Financial Integrity Implications of Retail Central Bank Digital Currencies (rCBDCs)

Kathleen Kao, Ke Chen, Ben Aldersey, Stephanie Forte Walker, and Giulio Soana

NOTE/2025/010

FINTECH NOTE

Financial Integrity Implications of Retail Central Bank Digital Currencies (rCBDCs)

Prepared by Kathleen Kao, Ke Chen, Ben Aldersey, Stephanie Forte Walker, and Giulio Soana

November 2025

This Fintech Note was prepared under the supervision of Nadine Schwarz.

Financial Integrity Implications of Retail Central Bank Digital Currencies
Note 2025/010
Prepared by Kathleen Kao, Ke Chen, Ben Aldersey, Stephanie Forte Walker, and Giulo Soana*

Cataloging-in-Publication Data
IMF Library

Names: Kao, Kathleen, author. | Chen, Ke (Financial Sector Expert), author. | Aldersey, Ben, author. | Forte, Stephanie, author. | Soana, Giulio, author. | International Monetary Fund, publisher.
Title: Financial integrity implications of retail central bank digital currencies (rCBDCs) / Kathleen Kao, Ke Chen, Ben Aldersey, Stephanie Forte, and Giulio Soana
Other titles:.
Description: Washington, DC : International Monetary Fund, 2025. | Nov. 2025. | NOTE/2025/010. | Includes bibliographical references.
Identifiers: ISBN:
9798229029308 (paper)
9798229029353 (ePub)
9798229029414 (WebPDF)
Subjects: LCSH: Digital currency—Law and legislation. | Money laundering—Law and legislation. | Financial services industry—Technological innovations.
Classification: LCC HG1710.K3 2025

RECOMMENDED CITATION: Kathleen Kao, Ke Chen, Ben Aldersey, Stephanie Forte, and Giulo Soana 2025. “Financial Integrity Implications of Retail Central Bank Digital Currencies” IMF Fintech Note 2025/010, International Monetary Fund, Washington, DC.

Publication orders may be placed online or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, U.S.A.
T. +(1) 202.623.7430
publications@IMF.org
IMFbookstore.org
elibrary.IMF.org

*The authors are grateful to Nadine Schwarz, Nadim Kyriakos-Saad, and Trevor Rajah for their guidance throughout the process. We would like to thank Steve Dawe, Kristel Grace Poh, Luisa Malcherek, Indulekha Thomas, André Reslow, and Victor Budau (all IMF) for their helpful contributions, and Olivier Kraft and Jason Manchester for their peer review. Finally, the authors would also like to thank the FATF Secretariat for providing a sounding board on the application of the FATF Standards in the CBDC context.

Contents

BOXES

FIGURE

TABLES

Acronyms

AML/CFT	Anti–Money Laundering and Combating the Financing of Terrorism
CBDC	Central Bank Digital Currency
CDD	Customer Due Diligence
DLT	Decentralized Ledger Technology
DNFBPs	Designated Nonfinancial Businesses and Professions
ECB	European Central Bank
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
G-20	Group of Twenty Countries
IMF	International Monetary Fund
ML/TF	Money Laundering/Terrorism Financing
P2P	Peer to Peer
PF	Proliferation Financing
R.	Recommendation
rCBDC	Retail Central Bank Digital Currency
SDD	Simplified Due Diligence
TFS	Targeted Financial Sanctions
VA	Virtual Asset
VASP	Virtual Asset Service Provider

Introduction

Central banks are innovating and modernizing legacy payment systems, notably through central bank digital currencies (CBDCs). Although there is no universal definition of CBDCs, the concept is generally understood as a digital form of central bank money (IMF 2023a, p. 1; Patel, Kasiyanto, and Reslow 2024, p. 4). CBDCs can be distinguished from e-money (electronically stored money typically issued by nonbank financial institutions) and virtual assets (VAs) (digital assets issued by private entities). As of 2025, almost every country is exploring or has explored a CBDC for use by individual customers, that is, a retail CBDC (rCBDC).[1] Three jurisdictions (The Bahamas, Jamaica, and Nigeria) have launched an rCBDC. Several other jurisdictions (for example, China, Ghana, India, Kazakhstan, and Türkiye) and one regional body (the Eastern Caribbean Currency Union) have piloted an rCBDC. Other jurisdictions are in advanced stages of research and technological experimentation and evaluating the case for introducing an rCBDC (for example, European Union, Indonesia, Morocco, Sweden, United Arab Emirates, and United Kingdom). Some jurisdictions have also paused or terminated rCBDC explorations (for example, Canada and Ecuador). CBDC explorations vary widely in terms of their size, scope, use cases, and the volume of CBDC in circulation. Some CBDCs are being piloted to millions of users (for example, China and India), whereas the three launched rCBDCs have a comparatively smaller user base. This Fintech Note draws primarily from the experiences of jurisdictions with launches, pilots, or more advanced research and development.

Effective implementation of relevant international standards is required to ensure that rCBDCs do not diminish financial integrity. Like other forms of assets, rCBDCs can be misused for money laundering (ML), terrorist financing (TF), proliferation financing (PF), and other financial crimes; indeed, at least one issuing jurisdiction has already detected instances of criminal misuse (Shen 2022).[2] If widely adopted, rCBDCs could have a significant impact on the integrity of the global financial system. As part of its mandate, the International Monetary Fund (IMF) emphasizes the importance of effective anti–money laundering/combating the financing of terrorism (AML/CFT) frameworks to deter financial crime and safeguard global macroeconomic and financial stability (IMF 2023b). IMF staff help members strengthen their AML/CFT regimes through surveillance, lending, policy development, and capacity development. The IMF Executive Board has endorsed the Financial Action Task Force (FATF)[3] Standards (comprised of 40 Recommendations, their Interpretive Notes, and Glossary) (FATF 2025a) as the relevant standard for the purposes of the Fund's AML/CFT work.[4]

This Fintech Note analyzes the application of the FATF Standards in an rCBDC context and highlights areas for further discussion. At the time of drafting, there was limited practice and guidance with respect to the implementation of the FATF Standards in an rCBDC context. As a result of this, a number of jurisdictions have sought technical assistance from the IMF's Legal Department in this area.

[1] See Atlantic Council (2025). In this Fintech Note, "explorations" refer to CBDC launches, pilots, and advanced research.

[2] Shen, Timmy. 2022. "China busts 'world's dumbest thieves' in digital yuan money laundering case." *Forkast.News*, September. https://forkast.news/china-busts-digital-yuan-money-laundering-case/

[3] The Financial Action Task Force (FATF) is an intergovernmental body established in 1989 to set standards on effective implementation of legal, regulatory, and operational measures for combating money laundering (ML)/terrorist financing/proliferation financing. It comprises 40 members representing most major financial centers in the world.

[4] The FATF Standards were revised in 2012 (including to address proliferation financing), and in 2014, the IMF Executive Board endorsed the revised Standards and assessment methodology for the IMF's operational work (IMF 2014).

The purpose of this Note is twofold: to guide policymakers and competent authorities on implementation of international AML/CFT standards in an rCBDC setting and to highlight specific aspects of the AML/CFT standards that may require further thought.[5] To these ends, the Note is structured to (i) explain the main categories and characteristics of rCBDCs that have an impact on financial integrity and (ii) to analyze the implementation of the FATF Standards in an rCBDC setting (see Annex I), focusing on those that present novel considerations or challenges. This Fintech Note is not intended to represent or preempt the views of the FATF.

This Fintech Note provides an analysis based on rCBDC design choices and the FATF Standards at a specific point in time. CBDC explorations may change dramatically. As such, the design options considered for the purpose of this Note may not represent the totality of all design choices that may be pursued. Similarly, the FATF Standards continue to evolve to adapt to the changing financial landscape and ML/TF typologies. This Note is aimed at guiding jurisdictions on how best to design CBDCs to conform to existing international standards. However, with the development of new or different CBDC features or functionality and updates to international standards, some of the issues raised in this Note may be addressed, although new ones may arise.

The analysis underpinning this Fintech Note was funded by the IMF's AML/CFT Thematic Fund[6] and benefited from information gathered through the IMF's work and public sources. This Fintech Note also draws from discussions in a virtual roundtable on the financial integrity implications of rCBDCs convened by the Legal Department's Financial Integrity Group in January 2025 (see Annex II for key takeaways from the roundtable).

[5] In some jurisdictions, entities other than the central bank, such as the Ministry of Finance, participate in retail central bank digital currency (rCBDC) policymaking and design decisions. References to central banks throughout this Note are intended to acknowledge their role as the rCBDC issuer and primary decision-maker on CBDC design, without prejudice to the role played by other public authorities.

[6] The AML/CFT Thematic Fund Phase III is supported by Canada, France, Germany, Italy, Japan, the Republic of Korea, Luxembourg, the Netherlands, Qatar, Saudi Arabia, Switzerland, and the United Kingdom.

Overview of Relevant Characteristics of Retail Central Bank Digital Currencies

To date, no two rCBDCs (existing or considered) are identical, and there is limited consensus on how to categorize them.[7] Multiple different configurations are possible, and different design choices have different implications for financial integrity as they pose different ML/TF risks and AML/CFT challenges. This chapter identifies the main characteristics of rCBDCs that are most relevant from an AML/CFT perspective. Like the concept of CBDCs itself, the characteristics and the terms used to describe them do not have universally accepted definitions—they are used in this Note solely for ease of discussion and, in most instances, their proposed explanation reflects a consensus among the participants in the IMF Legal Department's January 2025 roundtable.

Retail versus Wholesale Central Bank Digital Currency

CBDCs may be designed for different user bases and use cases. For the purposes of this Note:

- **An rCBDC** is distributed to the general population to be used for day-to-day payments. All three fully launched CBDCs (The Bahamas, Jamaica, and Nigeria) are retail.
- **A wholesale CBDC** is distributed to selected financial institutions for the purpose of settling large value transactions.

Wholesale and retail CBDC pursuits are not mutually exclusive. Although early CBDC explorations (for example, China) centered on a single user base, some jurisdictions are now exploring both in tandem (for example, Israel and the United Arab Emirates).

This Note focuses on rCBDCs. Global AML/CFT standards are largely aimed at preventing ML/TF/PF through retail banking activities (for example, accepting deposits, offering money transfer services, issuing and managing payments), rather than activities such as bank-to-bank lending or settlement or other nonconsumer facing activities, which generally involve funds that have already been subject to AML/CFT measures.

Token-Based versus Account-Based Central Bank Digital Currency[8]

CBDC systems can differ in how they track the transfer of value:

- **A token-based CBDC** relies on an object bearing intrinsic value (the token) and essentially represents a digital bearer instrument. Ownership is demonstrated by possession and transfers can occur without intermediaries. The transfer validation process hinges on verifying the token's authenticity. A classic example of a pure token system in traditional finance is cash. Cash is

[7] For example, the FATF, in its report to the G20, identified three "different types of CBDCs that vary depending on who has access and on the technology used: a) digital central bank tokens that can be used by financial institutions (e.g., for interbank and securities settlements); b) accounts at the central bank for the general public, and c) digital 'cash' that could be used by the general public in retails payments." This Fintech Note discusses in more detail the variations of b) and c).

[8] The concepts of token-based and account-based CBDCs discussed in this Fintech Note are aimed at illustrating financial integrity implications of different CBDC characteristics and are not intended to reflect any legal definitions. For a discussion of the requirements to meet the legal definitions of these terms, see Bossu and others (2020) ("Fintech Note on Legal Aspects of CBDCs").

exchanged based on its value; parties to the transaction do not need to divulge their identities for the transaction to take place, and no record of the transaction is generated as an inherent feature of its use. Although CBDCs with primarily token-based characteristics are technologically feasible (for example, pre-funded/loaded vouchers akin to prepaid cards distributed by the issuer to the public at large), to date no jurisdiction has seriously pursued such a model.[9]

- **An account-based CBDC** operates by generating claims and liabilities on user accounts, satisfied by debiting and crediting such accounts. An account-based (or balance-based) system relies on a third party to maintain an objective record of transactions. An example of an account-based system is a bank account.

In practice, the token-/account-based distinction is somewhat academic. Most CBDC designs combine features of both models using secure authentication to prevent double spending (as in token systems), while recording balances and enabling account management (as in account systems). All advanced pilots and launches bear both token- and account-based characteristics (for example, the electronic Chinese yuan (e-CNY) described as a hybrid instrument with token-like transferability and account-like controls[10].

Mode of Distribution

rCBDC systems could largely preserve the current system of financial intermediation or drastically alter how financial services are provided.

- **In a direct (or one-tiered, or un-intermediated) system,**[11] the central bank distributes CBDCs to end users and opens and manages wallets/accounts of end users. The central bank takes on a customer-interfacing role. Intermediaries and service providers may provide ancillary services but are not involved in CBDC distribution or account management.
- **In an indirect (two-tiered, or intermediated) system,** CBDCs are distributed by the central bank to identified intermediaries (usually banks, but potentially a broader range of nonbank financial institutions, or—in some cases—nonfinancial institutions) and users open accounts with (or obtain wallets from) an authorized intermediary through which they can transact in CBDC (see Table 1 for examples). Indirect rCBDC systems differ from the current notion of a two-tiered financial system (whereby central banks issue central bank money to commercial banks and commercial banks issue commercial bank money to customers). Because of the widely accepted principle that a "true" CBDC must be a liability on the balance sheet of the central bank,[12] CBDCs are not issued to customers through intermediaries—intermediaries do not legally hold customer accounts; rather, intermediaries constitute a customer-interfacing layer to avoid the central bank assuming compliance and other customer-interfacing functions.

[9] "Anonymity vouchers" were explored by the ECB (see European Central Bank 2019), but this feature is not mentioned in more recent publications and statements about privacy and the digital euro (see Daman 2024)

[10] Working Group on E-CNY Research and Development of the People's Bank of China (2021).

[11] There are not yet universally accepted terms describing the different CBDC systems, and different bodies and jurisdictions use different terminology. Further, language describing CBDCs may be limiting; for instance, two-tiered models are used to describe multitiered systems that may contain more than two layers. In addition, some "direct" models may still employ or envision involvement by financial intermediaries.

[12] See Fintech Note on Legal Aspects of CBDCs.

The nature of intermediation varies widely among rCBDCs. In indirect models, central banks can either maintain the full ledger and record retail transactions or can maintain only the wholesale ledger with intermediaries maintaining sub-ledgers of retail transactions (which are reconciled periodically with the central bank's ledger) (Bank for International Settlements 2022)—in both cases, intermediaries assume some customer-interfacing functions. Some central banks are exploring the possibility of allowing multiple intermediaries to interact with a single customer's account, which would be legally held by the central bank (for example, Project Sela). Given the myriad permutations of ledger technology, types of intermediaries, and assignment of roles and responsibilities between the central bank and any intermediaries, attempts to create well-defined categories may be quickly overtaken by the pace of innovation. A system that may be labeled by some a "two-tiered" or "indirect" system may be categorized by others a "direct" or "hybrid" system that externalizes gatekeeping functions. The emphasis in this Note is on the functional roles undertaken by the central bank and other intermediaries rather than the label.

All rCBDC explorations to date have focused on some form of intermediated system, with no central bank seriously pursuing an un-intermediated direct distribution system. Participants in the roundtable overwhelmingly chose indirect (intermediated) models, although no two jurisdictions had identical approaches within that category in terms of ledger infrastructure, the types of intermediaries, and the roles of actors in the CBDC ecosystem.[13]

Table 1. Examples of CBDC Intermediaries

Intermediaries	Core Responsibilities of Intermediaries
The Bahamas (Sand Dollar)—*Launched* • Commercial banks, credit unions, money transmission businesses, payment service providers	• Wallet provision • CDD • Connecting deposit accounts with mobile wallets
China (e-CNY)—*Pilot* • Commercial banks and licensed nonbank payment institutions that meet compliance requirements (including AML/CFT requirements)	• Wallet opening and setting transaction and balance limits based on customer identification information • CDD • Wallet management • Exchanging and circulating e-CNY • Retail management (including payment product design and system development)
Euro Area (Digital Euro)—*Advanced Research* • Credit institutions and payment service providers ("supervised intermediaries")	• Opening accounts or wallets • CDD • Providing devices or interfaces to pay with digital euro in physical stores, online or person-to-person • Transaction management (initiation, authentication, validation and post-settlement activities, including reconciliation)
Ghana (e-Cedi)—*Pilot* • Commercial banks • Mobile money operators and nonbank financial institutions (for example, microfinance, rural and community banks,	• CDD • CBDC distribution (role of commercial banks) • Providing technology services (for example, consumer wallets and applications, merchant products and services, developing and branding new services such

[13] The CBDC ecosystem includes the issuer and administrator (both the central bank in all current rCBDC pursuits), end users, intermediaries, service providers providing administrative or IT support, and any transaction validators.

credit unions, remittance companies, savings and loans companies)	as programmable money and machine-to-machine based payments)
India (Digital Rupee)—*Pilot* • Commercial banks	• CDD • User onboarding • Wallet issuance • Transaction facilitation
Jamaica (Jam-Dex)—*Launched* • Deposit-taking institutions (commercial banks, merchant banks, building societies) and authorized payment service providers	• User onboarding • CDD • Providing digital wallet • Wallet funding
Kazakhstan (Digital Tenge)—*Pilot* • Commercial banks	• CDD • Open digital tenge accounts for users • Hold tokens • Conduct transactions on request from users • Convert noncash tenge to digital tenge and vice versa
Nigeria (eNaira)—*Launched* • Financial institutions, international money transfer operators, agents	• CDD • Payment facilitation • Dispute resolution

Sources: Information extracted from CBDC white papers and statements from central banks: Central Bank of The Bahamas 2019; People's Bank of China 2021; European Central Bank 2022; Bank of Ghana 2022; Reserve Bank of India 2025; Bank of Jamaica (2020); National Bank of Kazakhstan 2022; Central Bank of Nigeria 2021; 2023.
Note: AML/CFT = anti–money laundering and combating the financing of terrorism; CBDC = central bank digital currency; CDD = customer due diligence; e-CNY = electronic Chinese yuan.

Centralized versus Decentralized

rCBDC systems can have varying degrees of centralization and decentralization in terms of operational control and management over a system's core infrastructure:

- Centralized systems are fully controlled by the central bank, which operates the core infrastructure, maintains the ledger, and validates all transactions.
- Decentralized systems disperse ledger maintenance and transaction validation across multiple nodes, either within the public sector or involving private actors.

Varying degrees of centralization and decentralization can exist within one rCBDC model. Systems may have some functions that are centralized (such as issuance, policy enforcement, and administrative control), whereas others are decentralized (such as identity management and transaction validation).[14] Most participants in the IMF Legal Department's roundtable leaned toward centralized systems although some reported exploring both centralized and decentralized features in their rCBDCs (see Annex I).

[14] For more details, please refer to an upcoming Fintech Note on "Layered Decentralization for Central Bank Digital Currencies (CBDC)."

Ledger Access and Technology

Access to the CBDC network and ledger can be restricted or open:

- **Permissioned (closed or controlled access) system:** Access to the ledger and participation in the network is restricted to an authorized group of persons/operators who can only perform the specific actions permitted by the ledger administrator. The three launched rCBDCs and all the other models represented in the roundtable are permissioned systems.
- **Permissionless (open access) system:** Open networks available to everyone; access to the ledger is unrestricted and available to any person without pre-authorization. To date, no fully permissionless system has been seriously pursued (although some jurisdictions may have begun looking into permissionless public chains for rCBDCs).

A combination of restricted and unrestricted access to different parts of the same ledger can also be considered. For instance, the CBDC asset layer (the underlying technology and infrastructure) could be permissioned, whereas the CBDC services layer (the Application Programming Interface layer) could be permissionless.[15]

Moreover, a CBDC ledger can also take different forms, for instance a centralized ledger or traditional database or a distributed system (for example, distributed ledger technology [DLT]).[16] Most roundtable participants reported focusing on a form of centralized ledger, although a few have seriously pursued a DLT-based CBDC with several exploring both centralized and distributed ledgers.

Domestic versus Cross-Border

rCBDCs can be designed solely for domestic use or also for cross-border use. Key considerations include:

- **Access:** Jurisdictions must decide whether only residents can hold and use the CBDC or whether to extend access to nonresidents (for example, tourists).
- **Territorial limitations:** To date, no jurisdiction has imposed any technological restriction preventing use outside of the country (for example, in a close proximity offline exchange with another CBDC wallet of the same jurisdiction), although jurisdictions expect that, in practice, without an available CBDC exchange system in place, little use for a CBDC exists outside of its domestic currency zone.
- **Cross-border architecture:**
    - **Single currency/shared platform:** A common CBDC infrastructure across jurisdictions using the same currency (for example, DCash in the Eastern Caribbean Currency Union and the Digital Euro in the Euro Area).
    - **Cross-currency arrangements:**
        i. **Interlinking (or "bridging") platforms**: Independent domestic systems connected through contractual agreements, technical standards, and interoperability arrangements, with foreign exchange conversion facilitated by intermediaries.[17]

[15] For more details, please refer to an upcoming Fintech Note on "Layered Decentralization for Central Bank Digital Currencies (CBDC)."

[16] Distributed systems refer to operations (for example, the dispersion of data storage and processing functions across multiple nodes)—to be distinguished from decentralized systems, which distribute control across a network of actors.

[17] An example is Project Icebreaker, which experimented a "hub-and-spoke" model to connect domestic rCBDCs through a common hub, with foreign exchange providers facilitating cross-currency transactions. See BIS (2023a).

ii. **Common platform:** Multiple jurisdictions share a single infrastructure for different currencies, requiring strong legal and governance alignment.[18]

As of 2025, all rCBDC pilots and launches are unilateral and designed solely for domestic use. Explorations into cross-border functionality for rCBDCs exist but are nascent.

Offline Functionality

Central banks are also exploring functionality for offline payments for their rCBDC systems. An offline payment with CBDC is a transfer of rCBDC value between devices that does not require connection to any ledger system, often in the absence of internet or telecoms connectivity. A user device may be online (connected to the internet) but still disconnected from a ledger system (BIS 2023b). Offline functionality is possible with any of the aforementioned design options. Jurisdictions seeking to enable offline functionality for CBDC transactions are motivated by a range of factors, including payment resilience, financial inclusion, offering a cash-like option, and preservation of privacy.[19]

The frequency and degree to which users are required to connect back to the ledger to settle offline payments varies. Requirements for connectivity to the ledger range from:

- **Fully offline systems where the payer and payee can remain offline indefinitely** and do not need to connect the ledger to complete a payment. So far, no jurisdictions are pursuing fully offline systems, which may be because of policy concerns, such as those related to double spending and financial integrity as well as operational resilience needs, such as receiving updates.
- **Systems where users cannot remain offline indefinitely** and do not need to connect to the ledger to complete a payment or exchange value, but require the payer and payee to reconnect to the ledger at intervals (for example, after a certain number of transactions, once a holding limit is exceeded, or after a set period offline) to continue transacting or spend value transferred.[20]

Privacy Preserving Features

The degree of privacy afforded to users is a programmable design feature. From a technological perspective, rCBDCs can fall anywhere on a spectrum of total availability of information (beneficial for crime prevention and enforcement but contrary to privacy) to total anonymity (the maximum privacy protection but contrary to other policy objectives). Information on the ledger could support and enhance public functions, but elevated transparency could raise concerns about mass surveillance, data security, and the erosion of financial privacy, which could hamper widespread adoption.

CBDC designs can minimize the amount of data collected, viewable, or accessible by the central bank. This Note focuses on the design choices to further the following privacy objectives:

[18] To date, such a model has not been in focus for retail CBDC but has been heavily experimented with in the wholesale space (see, for example, projects mBridge and Dunbar). That said, multicurrency non-CBDC payment infrastructures to facilitate retail do already exist (see, for example, TARGET Instant Payment Settlement (TIPS), and could in principle also exist for CBDC.

[19] Unstructured Supplementary Service Data-based solutions (for example, 2G or 3G) may also be considered as alternative approaches to enable payments in low connectivity environments. On this point, see the forthcoming Fintech Note, “CBDC Solutions in Connectivity Challenged Environments.”

[20] For a detailed discussion on the modes of CBDC offline payment, see BIS (2023b, 2023c).

- **Privacy from the ledger administrator:** Most central banks opt for a pseudonymous ledger where users are identified by a pseudonym (such as a private key or other identifier) and personally identifiable information is not recorded on the ledger (rather, it is held privately by an intermediary). Although peer-to-peer (P2P) transactions without involvement of any intermediary (thus no user information is collected by central bank or any intermediary) are technically feasible in an rCBDC setting, the feature is not presently being pursued by any jurisdiction represented at the round table.
- **Privacy in transacting:**
    - Tiered rCBDC systems in which the lowest tier (generally with restrictive holding and transaction limits) require minimal or no identification of the user by the intermediary are widely pursued (with roundtable participants being divided between requiring very basic forms of identification and requiring only a mobile number in the lowest tier).
    - Other design options being considered include small-value unnamed accounts or wallets, or other mechanisms to permit a restricted amount of rCBDC to be transferred anonymously within a certain timeframe, and tokens that require identification only at the point of entry/exit when funding or defunding the wallet but guarantee anonymity for the transactions taking place in between. These models often include mitigation measures, such as strict holding or transacting caps or proximity restrictions on transactions.

Most central banks are also exploring technological innovations to protect privacy within transactions (Murphy 2024). Encryption techniques (often called “privacy enhancing technologies”), such as Zero-Knowledge Proof or secure multiparty computation, also can be used to shield certain types of information (for example, on the identity of the user and transactions) from persons that are not parties to the transaction (including the administrator of the ledger). Instructions sent to the ledger by the intermediary do not need to be accompanied by any information beyond the fact of the transaction itself.

It is important to note that the relevant baseline in financial transactions is not complete privacy. Financial institutions, in the course of applying financial crime controls, already routinely monitor and analyze clients’ behavior and information in order to identify unusual or suspicious activities in transactions (for example, attempted fraud). The privacy protecting features described earlier are generally aimed at shielding personally identifiable information from the ledger administrator and any other infrastructure service providers, but not intermediaries.

All rCBDC launches, pilots, and advanced explorations employ some form of privacy protection in their design. Most participants in the IMF roundtable reported exploring a combination of options described earlier, which reflects global trends. Although some prospective rCBDC issuers have explored various mechanisms for a segment of CBDC transactions to occur anonymously (for example, European Central Bank’s (ECB 2019] study of “anonymous vouchers”), to date no country is exploring a fully anonymous rCBDC (regardless of what may be reflected in the CBDC’s name).

Application of the Financial Action Task Force Standards

Limited information and guidance on the implementation of AML/CFT measures in an rCBDC context is currently available. The FATF Standards[21] do not explicitly refer to CBDCs. The FATF has nevertheless confirmed in a 2020 report to the Group of Twenty (G-20) countries that its standards "apply to central bank digital currencies similar to any other form of fiat currency issued by a central bank." Therefore, "the activities of financial institutions, designated nonfinancial businesses and professions, and virtual asset service providers (VASPs) using CBDCs would be covered [under the FATF Standards] as if they were using cash or electronic payments."[22] At the time of drafting of this Note, none of the AML/CFT assessor bodies[23] had assessed the effective implementation of an AML/CFT regime of a country that had issued or piloted an rCBDC, and scant literature on the application of the FATF Standards in a CBDC context was available.[24] Similarly, limited information was available on the assessment and mitigation of ML/TF risks in the context of CBDCs launches and pilots.

This section analyzes the implementation of the FATF Standards in an rCBDC context that generates novel considerations or challenges. For the most part, the FATF Standards will be implemented in an rCBDC setting in a straightforward manner and their implementation will be the same as with activities using traditional forms of money (for example, criminal penalties for ML involving CBDCs should be effective, proportionate, and dissuasive just as in the case of ML involving any other asset and CBDCs should be subject to asset recovery provisions, like other funds or assets that comprise criminal property). In other instances—as discussed herein—implementation might be different in a CBDC context or more challenging. In others still, the correct way to effectively apply the FATF Standards is unclear because some of the characteristics of rCBDCs (as currently launched, piloted, or explored) do not find an easy fit with the present formulation of the Standards or raise questions about the current global approach to AML/CFT efforts. A summary of the anticipated level of challenges in the implementation of all 40 Recommendations in an rCBDC context can be found in Annex I. This section focuses on the FATF Recommendations that members consider to be more challenging to implement and that would benefit from further discussions by the international community and guidance from the standard setter.

Assessing Risks and Applying a Risk-Based Approach to Retail Central Bank Digital Currency

The FATF Standards require jurisdictions to assess and mitigate their ML/TF risks. Recommendation (R.) 1 requires jurisdictions to identify, assess, and understand their ML/TF risks and apply appropriate

[21] The FATF Standards comprise the Recommendations themselves and their Interpretive Notes, together with the applicable definitions in the Glossary.

[22] FATF (2020), Annex B, "Central Bank Digital Currencies."

[23] These include the FATF, the nine FATF-style regional bodies, the IMF, and the World Bank.

[24] Examples of literature examining AML/CFT considerations relating to CBDCs include Financial Intelligence Unit of Latvia (2023), Kakebayashi and others (2023), and Soana and de Arruda (2024).

mitigating measures.[25] The FATF also cautions that "ML/TF risks should be addressed in a forward-looking manner before the launch of any CBDCs."[26]

The FATF also requires jurisdictions and financial institutions to identify and assess the ML/TF risks related to new technologies (R.15). From the perspective of a financial institution, a risk assessment should be conducted prior to the launch of any new products, services, or delivery mechanisms and appropriate measures should be taken to manage and mitigate the risks identified. The FATF has previously noted that in the case of CBDCs, ML/TF risk mitigation should be "led by the issuer of the CBDC (most likely, a jurisdiction's central bank) or the CBDC system operator, if they are not the same."[27] This requirement complements broader risk management expectations of central banks to identify and assess existing and emerging risks arising from new products, projects, or technologies.

rCBDCs may present varying degrees of ML/TF risks compared to existing financial products and payment methods (such as those using cash, bank transfers, VAs, e-money, and prepaid cards).[28] In addition, design choices that increase transparency and traceability of transactions and financial flows could result in a lower level of risk for rCBDC transactions, particularly when compared to cash. On the other hand, the speed and ease with which rCBDC transactions can take place and the possibility of services being offered remotely could pose regulatory, supervisory, and enforcement challenges similar to those faced with VAs. Finally, rCBDCs may introduce entirely new risks and offer new mitigation tools in the case of mass adoption. For instance, although programmability of money remains a controversial topic,[29] it offers a distinct technological advantage in underwriting certain rules into the currency itself (see Box 2). Table 2 illustrates a simplified comparison[30] of ML/TF risk factors and mitigating measures comparing payments and transfers using rCBDCs with select other financial products, such as VAs, cash, bank accounts, and prepaid cards.

[25] FATF (2019, 2021a, and 2024).

[26] FATF (2020), Annex B, paragraph 91.

[27] FATF (2020), Annex B, paragraph 93.

[28] As the inherent risk factors and mitigating factors vary from jurisdiction to jurisdiction, they are discussed in a generic manner in this paragraph and Table 2.

[29] Some jurisdictions have explicitly ruled out programmability of a potential rCBDC other than under user control and with user consent.

[30] This comparison does not fully capture the risk implications of use cases. From an ML/TF risk perspective, rCBDC as a legal tender serving as day-to-day means of payment, would differ from virtual assets (VAs) or prepaid cards. While at present, rCBDCs have a limited usage compared to most existing products, presenting lower ML/TF risks, this may change when and if rCBDCs are widely adopted with potential cross-border usage.

Table 2. ML/TF Risk Factor Comparison

	rCBDCs	VAs	Cash	Bank Accounts	Prepaid Cards
Potential level of inherent ML/TF risk depending on factors					
Anonymity	Lower to Higher[31]	Lower to Higher (depending on whether there is a VASP involved)	Higher	Lower	Lower to Higher (depending on use cases)
Convertibility to other assets	Higher	Higher	Higher	Higher	Higher
Geographical reach	Lower to Higher (depending on design)	Higher	Moderate	Lower to Higher (for example, could depend on correspondent banking relationships)	Moderate (for example, may be accepted for foreign transactions)
Availability (online or offline)	Lower to Higher (offline use may be subject to limits on the number, value, and purpose of transactions)	Lower to Higher (fully online)	Higher (fully offline)	Lower to Higher (fully online)	Lower to Higher (fully online)
Speed of use	Higher	Higher	Moderate	Moderate to Higher	Higher
Portability	Higher	Higher	Moderate	Higher	Moderate to Higher
Strength of mitigation depending on factors					
Traceability	Stronger	Weaker to Stronger (depending on type of VA)	Weaker	Stronger	Stronger
Transaction limits applied	Stronger (transaction limits possible)as seen in launched and piloted CBDCs)	Weaker (No limits)	Weaker to Stronger (limits possible as some jurisdictions impose limits	Stronger (transaction limits possible, for example, low-value accounts)	Stronger (transaction limits possible, that is, restricted by loaded value)

[31] Widescale anonymity is unlikely based on current explorations.

			on cash transactions to mitigate ML/TF risks)		
CDD measures applied	Stronger	Weaker (unhosted wallet with no AML/CFT obliged entity) to Stronger (VASP-intermediated)	Weaker (No CDD)	Stronger	Weaker to Stronger (CDD requirements may depend on card value)
Record-keeping requirements	Stronger	Weaker (unhosted wallet with no AML/CFT obliged entity) to Stronger (VASP-intermediated)	Weaker	Stronger	Weaker to Stronger (depending on record-keeping requirements imposed by country)
Monitoring of transactions	Stronger	Weaker (unhosted wallet with no AML/CFT obliged entity) to Stronger (VASP-intermediated)	Weaker	Stronger	Stronger

Source: Authors' analysis and Financial Action Task Force (2014).
Notes: Higher risk characteristics of each asset type are highlighted in red, lower risk characteristics are highlighted in green, and characteristics which present medium risks or where the ML/TF risks may be higher or lower depending on other factors are highlighted in orange. Factors relating to CBDC are based on current trends in CBDC launches, advanced pilots, and research. AML/CFT = anti–money laundering and combating the financing of terrorism; CBDC = central bank digital currency; CDD = customer due diligence; ML/TF = money laundering/terrorism financing; rCBDC = retail central bank digital currency; VA = virtual assets; VASP = virtual asset service providers.

ML/TF risk understanding should inform both the design decisions for rCBDCs and the development of mitigating measures. A solid analysis and understanding of a jurisdiction's overall ML/TF risks at the national level prior to the launch of CBDCs is key. Jurisdictions should take into account the potential implications of different rCBDC design choices (including those relating to the intended ecosystem and use cases) on the AML/CFT regime. Likely threats and vulnerabilities should be identified at the design stage and a phased plan to enable data collection and analysis to advance risk understanding should be developed as an rCBDC is rolled out. Such efforts should be ongoing or recurrent and be based on real-world data and operational experiences, drawing insights from any rCBDC pilots and on-the-ground experiences, with continual refining of the assessment criteria in tandem with the changing financial landscape. Jurisdictions may opt to conduct a targeted risk assessment for rCBDCs and the findings of the latest national risk assessment and relevant sectoral assessments (for example, risk assessment for e-money) could provide a useful starting point. Assessment of the ML/TF risks of rCBDCs may be more complex than for other financial products at present as a result of the novelty of rCBDC systems. Given the multiplicity of factors, central banks should adopt a collaborative approach that engages all relevant stakeholders in the risk assessment process.

Advisable practices:

- Prior to launching an rCBDC, jurisdictions should conduct ML/TF risk assessments taking into account the intended user base and use cases to inform the rCBDC design choices and drive the implementation of appropriate mitigating measures. Risk assessments should be ongoing or recurrent, consider new information or data gathered in the context of pilots or other trials, and involve all relevant stakeholders, including intermediaries and key competent authorities. ML/TF risk assessment may be complex, so jurisdictions should allow for sufficient time and resources.
- Consideration should be given to the jurisdiction's broader ML/TF risk and context, including the inherent risks and vulnerabilities associated with other parts of the financial system when designing an rCBDC.

Anti–Money Laundering/Combating the Financing of Terrorism Preventive Measures

The FATF Standards include a suite of measures aimed at preventing, detecting, and deterring ML/TF activities. All actors in a CBDC ecosystem meeting the FATF's definition of financial institution,[32] VASP,[33] or designated nonfinancial business or profession (DNFBP)[34] (also referred to as "reporting entities") should be subject to AML/CFT obligations, in particular, the implementation of AML/CFT preventive measures (described in the following). Some of these measures need to be taken at the outset of developing a customer relationship (for example, identifying the customer), whereas others need to take place continuously during the customer relationship (for example, ensuring customer due diligence [CDD] documentation is kept up to date). Others should be taken under certain circumstances even where no customer relationship is involved (for example, in the context of occasional transactions above a certain threshold). The FATF, in its 2020 report to the G-20, clarified that "once a CBDC is established, [reporting entities] that deal in the CBDC will have the same AML/CFT obligations as they do with fiat currencies or cash."[35]

rCBDC advancements may see the propagation of new service providers or existing service providers newly taking on AML/CFT roles and responsibilities. Most CBDC models rely on financial institutions or other intermediaries to distribute CBDCs to their customers through the opening of accounts or provision of wallets. Some jurisdictions are also considering ways to disseminate CBDCs without requiring an

[32] The Glossary to the FATF Standards defines "financial institutions" as any natural or legal person who conducts as a business one or more of 13 specified activities or operations for or on behalf of a customer. Examples of the activities or operations conducted by financial institutions are acceptance of deposits and other repayable funds from the public, lending, money or value transfer service, issuing and managing means of payment, safekeeping and administration of cash or liquid securities on behalf of other persons, and otherwise investing, administering or managing funds or money on behalf of other persons. See the FATF Glossary for the full list of covered activities.

[33] The Glossary to the FATF Standards defines "virtual asset service provider" to mean any natural or legal person who is not covered elsewhere under the FATF Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (1) exchange between VAs and fiat currencies, (2) exchange between one or more forms of Vas, (3) transfer of Vas, (4) safekeeping and administration of VAs or instruments enabling control over VAs, and (5) participation in and provision of financial services related to an issuer's offer and sale of a VA.

[34] The Glossary to the FATF Standards defines "designated non-financial businesses and professions" as (1) casinos; (2) real estate agents; (3) dealers in precious metals; (4) dealers in precious stones; (5) lawyers, notaries, other legal professionals, and accountant; and (6) trust and company service providers which as a business provide specified services to third parties. See the FATF Glossary for the full list of covered activities.

[35] FATF (2020), Annex B, paragraph 94.

account (see Box 1).[36] Where a wallet service provider is an entity (for example, a technical payment service provider) tasked only to provide the necessary software to users, it may not meet the FATF definition of a financial institution, DNFBP, or VASP). In other cases, still, a wallet provider or telecom operator (despite not being a reporting entity) might be tasked to conduct compliance functions (for example, customer identification) on behalf of a financial institution or other AML/CFT reporting entity, with the ultimate responsibility remaining with the outsourcing FI (see the following discussion on third-party reliance and outsourcing arrangements).

Box 1. Approaches to Retail Central Bank Digital Currency Wallets

Although retail central bank digital currencies (rCBDCs) are held in wallets,[37] the term "accounts" is used in many jurisdictions to refer to the arrangement between an rCBDC user and an intermediary (usually, but not always, a financial institution). No prevailing consensus exists on the conceptual distinction between wallets and accounts, and some central banks use the terms interchangeably. For the purpose of this Note, the term "**account**" is used in scenarios in which a customer relationship exists with an intermediary, whereas a "wallet" is used to refer to an application for holding and transacting in CBDC directly. Where the Note is agnostic about the nature of the relationship, it will use the term "*wallet/account*."

Some examples of how different jurisdictions link the opening of rCBDC wallets to the holding of accounts with financial institutions are provided in the following:

- **China—e-CNY (pilot):** Persons can open e-CNY wallets with authorized operators (e.g., banks). This allows them to hold and transact in CBDC through an e-CNY App, without bank accounts. The relationship between the authorized operator and e-CNY holders is governed by contractual agreements. A tiered approach is adopted where the transaction limits and functionalities are implemented in line with the level of risk and customer due diligence undertaken. An e-CNY wallet can also be opened by foreign residents temporarily in China (for example, tourists) to meet their daily payment needs without needing to open a domestic bank account.
- **Eastern Caribbean—DCash (pilot):** Persons who do not have an account with a financial institution can access the lowest tiers of DCash through a "value-based wallet" through an agent authorized by the Eastern Caribbean Central Bank. Persons with an account at a financial institution may access higher DCash tiers through a "registered-based wallet," which is linked to that account. For registered-based wallets, the financial institution is responsible for customer due diligence and determining the threshold for DCash wallet transactions and balances for each user.
- **India—Digital Rupee (pilot):** A bank account is currently required to open a Digital Rupee wallet. The Digital Rupee wallet is linked to the bank account to streamline user onboarding and eliminate the need for additional customer due diligence processes. Additional models for user onboarding are being explored based on feedback and emerging use cases.

[36] Given the ML/TF risks, it is highly unlikely that any jurisdiction would pursue *mass* distribution of CBDCs not linked to an account. Mass distribution of CBDCs would likely be in conjunction with other safeguards (such as CBDCs being distributed and used through accounts).

[37] A CBDC wallet is an interface (for example, an app or hardware) that allows individuals to send and receive CBDCs: BIS (2024a).

Box 1. (Continued)

- **Nigeria—eNaira (launched):** The lowest tiers of eNaira wallets can be accessed by persons without a bank account and are opened with basic information (such as a photograph, telephone number, and national identity number). Bank account holders can access higher tier eNaira wallets which are linked to their bank verification number (a unique identifier for customers in Nigeria's financial system) and require verification of customer information.

Sources: Central Bank of Nigeria (2021, 2023); Eastern Caribbean Central Bank (2021); People's Bank of China (2021); Reserve Bank of India (2025); Virtual roundtable on CBDCs.

Under some rCBDC models, the central bank could undertake activities that prompt AML/CFT obligations under the FATF Standards. This scenario would arise if the central bank conducts for or on behalf of a customer and as a business one or more of the 13 activities listed in the FATF's definition of a "financial institution."[38] A pertinent question would be whether the central bank is undertaking such activities "as a business."[39] Some central banks already have occasional or small-scale retail activities that trigger limited AML/CFT obligations (for example, purchasing coins or banknotes or in the context of issuing securities). In such cases, under domestic laws, although these central banks are required to implement limited AML/CFT controls, they are generally not considered AML/CFT reporting entities or "financial institutions" for AML/CFT purposes.[40] In a CBDC context, the nature and scale of a central bank's retail activities will likely differ significantly from those undertaken at present, but as a public body, it is questionable whether a central bank's activities would be considered commercial in nature. If a central bank meets the FATF definition of a financial institution, based on the activities it carries out, it should be subject to the full range of AML/CFT requirements under the FATF Standards.

Policymakers need to consider the types of service providers in an rCBDC ecosystem and the central bank's role to ensure adequate implementation of AML/CFT preventive measures. Most rCBDC explorations to date aim to preserve much of the current system of intermediation and gatekeeping. All participants in the IMF roundtable with more advanced rCBDC pursuits (that is, launches or pilots) have adopted models with private sector intermediaries being responsible for customer-interfacing functions, including implementation of AML/CFT preventive measures. Variances may nevertheless appear in the future and jurisdictions will need to ensure that there are no gaps in the preventive net.

Advisable practices:

- Jurisdictions should ensure that all actors in the rCBDC ecosystem that qualify as a reporting entity are subject to AML/CFT obligations.

[38] The activities are as follows: (1) Acceptance of deposits and other repayable funds from the public; (2) Lending; (3) Financial leasing; (4) Money or value transfer services; (5) Issuing and managing means of payment (for example, credit and debit cards, cheques, traveler's cheques, money orders and bankers' drafts, electronic money); (6) Financial guarantees and commitments; (7) Trading in: (a) money market instruments (cheques, bills, certificates of deposit, derivatives, and so on); (b) foreign exchange; (c) exchange, interest rate, and index instruments; (d) transferable securities; and (e) commodity futures trading; (8) Participation in securities issues and the provision of financial services related to such issues; (9) Individual and collective portfolio management; (10) Safekeeping and administration of cash or liquid securities on behalf of other persons; (11) Otherwise investing, administering, or managing funds or money on behalf of other persons; (12) Underwriting and placement of life insurance and other investment related insurance; and (13) Money and currency changing.

[39] The FATF Standards do not define the circumstances in which financial institutions conduct activities "as a business." However, FATF guidance in the context of VAs indicates that "as a business" is meant to refer to functions carried out on behalf of another natural or legal person for commercial reasons, and on a sufficiently regular basis. See FATF (2021c).

[40] For instance, the South African Reserve Bank and the Bank of Jamaica.

- Central banks should be prepared to take on ultimate responsibility for AML/CFT compliance where they meet the FATF definition of a financial institution by ensuring they have adequate resources, building capacity, and making the necessary organizational changes (for example, developing a separate compliance department or unit).

Customer Due Diligence

The FATF Standards require all financial institutions, VASPs, and DNFBPs to conduct CDD under certain circumstances. These circumstances include when entering into a business relationship and carrying out some occasional transactions (above a certain threshold). Identification of the customer is a cornerstone of the FATF Standards. Pursuant to R.10 (to which Rs.15 and 23 also refer), CDD measures include identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information; identifying the beneficial owner; and taking reasonable measures to verify the identity of the beneficial owner.

CDD does not only take place at the point of customer on-boarding but should last throughout the business relationship. In addition to identifying the customer, CDD measures include understanding and obtaining information, as appropriate, on the purpose and intended nature of the relationship and monitoring the relationship and transactions to identify activity that is not in line with the intermediary's knowledge of the customer.

Some rCBDC designs are more conducive to CDD than others. An account-based rCBDC, which intrinsically includes a regime for account management, including systems to verify and authenticate users and record the transaction flow, would evoke similarities with present systems (for example, bank accounts) in terms of CDD. In a token-based system, intermediation and wallet/account management are not inherent, so the stage at which CDD is undertaken (for example, at the time of wallet distribution) and the parties responsible for CDD (for example, intermediaries tasked with wallet distribution, account opening, or other customer interfacing roles) must be proactive design choices.

The main aspects of R.10 that raise unique or notable considerations in a CBDC setting are as follows:

a) Prohibition on anonymous accounts

R.10 prohibits financial institutions from keeping anonymous accounts. Anonymous accounts and transactions pose a distinct challenge because they hinder the detection of illicit activity and the tracing/tracking of illicit financial flows. For this reason, the FATF consistently highlights risks associated with anonymity, for example in relation to VAs, owing to their ability to offer users high degrees of anonymity, which can be exploited for illicit purposes.

Two main aspects of the prohibition on anonymous accounts must be considered:

1. **Anonymous:** Although the FATF does not explicitly define the notion of "anonymous," the focus of this prohibition is generally understood as being on the willful concealment or misrepresentation of identity to avoid detection by competent authorities or law enforcement agencies. For the purposes of this Note, the term refers to a state of not being directly identified by name. Unnamed tiers or wallets/accounts would be seen as anonymous unless identifying information that would satisfy CDD requirements could be obtained immediately from a source (likely the onboarding entity).
2. **Account:** The FATF Glossary does not provide any definition for "account" but states that references to "accounts" should be read as "including other similar business relationships

between financial institutions and their customers" (implying that a customer relationship must be present). Whether an rCBDC wallet falls into the definition of account depends on the nature of the relationship (if any) between the wallet provider and the user. From a functional perspective, if a digital wallet functions similarly to a traditional bank account, allowing deposits, withdrawals, and transfers, it may warrant similar regulatory treatment. Another perspective could be whether—in addition to the provision of the wallet software—the wallet service provider is performing any of the activities listed under the FATF's definition of a financial institution (which would imply a customer relationship).

Some privacy preserving features may conflict with the FATF prohibition of anonymous accounts. In the absence of true P2P functionality (transactions among users without the involvement of a reporting entity), rCBDC systems that are designed to have "cash-like" features and require no identification by an intermediary would be highly unlikely to satisfy even the most basic/simplified CDD (SDD) requirements. In some cases, even if no identifying information or self-declaration of name is provided to the intermediary opening an rCBDC wallet/account, identifying information may be available through other channels (for example, through the telecom operator and in the context of mandatory subscriber identity module [referred to as "SIM"] registration frameworks). The use of such information for CDD purposes depends on a number of circumstances and may not always satisfy AML/CFT requirements (see the following section on reliance on third parties and outsourcing arrangements). A straightforward solution would be to allow for P2P transacting (for example, through unhosted wallets); however, jurisdictions should keep in mind the associated risks and conduct the necessary risk assessments prior to pursuing such design features. The FATF has also specifically highlighted as a risk mitigating measure in a CBDC context "limiting the ability for anonymous peer-to-peer transactions."[41] To date, no jurisdiction has pursued true P2P functionality in their rCBDC systems.

The foregoing features also should be considered against comparable existing products, such as prepaid cash cards that allow users to fund and defund the card anonymously within certain parameters.[42] Similar to some privacy features envisioned in CBDCs, prepaid cards also pose risks associated with anonymity at the point of purchase, loading/reloading, and use and often include similar mitigation measures (for example, funding or purchasing limits, reload limits, cash access, and territorial restrictions). Pursuant to a risk-based approach, prepaid cards in some jurisdictions are exempt from CDD where a low level of risk is demonstrated, although prepaid card regimes vary widely across jurisdictions and may bear important distinctions compared to CBDC tiered systems, which are also not uniform in nature[43] (see the following discussion on low-risk products). Jurisdictions may wish to reference similarities and distinctions with existing products in their assessment of the ML/TF risks of any anonymous rCBDC features.

b) Simplified CDD and CDD exemptions

Pursuant to a risk-based approach, jurisdictions should allow and encourage simplified due diligence measures where lower ML/TF risks have been identified based on an assessment of ML/TF risk and can be justified on this basis. The FATF Standards do not specify the exact information that must be collected

[41] The FATF has expressed concerns about products and services that may enable greater transaction anonymity, potentially increasing their appeal for illicit activities. See FATF (2010, 2020), paragraph 93.

[42] Prepaid cards can be funded in various ways with different degrees of CDD including through banks, the Internet, at small retail shops, or at automated teller machines. See FATF (2013).

[43] For instance, applicable thresholds for loading/funding and use vary widely. Different prepaid cards have different permissions and restrictions and involve different types of intermediaries (not in all cases AML/CFT reporting entities). Some prepaid card regimes allow for the total exemption of CDD, whereas others permit only simplified CDD.

in the identification process and allow some flexibility for financial institutions in terms of the type of customer information they collect when starting a business relationship. The Interpretive Note to R.10 clarifies that jurisdictions may establish SDD regimes (entailing less intensive and formal means of information gathering and monitoring) for specifically defined lower risk customers, services, or products. In such cases, SDD measures can be applied (indeed are encouraged) based on a financial institution's institutional risk analysis. Simplified measures should be proportionate to the risk factors and are not acceptable where there is a suspicion of ML/TF.

SDD is often applied to an identified lower risk population or demographic to promote financial inclusion.[44] Examples of possible simplified measures could include, for instance, identifying the customer through a tax card or nonphoto ID and verifying the identity of a customer through information already obtained from the customer, such as official identity documents, provided these give a reasonable level of assurance. Such measures would allow financially excluded individuals access to accounts or other financial services with limited functionalities.[45]

It is important to distinguish between identifying the customer and verifying the customer's identity. SDD does not mean a total exemption from CDD measures (see the following discussion for circumstances under which CDD exemptions may be warranted), but a calibrated approach that includes an identification and verification process that is proportionate to the risk of the customer. In assessed lower risk situations, where SDD is applied, customer identification can be achieved by gathering information on the customer from alternative forms of identification (for example, an expired ID or tax card). In assessed lower risk situations, verification can be delayed or achieved using information already obtained or publicly available.

Less stringent identification and verification can be in line with the FATF Standards if based on proper risk assessment and accompanied by appropriate mitigation measures. For a tiered rCBDC model to satisfy SDD requirements, likely at a minimum, a user would need to self-declare his/her name at the most basic tier. Jurisdictions also need to determine whether a tiered model is appropriate, based on considerations such as the level of risk associated with the customer of the rCBDC and the impact of any mitigating measures that are put in place. For example, SDD may be appropriate for lower-risk customers and activities requiring a CBDC account with basic functionality and safeguards such as transaction and balance limits.

The standards also allow exemption from AML/CFT measures (including CDD) in limited circumstances when it relates to a particular type of activity and the ML/TF risk is assessed to be low.[46] Some rCBDC wallets/accounts may also warrant CDD exemption in limited circumstances, for instance where rCBDC design choices bear resemblance to certain low risk products, where there is an assessed low risk and proportionate mitigating measures are in place. By way of example, parallels may be drawn between close-loop prepaid cards with a cap of the amount that can be loaded and an rCBDC account/wallet with a similar cap and can only be used for payment for goods and services sold by a specific merchant.

[44] FATF (2025b) includes as a lower risk example "financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes." It could be reasonable to apply SDD measures for products fulfilling those conditions "provided that lower risk circumstances have been confirmed, based on a risk assessment, conducted at the national, sectoral or at the [financial institution] level."

[45] Some governments authorize banks to open a "small" or "no frills" savings account for low-income customers lacking acceptable forms of identification, using SDD norms. These types of accounts can be subject to strict limitations on the yearly aggregate of all credits, the monthly aggregate of all withdrawals and transfers, and the balance at any point.

[46] See paragraph 8 of the Interpretative Note to FATF R.1.

Without an assessment of the risks associated with specific thresholds and limits, and possible use cases, the low level of risk attributed to basic the lowest tiers may be too generalized. In most cases at present, the determination of the appropriate holding or transacting amounts is not always based on any assessment of the ML/TF risks associated with tiered models more generally or the specific thresholds and limits more specifically. A risk assessment taking into consideration the applicable user base and likely use cases should inform the thresholds and limits to be applied as well as the necessary mitigation measures.

c) Third-party reliance and outsourcing arrangements

The FATF Standards allow reporting entities to rely on third parties to perform some aspects of their CDD obligations. The FATF Standards envision two ways CDD functions may be externalized. In a third-party reliance scenario (as described in Recommendation 17), the third party is itself an entity with AML/CFT obligations and is subject to regulation and supervision to ensure it complies with them.[47] The third party will usually have an existing business relationship with the customer in question—which is independent from the relationship to be formed by the relying financial institution—and applies its own procedures to CDD measures. In contrast, in an outsourcing/agency scenario, the entity to which CDD tasks are outsourced is not subject to AML/CFT obligations; therefore, the measures they undertake must be in accordance with the relying financial institution's instructions and procedures and subject to the delegating financial institution's control/oversight to ensure that they are in line with AML/CFT requirements.

In both third-party reliance and outsourcing arrangements, the ultimate responsibility for adherence to AML/CFT requirements remains on the reporting entity. In other words, compliance failures on the part of the third-party financial institution or entity to which CDD was outsourced are the responsibility of the relying financial institution. In direct models where a central bank meets the definition of a financial institution, the central bank may choose to rely on commercial banks for CDD under third party reliance, but it would still retain the ultimate responsibility for AML/CFT compliance.

Whether information collected by a non–AML/CFT reporting entity can be used to satisfy CDD obligations depends on several factors, including the information itself and the processes put in place between the collecting institution and the financial institution to ensure all requirements are met. Where the collecting entity is not an AML/CFT reporting entity, the relationship cannot be equated to a third-party reliance arrangement; however, it could be considered to come under an outsourcing/agency agreement where certain conditions are met.

Some rCBDC systems may benefit from outsourcing arrangements, provided that the proper frameworks and procedures required by the FATF Standards are in place. Telecom operators and financial institutions would have to have agreed upon protocols in place, including oversight mechanisms by the financial institution to monitor compliance with such protocols. However, depending on the policy objectives implicated, it may be contrary to the goals of the design choice for the name and documentation on a customer to be made available to a financial institution in all cases; it should be noted that such a model would be problematic for CDD purposes under the current standards.

[47] A financial institution may rely on a third party to identify and verify the identity of a customer, identify the beneficial owner of a customer, and obtain information on the purpose and intended nature of the business relationship if such information is immediately obtained by the financial institutions, adequate measures are taken by the financial institution to assure itself that relevant documentation will be available, and that the third party is regulated and supervised for AML/CFT obligations and has the necessary procedures in place.

d) Payment transparency

FATF R.16 requires basic identifying information on the originator and beneficiary to be collected and shared by financial institutions involved in a cross-border payment or value transfer (sending, intermediary, and receiving).[48] Based on a risk-based approach, jurisdictions may adopt a *de minimis* threshold (no higher than USD/EUR 1,000), below which payments or transfers need to be accompanied by a more limited set of information; such information need not be verified for accuracy unless the intermediary has a specific ML or TF suspicion. For domestic transfers, the accompanying information required can be reduced to the account number or a transaction reference number if other required information can be made available to the beneficiary financial institution and appropriate authorities by other means.[49]

Implementation of requirements for payment or value transfers in an rCBDC context may vary depending on the underlying technology. For models where such information is already contained on the ledger and accessible by relevant parties in the payment chain, it may not need to be transmitted separately. This option would require that financial institutions on both ends of a transfer include certain information on the ledger and for both institutions to have access to that information. As most ledgers are designed to be pseudonymous, CDD information is generally not held on the ledger (see the following section on record keeping). In these instances, the required information will need to be sent by the originating intermediary to the receiving intermediary. How these systems will work in practice will depend on the technological architecture of the CBDC, particularly in a cross-border context where interoperability presents a broader challenge. Messaging platforms or systems could be developed in tandem with wider adoption of CBDC (similar to the synchronicity of SWIFT with current payment systems) or the transmittal of CDD information could more closely resemble—from a technological standpoint—how VASPs comply with Travel Rule requirements under FATF R.15).[50] In all cases, consideration of relevant data protection requirements will need to be considered in order to ensure personal information is safeguarded in line with legislative requirements.

e) Occasional transactions and P2P

The FATF Standards do not require AML/CFT preventive measures to be applied in all financial transactions. For example, CDD is not required for occasional transactions (that is, without an account or similar customer relationship through an intermediary under USD/EUR 15,000, except payments or transfers, for which the threshold is USD/EUR 1,000—see earlier discussion) where no suspicion of ML/TF exists. It is unclear at this stage whether any rCBDC models will include functionality to allow for occasional transactions, but if this option is built into a particular rCBDC model, the same requirements as currently exist within the FATF Standards would need to be met (that is, CDD would be required above the *de minimis* thresholds).

[48] All cross-border payments or value transfers above a *de minimis* threshold must include names of the originator and beneficiary; account or unique transaction reference number of originator and beneficiary; address of originator; beneficiary's country and town; date of birth of any natural person originator; unique official identifier, legal entity identifier, or connected business identifier code of any legal person originator and beneficiary.

[49] Where the information accompanying the domestic wire transfer can be made available to the beneficiary financial institution and appropriate authorities by other means, the ordering financial institution needs only to include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary. The ordering financial institution should be required to make the information available within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.

[50] Regarding compliance with the Travel Rule, see FATF (2021), paragraphs 281–297.

It is also unclear whether P2P payment functionality will be built into any rCBDC models. At present, no true P2P functionality is being seriously explored in a pilot or launch. As such, all transactions are conducted with some involvement by an intermediary. If an rCBDC is designed with cash-like features (for example, it can be physically exchanged between two individuals without the need for a payment platform), it would unlikely be subject to AML/CFT requirements and would generate higher ML/TF risk.

Advisable practices:

- In line with R.10, jurisdictions pursuing rCBDC models that permit unnamed wallets should undertake robust risk assessments to inform system design, including any applicable thresholds/limits and other mitigating measures commensurate with the risks.
- Jurisdictions should ensure that any simplified measures or CDD exemptions are justified based on risk assessments. Where simplified measures are applied, jurisdictions should require—at a minimum—a self-declaration of name.
- Where AML/CFT responsibilities are externalized (by either the central bank or intermediary financial institutions), appropriate governance arrangements need to be established to satisfy the requirements of R.10 and R.17.
- Jurisdictions pursuing tiered rCBDC models that envisage some customer information being collected by nonreporting entities under an outsourcing arrangement should provide guidance to all parties on the proper procedures and protocols to be established to enable fulfillment of AML/CFT obligations.

Targeted Financial Sanctions

The FATF Standards require jurisdictions to implement targeted financial sanctions (TFS) regimes to comply with United Nations Security Council Resolutions related to TF and PF. TFS are aimed at preventing terrorists and terrorist financiers and persons involved in the proliferation of weapons of mass destruction from raising, using, and moving funds. Unlike other AML/CFT obligations, TFS requirements in Rs.6 and 7 (in the form of either obligations to freeze any funds or assets belonging to designated individuals or entities or prohibitions in economic dealings with such individuals or entities) apply to *all* persons in a jurisdiction (not only to reporting entities) and all transactions involving any kind of asset. Although the FATF Standards do not specify sanctions screening as an explicit requirement to implement TFS, sanctions screening (along with additional investigative techniques) is the primary way to implement TFS requirements. It should be further noted that lack of knowledge or intent is generally not a defense to violating TFS obligations.

The most significant challenges anticipated in a CBDC context would likely be similar to those stemming from P2P transactions or offline VA transfers. Currently, in transactions in cash or other economic assets that would not require the involvement of a reporting entity, it is unlikely that parties to the transaction would be conducting sanctions screening (despite being subject to the broad prohibition). In an rCBDC setting, this scenario is most likely to arise where offline functionality or other “cash-like” features are pursued. Depending on the design, rCBDC transfers may also present similar issues to those presented by VA transfers through unhosted wallets. The main issues raised are as follows:

- **Accounts subject to SDD or exempt from CDD:** By their nature, TFS are inextricably linked to the names, aliases, and other identifiers of designated persons and entities. TFS are therefore challenging to implement in rCBDC models that permit customers/users to remain anonymous or be identified in a way other than by name (that is, where aliases or pseudonyms are not linked to a real-world identity). However, unlike the cash or unhosted wallets scenarios described earlier,

all rCBDCs (even those allowing for unnamed wallets/accounts) still involve supervised entities as intermediaries that may find it difficult (or impossible) to comply with their AML/CFT obligations within the parameters of the rCBDC designed by the central bank.

- **Timing of screening**: The FATF Standards require the funds and other assets of designated individuals and entities to be frozen "without delay." Unless a strict limit is set on the amount of time a wallet may be offline, a substantial amount of time could pass before an intermediary detects an unlawful transaction, which would prevent expeditious freezing, diluting the preventive nature of TFS.
- **Offline transactions:** Where offline functionality exists, transactions can be conducted P2P while devices are not connected to the ledger. Realistically, sanctions screening will be conducted only when the devices come back online and are reconciled with the intermediary's ledger. *Ex post facto* detection (while better than no detection) does not stop or prevent a transaction with a designated entity or individual from going through, and the longer it takes for ledger reconciliation, the greater the risk of funds being used for illicit activity.

Joint implementation of TFS by service providers could offer a solution to the challenges faced by intermediaries in models with unnamed tiers. As long as another method could be conceived to allow for the freezing of funds without delay, intermediaries could still be considered in compliance with TFS obligations. For instance, where tiered models are linked to mobile numbers, a regulatory framework potentially could be developed to require mobile operators to immediately notify any financial institutions of positive hits against a sanctions list to allow the financial institution to comply with the freezing obligation without delay. However, as noted earlier, financial institutions would remain responsible for failing to freeze the funds of a designated person where the mobile operator fails to detect a designated individual or entity.

An important consideration is whether TFS shortcomings in CBDC systems will result in misuse of formal financial channels. Although implementation challenges exist in the present financial system (for example, in the context of P2P cash transactions), TFS still generally restrict the access of terrorist and terrorist financiers to formal financial channels. The primary case for the effectiveness of TFS is that—in cutting off access to the regulated (that is, formal) financial system—they force terrorists and terrorist financiers to use slower, more expensive, and less reliable/less secure methods to raise, store, and transfer/move their funds. Where CBDC models allow for unidentified wallets/accounts or for persons to transact unidentified off-line, the probability of sanctions evasion through formal financial channels could increase, potentially raising the level of TF risk.

Advisable practices:

- In jurisdictions pursuing tiered models that permit no or minimal identification other than name, intermediaries should partner with other entities—such as telecom companies—(where warranted by the specific model) to implement TFS (while keeping in mind that intermediaries are not relieved of liability).
- Jurisdictions pursuing offline rCBDC systems should implement measures, such as a requirement for users to connect to the ledger periodically, to prevent undue delays in implementing TFS.
- Along with other mitigating measures, jurisdictions are encouraged to explore technological solutions to prevent wallets/accounts from being misused to circumvent sanctions.

Record-Keeping

FATF R.11 requires reporting entities to retain records of transactions and information obtained from CDD measures. The record-keeping requirement aims to ensure that relevant information is preserved and can be made readily available to competent AML/CFT authorities. Although the FATF Standards provide examples of the types of records obtained through CDD measures that are covered under R.11, this list is not exhaustive. In the context of rCBDCs, this CDD-relevant information could include digital identifiers such as public keys or wallet addresses, which may serve similar functions to account numbers in traditional financial systems.

The implementation of record-keeping obligations within a CBDC ecosystem will be influenced by the design choices underpinning the system. Ledgers can also be designed so that the central bank holds the entire ledger and intermediaries only see a "mirror" of a customer's wallet/account, or intermediaries hold their own sub-ledgers. Depending on the architecture of the ledger, the intermediary may not be the actual record-keeper of some information (for example, on transactions) required to be maintained under the R.11 (in that the central bank—in a centralized ledger scenario—may be the official holder of the information). In practice, this distinction may not have any meaningful consequence as the information is still recorded; however, a question arises as to whether any record-keeping failures (for example, ledger malfunction) would be imputed onto the intermediary.

A direct model presents both institutional and technical record-keeping challenges by placing the central bank at the forefront of record-keeping where it meets the definition of a financial institution.[51] Such a scenario would require a significant expansion of the central bank's mandate and operational capacity. A direct model would more likely amass personal data on the ledger, which may raise data protection and privacy concerns for the central bank (although less so in the case of a pseudonymous ledger).

Regardless of the model, the ledger should be developed with data protection principles (such as the "right to be forgotten") in mind. Although DLTs offer opportunities for robust and tamper-resistant record-keeping, their immutability can also infringe on privacy. To counter these and other privacy concerns, at present, most (if not all) rCBDC ledgers are designed to be pseudonymous, with personal information collected through CDD held privately by intermediaries (as in traditional financial systems).

Advisable practices

- Central banks should understand the implications of the technological infrastructure on record-keeping responsibilities and modalities to identify and undertake necessary legal, regulatory, and technological upgrades that would be needed to satisfy record-keeping requirements. Where the central bank holds the entire rCBDC ledger, it should be equipped with the necessary resources and capacity (human and IT) to meet its record-keeping obligations.
- In considering information-sharing opportunities, for example, broadening access to information on the ledger, jurisdictions should endeavor to protect user data.

Transaction Monitoring and Reporting of Suspicious Transactions

The FATF Standards require reporting entities to report suspicious activity. Under FATF R.20, reporting entities are required to report suspicious activity where reasonable grounds exist to suspect that funds

[51] See the earlier discussion on the circumstances in which a central bank could be considered a financial institution for the purposes of the FATF Standards.

are the proceeds of a criminal activity or are related to TF. In such cases, reporting entities should promptly file a suspicious transaction report to the financial intelligence unit (FIU).

Methods for transaction monitoring in the CBDC setting will likely closely resemble current practices in intermediated models. Intermediaries should monitor transactions on an ongoing basis to determine whether the transactions being conducted are consistent with the intermediary's understanding of the customer, their business, and risk profile, and to identify suspicious transactions (including attempted transactions).[52] CBDC intermediaries will likely heavily rely on automated monitoring systems which employ machine learning and other technologies to analyze large volumes of transactional data and identify anomalies in behavior that indicate suspicious activity, based on predefined rules, algorithms, and pattern recognition techniques.

Although there may not be a radical shift in the methods for transaction monitoring, additional challenges may arise in rCBDC arrangements in direct models, particularly those which allow for anonymity or pseudonymity and those with offline functionality:

- **Direct models:** As with other AML/CFT preventive measures, the obligation to report suspicious transactions will, in most cases, be a novel one for central banks meeting the definition of a financial institution in direct distribution systems. The central bank may have limited or no institutional capacity for monitoring transactions, and in addition to the need to acquire monitoring systems, may need to build the capacity of relevant staff to detect and report suspicious transactions.
- **Basic wallets/accounts with limited information:** Some rCBDC arrangements may permit lower risk users to open wallets/accounts with very limited identification requirements (for example, provision of a mobile number only with the knowledge that the mobile number is registered to an individual by the telecom company). In such scenarios, and in line with existing FATF Standards, the intermediary would have to have procedures in place to obtain additional information on the wallet owner should this be needed.
- **Offline functionality:** ML/TF risks relating to offline functionality have been identified by central banks as among the most significant.[53] Offline functionality may affect the availability of transaction records and the integration of verification systems to prevent double-spending and counterfeiting (Reserve Bank of New Zealand 2021Financial Intelligence Unit of Latvia 2023; Bank of England 2025, p. 22, fn. 40). Offline wallets could offer higher levels of privacy in scenarios where the connected transactions would not be recorded on a shared ledger but solely saved in the device, which would essentially transform the CBDC into a digital bearer instrument. Measures currently being explored by central banks to mitigate these risks include holding limits, velocity limits, value limits, and identification of the user at funding and defunding. In addition, since reconciliation of offline transactions with the intermediary's ledger will take place once one or both wallets are back online, there is the possibility of some delay in the detection of suspicious transactions, which as a consequence, will affect the time that will elapse before the intermediary can form a suspicion of ML/TF that should be reported to the FIU. Measures to address this risk could include limits on the time that may elapse or the number of transactions that may be conducted before the wallets have to go online. However, these mitigating measures are effective only when wallets eventually go back online.

[52] FATF R.10 and Interpretive Note to FATF R.10.

[53] See BIS Innovation Hub, Central Bank Survey on Offline Payments with CBDC, Annex 2, BIS (2023b).

Notwithstanding these challenges, rCBDCs present potential opportunities to enhance transaction monitoring by intermediaries. For example, the approaches from existing private and public sector initiatives for data pooling and collaborative analytics could be applied to rCBDC explorations. Where legally permitted, intermediaries may enter into agreements to share and collectively monitor CBDC transaction data across their ledgers, which can improve the detection of suspicious activity, drawing on a more complete pool of data (see Box 2).[54] Some jurisdictions are considering the most effective means of balancing transaction monitoring and other potential mitigants with privacy protection.

Advisable practices**:**

- Jurisdictions pursuing tiered models that permit wallets with minimal or no identification should take measures to facilitate the detection of suspicious transactions, such as requiring CDD when the wallet is involved in an unusual transactions and prohibiting such wallets from remaining in the low tier minimal identification status.
- Jurisdictions pursuing offline rCBDC systems should facilitate timely detection of suspicious transactions by requiring users to connect to the ledger periodically.

Anti–Money Laundering/Combating the Financing of Terrorism Supervision

Effective AML/CFT supervision of the rCBDC ecosystem is essential for maintaining the integrity of the financial system**.** Pursuant to Rs.15, 26, and 28, jurisdictions should ensure that financial institutions, DNFBPs, and VASPs are subject to adequate regulation and AML/CFT supervision/oversight. Supervisors should also have adequate powers to monitor compliance and impose a range of disciplinary and financial sanctions on institutions that fail to meet their obligations (including the power to withdraw, restrict, or suspend the financial institution's license, where applicable) (R.27).

AML/CFT supervision in intermediated rCBDC models will be largely identical to AML/CFT supervision in the current financial system, although, as for any other payment service provider, regulators and supervisors should be cognizant of any new service providers (or existing service providers newly taking on AML/CFT obligations). Where new service providers emerge, supervisory frameworks and systems may need to be updated.

Direct rCBDC models pose the most unique supervisory considerations and challenges. In such a model, if the central bank meets the definition of a financial institution, it would need to comply with AML/CFT obligations (see the "AML/CFT Preventive Measures" section) and be subject to AML/CFT supervision. The following challenges are envisioned:

- **Conflicts of interest:** Both direct and hybrid rCBDC models pose potential conflicts of interest for AML/CFT supervisors, especially where AML/CFT supervisors are a part of the central bank itself. Tensions could arise between promoting financial inclusion and innovation through CBDCs and safeguarding against illicit financial activities. Any conflicts of interest must be addressed through the establishment of clear governance frameworks and potential organizational restructuring to separate the central bank's respective (and potentially competing) roles. For example, a separate department or ringfenced entity could be created within the central bank, similarly to some FIUs that are established in central banks or AML supervisors. Supervisory

[54] See examples of approaches that could be adapted to a CBDC setting in FATF (2021b), Box 4.1: United Kingdom Tribank pilot; Box 4.2: Japan proof of concept on machine learning and artificial intelligence, and Box 4.4: Transaction Monitoring Netherlands initiative.

functions must be able to perform their duties without undue influence relating to financial innovation or business-motivated priorities.

- **Challenges to central bank independence:** Central banks enjoy strong law-mandated independence. If a central bank becomes a reporting entity under the AML/CFT regime, it would be subject to AML/CFT oversight (including the imposition of sanctions for noncompliance). Becoming a reporting entity may also expose the central bank to new reputational risks stemming from compliance failures. A clear framework would need to be established to allow for oversight of central bank compliance in accordance with Rs.26 and 27 without infringing on its autonomy; however, allowing for this type of oversight of the central bank may not be permitted under many domestic regimes. Even where appropriate safeguards are in place, the possibility of imposing penalties on the central bank (if legally permitted) for AML/CFT regulatory breaches creates a risk of undermining its independence. Sanctions, especially in jurisdictions with weak rule of law and pervasive corruption, could become a form of retaliation and undue political pressure. Where sanctions on the central bank are not possible in a direct model, the requirements of R.27 cannot be satisfied.

Cross-border rCBDCs may result in regulatory and supervisory gaps. As with present-day international payments, regulatory arbitrage and inconsistent enforcement of AML/CFT obligations could occur in the case of widespread cross-border rCBDC adoption. As these problems are likely to be similar to existing challenges in multijurisdictional contexts (for example, multinational banks, VASPs), supervisors can, along with building their capacity, draw inspiration from existing solutions, such as mechanisms to foster supervisory coordination, similar to how bank supervisors from multiple jurisdictions collaborate to oversee multijurisdictional financial institutions (for example, group supervision and supervisory colleges).

Advisable practices:

- Central banks considering a direct rCBDC model should address any conflicts of interest by establishing clear governance frameworks to separate the central bank's potentially competing roles as an AML/CFT-obliged entity and supervisor.
- Jurisdictions may also need to update their legal and regulatory frameworks to allow for external oversight of the central bank, depending on the model.

Criminal Enforcement

The FATF Standards prescribe the law enforcement measures that jurisdictions should take to combat ML and TF effectively and recover the proceeds of crime: criminalization of ML and TF (Rs.3 and 5), investigation and prosecution of ML and TF activities (Rs.30, 31, 32), freezing, seizing, and confiscating proceeds and instrumentalities of ML and underlying criminal activity (R.4), and cooperation with foreign counterparts (Rs.36 to 40). The requirements contained in the aforementioned Recommendations apply regardless of the type of asset involved and should apply to activities in CBDCs.

Actions such as freezing and seizing digital assets and stopping or reversing transactions may require direct access to the rCBDC ledger and the authority to intervene in wallet operations—capabilities that can be granted to any authority in a centralized system at the design phase, but likely to be vested only to the central bank or designated administrators. If a system allows law enforcement agencies and other competent authorities to have direct access to the ledger (for example, by creating a node for certain law enforcement bodies), legislative clarity about when and how such interventions can occur would be needed, as well as technical interoperability between law enforcement systems and the CBDC

infrastructure. In such systems, rule of law weaknesses can be particularly harmful where safeguards are not in place or not adequately implemented. In cases where law enforcement bodies do not have direct access to the ledger, jurisdictions need to designate the central bank as a competent authority to intervene in wallet operations or implement mechanisms for the central bank to take such actions as an agent of law enforcement authorities.

Depending on the rCBDC design, closer cooperation between the central bank and law enforcement authorities may be required. Law enforcement and prosecution agencies as well as the courts often require specific information (for example, identification documentation) or measures (for example, freezing a wallet/account) from intermediaries for the purposes of their investigations and prosecutions. In an indirect or intermediated rCBDC model, they would (continue) to request that information from the intermediaries that play the customer-interfacing role and hold the relevant information. In a direct rCBDC model, however, the central bank would step into the role of having to respond to requests from law enforcement authorities, both domestic and international. In the roundtable, rCBDC explorations were divided along those that put the locus of control in the central bank (who would have the authority to freeze, seize, stop transactions, and so on) and those that prefer to remain closer to the current state of affairs (with commercial entities being charged with the function to freeze, seize, or stop transactions). In all cases, participants noted that current due processes and legal requirements would apply.

Advisable practices:

- Central banks may need to establish mechanisms for information sharing with law enforcement, depending on the record-keeping system.
- Jurisdictions should consider opportunities to build measures into the technological infrastructure to better facilitate the freezing, seizing of criminal assets held as rCBDCs.
- Where law enforcement authorities are granted rights directly on the ledger, safeguards need to be put in place to ensure due process.

Depending on the specific design features adopted, rCBDCs could introduce new procedural and technological challenges as well as opportunities. In a fully decentralized system, competent authorities would have limited ability to exercise control over the ledger. This notably means that they would have limited capacity to stop or reverse transactions or freeze assets, as such actions—if even possible—could only be done with the consensus of all operators on the ledger. Centralized and semi-centralized ledgers would provide the governing body the ability to take these actions alone or in tandem with operators (either other public authorities as well as private sector intermediaries or other service providers) (see Box 2).

Box 2. Opportunities to Facilitate Anti–Money Laundering/Combating the Financing of Terrorism Compliance

Retail central bank digital currencies (rCBDCs) could offer opportunities for enhanced transaction monitoring:

- **A unified CBDC ledger** (one that is not partitioned) could enhance transaction monitoring by expanding the set of available information (from information on transactions held by individual institutions to all transactions captured on the central bank ledger), improving monitoring accuracy. The extent of information available will depend on the ledger design and whether the central bank would hold the entire ledger or only the wholesale ledger. Access to and use of information held on the ledger also must be subject to applicable data protection rules and principles.

Box 2. (Continued)

- **Direct access to a unified ledger by competent authorities** could enable them to directly analyze the information on the ledger to identify suspicious transactions/patterns promptly, without waiting on suspicious transaction reports from the designated intermediaries. If necessary, the authorities could then seek further identifying information on the owner of the specific wallet/account from the relevant intermediary. This opportunity will depend on the access rights granted to various parties, including competent authorities (to be determined at the design stage). Where access rights are granted to a broader set of authorities, applicable procedural safeguards, including to ensure data protection, should be built into the design.

Unified ledgers holding information from all intermediaries offer opportunities for more efficient data sharing. The recordkeeping structure of rCBDCs could improve customer due diligence (CDD) processes and streamline data sharing by reducing redundancies and duplication resulting from the collection of the same set of information on customers by multiple financial institutions (for example, through the use of a "Know Your Customer token"). Limitations would depend on ledger design (how much information is recorded on the ledger and what parties may access this information). The quality of the underlying data is also key;

where inadequate CDD regimes are in place, or where reporting entities are not sufficiently supervised for carrying out anti–money laundering/combating the financing of terrorism (AML/CFT) preventive measures, CDD systems would not be improved by the sharing and increased availability of inaccurate or incomplete information. Rigorous discrepancy reporting mechanisms should be in place to ensure accuracy and quality of data.

The digitalization of financial transactions, including through CBDCs, may pave the way for the "automation" of certain AML/CFT requirements. Having all financial transactions executed in a single digital environment, under the control of a public authority, could enable policymakers—depending on the rCBDC design—to encode regulations in the underlying architecture of the CBDC (for example, by writing regulatory requirements directly into a smart contract) to facilitate compliance-by-design with some AML/CFT requirements (and potentially also in other fields such as tax collection). Programmable compliance mechanisms could improve effectiveness and transparency and reduce costs.

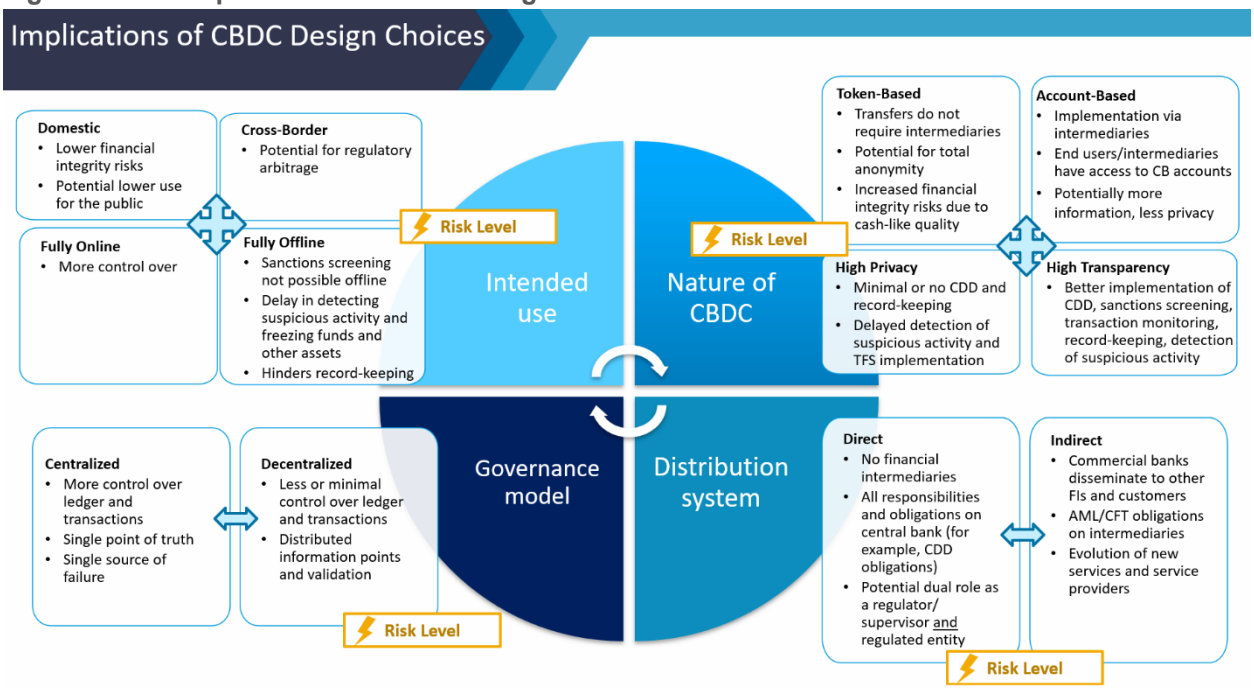
Although compliance-by-design mechanisms present opportunities, these initiatives should not be considered a panacea or a silver bullet to compliance challenges. Similar initiatives (for example, "e-Know Your Customer" regimes) have been pursued for existing payment services and have not been demonstrated to be effective in all cases. The compliance solutions described here have not been tested in all cases and are not endorsed by the IMF and more research in this area is needed.

Source: Authors' analysis.

Conclusion

Although rCBDC usage is still limited, it is clear that the financial integrity implications vary greatly depending on the specific design choices adopted. Some design features present inherently more risk to financial integrity than others. Pure token-based models inherently present higher ML/TF risks than pure account-based models because they do not intrinsically include any aspects of account management; however, with the proper mitigation measures (for example, ensuring that the distribution of tokens is linked to wallets that require customer identification), such risks can be effectively managed. Highly decentralized and permissionless systems could present higher risks to financial integrity because there is less control vested in the central bank and other authorities; however, highly centralized systems may not yield some of the benefits and solutions that innovative technological solutions can offer. A pure direct, un-intermediated rCBDC model envisions a significant disruption to the current financial system by placing the central bank at the forefront of AML/CFT preventive measures, whereas an indirect, intermediated system leverages existing infrastructure (but may perpetuate existing weaknesses) and more closely aligns with current policy and standards frameworks. Offline and privacy-preserving features may undermine some aspects of CDD and ML/TF risk mitigation. Figure 1 summarizes where the higher ML/TF risks might lay.

Figure 1. Risk Implications of CBDC Design Choices



Source: Authors.

Note: Design features that present higher risks are denoted by "Risk Level." AML/CFT = anti–money laundering/combating the financing of terrorism; CBDC = central bank digital currency; CDD = customer due diligence.

rCBDCs do not operate in a vacuum. Existing weaknesses and vulnerabilities in a country's AML/CFT framework will likely be perpetuated and even exacerbated. Jurisdictions should therefore endeavor to rectify their main AML/CFT deficiencies prior to issuing an rCBDC. Similarly, existing strengths will

continue to exist and should be leveraged. When designing an rCBDC, jurisdictions should take into consideration the totality of their circumstances and design a CBDC that capitalizes on their strengths and will not worsen existing shortcomings.

Implementation of AML/CFT measures pursuant to the FATF Standards may present novel challenges for issuing jurisdictions. Although some aspects of the FATF Standards will be implemented in a similar or identical manner as in traditional financial systems, others (namely, the ones discussed in this Note) may prove more challenging to implement in light of the complexity of rCBDCs (for example, the risk assessment) or raise new questions in the interpretation of the FATF Standards (for example, the notion of "account" in an rCBDC setting). They may require the international community to revisit the current approach to rCBDC design or global AML/CFT efforts. rCBDCs could also offer an opportunity to recalibrate some aspects of existing financial systems.

Ultimately, rCBDCs may raise questions about the desired nature of financial intermediation and AML/CFT prevention. Under the current FATF Standards, AML/CFT responsibilities are delineated between private sector and competent authorities, with the private sector being responsible for applying AML/CFT preventive measures and competent authorities being responsible for regulation, supervision, and enforcement. In indirect models, historic patterns of intermediation and compliance would remain; however, in direct models, central banks would step into the gatekeeping role. Even in intermediated models where the central bank outsources or delegates customer interfacing functions, it may meet the FATF definition of a financial institution and, as such, would retain the ultimate responsibility for implementing AML/CFT requirements regardless of any delegated/outsourced functions.

Even where a central bank does not assume AML/CFT obligations, the nature of its relationship with intermediaries in an rCBDC system affects the nature of intermediation. Where central banks legally hold the wallets/accounts of users and are in control of executing transactions in an indirect model, intermediaries may develop a different type of relationship with end users. In some intermediated rCBDC models, intermediaries might act as gatekeepers in the truest sense of the word (not having any control over customer wallets/accounts or funds, simply providing a vetting service whereby instructions from cleared customers are sent through to the ledger for processing). In such cases, challenges in effective implementation of AML/CFT preventive measures may arise.

At present, under existing rCBDC designs, all transactions are subject to AML/CFT measures as they are conducted through wallets/accounts held with regulated intermediaries. In the case of mass adoption where rCBDC becomes the primary form of central bank money for retail payments, there would be virtually no space for unmonitored and unidentified transactions under current CDD rules if all CBDC activities are to be channeled through an intermediary. Although "cash-like" features (such as privacy in transacting and P2P transacting) may not currently be a priority for every jurisdiction, these features may become more desirable in the context of widespread adoption. Unless true P2P functionality—such as unhosted wallets similar to those in the VA context or CBDC vouchers similar to prepaid cards—is incorporated into an rCBDC system, "cash-like" features are likely to not only create practical challenges for the risk-based implementation of AML/CFT measures but potentially result in a financial system where very little space exists for transactions to fall outside the AML/CFT remit (at the moment, proportionally less transactions in traditional forms of fiat are subject to AML/CFT controls).

rCBDCs may require reconsideration of some broader policy objectives, for instance those relating to cash and P2P activities. Although some jurisdictions may embrace technological advancements that

allow for more private and secure transacting, others may see CBDCs as an opportunity to eliminate (or greatly reduce) ML/TF and other risks associated with cash usage. Although P2P functionality is not presently being pursued by any jurisdiction with a pilot or launch, jurisdictions may consider this as an alternative or complement to other "cash-like" features (such as unnamed wallets/accounts in a tiered system). Broader policy questions, such as the role and desirability of cash in the economy may come to the forefront as rCBDC explorations advance. Policymakers may wish to consider whether P2P transactions (similar to cash transactions in fiat currency) should be replicated in a CBDC setting or whether they should be minimized or eradicated.

Central banks should ensure that their CBDC does not create substantial new loopholes that criminals or terrorists could easily exploit (for instance, where a CBDC offers anonymity normally afforded only by cash transactions). AML/CFT measures should be commensurate with ML/TF risks; the FATF Standards are both prescriptive and nonprescriptive in that they set out a set of rules and principles but allow for flexibility in the manner of national implementation. Application of the FATF Standards may pose unique challenges and considerations not currently faced with existing products. Table 3 proposes some good practices to support effective application of the FATF Recommendations in a CBDC environment.

As the situation stands, central banks may benefit from further clarity on how specific aspects of international AML/CFT standards can be effectively applied to CBDCs. Virtual roundtable participants agreed that the application of the FATF Standards in a CBDC setting is not always clear. Questions remain on: (1) the proper role of the central bank vis-à-vis intermediaries and whether the nature of AML/CFT gatekeeping may change; (2) whether certain AML/CFT obligations may need to be adjusted to account for the design and technological realities of rCBDCs; (3) whether any rCBDC models can build in certain "cash-like" features (to serve other policy objectives such as preserving privacy and financial inclusion) and not run afoul of the FATF Standards; (4) how to effectively carry out certain AML/CFT measures, such as TFS and suspicious transaction reporting, in the context of unnamed/unidentified wallets/accounts and offline functionality; (5) how to properly carry out risk assessments of rCBDCs given their novelty and the new role of a public body in designing a new product and delivery channel; and (6) the kinds of technological opportunities that can or should be leveraged to facilitate AML/CFT compliance and ML/TF risk mitigation. Table 3 sets out the specific issues where—given the still early stages of global rCBDC development—concrete answers are not yet available.

Advisable Practices in Applying the Financial Action Task Force Standards to Central Bank Digital Currencies

Although international best practices are still developing, some advisable practices for implementing the FATF Standards in the CBDC context can already be identified. The advisable practices listed in Table 3 are intended to complement and aid in issuing jurisdiction's implementation of the FATF Standards in a CBDC setting.

Certain aspects of international AML/CFT standards may require further clarification to support their effective application to CBDCs. Open questions identified through the analysis in this Note are included in Table 3. Although many of the open questions listed in the following could benefit from views by the FATF (as the international standard setting body for AML/CFT purposes), these questions likely cannot be resolved by any single international body and will need the involvement of national policymakers and stakeholders as well.

Table 3. Advisable Practices and Open Questions

Advisable Practices for Implementing the FATF Standards in the CBDC Context		Open Questions
Risk-Based Approach		
Assessing the ML/TF risks and applying a risk-based approach to rCBDCs	Prior to launching an rCBDC, jurisdictions should conduct ML/TF risk assessments taking into account the intended user base and use cases to inform the rCBDC design choices and drive the implementation of appropriate mitigating measures. Risk assessments should be ongoing or recurrent, consider new information or data gathered in the context of pilots or other trials, and involve all relevant stakeholders, including intermediaries and key competent authorities. ML/TF risk assessment may be complex so jurisdictions should allow for sufficient time and resources. Consideration should be given to the jurisdiction's broader ML/TF risk and context, including the inherent risks and vulnerabilities associated with other parts of the financial system when designing an rCBDC.	In the context of rCBDCs, to what extent should risk assessment and mitigation take place at the level of the issuer vis-à-vis the level of the financial institution offering such products and services to end users?
Preventive Measures		
Role of the central bank and intermediaries	(1) Jurisdictions should ensure that all actors in a CBDC ecosystem that qualify as an AML/CFT reporting entity are subject to AML/CFT obligations. (2) Central banks should be prepared to take on ultimate responsibility for AML/CFT compliance where they meet the FATF definition of a financial institution by ensuring they have adequate resources, building capacity, and making the necessary organizational changes (for example, developing a separate compliance department or unit).	Given that the nature of intermediation may change, should central banks qualify as a financial institution as defined in the FATF Glossary and be subject to AML/CFT measures, and if so, under what circumstances? Should any AML/CFT obligations for reporting entities be adjusted or differentiated based on the potentially changing nature of intermediation and the technological realities posed by rCBDCs?
CDD	In line with R.10, jurisdictions pursuing rCBDC models that permit unnamed wallets should undertake robust risk assessments to inform system design, including any applicable thresholds/limits and other mitigating measures commensurate with the risks. Jurisdictions should ensure that any simplified measures or CDD exemptions are justified based on risk assessments. Where simplified measures are applied, jurisdictions should require—at a minimum—a self-declaration of name. Where AML/CFT responsibilities are externalized (by either the central bank or intermediary financial institutions), the necessary protocols and procedures	What type of customer information would be needed to satisfy minimum (that is, the most simplified) CDD requirements in an rCBDC context? Should a more limited role in intermediation be accompanied by reduced or modified CDD obligations? Should some CDD obligations (such as identification of customers and ongoing monitoring) be shared with the central bank given its more prominent role or satisfied by technological solutions?

	need to be established upfront to satisfy the requirements of R.10 and R.17. Jurisdictions pursuing tiered models that would envision some customer information being collected by nonreporting entities under an outsourcing arrangement should provide guidance to all parties on the proper procedures and protocols to be established to enable fulfillment of AML/CFT obligations.	For the purpose of applying CDD and the prohibition against anonymous accounts, do rCBDC wallets qualify as "accounts" for the purposes of the FATF Standards in all cases, and if not, what are the circumstances that would warrant treating a wallet as an account? Given the similarities CBDCs bear to both fiat and VAs, should the thresholds for identification and reporting be adjusted in a CBDC context?
Implementation of TFS	In jurisdictions pursuing tiered models that permit no or minimal identification other than name, intermediaries should partner with other entities—such as telecom companies—(where warranted by the specific model) to implement TFS (while keeping in mind that intermediaries are not relieved of liability). Jurisdictions pursuing offline rCBDC systems should implement measures, such as requiring users to connect to the ledger periodically, to prevent undue delays in implementing TFS. Along with other mitigating measures, jurisdictions are encouraged to explore technological solutions to prevent wallets/accounts from being misused to circumvent sanctions.	How can TFS be adequately implemented in models with unnamed wallets/accounts (if such arrangements are deemed acceptable, see discussions on CDD earlier) or offline functionality?
Record-keeping	Central banks should understand the implications of the technological infrastructure on record-keeping responsibilities and modalities to identify and undertake necessary legal, regulatory, and technological upgrades that would be needed to satisfy record-keeping requirements. Where the central bank holds the entire rCBDC ledger, it should be equipped with the necessary resources and capacity (human and IT) to meet its record keeping requirements. In considering information-sharing opportunities, for example, broadening access to information on the ledger, jurisdictions should endeavor to protect user data	As there may be rCBDC systems where some information (such as on transactions) is kept on the ledger managed by the central bank or third parties, should some record-keeping responsibilities be shared by parties managing the ledger, and how should liability/responsibility be assigned in the event of record-keeping failures on the ledger?
Reporting of suspicious transactions	(1) Jurisdictions pursuing tiered models that permit wallets with minimal or no identification should take measures to facilitate the detection of suspicious transactions, such as requiring CDD when the wallet is involved in an unusual transactions and prohibiting such wallets from remaining in the low tier minimal identification status; (2) Jurisdictions pursuing offline	Should jurisdictions prescribe risk-based holding limits, velocity limits, value limits, and stipulate a maximum period for offline wallets to stay unconnected to the ledger before transacting again.

	rCBDC systems should facilitate timely detection of suspicious transactions by requiring users to connect to the ledger periodically.	
Risk mitigating design features	Jurisdictions are encouraged to explore building mitigating measures, including through technological solutions, into the rCBDC design.	As a policy question, should jurisdictions build features into their rCBDC that facilitate or automate compliance with AML/CFT requirements (such as automatic asset freezing for TFS purposes)?
Supervision		
AML/CFT supervision	Central banks considering direct rCBDC models should address any conflicts of interest by establishing clear governance frameworks to separate the central banks potentially competing roles as AML/CFT obliged entity and supervisor. Jurisdictions may also need to update their legal and regulatory frameworks to allow for external oversight of the central bank, depending on the model.	Where central banks assume AML/CFT obligations, how should AML/CFT oversight be reconciled with central bank independence?
Criminal Enforcement		
ML/TF enforcement measures	Central banks may need to establish mechanisms for sharing information with law enforcement, depending on the record keeping systems. Jurisdictions should consider opportunities to build measures into the technological infrastructure to better facilitate the freezing, seizing of criminal assets held as rCBDCs. Where law enforcement authorities are granted rights directly on the ledger, safeguards need to be put in place to ensure due process.	What kinds of mechanisms should be in place to facilitate central bank and law enforcement coordination/cooperation in an rCBDC context? As a policy question, should law enforcement agencies be granted certain permissions on the ledger?

Source: Authors.
Note: AML/CFT = anti–money laundering and combating the financing of terrorism; CBDC = central bank digital currency; CDD = customer due diligence; FATF = Financial Action Task Force; ML/TF = money laundering/terrorism financing; rCBDC = retail central bank digital currency; TFS = targeted financial sanctions; VA = virtual assets; VASP = virtual asset service providers.

Annex I

Annex Table 1.1 Financial Action Task Force (FATF) Recommendations

FATF Rec	Anticipated level of challenges in adapting the FATF Recommendations to Central Bank Digital Currencies (CBDCs) Minimal Moderate or Significant
1	Assessing risks and applying a risk-based approach
2	National cooperation and coordination
3	Money laundering offense
4	Confiscation and provisional measures
5	Terrorist financing offense
6	Targeted financial sanctions related to terrorism and terrorist financing
7	Targeted financial sanctions related to proliferation
8	Nonprofit organizations
9	Financial institution secrecy laws
10	Customer due diligence
11	Record-keeping
12	Politically exposed persons
13	Correspondent banking
14	Money or value transfer services
15	New technologies
16	Payment transparency
17	Reliance on third parties
18	Internal controls and foreign branches and subsidiaries
19	Higher-risk jurisdictions
20	Reporting of suspicious transactions
21	Tipping-off and confidentiality
22	DNFBPs: customer due diligence
23	DNFBPs: other measures
24	Transparency and beneficial ownership of legal persons
25	Transparency and beneficial ownership of legal arrangements
26	Regulation and supervision of financial institutions
27	Powers of supervisors
28	Regulation and supervision of DNFBPs
29	Financial intelligence units
30	Responsibilities of law enforcement and investigative authorities

31	Powers of law enforcement and investigative authorities
32	Cash couriers
33	Statistics
34	Guidance and feedback
35	Sanctions
36	International instruments
37	Mutual legal assistance
38	Mutual legal assistance: freezing and confiscation
39	Extradition
40	Other forms of international cooperation

Source: Authors.

Annex II

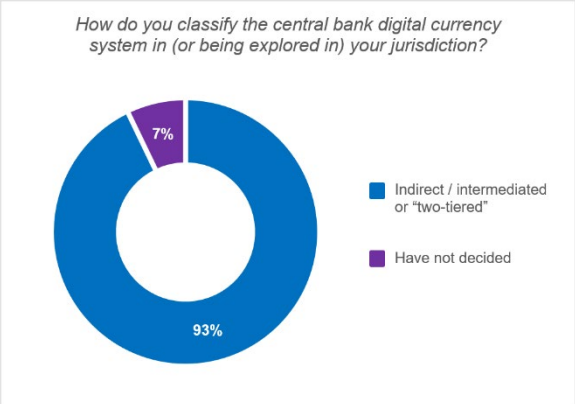
Virtual Roundtable on Retail Central Bank Digital Currencies

This Annex presents key takeaways from a virtual roundtable on the financial integrity implications of central bank digital currencies (CBDCs) convened in January 2025 by the IMF Legal Department (Financial Integrity Division). The roundtable comprised participants from central banks and other relevant agencies from 14 jurisdictions and regional bodies[55] at various stages of an rCBDC issuance, pilot or exploration, as well as representatives from other IMF departments and the FATF Secretariat. Participants shared their practical experiences regarding the financial integrity implications of retail CBDCs (rCBDCs), informed by their involvement in designing and developing rCBDCs, as well as anti–money laundering/combating the financing of terrorism (AML/CFT)/counter-proliferation financing (CPF) policymaking, regulation, and supervision. They also completed a survey on their rCBDC systems and explorations. This Annex summarizes key insights from the discussions and presents the survey results (depicted in the figures contained in this Annex).

Distribution Model and Ecosystem

Most participants in the CBDC roundtable reported pursuing intermediated rCBDCs, reflecting global trends (Annex Figure 2.1).

Annex Figure 2.1 Distribution Model

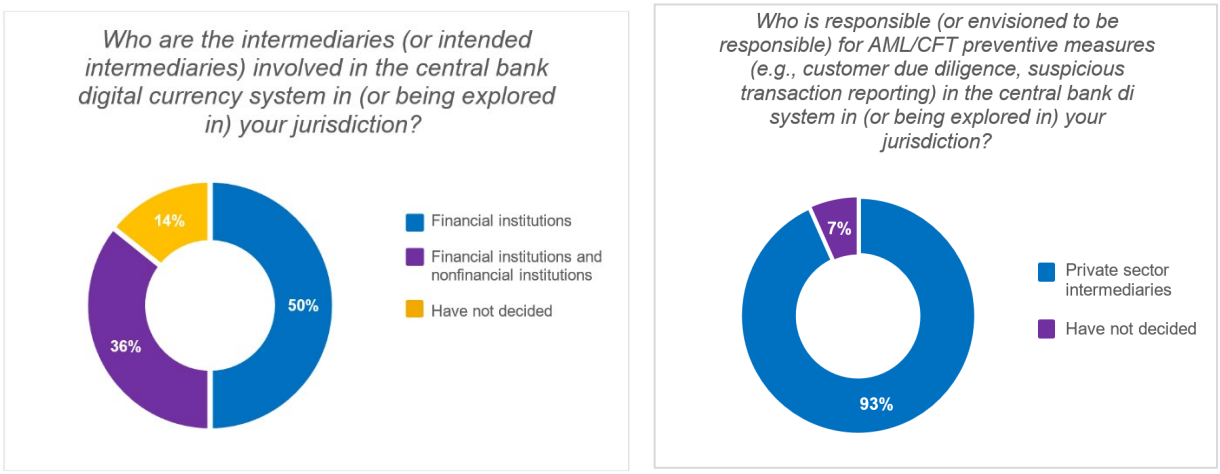


Note: CBDC = central bank digital currency.

Roundtable participants generally adopted models where responsibility for the application of AML/CFT preventive measures rested with licensed financial institutions. Half of the roundtable participants were considering permitting only financial institutions as CBDC intermediaries, whereas over a third envisaged a mix of financial and nonfinancial institutions as intermediaries (Annex Figure 2.2). Some participants expressed openness to including intermediaries such as telecom operators that do not traditionally have AML/CFT responsibilities, but which potentially tap into large customer bases. In such cases, some participants noted that entities could partner with licensed financial institutions for the application of AML/CFT preventive measures.

[55] The Bahamas, China, the Eastern Caribbean Central Bank, the ECB, Ghana, Hong Kong SAR, Japan, Kazakhstan, Morocco, New Zealand, Nigeria, Sweden, Türkiye, and one jurisdiction that prefers to remain unnamed.

Annex Figure 2.2. Intended Intermediaries and Allocation of Responsibility for AML/CFT Preventive Measures

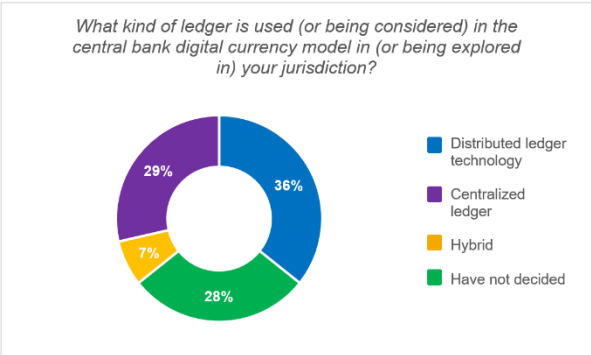


Source: Survey results from virtual roundtable on rCBDCs.
Note: AML/CFT = anti–money laundering/combating the financing of terrorism; CBDC = central bank digital currency.

Infrastructure and Governance

Over a third of roundtable participants represented jurisdictions that employed a distributed ledger (for example, distributed ledger technology), although still with a more centralized mode of governance. There was almost an even number of participants that were still deciding on their ledger infrastructure, and those employing a centralized ledger as well as a centralized form of governance, which includes vesting the power to mint, issue, and destroy CBDCs as well as administrative control over the ledger with the central bank. In a limited number of cases, jurisdictions were exploring systems with both centralized and decentralized features. No participants reported exploring fully decentralized or permissionless systems (Annex Figure 2.3).

Annex Figure 2.3. Ledger Infrastructure

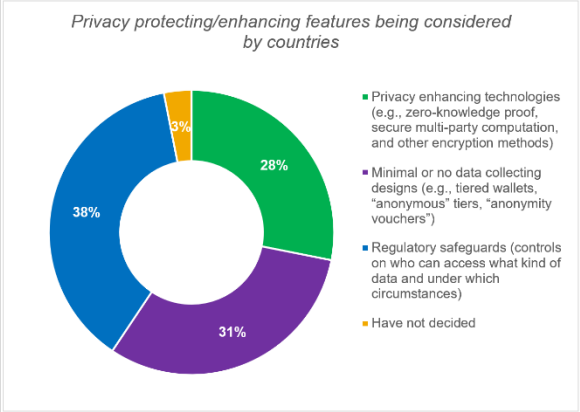


Source: Survey results from virtual roundtable on rCBDCs.
Note: CBDC = central bank digital currency.

Central Bank Digital Currency Features

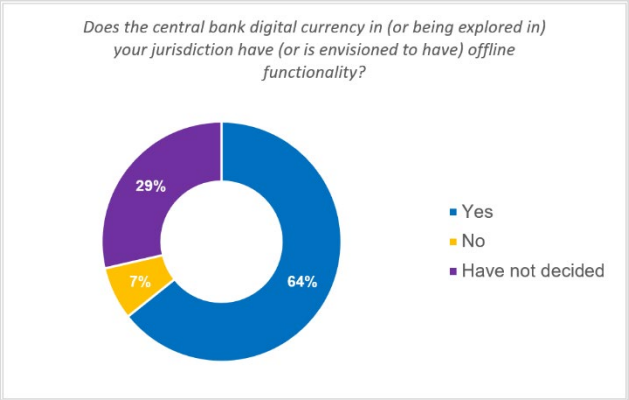
- **Privacy: Although no country is pursuing a fully anonymous CBDC, various privacy protecting or privacy enhancing features are being considered in CBDC designs.** These include privacy enhancing technologies, minimal or no data collecting designs, and regulatory safeguards. Most roundtable participants already integrated or were considering one or more privacy protecting or privacy enhancing features in their rCBDCs (Annex Figure 2.4).
- **Offline functionality: Most central banks consider the ability to make offline CBDC payments to be vital or advantageous.**[56] This was also reflected in the roundtable, where almost two-thirds of participants were pursuing offline functionality in their rCBDC explorations (that is, prohibiting the purchase of certain goods or services offline) or requiring that offline transactions must be done where the parties are in close physical proximity (Annex Figure 2.5).

Annex Figure 2.4. Privacy Protecting/Privacy Enhancing Features Being Considered by Jurisdictions



Source: Survey results from virtual roundtable on rCBDCs.

Annex Figure 2.5. Jurisdictions Pursuing Offline Functionality



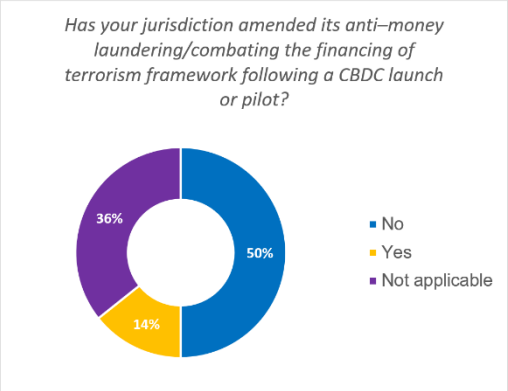
Source: Survey results from virtual roundtable on rCBDCs.
Note: CBDC = central bank digital currency.

[56] See BIS Innovation Hub, Central Bank Survey on Offline Payments with CBDC, Annex B, BIS (2023b).

Anti–Money Laundering/Combating the Financing of Terrorism Legal Framework

A few roundtable participants had amended their AML/CFT-related laws to accommodate rCBDC issuance and use, whereas others were contemplating whether changes were necessary (Annex Figure 2.6). Several participants decided to leverage existing legal frameworks for payments and focus less on new legal frameworks specifically for rCBDCs. Where the legal framework was updated (or updates were planned), jurisdictions focused on introducing provisions to define CBDC as fiat and authorize the central bank to issue CBDC, or regulations and guidelines addressing the activities of CBDC intermediaries.

Annex Figure 2.6. Amendments to AML/CFT Legal Framework Connected with CBDC Launch or Pilot



Source: Survey results from virtual roundtable on rCBDCs.
Note: AML/CFT = anti–money laundering/combating the financing of terrorism; CBDC = central bank digital currency; N/A = Not applicable.

References

Atlantic Council. 2025. "Central Bank Digital Currency Tracker." https://www.atlanticcouncil.org/cbdctracker/

Bank of England. 2025. "Digital Pound Experiment Report: Offline Payments." https://www.bankofengland.co.uk/report/2025/digital-pound-experiment-report-offline-payments

Bank of Ghana. 2022. "Design Paper of the eCedi." https://www.bog.gov.gh/wp-content/uploads/2022/03/eCedi-Design-Paper.pdf

Bank for International Settlements. 2022. "Project Aurum: A Prototype for Two-Tier Central Bank Digital Currency (CBDC)." https://www.bis.org/publ/othp57.pdf

Bank for International Settlements. 2023a. "Project Icebreaker: Breaking New Paths in Cross-Border Retail CBDC Payments." https://www.bis.org/publ/othp61.htm

Bank for International Settlements. 2023b. "Project Polaris: Part 1: A Handbook for Offline Payments with CBDC." https://www.bis.org/publ/othp64.pdf

Bank for International Settlements. 2023c. "Project Polaris: Part 4: A High-Level Design Guide for Offline Payments with CBDC." https://www.bis.org/publ/othp79.pdf

Bank for International Settlements. 2024a. "A Proposal for a Retail Central Bank Digital Currency (CBDC) Architecture," https://www.bis.org/publ/othp89.pdf

Bank of Jamaica. 2020. "A Primer on BOJ's Central Bank Digital Currency." https://boj.org.jm/a-primer-on-bojs-central-bank-digital-currency/

Bossu, Wouter, Masaru Itatani, Catalina Margulis, Arthur Rossi, Hans Weenink, and Akihiro Yoshinaga. 2020. "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations." IMF Working Paper 20/254, International Monetary Fund, Washington, DC.

Central Bank of Nigeria. 2021. "Regulatory Guidelines on the eNaira ." https://www.cbn.gov.ng/Out/2021/FPRD/eNairaCircularAndGuidelines%20FINAL.pdf

Central Bank of Nigeria. 2023. "Design Paper for the eNaira." https://enaira.gov.ng/wp-content/uploads/2023/06/Design-Paper-for-Nigerias-CBDC-02_Oct-2021.pdf

Central Bank of The Bahamas. 2019. *Project Sand Dollar: A Bahamas Payment System Modernization Initiative*. https://www.centralbankbahamas.com/viewPDF/documents/2019-12-25-02-18-11-Project-Sanddollar.pdf

Daman, Maarten. 2024. "Making the Digital Euro Truly Private." *The ECB Blog*, June 13. https://www.ecb.europa.eu/press/blog/date/2024/html/ecb.blog240613~47c255bdd4.en.html

Eastern Caribbean Central Bank. 2021. "The ECCB's Digital Currency (DCash) is a Critical Step in the Buildout of a Digital Economy in the ECCU". *ECCB Blog*, March 1. https://www.eccb-centralbank.org/blogs/the-eccb-s-digital-currency-dcash-is-a-critical-step-in-the-buildout-of-a-digital-economy-in-the-eccu

European Central Bank. 2019. "Exploring Anonymity in Central Bank Digital Currencies." https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

European Central Bank. 2022. "Progress on the Investigation Phase of a Digital Euro – Second Report." https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov221221_Progress.en.pdf

Financial Action Task Force. 2010. "Money Laundering Using New Payment Methods." https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20using%20New%20Payment%20Methods.pdf.coredownload.pdf

Financial Action Task Force. 2013. "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services." https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-NPPS.pdf.coredownload.pdf

Financial Action Task Force. 2025. "Guidance on Financial Inclusion and AML/CFT measures." https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf

Financial Action Task Force. 2019. "Terrorist Financing Risk Assessment Guidance" https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html

Financial Action Task Force. 2020. "Report to the G20 on So-Called Stablecoins." https://www.fatf-gafi.org/en/publications/Virtualassets/Report-g20-so-called-stablecoins-june-2020.html

Financial Action Task Force. 2021a. "Guidance on Proliferation Financing Risk Assessment and Mitigation." https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

Financial Action Task Force. 2021b. "Stocktake on Data Pooling, Collaborative Analytics and Data Protection." https://www.fatf-gafi.org/en/publications/Digitaltransformation/Data-pooling-collaborative-analytics-data-protection.html

Financial Action Task Force. 2021c. "Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers." https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

Financial Action Task Force. 2024. "Money Laundering National Risk Assessment Guidance." https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Guidance.html

Financial Action Task Force. 2025a. "International Standards on Combating Money Laundering and Financing of Terrorism & Proliferation." https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Financial Action Task Force. 2025b. "Guidance on: Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures." https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf

Financial Intelligence Unit of Latvia. 2023. "The AML/CFT Implications of Central Bank Digital Currency and the Digital Euro." https://fid.gov.lv/uploads/files/2023/cbdc/CBDC%20Digital%20Euro%20Risks%20Final.pdf

International Monetary Fund. 2014. "IMF Executive Board Reviews the Fund's Strategy for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)." Press Release No. 14/167, April 11, 2014. https://www.imf.org/en/News/Articles/2015/09/14/01/49/pr14167

International Monetary Fund. 2023a. "Central Bank Digital Currency – Initial Considerations." IMF Policy Paper No. 2023/048, International Monetary Fund, Washington, DC. https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/11/14/Central-Bank-Digital-Currency-Initial-Considerations-541466

International Monetary Fund. 2023b. "Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy." Policy Paper No. 2023/052, https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015

Kakebayashi, Michi, Gerard P. Presto, Tomonori Yuyama, and Shin'ichiro Matsuo. 2023. "Policy Design of Retail Central Bank Digital Currencies: Embedding AML/CFT Compliance." http://dx.doi.org/10.2139/ssrn.4366778

Murphy, Kieran, Sun Tao, Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, and Kristina Miggiani. 2024. "Central Bank Digital Currency Use and Privacy Protection." International Monetary Fund Fintech Note 2024/004, International Monetary Fund, Washington, DC. https://www.imf.org/en/Topics/digital-payments-and-finance/central-bank-digital-currency/virtual-handbook#chapter9

National Bank of Kazakhstan. 2022. "Digital Tenge 2022 White Paper." https://www.nationalbank.kz/file/download/85870

Patel, Manisha, Safari Kasiyanto, and André Reslow. 2024. "Positioning Central Bank Digital Currency in the Payments Landscape." IMF Fintech Note 2024/006, International Monetary Fund, Washington, DC. https://www.imf.org/en/Topics/digital-payments-and-finance/central-bank-digital-currency/virtual-handbook#chapter6

People's Bank of China. 2021. "Progress of Research and Development of E-CNY in China." http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf

Reserve Bank of India. 2025. "Digital Rupee FAQs." https://www.rbi.org.in/commonman/Upload/English/FAQs/PDFs/DigitalRupee09012025.pdf

Reserve Bank of New Zealand. 2021. "Future of Money – Central Bank Digital Currency." https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/consultations/banks/future-of-money/cbdc-issues-paper.pdf

Shen, Timmy. 2022. "China Busts 'World's Dumbest Thieves' in Digital Yuan Money Laundering Case." *Forkast News*, September. https://forkast.news/china-busts-digital-yuan-money-laundering-case/

Soana, Giulio, and Thomaz de Arruda. 2024. "Central Bank Digital Currencies and Financial Integrity: Finding a New Trade-Off between Privacy and Traceability within a Changing Financial Architecture." *Journal of Banking Regulation* 25: 467–86.

PUBLICATIONS

Financial Integrity Implications of Retail Central Bank Digital Currencies (rCBDCs)
NOTE/2025/010