmability.
- **Private Key:** The secret key within public-key cryptography that is used for authentication and grants control of digital currency held by the associated wallet.
- **Processing Agent:** Distributors that directly process their own customers' individual-level transactions and/or provide CBDC services to third-party PSPs.

- **Programmable:** The attribute of a system that supports self-executing software programs that trigger when certain conditions, specified in the code, are met.
- **Pseudonymous:** A system in which a unique identifier is linked to each individual's transactions but does not provide identity information.
- **Stablecoin:** A digital currency that is pegged to a traditional reserve asset, like the U.S. dollar or gold, or a basket of reserve assets.
- **Retail CBDC:** A CBDC that exists within national borders and is accessible to individuals.
- **Token-based access:** An access solution whereby a user needs only to provide a digital token such as a private key to transact with their CBDC holdings.
- **Transaction data:** The data needed to process a transaction, such as sender ID, recipient ID, and amount.
- **Transaction metadata:** Contains information about a transaction that may include counterparty information and additional text fields with transaction notes.
- **Two-tier CBDC:** A CBDC system in which the central bank relies on private sector participants to act as intermediaries and serve as the gateway between individual users of CBDC and the CBDC system.
- **System Design Configuration:** The specific implementation of customizable technology that results from a variety of technical decisions that define the logical interrelationship between a system's critical roles and functions.
- **Technology Solution:** A set of functional design choices, that specify how the CBDC core system works and how it is accessed by participants in the broader market.
- **Wholesale CBDC**: A CBDC for which central bank liabilities are accessible exclusively to institutions and meant to provide a final means of settlement for high value payments made with deposits or other types of private sector monies.
- **Wholesale processor:** A distributors that holds distributor-level accounts and manages individual-level accounts including their creation and transaction processing.
- **UTXO-based system:** System in which a digital asset is represented as a unique unspent transaction output (UTXO) with a value and history that can serve as an input to a future transaction.

Appendix B. Connection to literature

There is a robust literature on retail CBDCs, with an explosion of new papers in the past year. We hope this paper adds to the discussion. We recognize there are a number of different frameworks and definitions, so in this section we discuss how this paper connects to other published work. Note, the references below are not exhaustive of all papers in this quickly developing space.

Connection to policy literature

As we have highlighted in this report, it is critical that each country makes its own decision on whether or not to launch a CBDC based on its policy objectives and careful consideration of risks, benefits and trade-offs. Recent BIS surveys have expanded on the various motivations central banks have for exploring CBDCs and how these differ between emerging markets and advanced economies.[1] Central banks have begun to articulate overarching principles[2] as well as specific objectives[3] and trade-offs[4] through reports and public consultations. Many reports also expand on the potential risks of CBDCs,[5] and how those may differ for emerging markets[6] and least developed countries.[7]

To help policy makers in their decision process, recent papers have provided an overview of design choices,[8] as well as a toolkit for how to carry out the decision, spanning retail and wholesale CBDCs.[9] A prior Oliver Wyman report has expanded on mistakes that policy makers should avoid when considering retail CBDCs.[10] Our paper adds to this discussion by focusing on the relationship between policy, technology, and competitive considerations related to retail CBDC design.

Our discussion of policy design principles also builds on a robust and growing literature. On the division of roles between the private and public sector, we observe that an increasing number of central banks are opting for some form of collaboration between them.[11] Different potential models for cooperation are taking shape[12] and, as discussed in Section 2.3, will require different trade-offs.[13] We expand further on our terminology around intermediation below.

With regards to discussions on privacy and individual rights, a recent BIS paper summarizes the literature on data privacy and integrity.[14] As noted in Section 2, considerations around individual rights will depend on a deep understanding of individual preferences within each jurisdiction. Many central banks are already taking note of this,[15] with active contributions from think tanks and research centers.[16]

There is extensive and growing research around CBDC remuneration and its impact on user adoption and financial stability. Central banks and economists across research institutions have been looking to estimate and quantify the potential uptake of retail CBDCs.[17] While we explore interest rate and account limits, additional options are under study including waterfall accounts[18] and making use of collateral and quantity requirements.[19]

The relationship between CBDCs and questions of competition is a very nascent space in the literature. A recent BIS working paper[20] highlights this as an area for further research, and competition is one of the key themes in a recent study commissioned by the ECB.[21] We see Section 4 as a novel contribution to this space, articulating the relationship between design choices and competitive factors.

Connection to solution and technology literature

Role of distributor and intermediation models

Various publications have addressed the structure of the private sector model supporting CBDC delivery. This includes the use of alternative terms for the role we refer to as a "distributor" providing gateway access for users to the CBDC system. These alternative terms include payment interface provider,[22] payment services provider,[23] participant,[24] and intermediary.[25]

In Section 4 we use various terms to describe the way in which distributors intermediate between the CBDC system and end users. We use the terms "gateway" and "custodian" to describe roles for distributors in a centralized transaction processing model where they act purely as gateways. Elsewhere the term "gatekeeper" has been used to describe this model of intermediation.[26] We use the terms "processing agent" and "wholesale processor" to describe a model in which the distributor also has a lead role in processing transactions for all end users. Elsewhere the term "settlement agent" has been used to describe that model of intermediation.[27]

The term "two-tier" is also used in different ways – both to describe a solution in which the central bank does not have any direct relationship with individual CBDC users and real-time payments are handled by intermediaries,[28] and to describe a system in which there is one system managing "distributor-level accounts" and one or more systems managing "individual-level accounts.[29] The BIS terms the latter an "intermediated" model. [30] The term "two-tier" is also used in an entirely different sense to refer to different remuneration models for CBDC. [31]

There has been significant discussion on the variety of roles for the private sector as service providers operating CBDC. This includes description of a tiered model for provision of services to CBDC users in which some providers participate directly in processing transactions and others do so indirectly via API access to distributors.[32]

Transaction management models

The transaction processing model that we refer to as "centralized" in this paper aligns to the approach described as the "platform model" by the Bank of England.[33] Elsewhere this approach is explored in detail and described as "centralized" in terms of the CBDC system while emphasizing that infrastructure may be distributed for resiliency. [34] It does not align directly to any of the models described by BIS in their paper on different intermediation models,[35] although it has been characterized[36] as being a variation on the "direct" model in that paper but with all customer-facing activities carried out by distributors.

The transaction processing model we refer to as "hybrid," in which the validation of UTXOs is performed by the central bank and distributors carry out the other transaction processing activities, aligns to models described in several publications.[37] Most recently, the US Federal Reserve Bank of Boston released its Project Hamilton architecture that provided an alternate division of transaction processing, though it retains centralized transaction processing.[38]

The transaction processing model we refer to as "distributed" is similar to that described in the context of RTGS transactions using ConsenSys Quorum.[39] This approach is also proposed as one option for a Euro retail CBDC.[40] In other publications the term "distributed" is used in the conventional sense to described a CBDC infrastructure that is distributed across a number of servers in geographically isolated locations for resiliency but remain under central control.[41] This model would be referred to as "centralized" in this paper.

Both the hybrid and distributed transaction management approaches described in this paper could be combined with the use of a separate, parallel, distributor-level account management system for processing wholesale level transactions.[42] This would align with the approach referred to as "intermediated" by BIS,[43] an example of which is described in detail by the HKMA.[44] In this approach individual user level transactions are carried out in one system and transactions between distributors, and between distributors and the central bank, take place in another. A model for this approach is also described in another publication without using the term "intermediated."[45] In these models the transactions at the two levels, or tiers, can be linked and performed together[46] or be loosely coupled as contemplated by BIS,[47] operating as independent but linked parallel systems.[48]

Anonymity and Privacy

Pseudonymity from the central bank has been explored in the context of a centralized solution.[49] Pseudonymity to provide privacy from other distributors is also considered with additional details about potential approaches to improve privacy by making it more difficult to infer the identity of a user from their transaction history.[50] This approach has also been referred to elsewhere as "external identity provider and identity token on chain."[51]

Anonymity from the central bank can be achieved in a variety of solutions, including hybrid transaction processing[52] and a wide range of intermediated solutions and solutions involving distributor level wallets.

Additional approaches to provide privacy of transaction data and user account balances, such as the use of private transactions, payment channels, and zero knowledge proofs, are also considered in the literature. [53]

References

[1] Raphael Auer, Codruta Boar, Giulio Cornelli, Jon Frost, Henry Holden and Andreas Wehrli (2021): CBDCs beyond borders: results from a survey of central banks, BIS Papers, no 116, June.

[2] See for example: G7 (2021): Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs). Report and Group of Central Banks (2020): Central bank digital currencies: foundational principles and core features", Joint Report no 1.

[3] For a comparison of policy goals across CBDC projects, see: Gabriel Soderberg in collaboration with Marianne Bechara, Wouter Bossu, Natasha Che, John Kiff, Inutu Lukonga, Tommaso Mancini-Griffoli, Tao Sun, and Akihiro Yoshinaga (2022): Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons, International Monetary Fund. FinTech Note 2022/004.

[4] Discussions on trade-offs span different types of considerations. For a discussion on trade-offs between policy principles, see G7 (2021): Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs). For a discussion on trade-offs between design options and social and financial costs, see Hanna Armelius, Gabriela Guibourg, Stig Johansson, and Johan Schmalholz (2020): E-krona design models: pros, cons and trade-offs, Sveriges Riksbank Economic Review 2020:1, pp 80-96.

[5] For an overview of risks, see BIS (2020): Central banks and payments in the digital era, Annual Economic Report, Chapter III. For a deeper discussion on potential risks to consumers, see World Economic Forum (2021): Digital Currency Consumer Protection Risk Mapping, Digital Currency Governance Consortium White Paper Series 3 out of 8.

[6] Erik Feyen, Jon Frost, Harish Natarajan and Tara Rice (2021): What does digital money mean for emerging market and developing economies, BIS Working Paper No 973.

[7] Foster, Katherine and Blakstad, Sofie and Gazi, Sangita and Bos, Martijn (2021): Digital Currencies and CBDC Impacts on Least Developed Countries, The Dialogue on Global Digital Finance Governance Paper Series.

[8] See for example: Brookings (2020): Design Choices for Central Bank Digital Currency: Policy and Technical Considerations; IMF (2020): A Survey of Research on Retail Central Bank Digital Currency; and Tommaso Griffoli, Maria Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu and Celine Rochon (2018): Casting Light on Central Bank Digital Currencies. IMF Staff Discussion Notes. 18. 1. 10.5089/9781484384572.006.

[9] World Economic Forum (2020): Central Bank Digital Currency Policy-Maker Toolkit

[10] Douglas Elliott and Larissa de Lima (2021): CBDCs: Six Policy Mistakes to Avoid

[11] This is the case across all countries or blocs that have launched CBDCs (Bahamas, China, Eastern Caribbean Currency Union, and Nigeria), as well as those currently in pilot phase (Jamaica, Sweden, Ukraine, South Korea and Kazakhstan) as of January 2022.

[12] See Group of Central Banks (2021): Central bank digital currencies: system design and interoperability, BIS Other Publications, Report no 2.

[13] To see how central banks may have to choose between a complex technical infrastructure or a complex supervisory regime, see Raphael Auer and Rainer Boehme (2021): Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers, no 948, June.

[14] Raphael Auer, Jon Frost, Leonardo Gambacorta, Cyril Monnet, Tara Rice and Hyun Song Shin (2021): Central bank digital currencies: motives, economic implications and the research frontier, BIS Working Papers No 976.

[15] Group of Central Banks (2021): Central bank digital currencies: user needs and adoption", BIS Other Publications.

[16] See for example, Maiden Research (2021): Centering Users in the Design of Digital Currency (focused on the US); Jian (2020): "CBDC adoption and usage: some insights from field and laboratory experiments" Bank of Canada Staff Analytical Note 2020-12; and Michiel Bijlsma, Carin van der Cruijsen, Nicole Jonker and Jelmer Reijerink (2021): What triggers consumer adoption of CBDC? De Nederlandsche Bank Working Paper No. 709

[17] See for example, Bank of England (2021): New Forms of Digital Money, June. and Group of Central Banks (2021) Central Bank Digital Currencies: Financial Stability Implications, BIS, September.

[18] See Central Bank of the Bahamas (2019) Project Sand Dollar: A Bahamas Payments System Modernisation Initiative and Ulrich Bindseil, Fabio Panetta and Ignacio Terol (2021) Central Bank Digital Currency: Functional Scope, Pricing, and Controls, ECB Occasional Paper Series No 286, December.

[19] Katrin Assenmacher, Aleksander Berentsen, Claus Brand, Nora Lamersdorf (2021) A Unified Framework for CBDC Design: Remuneration, Collateral Haircuts, and Quantity Constraints, ECB Working Paper Series No 2678.

[20] Raphael Auer, Jon Frost, Leonardo Gambacorta, Cyril Monnet, Tara Rice and Hyun Song Shin (2021) Central bank digital currencies: motives, economic implications and the research frontier, BIS Working Papers No 976.

[21] Brunnermeier, M.K. and Landau, JP. (2022): The digital euro: policy implications and perspectives, Publication for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

[22] See Bank of England (2020): Central Bank Digital Currency: opportunities, challenges, and design, Discussion Paper.

[23] See Raphael Auer and Rainer Boehme (2021): Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers, no 948, June; Amazon Web Services (2021): Central Bank Digital Currency: Objectives and architectural considerations; and Amazon Web Services (2021): Central Bank Digital Currency: Technology options and performance criteria.

[24] Sveriges Riksbank (2021): E-krona pilot phase 1, Report.

[25] See Eurozone Group (2021): Digital Euro experiment: Combined feasibility – Tiered model, Hong Kong Monetary Authority (2021): e-HKD: A technical perspective, and Group of Central Banks (2021): Central bank digital currencies: system design and interoperability, BIS Other Publications, Report no 2.

[26] See European Central Bank (2020) Report on a digital euro, and Banca d'Italia (2021): A digital euro: a contribution to the discussion on technical design choices. To note, this was part of Workstream 2 of the Digital Euro experiments.

[27] *Ibid, endnote 26.*

[28] See Raphael Auer and Rainer Boehme (2021): Central bank digital currency: the quest for minimally invasive technology, BIS Working Papers, no 948, June, which introduces the term "Intermediated" model for Distributor Level accounts.

[29] *Ibid, endnote 25.*

[30] *Ibid, endnote 28.*

[31] Ulrich Bindseil (2020): Tiered CBDC and the financial system, ECB Working Paper Series No 2351, January. This working paper describes an approach to remuneration of CBDC based on different tiers.

[32] See R3 (2020): Central Bank Digital Currency: an innovation in payments, White Paper, which introduces the two layer system of "distributors" and non-distributors in the context of a Hybrid System Management solution. See also Eurozone Group (2021): Digital Euro experiment: Combined feasibility – Tiered model.

[33] *Ibid, endnote 22.*

[34] Banca d'Italia (2021): A digital euro: a contribution to the discussion on technical design choices.

[35] *Ibid, endnote 28.*

[36] Hong Kong Monetary Authority (2021): e-HKD: A technical perspective.

[37] See for example HKMA (2021): e-HKD: A technical perspective; David Chaum, Christian Grothoff and Thomas Moser (2021): How to issue a central bank digital currency, Swiss National Bank Working Paper 2021-03; Sveriges Riksbank (2021): E-krona pilot phase 1, Report; and R3 (2020): Central Bank Digital Currency: an innovation in payments, White Paper.

[38] See Federal Reserve Bank of Boston and Massachusetts Institute of Technology Digital Currency Initiative (2022) Project Hamilton Phase 1: A High Performance Payment Processing System Designed for Central Bank Digital Currencies and the associated technical paper: James Lovejoy, Cory Fields, Madars Virza, Tyler Frederick, David Urness, Kevin Karwaski, Anders Brownworth, and Neha Narula (2022): A High Performance Payment Processing System Designed for Central Bank Digital Currencies.

[39] Monetary Authority of Singapore (2017): Project Ubin Phase 2 Report: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies.

[40] *Ibid, footnote 34.*

[41] *Ibid, footnote 34.*

[42] See Amazon Web Services (2021): CBDC: Technology options and performance criteria.

[43] *Ibid, footnote 30.*

[44] *Ibid, footnote 36.*

[45] *Ibid, footnote 34.*

[46] *Ibid, footnote 36.*

[47] *Ibid, footnote 30.*

[48] Eurozone Group (2021): Digital Euro experiment: Combined feasibility – Tiered model.

[49] See Bank of England (2020): Central Bank Digital Currency: opportunities, challenges, and design, Discussion Paper and Banca d'Italia (2021): A digital euro: a contribution to the discussion on technical design choices.

[50] *Ibid, footnote 36.*

[51] *Ibid, footnote 48.*

[52] See David Chaum, Christian Grothoff and Thomas Moser (2021): How to issue a central bank digital currency Swiss National Bank Working Paper 2021-03, and Banca d'Italia (2021): A digital euro: a contribution to the discussion on technical design choices.

[53] See for example Eurozone Group (2021): Digital Euro experiment: Combined feasibility – Tiered model, and World Economic Forum (2021) Digital Currency Governance Consortium White Paper Series, Compendium Report, November.

AWS Service and Technology References

Amazon Aurora Serverless is an on-demand, auto-scaling configuration for Amazon Aurora.

Amazon CloudFront is a content delivery network (CDN) service built for high performance, security, and developer convenience.

Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale.

Amazon's event driven architecture uses events to trigger and communicate between decoupled services and is common in modern applications built with microservices.

AWS Fargate is a serverless, pay-as-you-go compute engine that lets you focus on building applications without managing servers.

Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log.

AWS Well-Architected framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads. Built around six pillars—operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability—AWS Well-Architected provides a consistent approach for customers and partners to evaluate architectures and implement scalable designs.

Author Bios

Lead Authors

Larissa de Lima co-leads the Future of Money initiative for the think tank Oliver Wyman Forum and she is focused on enabling new forms of money and payments that foster society wide value.

larissa.delima@oliverwyman.com

Erica M Salinas leads digital asset initiatives for Amazon Web Services within the worldwide public sector and brings expertise in blockchain, financial services, and financial inclusion.

Contributing Authors

Douglas J Elliott focuses on the intersection of finance and public policy, building on decades as an investment banker and then scholar at the Brookings Institution and the International Monetary Fund.

douglas.elliott@oliverwyman.com

David MacKeith is a principal business lead for Amazon Web Services government financial services in EMEA, bringing experience in digital currencies, monetary analysis, and regulatory reporting.

Jean-Baptiste Lepetit is a Principal in Oliver Wyman's banking practice, focusing on digital transformation topics for large European financial institutions (including payments, digital assets and CBDCs).

jeanbaptiste.lepetit@oliverwyman.com

Paul Cauchon supports the design and development of highly performant mission critical financial system architectures for Amazon Web Services worldwide public sector customers.

Ramiro de la Rosa leads Oliver Wyman's strategic partnerships, focusing on elaborating new value propositions and thought leadership in collaboration with other leading companies.

ramiro.delarosa@oliverwyman.com

About the Oliver Wyman Forum

The Oliver Wyman Forum is committed to bringing together leaders in business, public policy, social enterprises, and academia to help solve the world's toughest problems. The Oliver Wyman Forum strives to discover and develop innovative solutions by conducting research, convening leading thinkers, analyzing options, and inspiring action on three fronts: Reframing Industry, Business in Society, and Global Economic and Political Change. Together with our growing and diverse community of experts, we think we can make a difference.

For more information, visit www.oliverwymanforum.com

About Amazon Web Services

For over 15 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud offering. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 200 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 84 Availability Zones within 26 geographic regions, with announced plans for 24 more Availability Zones and eight more AWS Regions in Australia, Canada, India, Israel, New Zealand, Spain, Switzerland, and the United Arab Emirates. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs.

To learn more about AWS, visit aws.amazon.com.