International Telecommunication Union

DIGITAL CURRENCY GLOBAL INITIATIVE

TELECOMMUNICATION
STANDARDIZATION SECTOR

(01/2025)

Central Bank Digital Currency Reference Architecture

Report of CBDC Workstream of Architecture, Interoperability Requirements and Use Cases Working Group (AIRU)

DISCLAIMER

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of Digital Currency Global Initiative (DCGI) partners, including the International Telecommunication Union (ITU), or Stanford University. The mention of specific companies, or of certain manufacturers' products does not imply that they are endorsed nor recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters. The DCGI partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the DCGI partners concerning the legal status of any country, territory, city, or area or of its authorities or the endorsement or acceptance of such boundaries.

About this report

This document is the output of the Architecture Working Group of the Digital Currency Global Initiative.

The report was prepared by John Kiff, Jacques Francoeur, Stephen Phillips, Marc Liberati, and Vinay Mohan, with input from members of the Architecture Working Group of the Digital Currency Global Initiative.

The report also benefited from comments from Arvinder Bharath, Vipin Bharathan, Victor Budau, Lars Hupel, Samuel Kamau, Chris Kameir, Tom Kudrycki, Patrick McConnell, Benjamin Muller, Alex Nikolov, Herve Tourpe, and Nicolas Zhang.

Abstract

This technical report aims to improve the development of a central bank digital currency (CBDC) reference architecture that can standardize how different CBDCs can be evaluated and compared. The report was derived from the ITU (2024b) digital currency ontological work and is organized around the Budau and Tourpe (2024) "ASAP" model that describes digital asset systems in terms of four functional layers - access, service, asset, and platform. The resulting reference architecture is based on, and informed by, recent CBDC launches, pilots and proofs of concept (i.e., it does not consider prospective future architectures).

Keywords

central bank digital currency, CBDC, reference architecture, retail CBDC, wholesale CBDC

Editor: John Kiff
Lead of CBDC Workstream of DCGI AIRU WG
Independent Consultant
United States of America
Email: kiffmeister@gmail.com

Table of Contents

DCGI Technical Report: Central Bank Digital Currency Reference Architecture

1 Scope

The scope of this technical report is to develop a central bank digital currency (CBDC) reference architecture that standardizes how different CBDC's can be evaluated and compared, and test fit it to seven currently launched and piloted CBDCs.[1] In this report, a CBDC is a digital payment instrument, denominated in the national unit of account, that is issued by and a direct liability of the central bank (BIS, 2020a).[2] It can be designed for use among financial intermediaries only ("wholesale") or by the wider economy ("general-purpose" or "retail").[3] The reference architecture will define the process components and life cycle management processes required to implement CBDCs, covering issuance, distribution, exchange, system interaction and user interfaces, use cases, user interfaces (e.g., "wallets"), and identify areas where technical standards are needed (Table 1).

Table 1: CBDC Reference Architecture Components

Operating Model: What are the key responsibilities in the CBDC ecosystem and who is responsible for what? What roles do intermediaries play? Are they compensated (e.g., by charging transaction fees)?			
Key Management: How does central bank and other CBDC stakeholders/roles ensure the confidentiality, integrity, and availability of cryptographic keys?			
From Production to Distribution to Transferring			
Platform Layer CBDC production, transfers and record-keeping: - Platform technology (core ledger attributes (balance- v provenance-based), centralized v distributed access and governance) - Privacy (who sees what?)	**Asset Layer** Core functions and constitutive attributes: - Unit characteristics (entry- v object-based, remuneration, unique unit identifiers, denominations, programmability) - Production characteristics (authorization, governance and isolation) - Supply release and removal - Unit rights (usage/holding limits and fungibility)	**Service Layer** Functions that utilize the CBDC to facilitate financial services implementation: - Programmable payments?	**Access Layer** Functions and interfaces that enable clients such as users, applications, and other market components, to engage with the underlying service, asset, and platform infrastructure layers: - Online wallets - Offline wallets - Holding/transaction limits
Interoperability: How does the CBDC interact with other digital assets and liabilities?			

The end goals of this reference architecture and the ITU (2024b) digital currency ontological work, are very similar. An ontology is a formal and explicit representation of concepts and their relationships in a particular domain, CBDCs in this case. An ontology must be complete by design, so there can only be one ontology representing a given domain scope that covers "all matters" in that domain. For example, a CBDC ontology must cover all characteristics (or "distinctions") of all CBDC types. The implication of an ontology is that only one can exist for a given scope, so that all types can be generated by the same ontology simply by selecting different distinctions. Change the value of

[1] See Tourpe et al. (2023) for an explanation of what distinguishes the five typical phases of CBDC product development (preparation, proof-of-concept, prototype, pilot, and production (launch)).

[2] Also, according to BIS (2020a) a liability issued by a central bank that is not in its own currency (i.e., where it does not have monetary authority) is not a CBDC.

[3] This paper focuses on CBDC issued by, and a direct liability of, the central bank, as opposed to "synthetic" CBDC which is privately-issued digital money backed by central bank reserves, regulated, and supervised by the central bank (Adrian and Mancini-Griffoli, 2019).

one distinction and the outcome is a different instantiation. (See Annex 1 for more on the ontological approach).

2 References

Adrian, T., and T. Mancini-Griffoli. 2019. "The Rise of Digital Money," IMF Fintech Note 19/01.

Agur, I, J. Deodoro, X. Lavayssière, S. Martinez Peria, D. Sandri, H. Tourpe, and G. Villegas-Bauer. 2022. "Digital Currencies and Energy Consumption," IMF Fintech Note 2022/006, June.

Alliance for Financial Inclusion. 2022. "Central Bank Digital Currency – An Opportunity for Financial Inclusion in Developing and Emerging Economies?"

Auer, R., B. Haslhofer, S. Kitzler, P. Saggese and F. Victor. 2023. "The Technology of Decentralized Finance (DeFi)," Bank for International Settlements Working Papers No 1066, January

Amazon Web Services and Oliver Wyman Forum (AWS-OWF). 2022. "Retail Central Bank Digital Currency: From Vision to Design."

Armelius, H., G. Guibourg, S. Johansson and J. Schmalholz. 2020. "E-krona Design Models: Pros, Cons and Trade-Offs," Sveriges Riksbank *Economic Review*, June.

Athanassiou, P.L. 2021. "Wholesale Central Bank Digital Currencies: An Overview of Recent Central Bank Initiatives and Lessons Learned," in European Central Bank (ECB). 2021. "European System of Central Banks (ESCB) Legal Conference 2020."

Auer, R., and R. Boehme. 2020. "The Technology of Retail Central Bank Digital Currency," BIS Quarterly Review, March 1.

----. 2021. "Central Bank Digital Currency: The Quest for Minimally Invasive Technology," Bank for International Settlements Working Paper No. 948.

Auer, R. H. Banka, N.Y. Boakye-Adjei, A. Faragallah, J. Frost, H. Natarajan and J. Prenio. 2022. "Central Bank Digital Currencies: A New Tool in the Financial Inclusion Toolkit? BIS FSI Insights No. 41, April 12.

Auer, R., B. Haslhofer, S. Kitzler, P. Saggese and F. Victor. 2023. "The Technology of Decentralized Finance (DeFi)," BIS Working Paper No. 1066, January 19.

Bains, P. 2022. "Blockchain Consensus Mechanisms: A Primer for Supervisors," IMF Fintech Note 2022/003, January.

Bank of Canada. 2017a. "Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement," White paper prepared by Payments Canada, Bank of Canada and R3.

----. 2018. "Jasper Phase III: Securities Settlement Using Distributed Ledger Technology."

Bank of Canada and Monetary Authority of Singapore (BoC/MAS). 2019. "How Do Hashed Time-Locked Contracts (HTLC) for Cross-Border Payments Work?" Annex to "Central Banks of Canada and Singapore Conduct Successful Experiment for Cross-Border Payments Using Distributed Ledger Technology," Joint Press Release, May 2.

Bank of England. 2020. "Central Bank Digital Currency: Opportunities, Challenges and Design," Discussion Paper, March 12.

----. 2023. "The Digital Pound: Technology Working Paper," February 7.

Banque de France. 2023. "Wholesale Central Bank Digital Currency Experiments with the Banque de France," July.

Bank for International Settlements (BIS). 1997. "Real-Time Gross Settlement Systems," Report prepared by the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries.

----. 2012. "Principles for Financial Market Infrastructures," Committee on Payments and Market Infrastructures, April.

----. 2020a. "Central Bank Digital Currencies: Foundational Principles and Core Features," Joint report by The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements, October.

----. 2020b. "Project Helvetia Phase I: Settling Tokenized Assets in Central Bank Money," BIS Innovation Hub, December.

----. 2021a. "CBDCs: An Opportunity for the Monetary System," BIS Annual Report, June.

----. 2021b. "Central Bank Digital Currencies: System Design and Interoperability," Joint report by The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements, September.

----. 2022a. "Project Helvetia Phase II: Settling Tokenised Assets in Wholesale CBDC," BIS Innovation Hub, January.

----. 2022b. "The Future Monetary System," BIS 2022 Annual Report, June.

----. 2023a. "A Handbook for Offline Payments with CBDC," BIS Innovation Hub, May.

BIS. 2023b. "Project Rosalind: Building API Prototypes for Retail CBDC Ecosystem Innovation," BIS Innovation Hub, June.

----. 2023c. "Blueprint for the Future Monetary System: improving the Old, Enabling the New," Chapter III of the BIS 2023 Annual Economic Report, June 20.

----. 2023d . "A High-Level Design Guide for Offline Payment," BIS Innovation Hub, October.

----. 2023e . "Project mBridge: Experimenting with a Multi-CBDC Platform for Cross-Border Payments," BIS Innovation Hub, October.

----. 2023f . "High-level technical requirements for a functional central bank digital currency (CBDC) architecture," Report by the Consultative Group on Innovation and the Digital Economy (CGIDE) established at the BIS Representative Office for the Americas, December.

BIS, Committee for Payments and Market Infrastructures, International Monetary Fund, and World Bank Group (BIS-CPMI-IMF-WBG). 2021. "Central Bank Digital Currencies for Cross-Border Payments," July 9.

----. 2022. "Options for Access to and Interoperability of CBDCs for Cross-Border Payments – Report to the G20," July.

----. 2023. "Exploring Multilateral Platforms for Cross-Border Payments," January.

Baqer, K., R. Anderson, L. Mutegi, J.A. Payne, and J. Sevilla. 2017. "DigiTally: Piloting Offline Payments for Phones," Thirteenth Symposium on Usable Privacy and Security, Santa Clara, CA, July 12-14.

Beck, R., C. Müller-Bloch, and J.L King. 2018. "Governance in the Blockchain Economy: A Framework and Research Agenda," Journal of the Association for Information Systems, Vol 19, No. 10.

Bindseil, U. 2020. "Tiered CBDC and the Financial System." European Central Bank Working Paper No. 2351, ECB, Frankfurt, Germany.

Bindseil, U., F. Panetta, and I. Terol. 2021. "Central Bank Digital Currency: Functional Scope, Pricing and Controls," European Central Bank Occasional Paper No. 286, December.

Budau, V., and H. Tourpe. 2024. "ASAP: A Conceptual Model for Digital Asset Platforms," IMF Working Paper No. 2024/019, February.

Buterin, V. 2014. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform."

Chaum, D., and T. Moser. 2022. "eCash 2.0: Inalienably Private and Quantum-Resistant to Counterfeiting." Unpublished.

Committee on Payments and Market Infrastructures (CPMI). 2017. Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework, Bank for International Settlements, February.

Dixon, C. 2024. *Read Write Own: Building the Next Era of the Internet*. Random House.

European Central Bank (ECB). 2022. "Digital Euro Privacy Options."

—-. ECB. 2024 . "Second Update on the Work of the Digital Euro Scheme's Rulebook Development Group," January 3.[4]

Flodén, M., and B. Segendorf. 2021. "The Role of Central Banks When Cash is no Longer King: Perspectives from Sweden," in Niepelt, D. 2021. Central Bank Digital Currency Considerations, Projects, Outlook, Centre for Economic Policy Research (CEPR), November.

Garratt, R., M. Lee, B. Malone, and A. Martin. 2020. "Token- or Account-Based? A Digital Currency Can Be Both," New York Federal Reserve Bank Liberty Street Economics, August.

Gross, J., J. Sedlmeir, and S. Seiter. 2022. "How to Design a Compliant, Privacy-Preserving Fiat Stablecoin via Zero-Knowledge Proofs." Etonec (blog), December 15.

He, D. 2018. "Monetary Policy in the Digital Age." *Finance and Development* 55 (2).

Holbrook, J. 2020. *Architecting Enterprise Blockchain Solutions*, John Wiley & Sons.

Hupel, L. 2023. "Interoperability Aspects of CBDC Across Ecosystems and Borders," *Journal of Payments Strategy & Systems*, Vol. 17, No. 4.

----. 2024a. "Secure Wallets for CBDC: How Do They Work?" *The Paypers*, February 6.

----. 2024b. "Why Accounts Do Not Solve Double-Spending," *The Paypers*, March 13.

Infante, S., K. Kim, A. Orlik, A.F. Silva, R.J. Tetlow. 2023. "Retail Central Bank Digital Currencies: Implications for Banking and Financial Stability," U.S. Federal Reserve Board Finance and Economics Discussion Series 2023-072, November.

International Organization for Standardization (ISO). 2015. "Information technology — Vocabulary."

International Telecommunications Union (ITU). 2017. Digital Financial Services (DFS) Glossary. ITU-T Focus Group Digital Financial Services Focus Group Technical Report, January.

----. 2019. Taxonomy and Definition of Terms for Digital Fiat Currency. ITU-T Focus Group Digital Currency including Digital Fiat Currency, Reference Architecture Working Group Deliverable, June.

----. 2024a. "ITU and Linux Foundation join forces to create OpenWallet Forum," May 30.

---- . 2024b. "Digital Currency Ontology," Digital Currency Global Initiative, Architecture, Interoperability Requirements and Use Cases (AIRU) Working Group, August.

Kahn, C. M. and W. Roberds. 2009. "Why Pay? An Introduction to Payments Economics," *Journal of Financial Intermediation*, 18 (1).

[4] For rulebook updates see: https://www.ecb.europa.eu/paym/digital_euro/governance/html/index.en.html

Kiff, J. 2023. "Offline Digital Currency Technical Considerations," *Central Bank Payment News*, April 20.

Kiff, J., J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H.K. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. 2020. "A Survey of Research on Retail Central Bank Digital Currency." IMF Working Paper 20/104, June.

Levitin, A.J. 2018. "Pandora's Digital Box: The Promise and Perils of Digital Wallets," University of Pennsylvania Law Review, Vol. 166, No.2., p.p. 305-376.

Lipton, A. and A. Treccani. 2022. *Blockchain and Distributed Ledgers: Mathematics, Technology, and Economics*, World Scientific Publishing Company.

Liu, Y., F. Rivadeneyra, E. Reshidi, O. Shcherbakov, A. Stenzel. 2024. "Ecosystem Models for a Central Bank Digital Currency: Analysis Framework and Potential Models," Staff Discussion Paper 2024-13, September.

Lovejoy, J., A. Brownworth, M. Virza, and N. Narula. 2023."PARSEC: Executing Smart Contracts in Parallel," MIT Media Lab Digital Currency Initiative.

Mancini-Griffoli, T., M.S. Martinez-Peria, I. Agur, A. Ari, J. Kiff, A. Popescu, and C. Rochon. 2018. "Casting Light on Central Bank Digital Currencies," IMF Staff Discussion Note No. 2018/008.

Monetary Authority of Singapore (MAS). 2021a. "Multi-CBDCs: Designing a Digital Currency Stack for Governability," April 21.

----. 2021b. "Foundational Infrastructures for Inclusive Digital Economies," April 26.

----. 2022. "Project Orchid: Programmable Digital SGD," October 31.

National Bank of Ukraine. 2019. "Analytical Report on the E-Hryvnia Project."

Nikhil, G.,T. Dryja, and N. Narula. 2023. "A Framework for Programmability in Digital Currency," MIT Media Lab Digital Currency Initiative.

Ølnes, S., J. Ubacht, M. Janssen. 2017. "Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing," Government Information Quarterly, Vol. 34, No. 3, p.p. 355-364.

Oyinloye, D.P., J.S. Teh, N. Jamil, and M. Alawida. 2021. "Blockchain Consensus: An Overview of Alternative Protocols," *Symmetry*, Vol. 13, No. 8.

Ponce, J. 2020. "Digitalization, Retail Payments and Central Bank Digital Currency," *Financial Stability Review*, Banco de España, November.

Prates, M.M. 2021. "The Big Choices When Designing Central Bank Digital Currencies," CoinDesk, September 14.

Rahman, A.A. 2022. "A Decentralized Central Bank Digital Currency," Munich Personal RePEc Archive, January 3.

Reserve Bank of India (RBI). 2022. "Concept Note on Central Bank Digital Currency." October.

Ripple. 2023. "Ripple CBDC Platform: Functional and Technical Overview. v0.1 (DRAFT)," Received on June 27 (unpublished).

Schär, F. 2021. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," *Federal Reserve Bank of St. Louis Review*, Vol. 103, No 2, pp 153–74.

Shah, D., R. Arora, H. Du, S. Darbha, J. Miedema, and C. Minwalla. 2020. "Technology Approach for a CBDC," Bank of Canada Staff Analytical Note 2020-6.

Soderberg, G., M. Bechara, W. Bossu, N.X. Che, S.Davidovic, J. Kiff, I. Lukonga, T. Mancini-Griffoli, T. Sun, A. Yoshinaga, 2022, "Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights, and Policy Lessons," International Monetary Fund Fintech Note 2022/004, February.

Soderberg, G., J. Kiff, H. Tourpe, M. Bechara, S. Forte, K. Kao, A, Lannquist, S. Sun, and A. Yoshinaga. 2023. "How Should Central Banks Explore Central Bank Digital Currency?" IMF Fintech Note No. 2023/008, September.

South African Reserve Bank (SARB). 2018. "Project Khokha: Exploring the Use of Distributed Ledger Technology for Interbank Payments Settlement in South Africa."

----. 2022. "Project Khoka 2: Exploring the Implications of Tokenization in Financial Markets."

Sveriges Riksbank. 2021. "E-Krona Pilot Phase 1".

----. 2022. "E-Krona Pilot Phase 2".

----. 2023. "E-Krona Pilot Phase 3".

----. 2024. "E-Krona Pilot Phase 4".

Swiss National Bank (SNB). 2023. "SNB Launches Pilot Project with Central Bank Digital Currency for Financial Institutions," Press Release, November 2.

Tourpe, H., A. Lannquist, and G. Soderberg. 2023. "A Guide to Central Bank Digital Currency Product Development," IMF Fintech Note No. 2023/007, September.

World Economic Forum (WEF). 2021. "Self-sovereign identity: the future of personal data ownership?" August 12.

----. 2023. "Central Bank Digital Currency Global Interoperability Principles," WEF White Paper, June.

Zhang, T., and Z. Huang. 2022. "Blockchain and Central Bank Digital Currency," ICT Express, Vol. 8, No. 2, p.p. 264-270.

3 Terms and definitions used in this report

Acceptance: Degree to which recipients are obliged to accept incoming push transfers.

Application programming interface (API): A set of defined rules and protocols that are used to allow applications and systems to communicate with each other, for example to process requests to perform specific tasks or access specific data.

Base Unit: The smallest possible value of a currency unit, for example $0.01 in the case of U.S. dollars.

Blockchain: A blockchain is a type of distributed ledger that organizes data in a chain of blocks, each containing data that are verified, validated, and then "chained" to the next block.

Central bank money: Money that is a liability of a central bank, the typical forms of which are cash and bank reserves, and financial institutions' deposits at the central bank. (ITU, 2019)

Central bank reserves: Commercial bank deposits held in accounts with the central bank.

Consensus mechanism (in DLT): Process by which the nodes in a network agree on a common state of the ledger. This process typically relies on cryptographic tools, a set of rules or procedures reflected in the protocol, and, either economic incentives (applicable to any network configuration) or governance arrangements. (ITU, 2019)

Denomination: Classification of the face value of a currency unit. It could be fixed (e.g., $1, $5, $10, $20, $50, and $100 in the case of U.S. physical currency), or variable (e.g., on demand and/or multiples of the base unit).

Distributed ledger (in DLT): A consensus of replicated, shared, and synchronized digital data spread across multiple sites, countries, and/or institutions. (ITU, 2019).

Distributed ledger technology (DLT) refers to the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes. In the context of payment, clearing, and settlement, DLT enables entities, using established procedures and protocols, to carry out transactions without necessarily relying on a central authority to maintain a single "golden copy" of the ledger. (ITU, 2019)

Fungibility: The property whereby currency units are interchangeable, and any denomination is a multiple of a base unit. For example, a $10 currency unit would be fungible if it is exchangeable for any other $10 currency unit, for ten $1 currency units, or for a thousand $0.01 currency units.

Ledger: A database that typically tracks transactions or activities over time in a sequential or chronological order.

Node: In computer science, a node is the basic computing unit of a network. In the context of this report, a node refers to a computer participating in the operation of a DLT arrangement. (ITU, 2019)

Permissioned ledger (in DLT): Ledger that is encrypted to allow nodes to only view in its decrypted form the elements of the ledger they are permissioned to see. (ITU, 2019)

Permissionless ledger (in DLT): A ledger in which all participant nodes are able to view all elements of the ledger. (ITU, 2019)

Programmability: A feature of DLT and other technologies whereby actions can be programmed or automated. (BIS, 2022)

Proof-of-Stake: A method by which validators pledge or "stake" coins that are used as an incentive that transactions added to the distributed ledger are valid. (BIS, 2022)

Proof-of-work: A method by which validators compete to perform mathematical computations to verify and add transactions to the distributed ledger. **(BIS, 2022)**

Real-time gross settlement (RTGS) system: Interbank funds transfer systems, usually operated by a country's central bank, where the transfer, typically via the banks' accounts at the central bank (e.g., their reserve accounts), takes place on a real-time and on a gross transaction-by-transaction basis. (BIS, 1997)

Smart contracts: Programmable electronic procedures that can trigger financial flows or holding transfers if specific events occur and may be used to automate transactions and business processes. (ITU, 2019)

Unspent transaction output (UTXO): An Unspent Transaction Output or UTXO is an unused or leftover cryptocurrency in a transaction. Every cryptocurrency transaction consists of an input and an output. Every time a transaction is executed, the input is deleted, and the output is generated. Any output that is left behind and is not spent immediately is an Unspent Transaction Output that can be later spent in a new transaction.

Validation (in DLT): The process in which nodes identify state changes that are consistent according to the rules of the arrangement (that is, assets are available to the originator, and the originator and beneficiary are entitled to exchange the assets). To do so, each node needs to rely on a record of previous states, either as a "last agreed state" or as a "chain of previous states". (ITU, 2019)

4 Abbreviations used in this report

AML	anti-money laundering
ASAP	Access, service, asset, platform
API	Application programming interface
B2B	business-to-business
CBDC	Central bank digital currency
CFT	Countering financing of terrorism
CVV	Card verification value
DAG	Directed Acyclic Graph
DC	Digital currency
DeFi	Distributed finance
DLT	Distributed ledger technology
DVP	Delivery versus payment
EAV	Entity-Attribute-Value
EMV	Europay, MasterCard and Visa (chip)
HTLC	Hash time-locked contract
IFTTT	If this then that
KYC	Know your customer
LMM	Ledger maintenance mechanism
NFC	Near-field communication
OSI	Open Systems Interconnection
P2B	Person-to-business
P2P	Person-to-person
PAD	Payment authorization data
PBM	Purpose-bound money
PII	Personally identifiable information
PSP	Payment service provider
PVP	Payment versus payment
QR	Quick response (code)
RTGS	Real-time gross settlement system
SIM	Subscriber identity module (card)
UTXO	Unspent transaction output
ZKP	Zero knowledge proof

5 Introduction

Central banks are exploring and launching CBDCs with several motivations in mind (Soderberg et al., 2022 and 2023). Retail CBDC could help improve or safeguard the ability of individuals to make payments, by overcoming challenges such as cash shortages in remote areas, and merchants' unwillingness to accept cash. In areas where cash usage is declining, retail CBDC can provide public access to risk-free central bank money in digital form. Retail CBDC could potentially help lower some of the barriers to financial inclusion in countries with underdeveloped financial systems, low financial penetration, or low access to high quality affordable financial products and services that fit user needs (Auer et al., 2022, Alliance for Financial Inclusion 2022).

Central banks are also considering retail CBDC to maintain monetary policy effectiveness in the face of falling cash usage in parts of the world (He, 2018; Floden and Segendorf (2021); Bindseil, Panetta and Terol (2021). Also retail CBDC could potentially improve the competitiveness of the domestic currency versus foreign currencies or other privately issued digital money if it is well-designed with attractive use features.

Also, because of large economies of scale and network effects, retail payment systems could be dominated by a few very large private service providers (PSPs). This could subject payment systems to risks such as lack of contestability, high fees, and service disruptions. If designed to encourage participation of private PSPs, a retail CBDC could also stimulate innovation and competition that may help lower payment fees and improve payment system efficiency.

Central banks are exploring wholesale CBDC with an eye towards increasing the efficiency of cross-border payments and the settlement of asset purchases and sales (BIS, 2020b, 2022a and 2023e; BIS-CPMI-IMF-WBG, 2021 and 2022).

The purpose of this report is to propose a CBDC reference architecture based on recent CBDC launches, pilots and proofs of concept (Annex 2). There are two pilots, notable by their absence (China and India) due to a lack of technically focused contact information. However, where possible, this report will draw what it can from the relevant central banks' press releases, speeches, consultative reports, international financial institutions' policies, and white papers, plus news from what are believed to be reliable sources. The report will also draw on information gathered from the advanced research of other central banks, for example, from consultative reports and white papers. It should be noted that Annex 2 only covers wholesale CBDC projects that are based on distributed ledger technology (DLT), which is covered in more detail later in the paper, although the rest of the paper will take an agnostic approach to the ledger technology.[5]

The reference architecture will be described in following subsections in terms of the basic CBDC ecosystem functions; CBDC creation, issuance, movement (between digital stores), redemption and destruction.[6] The last subsection will assess the reference architecture fit to actual launches, pilots, and proofs of concept, plus what is emerging from central bank research.

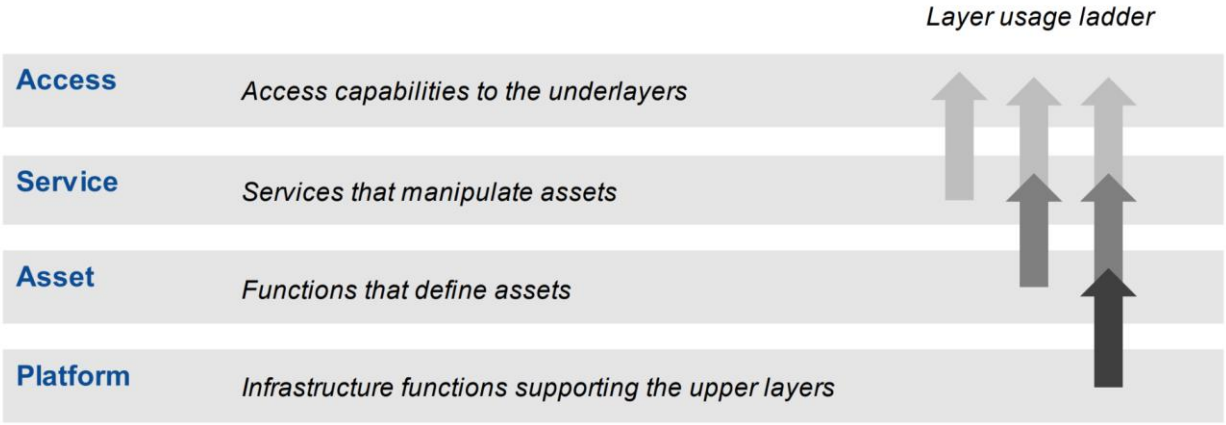
[5] Mancini-Griffoli et al. (2018) characterized central bank reserves as a "wholesale form of CBDC used exclusively for interbank payments''. By this definition, wholesale CBDC or "the issuance by central banks of digital liabilities and the corresponding holding, by third parties of intangible money claims against the balance sheet of the digital liability-issuing central bank would not represent a genuine novelty" (Athanassiou, 2021). However, what is novel about recent wholesale CBDC projects is that they use DLT-based platforms.

[6] A digital currency "store" is where digital currency units exist, maintained, and updated.

6 ASAP Structure Components

Leveraging the Budau and Tourpe (2024) ASAP model, CBDC systems are described in terms of four functional layers - access, service, asset, and platform (Figure 1). This model defines functions and their interrelations to provide a common understanding for CBDC systems. The ASAP model serves as a high-level framework for policymakers, regulators and financial institutions to assess the evolving landscape of digital finance and how it can be effectively regulated and managed. Drawing parallels to the Open Systems Interconnection (OSI) model as an architectural or layered approach to systems for network communications from the International Organization for Standardization where the OSI framework "provides a common basis for the coordination of standards development for the purpose of systems interconnection" the ASAP model serves a distinct purpose in the domain of financial and digital ecosystems, examining digital asset platforms such as CBDC systems from the perspective of vertical organization of functions and roles within the system.[7]

Figure 1: ASAP (Access, Service, Asset and Platform) Model Overview



6.1 Platform Layer

Commonly referred to as the "settlement layer", the platform layer facilitates asset transfers and the record-keeping of financial assets such as CBDC units.[8] The platform, as the lowest layer of the financial asset infrastructure, provides a range of foundational features to support the operation of a CBDC system. Given the choice of centralized or distributed databases, the platform layer facilitates identification, transaction authentication, authorization, and consensus in the case of distributed ledgers. There are two main options we discuss for ledger accounting within the platform layer, balance-based ledgers, and event-based ledgers. units.[9]

[7] The ASAP model was informed by a couple of other similar frameworks. Schar (2021) describes decentralized finance (DeFi) stacks in terms of settlement, asset, protocol and application layers, which map virtually one-to-one into the ASAP model. MAS (2021a) defines CBDC stacks in terms of platform, application, asset and wallet layers, which flips the middle two ASAP layers. Auer et al. (2023) describes DeFi stacks in terms of settlement, application and interface layers, with the ASAP model's asset layer being part of the application layer.

[8] AWS-OWF (2023) defines technology 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".

[9] Currently, all CBDCs that have been launched or piloted, or are being (or have been) subjected to proof-of-concept testing, run (or have run) on ledger-based platforms. That is not to say that a cash-like CBDC could not be issued without an underlying ledger. This could be an "object-based" digital currency, as described in the access layer section below, issued directly (or via an intermediary) into user wallets that then passes directly between wallets without any underlying ledger tracking.

6.1.1 Balance-Based Ledgers

This type of ledger records the current financial value of assets and focuses on tracking how much is held (value) by a key (unique identifier) for a specific key-value pair in the underlying data storage mechanism. The ledger maintains accurate current balances (values) that reflect any changes due to authorized transactions. Authorized transactions execute debits in balances in one key-value pair in the data store and credits the balance in another key-value pair within the data store[10], thereby maintaining an accurate balance for all records within the data store.

6.1.2 Event-Based Ledgers

Event-based ledgers record state changes as unique identifiers or "events" with no direct storage of account balances. These state changes can refer to previous transactions to show how control of an asset changed while ensuring that each transaction is unique, preventing double spending. These ledgers might utilize different data models depending on the implementation. For example, state transition models treat each event as a transition in a replicated state machine. Events are ordered and processed to move the system from one valid state to the next (Buterin, 2014).

6.1.3 Platform Access and Governance

Platform owners implement governance policies for access control and value creation on the platform whether the infrastructure is based on a centralized or a distributed network architecture such as blockchain.

6.1.3.1 Centralized Ledger Infrastructure

Serving as a single source of truth for bookkeeping data, the centralized ledger also provides a single source of control and transaction finality. This technology is typically employed within centralized organizations such as central banks for recording transactions (e.g. real-time gross settlement system) and is typically regarded as the most extensively used data storage mechanism. On centralized ledger-based platforms transaction validation and recording is performed by a single entity, which in the case of a CBDC would be the central bank.

6.1.3.2 Distributed Ledger Infrastructure

DLT platforms' access can be "public" (accessible by anyone) or restricted to a group of selected participants ("private"). Ledger integrity can be managed by all network participants ("permissionless") or a selected group of users ("permissioned") (Table 2). No central banks are currently considering issuing CBDC on public permissionless DLT platforms, as they are seen as falling short on scalability, settlement finality, and financial integrity risk management (Kiff et al., 2020; Zhang and Huang, 2022, BIS, 2023f). Furthermore, some such platforms are based on proof-of-work (PoW) consensus mechanisms, which are frowned on by the central banking community on account of their energy consumption and e-waste (Agur et al., 2022).[11]

Permissioned DLT platforms are to some extent similar to traditional centralized payment systems but can provide new functionalities and new features such as programmability[12] and tokenization.

---

[10] This is also the case for distinct data stores in the case of offline payments between different hardware payment and storage devices.

[11] Proof of work is a technique used to validate new transactions that are added to a distributed ledger. The system requires "miners" to compete to be the first to solve mathematical puzzles to get to add the newest batch of transactions to the distributed ledger. It allows anonymous entities in decentralized networks to trust each other. To solve the mathematical puzzles, miners need to run through all possible solutions until the solution is found which uses significant computing and electrical power. (Bains, 2022)

[12] Nikhil et al. (2023) offers a comprehensive overview of programmable money, aiming to establish a shared language for both practitioners and policymakers while dispelling prevalent myths about this concept

Federated networks provide a permissioned governance approach for trusted entities to interact within a distributed network who share a common goal with a central management framework that enforces consistent configuration and governance policies (Oyinloye et al., 2021).

Table 2: Distributed Ledger Technology (DLT) Typology

Access to transactions	**Access to transaction validation**	
	Permissioned	Permissionless
Public	All nodes can read and submit transactions. Only authorized nodes can validate transactions.	All nodes can read, submit, and validate transactions.
Private	Only authorized nodes can read, submit, and validate transactions.	Not applicable

Source: Beck et al. (2018)

Table 3 summarizes some of the considerations that may make one technology more suitable than another. The mechanics of entry-based platforms are delved into below, starting with centralized and then covering DLT-based ones. But regardless of the type of platform, they all begin with a similar transaction flow of a sender transferring value to a recipient, the mechanics of which are delved into more deeply in the access layer section below.

Table 3: Potential Advantages of Centralized Databases versus Permissioned DLT

Advantages of Centralized Databases	Advantages of DLT (if implemented properly)
▪ Competencies more readily available for technology, security, and vendor relationship ▪ Better control of privacy ▪ Easier to scale ▪ Easier to upgrade ▪ Large available product base built on top	▪ More resilient by design if no single point of failure is introduced ▪ Offers new governance options ▪ Central bank does not have to hold any private data ▪ Could increase compatibility with DLT-based tokenized financial assets ▪ Innovative domain, with new solutions emerging from decentralized finance

Source: Soderberg et al. (2023)

6.1.3.2.1 DLT-Based Transaction Validation

In a DLT-based network, consensus among the participants (“nodes'') must be reached to validate a transaction. The private-permissioned DLT networks preferred by central banks rely on a variety of mechanisms to reach consensus in the transaction validation process.

Hyperledger Fabric, Corda and Quorum offer flexibility in how consensus is achieved.[13] Fabric adopts a modular and pluggable consensus mechanism. Quorum is a permissioned version of the public

including those highly relevant to programmability. The framework introduces a taxonomy categorizing the various "levels" of programmability, ranging from basic application programming interfaces (APIs) to more sophisticated stateful smart contracts including those embedded in DLT networks. In addition, the paper introduces a parallelized architecture for scalably executing smart contracts (PArSEC) which is a technical solution in the development of smart contracts and other tools that add new functionalities to digital assets and payment systems (Lovejoy et al., 2023). In essence, the framework serves as a complimentary guide for understanding the nuanced landscape of programmable money, fostering informed discussions and guiding future developments in this rapidly evolving field.

[13] See Holbrook (2020) for an overview of the consensus mechanisms used by Corda, Fabric and Quorum, and Lipton and Treccani (2022) for Ripple. For more detail see the detailed documentation:

- Corda: https://docs.r3.com/en/platform/corda.html

permissionless Ethereum network that allows different consensus algorithms. All three allow the central bank to set up its own governance and consensus rules and choose validators. Ripple takes a more centralized approach to validator selection, imposing a default list of trusted validators curated by Ripple Labs.

These platforms assign specialized roles to validators (Table 4). For example, in Corda participating validators ensure that the details of the transaction are correct and have been agreed to by both sender and receiver, and notaries confirm the uniqueness and ordering of transactions to prevent double-spending. There can also be a supervisory node, typically assumed by the central bank, that has full view of the ledger to aid in system oversight and compliance. In Fabric, participating nodes (or endorsing peers) validate transactions against the endorsement policy and pass them onto an "orderer" that packages them into blocks that are passed back to the participating nodes for final validation and commitment to the ledger. Fabric also utilizes a Membership Service Provider typically run by the network governing authority, that defines the identity and access control framework for the network.

Table 4: High-Level View of Validator Roles in Select Private-Permissioned DLT Networks

	Validator choice	Transaction execution	Double-spend detection
Corda	Central bank (owner)	Initiator node	Notary node
Fabric	Central bank (owner)	Endorsing peer	Orderer
Quorum	Central bank (owner)	Based on voting amongst all approved validators	
Ripple	Ripple Labs (UNL)	Based on voting among UNL members	
Note: UNL = unique node list			

6.1.3.2.2 DLT-Based Governance Frameworks

DLT governance can broadly play two different roles as highlighted by Ølnes et al. (2017), governance of the distributed ledgers and governance by the distributed ledgers where within a DLT based platform layer both forms of governance are highly relevant for central banks considering their platform choice.

Governance of the distributed ledgers concerns the development, modification, and DLT maintenance. This can be managed via on- or off-ledger governance. On-ledger refers to decision making processes that occur directly on the DLT and is commonly used to decide on the DLT protocol, rules, or parameters. Off-ledger governance refers to decision making processes that occur outside of the DLT. Governance by the distributed ledger refers to the use of DLT in a supporting role to improve existing governance processes more efficiently and transparently (Table 5).

- Fabric: https://hyperledger-fabric.readthedocs.io/en/latest/index.html
- Quorum: https://docs.goquorum.consensys.io
- Ripple: https://docs.ripple.com

Table 5: Network Governance				
Network	**Governing Body**	**Governance Method**	**Pros**	**Cons**
DLT with Off-ledger Governance	Community (eg. Token holders, Federation)	Informal, emergent from network structure	Changes slowly, mostly limited to technical upgrades	Risk of takeover by large validator nodes, slow moving
Centralized Network Governance	Central Bank	Legal ownership	Fast unilateral decision making	Opaque, undemocratic, serves singular interest
DLT with On-ledger Governance	Community (eg. Token holders, Federation of banks)	Formal through token voting	Intentionally designed, resilient to network changes	Risk of plutocracy; big token holders with too much power
Note: Adapted from a diagram depicting governance options in Dixon (2024 p. 166).				

6.1.4 Privacy and Anonymity

Central banks are considering various aspects and norms relating to privacy of retail CBDC transaction data. One of the primary facets of privacy relates to rights and responsibilities surrounding the collection and use of personal information. Besides complete anonymity, which would conflict with anti-money laundering and combating the financing of terrorism (AML/CFT) policies and procedures, according to ECB (2022) there are three plausible forms and degrees of data privacy in ascending order of privacy:

- Fully transparent to the central bank, in which all data related to transactions and customer due diligence are visible to the central bank.
- Transparent to intermediary, in which all transaction and customer due diligence data are visible to the intermediary.[14]
- Privacy threshold, in which there is a high degree of privacy for low-value transactions and/or maximum holdings, whereas large-value transactions and holdings are subject to stringent customer due diligence checks (e.g., know your customer (KYC) checks that require government identification documents). Privacy dimensions could also depend on the type of wallet/user (e.g., unidentified versus fully KYCed user, individual versus commercial entity).

Most, if not all, central banks are all opting for a combination of the last two models, in which intermediaries are responsible for overseeing AML/CFT compliance using tiered thresholds. This is seen as an optimal compromise between guaranteeing privacy of payments, while accounting for regulatory requirements. However, the central banks have access to pseudonymous data, which can de-anonymized it if they can show probable cause, such as with a court order (Table 6).[15]

Another privacy management option could be facilitated through a privacy-enhanced consortium between central banks, intermediaries, and other relevant stakeholders, including state and non-state parties, where personally identifiable information (PII), such as data related to transactions and customer due diligence, can be shared on a data minimized and need to know basis between

[14] In this case, the central bank may still have access to aggregated transaction and holding data as it informs monetary policy and money aggregates in the system.

[15] Technology solutions have been developed that could potentially offer ways to increase privacy for select types of transactions. Gross et al. (2022) have proposed a CBDC system that enables cash-like private transactions up to specific monetary limits. Chaum and Moser (2022) have proposed a CBDC system based on blind signatures that allows central banks to issue tokens through PSPs without knowing who holds specific tokens. The BIS Innovation Hub's Swiss Centre has launched Project Tourbillon, which will build and test this eCash 2.0 platform.

authorized stakeholders through privacy-enhancing technologies such as zero-knowledge proofs (ZKPs).

Table 6: Central Bank CBDC Transaction Data Access

	Transaction Visibility to Central Bank
Bahamas Sand Dollar	CB maintains the ledger in a centralized server. CB has visibility into transactions to monitor suspicious behavior and take legal action (such as freezing wallets) if needed. PII is not shared with CB but with onboarding financial institutions who perform KYC checks i.e. pseudonyms at CB level ensure end-user anonymity.
Eastern Caribbean DCash	CB can see anonymized transaction data and outstanding CBDC in each digital wallet. Registered financial institutions can fully observe the identity of payers and payees and the purpose of transactions.
Jamaica JAM-DEX	The CB does not maintain data on users. Wallet providers maintain the identities of their respective users and transactions in line with AML/CFT regulations.
Ghana eCedi	N/A
Uruguay ePeso	User data is segregated across different databases. Transaction data per (anonymous) digital wallet can be decrypted to reveal the user's identity under very restrictive conditions – e.g., a competent authority prosecuting someone that has probable cause to access the transaction data.

6.2 Asset Layer

The asset layer encompasses core functions that purely define a financial asset and for CBDCs will represent a distinct set of core or primitive functions (e.g. currency creation and, transfers destruction) and some constitutive attributes – like the representation of units of value, and the programmability functions (e.g. remuneration, programmable money). Fundamental rules for the CBDC are typically governed via the definition of the CBDC as an asset on the platform layer such as rules which define privileges and any restrictions.

CBDCs, as a subclass, have unique characteristics that distinguish them from other forms of digital currencies. The characteristics of digital currencies are grouped into "unit characteristics", "production characteristics", "available supply" and "unit rights" which are discussed below .

6.2.1 Unit Characteristics

Unit characteristics define the key CBDC attributes inherent to CBDC units that are enforced on-ledger and distinguish digital currencies units. They include form, denomination, identification, programmability, and remuneration.

6.2.1.1 Form

The underlying data structure for the CBDC can either be a ledger entry- or object-based. CBDCs which are entry-based, leverage the underlying platform layer (ledger) to change control or update balances where the data structure is updated via transactions to maintain accurate records of these changes. Object-based CBDCs represent a cryptographically secure digital object that can only reside in a single store at any given time. These objects can often leverage the underlying platform to validate their authenticity, prevent double-spending attacks and track where the token is stored and where it has been.

This data structure taxonomy diverges from the traditional "account" versus "token" taxonomy, which has been shown to be ambiguous. (See also Box 1)

6.2.1.2 Denomination

CBDC units could be produced with fixed denominations or variable values.[16] Fixed value CBDC units are indivisible whereas variable value units are divisible to specific decimal points. Among physical currencies, denominations refer to the classification for their stated or face value. For example, U.S. banknotes come in seven different fixed denominations ($1, $2, $5, $10, $20, $50, and $100) and coins come in six fixed denominations (1¢, 5¢, 10¢, 25¢, 50¢ and $1). In practice, this requires the "making of change" when value is being transferred. For example, if A owes B $13 but A only has a $20 banknote, A transfers the $20 banknote to B and B returns change in the form of some combination of banknotes and coins that adds up to $7 (e.g., one $5 banknote and two $1 banknotes). Or A goes to the bank and trades in the $20 banknote for smaller notes to pay B.

Box 1: A New Taxonomy for Classifying Digital Currencies

This box compares the four-quadrant digital currency classification scheme used in this report to the popular "account" or "token" based. An account-based system requires verifying the identity of the payer, while a token-based system requires verifying the validity of the object used to pay (Kahn and Roberds, 2009). However, many digital currencies exhibit characteristics of both tokens and accounts, so the scheme does not create mutually exclusive categories.

Garratt et al. (2020) give the example of Bitcoin, for which an address and private key is required as payer proof of identity, which makes it account-based. However, the protocol also requires validation of the payer's account history (i.e., UTXO), which makes it token-based.

This report uses a more nuanced classification system that provides clarity in the identification and classification of digital currencies based on the unique technical implementation of the underlying platform and the asset's form:

- **Ledger tracking at the platform layer** categorizes how the ledger manages transactions either as "events" or "balances". Event-based ledgers record transactions as discrete events that can occur independently. Balance-based ledgers record and track the ongoing balances associated with accounts based on the transactions they engage in.
- **Digital currency form at the asset layer** distinguishes how the digital currency is represented and transferred, either be as an "object" or as an "entry" in a ledger. Objects exist as cryptographically secured digital objects that can be transferred directly from one data store to another without needing an intermediary. Entry-based digital currencies exist as records on a ledger where transactions are settled by updates to the ledger.

Combining these two dimensions creates a classification matrix with four quadrants:

	Events (Tracking Method)	**Balance** (Tracking Method)
Object (Form)	ePeso – Uruguay Pilot, G+D Filia, JamDex	
Entry (Form)	Bitcoin, Sand Dollar	Ethereum, eNaira, DCash – ECCB Pilot, Hashgraph

By utilizing this classification framework, stakeholders can gain a clearer understanding of the different forms of digital currencies and how they operate, ultimately supporting better decision-making in regulation, adoption, and technological development.

[16] It is also possible for the user interface (UI) to present to users the appearance of fixed denominations (in the access layer), but here we are describing denominations that are fixed in the asset layer.

CBDC may also be produced and issued in fixed denominations aligned with existing physical currency denominations to provide users with a physical cash-like experience, to induce wider acceptance and adoption (RBI, 2022). However, they could increase the technical requirements of the system when, for example, the particular e-Peso denomination is not appropriate to make the transaction (Ponce, 2020).

However, digital currency opens the possibility of variable denominations, which are not possible for physical currencies. For example, A could convert her $20 into $13 and $7 digital banknotes and pay B the $13. This is essentially how the Sveriges Riksbank proof-of-concept works (Sveriges Riksbank, 2021). Like krona banknotes, each e-krona unit is uniquely identifiable, and each e-krona unit carries a specific value. However, while banknotes have specific denominations, the value of an e-krona unit can vary. The e-krona units can be divided and combined into new units that represent a smaller or larger amount of e-kronor (Sveriges Riksbank, 2022).

6.2.1.3 Identification

Defines whether the CBDC units can be uniquely identified. Identifiers can be applied to both forms of CBDC (entry or object-based). Among physical currencies, banknotes are typically uniquely identifiable by serial numbers, but coins are not. In the Uruguay pilot, for example, each e-Peso digital note was minted with a specific denomination and included an identification serial number so these digital notes could be traced back to a specific user, and each time that an operation was done the digital notes could be spread in smaller denomination notes with their own unique serial number (Ponce, 2020). Hence, each digital note includes security aspects, and the use of each note can be traced from one wallet to another. This identification and monitoring also mitigates double spending and counterfeiting risks.

6.2.1.4 Programmability

At this layer, programmability of CBDC units defines the possibility of embedding rules or programming logic (e.g., embedded and enabled smart contracts) directly within the CBDC unit as medium of exchange itself (MAS 2022). This is commonly referred to as programmable money features. Programmability features within the CBDC units can be implemented for a myriad of features and are aligned with specific policy objectives such as restricting CBDC transfers. For example, there could be restrictions on which participants can transfer CBDC to, from, for what, when and where.

6.2.1.5 Remuneration

Defines a positive or negative value that can be applied for holding the CBDC within the timeframe set out in its contract. Although none of the CBDCs launched or piloted to date have been remunerated, there are reasons to consider interest-bearing CBDC, such as supporting monetary policy (Soderberg et al., 2023). Remuneration could also be used to modulate CBDC demand by increasing (decreasing) rates to ramp up (dampen) demand. To mitigate disintermediation risk, “tiered remuneration” (high interest rates for small holdings and low rates for high balances) can be used to discourage demand for CBDC as a store of value (Bindseil, 2020).

6.2.2 Production Characteristics

Production characteristics determine the mechanisms and governance frameworks for how digital currency units are produced or destroyed. They include authorization mechanisms, and production governance. (“Production” should not be confused with “issuance”, the former being concerned with the creation and destruction of digital currency units, and the latter being concerned with the release into, or removal from, circulation of digital currency units.)

6.2.2.1 Authorization mechanisms

The processes for the creating or destroying digital currency units can be executed either via offline transaction signing (air-gap signing) or online transaction signing. Online signing is the more

standard approach for many digital currencies where users sign transactions directly within a software wallet connected to the digital asset platform. Offline creation follows a similar process to the production of paper banknotes and prioritizes security by keeping the private key completely isolated from the internet. Typically, central banks utilize key signing ceremonies for minting or destroying CBDC units which can be implemented via direct interaction with the digital asset platform or via offline transaction signing. Generally, key signing ceremonies are implemented to ensure the necessary governance controls and protocols are followed. For example, the Central Bank of Uruguay (BCU) pilot, the BCU first generated secure cryptographic key-pairs and signed a fixed amount of Uruguayan digital pesos in existing cash denominations' values. The key pairs are then stored in a secure hardware module. Following the same authorization and verification principles in place for emission of physical cash, the CBDC units are generated and signed with the BCU private key and stored in a digital reserve vault. Then units are distributed to authorized PSPs, following a workflow that is similar to the way that physical cash is issued and delivered to commercial banks.

6.2.2.2 Production Governance

Determines the governance framework for authorizing the creation and destruction of new digital currency units. These functionalities can be executed by a single entity, very likely in the case of CBDC units

6.2.3 Available Supply

The available supply for digital currencies can be limited (fixed) or unlimited. Digital currencies with a limited supply can have this limit implemented in their source code. For example, ERC-20 smart contracts can define a 'totalSupply' value that is typically a fixed number that is stored on the ledger and cannot be directly modified after deployment. CBDCs as a form of central bank money generally have an unlimited supply which is managed by governance processes within the issuing central bank that can create new or destroy existing digital currency units. There are also processes in place to take CBDC out of circulation. In the latter case, the CBDC could be merely withdrawn from circulating supply and held at the central bank and/or the central bank can "lock" them (in a digital vault held by the central bank), so they remain in circulating supply but are unusable in payments.

6.2.3.1 Supply Release Timing

Supply release timing determines how CBDCs are made available or released into circulation to be used. Release could be immediate (all at once), gradual (e.g., a percent of total created), or on demand.[17] Of the retail CBDCs that have been launched or piloted, two release(d) CBDC units into supply immediately (Uruguay ePeso and SNB's Helvetia), and four release(d) CBDC on demand (Bahamas Sand Dollar, Ghana's eCedi, Jamaica's JAM-DEX and the Eastern Caribbean Union's DCash).

6.2.3.2 Supply Retraction Timing

CBDC can be removed from available CBDC supply either permanently (by destroying) or temporarily (by locking). As an example of the permanent removal approach, in the Sveriges Riksbank proof-of-concept, an e-krona unit can only be used once. Each transaction with e-krona means that the unit used is registered as consumed and the e-krona included in the transaction gains new representation in the form of a new unit for the recipient and if necessary, a new unit with the change is returned to the payer (Sveriges Riksbank, 2021).

[17] Another possibility is conditional release. An example of this is the way Bitcoin releases new units as a reward for miners who successfully solve a cryptographic puzzle and add a new block of transactions to the blockchain. However, conditional release is quite antithetic to CBDC norms.

6.2.4 Unit Rights

Digital currency units can be implemented with explicit rights that are enforced (programmatically) on-ledger providing users with guarantees of the ability to exercise the right. An example of this could be voting rights.

6.2.4.1 Holding Rights

Holding rights determine on-ledger rights granted for users to access the digital currency units based on any number or factors or types of authentication. The People's Bank of China, in their digital yuan pilots, appears to be piloting different combinations of factors for holding rights such as geographic location and user identity information when considering access to its digital yuan pilots.

6.2.4.2 Fungibility

The property whereby the value and usage of digital currency units can be indistinguishable (fungible) or distinguishable (non-fungible) should follow from the central bank's readiness to provide par convertibility. Fungible CBDC units generally have a fixed value and can be used identically within the same context with any other CBDC units with the same discrete denomination or any multiple of a base unit. For example, a $10 unit would be fungible if it is exchangeable for any other $10 unit, for ten $1 units, or for a thousand $0.01 units. All of the CBDC projects of Table 1 share the fungibility property. Implementing programs into the CBDC units may alter their fungibility by changing their value, whether perceived or actual face value, as well as alter their usage (e.g., programmable money)potentially making them non-fungible with CBDC units without this specific this functionality due to these distinguishable characteristics.

6.3 Service Layer

The service layer covers functions that handle or utilize the financial assets deployed on the platform to facilitate the implementation of financial services. These financial services are implemented via standalone use cases determined by business logic such as conditional transfer, lending, and asset exchange.

Decentralized finance (DeFi) provides financial services without centralized intermediaries, operating through automated protocols on distributed ledgers. Instead of transacting with a counterparty, DeFi users thus interact with software programs that pool the resources of other DeFi users to maintain control over their funds.[18]

6.3.1 Programmable Payments

Payments can be automated within the service layer where they are executed once a predefined set of conditions are met. Restrictions could be logically based on combinations of factors. It could enable CBDC network participants to provide programmable payments functionality as overlay services outside of the retail CBDC system. Also, if-this-then-that (IFTTT) logic could be applied to coordinating payment and delivery. Such smart contract-based programmability is integral to wholesale CBDC functionalities, such as atomic settlement, the instant exchange of two assets that are linked so that the transfer of one asset occurs if and only if the transfer of the other asset also occurs. This is used in Project mBridge to achieve simultaneous foreign exchange transaction payment-versus-payment (PVP) and in Project Helvetia to achieve simultaneous securities delivery-versus-payment (DVP) transaction settlement (BIS, 2023e; BIS, 2020b; BIS, 2022a).[19]

---

[18] Section 4 explores the multi-layer aspects of DeFi.

[19] See also the BIS (2023c) "unified ledger" concept. A unified ledger where central bank digital is a "common venue" where tokenized commercial bank deposits, and other tokenized assets coexist on the same programmable platform, using wholesale CBDC as the settlement instrument (BIS, 2023c). It would allow for the use of smart contracts and composability, so that any sequence of transactions in tokenized money and

Another model for programmable payments is “purpose bound money” (PBM) by which CBDC units are wrapped by removable programming logic (MAS, 2023). Once the conditions specified in the PBM wrapper are met, the underlying CBDC unit can be released and used without any constraints or functionality that may have been defined in the PBM wrapper. PBMs have been proposed for use to digitalize vouchers used for example within social welfare programs where the vouchers are distributed to eligible households and programmed to be spent for specific purposes, such as food stamps and grants, at merchants. On receiving the PBM from the sender the PBM wrapper is removed, and the recipient can then use the underlying CBDC units without any of the constraints or functionality previously within the PBM wrapper.

6.4 Access Layer

The access layer contains functions and interfaces that enable clients such as users, applications, and other market components, to engage with the underlying service, asset, and platform infrastructure layers. The access layer provides the capabilities for stakeholders to interact with the services and underlying CBDC within the ecosystem, including conducting transactions and transferring CBDC amounts from source CBDC stores to destination stores. This can be accomplished by leveraging a number of software components or tools such as wallets, web API gateways, and client applications. The first subsection deals with retail CBDC and the second with wholesale CBDC, which is restricted to banks and other financial institutions with accounts at the central bank.

6.4.1 Retail CBDC Transfer

The architecture of a retail CBDC offers an additional layer of complexity, in that it requires two tiers of movement of CBDC issuance:

1. CBDC needs to transfer between the central bank and financial intermediaries (tier-1 issuance among a set of trusted counter-parties), and
2. CBDC needs to be distributable from financial intermediaries to and among consumers and businesses who have individual wallets.

These users are not uniform and may have different wallet holding limits (based on their KYC or other conditions) and a diverse set of end-applications for the CBDC they hold.

6.4.1.1 Wallets (Control Devices)

Wallets provide the core functionality of storage and directing transfers of CBDC amounts between digital stores. Wallets can be software applications or physical control electronic devices. For entry-based platforms, wallets generally allow for the storage of cryptographic keys. On object-based platforms with physical control electronic devices, wallets facilitate the storage of a variety of cryptographic assets such as encrypted data (CBDC tokens) while also facilitating transfers.

In the context of retail CBDC payments systems, central banks have tended to prefer a custodial model where licensed financial institutions or other third-party service providers manage user keys, which facilitates wallet and funds recovery. The primary feature of custodial wallets is convenience. Such wallets provide a high level of support and ease of access, within a framework of rules and user experience workflows (akin to a “walled garden”).

digital assets could be automated and seamlessly integrated. By residing on the same platform as the other tokenized assets and liabilities, the wholesale CBDC ensures settlement finality and singleness of money. It also ensures compliance with the CPMI/IOSCO Principles for Financial Market Infrastructures which states that financial market infrastructures, which a unified ledger effectively is, should provide clear and certain final settlement (Principle 8) in central bank money where practical and available (Principle 9)(BIS, 2012).

A self-custodial wallet model, on the other hand, allows users to have full control over their private keys but can undermine the potential recoverability of lost wallets and funds.[20] Such wallets are provided by a CBDC issuing authority (for example, in the case of the Sand Dollar), unlike the case of crypto-assets where wallet providers are not necessarily affiliated with the issuer or issuing protocol. Self-custodial CBDC wallets are typically designed to provide users with a simple means to sign-up, and manage the storage, verification, and transfers.

Self-custodial CBDC wallets can deviate from those associated with the decentralization ethos of crypto-assets in certain key ways:

- Last resort controls: The central bank may still be able to monitor the user's transactions and impose conditions such as freezing / unfreezing of a user's wallet and reversing user transactions, should any fraudulent activity occur. Such actions are typically backed by regulation and central bank policies and occur on the back of a legal investigation. Given the centralized nature of CBDCs, central banks and issuing authorities can also impose whitelisting rules and transfer limits that prevent certain parties or amounts over a certain value from transacting on the CBDC network.
- Common security standards: The central bank may impose a singular set of rules and security practices with a view to protecting the user and allowing for seamless adoption of the CBDC. This enables the user to rely on a common security standard and reduce any overhead in terms of relying on their own limited security preparations and third-party tools.
- Guided recovery and rescue: Central banks can enable mechanisms in the wallet infrastructure they provide to help users recover access to their wallets in the event of device loss, theft or damage. The design nuance to take note of here is the location of the funds i.e., although self-custodial in appearance, the CBDCs may not be stored in the device or within the user's control, but on a central bank ledger. The wallet app in this case would merely serve as a control / signing solution and a pointer to an address on a central bank's ledger. This feature guarantees users' true control and ownership of their funds.

Transactions can either be "push" or "pull":

- In a push transaction the sender's store controller device (or app) sends payment authorization data (PAD) to the ledger maintenance mechanism (LMM) instructing it to transfer value from its store to the recipient's store. The PAD will typically include the amount of value, the recipient's store coordinates, and a verification code. In a push transaction there is also the question of whether the recipient must formally accept it before the transfer goes through. None of the currently launched or piloted CBDC projects include this requirement, but there may be reasons to do so.
- In a pull transaction, the recipient's store controller device (or app) sends the PAD to the LMM instructing it to transfer value from the sender's store to its store.

Box 2 provides a high-level view of this process for "push" transactions with entry-based assets, and Box 3 covers object-based assets. The process by which source and destination store controllers ("wallets") communicate transfer instructions takes place in two dimensions:

- First there are those that take place between the two wallets - i.e., the exchange of store coordinates and amounts. For entry-based assets, these are data that will be sent to the CBDC ledger for action, and for an object-based asset, the data needs only be communicated between

[20] The phrase "not your keys, not your crypto" popularized in the crypto community emphasizes the relevance of private key control when considering security and sovereignty around who has the necessary cryptographic material to execute transfers.

the two wallets and does not necessarily require a ledger update (see below). That could be via the short-range exchange of information via quick response (QR) codes or near-field communication (NFC) connections. Or it could be one user verbally communicating store coordinates and amounts to the other, or via email or some other messaging service.

- Second there are those that take place between the wallets and the CBDC ledger. For entry-based assets these are instructions to transfer amounts between stores on the ledger. For an object-based asset, these are "information-only" data, so the ledger can keep up to date with the wallets. These would use long-range electronic data exchange protocols like internet or mobile connections.

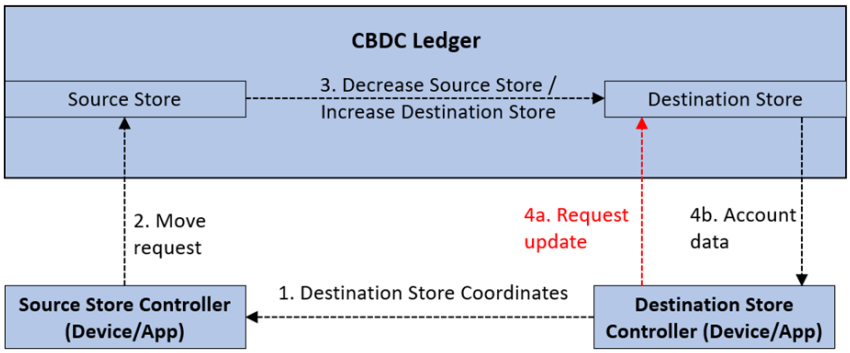
Also important is the role of intermediaries through which transfer instructions are handled, of which broadly speaking there are two modes, depending on where individual participant holdings are recorded:

- They could be recorded directly on the core CBDC ledger with intermediaries effectively performing a pass-through function (Bank of England, 2023).[21]
- They could be recorded in an account maintained by an intermediary, with the core CBDC ledger recording only the total CBDC holdings of each intermediary, even though individual participant holdings remain a liability of the central bank. However, individual participant holding balances are reported to the central bank at regular intervals, to mitigate the risk of those amounts being lost in the wake of the failure of an intermediary. (AWS-OWF, 2022)

Box 2: Transaction Flow on Entry-Based CBDC Platforms

This box concerns how users direct the transfer of retail CBDC amounts from one store to another on an entry-based platform. The figure below provides a high-level view of this for "push" transactions. A push transaction is one in which a sender pushes a CBDC amount to a recipient.[a] In this case, the recipient's destination store controller (application/ device) sends its coordinates to the sender's source store controller (step 1), which then sends a request to the CBDC ledger to decrease the sender's source store and increase the recipient's destination store (2).[b] After the transfer is complete (3) the recipient may then send a request to the CBDC ledger for an update on the contents of the destination store (4a).

Push Transaction on an Entry-Based Retail CBDC Platform



a. In a "pull" transaction a recipient pulls a CBDC amount from a sender. In this case, the sender's source store

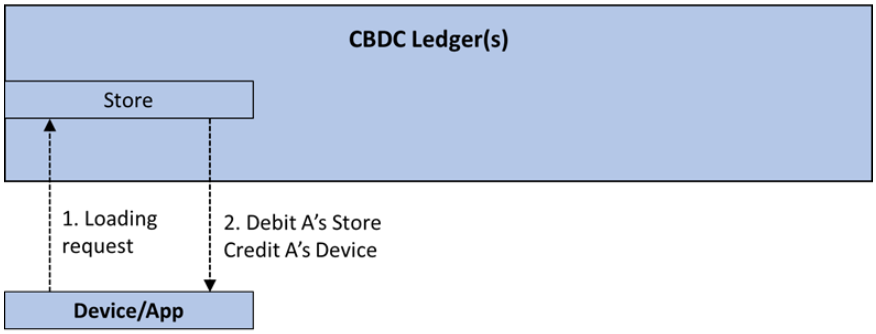
[21] In more technical terms, in what the Bank of England (2023) calls a "platform" model, intermediaries do not hold cryptographic secret keys to access digital stores. This is thought to decrease technical risk and increase portability between intermediaries. (Thanks to Lars Hupel for pointing this out.)

controller sends the source store coordinates, a verification code, and the transaction amount to the recipient's destination store controller which then sends a transfer request to the ledger to decrease the source store and increase the destination store. The verification could be static (e.g., embedded in a card's magnetic stripe data, or a multi-digit CVV (card verification value) number on the back of a card) or dynamic (e.g., EMV (Europay, MasterCard, and Visa) chip generated).
b. In retail payments vernacular "store controllers" are called "wallets". For example, Levitin (2018) defines a digital wallet as a computer software application that stores and transmits payment authorization data.

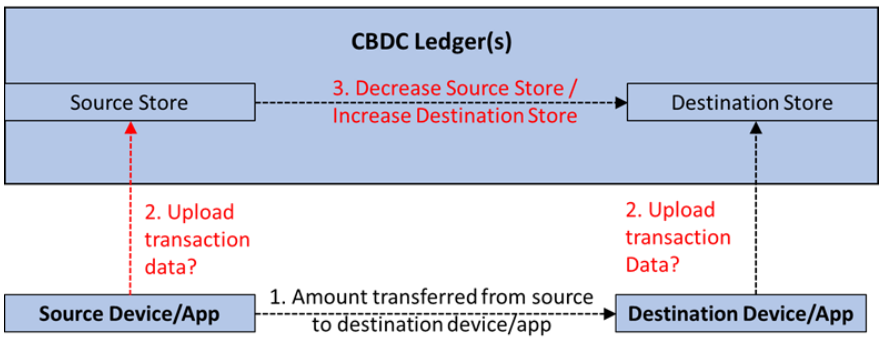
Box 3: Transaction Flow on Object-Based CBDC Platforms

This box concerns how users direct the transfer of retail CBDC amounts directly from one wallet (device or app) to another.[a] The first figure below shows the first step in this process – the transfer of CBDC from the ledger to a participant's wallet. The participant sends a CBDC amount loading request to the ledger (step 1) and the ledger transfers the CBDC amount to the participant's wallet (2). The second figure shows the transfer of a CBDC amount from one participant to another (step 1) coupled possibly with a mirroring of the transaction on the ledger (2 and 3).

Loading Wallets on an Object-Based Retail CBDC Platform



Push Transaction on an Object-Based Retail CBDC Platform



—----------

a. See Kiff (2023) for a high-level description of how a particular variation (offline) of object-based transactions work, and Baqer et al., (2017) for a more technical description.

6.4.1.2 Offline Access

Offline CBDC platforms run on various hardware/software configurations. Some transfer funds between dedicated devices and/or smartphones via quick response (QR) codes, near-field communication (NFC) Bluetooth (BLE), or by manually typing in the authorization/transfer codes. Others transfer funds between dedicated devices via intermediary devices (typically smartphones), to keep the cost of the dedicated devices down and eliminate the need for an internal battery.

Dedicated hardware devices come in several formats, with a credit/debit card-like form factor being popular. Another form factor is an overlay SIM card (sticker SIMs) that is stuck on top of an existing SIM card that converts the phone into an offline retail CBDC device while allowing it to still work as a phone.

Offline payment platforms allow users to transfer value where either the payer or payee or both cannot connect online to the ledger, but the degree of payment finality can vary (BISIH, 2023a and 2023d). Fully offline platforms offer immediate offline settlement finality, and the payee can onward spend it (Figure 2). However, on intermittently offline platforms settlement finality occurs offline, and funds may be onward spent offline, but offline wallets must connect to the ledger based on risk limits set by the issuer (Figure 3). Payments on "staged offline" platforms are not settled, and the payee cannot spend them until she connects to the ledger (Figure 4).

Some offline platforms are based on tokens that are produced and certified by the issuer that transfer independently between users, each digital token having a unique identity like a physical banknote. This method makes it hard to transfer values that are not multiples of one of the denominations held by the sender, resulting in "change" needing to be paid back to the payer from the payee. However, some offline payment platforms represent the balance as a numeric amount, without a unit token, allowing transfers without identifying the individual tokens or their history. Instead, they rely on the payee accepting transfers because she trusts the sender wallet and accepts the value transferred as genuine.

Figure 2: Fully Offline Retail CBDC Transaction

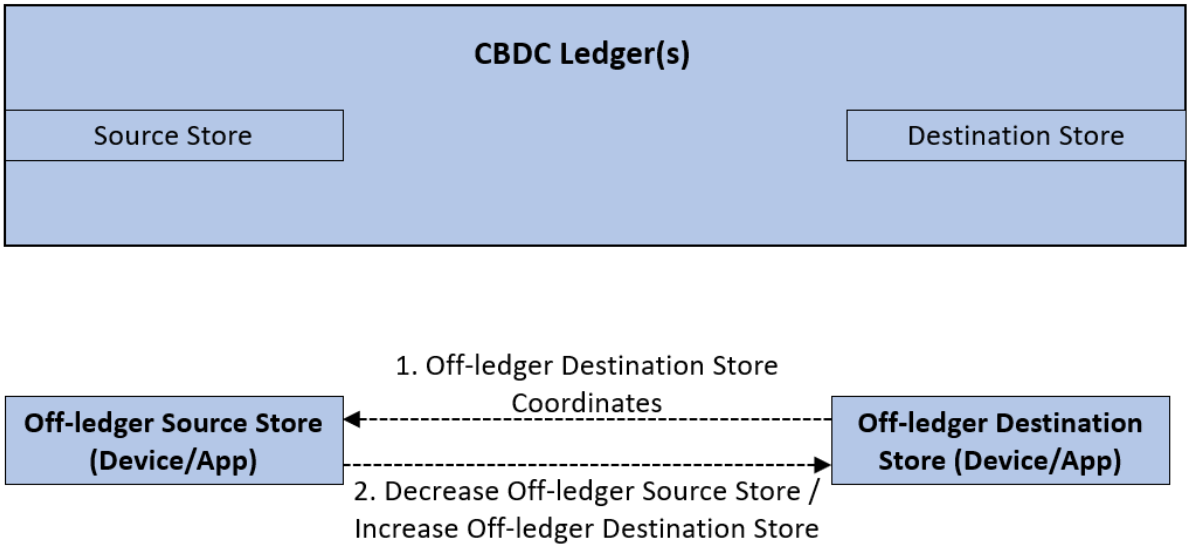
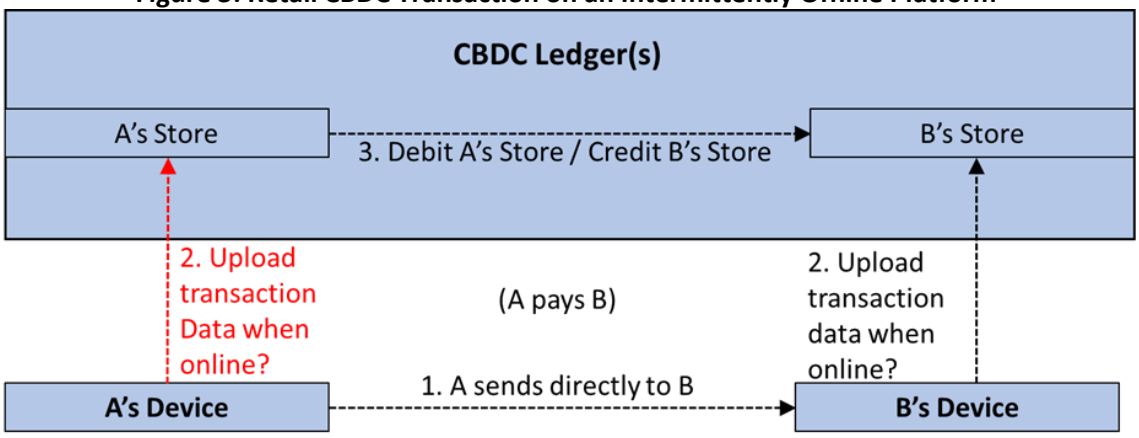
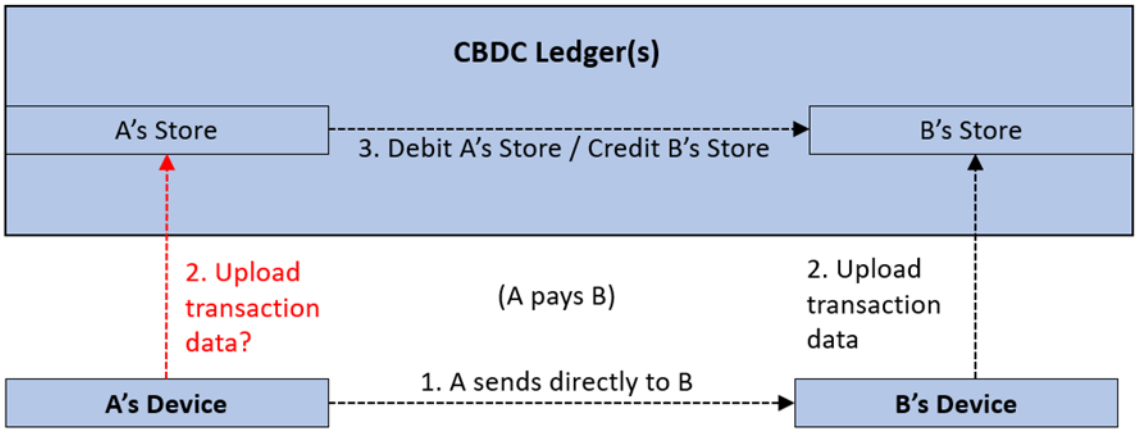


Figure 3: Retail CBDC Transaction on an Intermittently Offline Platform



The payer and payee do not need to connect to a ledger system to exchange value, and the exchanged value is immediately available to the payee to spend onward. However, user devices must synchronize with the ledger intermittently to continue to function.

Figure 4: Retail CBDC Transaction on a Staged Offline Platform



The payer and payee do not need to connect to the ledger to exchange value, but the value exchanged is not settled on the payee until the payee (and/or payer) connects to the ledger system (i.e., final settlement occurs online). Value transferred to the payee cannot be spent until this second stage of online settlement has occurred.

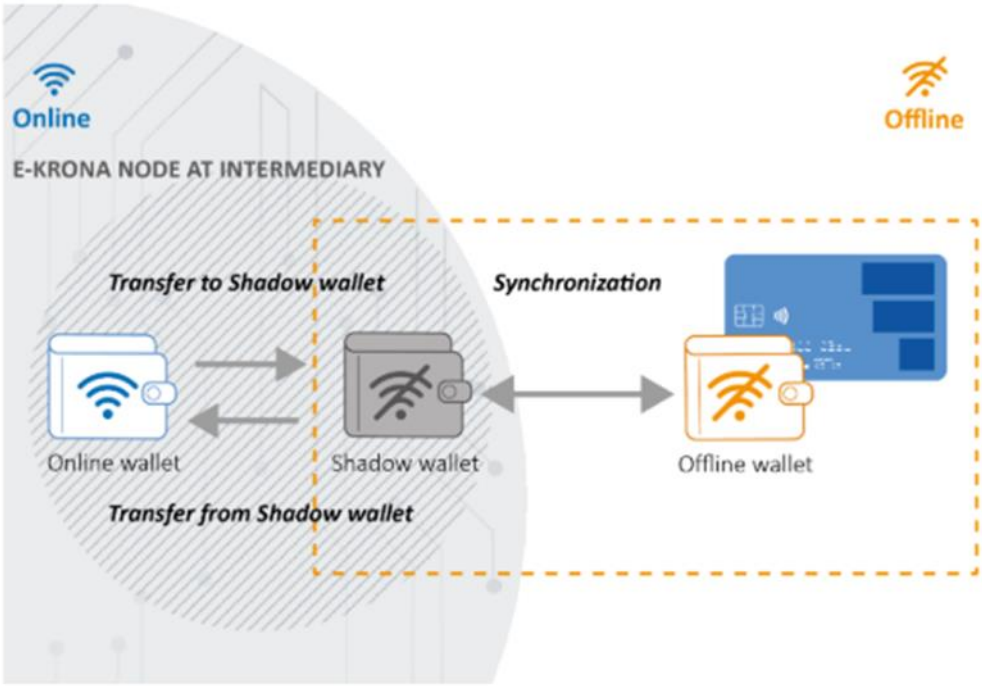
The offline wallet must first be loaded with value by requesting a transfer from another offline device, or from an online account while online. Value is transferred between two offline wallets via the exchange of multi-digit transaction codes that establish agreement between the payer and the payee on the transaction details (payer, payee, and amount). The codes are computed cryptographically, based on the transaction details.

The Riksbank e-krona phase 4 (Sveriges Riksbank, 2024) project discusses the design and testing of an offline payment solution. The solution uses a balance-based approach, where e-krona is reserved for offline use in a shadow wallet (Figure 5). Users can top up their offline wallets from their online wallets. Offline payments are made using payment cards. These cards communicate with point-of-sale terminals. The payment instrument, a card, stores the balance and offline transactions. Offline payments are settled when the card is synchronized with the online system. Security features are designed to prevent fraud, however, some challenges remain, such as liquidity problems and the inability to cancel payments.

Offline payments are prone to transaction interruption, for example, if one of the devices runs out of power, or two devices are interacting using NFC technology and one device is removed from the NFC field too early. Such interruptions could result in “torn transactions” and loss of retail CBDC when the payer’s wallet is debited while the payee’s is not credited. In such cases, the offline payment platform should allow for retransmissions. Offline retail CBDC platforms are also vulnerable to double spending attacks if the attacker can take a snapshot of the state of the offline application environment, execute a transaction, and restore the state of the environment from the snapshot. Mitigating this rollback risk starts with the use of within-wallet tamper resistant offline trusted environments (Hupel, 2024a and 2024b).

So far, only the Bank of Ghana and Bank of Thailand has piloted offline retail CBDC, and that was on the G+D Filia intermittently-offline platform.

Figure 5: The Sveriges Riksbank (2024) Balance-Based Offline Shadow Wallet



6.4.1.3 Holding and Transaction Limits

A retail CBDC could be used not only as a means of payment but also as a store of value. As such, it could undermine commercial bank intermediation. The potential for disintermediation depends on the design of retail CBDC, particularly the level of remuneration via interest rates. None of the launched or piloted retail CBDC to date is interest bearing. To reduce risks of bank disintermediation, holdings of retail CBDC are capped in all Annex 2 retail CBDC launch cases (Table 7).

In order to limit illicit finance risk, central banks are also applying risk-proportional tiered holding and transaction limits, where the limits depend on the KYC process intensity.

Table 7: Holding/Transaction Limit Structures

	Holding Limit
Bahamas Sand Dollar	Physical/email address, phone number and photo for low-limit access (B$500 holding and B$1,500/month transaction). Plus, government-issued photo identification for higher limits (B$8,000 holding and B$10,000/month).
Eastern Caribbean DCash	Physical/email address, phone number, photo and birth date/place for low limit access (EC$1,000 to EC$2,700/month transaction depending on risk profile). Plus, full name and bank account for higher limits (EC$3,000 to EC$20,000/day).
Jamaica JAM-DEX	Government-issued identification to activate any PSP wallet but no holding limits, nor spending limits imposed by the central bank. Limits are left to the PSPs. For example, Lynk imposes no holding limits but there is a person-to-person transaction limit of J$100,000/day. Cash-out limit is J$100,000/day, cash-ins are limited to J$50,000/day from a bank account, J$50,000/month from a debit/credit card.
Ghana eCedi	N/A
Uruguay ePeso	Physical/email address, SIM card and national identification for low limit access (UYU30,000). No higher limits except for businesses (UYU200,000).

Holding restrictions can be applied at more granular levels by, for example, by geography, or industry. The ECB's digital euro project is seeking to ensure a balance between bank deposits and central bank money, with individual holding limits that would rein in the digital euro as an investment option. Such limits aim to maintain financial stability and prevent sudden large-scale shifts from bank deposits to digital euro, which could impact short-term liquidity and commercial bank funding. It could include "waterfall" functionalities that would automatically transfer funds to/from users (bank) accounts when minimum or maximum holding thresholds are reached that would allow for the execution of a transaction once the threshold becomes binding by optionally linking the digital euro account with a payment account. (ECB, 2024)

Limits enforcement is determined by the type of wallet used for the CBDC which in turn propagates the underlying governance policy up to the user level. In practice to date, most central banks issuing CBDC have provided the overarching rules based on total value held or total transferred in a period (e.g., day or month) in the form of tiers (e.g., a Tier-1 wallet has a total hold limit of $100 and a total daily transfer limit of $500, and a Tier-2 wallet can hold $500 and transfer $1,000 per day). Such rules are often propagated to both custodial and self-custodial wallets. This in turn means, if a commercial bank offers its own proprietary wallet infrastructure for a customer to use a CBDC i.e., in a custodial wallet, then this wallet too must follow the central bank's limit enforcement. Such rules are enforced by way of central bank audits and periodic reporting to ensure all intermediaries comply with overarching limit enforcements.

Central banks that have issued CBDCs to date have also provided the rationale and policies for users to be able to change their limits. Often this occurs when a user places a request via an onboarding intermediary (since the central bank does not directly onboard new users and perform KYC verification). The user can then submit additional KYC information to request a limit upgrade, which in turn allows the intermediary to assess whether the user fits the central bank's conditions to increase their wallet limit (e.g., the submission of bank account records or financial statements may qualify a merchant for a higher tier wallet offering a hold limit).

Limits can also be directly downgraded by either the intermediary (if custodial) or the central bank (if self-custodial) in the event of any misuse or fraud.

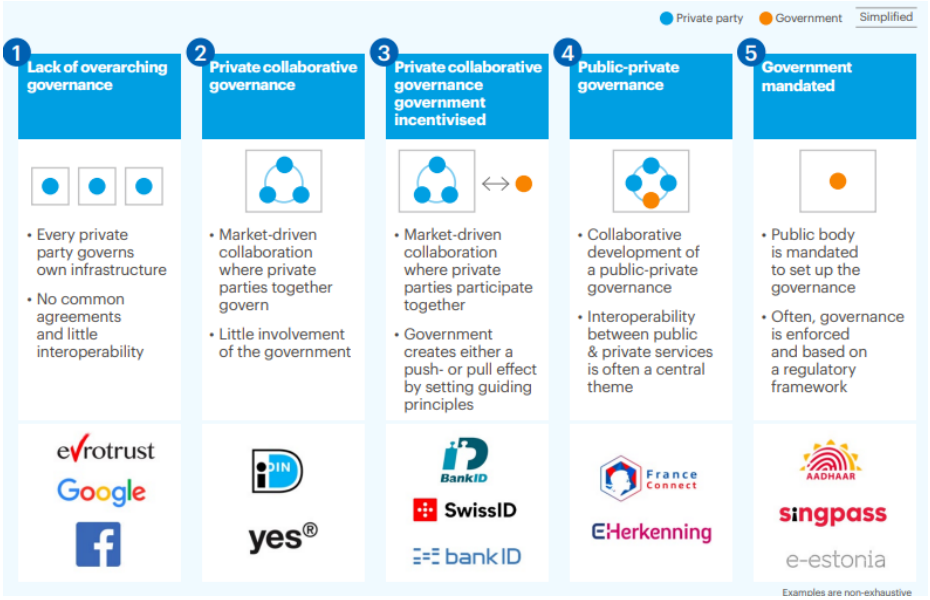
6.4.1.4 Digital Credentials

Digital credentials play a critical role in enabling central banks to implement control and governance over CBDC distribution and usage, including the enforcement of holding and transaction limits. For example, without digital credentials, illicit transactions could be laundered into many smaller transactions and accounts, or users could exceed holding limits by opening multiple accounts.

Beyond that, digital credentials also help streamline transactions by providing a seamless method of authentication and authorization, which is essential for KYC and AML/CFT requirements compliance.

Digital credential schemes have already emerged in several countries, but their specific designs and the relative roles of the public and private sector differ substantially (BIS, 2021a). The main drawback of purely private systems (panels 1 and 2 in Figure 6) is that they lead to "walled gardens" with limited interoperability.[22] On the other hand, government-run systems (panel 5) will face political opposition in jurisdictions in which trust in the authorities is low. Other possibilities include self-sovereign systems based in which individuals own and control their credentials that can be selectively shared with counterparties (WEF, 2021).

Figure 6: Spectrum of public and private solutions for digital credential platforms (MAS, 2021b)



6.4.2 Wholesale CBDC Transfer

In some sense, wholesale CBDC transfer architecture is much simpler than that for retail CBDC because they all run on single-tier (the participants are financial institutions), so the wallet mechanics are almost identical to the illustrative high-level mechanics of Boxes 2 and 3. For example, because all of the participants are trusted central bank counterparties, there is not typically the need for transaction and holding limits, and offline access is not feasible since the multi-ledger use cases all depend on complete connectivity.[23] However, wholesale CBDC transfers will make more extensive use of programmability (e.g., smart contracts) and have to be interoperable in more complex ways for use cases such as PVP and DVP cross-asset transactions (see Box 4).[24]

Within the wholesale context, controls for acceptance of CBDC transfers (value transfers) is more likely than in the retail scenario and can be implemented to determine if a payee (central bank) has

[22] Of note, the ITU and the Linux Foundation have formed the OpenWallet Forum to drive multistakeholder collaboration and discussions on interoperable digital wallet (and credential) systems (ITU, 2024a). Also, the World Wide Web Consortium (W3C) Verifiable Credentials Working Group is working to make expressing and exchanging digital credentials that have been verified by a third party easier and more secure,

[23] Perhaps there might be more of a need for limits for multiple CBDC cross-border applications like mBridge, since the counterparties span borders, and one central bank may want to put controls on usage by foreign institutions in the global network (BIS, 2023e).

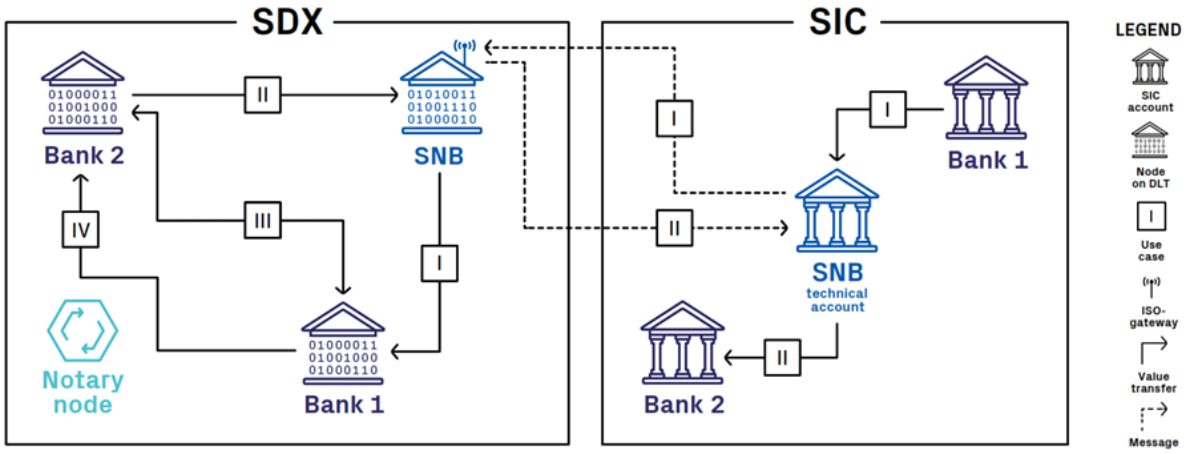
[24] For example, PVP and DVP transactions might use hashed time-locked contracts (HTLCs) to synchronize the actions making up a transaction, so that either they all happen, or none happen (BoC/MAS, 2019).

any control in the receipt of funds to their wallet (store) from a given payer (commercial bank). Redemptions are a potential use case for this control where the central bank may adopt any number of policies to control redemptions and/or conversion of CBDC units by commercial banks.

Box 4: Swiss National Bank Project Helvetia Pilot (BIS, 2020b)

Project Helvetia was a multi-phase proof-of-concept project by the BIS Innovation Hub, the Swiss National Bank (SNB) and the financial infrastructure operator SIX. It demonstrated that a wholesale CBDC can be integrated with existing core banking systems and processes of commercial and central banks. Furthermore, it showed that issuing a wholesale CBDC on a DLT platform operated and owned by a private sector company is feasible under Swiss law (BIS, 2022a). It has since moved into its pilot phase (SNB, 2023).

The settlement process starts with the issuance of wholesale CBDC. A commercial bank (Bank 1) initiates the issuance by transferring funds from its SIC account to an SNB technical account in its Swiss RTGS Swiss Interbank Clearing (SIC) system account. This triggers a message from SIC to the SNB node in the SIX Digital Exchange (SDX). Upon receipt of the message, the SNB node issues the equivalent amount of wholesale CBDC to the Bank 1 node, with the notary node validating the transaction. Once wholesale CBDC exists on the platform (step III), Bank 1 can conduct delivery-versus-payment (DVP) transactions with Bank 2 (step III) in addition to wholesale CBDC free-of-delivery payments to Bank 2 (step IV). State changes to the ledger stemming from the transactions are signed and time-stamped by the notary node. The process ends with the redemption of wholesale CBDC which the Bank 2 node triggers by sending a redemption request to the SNB node (step II).



7 Multi-Layer Concepts

Multi-Layered concepts are those which are better understood by examining them through distinct, yet interconnected, layers of the digital asset platform.

7.1 Operating Model

CBDC operating models are broadly placed in two categories: single- or multi-tier. In the single-tier model, generally associated with wholesale CBDC, central banks carry out all of the CBDC lifecycle functions from production ("minting") to destruction ("burning"). In multi-tier models, generally associated with retail CBDC, central banks create and destroy CBDC, but delegate some or all of the operational and user-facing work to intermediaries (Figure 7). This work includes onboarding users, including performing, AML/CFT compliance checks, designing, and managing user interfaces, managing user data, and providing customer service (e.g., help desks).

In both models, the central bank creates CBDCs and releases them to available supply by distributing them to users (in the case of a single-tier model) or financial intermediaries (in the case of a multi-tier model) in exchange for debiting their accounts at the central bank. In the case of the multi-tier model, the financial intermediaries distribute CBDC to users via interfaces in exchange for cash or by debiting user accounts at the intermediary. Users then make payments among each other. That process runs in reverse when users "cash in" CBDC in exchange for cash or credits to their accounts. In the case of multi-tier models, the intermediaries then submit the CBDC to the central bank in exchange for credits to their accounts at the central bank.

Figure 7: Distribution of CBDC Functions Between the Central Bank and the Private Sector

	Minting		Issuance		Distribution		Validation		Ledger Updates		KYC/AML/ CFT		User Interface		User Data		Customer Service	
	Owner	Executor	Owner	Executor	Owner	Executor	Owner	Executor	Owner	Executor	Owner	Executor	Owner	Executor	Owner	Executor	Owner	Executor
Bahamas																		
China	n/a																	
ECCB	n/a																	
Jamaica																		
Nigeria	n/a																	
Uruguay																		
Canada	n/a																	
Sweden	n/a														n/a			
Eurozone	n/a																	

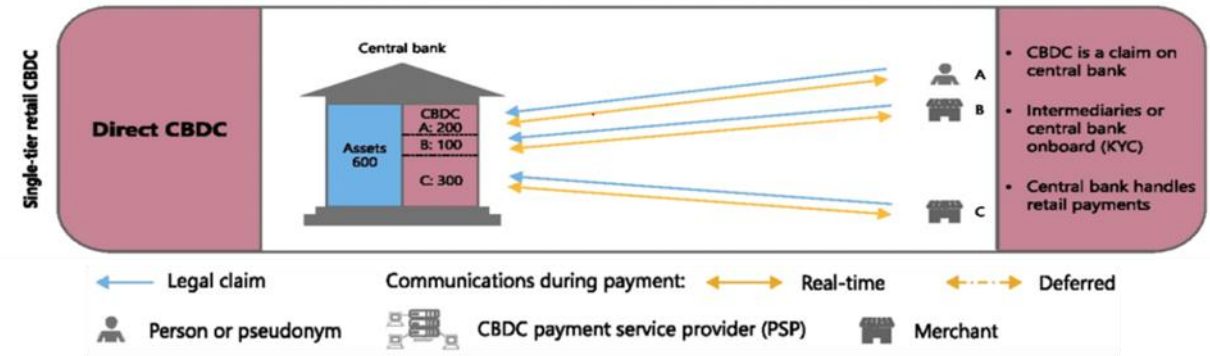
Color scheme: yellow = central bank; blue = intermediaries; purple = shared; gray = not available or still exploring

Source: Soderberg et al. (2023) and authors

7.1.1 Single-Tier Operating Models

In a single-tier model, CBDC transactions resemble transactions with commercial banks, except accounts would be held with the central bank (Figure 8). A payor would log in to an account at the central bank through a web or mobile application and request a transfer of funds to a recipient's account, also at the central bank. The central bank would ensure settlement by updating a master ledger, but only after verification of the payer's authority to use the account, enough funds, and authenticity of the payee's account. This mode gives central banks more control over the product design and implementation process.

Figure 8: Single-Tier Operating Model



Source: Auer and Boehme. 2021. "Central bank digital currency: the quest for minimally invasive technology."

However, the single-tier model requires the central bank to assume an active role in distribution and payment services that may exceed the scope of its core mandate and capacity. Moreover, central banks would directly compete with existing digital payment service providers (PSPs) creating disintermediation risk. Conceptually, the single-tier model may be appropriate for a country with a well-resourced central bank in which the financial sector is extremely underdeveloped, so that there

are no institutions to assume distribution and provision of payment services, as may be the case in some low-income countries.

7.1.2 Multi-Tier Operating Models

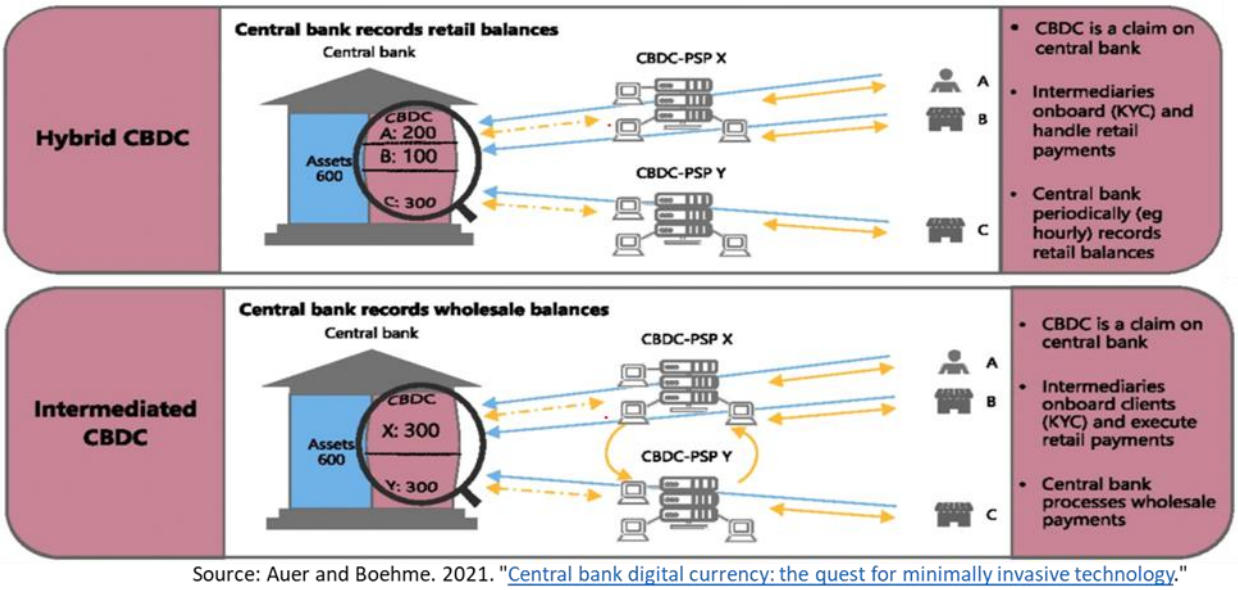
In multi-tier models, the central bank issues CBDC but outsources some or all the work of administering the accounts and payment services, although the CBDC remains the liability of the central bank and thus CBDC holders would not be exposed to default risk of the engaged PSPs (Figure 9).

The multi-tier model has been the overwhelmingly preferred solution in CBDC pilots and launches so far. Running currency distribution is not something the central bank is well-suited to perform, requiring customer-facing activities that may be beyond their capacity. Also, the multi-tier model is less disruptive than the single-tier one as financial institutions play their traditional roles in distribution and payment services. In addition, this layered approach facilitates the integration of new types of consumer electronic devices without the need to alter the core of the system, and it supports the ability for third parties to build on top of the core (Shah et al., 2020; Armelius et al., 2020).

Auer and Boehme (2021) discuss two different multi-tier models that differ in terms of the records kept by the central bank. In a "hybrid" architecture the central bank records all retail CBDC holdings and the CBDC is never on PSP balance sheets so that user holdings are not exposed to claims by PSP creditors in the event of PSP insolvency (first panel of Figure 8). PSPs would connect with the central bank core ledger via an application programming interface (API) to provide customer facing CBDC payment services (Bank of England, 2020). This model effectively "combines indirect connection to the central bank with direct access to the central bank balance sheet and the CBDCs." (Prates, 2020)

The Bank for International Settlements (BIS) and Bank of England explored the building blocks of a retail CBDC ecosystem and how APIs could support innovation in Project Rosalind (BIS, 2023b). The project developed a prototype API layer, with 33 API endpoints in six functional categories. The design and functionalities of the APIs were tested and validated through more than 30 use cases identified and explored by public and private sector collaborators. It demonstrated that an API layer could work with different private sector applications and central bank ledger designs and that a set of simple and standardized API functionalities could support a diverse range of use cases.

Figure 9: Multi-Tier Operating Models



Source: Auer and Boehme. 2021. "Central bank digital currency: the quest for minimally invasive technology."

In an "intermediated" architecture the central bank only runs a ledger of PSP wholesale CBDC holdings (second panel). Central banks may prefer this architecture due to privacy and data security concerns. However, the central bank still must honor CBDC holder claims in the event of PSP insolvency or data breaches, relying on the integrity and availability of the PSP's records. This will require close supervision to ensure that the wholesale holdings add up to the sum of all retail accounts at all times.

Auer and Böhme (2020) suggest that, in an intermediated architecture, there be a legal framework that keeps user CBDC holdings segregated from PSP balance sheets so that the holdings are not considered part of a failed PSP's estate available to creditors. They also suggest that the legal framework could give the central bank the power to switch user accounts in bulk from a failed PSP to a functional one. To do this expeditiously, the central bank would likely have to retain a copy of the records of all retail CBDC holdings.

7.1.2.1 Multi-Tier Model Considerations

The multi-tier CBDC ecosystem should be designed to create economic incentives for PSPs to participate in ways that serve central bank interests (making the CBDC broadly available to the public, across regions, etc.). There should be a cost-effective business model for such PSPs with enough revenues from interest spreads, fees, and cross-subsidization, as well as controllable fixed and variable costs. Also, regulations should leave room for enough users to reach critical mass and incentivize network buildup while promoting PSP market competition.

Fees may be paid to PSPs to offset some of their costs and ease their participation in the CBDC network. They may also be levied by the central bank as a way to offset the cost of setting up the retail CBDC infrastructure for all parties. There could also be business-to-business (B2B) or person-to-person (P2P) fees depending on the underlying entity and business relationships.

Fees may bear the following additional properties:

- Type: Transactional vs. Specific charges / levies
- Calculation: Pre-defined vs. on-the-fly
- Value: Fixed amount (flat rates or tiers) vs. variable (percentage or volume)
- Recurrence: Ad-hoc vs. periodic
- Payment: Deducted at-source vs. paid post facto (as a separate workflow)

It is important to view fee management as a general capability and a feature of a well-designed retail CBDC system, and not as an essential / mandated component in the CBDC lifecycle.[25] Fees in a retail CBDC environment can also follow a highly bespoke plan. For example, in the National Bank of Ukraine (2019) pilot project, P2P transactions were free of charge, but PSPs were able to charge up to one percent of the transaction amount on P2B and B2B transactions, which is slightly less than what is charged on other digital payment instruments and payment cards. Also, eliminating interchange fees on CBDC transactions, along with a reduction/ elimination in the cost of handling cash, would incentivize some retailers to encourage consumers to adopt and use retail CBDC,

[25] A unified retail CBDC infrastructure binds the various entities in the monetary lifecycle within the same type of currency data structure. This feature allows for fee payments and deductions to be conducted as a native capability within the retail CBDC system instead of being done outside of it. This is particularly useful to avoid situations where conversions are needed for the fee to be payable in an acceptable currency type, and delays are incurred due to the billing process taking place outside the transaction.

assuming the foregone fees are not passed on to users.[26] None of central bank pilots and launches of retail CBDC in Table 1 are currently applying transaction fees.

It may be worth noting variants of the aforementioned structures exist; with the CBDC ecosystem and the position of its actors defining the wider operating model as well as the downstream adoption of the currency. For example, Liu et al. (2024) propounded three principal types of configurations based on economic, technological and impact trade-offs:

- Model 1: The central bank is responsible for providing the network infrastructure. Intermediaries provide all end-user services.
- Model 2: The central bank is responsible for providing the network infrastructure and a basic wallet for end users. Intermediaries provide all other end-user services.
- Model 3: The network infrastructure is provided by a regulated entity. Intermediaries provide all end-user services.

The above configurations consider the central bank, financial intermediaries and end users (individuals, merchants) as the three main actors in the CBDC ecosystem. Liu et al. (2024). further considers the following parameters or "contractual terms" as chiefly regulating the ecosystem:

- Entry terms: Who can perform different activities.
- Pricing: At what prices activities can be offered.
- Quality standards for services provided upstream and downstream in the ecosystem.
- Privacy: what can be done with the data of the ecosystem.

7.2 Interoperability

"Interoperability is the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units." (ISO, 2015). Interoperability within the CBDC ecosystem and between other payment systems is important to achieving end user adoption and reducing the risk of fragmentation and closed loop systems (BIS, 2021b). The absence of intra-ecosystem interoperability would undermine the possibility of universal and seamless retail CBDC P2P transactions. The absence of inter-payment system interoperability would thwart the ability to transfer funds into and out of the CBDC ecosystem, and lock users into single intermediaries.[27]

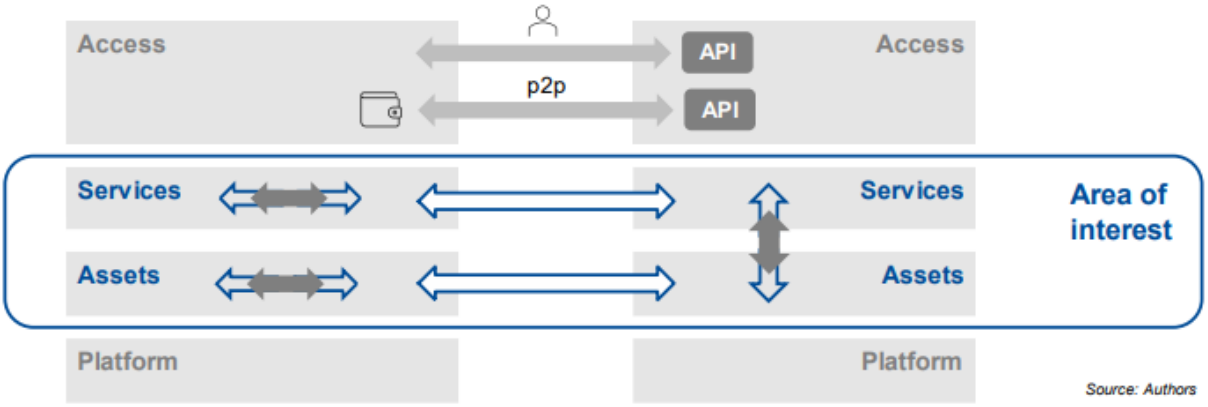
Interoperability implementation takes place at multiple layers (WEF, 2023). It would involve setting technical specifications, messaging and data formatting and structuring standards (Figure 10). At a technical level, the CBDC systems should provide well-defined and standardized APIs at the access layer that allow easy integration with other financial infrastructures, supporting transaction processing, identity verification and data exchange. They should incorporate bridging mechanisms that enable the transfer of value between different payment networks, and oracles that ensure the accuracy, reliability and integrity of the information obtained from external systems.[28]

[26] Interchange fees are paid between banks for accepting card transactions. For ATM cash withdrawals transactions, interchange fees are paid by a card-issuing bank to an acquiring bank (for the maintenance of the ATM). Interchange fees are typically set by the operator of the card networks.

[27] Another example of the importance of interoperability is the implementation of "waterfall" functionality that automatically transfers amounts to (and from) linked private money accounts when minimum (or maximum) holding thresholds are reached (Bindseil, 2020).

[28] See Hupel (2023) for a discussion of different interoperability technical options.

Figure 10: Area of Interest for Interoperability Implementation



Source: Budau and Tourpe (2024)

Interoperability between different CBDC systems can be achieved in three ways, compatibility, interlinking and a single system. Compatibility refers to individual CBDC systems using common standards. Interlinking refers to establishing a set of contractual agreements, technical links, standards, and operational components between CBDC systems allowing participants to transact with each other without participating in the same system. A single system refers to an arrangement that uses a single common technical infrastructure hosting multiple CBDCs.[29]

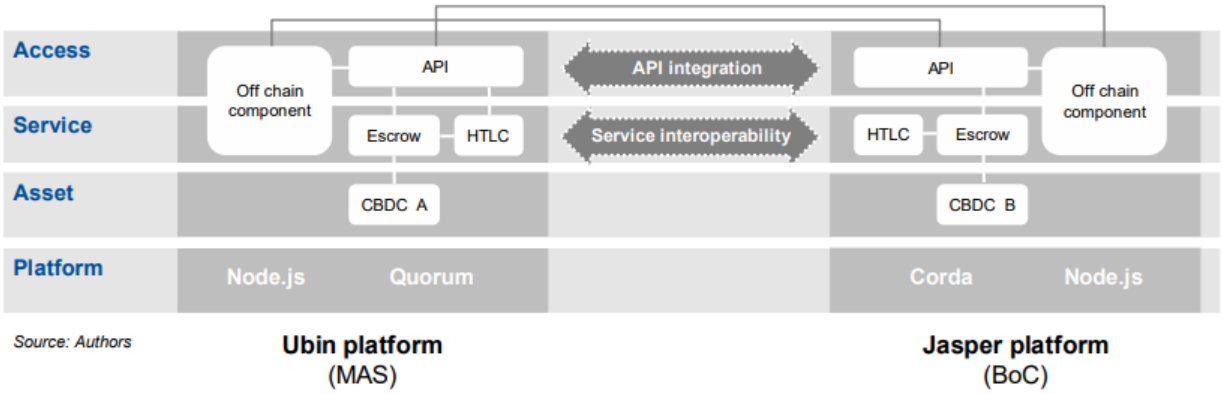
Project mBridge experiments with multiple central bank digital currencies on a single system or common platform for wholesale cross-border payments (BIS, 2023e). This platform supports real-time, peer-to-peer, cross-border payments and foreign exchange transactions using CBDCs and interoperability with Commercial Bank internal systems using APIs based on the global ISO 20022.

Considering interlinking of heterogeneous CBDC systems allowing for the transfer of value between these systems it will be necessary to ensure alignment of the characteristics of the CBDC itself for example programmability or specific privacy characteristics may not be interoperable.

The design of the access and service layers of the CBDC system play a significant role in determining the potential for interoperability as experimented in project Jasper-Ubin led by Bank of Canada and the Monetary Authority of Singapore. This experiment leveraged a service hashed time-locked contracts (HTLC) on both heterogeneous CBDC networks (Figure 11) which allows for payments on each platform to be simultaneously executed or collectively rolled back, ensuring transaction finality, and reducing counterparty risk (BoC/MAS, 2019). Basic interoperability was achieved through API integration at the access layer and service layer interoperability was achieved through common services (HTLC) for asset exchange between two platforms. Importantly, Banque de France (Banque de France, 2023) showed, in its experimentation series that interoperability does not hinge on the convergence of the local service implementation but rather agreeing on the use of the same specification and parameters, such as secret format, cryptographic protocols and the timeframe of asset escrowing on both platforms.

[29] Rahman (2022) proposes a decentralized CBDC (dCBDC) allocated collectively through a United Nations (UN) framework. The UN framework would support interoperable transactions among monetary blocs, while domestic transactions would still utilize each bloc's respective currency. By leveraging digital technologies, this dCBDC aims to enable real-time reconciliations between central banks, enhancing efficiency. Additionally, this single system model could provide international liquidity to all participating blocs, effectively addressing global imbalances and stabilizing exchange rates without necessitating extensive economic integration, offering a more inclusive approach to global monetary stability.

Figure 11: Asset exchange protocol between two CBDC platforms



Source: Budau and Tourpe (2024)

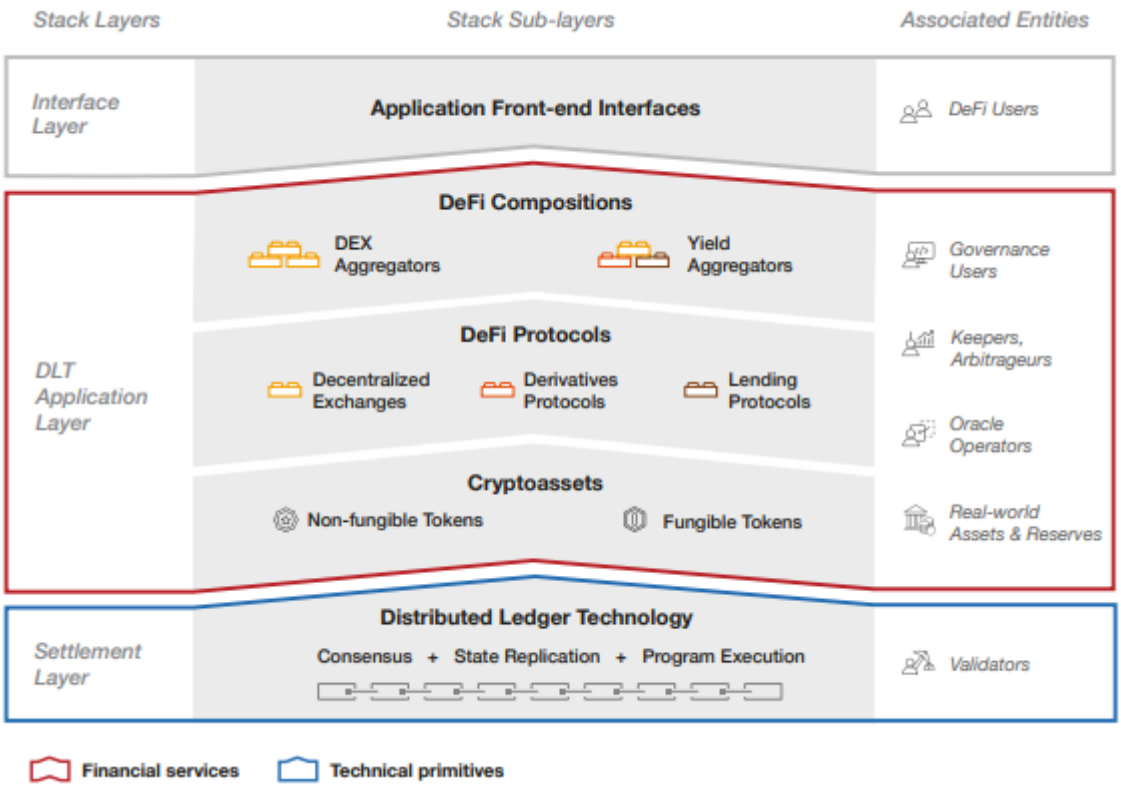
7.3 Management

Key management is a core concern in any cryptographic system including digital currencies. For CBDCs, central banks need to implement key management approaches that ensure the confidentiality, integrity, and availability of cryptographic keys. Compromised keys can lead to unauthorized access to assets and services. Key management interacts with the service, asset, and the platform layers providing a foundation for a secure digital asset platform. On the service layer, keys are used for signing transactions for digital currency creation, transfer and destruction as well as controlling access to digital currency units. Key management on the asset layer is used to validate public keys to verify the asset holder and transaction authenticity and on the Platform layer, robust mechanisms for securely storing cryptographic keys (often hardware security modules or other secure enclaves) and key lifecycle management which involves secure generation, rotation, and the potentially revocation of keys throughout their life cycle within the digital asset platform. CBDCs require central banks to consider the specific implementation approach for key management where the primary options include self-custody (user-managed keys) where users have full control over their private keys or key management services where services store and manage private keys for users. This policy decision has potential implications for the accessibility, recoverability, and usability for users within CBDC systems especially within a retail context where self-custody can be considered to be more complex and unfamiliar for the majority users thereby introducing the potential for additional risks.

7.4 Decentralized Finance

As mentioned above, DeFi refers to financial applications run by self-executing code referred to as smart contracts on distributed ledgers or blockchain technologies, typically on a permissionless (i.e., public) network (Auer et al., 2023). DeFi protocols also operate across multiple layers of the ASAP model and leverage the settlement layer to reach agreement on the global state of the digital asset system. DeFi services are described by Auer et al., 2023) as spanning at least two distinct layers of ASAP model, where crypto-assets correspond to the asset layer and DeFi protocols and compositions combine to provide decentralized financial services to users at the access layer (Figure 12).

Figure 12. DeFi Stack Reference (DSR) Mode



Source: Auer et al. (2023)

8 CBDC Reference Architecture Test Fitting

Table 8 test fits the CBDC launches, pilots and proofs-of-concept with reference architecture highlighting what is common, and what is different.

9 Observations and Conclusions

This technical report presents a reference architecture for CBDCs. This framework provides a foundational structure for comprehending CBDCs as digital asset platforms within the digital monetary system, emphasizing the critical role of standards for interoperability. By applying the framework to diverse CBDC projects such as JAM-DEX (Jamaica), DCash (Eastern Caribbean), Sand Dollar (Bahamas), mBridge (BIS) and ePeso (Uruguay) and others, we have demonstrated its effectiveness in identifying differences in technical functionality that can guide the development of interoperable DC systems through the reference architecture. The findings underscore the framework's potential to promote collaboration and communication among central banks, ultimately paving the way for a more efficient, inclusive, and interoperable digital monetary landscape.

Table 8: Reference Architecture Component Test Fitting								
CBDC:		e-Peso	Sand Dollar	JAM-DEX	DCash	e-Cedi	Helvetia	mBridge
Jurisdiction:		Uruguay	Bahamas	Jamaica	ECCU	Ghana	Switzerland	BISIH
Platform		Giori	MovMint	eCurrency	Bitt	G+D Filia	N/A	N/A
Access Layer: Functions and interfaces that enable clients such as users, applications, and other market components, to engage with the underlying service, asset, and platform infrastructure layers								
- Wallets (Control Devices)	What are the hardware and/or software processes to direct CBDC amount transfers from one store to another?	Authorization via 6-digit PIN codes.		Managed by PSPs outside CB domain		Hardware & software		
- Offline Payments	How are CBDC amount transfers executed when the source and destination stores are in close physical proximity, but are offline (i.e., outside of data or mobile connectivity range)?	No offline capability	No offline capability	Planned but not currently deployed	No offline capability	Has offline capability	n/a	n/a
- Limits	Are limits applied to holdings and/or transaction sizes?	User-type based	KYC-related tiered	Transaction only	KYC-related tiered	N/A	No	No?
Service Layer: Functions that handle or utilize the financial assets deployed on the platform to facilitate the implementation of financial services.								
- Operating Model	Single or multi-tier?	Multi	Multi	Multi	Multi	Multi	Single	Single?
	If multi-tier, how are intermediaries compensated?	N/A (pilot)	None			N/A (pilot)		
- Programmable Payments	Payments executed once a predefined set of conditions are met.	No	No	No	No	By wallet operators	n/a	n/a
Asset Layer: Functions that define the CBDC representing a distinct set of core or primitive functions and some constitutive attributes.								
- Unit Characteristics	Entry-based (centralized or distributed control), or object-based?	Object-based Centralized	Entry-based Distributed Permissioned	Object-based Distributed Permissioned	Entry-based Distributed Permissioned	Object-based Centralized	Entry-based Distributed Permissioned	Entry-based Distributed Permissioned
	Units uniquely identifiable?	Yes	No	Yes	No	Yes	No	No
	Fixed (or variable) denominations?	Fixed	Fixed	Variable	Variable	Variable	Variable	Variable
	Programmable?	No	No	No	No	No	Yes	Yes
	Remunerated?	No	No	No	No	No	No	No
- Production Characteristics	Created in isolation (or via direct connection)?	Isolation	Isolation	Isolation	Isolation	Isolation	Direct	Direct
	How is production governed?	Issuer policy	Issuer policy	Issuer policy	Issuer policy	Issuer policy	Issuer policy	Issuer policy
	Authorization mechanisms?	Cryptographic inputs + 4-eyes	User-linked multi-sig authentication	Quorum of CB-designated officers				
	Production limits?	No	No	No	No	No	No	No
- Available Supply	How are units released into circulation?	Immediate	On demand	On demand and by CB policy	On demand	On demand	Immediate	Immediate?
	How are units removed from supply? (reused or destroyed?)	Issuer policy	On demand and by CB policy	On demand and by CB policy			De-tokenization	
- Unit Rights (explicit)	Usage/holding restrictions?	Issuer policy	CB-issued policy		Configurable		Bond transactions	
	Fungible?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Platform (or Settlement) Layer: Facilitates CBDC amount/unit transfers and the record-keeping.								
- Technology Platform	Event-based (centralized or distributed control), or balance-based?	Event-based Centralized	Event-based Distributed Permissioned	Event-based Distributed Permissioned	Balance-based Distributed Permissioned	Event-based Centralized	Balance-based Distributed Permissioned	Balance-based Distributed Permissioned
- Privacy and Anonymity	Who sees what transaction data? [Could be "baked in" at the platform level or applied in service level]	CB sees only anonymized data.[1]	CB sees only anonymized data.	PSPs see all data for their subscribers, CB sees anonymized data	CB sees only anonymized data.[1] PSPs see all	Anonymous at ledger level	CB sees holdings and transactions on need-to-know basis	?
1. Central bank (CB) can remove anonymity only with court order upon proving that the anonymous data indicates illicit use.								

10 Annex 1: Digital Currency Ontology Primer

An ontology is a formal and explicit representation of concepts and their relationships in a particular domain. An ontology must be complete by design, so there can only be one ontology representing a given domain scope that covers “all matters” in that domain. For example, a CBDC ontology must cover all “distinctions” of all CBDC types. The implication of an ontology is that only one can exist for a given scope, so that all types can be generated by the same ontology simply by selecting different distinctions. Change the value of one distinction and the outcome is a different instantiation. One type is defined by all distinctions having been assigned a value. Change one value of one distinction, and you have a different type.

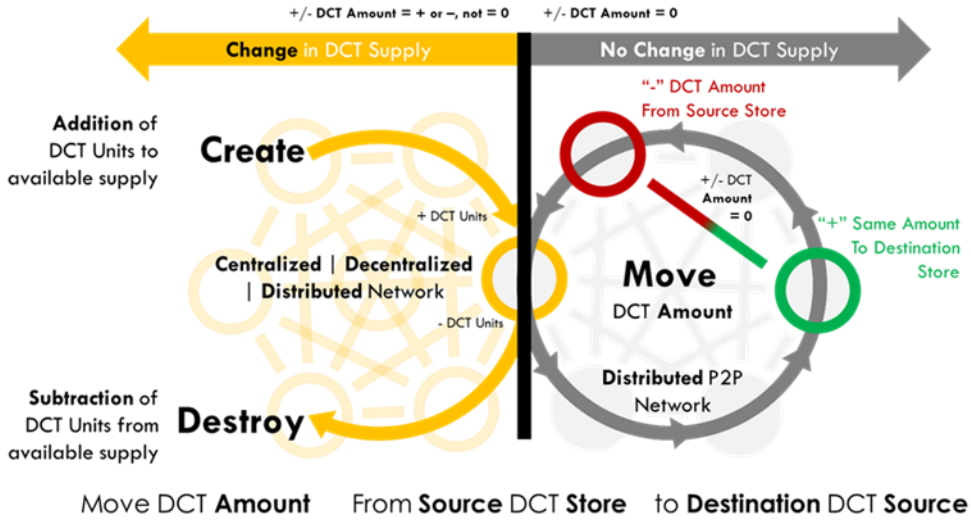
An ontology should be bounded, specific, and provide explicit scope of knowledge of a domain. Once the breadth of the scope is defined, a principle of completeness is applied in the decomposition process of defining, with increasing precision, the structure within the scope.

- The ontology is first described by a set of high-level notions, referred to as “level 1 notions”. Each notion is separated from others at the same level by a fundamental distinction present and unique to the “thing being modeled.” Notions must be mutually exclusive from each other, there cannot be any coverage overlap, and aspects of one notion cannot exist in another.
- Each level 1 notion is then in turn subdivided into distinctions, fundamental differences in that notion that must be unique: described, accounted for, and located once, and nowhere else in the ontology. The cumulative coverage of a notion’s distinctions must equal that of the notion. That is, distinctions of a notion must be complete.
- Level 1 notions decompose into level 2 distinctions; these level 2 distinctions become level 2 Notions which in turn can decompose further into level 3 distinctions. This process continues for each individual notion separately until no further distinctions can be made and only values of the distinctions can be provided. This is the “bottom” of one path of the distinction tree.

For example, the DC issuance ontology consists of five level 1 notions –unit characteristics, production characteristics, value determination, available supply, and unit rights. Then the unit characteristics level 1 notion has five level 2 distinctions – form, denomination, identification, programmability, and remuneration. And the form level 2 distinction has two level 3 distinctions – entry and object data structure. Then each of those two level 3 distinctions have multiple level 4 distinctions, and so on.

The full CBDC ontology would describe a universal ecosystem in which a single CBDC type can be viewed through a high-level understanding of its basic functions: creation, issuance, agreement/ movement, redemption, and destruction. Within the CBDC issuance ontology, issuance defines the key CBDC characteristics and the number of units available as supply in the CBDC ecosystem. It corresponds to the left side of the figure below, which would be the subject of a CBDC issuance ontology. The right side is concerned with how transactions move CBDC amounts from a source CBDC “store” to a destination store.

Linking this to the ASAP-based CBDC reference architecture, the left side corresponds to the “AP” (asset and platform) layers, and the left side to the “AS” (access and service) layers. The model divided the universe of all digital currencies (DCs) according to one separation rule. On the left, changes in available DC supply can occur, and on the right, changes in available supply cannot occur. On the right, a "move" involves subtracting a DC value amount from one DC store and depositing the same amount in a destination store. The left side of the model allows the supply of DC to be issued centrally, de-centrally, or distributed while all moves on the right side of the model occur between a sender and a receiver store on a direct peer-to-peer network.



Move DCT **Amount** From **Source** DCT **Store** to **Destination** DCT **Source**

11 Annex 2: Recent CBDC Launches, Pilots and Proofs of Concept (not necessarily exhaustive)

Platform **Technology**	**Wholesale DLT-based CBDC Projects**	**Use Case**
Consensys	Inthanon-LionRock Phases (2020) (HKMA and BOT)	Cross-Border Payments
DAML/Canton	Regulated Liability Network (2023) (New York Fed)	Domestic Payments
Dashing	mBridge (2023) (BIS, BDF, BOT, CBUAE, MAS, PBOC, SNB)	Cross-Border Payments
HotStuff+	mBridge (2023) (BIS, BDF, BOT, CBUAE, MAS, PBOC, SNB)	Cross-Border Payments
Hyperledger Besu	Mariana (2023) (BIS, BDF, MAS and SNB)	Cross-Border Payments
	Drex (2023) (BCB)	Tokenized bank deposits
Hyperledger Fabric	Aber (2020) (CBUAE and SAMA)	Cross-Border Payments
	Ubin Phase 2 (2021) (MAS)	Domestic Payments
	Cross-Border CBDC Experiment (2022) (BDF, HSBC and IBM)	Securities Settlement
Quorum	Dunbar (2021) (BIS, BNM, BNM, MAS, SARB)	Cross-Border Payments
	Jasper-Ubin (2019) (BOC and MAS)	Cross-Border Payments
	Khokha Phase 1 (2018)	Domestic Payments
	Ubin Phase 2 (2021) (MAS)	Domestic Payments
R3 Corda	Dunbar (2021) (BIS, BNM, BNM, MAS, SARB)	Cross-Border Payments
	Jasper Phase 2 (2017) and 3 (2018)(BOC)	Domestic Payments
	Jasper-Ubin (2019) (BOC and MAS)	Cross-Border Payments
	Helvetia (2023) (SNB)	Securities Settlement
	Inthanon Phase 1 (2019) (BOT)	Domestic Payments
	Inthanon Phase 2 (2019) (BOT)	Securities Settlement
	Inthanon-LionRock (2020) (HKMA and BOT)	Cross-Border Payments
	Jura (2021) (BIS, BDF, and SNB)	Cross-Border Payments
	Khokha Phase 2 (2022) (SARB)	Securities Settlement
	Ubin Phase 1 (2017) (MAS)	Domestic Payments
	Cross-Border CBDC Experiment (2022) (BDF, HSBC and IBM)	Securities Settlement
	Retail CBDC Projects	**Network Type**
Hyperledger Fabric (Bitt)	ECCB DCash (pilot launched 2021)	Distributed Ledger
	Nigeria eNaira (launched 2021)	
Movmint	Bahamas Sand Dollar (launched 2020)	Centralized and Distributed Ledger (Hybrid)
Gioridigital	Uruguay ePeso (pilot completed in 2018)	Centralized Ledger
eCurrency	Jamaica JAM-DEX (launched 2022)	Centralized Ledger
Ripple	Bhutan eNgultrum (PoC)	Distributed Ledger
G & D	Ghana eCedi (pilot)	Centralized Ledger
Hedera Hashgraph	Ghana eCedi (PoC)	Distributed Ledger
OpenCBDC	U.S. Project Hamilton (PoC)	Centralized Ledger

Abbreviations: BCB (Banco Central do Brasil), BDF (Banque de France), BNM (Bank Negara Malaysia), BOC (Bank of Canada), BIS (Bank for International Settlements), BOT (Bank of Thailand), CBUAE (Central Bank of the United Arab Emirates), HKMA (Hong Kong Monetary Authority), MAS (Monetary Authority of Singapore), PBOC (People's Bank of China), RBA (Reserve Bank of Australia), SAMA (Central Bank of Saudi Arabia), SARB (South Africa Reserve Bank), and SNB (Swiss National Bank).
Sources: Publicly- available information from central banks and vendors per hyperlinks above and CBDCTracker.org.