# DECODING CBDC:

## ENTERING THE NEXT PHASE OF CBDC EXPLORATION

*PRESENTED BY* CURRENCY RESEARCH AND LIPIS ADVISORS

Currency Research

REPORT SERIES

PARTNER

ripple

## COMPANY DESCRIPTIONS

**Lipis Advisors** is an international consultancy focused exclusively on the payments industry. Based in Berlin, Germany, Lipis Advisors was founded in 2007 and has provided consulting services to clients in 100+ countries around the world, including financial institutions, investors, payment service providers, retailers, fintechs, payment schemes, payment system operators, technology vendors, industry associations, and regulators. In addition to this report, Lipis Advisors have long been recognized as thought-leaders in the field of payments and have authored numerous whitepapers over the past two decades that explore the changing payments landscape. To learn more, visit our website.

**Currency Research's** mission is to inspire and progress industry dialogue and efficiency across cash and payments through their core initiatives of Conferences, Consulting, Communication and Community. CR has successfully positioned itself as the leading global resource for central banks, their suppliers, and the related supply chain for currency and payment systems. CR has published a number of research-driven reports considered mandatory reading by the industry, publishes the monthly Central Bank Payment News, and provides consulting services with a focus on strategy and policy to central banks, regulators and commercial organizations. To learn more, visit our website.

## AUTHOR BIOS

**Bonni Brodsky** is a senior consultant at **Lipis Advisors** and has advised clients on a variety of topics in payments, including infrastructure modernization, real-time payment adoption, cross-border payments processing, and central bank digital currencies. Prior to joining Lipis Advisors, Bonni spent over five years as a Senior Trader and Markets Analyst at the Federal Reserve Bank of New York where she focused on monetary policy implementation and reference rate administration. She holds a Masters in International Economics from Johns Hopkins University and a BA in International Relations from Brown University.

**David Tercero-Lucas** is a consultant at **Lipis Advisors** and part of the research team on topics related to cryptocurrencies, stablecoins, cross-border payments, and Central Digital Currencies (CBDCs). He completed his PhD in Applied Economics at the Autonomous University of Barcelona, is a member of the Associate Team of the Digital Euro Association and his research has been published in different journals such as the Journal of Financial Stability and the European Journal of Political Economy. During his doctorate, he did an internship at the BIS and at the European Central Bank.

**Gonzalo Santamaria** is VP of Payments at **Currency Research** and has led the payments business stream since 2015. He has honed much of his leadership skills and industry knowledge within a realm spanning more than 36 years of technical, commercial and managerial experience in the currency and payments sectors. He forged much of his background first in the technical, and consequently in the commercial/ business development streams within world-class technology companies in the industry. During these tenures, he successfully assisted in designing and implementing state-of-the-art automated currency vault solutions, cash management re-engineering including commercial cash processing patents, and supply chain optimization solutions.

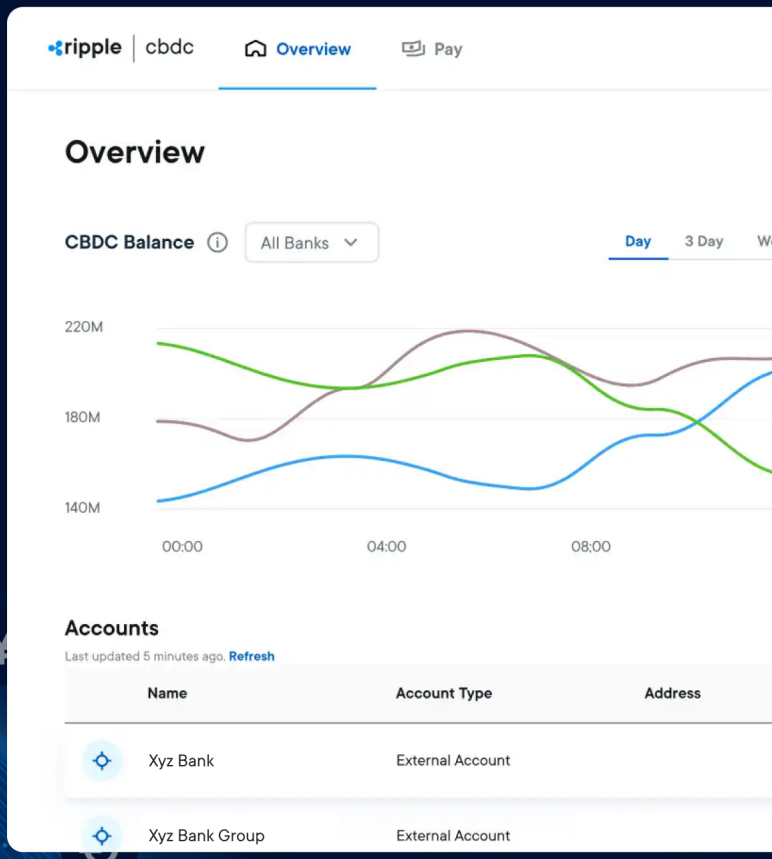
**Acknowledgments**

The authors would like to acknowledge Shiva Bissessar (Pinaka Consulting Ltd), Sonja Davidovic (BIS / MAS), Mary Hall (Ripple), Mehmet Kerse (CGAP / World Bank), Carlos León (FNA), Andrey Kocevski (WhisperCash), Javed Samuel (Pinaka Consulting Ltd) and Vasileios Theodosiadis (IBM) for their thoughtful contributions and insights.

Business impact, powered by digital currency

# We help companies around the world accelerate their business.

Ripple is a leader in enterprise blockchain technology offering a comprehensive platform for minting, managing, transacting, and redeeming Central Bank Digital Currencies (CBDCs). Ripple is currently engaged globally with Central Banks on CBDC projects.




With Ripple's CBDC Private Ledger, Central Banks can manage the CBDC lifecycle, offering these benefits:

- Stability, security, and resilience
- Easy access and financial Inclusion
- Interoperability with disparate payment systems and overlay services
- Low energy consumption to promote sustainability

### Royal Monetary Authority of Bhutan

Piloting retail, cross-border and wholesale payment use cases for a digital Ngultrum using Ripple's sustainable, interoperable solution.

### Republic of Palau

Developing strategies for cross-border payments and a USD-backed digital currency for Palau (which uses USD as its fiat) which could see the implementation of the world's first government-backed national stablecoin in the first half of 2022 on the XRPL.

ripple

Learn more about Ripple's solutions for Central Bank Digital Currencies, at Ripple.com

# PART 3: ENTERING THE NEXT PHASE OF CBDC EXPLORATION

## Introduction

Central banks today have increasingly shifted away from theoretical discussions of central bank digital currencies (CBDC) to real-world testing and experimentation. Roughly a dozen countries are already undergoing pilot programs, with an increasing number of countries likely to be added soon to that list.[1] In our last white paper, we analyzed the landscape of CBDC technology and infrastructure providers for central banks as they begin to launch Proof-of-Concepts or early pilot programs. We put forth a framework for differentiating among transaction networks/infrastructures, end-to-end solution providers, technology partners and research partners. We also presented a snapshot comparing the functionality and features across a sample full-stack CBDC solutions for central banks, laying out key areas of convergence (e.g., POS and mobile wallet support) and differentiation (e.g., type of ledger used) between available solutions.

But central banks are now entering a new and more advanced phase of CBDC exploration, which requires much more than choosing technology solutions and partners. It requires laying down the foundation for end-user adoption and developing an ecosystem that will fuel innovation and value-added services. In this paper, part III of our series on Central Bank Digital Currencies, we shed light on a series of questions that central banks must consider as they mature in their CBDC journey. We detail key lessons learned thus far, identify areas for additional experimentation, and provide a list of best practices for engaging with the existing payments ecosystem. We conclude with an examination of the innovations that may influence CBDC design and architecture choices in the future.

## What insights can central banks take away from CBDC exploration to date?

**There is no 'one-size fits all' design for CBDCs**. Looking at the diverse approaches to CBDC technology and design to date, there is no universal design for a CBDC. Some markets have focused on wholesale, retail, or both. Some central banks are leveraging conventional infrastructure like in Ghana, Jamaica, or Thailand, while others are basing their projects on distributed ledger technology (DLT) like in the Eastern Caribbean, Nigeria, and Sweden. Each central bank's mandate is also different, as is the public policy context. Moreover, cultural expectations around digital privacy differ greatly, which may drive decisions around programmable or offline CBDC. All in all, a clear takeaway for central banks and monetary authorities is that they must avoid emulating technology or design decisions made in other markets and focus on what will work best for their market.

**Establishing partnerships with private technology companies has been imperative to advancing CBDC exploration.** Most central banks and monetary authorities have relied extensively on public-private partnerships in exploring CBDC for their jurisdiction. External technology companies supply the back-end infrastructure and the required application stack necessary to mint and issue CBDC, as well as provide consulting and project management services to help central banks bridge gaps in their technical expertise. Many tech providers have developed CBDC test environments or sandboxes to help central banks build knowledge and gain insights into the supporting technology and how to best develop a business case. In the long term, however, this may be a potential conflict area if the central bank seeks to augment its capacity independently of the service provider.

[1] https://www.atlanticcouncil.org/cbdctracker/

It is incumbent on central banks to participate in CBDC research. However, it cannot be assumed that all central banks have ready access to technical resources and are familiar with advanced concepts under the CBDC banner e.g. aspects of distributed ledger technology, cryptography, etc. Establishing partnerships with private companies serves to increase the capacity of the monetary authority towards managing overall solution development and implementation." – Shiva Bissessar (Managing Director & Principal Consultant, Pinaka Consulting Ltd).

Non-traditional public-private research partnerships have also resulted in notable insights. For example, the Federal Reserve Bank of Boston (Boston Fed) and the Massachusetts Institute of Technology's Digital Currency Initiative (MIT DCI) have collaborated on an exploratory research project known as Project Hamilton, a multiyear initiative to explore the CBDC design space and gain a hands-on understanding of a CBDC's technical challenges and opportunities.[2] Through this collaboration, they have sought to help answer questions related to what kind of CBDC system can support the scale of national retail payments while being secure and resilient to security threats, what is the underlying CBDC protocol and who can access it, as well as others. Using open-source research software – dubbed OpenCBDC – they have been able to create a Proof-of-Concept for a core processing engine for a retail CBDC, based on two architectures, one of which demonstrated throughput of 1.7 million transactions per second. As an open-source project, all developers in the world can access the code and make contributions. The second phase of the project will explore alternative technical designs to improve privacy, resiliency, and functionality of the architectures outlined in the first phase.[3] The research insights that Project Hamilton has produced have already had meaningful implications and consequences for what technology options may be available to central banks globally.[4]

**While DLT-based CBDC has been successfully tested and even issued in a couple markets, further research around use of DLT for CBDC is needed.** For example, while many central banks and monetary authorities have experimented with issuing CBDC on distributed ledgers, these efforts have largely demonstrated the technical feasibility of issuing DLT-based CBDC. More work is still needed to assess the potential benefits and costs of using DLT-based infrastructure over conventional infrastructure in a production scenario. This is particularly important in identifying scalability constraints and minimizing resource consumption, as well as assessing operational complexity and risks.[5] Moreover, investigation into interoperability arrangements between different DLT-based platforms has thus far been relatively limited.

[2] https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx

[3] Ibid.

[4] Building on the success of its partnership with the Boston Fed, MIT also recently partnered with the Bank of England and Bank of Canada to embark upon on a twelve-month research project on CBDC to examine the opportunities, risks and technical challenges related to design of a CBDC.

[5] https://www.bis.org/fsi/publ/insights41.pdf

## What areas should central banks explore further as part of the next stage of CBDC development?

**Offline payments.** An offline payment is a digital transaction that does not require internet connectivity. Offline payments have become an important design requirement for CBDC not only in emerging markets with less reliable internet access, but also in advanced economies that seek to emulate properties of cash. Indeed, the importance of enabling consumers to use CBDCs while not connected to the internet has been widely acknowledged by the Bank for International Settlements (BIS) and other organizations. Allowing for offline CBDC requires the operation of parallel infrastructure, an online ledger as well as offline infrastructure, which consists of offline wallets, or hardware bearer instruments that will rely on tamper-resistant hardware to maintain integrity. Hardware bearer instruments must be issued on tamper-resistant chips (e.g. Secure Elements, or SEs) to prevent counterfeiting and double-spending. Hardware bearer instruments communicate with each other, typically using near-field communication (NFC) technology.

Many Central Banks in developing countries cannot rely on internet and smartphone access and hence CBDCs solely in the form of Distributed Ledger Technology would be deemed unusable in those areas. Therefore, Hardware Bearer Instruments fill the gaps where Distributed Ledger Technology falls short." – Andrey Kocevski (Cofounder of WhisperCash).

Offline payments have yet to be successfully implemented in any live CBDC or advanced pilot project due to challenging questions around implementation.[6] They inherently introduce challenges for CBDC design such as avoiding double spending and forging, the possibility of loss of funds if the device is damaged and the risk of non-repudiation, which applies to those situations when company that receive the CBDC insists that they did not receive it or it is fake. Another challenge is that the number of specialist firms in this space is still limited.[7] The supply chain of devices containing SEs, and the legal framework allowing the private sector to participate in the system are also challenges to consider for central banks. For example, some mobile phone manufacturers include SEs in their phones, but they keep tight control of fabrication and external software access.

Examples of active experimentation in this area include the Bank of Ghana, which is testing an offline CBDC platform based on a contactless smart stored-value card.[8] The People's Bank of China has been experimenting with "delayed offline single-hop transactions." A person can use the e-CNY to pay offline only once, and the payer and receiver need to synchronize online until they can pay/receive again. Nonetheless, this solution is far from being a pure offline CBDC solution. Further experimentation is required however to determine how to best manage the interface between the online and offline systems and how to manage risks relevant to insufficient funds or fraudulent payments.

[6] The D-cash and the e-Naira cannot be used offline (see https://www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central- Bank-Digital-Currency-512174).

[7] Examples of specialist providers in this area include Crunchfish, G+D, WhisperCash, and others.

[8] https://www.gna.org.gh/1.21489378

**Benefits and risks around programmability.** There has been significant industry hype regarding the benefits of programmability for digital currencies and assets, but programmable CBDC and relevant use cases have yet to be fully explored. Programmable CBDC would be endowed with inherent logic to limit its use. For example, CBDC could be programmed to expire after a fixed date, or its use restricted to a certain set of goods or services. A programmable CBDC could also have social purposes, be employed to deploy rapid and effective resources to low-income citizens or refugees or be used as a disaster management tool to release funds automatically to affected citizens. China is the only major market that has tested programmable CBDC in a real-world setting. Its e-CNY could only be spent on public transportation (subway and bus tickets) and shared bike services.[9] But a CBDC with such restrictions clearly has risks, such as limiting adoption. It also raises questions about anonymity and privacy of CBDC users and the role of central banks in strictly controlling how money can be spent. Central banks need to put additional resources as exploring these issues is required.

Alternatively, CBDC could also be used to catalyze greater usage of programmable payments, or payments that are automatically executed if certain conditions are met.[10] Although programmable payments already exist today in a broad sense (e.g. direct debits), programmable payments in a CBDC context can be enabled via DLT-based smart contracts or through the use of APIs. There may be several compelling use cases for central banks to explore. For instance, central banks or tech providers may be able to develop fully automated payments initiated by a device based on predefined conditions (e.g. machine-to-machine payments). Another use case is the so-called "digital payment-on-delivery", a payment instantly executed when there is confirmation that the product, good or service has been delivered or provided.

**How to leverage the cloud.** The benefits of leveraging cloud-based infrastructure in payments and financial services have been well-researched. Systems housed in the cloud can be deployed much faster than on-premise infrastructures, are highly available and resilient, and are almost infinitely scalable platforms.[11] Stakeholders may want to create a more decentralized setting where organizations such as financial companies actively participate and may be able to keep copies of ledgers. Given these benefits, some central banks should consider how the cloud can be used to achieve the highest levels of availability and resiliency for CBDC, such as mitigating potential service disruptions resulting from denial of service (DOS) attacks or natural disasters.[12] But further exploration of the benefits and risks of hosting CBDC applications in the cloud is required. For example, implications for data ownership and privacy must be evaluated as well as regulatory frameworks for cloud providers in financial services.[13] Another relevant concern is that some cloud providers only have data centers in a select number of countries.

**Cross-border interoperability.** Work from the BIS and other public sector organizations has stressed the importance of developing CBDC that is interoperable with other CBDC systems as part of global efforts to improve cross-border payments. There has been some exploration into the various models for CBDC interoperability (e.g. compatible CBDC systems, interlinked CBDC systems, and a single system for CBDC where multiple CBDCs have been integrated), but more real-world experimentation is required to determine their respective strengths and weaknesses.[14] Examples of the latter are the BIS' Inthanon-LionRock project[15] Bank of Thailand and Hong Kong Monetary Authority, and the mCBDC Bridge initiative[16]

---

[9] https://www.theblock.co/post/110377/china-digital-yuan-test-programmable-chengdu

[10] Programmable payments exist in the current financial system (e.g., standing orders or direct debits).

[11] https://www.weforum.org/agenda/2021/04/how-businesses-can-realize-the-benefits-of-the-cloud/

[12] This is especially important for fragile states that are vulnerable to natural disasters (see http://www3.compareyourcountry.org/states-of-fragility/overview/0/).

[13] A small but growing group of central banks is exploring use of cloud. One example is Israel, which set up a DLT infrastructure on the Microsoft Azure cloud for its digital shekel. In the second stage of the experiment, a VMware blockchain infrastructure was established in an AWS cloud. The Federal Reserve Bank of Boston and the MIT – in Project Hamilton, also deployed its codebase in AWS.

[14] https://www.bis.org/publ/bppdf/bispap115.pdf

[15] https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf

[16] https://www.bis.org/publ/othp40.pdf

(also known as mBridge), run by the BIS Innovation Hub in partnership with several other central banks. Greater experimentation from the private sector is also necessary, as it has been limited to date. SWIFT proved to succeed enabling a cross-border transaction between two entities on a RTGS system and a DLT-based CBDC system.[17] Recently SWIFT, partnering with Capgemini, launched a new series of CBDC interoperability experiments.[18]

## How can central banks best engage the existing payments ecosystem?

In addition to the areas identified above, entering more advanced stages of CBDC exploration requires deeper forms of engagement with the existing ecosystem, which can play an important role in solving technical bottlenecks, setting standards, exploring new use cases, and laying the foundation for an ecosystem of services. Looking at the current landscape, CBDC experiments can be classified into three groups when it comes to their engagement with the private sector:

- **Low engagement.** Technology providers and consultancies are the only external players involved in the CBDC project. They provide distinct services within the value chain, helping to define design requirements, sourcing the CBDC technology and implementing the solution in a test environment. This level of engagement is typical of early stage CBDC projects.
- **Medium engagement.** Some financial institutions and other potential intermediaries are allowed access to the CBDC network. They play the role of testing the infrastructure and interoperability with their internal IT systems to identify problems or issues. The Swedish Riksbank was one of the first central banks to involve external participants in the second phase of its e-krona project.[19] Other examples of markets that have reached this level of engagement include South Africa and South Korea. An increasing number of CBDC projects are moving toward this level of engagement.
- **High engagement.** With a high level of private sector engagement, the central bank allows not only selected intermediaries, but also a broader group of stakeholders such as a group of merchants and consumers to access, use and transact in CBDC. There are already several CBDC pilots that have reached this level of engagement. For example, in China, some commercial banks and online banks may distribute the e-CNY, which can be used by selected merchants (for example, JD.com allowed customers to purchase items with the e-CNY and they pay the salary to their employees[20]) and select individuals. In the digital Ruble pilot, 12 Russian banks have been testing C2C transactions, B2B transactions, and B2G transactions, and particular clients were also able to exchange non-cash rubles in their accounts for digital ones.[21] From late-2022 to mid-2023, Thailand will allow its CBDC to be used by 10,000 retail users and three companies within limited areas.[22]

[17] https://www.swift.com/news-events/news/exploring-central-bank-digital-currencies-swift-and-accenture-publish-joint-paper

[18] Swift and Capgemini are exploring ways to interlink domestic-based CBDCs with existing payment infrastructures regardless of the technology employed in the CBDC (see https://www.ledgerinsights.com/swift-in-cross-border-cbdc-interoperability-trial-with-cap-gemini/).

[19] During the second phase of the e-krona project, for example, Handelsbanken and Tietoevry participated in the e-krona network to test the Corda-based CBDC solution.

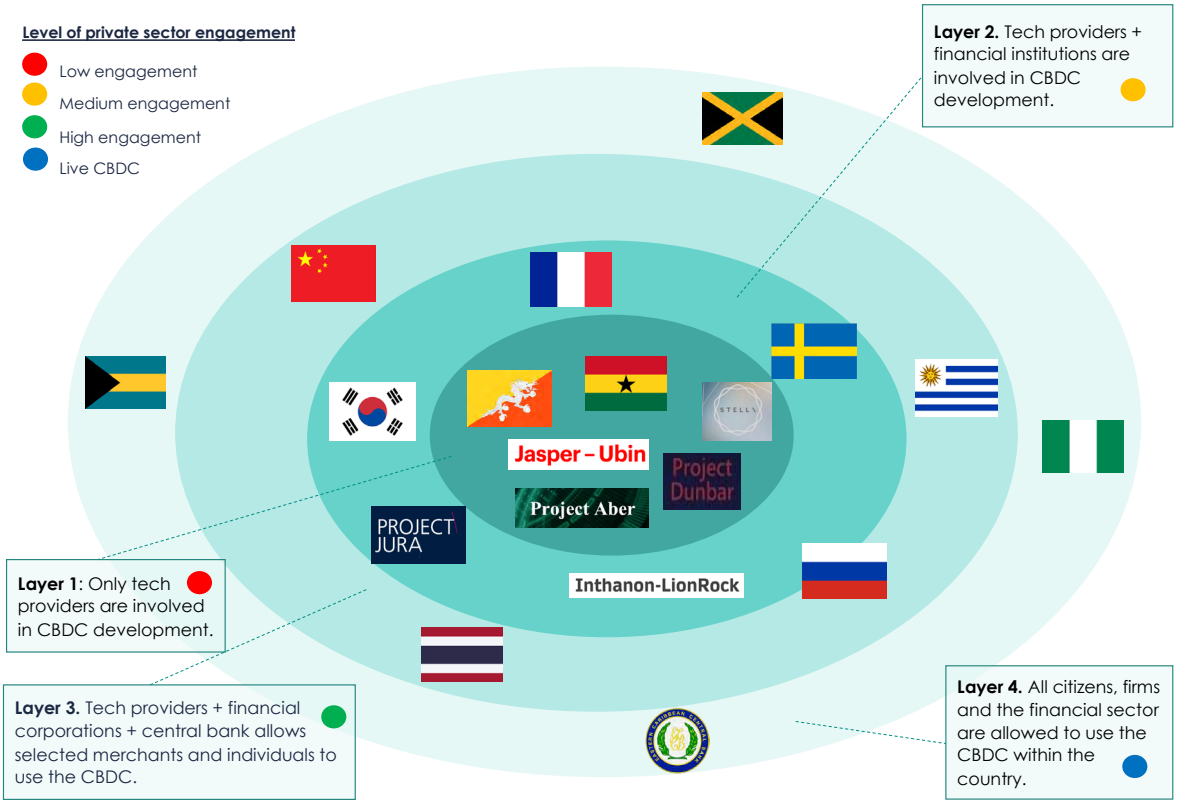
[20] https://www.cnbc.com/2021/04/27/chinas-digital-currency-used-by-jdcom-to-pay-some-employees.html

[21] https://www.cbr.ru/eng/press/event/?id=12692

[22] https://www.bot.or.th/English/PressandSpeeches/Press/2022/Pages/n3965.aspx

The below figure shows the CBDC projects categorized according to the above classification.

**Degree to which the private sector is currently involved in CBDC projects**




Note: Pilots that have already concluded (e.g., Uruguay) are also included. Recently, The Republic of Palau has partnered Ripple to develop their own digital currency. However, it cannot be considered a "traditional" CBDC because they do not have an official currency or a central bank. The Royal Monetary Authority of Bhutan is also working with Ripple on a CBDC pilot.

The speed with which CBDC pilots can move from one level of engagement to another will depend on central bank's goals and its priorities, the urgency of meeting its goals, and how easy it is to accomplish them. Advancements of tech providers in the space are making it increasingly easy to deploy applications and set up CBDC pilots with the private sector, allowing for more rapid engagement through these various layers. Figure updated as 2022 Q2.

## *Channels for market engagement*

**External advisory groups.** Some central banks have created advisory groups or committees with the purpose of analyzing and making recommendations about the design, distribution, and impact on CBDCs. For example, the ECB has created the Digital Euro Market Advisory Group composed by a large group of individuals that represent the euro area's payments ecosystem. The Bank of England and HM Treasury announced in 2021 the membership of two different advisory groups: the CBDC Engagement Forum and the CBDC and Technology Forum. Putting together senior stakeholders from industry, civil society and academia, the aim of the Engagement Forum consists of gathering strategic information on policy considerations and functional requirements related to a hypothetical digital pound. The CBDC Technology Forum engages stakeholders and focuses on all technology aspects of CBDC. In the private sphere, the Digital Dollar Project – lead by a non-profitable foundation named Digital Dollar Foundation - announced a 22 member advisory group[23] that will help set up the framework for establishing a U.S. CBDC.[24]

[23] https://digitaldollarproject.org/advisory-group/

[24] They recently announced the launch of its Technical Sandbox Program – made up by several technology providers such as Ripple - to jumpstart further exploration of technical implementations of a U.S. CBDC.

Through these channels of engagement, central banks have already started to identify and prioritize relevant use cases of their CBDCs that may drive market adoption. The Reserve Bank of Australia, for example, will work with the Digital Finance Cooperative Research Centre to research and explore use cases for a CBDC in the country. The ECB's Digital Euro Market Advisory Group was tasked with identifying four main use cases for the first phase of a possible digital euro: person-to-person, payments for goods or services purchased (consumer-to-business), payments between two businesses or from a business to an individual (business-initiated), and payments to the government. They argued that use cases must support the main objectives of the CBDC and target market segments that can lead to network effects.[25] The economic literature has stressed that new payment mechanisms see greater adoption in one-sided markets (e.g., person-to-person or business-to-business).[26]

**Hackathons.** In the recent years, central banks have sponsored competitions or 'hackathons' in the CBDC sphere. A hackathon is usually presented as a chance for young and mature enterprises to showcase their potential and bring innovative and applicable solutions related to an unsolved problem as well as increase public awareness. They are an opportunity to encourage new open standards, uncover new solutions and firms, and provide synergies among participants. Examples of central bank hackathons include the G20 TechSprint hackathon – organized by the Central Bank of Indonesia and BIS with the aim of building effective and robust means to distribute and transfer CBDCs providing solutions to enable financial inclusion, and improving connectivity and interoperability[27]; the eNaira Hackathon enabled by the central bank of Nigeria focusing on issues related to financial inclusion, SMEs growth, innovation and entrepreneurship and facilitation of cross border trades and transfers as well as international remittances and FX exchanges[28]; the Bank of Thailand Hackathon whose purpose is presenting business use cases for retail CBDC[29], and the Central Bank of Brazil's LIFT challenge, that aims to evaluate use cases of a digital real.[30]

Central banks can take cues from private sector actors, who have also initiated similar types of events. Examples of private hackathons are Ripple's CBDC Innovate, which had the aim of promoting the development of applications for financial inclusion, interoperability & retail CBDCs[31]; and the Barclays CBDC Hackathon 2022, which had the purpose of providing a solution to be able to connect to a Barclays simulation of both a central bank and commercial banks.[32]

**API sandboxes.** Offering API access to payment service providers and other non-bank players can maximize inclusion, improve interoperability, and foster competition for customer-centric services, which are all extremely important in CBDC adoption. However, many central banks do not have the resources or technology to develop API portals or sandboxes. Hence, they may partner with banks and technological firms to create APIs. Private operators are already providing CBDC APIs that central banks may use, including Mastercard.[33] In their case, the CBDC APIs allow for the seamless on-boarding of financial entities.

---

[25] https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220504_usecase.en.pdf

[26] https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.467&rep=rep1&type=pdf

[27] https://www.bis.org/press/p220425.htm

[28] https://leadership.ng/cbn-enaira-hackathon-deepening-payment-system-boosting-digital-economy/

[29] https://www.bot.or.th/English/PressandSpeeches/Press/2022/Pages/n3965.aspx

[30] https://www.bcb.gov.br/en/pressdetail/2433/nota

[31] Ripple's CBDC Innovate Hackathon just completed Phase I of the challenge. In 90 days, CBDC Innovate ended with 481 entrants, 44 submissions and 14 finalists. The sheer number of participants demonstrates that CBDC applications are coming of age and that developers are eager to develop digital currencies. https://ripplecbdc.devpost.com/

[32] https://thefintechtimes.com/barclays-rise-hackathon-to-test-the-full-capabilities-of-retail-and-wholesale-cbdcs/

[33] https://developer.mastercard.com/cbdc/documentation/

**Marketing campaigns.** Central banks do not only have to develop and design their own CBDCs, but they must also make plans for getting their citizens to use them once they are minted. Consequently, some monetary authorities are now implementing marketing plans to increase citizens usage of their live CBDCs. Central banks must also make sure their country's infrastructure and internet access is reinforced so that citizens can have consistent access to digital wallets and mobiles apps to enable virtually 24/7 access.

## Taking a longer-term view, what innovations should central banks monitor as CBDC exploration advances?

CBDC technology is evolving rapidly, with advances in the crypto technology and digital money worlds having the potential to directly influence CBDC policy and design choices in the future. In this last section, we detail a few of these innovations and their potential impact on the future of CBDC design.

**Zero Knowledge Proofs (ZKPs).** ZKPs are a type of privacy-enhancing cryptographic technique that has received considerable attention in recent years. ZKPs are implemented to secure the integrity of payments by ensuring a high level of privacy for the user and avoiding double-spending. ZKPs have been mainly adopted in the context of privacy-oriented blockchains. For instance, Zcash allows fully private transactions built on zero-knowledge proofs.[34]

ZKPs tend to have a high degree of complexity and limited scalability. For example, participants in the BIS' Project Aber ruled out use of ZKPs for validation due to being so computationally expensive.[35] ZKPs also tend to involve computational overhead for users that is slower than regular transactions.[36] As ZKPs remain areas of active research, however, it may be the case that they could be used in CBDC projects in the future and offer a new degree of flexibility for central banks to balance user privacy with KYC/AML considerations. There are already some proposals that provide high scalability, untraceable transactions, and privacy-preserving regulation mechanisms.[37] In the digital shekel project, the central bank of Israel is experimenting with the use of ZKPs to preserve a high degree of privacy for CBDC transactions. Setting up a VMware blockchain infrastructure in a public cloud – AWS – that supports ZKP technologies for limited privacy, they concluded that it was difficult to use encryption keys in a distributed architecture, though they will continue to experiment with other mechanisms involving ZKPs.

**Connecting to private digital asset ecosystems.** It may be the case that some central banks want to explore connecting to some private digital asset ecosystems that have been developing. Permissioned blockchains used by central banks in their CBDC projects can be connected to permissionless blockchains through oracles. Oracles are third-party services enabling blockchain smart contracts to access instant real-world data. The oracle allows the smart contract the ability to access a live feed of information that is external to the blockchain. In the future, it is possible that oracles could be used as a bridge to DeFi, though a greater exploration of the risks and technical challenges is needed.

**Use of satellite communication to improve resiliency and access of CBDC infrastructure.** As technology using satellite communication has evolved, it has also become more affordable and accessible. As such, it may lead to new avenues for governments and central banks to explore improving digital infrastructure in rural areas, or where internet access is unreliable or limited. In the future, this could be game-changing in terms of ensuring access and resiliency.

---

[34] https://z.cash/technology/zksnarks/

[35] https://www.centralbank.ae/sites/default/files/2020-11/Aber%20Report%202020%20-%20EN_4.pdf

[36] https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/?utm_source=jerrybrito&utm_medium=email&utm_campaign=stablecoin-follow-up-plus-occ-guidance-central

[37] See https://eprint.iacr.org/2021/1443.pdf.

**Implement digital identity systems for CBDCs.** Digital identity systems are used to validate, storage and transfer identify data as well as allow identity verification and authentication. As a kind of electronic KYC systems, central banks may use them to help customer onboarding and customer due diligence. These methods may support the access to and adoption of CBDC since they can also be used for stronger in-person (and offline) authentication.

## Conclusion

To conclude, there are numerous issues that central bankers must weigh as they embark upon the next phase of CBDC exploration. It is imperative that central banks continue to experiment with aspects of CBDC like programmable and offline payments given that this is largely terra nova, and the technical and policy challenges are significant. It is important that central banks apply best practices for private sector engagement to lay down the groundwork for a successful adoption and usage of CBDC by end-users in the future. It is also necessary to continue monitoring developments and innovations in the space, as they could quickly change the CBDC conversation and directly influence CBDC policy and design options in the not-so-distant future.

**Advancements in quantum computing**. Another innovation for central banks to monitor that may impact not only the world of cryptography – and therefore CBDCs – but also other sectors is quantum computing. Calculations made by quantum computing follow the laws of quantum mechanics. This will overcome the conventional computing' binary bits, which can only consider two positions: zero or one. Quantum computing has the capacity to cope with extremely big and disordered data sets, at high speeds. However, quantum computers may compromise major data encryption methodologies and all the cryptographic primitives used for protecting all the features of data stored, i.e., access, integrity and confidentially. The current degree of sophistication of cryptography employed to secure CBDC accounts cannot prevent quantum-based hackers from disrupting the system, even without being detected. There are already competitions to encourage firms to develop quantum-resistant public-key cryptographic algorithms, such as the ongoing NIST Post-Quantum Cryptography contest.[38]

Our final message to central bankers: to move further along in the space, you must do much more than just investigate technology options. It is crucial that you engage private sector actors to lay the foundation for a business case that will incentivize usage and the development of an ecosystem. Along these lines, the need for independent consulting expertise cannot be overstated. It is related to the principles of good governance, transparency, and independent assessment. Failure to engage independent parties could result in poor design choices that limited adoption, ultimately hampering your ability to achieve policy goals.

[38] https://csrc.nist.gov/Projects/post-quantum-cryptography