



# FINTECH

---

## NOTES

---

### **Selected Legal Considerations for Central Bank Digital Currencies**

Marianne Bechara, Adrian Dumitrescu-Pasecinic, and Tomoyuki Kubota

---

**FINTECH NOTE**

# **Selected Legal Considerations for Central Bank Digital Currencies**

Prepared by Marianne Bechara, Adrian Dumitrescu-Pasecinic, and  
Tomoyuki Kubota

November 2025

---

---

©2025 International Monetary Fund

## Selected Legal Considerations for Central Bank Digital Currencies

Note 2025/006

Prepared by Marianne Bechara, Adrian Dumitrescu-Pasecinic, and Tomoyuki Kubota <sup>\*†</sup>

### Cataloging-in-Publication Data

#### IMF Library

Names: Bechara, Marianne, author. | Dumitrescu-Pasecinic, Adrian, author. | Kubota, Tomoyuki, author. | International Monetary Fund, publisher.

Title: Selected legal considerations for central bank digital currencies / Marianne Bechara, Adrian Dumitrescu-Pasecinic, and Tomoyuki Kubota

Other titles: Selected legal considerations for CBDCs. | Fintech note.

Description: Washington, DC: International Monetary Fund, 2025. | Nov. 2025. | NOTE/2025/006. | Includes bibliographical references.

Identifiers: ISBN:

9798229028004 (paper)

9798229028257 (ePub)

9798229028134 (WebPDF)

Subjects: LCSH: Digital currency—Law and legislation. | Digital currency—case studies.

Classification: LCC HG1710.B4 2025

**DISCLAIMER:** Fintech Notes offer practical advice from IMF staff members to policymakers on important issues. The views expressed in Fintech Notes are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

**RECOMMENDED CITATION:** Bechara, Marianne, Adrian Dumitrescu-Pasecinic, and Tomoyuki Kubota. 2025. "Selected Legal Considerations for Central Bank Digital Currencies." IMF Fintech Note 2025/006, 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

\* This Note has benefited from comments from IMF staff and Julio Baquero Cruz; Manuel Baschung; Nuntapun Bhensook; Susanne Bohman; Ross P. Buckley; Tim Chung; Assaf David-Margalit, Bank of Israel; Noémie Dentu; Jeanelle Dundas; Lucas Alves Freire; Louise Gullifer; Guilherme Centenaro Hellwig; Masaru Itatani; Andreas Josuran; Hideki Kanda; Klaus Löber; colleagues from Bank Negara Malaysia; Nick McBride; Cristina Elena Moldovan; Florent Nicol; Taiga Okuyama; Panagiotis Papapaschalis; Onenne Partsch; Alina Radut; John Risness; Marcus Paulus Rosa; Arthur Rossi; Jayoung Seo; Yoav Soffer, Bank of Israel; Ploysri Tannirandorn; Elsa Themner; Alexander Tollast; Hans Weenink; Paul Yuen; and Corinne Zellweger-Gutknecht. IMF Legal Department reviewers include Mses. Yan Liu, Carine Antoine Chartouni, Juliana Bolzani, Hue Ting Chong, and Messrs. Brian David Patterson, Bernhard Steinki, Alessandro Gullo, Mario Tamez, Donato Messineo. Of course, any mistakes, errors, or omissions are the authors' alone.

<sup>†</sup> This Note is financially supported by the Government of Japan.

---

# Contents

<b>I. Introduction .....</b>	<b>1</b>
<b>II. The Legal Nature of rCBDC in Public Law.....</b>	<b>3</b>
Definition and Key Features .....	3
▪ <i>Liability of the Central Bank</i> .....	3
▪ <i>Availability to the General Public</i> .....	4
▪ <i>Inherently Digital</i> .....	4
▪ <i>Designed to Serve as Money</i> .....	5
rCBDC as Currency .....	5
▪ <i>Monopoly of Issuance</i> .....	6
▪ <i>Cours Forcé</i> .....	6
▪ <i>Legal Tender</i> .....	7
▪ <i>Privileges under Private Law</i> .....	8
▪ <i>Criminal Law Protection</i> .....	9
<b>III. rCBDC Implications on the Legal Mandate of Central Banks.....</b>	<b>10</b>
Legal Foundation to Issue rCBDC as Currency .....	10
Legal Foundation to Deploy rCBDCs as Payment Platforms .....	11
▪ <i>Ownership and Operation of rCBDC Payment Platforms</i> .....	11
▪ <i>Front-End Role by a Central Bank in a Two-Tier rCBDC System</i> .....	12
▪ <i>Outsourcing rCBDC Platform Operations to a Third Party</i> .....	13
▪ <i>Dual Central Bank Role: Operator and Regulator/Overseer of an rCBDC Platform</i> .....	14
Legal Foundation to Regulate and Supervise rCBDC Service Providers .....	15
▪ <i>Regulatory Regime</i> .....	15
▪ <i>Mandatory Participation of rCBDC Service Providers in rCBDC Platforms</i> .....	16
▪ <i>Power to Impose rCBDC Wallet/Service Account Portability in Exceptional Cases</i> .....	17
<b>IV. Legal Relationships in an rCBDC Landscape .....</b>	<b>18</b>
Legal Relationship between Issuing Central Bank and rCBDC Users .....	18
▪ <i>Asset Link</i> .....	19
▪ <i>Technological Link</i> .....	19
Legal Relationship between Issuing Central Bank and Intermediaries .....	20
▪ <i>Legal Relationship as Regulated rCBDC Service Providers</i> .....	21
▪ <i>Legal Relationship as Participants in the rCBDC Payment Platforms</i> .....	22
Legal Relationship between Intermediaries and rCBDC Users .....	22

<b>V. Specific Functionalities: Limits, Interest, Programmability, and Offline Transactions .....</b>	<b>25</b>
Limits on rCBDC under the Lens of Law .....	25
▪ <i>Limits on the Aspect of Store of Value: rCBDC Holding Amount</i> .....	25
▪ <i>Limits on the Aspect of Means of Exchange: rCBDC Transaction Amount</i> .....	25
▪ <i>Limits on Fees Charged for rCBDC Services</i> .....	26
Interest Bearing rCBDC .....	26
Programmability .....	26
Offline rCBDC Transactions .....	28
<b>VI. Selected Legal Aspects of wCBDC .....</b>	<b>30</b>
Definition and Scope .....	30
Legal Aspects .....	30
▪ <i>Legal Certainty over the Nature and Validity of Operations of Tokens</i> .....	30
▪ <i>Mandate of the Central Bank to Issue wCBDC</i> .....	31
▪ <i>Central Bank Operation and Control of the wCBDC Platform</i> .....	31
▪ <i>Legal Relationship between Central Bank and wCBDC Users</i> .....	32
▪ <i>Settlement Finality</i> .....	33
<b>VII. Conclusion .....</b>	<b>34</b>
<b>Annex: Key Legal Considerations with Practical Approaches .....</b>	<b>36</b>
<b>References .....</b>	<b>40</b>

## BOXES

Box 1. Acceptance of Legal Tender under the Law .....	8
Box 2. PFMI Standards and rCBDC Payment Platforms .....	13
Box 3. Mitigating Conflict of Interest in Multiple Roles of a Central Bank .....	15
Box 4. General Legal Principles Applicable to Both Central Bank–Users and Central Bank–Intermediaries Relationships .....	24

# I. Introduction

This Note aims to guide policymakers, including central banks, in assessing their legal frameworks to ensure a sound basis for the issuance of central bank digital currencies (CBDCs). It is not intended to constitute, and should not be construed as, a recommendation for member jurisdictions to issue CBDCs—its purpose is rather to navigate the authorities on the key legal considerations guiding their decision-making process. Exploring CBDC is a significant undertaking that involves complex decisions and considerations. Authorities should carefully assess whether and how it should be implemented. This assessment should include a comprehensive review of the legal frameworks, and if necessary, authorities should pursue legislative amendments prior to CBDC issuance to mitigate any legal, financial, operational, and reputational risks.

This Note is part of a broader IMF Legal Department (LEG) initiative to assist member countries in navigating legal challenges related to CBDCs. It mainly builds upon two key earlier LEG publications: an IMF Working Paper (Bossu and others 2020) mostly examining the legal foundations of retail CBDC under central bank law and their treatment under monetary law,<sup>1</sup> and an IMF Fintech Note (Bechara and others 2025) analyzing the private law aspects of token-based CBDCs primarily intended for retail use.<sup>2</sup>

This Note mainly focuses on retail CBDC (rCBDC), with a separate analysis of wholesale CBDC (wCBDC), recognizing their distinct purposes and challenges. rCBDC denotes a digital form of central bank money available to the general public for retail payments, whereas wCBDC refers to a tokenized form of central bank money accessible only to a restricted group, typically of financial institutions.

This Note explores selected legal considerations for both rCBDC and wCBDC, drawing on examples from enacted laws, regulations, and public drafts.<sup>3</sup> First, with respect to rCBDC, this Note discusses the mechanisms through which rCBDC is sanctioned as a currency; the legal basis for its issuance and provision of a payment platform; and the central bank's mandate to regulate rCBDC service providers. It examines the nature and impact of legal relationships in the rCBDC landscape, among others, aiming to help central banks better assess potential legal risks. The analysis also considers specific rCBDC design features, including holding and transaction limits, fee caps, interest accrual, programmability, and offline capabilities. Subsequently, this Note addresses wCBDC-specific legal considerations such as the legal nature of wCBDC; the central bank's mandate to issue wCBDC and to operate its platform (whether directly or through third parties); the legal relationship between the central bank and users; and settlement finality of wCBDC transactions.

This Note proceeds from certain CBDC design assumptions reflecting specific policy decisions. For rCBDC, this Note assumes that rCBDC is meant to function as “digital cash” distributed through

---

<sup>1</sup> This paper concludes that (a) central banks need a robust legal basis for issuing retail CBDC and (b) the status of retail CBDC must be clear under monetary law.

<sup>2</sup> This note explores (a) the legal nature of rCBDC as property and the legal implications thereto; (b) how rCBDC's ownership rights can be held and evidenced, focusing on the roles of ledgers, registries, and wallets; (c) the finality of transfers and the impact of payer insolvency, the protection of payees acting in good faith, and legal arrangements for rCBDC safekeeping and custody; (d) the protection of rCBDC holders against intermediary insolvency, the impact of depositing rCBDC with commercial banks, and using them as collateral; and (e) the legal considerations related to cross-border holding of rCBDC and the suitability of private international law for such transactions.

<sup>3</sup> This Note addresses the most frequently asked legal questions raised during IMF capacity development activities.

intermediaries, whereas the central bank retains at least control over issuing and redeeming the instrument (public–private partnership). For wCBDC, this Note considers wCBDC designs that embed an issuance of tokens by the central bank. Consequently, it does not analyze projects solely connecting tokenized markets to existing central bank settlement systems and money (for example, Real-Time Gross Settlement (RTGS)), so-called trigger solutions, nor settlement models relying solely on privately issued forms of money (for example, tokenized deposits or stablecoins). Finally, this Note generally assumes that—unlike rCBDC distribution—wCBDC circulation does not involve intermediaries.

This Note is subject to several important caveats. First, this Note recognizes the significant role of different national legal traditions. Whereas it aims to provide guidance on general legal principles common to many jurisdictions, it refrains from drawing conclusions based on any specific national or regional (monetary union) law. Second, given that CBDC designs can vary and new designs and features will likely emerge, this Note does not intend to offer a “one size fits all” solution. Instead, it aims to highlight potential legal challenges and suggests possible approaches. Accordingly, the legal questions addressed here are not exhaustive. Third, certain domains—including cross-border use, taxation, civil procedure, administrative law, competition and interoperability with existing payment systems, capital flow management, privacy, and anti–money laundering/combating the financing of terrorism—lie beyond the scope of this Note. It primarily focuses on central bank, monetary, financial and payment laws, with only limited forays into private law areas to complement Bechara and others (2025). Finally, it must be emphasized that this Note analyzes an instrument yet to be issued on a large scale. A key challenge is the scarcity of enacted legislation specifically addressing CBDC issuance—although several jurisdictions have made progress on this front—and the lack of notable judicial decisions that would allow for cross-country comparisons.

This Note is structured as follows. Section II addresses the legal nature of rCBDC under public law. Section III focuses on the main implications for central banks' legal mandates in issuing rCBDC. Section IV examines the key legal relationships in an rCBDC landscape. Section V analyzes the major rCBDC functionalities commonly discussed. Section VI is dedicated to wCBDC, discussing key legal aspects that should be addressed before issuing wCBDC. Finally, Section VII concludes this Note. The Annex includes a table summarizing the key legal considerations with practical approaches discussed in this Note.



## II. The Legal Nature of rCBDC in Public Law

### Definition and Key Features

rCBDC is designed to be issued by a public authority and from this perspective raises key public law considerations.<sup>4</sup> As such, public law—specifically associated with central bank law and monetary law—will mainly govern the nature of rCBDC as well as the authority for its issuance. These legal frameworks might need adjustments based on the functional definition and design features adopted for rCBDC.

There are various definitions of rCBDC proposed by central banks and international financial institutions, yet they all share key characteristics. In Bossu and others (2020), rCBDC is defined as “a new form of money, issued digitally by the central bank and intended to serve as legal tender.” For the Bank of England, rCBDC represents “an electronic form of central bank money that could be used by households and businesses to make payments and store value” (Bank of England 2020). The authorities in Japan describe rCBDC as “a new form of electronic central bank money issued as a direct liability of the central bank, denominated in legal tender of each jurisdiction” (Relevant Ministries and the Bank of Japan Liaison Meeting on CBDC 2024). The European Central Bank (ECB) views rCBDC as “a central bank liability offered in digital form for use by citizens and businesses for their retail payments” (European Central Bank 2020). These rCBDC definitions all share the following key characteristics: rCBDC is (i) *a liability of the central bank*, (ii) *available to the public*, (iii) *in inherently digital form*, and (iv) *designed to serve as money*. This Note begins with an analysis of key legal considerations related to the nature of rCBDC under public law based on those four common traits.

### *Liability of the Central Bank*

Countries that have issued or are exploring rCBDC generally characterize it as a *liability* of the central bank.<sup>5</sup> This characterization might result directly from the law. Examples of legal frameworks explicitly characterizing rCBDC as a liability of a central bank include the Bank of Jamaica Act 2022 which provides that its “monetary liabilities” include notes, coins, and central bank digital currency.<sup>6</sup> A similar example appears in the Regulatory Guidelines on the eNaira 2021 stating that the eNaira is a direct liability of the Central Bank of Nigeria.<sup>7</sup> Moreover, this legal characterization could also be implied in some central bank laws, such as those requiring an “asset cover” for currency in circulation:<sup>8</sup> Similar to

---

<sup>4</sup> This section focuses on the “public law” nature of rCBDC. The “private law” nature of rCBDC is analyzed in detail in Bechara and others (2025). “Public law” in this Note refers to the area of law governing the “vertical” relationships between the State and its subjects (through the exercise, for instance, of administrative powers typically enforced by the State), as opposed to “private law” that governs the “horizontal” relationship between these subjects. The two areas may be blurred when the central bank uses private law instruments for the exercise of its functions, including in the case of the distribution and operation of rCBDC.

<sup>5</sup> This Note refers to the term “liability” as defined from the accounting perspective. According to the Conceptual Framework for Financial Reporting, issued by the International Accounting Standards Board, “a liability is a present obligation of the entity to transfer an economic resource as a result of past events.” In jurisdictions where the nature of cash is a claim, the interpretation might be that rCBDC users have a claim against the central bank, but in jurisdictions where the nature of cash is not a claim, the interpretation might be different. rCBDC users have assets that constitute liabilities on the central bank’s balance sheet, which constitute claims in some jurisdictions, and do not constitute claims but property in other jurisdictions.

<sup>6</sup> Section 2 of the Bank of Jamaica Act, as amended in 2022.

<sup>7</sup> Section 1.0 of the Regulatory Guidelines on the eNaira 2021.

<sup>8</sup> Some central bank laws require the central banks to maintain a combination of official foreign reserve assets and local government bonds in an amount equal to the currency in circulation. See paragraph 33 of Bossu and others (2020).



banknotes and coins, rCBDC would be counted as a liability for that purpose. In addition, some argue that rCBDC would be characterized as a liability from a *legal* perspective based on its *accounting* treatment as a liability (just as other forms of money of central bank (for example, banknotes and reserves)). For instance, such accounting treatment can be observed in the Central Bank of The Bahamas' 2022 financial statements that list "notes in circulation," "coins in circulation," and its rCBDC "Sand Dollar in circulation" under "financial liabilities."

As a central bank liability, rCBDC is a credit risk-free instrument, unlike privately issued instruments. From a creditworthiness perspective, as a central bank liability, rCBDC would be as safe and risk-free as traditional central bank money. Unlike bank deposits and other liabilities on private financial institutions, such as electronic money or some types of stablecoins, rCBDC would not carry any private credit risk. However, indirect risks might arise if rCBDC issuance leads to an expansion of the central bank's balance sheet, a change in the allocation of central bank assets, or a reduction in retail deposits at commercial banks (as discussed in Section V).

rCBDC should remain a central bank liability under any system architecture. The legal framework should consistently ensure that rCBDC remains a central bank liability regardless of its design or distribution mechanism:<sup>9</sup> It does not suffice that the rCBDC is classified as a central bank liability, but the design of the rCBDC should be in line and not in contradiction with such objective and principle. For example, China's rCBDC (e-CNY) is a direct liability of the People's Bank of China (PBOC). In that vein, the e-CNY uses a two-tier architecture: the PBOC handles issuance and redemption, whereas intermediaries provide e-CNY services. Because rCBDC is a liability of the central bank, not the intermediaries, their insolvency should not affect the value of e-CNY held by rCBDC users.

### ***Availability to the General Public***

General public availability is a defining characteristic that sets rCBDC apart from other digital central bank money (reserves). This broad availability is a basic feature distinguishing rCBDC from existing central bank digital money often assimilated to central bank reserves (credit balances on accounts commercial banks hold at the central bank). Central bank reserves can only be held by a narrow set of eligible institutions, whereas rCBDC is intended for a wider user, including individual consumers. rCBDC thus enables households and businesses to make payments and store value (to some extent) using a digital form of central bank money.

### ***Inherently Digital***

Because rCBDC exists only in digital form, many legal provisions applicable to physical currencies may not be relevant for rCBDC. For instance, a digital currency may not require multiple denominations (for example, 1-, 5-, or 10-dollar bills)—though other design options are possible—therefore some related legal provisions might need adjustment in the case of rCBDC. A pertinent example is India's amendments to the Reserve Bank of India Act, 1934, which broadened the definition of "banknote" to

---

<sup>9</sup> Strictly speaking, indirect liability, also known as synthetic CBDC, is not CBDC. In the case of synthetic CBDC, the liability is issued by a commercial bank but is fully backed by central bank liabilities. Liabilities of commercial banks, even if backed by a 100-percent cash deposit in the books of the central bank, are not a central bank liability. For further details, see Bechara and others (2025).

include currency in digital form and explicitly disappplied certain sections relevant only to physical currency (such as those dealing with denominations, physical form, or acts of mutilation of currency) to rCBDC.<sup>10</sup>

Furthermore, the digital form of rCBDC introduces new legal risks requiring careful consideration. For example, the legal framework should include basic rules to govern the transfer of rCBDC, its loss, illegal transfers, and good-faith acquisition, as well as the impact of insolvency on rCBDC transactions.<sup>11</sup> In addition, emerging cybersecurity threats may not be captured by existing laws. Jurisdictions must carefully assess the obsolescence of certain legacy provisions and consider the need to proactively legislate for digital-era monetary risks, thereby ensuring legal clarity and user protection.

### ***Designed to Serve as Money***

To function as money, rCBDC must be denominated in an existing unit of account and serve as both a medium of exchange and a store of value. Currency fulfills those three functions well. Indeed, the legal concept of “money” includes the narrower concept of “currency” (banknotes and coins) in addition to central bank and commercial bank “book money” (account balances) and electronic money. Consequently, designating rCBDC as currency would allow it to serve as money.<sup>12</sup> It should be noted that for policy purposes, jurisdictions may set limits on rCBDC use as a medium of exchange or store of value (as discussed in Section V).

Many jurisdictions conceptualize rCBDC as a form of “digital cash.” To realize this vision, it is essential that the legal framework enables rCBDC with key attributes traditionally associated with “physical cash.” These include its recognition as legal tender (or currency as discussed in this section), as well as the ability to function offline (explored further in Section V). Offline functionality is especially important to ensuring universal accessibility, including in areas with limited or no internet connectivity. However, whether rCBDC can fully replicate all other key attributes of cash remains an open question. Although rCBDC can emulate many cash-like features—such as bearer instrument status and instant settlement—achieving complete anonymity and fully risk-free offline use remains challenging in a digital environment.<sup>13</sup> Given these complexities, rCBDC aims to provide a functional equivalent of cash that upholds its convenience, accessibility, and trustworthiness, even if a perfect digital replication may not be feasible.

### **rCBDC as Currency**

To be legally classified as currency, rCBDC must possess the features of a currency. Generally, “currency” can be defined as the official means of payment of a country, recognized as such by its laws,

---

<sup>10</sup> Section 22A of the Reserve Bank of India Act, 1934, as amended, provides that “Nothing contained in sections 24, 25, 27, 28 and 39 shall apply to the bank notes issued in digital form by the Bank.” These sections are: 24. Denominations of notes; 25. Form of bank notes; 27. Re-issue of notes; 28. Recovery of notes lost, stolen, mutilated, or imperfect; and 39. Obligation to supply different forms of currency.

<sup>11</sup> See Bechara and others (2025) for further details.

<sup>12</sup> Introducing rCBDC does not create a new official monetary unit: rCBDC would be a means of payment issued in the existing official unit, so there is no need to amend the definition of the currency unit (rCBDC is not a new “currency unit”).

<sup>13</sup> Furthermore, many jurisdictions are cautious with these designs for policy considerations. This discussion is outside the scope of this Note (see Murphy and others 2024).

and denominated by the official monetary unit of that country.<sup>14</sup> If rCBDC is meant to be “currency” under the law, it is generally recognized that the State would sanction its use through five important legal mechanisms: (i) *the monopoly of issuance by the State (or its agent)*; (ii) *cours forcé*; (iii) *legal tender status*; (iv) *privileges under private law*; and (v) *protection under criminal law*. The following paragraphs describe various national approaches to these features as they relate to rCBDC.

## ***Monopoly of Issuance***

The State’s monopoly on currency issuance should extend to rCBDC. A monopoly of issuance is a fundamental monetary law provision granting the State the exclusive right to issue currency within its jurisdiction or currency area. Historically, the use of means of payment and monetary sovereignty are two intricately connected concepts, as illustrated, for instance, by the presence of the emperor’s or king’s figure on coins and banknotes. In nearly all countries today, official means of payment (currency) are issued by the State, typically through the central bank. If rCBDC is to be equated with “currency,” it follows that the central banks should similarly be granted the monopoly for the issuance of digital currency. For example, the Bank of Jamaica Act provides: “the Bank shall have the sole right and authority to issue notes, coins and central bank digital currency.”<sup>15</sup> In the EU, the European Central Bank (ECB) will have the exclusive right to authorize the issue of the digital euro, and the ECB and the national central banks may issue it.<sup>16</sup>

## ***Cours Forcé***

Cours forcé is an important currency feature and thus applies to rCBDC with currency status. The contemporary meaning of cours forcé is that the value of a banknote is the amount of the official monetary unit printed upon it.<sup>17</sup> Ideally, legislation should confer cours forcé status on rCBDC. For instance, in the EU, the draft digital euro regulation provides for acceptance at full face value, stating that “the monetary value of digital euro tendered in payment of a debt shall be equal to the value of the monetary debt.”<sup>18</sup> Cours forcé entails that merchants cannot charge an additional amount for using rCBDC. However, at least from the legal perspective, they could offer discounts on other payment methods. It should be noted that such discounts do not directly penalize or add an extra charge when using rCBDC; rather, they reward the use of alternative methods. In other words, because the discounts

---

<sup>14</sup> Although currency is usually described by linking to the economic function of money (unit of account, store of value, medium of exchange), there is no universal definition under central bank laws. Georg Knapp’s *State Theory of Money* (1905) asserted that money is fundamentally a creation of the legal system. According to Knapp, the state—through its laws—establishes the currency as a means of payment. National monetary laws typically refer to currency as banknotes and coins. The term “currency” can also be found in provisions stating that the central bank is authorized to issue currency and provisions identifying the currency as the “monetary unit.”

<sup>15</sup> Section 12(1) of the Bank of Jamaica Act, as amended in 2022.

<sup>16</sup> Article 4(1) of the draft digital euro regulation.

<sup>17</sup> The historical concept of “cours forcé” referred to a situation where banknotes were declared legal tender by law, but were not convertible into gold or silver (that is, not backed by a metallic standard). This typically occurred during times of economic crisis, war, or financial instability when governments suspended the convertibility of paper money into specie (metal coins). Under cours forcé, individuals and institutions were legally required to accept the paper currency at its face value, even if it had depreciated or was no longer backed by precious metals.

<sup>18</sup> In general, the concept of cours forcé should not be confused with the legal tender. Cours forcé focuses on the nominal value of the means of payment, whereas legal tender concerns mainly the power of the means of payment to discharge from debt. The concept of cours forcé should also be distinguished from the concept of convertibility (as discussed in this section).

do not reduce the obligation of the payee to accept rCBDC at nominal value, the fundamental rule of *cours forcé* could remain intact.

A related feature to *cours forcé* is convertibility. In the same context of the stability of value and singleness of money, rCBDC convertibility into other forms of money accessible to the public (for example, banknotes or commercial bank money) is key. This requires an enabling legal foundation on at least two fronts:

- First, the law should explicitly require that rCBDC be convertible at par *with other central bank money* available to the public. This ensures users can freely choose between different forms of retail central bank money. The ECB has observed that the full convertibility at par between the digital euro and euro cash is a natural consequence of their shared legal tender status: the draft digital euro regulation provides that “the digital euro shall be convertible with euro banknotes and coins at par.” Similarly, Nigeria guarantees a 1:1 exchange between the eNaira and the physical Naira cash.<sup>19</sup> In that vein, it should be noted that some rCBDC designs may bring legal issues. For instance, when rCBDC is designed as programable money (as discussed in Section V), it might result in an instrument having a different market value than its nominal value (as opposed to banknotes). Another relevant example is that if rCBDC does not have “full” legal tender status as banknotes, it might therefore be viewed as a “weaker” form of central bank money. One other example is when an rCBDC holds interest rate and therefore its market value might be different from the nominal value of banknotes.
- Second, convertibility between rCBDC and *commercial bank money* is crucial to preserve the singleness of money. Achieving this requires, at a minimum (as with traditional central bank money), robust enabling legal and regulatory mechanisms, such as adequate bank regulation and supervision, and deposit protection. Legal provisions may explicitly mention this convertibility. For instance, in Ghana, the eCedi is designed to be convertible 1:1 into commercial bank deposit money (Bank of Ghana 2022). Likewise, the draft digital euro design foresees convertibility at par with bank deposits and electronic money: the digital euro is designed to be convertible at par with “scriptural money” and electronic money.<sup>20</sup>

## Legal Tender

There is no globally established legal definition of legal tender,<sup>21</sup> and the national laws typically do not provide a comprehensive definition for this concept.<sup>22</sup> The common feature of legal tender found in most jurisdictions is having the power to extinguish payment obligations and to discharge the debtor once accepted. In addition, in some countries, accepting legal tender is mandatory, with administrative or criminal penalties on creditors that refuse it, whereas in others, the mandatory acceptance can be

---

<sup>19</sup> Section 1.0 of the Regulatory Guidelines on eNaira 2021.

<sup>20</sup> It is noted that legal convertibility can only be achieved in practice if the rCBDC design includes technical convertibility, meaning interoperability with other forms of digital money. For instance, users might not be able to technically convert their rCBDC into other forms of digital money, even though the law has given them the legal right to convert it.

<sup>21</sup> Instead, the national laws usually include only a legal statement indicating what forms of money (for example, banknotes and coins) are legal tender.

<sup>22</sup> A rare exception is the euro area which is a jurisdiction benefiting from a clear legal definition of legal tender given first in the Commission Recommendation 2010/191/EU of 22 March 2010 on the scope and effects of legal tender of euro banknotes and coins, and endorsed by the European Court of Justice decision of 2021. This definition includes (i) mandatory acceptance, (ii) at full face value, and (iii) with the effect of extinguishing payment obligations.

derogated based on the freedom of contract. In other countries, although acceptance of legal tender is not mandatory at all, its refusal is discouraged through economic or legal disincentives. For instance, some jurisdictions bar creditors from enforcing their obligations in courts, whereas other jurisdictions bar charging interest on the debtors or allow the recovery of costs related to lawsuits (see Box 1). Lastly, legal tender status for rCBDC is generally explicitly granted by law. For example, the Bank of Jamaica Act has been adapted to provide that “CBDC shall be legal tender for the payment of any amount.”<sup>23</sup> In Ukraine, the amended central bank law provides that the digital currency is a legal tender in Ukraine.<sup>24</sup>

### Box 1. Acceptance of Legal Tender under the Law

**Absolute mandatory acceptance:** Some jurisdictions prohibit merchants from refusing cash based on contractual freedom. For example, France legally requires accepting cash; under Article R642-3 of the Penal Code, refusing legal tender banknotes and coins is punishable by a fine (currently €150). In Brazil, refusing to accept legal tender currency is a criminal contravention punishable by a fine (Decree-Law 3,688/1941, Article 43).

**Relative mandatory acceptance:** In other countries, although the law states that banknotes and coins are legal tender for monetary obligations, parties are allowed to contract otherwise. *Contractual freedom can limit legal tender provisions*, meaning parties may agree in advance to use a different means of payment. For instance, Article 452 of the Greek Penal Code punishes with a fine anyone who refuses to accept for payment money which is legal tender in Greece. However, the principle of contractual freedom allows contractual parties to agree on other means of payment apart from cash, leading to the discharge of the payment obligation.

**Non-mandatory acceptance:** In English law, where a debtor is obliged to pay a specific sum of money to a creditor a successful plea of tender does not discharge the debt, but if the creditor subsequently sues for debt, the debtor may, by paying the money into court and by proving the legal tender and its continuous willingness to pay the debt since the tender, bar any claim for interest or damages after the tender; the creditor will also be liable to pay the debtor its costs of the action, on the ground that the action should not have been brought.

Legal tender status is another important currency feature, but in some jurisdictions, it might need to be revisited to adapt it to the digital innovation of rCBDC. When the State confers legal tender status on a means of payment, that means of payment should be easily usable by most of the population. Authorities must assess whether the law should obligate the general public to accept rCBDC, given their dependence on technical infrastructure, varying digital literacy, and privacy concerns. In that vein, this obligation to accept rCBDC may be justified for users already accepting other forms of digital payments. In other words, a justified and proportionately limited scope of legal tender could be considered for the rCBDC. Notably, the draft digital euro regulation, after declaring the legal tender, sets out exceptions to such mandatory acceptance (for example, a payee who is a natural person acting in a purely personal or household activity). Finally, rCBDC’s legal tender status may face challenges, such as potential incompatibility with the concept of programmable money and may have specific nuances for offline functionality (as discussed in Section V).

### Privileges under Private Law

To promote the circulation of rCBDC as “digital cash,” certain private law privileges traditionally attached to physical currency should be extended to rCBDC. Under general private law, ownership rights typically

<sup>23</sup> Section 15 of the Bank of Jamaica Act, as amended in 2022.

<sup>24</sup> Article 35 of the Law on the National Bank of Ukraine.

allow recovery of lost or stolen property, even from good faith acquirers, pursuant to the *nemo dat quod non habet* principle (meaning that no one can give what they do not have). However, physical currency is often exempt from this rule to preserve liquidity and transactional certainty. For example, in *Miller v. Race* (1758), the English court held that a banknote received in good faith and for value conferred full legal title, extinguishing prior claims. Depending on its system design, extending a similar exemption to rCBDC would ensure that good faith acquirers retain title, even if the rCBDC were initially obtained unlawfully. When the privileged status of physical currency is grounded in its tangible nature, rCBDC's intangibility presents a legal challenge. A robust legal framework is required to replicate these protections for rCBDC, thereby supporting its function as a widely accepted and trusted medium of exchange.<sup>25</sup>

### ***Criminal Law Protection***

Criminal laws may require updating to extend sanctions traditionally protecting physical currency—such as those enforcing monopoly of issuance, recognizing legal tender, and preventing counterfeiting—to rCBDC. rCBDC introduces new cybercrime vulnerabilities.<sup>26</sup> Although some traditional crimes related to physical currency such as counterfeiting (that involves unauthorized reproduction of tangible notes or coins) could not be committed under rCBDC designs built on a ledger relying on cryptographic validation and ledger immutability, rCBDC use could nevertheless raise novel criminal concerns (such as unauthorized access, hacking, exploitation of digital wallets, and smart contract manipulation). Existing cybercrime, data protection, and financial fraud law will be essential in defining liability and enforcement mechanisms. Accordingly, it is imperative to modernize legal texts to address emerging cybersecurity threats and ensure comprehensive protection of rCBDC under criminal law such as *nullum crimen sine lege*, *nulla poena sine lege* (meaning that there is no crime without law, no punishment without law).<sup>27</sup>

---

<sup>25</sup> For a detailed analysis, see Bechara and others (2025).

<sup>26</sup> See Bossu and others (2020) for further details.

<sup>27</sup> Some jurisdictions have already taken steps. The Bahamas' 2020 legislation criminalizes counterfeiting or alteration of electronic money designated as legal tender. Jamaica's 2022 Bank of Jamaica Act prohibits unauthorized issuance of rCBDC, with penalties for violations. Similarly, draft amendments to China's Law on the People's Bank of China impose fines and confiscation for unauthorized digital tokens intended to replace the renminbi.

### III. rCBDC Implications on the Legal Mandate of Central Banks

Under the principle of attributed powers, a central bank must have statutory authority to issue rCBDC.<sup>28</sup> In most jurisdictions, existing central bank laws do not clearly empower issuing digital currency directly to the public. Traditionally, central banks are authorized to issue physical banknotes and coins, and to manage accounts for banks, financial institutions, and the government—a general-purpose digital currency falls outside many current statutes. Thus, introducing rCBDC (accessible to households and businesses) typically requires either new legislation granting the central bank additional powers or a reinterpretation of existing law. In public law terms, the central needs a clear statutory basis for this digital innovation.

An explicit legislative mandate for rCBDC issuance would mitigate legal, financial, and reputational risks.<sup>29</sup> A clear law authorizing rCBDC bolsters its legitimacy and reduces the risk of legal challenges, as well as associated reputational or financial fallout. Although each jurisdiction approaches legal interpretation differently, many central banks and governments caution against relying on strained readings of existing statutes to justify a public money innovation—stretching current central bank powers could invite court challenges or political pushback. Instead, an explicit legislative mandate provides legitimacy and clarity. For instance, the Bank of England and HM Treasury have indicated that primary legislation would be enacted before any digital pound launch to define the rCBDC's features and ensure appropriate governance and privacy safeguards (Bank of England and HM Treasury 2024).

The legal mandate to issue rCBDC would significantly affect central bank governance.<sup>30</sup> In proceeding with rCBDC initiatives, jurisdictions should ensure the autonomy of the central bank is preserved (for example, carefully delineating the respective roles and responsibilities of the central bank and political authorities in the design and implementation of the rCBDC).<sup>31</sup> Central banks may also need to adjust internal decision-making structures—reviewing oversight committee's competencies to hold sufficient technical expertise, and ensuring that they have legal authority to form specialized committees or adapt existing ones to the rCBDC initiatives (Bechara and others 2021).

#### Legal Foundation to Issue rCBDC as Currency

Jurisdictions should consider explicitly vesting the rCBDC issuance function in the central bank through statute.<sup>32</sup> Given rCBDC's novelty, central bank laws are usually amended to remove language limited to physical currency. For instance, the Bank of Jamaica Act was amended to define rCBDC as “a digital

---

<sup>28</sup> See Box 3 of Bossu and others (2020).

<sup>29</sup> See paragraph 95 of Bossu and others (2020).

<sup>30</sup> Central bank governance typically encompasses the institution's mandate, decision-making structure, autonomy, accountability, and transparency.

<sup>31</sup> Depending on rCBDC's system design, to the extent that the issuance of rCBDC inevitably involves access to personal data—strictly limited to what is essential and protected by privacy safeguards—the central bank should be held accountable under data protection laws for its data processing.

<sup>32</sup> See paragraph 23 of Bossu and others (2020).



form of currency.”<sup>33</sup> This general definition clearly empowers the central bank to create digital sovereign money. In addition, enabling clauses specify that the Bank of Jamaica may issue and redeem digital currency as part of its functions.<sup>34</sup> It is worth noting that launching certain rCBDC pilots might require such legal amendments to avoid legal risks. For instance, the Eastern Caribbean Central Bank (ECCB) Agreement was amended to clarify that currency includes digital currency when ECCB started its rCBDC (DCash) pilot (Article 2).

It should be noted that most central bank laws today do not permit opening current accounts for the general public in the context of rCBDC issuance.<sup>35</sup> In many jurisdictions, central banks are legally barred or restricted from offering current accounts to individuals. Enabling such a current account type of rCBDC accessible to everyone would require legislative amendments to grant the central bank the power to open and maintain current accounts for the general public.

rCBDC issuance designs have gravitated toward two-tier models rather than direct provision of current accounts by central banks, because of economic and market structure considerations.<sup>36</sup> In theory, a jurisdiction could authorize its central bank to roll out public current accounts for rCBDC, effectively turning the central bank into a retail account provider.<sup>37</sup> This would vastly expand central bank functions and expose it to new risks (including significant cybersecurity risk), raising policy questions beyond the legal realm (such as competition with banks, operational capacity, and privacy management). To date, no major jurisdiction has considered rCBDC through universal central bank current accounts, and obtaining political agreement for such a shift would likely be difficult. Instead, many central banks favor a two-tier model (public–private partnership): consumers and businesses use rCBDC through “rCBDC wallets” or “rCBDC service accounts” provided by private intermediaries (front-end services), whereas the central bank operates the core rCBDC ledger and its issuance in background (back-end services). Though legislators could amend laws to allow central banks to hold individual citizen accounts, most rCBDC designs deliberately avoid that approach.

## Legal Foundation to Deploy rCBDCs as Payment Platforms

### *Ownership and Operation of rCBDC Payment Platforms*

Under the principle of attributed powers, a central bank should have statutory mandate to own and operate an rCBDC payment platform.<sup>38</sup> Depending on its system design, an rCBDC might involve creating or using a payment platform.<sup>39</sup> This raises the question: on what legal basis does a central bank

---

<sup>33</sup> Section 2 of the Bank of Jamaica Act, as amended in 2022.

<sup>34</sup> Section 5 of the Bank of Jamaica Act, as amended in 2022.

<sup>35</sup> See paragraph 45 of Bossu and others (2020).

<sup>36</sup> Under the two-tier rCBDC model, private-sector intermediaries (for example, banks, payment service providers) handle rCBDC distribution, customer onboarding, and transaction processing whereas each digital unit of rCBDC remains a direct liability of the central bank. Also, many rCBDC system designs increasingly adopt a hybrid approach that merges token-based and account-based features into the two-tier rCBDC model (for example, leveraging tokenization technology with various service account structures).

<sup>37</sup> See paragraph 51 of Bossu and others (2020).

<sup>38</sup> In this Note, the rCBDC payment platform generally means a publicly governed retail payment infrastructure for digital central bank money with formal legal and contractual rules of its funds transfer operation and public oversight. The detailed scope of the rCBDC payment platform depends on the individual rCBDC system design.

<sup>39</sup> It should be noted that in some jurisdictions, the issuance of rCBDC and maintenance of an rCBDC ledger themselves may not qualify as the creation or operation of a payment system.

establish and operate this payment platform? Many central bank laws already mandate promoting safe and efficient payment systems and even empower central bank to operate payment systems (indeed, many central banks run RTGS systems for interbank payments).<sup>40</sup> However, those mandates may explicitly or implicitly be limited to wholesale (interbank) systems.<sup>41</sup> In such cases, legal reform would be needed to clarify that owning and operating a *retail* payment platform (as an rCBDC platform) falls within the central bank's remit.

If an rCBDC platform is operated by a new entity partly or wholly owned by the central bank, the legal framework should ensure that such equity participation is permitted. Some central bank laws broadly prohibit the central bank from acquiring shares or equity in private corporations unless specifically authorized. Nonetheless, certain laws allow central bank equity stakes when closely tied to its objectives (for example, owning a banknote printing company).<sup>42</sup> A company operating an rCBDC platform could be analogized to such exceptions, but explicit legal permission may be required.

An rCBDC payment platform might be designated as systemically important, requiring the Principles for Financial Market Infrastructures (PFMI) compliance and strong oversight. Many jurisdictions have payment systems laws empowering the central bank or other regulators to issue regulations and standards for payment systems and to supervise them in line with the PFMI. The introduction of an rCBDC payment platform could present gaps or interpretative issues in applying the PFMI framework, possibly necessitating further guidance or legal reforms (see Box 2).

### ***Front-End Role by a Central Bank in a Two-Tier rCBDC System***

Any front-end role the central bank plays—such as providing software or devices for public rCBDC access—must align with its mandate and serve public interest objectives such as financial inclusion and resilient universal access. In a two-tier model, private intermediaries handle most customer-facing tasks, but a central bank might choose to offer basic public rCBDC wallets for segments underserved by private intermediaries (for example, the unbanked or remote populations) or provide default rCBDC services to ensure universal, reliable access. Specifically, central banks' engagement in retail front-end service varies by policy priorities and legal frameworks. For instance, the EU opts for a legislated approach: recognizing the central bank's competence to provide front-end services as public options within a competitive payments market. Nigeria, on the other hand, launched a central bank–managed eNaira wallet app to advance financial inclusion under its existing legal mandate. In any case, the central bank's statute must authorize such retail-facing operations.

---

<sup>40</sup> One example is Article 4(9) of the Law of the People's Republic of China on the People's Bank of China (PBOC) charging the PBOC with maintaining the normal operation of the payment, clearing, and settlement systems. Another example is Section 44(1)(a) of the Central Bank of Malaysia Act stipulating that the Central Bank or any body corporate established or acquired by the Central Bank under paragraph 48(1)(c) of the Act or any person authorized by the Central Bank may establish or operate any system, electronic or otherwise, as may be necessary to facilitate the transferring, clearing and settlement of funds and debt securities.

<sup>41</sup> See paragraph 47 of Bossu and others (2020).

<sup>42</sup> Section 7 of the Reserve Bank of Australia (RBA) Act establishes that the RBA "is capable of acquiring, holding and disposing of real and personal property." In addition, Section 8 of the Act gives the Bank "such powers as are necessary for the purposes of this Act," along with a list of specific powers and a broad catch-all power "to do anything incidental to any of its powers." This combination of general and incidental powers is interpreted to allow the RBA to undertake whatever activities are needed to fulfill its functions—including creating or acquiring a subsidiary to conduct banknote printing.

## Box 2. PFMI Standards and rCBDC Payment Platforms

The Principles for Financial Market Infrastructures (PFMI) set international standards for systemically important financial market infrastructures (FMI). Given their unique public mandate, central banks should apply the PFMI to FMIs that they operate. Depending on its system design and role in the financial system, an rCBDC payment platform may be designated as systemically important, making PFMI standards applicable.<sup>[1]</sup> Key (non-exhaustive) legal considerations for rCBDC payment platforms under PFMI include:

**Legal Foundation and Settlement Finality:** FMIs must ensure a well-founded, enforceable legal framework for all material activities (Principle 1). For rCBDC payment platforms, this includes clear authority to issue rCBDC, its status of currency and direct liability of issuing central bank, and treatment of features like programmability or offline transactions. Furthermore, PFMI standards mandate that settlement finality must be legally clarified to provide irrevocable and unconditional payments (Principle 8). Especially in a distributed ledger technology model with probabilistic or distributed consensus or offline rCBDC transactions, law and system rules must carefully define when finality occurs.

**Governance:** FMIs need transparent governance that promotes safety, efficiency, and supports financial system stability as well as public and stakeholder interests (Principle 2). For rCBDC payment platforms, ensuring independent oversight (for example, a committee overseeing the rCBDC platform operations) and input from stakeholders (for example, government, private intermediaries, and end-users) would be essential. Questions of accountability must be addressed when the central bank regulates its own rCBDC platform (as discussed in Box 3).

**Legal and Contractual Arrangements for Operational Resilience:** FMIs should identify and mitigate operational risks, including business continuity and information security, through adequate measures (Principle 17). For rCBDC payment platforms, any disruption or cyberattack could have immediate systemic effects on rCBDC users, rCBDC platforms potentially with outsourced operations should be properly regulated to minimize downtime and prevent data breaches or fraud by legal and contractual means: ensuring continuous availability and rapid recovery from outages is not just technical—it is a legal mandate to preserve trust in the new form of currency.

[1] Although not legally binding, the PFMI constitute soft law and are widely recognized as authoritative benchmarks for the design and oversight of FMIs, including those operated by central banks.

Sources: (i) Committee on Payment and Settlement Systems (CPSS) and International Organization of Securities Commissions (IOSCO) 2012; (ii) Committee on Payments and Market Infrastructures (CPMI) and IOSCO 2015; (iii) CPMI and IOSCO 2022; and (iv) Bank of Canada, Swiss National Bank, European Central Bank, Bank of England, Bank of Japan, Board of Governors of the Federal Reserve System, Sveriges Riksbank, and Bank for International Settlements 2024.

## Outsourcing rCBDC Platform Operations to a Third Party

If a central bank outsources rCBDC platform operation to a third party, it must ensure such outsourcing is legally permissible and that the central bank retains full control through legal and contractual arrangements. Like other central bank services, certain rCBDC platform functions (software development, cybersecurity, day-to-day operation under oversight, and so on) might be performed by third parties.<sup>43</sup> First, from a public law standpoint, the central bank must confirm it has legal authority to outsource these operations—issuance of currency might be deemed core sovereign activities that must remain in-house and activities outsourced must be of incidental or ancillary nature that do not affect the

<sup>43</sup> The Bank of Jamaica (BOJ) partnered with a technology firm after a competitive procurement process. Reportedly, the private firm functions as the technology provider: it manages the core rCBDC infrastructure and provides ongoing platform support, updates, and security maintenance under the BOJ's oversight.

overall public responsibility of the central bank.<sup>44</sup> If outsourcing is allowed, contracts and oversight mechanisms should safeguard the public interest.<sup>45</sup> The central bank must retain control over the rCBDC platform to protect monetary sovereignty.<sup>46</sup> Through stringent contracts and/or statutory powers, the central bank should own the intellectual property in the core technology, have fallback arrangements, and secure enforceable rights to intervene unilaterally in platform operations when necessary to fulfill its mandate. The central bank should also oversee the third party's performance, including cybersecurity and data protection compliance.

Having a third party operate the rCBDC platform does not absolve the central bank from its legal responsibility for platform continuity and integrity. Laws and international standards dictate that a public authority remains accountable for outsourced functions.<sup>47</sup> Especially in the context of digital currency issuance, the central bank must ensure—through regulation and/or contracts—that a third-party operator adheres to the central bank's security standards, grants the central bank continuous access for audit and inspections (with regular reporting), and maintains effective business continuity and contingency plans. Central banks might also seek explicit protection in contracts (for example, an indemnity clause to cover losses caused by the third-party operator's faults).<sup>48</sup>

Central banks should develop an “exit strategy,” supported by legal and contractual measures, in case a third-party rCBDC operator fails or must be replaced. Outsourcing risks such as third-party lock-in, overdependence, or data portability issues must be mitigated in the issuance of rCBDC. This starts with well-crafted contracts with each operational partner (developers, service providers) that embed rights for the central bank to step in, access source code, port data, and smoothen transition operations if needed. Legal and regulatory frameworks should reinforce the central bank's rights and powers: empowering the central bank to act decisively if a third-party operator fails, and compelling the operator to design systems to be open and interoperable to facilitate transfer.

### ***Dual Central Bank Role: Operator and Regulator/Overseer of an rCBDC Platform***

If a central bank is both operator of the rCBDC platform and the regulator/overseer of payment systems, governance mechanisms must address conflicts of interest (self-regulation) concerns. A central bank operating an rCBDC platform is making operational decisions (technology, participant management) with, by its public objective, possibly regulating and overseeing payment systems generally. This means

---

<sup>44</sup> Section 48(1)(c) of the Central Bank of Malaysia Act provides that, notwithstanding section 76 of the Act, the Central Bank may establish a body corporate or acquire, hold or sell shares of a body corporate, wholly or partly, to operate payment systems or issue payment instruments, and undertake any other ancillary or incidental function or activity, for the purpose of promoting and developing payment systems and payment instruments in Malaysia.

<sup>45</sup> Many central banks are subject to procurement laws or internal policies that ensure transparency, competition, fairness, and value-for-money in selecting private partners. A legal consideration is therefore to align the rCBDC project with these procurement requirements—for example, conducting open, competitive tenders with Request for Proposals for technology providers. Failure to do so can invite legal challenges or reputational damage.

<sup>46</sup> The Eastern Caribbean Central Bank's CBDC (DCash) pilot engaged a fintech firm for the technology, but the central bank retained ownership of the project and could intervene when technical outages occurred.

<sup>47</sup> “An FMI that relies upon or outsources some of its operations to another FMI or a third-party service provider (for example, data processing and information systems management) should ensure that those operations meet the same requirements they would need to meet if they were provided internally” (Explanatory note of Principle 17, PFMI).

<sup>48</sup> Such indemnities are important safeguards for the central bank but partial. Since ultimate responsibility to the public still lies with the central bank, it cannot fully contract out reputational or systemic consequences (as discussed in Section IV). Central banks should thus carefully consider complementing any agreed contractual provision with the exercise of public law powers.

the central bank is regulating and overseeing its own activities: such conflict of interest can undermine effective regulation and oversight unless effectively managed. It could also create perceptions of unfairness if the central bank's payment system is not held to the same standards as private systems. This issue is not novel (for example, central banks both operate RTGS—and, in some cases, fast retail payment systems—and oversee payment systems), but it underscores the need for governance solutions to mitigate such conflicts (see Box 3).

### Box 3. Mitigating Conflict of Interest in Multiple Roles of a Central Bank

A central bank that regulates and oversees payment systems including retail ones and simultaneously operates an rCBDC payment platform, faces an inherent conflict of interest. Mitigating these risks is crucial to maintain safe, efficient payment systems and public confidence in rCBDC. Traditional mitigation measures span governance arrangements, operational structure, and external accountability:

**Independent Oversight Board:** Establish a dedicated oversight board or committee for rCBDC policy with independent members. For example, Australia formed a separate Payments System Board with a majority of external directors to manage such conflicts (Section 25A of the Reserve Bank of Australia Act). This board oversees both wholesale and retail payment systems regulation and its compliance (including the central bank's own systems) and helps ensure decisions are made in the public interest.

**Enhanced Transparency with Regular Audits:** Commit to transparent rule-making and regular audits. Major regulatory and oversight decisions affecting retail payments (for example, standards affecting rCBDC and private retail payment systems) should undergo public consultation. In addition, regular audits of rCBDC operations by independent auditors can verify that the central bank meets the same standards it expects of others.

**Internal Separation:** Create a clear separation between the team operating the rCBDC platform and the team regulating and overseeing payment systems. They should have separate reporting lines to the highest levels. Operational staff are walled off from non-public regulatory or oversight information, and do not influence regulatory decisions or the conduct of oversight. The "Chinese walls" prevent undue information sharing or influence that could favor the rCBDC operation over private retail payment systems or undermine the proper regulations and oversight.

**Periodic Public Reporting:** Require periodic public reports on rCBDC payment platform's performance and its interactions with the wider retail payment market. Public reporting forces self-assessment and allows legislators and stakeholders to hold the central bank accountable to its public mandate given by law.

## Legal Foundation to Regulate and Supervise rCBDC Service Providers

### Regulatory Regime

The regulation and supervision of rCBDC service providers should rest on a robust legal framework. Intermediaries providing rCBDC services (for example, rCBDC wallets, rCBDC service accounts) require effective regulation and supervision. Notably, in some jurisdictions, the central bank is not the regulator or supervisor for payment service providers.<sup>49</sup> Authorities might consider whether assigning that role to the central banks for rCBDC could make sense. The central bank's system-wide perspective and vested interest in payment stability make it a natural candidate, but the overarching goal is to close regulatory

<sup>49</sup> In these jurisdictions, financial services or payment services supervisory authorities typically have the power to license, regulate, and supervise payment services providers.

gaps and ensure all rCBDC payment activities and providers are properly regulated and supervised.<sup>50</sup> If existing regulatory regimes do not adequately cover rCBDC intermediaries, a new, tailored licensing and regulatory regime for them might be warranted (as discussed in the paragraphs of “Legal Relationship as Regulated rCBDC Service Providers” in Section IV).<sup>51</sup>

Authorities can integrate rCBDC services into existing legal categories to avoid reinventing the wheel, but certain adjustments may still be needed. In a two-tier model, intermediaries bridge rCBDC users to central bank’s rCBDC payment platform. These intermediaries (banks, e-money institutions, fintech payment providers, and so on) may already fall under current consumer protection and prudential regulations, but those rules might need tweaks for rCBDC (as discussed in the paragraphs of “Legal Relationship as Regulated rCBDC Service Providers” in Section IV). For instance, strict segregation requirements might be imposed to avoid commingling of rCBDC with claims against the intermediary itself or other rCBDC users. Legal definition might also be expanded (for example, including rCBDC in the definition of “funds” or equivalent concepts in payment laws) to bring rCBDC services under existing payments regulation.<sup>52</sup> This would ensure using rCBDC triggers the same consumer protections, rights, and obligations as other forms of money in payments.

### ***Mandatory Participation of rCBDC Service Providers in rCBDC Platforms***

Following a policy choice, some jurisdictions are considering compelling certain intermediaries—especially major banks—to participate in an rCBDC payment platform to promote universal availability. A challenge in launching rCBDC is achieving widespread adoption. If key payment service providers or banks opt out, the platform might fail to gain traction. To preempt this, some jurisdictions consider mandating participation, to a varying degree, for certain institutions.<sup>53</sup> For instance, the Central Bank of Nigeria (CBN) issued Regulatory Guidelines requiring all licensed financial institutions to serve as eNaira intermediaries. Also, the EU’s draft digital euro legislation stipulates that credit institutions already providing specific payment services (for example, execution of payment transactions) would have to offer basic digital euro services to their clients on their requests (for example, to obtain a digital euro wallet and convert money into digital euros).

Mandatory participation could also further objectives like financial inclusion and payment system resilience. Under such a mandate, rCBDC service providers might be required to serve unbanked or underbanked populations with rCBDC wallets—possibly through simplified onboarding with digital ID for financial inclusion. Ensuring a public alternative means of payment also enhances the overall payment

---

<sup>50</sup> Many financial regulatory or payment reforms have explicitly granted the central bank the power to oversee and regulate payment systems. Examples include: the United Kingdom (Banking Act 2009), the United States (Dodd-Frank Act 2010), India (Payment and Settlement Systems Act 2007), Brazil (Law No. 12,865 of 2013), Kenya (National Payment System Act 2011), Ghana (Payment Systems and Services Act 2019), and Singapore (Payment Systems (Oversight) Act 2006 replaced with the Payment Services Act 2019).

<sup>51</sup> The Bahamian Dollar Digital Currency (BDDC) Regulations, 2021, establish a bespoke licensing regime under which only Central Bank–registered wallet providers may offer BDDC services.

<sup>52</sup> For instance, the EU proposed a legislative package that extends the definition of “funds” to include all forms of central bank money issued for retail use (banknotes, coins, and central bank digital currency).

<sup>53</sup> In the context of fast payment systems (FPS), which are often compared with rCBDC payment platforms, jurisdictions differ in how they approach intermediary participation mandates. For instance, Brazil (Pix) ties mandatory FPS participation to institutional size, Malaysia (DuitNow) mandates all institutions route through its shared platform, and India (UPI) imposes an interoperability mandate on non-bank wallets through FPS. On the other hand, United States (FedNow), the United Kingdom (Faster Payments), and Singapore (FAST and PayNow) contemplate no mandatory participation.



system resilience. These policy purposes might be underpinned by general legal principles or rights (for instance, some view access to basic financial services as fundamental rights).<sup>54</sup>

Any mandatory participation requirement must be justified by public interest and designed proportionality. Forcing private firms to deliver rCBDC services might clash with freedom of enterprise. If jurisdictions choose this route, it should only occur through well-founded laws aiming at essential public goals. The legal justification hinges on demonstrating that the required participation serves a legitimate public purpose, is a suitable and necessary means to that end, and does not unduly or arbitrarily burden the private sector beyond what the public interest requires. By exempting smaller players, allowing cost recovery, and situating obligations in the broader regulated financial system, jurisdictions could reconcile such requirements with constitutional or treaty norms protecting economic freedoms.

### ***Power to Impose rCBDC Wallet/Service Account Portability in Exceptional Cases***

To ensure continuity of access to an rCBDC payment platform and associated services, central banks may be granted legal authority to transfer users' rCBDC wallets or service accounts to an alternative provider if the incumbent provider is unable to maintain rCBDC services.<sup>55</sup> Two main scenarios may prompt such a transfer: (i) the intermediary becomes insolvent or fails; and (ii) it loses relevant user data or has a sustained outage.<sup>56</sup> Under the first scenario, the applicable legal framework would fall within the scope of insolvency or resolution regimes, although additional tailored rules may be needed: the central bank or other relevant authority should be empowered to effectuate the immediate transfer of rCBDC wallets or service accounts as part of the resolution of critical services. Given the urgency and systemic implications, obtaining prior consent from individual users may neither be practical nor appropriate, consistent with established international standards governing the resolution of financial institutions. The second scenario also implicates sensitive legal considerations, in balancing the public interest with private rights. Accordingly, the legal framework enabling such a transfer should be subject to robust regulatory and contractual safeguards. These should include: clearly defined trigger events; specified conditions such as user consent; protections of users' rCBDC holdings and related data, and rigorous oversight and transparency mechanisms to prevent abuse. Though such a carefully structured approach, authorities can ensure continuous user access to their digital currency with minimal operational disruption, thereby bolstering public confidence in rCBDC and preserving the monetary stability.

---

<sup>54</sup> For example, "This Directive also defines a framework for the rules and conditions according to which Member States are required to guarantee a right for consumers to open and use payment accounts with basic features in the Union" (Article 1(2) of the Payment Accounts Directive (2014/92/EU)).

<sup>55</sup> Depending on its system design, from the perspective of privacy protection, a central bank would possibly not engage with the system for managing information about rCBDC users. In this case, another regulatory authority on the user information management component of the rCBDC system could be given such legal authority of rCBDC wallet/service account portability in exceptional circumstances.

<sup>56</sup> For instance, the proposed regulation on the digital euro envisions that in exceptional cases where a digital euro payment service provider is unable to carry out this function, such as when it has lost the necessary data related to the digital euro payment account, the ECB should have the authority to permit the transfer of digital euro payment accounts, and this would allow the new service provider, chosen by the digital euro user, to access the user's digital euro holdings and finalize the transfer without depending on the original, inaccessible rCBDC service provider.



## IV. Legal Relationships in an rCBDC Landscape

In the dynamic world of rCBDC landscape, central banks will have to navigate a complex web of legal relationships that can shape their responsibilities and create potential risks. The nature of these risks depends on rCBDC designs as well as on the type of legal relationships between the central bank and other parties. These relationships can stem from the force of law, either public law (for example, central bank, monetary and payment laws) or private law (for example, property and contract laws). These relationships are generally standardized (that is, identical terms are applicable to all) and enforceable through regulatory bodies and/or courts.<sup>57</sup> Central banks' relationships with other parties can also originate from contractual arrangements. Those are more flexible, limited to contractual terms, and only enforceable through courts. Thus, central banks should identify the type of legal relationships with other actors within the rCBDC landscape and then assess how to manage the allocation of responsibilities in order to mitigate risks. This Note focuses on the relationships between the central bank, intermediaries, and users.<sup>58</sup>

For policymakers and rCBDC users alike, understanding the type of legal relationships is equally important in mitigating risks within the rCBDC landscape. Users need to fully understand the nature and extent of their rights and obligations in rCBDC transactions (for example, whether the payment is final, or users have ownership rights over their rCBDC holdings). It is also essential for policymakers to analyze the legal implications of rCBDC transactions to ensure that key policy objectives (for example, preserving the credit risk-free nature of rCBDC in the case of intermediary failure) are not compromised. Therefore, having clear legal frameworks governing these relationships is vital to reinforce users' rights and public trust in rCBDC initiatives, both critical for the widespread use of this new form of currency. Clear allocation of responsibilities is key and should be addressed by laws (and regulation). Detailed contractual arrangements may also play a role.

### Legal Relationship between Issuing Central Bank and rCBDC Users

Although rCBDC is meant to function as digital cash, the issuing central bank's responsibilities to the rCBDC users could be broader than those to physical cash users. Although both enable users to transact in a *direct central bank liability*, rCBDC transactions could necessitate more intervention and commitments from the central bank compared to cash circulation. For instance, the deployment of a digital retail platform by central banks may be akin to operating a payment system providing direct services to citizens, with the integrity of this system resting on the central bank (as discussed in the paragraphs of "Ownership and Operation of rCBDC Payment Platforms" in Section III). Also, some rCBDC system designs might require the intervention of central banks to complete the execution of rCBDC transactions (for example, to enforce limits or transfer wallets in case of intermediaries' failure).

This section focuses on two types of *links* between the central bank and rCBDC users to assess whether they constitute legal relationships entailing responsibilities for the central bank. The "*asset link*" pertains

---

<sup>57</sup> It should be noted that in that context and as rCBDC activities relate to public mandates, the law sets key obligations on accountability and transparency on central banks toward the public and political authorities.

<sup>58</sup> Other key actors (such as merchants) have significant roles and liabilities in an rCBDC landscape although not within the scope of this Note.

to rCBDC as a direct liability of the central bank serving as money among users. The “*technological link*” pertains to the technological services provided by the central bank, either directly or indirectly, to ensure users’ access and functionality to the instrument and the retail platform.<sup>59</sup>

### **Asset Link**

The asset link could be classified as a direct legal relationship between the central bank and users on two main levels. As rCBDC users hold a *direct liability issued by the central bank*, this, in principle, creates a direct legal link between the two parties.<sup>60</sup> Furthermore, in most designs, this liability is *held* on the central bank’s retail platform. Central banks should carefully assess whether this *holding* creates any legal relationship with the users—and thus any responsibilities. A two-step analysis is useful here. First, there needs to be a distinction whether the user *accounts* on the rCBDC platform are simple identification tools (with no or minimal legal obligations) or whether they represent a legal relationship such as financial accounts (subject to strict legal rules and obligations). If classified as the latter, another layer of classification is required: They could be viewed as *current accounts* (provided legally allowed) where central banks will have, for instance, the legal obligation to promptly repay rCBDC balances upon demand—possibly in the form of banknotes—and abide by court orders requiring the funds’ release. Alternatively, financial accounts could be classified as *safeguarding accounts* imposing, for instance, on the central banks fiduciary duties toward the users (for example, duty to take all reasonable steps to prevent loss, theft or damage to the safeguarded rCBDC). These duties can result in liability for any losses incurred where courts may take action for breach.

Maintaining a direct liability link in two-tier rCBDC models is crucial. The legal framework must ensure that rCBDC remains a direct liability of the central bank at all times, even when they are distributed to the public or held through intermediaries. The law should be clear that such distribution and holding do not convert into claims against private intermediaries. For instance, if holdings at the intermediaries are categorized as traditional deposits with those intermediaries under the law, users’ funds could be subject to the bankruptcy of those intermediaries and users may face delays or losses in the recovery of their funds.<sup>61</sup> This should be resolved through proper legal design tackling at least two fronts: first, the need for a clear rCBDC legal classification (with at least proprietary rights attached thereto), and second, having a clear legal classification of the users–intermediaries relationship for users to fully understand the risks involved (as discussed in the paragraphs of “Legal Relationship between Intermediaries and rCBDC Users” in Section IV).

### **Technological Link**

The technological link may constitute a legal relationship originating from the law. This is based on at least two key legal principles. First, rCBDC is designed to be public goods accessible to all and serving important objectives such as monetary and financial stability; this may imply, in some jurisdictions, a

<sup>59</sup> In theory, the technological link may not exist at all between the central bank and users, for instance in the case where rCBDC are stored in a personal smart phone and the holder can access and use the tokens without any technical application provided by the central bank. It should also be noted that this technological link is also provided in some cases through intermediaries.

<sup>60</sup> In some jurisdictions, this link may not be viewed as a legal relationship with potential legal consequences, by comparing the legal treatment of rCBDC with that one of physical cash.

<sup>61</sup> See Bechara and others (2025) for further details.

legal obligation on central banks to ensure a continuous, universal, reliable and secure technological access thereto, regardless of socio-economic or geographic locations. This is even more true for central banks that have an explicit financial inclusion objective. This obligation would result in responsibilities such as maintaining accessibility, integrity, and security of the rCBDC platform as well as ensuring the proper execution of rCBDC transactions. Second, since currency issuance is a sovereign function, some jurisdictions may prohibit its outsourcing to private entities (as discussed in the paragraphs of “Outsourcing rCBDC Platform Operations to a Third Party” in Section III). This would require that central banks keep a minimum degree of legal and operational control—and therefore corresponding legal responsibility—over the technological services for the issuance and the “burning” of rCBDC. Therefore, when providing technological service directly to users, central banks should carefully assess their legal relationship with those users to understand any responsibility for damages under the law.<sup>62</sup>

The technological link can also arise from contractual arrangements. Beyond any duties stemming from the law as discussed earlier, central banks might opt to formalize their responsibilities and the details of the technological link relationship in general through user agreements.<sup>63</sup> For example, when rCBDC users download an rCBDC application, acceptance of terms and conditions would establish a direct contractual relationship with the central banks. These terms would typically outline the services provided, disclaim warranties and specify users and central bank responsibilities.<sup>64</sup> Central banks should carefully craft those agreements and fully understand the extent of their legal commitments, especially in cases of contractual breaches. For that purpose, those agreements should clearly define the scope of the services provided and the responsibilities of the central banks. Depending on the jurisdiction, central banks may be allowed to include clauses to limit warranties or liabilities for damages or to unilaterally amend terms (as discussed in Box 4). Such limitations, however, should be carefully designed to avoid undermining public policy goals like equivalence to cash or risking reputational harm.

## Legal Relationship between Issuing Central Bank and Intermediaries<sup>65</sup>

Central banks and intermediaries’ legal relationship is multifaceted and requires careful analysis to identify central bank responsibilities. Intermediaries often play at least two roles in an rCBDC landscape: facilitating rCBDC payment transactions and acting as participant in the rCBDC payment platform. These roles create legal relationships with issuing central banks that may arise directly from the laws (and regulations) as well as from contracts executed with those intermediaries.<sup>66</sup>

<sup>62</sup> We note that technological features also, in turn, shape legal relationships and should be clearly regulated in the law to avoid the reclassification risks.

<sup>63</sup> rCBDC users will be allocated “accounts” on the central bank CBDC ledger that will be generally accessed through the intermediaries. A key legal question would be whether the applicable law views this “account” as a financial account or a merely as an identification tool (as discussed in the paragraphs of “Asset Link” in Section IV).

<sup>64</sup> For example, in Nigeria, users must accept the terms and conditions of eNaira application to use and hold eNaira. Those terms state that this application is developed and owned by the CBN and enables “the Bank to provide services to Users” based on the set-up contractual relationship. The App is provided “as is” and the CBN expressly disclaims any warranty or liability in connection with its use and reserves the right to disable or suspend access thereto. Finally, the terms provide that the user is responsible for “safekeeping any passwords, PINs, private keys [...] any other codes to access” the App, but this seems to relate to the authentication codes to access the rCBDC wallet on the App rather than the private keys of the public addresses of the eNaira they hold.

<sup>65</sup> Relationships with the third-party operator and the central bank are covered in Section III for rCBDC and Section VI for wCBDC.

<sup>66</sup> This possibility of different approaches could be compared with the legal setup of traditional central banks’ operations such as monetary policy operations where in some countries they are governed by law whereas in others they are set up using a contractual approach.

## ***Legal Relationship as Regulated rCBDC Service Providers***

Intermediaries offering rCBDC services are likely to fall under the remit of existing legal payment regimes. Almost all rCBDC designs currently envision the use of intermediaries to mainly mitigate the legal, financial, operational, and reputational risks involved. When central banks are also the regulators (and supervisors) of payment service providers, one relevant question would be whether those intermediaries would fall under their remit as regulators. This would depend on whether they or their services offered are captured under existing payment regimes. To achieve this, it is essential to review at least key concepts in payment law, that is, “transfer” and “funds/money” to determine whether they would encompass rCBDC services. In the majority of the current rCBDC initiatives, these intermediaries are in fact viewed as falling under existing payment laws—as they offer a form of transfer of funds that trigger the application of payment laws—and thus are viewed as regulated payment entities. This legal relationship between intermediaries and central banks would stem from the law (rather than from contracts). This would give the central bank, as a regulator, the legal authority to impose specific terms to govern its relationship with the intermediaries and to directly sanction the noncompliance of those terms.

However, adapting existing payment regimes may be necessary to effectively govern rCBDC services and intermediaries. It is important to evaluate legal and regulatory regimes to address at least four primary areas:

- *Regulatory remit over rCBDC service providers as payment facilitators:* Some existing retail payment regimes distinguish—and treat differently—payment services providers that handle funds directly from those *facilitating* payments without handling funds.<sup>67</sup> Examples of such payment facilitators include payment initiators and gateways. In some jurisdictions, these facilitators fall under a less strict payment regime than that governing payment providers, whereas in others, they do not fall under payment regimes at all. Since rCBDC services should be offered in a manner that preserves the direct liability of the central bank at all times, some intermediary services would resemble facilitator’s services where they refrain from handling users’ rCBDC holdings (or recording them on their balance sheets). In the regimes that make these distinctions, authorities should assess whether rCBDC service providers would benefit from any leaner regime of facilitators.
- *New licensing regime for rCBDC service providers:* Many rCBDC designs propose multiple types of rCBDC services such as access, liquidity, and transaction management.<sup>68</sup> This may require issuing several types of licenses. One approach being explored by some authorities is to consider a special license for non-bank firms to serve as rCBDC service providers if not already covered under existing payment laws.
- *Regulatory adaptation to novel services and risks:* Regulatory regimes for rCBDC service providers must be carefully calibrated. Although some of their services might not involve the risks related to the transfer of funds, they present novel risks such as those linked to new functionalities such programmability or offline functionalities (as discussed in Section V). In addition, data portability allowing the central bank to transfer rCBDC wallets—possibly by taking

<sup>67</sup> The 2023 UNIDROIT principles on Digital Assets and Private Law and the use of the concept of control could be useful here to determine if the providers “enter into possession of funds.”

<sup>68</sup> See, for example, European Central Bank (2024).

direct control—to alternative providers (for example, in case of failure of an intermediary or system outage as discussed in the paragraph of “Power to Impose rCBDC Wallet/Service Account Portability in Exceptional Cases” in Section III) should be completed under clear regulatory safeguards. Existing regimes might not be sufficient to address those areas and might need to be updated.

- *Challenges in regulating rCBDC service providers with other core activities:* For providers offering rCBDC services to top off their primary non-payment businesses (for example, Big Tech integrating rCBDC with e-commerce), ensuring proper regulation and supervision is crucial. This regulatory and supervisory framework should be developed in line with international guidance and standards.<sup>69</sup> Supervisors must adequately identify and monitor the risks related to activities of these entities. This is key to mitigate any risks arising from the providers’ diverse activities but also any reputational risk on the issuing central bank. A robust legal framework is essential to grant supervisors the necessary tools, such as consolidated supervision powers, collaboration with other authorities, and efficient information sharing, to effectively manage these risks and protect the central bank’s reputation.

### ***Legal Relationship as Participants in the rCBDC Payment Platforms***

Intermediaries in an rCBDC platform classified as a payment system must adhere to contractual terms and conditions.<sup>70</sup> These terms, outlined in agreements or *rulebooks*, generally cover a single set of rules, standards, and procedures. Rulebooks should be clear, detailed and cover the key areas such as operation, compliance, allocation of liability, participant management, cost allocation, data sharing and technology requirements (Bank of Canada, Swiss National Bank, European Central Bank, Bank of England, Bank of Japan, Board of Governors of the Federal Reserve System, Sveriges Riksbank, and BIS 2024). In addition, mechanisms for dispute resolution between the central bank as the platform operator and intermediaries (for example, in case of fraud) must be clearly defined.

Rulebooks can also be issued through regulations. Although rulebooks primarily govern the relationship of the central bank and the intermediaries, they may also include terms on the intermediaries that affect third-party rights such as those of rCBDC users (for example, users’ rights in case of disputes with the intermediaries, fees limitations or fraud prevention). However, under the principle of privity of contract, only direct parties to an agreement can enforce its terms. Therefore, to enable users to enforce rights in the rulebook, they may need be issued in the form of a public law instrument, giving a public authority—depending on jurisdictions, possibly the central bank—the power to sanction noncompliance with its terms by the issuance of administrative sanctions such as fines. Furthermore, the rulebooks should clarify whether and how users can pursue legal action for any rulebook breaches.

### **Legal Relationship between Intermediaries and rCBDC Users**

If rCBDC services are classified as regulated services, the legal relationship between users and intermediaries will primarily be governed by payment laws. This imposes minimal flexibility for

---

<sup>69</sup> On the broader topic of Big Tech’s regulation and supervision in finance, see Bains, Sugimoto, and Wilson (2022).

<sup>70</sup> As discussed in section III, depending on the jurisdictions, participation in rCBDC platforms might be on a voluntary or mandatory basis. If the latter option is chosen, it is important that there is a legal foundation that justifies this mandatory approach.

intermediaries to customize terms (for example, limitation of liability or warranties) and allows supervisors to enforce user rights through fines or penalties. In case of regulatory gaps concerning specific functions such as programmability, offline services or data portability, regulations should ideally be updated as mentioned earlier. Alternatively, agreements between intermediaries and users could address these gaps provided they are consistent with the rulebooks intermediaries must follow as rCBDC platform participants. As rCBDC services vary—such as management of access, liquidity, and transaction—the extent of users’ recourse for damages against those intermediaries would be tailored in those agreements depending on the type of service provided.

To maintain the credit risk-free nature of rCBDC, users’ holdings must be legally ring-fenced from the intermediaries’ estates. This requires legal certainty and clarity, particularly in private and financial laws, in relation to two key areas. First, ideally, the legal classification of rCBDC should give the users propriety rights over the rCBDC. In addition, and as discussed in Bechara and others (2025), it should not be legally equating the service offered by the intermediary to an rCBDC “deposit” (where the legal title to this central bank direct liability—that is “deposited” at the private intermediary—could convert into a private claim against that intermediary to repay the same amount of rCBDC deposited upon demand). Failure to do so would not be conducive to a bankruptcy remote feature of the rCBDC’s holding nor would it protect the rCBDC holding from any attachment or seizure orders resulting from intermediaries’ actions.<sup>71</sup> Therefore, the legal relationship between rCBDC users and intermediaries must be structured using legal mechanisms that preserve this legal title to the rCBDC for the users, such as safekeeping, custody, or trust.<sup>72</sup>

The law should safeguard the users’ rights to retain (and recover) access to their rCBDC in case of intermediaries’ failure. If an intermediary fails to provide rCBDC services (including in the cases of operational failure or insolvency), its users might lose access to their rCBDC despite retaining legal title. Thus, the law should establish enforceable contingency mechanisms for users to regain technical access to their holdings. This could include granting the power to the issuing central bank to directly intercept and access the system of the intermediaries or to enable seamless wallet and data transfer to alternative rCBDC service providers through data portability provisions (as discussed in the paragraph of “Power to Impose rCBDC Wallet/Service Account Portability in Exceptional Cases” in Section III).

Clarity is needed regarding rCBDC users’ rights to seek indemnification from intermediaries. This is a two-pronged analysis. First, if damages arise solely from central bank-controlled failures (for example, system wide technical failure of the central bank core ledger that results in the delay of processing or breach of foundational security standards in the system design), users cannot claim indemnification from intermediaries unless explicitly provided for in the law or regulation (Bank of Canada, Swiss National Bank, European Central Bank, Bank of England, Bank of Japan, Board of Governors of the Federal Reserve System, Sveriges Riksbank, and BIS 2024). However, intermediaries might still be liable for

<sup>71</sup> In some jurisdictions, the principle “ownership of cash lies with the holder” could imply that if an intermediary handles rCBDC on a user’s behalf, the intermediary might be deemed the owner. To avoid this, agreements can specify that the intermediary handles the rCBDC as a specific identifiable asset of the user (for example, like “cash in an envelope”). However, in certain jurisdictions, contractual arrangements might not be sufficient, and legal reform might be needed.

<sup>72</sup> The 2023 UNIDROIT Principles on Digital Assets and Private Law could also be useful in this area.



inadequate contingency measures.<sup>73</sup> Second, when damages result from failures under both the central bank and the intermediaries' control, clear allocation of responsibilities as well as clear procedural mechanisms to follow up with any indemnification recovery process must be established. It is important to note that if intermediaries act on behalf of the central bank in an agency relationship, liability should be cautiously assessed accordingly. Some frameworks (for example, digital euro or digital pound) might be viewed as suggesting that liability—and ensuing legal responsibility to indemnify the users—follows control: intermediaries are responsible for tasks such as compliance and user interfaces, whereas central banks handle systemic integrity and fail-safes. Nevertheless, this approach may still be challengeable in court if the financial consideration for intermediaries in the relation between the central bank and intermediaries, or between intermediaries and users, is not existent or imbalanced.

#### Box 4. General Legal Principles Applicable to Both Central Bank–Users and Central Bank–Intermediaries Relationships

Whether the relationship arises from the law or contract, several general legal principles might apply:

- **Fundamental rights constraints:** rCBDC, as public goods, should be designed to respect fundamental rights principles. For example: (i) *Non-discrimination*: Authorities cannot introduce measures that arbitrarily disadvantage certain groups; (ii) *Proportionality*: Any restrictions imposed through monetary policy or financial regulations must serve legitimate public interests and be proportionate to the related public policy objectives; (iii) *Access to justice*: If the authorities' actions (for example, freezing an rCBDC wallet) affect individuals, those affected must have legal remedies; (iv) *Property rights*: For the legal regimes that classify property rights as fundamental rights, authorities must obtain users' consent prior to any actions that could infringe on their property rights (for example, requiring rCBDC users in a pilot to accept that their rCBDC holdings will be burnt at pilot's conclusion).
- **Immunities and legal protection:** In many jurisdictions, when a central bank acts as a public authority pursuing its mandate, they benefit from certain immunities and legal protection. For instance, central banks could be protected from lawsuits for acts or omissions performed pursuant to and in the course of their public duties (unless proven intentional wrongful conduct or gross negligence).
- **Other general legal principles:** Common general legal principles, like agency, may also be relevant. For instance, under *agency* principles, a principal is ultimately responsible for its agents' actions taken within the scope of their authority. This implies that even if central banks outsource some of their functions to private entities, central banks might remain ultimately responsible for their actions.

Even if rCBDC designs explicitly exclude any contractual relationship between the central bank and users, that alone may not eliminate all risks to the central bank: The law can stipulate that no contract exists between the central bank and users (to avoid implying an intent to enter into a contract). Nevertheless, depending on the legal traditions, central banks might still be held responsible to provide remedies to users harmed by the use of rCBDC because of their actions or omissions. This responsibility could arise from general principles of liability that are non-contractual liability (for example, tort) or specific laws (for example, general administrative law). Such responsibility is particularly relevant given the high operational risks (technical failures, cyber risks, data breaches) and third-party risks (for example, technology provider's failures) inherent in the rCBDC platform.<sup>[1]</sup>

[1] For instance, in the pilot, the Eastern Caribbean Central Bank (ECCB) had to go offline for a month in 2021, and the central bank's website had noted that the "ECCB guarantees all funds on the Dcash network against losses due to infrastructure failure for the duration of the pilot."

<sup>73</sup> "Pursuant to policy goals, each risk that could arise in the system might be clearly and unambiguously allocated through that framework to the party that is most appropriate to bear it or best able to mitigate it" (Bank of Canada, Swiss National Bank, European Central Bank, Bank of England, Bank of Japan, Board of Governors of the Federal Reserve System, Sveriges Riksbank, and BIS 2024).



## V. Specific Functionalities: Limits, Interest, Programmability, and Offline Transactions

### Limits on rCBDC under the Lens of Law

For financial and monetary stability policy purposes, jurisdictions may consider imposing justified and proportionate limits typically on rCBDC usage and fees for rCBDC services. This can be done through laws or regulations that cap rCBDC holding amounts, transaction sizes, and rCBDC transaction fees.

#### ***Limits on the Aspect of Store of Value: rCBDC Holding Amount***

Limits on rCBDC holdings are essential to mitigate financial disintermediation risks and must be clearly grounded in law. Although broad accessibility supports inclusion, rCBDC designs must preserve financial and monetary stability, particularly by preventing large-scale deposit outflows from commercial banks because of rCBDC's appeal as a safe and efficient instrument. Legally authorized caps on individual holdings can help contain such risks and should be exercised for public policy purposes. In that vein, some designs propose a “waterfall mechanism” to automatically redirect excess rCBDC balances to commercial bank accounts, which may raise property rights concerns in certain jurisdictions as a result of the conversion of central bank money into risk-bearing commercial bank deposits. To address this, the legal framework must ensure transparency, proportionality, and user consent. Jurisdictions have adopted varying approaches: the Bank of England proposes a £10,000–£20,000 cap during the digital pound's rollout; China applies tiered limits based on user identification levels; and Nigeria's eNaira imposes wallet limits ranging from 120,000 to 5,000,000 Naira for individuals, with no cap for merchants.<sup>74</sup>

The authority to set specific rCBDC holding limits should be vested primarily in the central bank, possibly in coordination with the government, to balance central bank's autonomy with the broader mandate of financial stability. Codifying such limits into law could impinge on the central bank's functional autonomy, as statutory provisions may lack the adaptability required to respond to evolving economic and financial conditions. Consequently, delegating this authority primarily to the central bank, with ensuring clear accountability mechanisms, may be warranted. Nonetheless, depending on each jurisdiction's legal and institutional framework, close coordination with the government remain key to achieve financial stability objectives without prejudice to the central bank's mandate.

#### ***Limits on the Aspect of Means of Exchange: rCBDC Transaction Amount***

Transaction limits fulfill multiple operational and policy purposes, and they must be based on a clear legal foundation. Operationally, caps on rCBDC transaction amounts can prevent demand spikes that could overwhelm the underlying infrastructure. From a financial stability perspective, they can also act as a safeguard against large and abrupt capital outflows or sudden shifts from commercial bank deposits into rCBDC, especially during periods of market stress. If the central bank is to wield this power, it must be legally authorized. For instance, in Russia, the law empowers the central bank to set digital ruble

---

<sup>74</sup> Section 10.4 of the Regulatory Guidelines on eNaira 2021.

transaction limits: Article 18 paragraph 17 point 18 of the Federal Law No. 86-FZ of July 10, 2002, “On the Central Bank of the Russian Federation (Bank of Russia)” states that the Bank of Russia determines the *maximum amounts of transactions* with digital rubles.

### **Limits on Fees Charged for rCBDC Services**

Limits on fees for rCBDC services help achieve the desirable attributes like legal tender status, which require a clear legal basis. Fee caps should be justified (including cost-linked issues) and proportionate, otherwise they could be seen as an unlawful reduction of face value. Setting limits on the fees is key for rCBDC to act as public money and also helps incentivize the use and trust of rCBDC. For example, the draft EU digital euro regulation aims to ensure free basic digital euro services for euro area residents (including certain former residents and visitors) in line with its legal tender status. It should be noted that, in some jurisdictions, financial regulators may lack the power to regulate the fees charged by payment service providers, unless explicitly empowered by law. Legally, two dimensions arise: (i) from the providers’ perspective, giving central banks authority to cap fees must consider free market principles; (ii) from the users’ perspective, in some jurisdictions, Constitutions guarantee the right to be financially included to basic financial services, making fee caps on basic rCBDC services easier to justify than on more advanced services.<sup>75</sup>

### **Interest Bearing rCBDC**

Allowing rCBDC to bear interest could have financial and monetary stability implications and must be consistent with other rCBDC desirable attributes. At least from the legal perspective, the question of remunerating rCBDC should be analyzed in conjunction with features like legal tender, *cours forcé*, and convertibility (as discussed in the paragraphs of “Cours Forcé” and “Legal Tender” in Section II). In the majority of rCBDC projects, rCBDC is non-remunerated.<sup>76</sup> For example, the Bank of England envisions the digital pound like a digital banknote, with zero interest. Russian law explicitly prohibits accruing interest on digital ruble balances (National Payment System Law, Article 30.8(4)). China’s e-CNY does not pay interest, nor does India’s retail digital rupee (e₹-R).<sup>77</sup>

### **Programmability**

Designing rCBDC as *programmable money* raises significant policy and legal concerns. Programmable money refers to digital money encoded with conditions on its use (for example, restricted to buying

---

<sup>75</sup> For example, the requirement under EU law for credit institutions to offer payment accounts with basic features either free of charge or for a reasonable fee is consistent with the principle of economic freedom. This obligation is established by Directive 2014/92/EU, which seeks to enhance financial inclusion and ensure access to essential banking services, particularly for vulnerable populations (as discussed in Section III). Although Article 16 of the Charter of Fundamental Rights of the European Union guarantees the freedom to conduct a business, this right is not absolute. Pursuant to Article 52, limitations may be imposed where they are prescribed by law, respect the essence of the right, and are proportionate and necessary to achieve objectives of general interest, such as consumer protection and the prevention of financial exclusion. The directive’s requirement is narrowly targeted, does not impede the overall conduct of business, and permits reasonable fees where justified. It thus represents a proportionate measure that appropriately balances commercial freedom with legitimate public policy objectives.

<sup>76</sup> Purely theoretically, rCBDC could be a monetary policy instrument to affect monetary transmission. For further details, see Das and others (2023).

<sup>77</sup> Some central banks, such as the Bank of Israel, consider the possibility of designing its CBDC as an interest-bearing instrument.

certain goods, or carrying an expiration date).<sup>78</sup> Most authorities have stated they will not make rCBDC programmable in this restrictive way.<sup>79</sup> This stems from policy motivations (for example, if rCBDC is designed as programmable money, this will not square with its legal characterization as currency with legal tender and convertibility as its key features discussed in the paragraphs of “Cours Forcé” and “Legal Tender” in Section II). There are also legal obstacles that would hinder the existence of such a design: Programmable money could violate fundamental private rights like property rights, often constitutionally protected, since restrictions on rCBDC owned can undermine users’ rights and reduce user autonomy, potentially amounting to state interference in private economic matters. Setting an expiration date may deprive rCBDC users of wealth retention, risking claims of expropriation if done without due process. Programming limits on who can hold or receive rCBDC could hinder market participation and contractual freedom, and may cause discrimination if not applied proportionately and transparently aligned with the public interest. If a jurisdiction did opt for a programmable rCBDC, explicit legal authorization would be required, along with safeguards to protect users from misuse or unintended outcomes and to ensure transparency in how programming operates.

Authorities should carefully assess how to address the legal implications for designing rCBDC that can be used for *programmable payments*. Programmable payments (or conditional payments) are initiated by the rCBDC user and do not alter the nature of the currency itself. This concept refers to payments that are executed automatically based on predefined conditions external to the currency (for example, an automatic rent payment each month or delivery-versus-payment conditions). Such functionality already exists in banking (for example, standing orders, recurring payments, spending limits) and is not new per se, but implementing it within central bank digital money for the public is novel. Although making rCBDC itself “programmable money” may be incompatible with its currency status, enabling conditional payments could spur rCBDC adoption by allowing automatic transfers when certain conditions are met.

Existing laws might need updating to accommodate unique functionalities like smart contracts in rCBDC in the context of programmable payments. Programmability could involve smart contracts—self-executing agreements that automatically validate and enforce terms once conditions are met. The rise of such novel techniques often brings legal uncertainty. Issues include whether agreements formed through smart contracts are legally binding, and how to interpret or enforce contract terms executed by code. Jurisdictions may need to clarify these points to ensure legal certainty in rCBDC operations that use smart contracts (Garrido 2023).

Authorities should assess whether programmable payments introduce new regulatory risks, and if so, how to adequately capture those risks under applicable laws. It is crucial that regulators have clear power to regulate programmable payments services related to rCBDC, to mitigate any financial stability or consumer protection concerns. Regulatory regimes might require updates to cover this new service type and its risks. Ensuring standardization and interoperability would also be key for the successful deployment of these programmable features.

---

<sup>78</sup> Modern technologies have been increasingly explored to provide programmability in payments. It is important to distinguish for the purpose of this Note between programmable *money* and programmable *payments*.

<sup>79</sup> For instance, although it may be possible to program the digital pound so that it could only work in certain ways, this is not relevant to HM Treasury and the Bank’s policy objectives for the digital pound. Further, this functionality could damage the uniformity of the rCBDC and cause user distrust. For these reasons, HM Treasury and the Bank will not pursue government or central bank-initiated programmable functions.

Jurisdictions should clarify liability allocation if users incur losses because of programmable features (for example, malfunctions or malicious exploits). Users could possibly lose funds because of coding errors locking their rCBDC or because of hacks targeting programmable functions. It is worth noting that in some rCBDC designs, the central bank does not directly offer programmability (even in limited forms like direct debits); instead, such features might be offered by intermediaries through their contracts with users. The overall framework should clearly delineate who bears responsibility in various scenarios involving programmable payments.

## Offline rCBDC Transactions

Many rCBDC designs explore offline payments functionality for policy purposes. Literatures such as the IMF Fintech Note on offline rCBDC transactions (Tourpe and others 2025) and the BIS project reports generally define offline rCBDC transactions as transfers of value between devices that occur without connecting to any ledger system.<sup>80</sup> Solutions include peer-to-peer or point-of-sale transfers using devices like smart phones or battery-powered smart cards. This feature is useful during network outages or in areas without connectivity, similar to physical cash's role when electronic systems fail.<sup>81</sup> Implementing offline payments can help achieve policy objectives like enhancing payment system resilience and promoting financial inclusion.<sup>82</sup>

The law should clearly specify when settlement finality occurs for offline rCBDC transactions.<sup>83</sup> Settlement finality is the irrevocable and unconditional transfer of an asset or discharge of an obligation in accordance with the terms of an underlying contracts (CPSS and IOSCO 2012). Whether rCBDC payment platforms would require the same level of settlement finality protection as interbank settlement system to neutralize insolvency rules depends on the risks and would relate to both online and offline transactions.<sup>84</sup> Independently, offline rCBDC transactions hold an additional layer of settlement concerns (for example, in the case of the insolvency of the payer) because of a potential lag between the time of

---

<sup>80</sup> See, for instance, BIS Innovation Hub (2023a). Also, the proposal for a digital euro regulation defines the “offline digital euro payment transaction” as a digital euro payment transaction, made in physical proximity, where authorization and settlement take place in the local storage devices of both payer and payee. The Bank of England defines an “offline payment” as a payment that occurs when neither payer nor payee has access to the CBDC network, usually because of the lack of an internet connection (Bank of England 2025).

<sup>81</sup> According to BIS, three offline modes are assumed: (i) Fully offline: Here, the value that has been exchanged from a payer to a payee can be spent again immediately and indefinitely. There is no requirement for connecting back to the online system; (ii) Intermittently offline: This is similar to fully offline but sets risk management or technological limits, the payer must reconnect to the online system before they can continue with further transactions; (iii) Staged offline: Here, after a payer has sent value to a payee, that value cannot be spent again until the payee who received that value connects back online (BIS Innovation Hub 2023b).

<sup>82</sup> According to the Bank of Canada experts, the choice of settlement mechanism for rCBDC transactions—whether instant or deferred—has significant implications for transaction finality and offline usability. Instant settlement, which enables immediate transfer of ownership, is essential for supporting transitivity in offline environments. In contrast, intermittent offline models, where funds are not stored locally, rely on deferred settlement and involve the creation of claims redeemable upon reconnection, raising risks such as double spending because of potential inconsistencies between offline and online records. Although embedding transaction histories may facilitate reconciliation, it introduces counterparty and operational risks and is constrained by current hardware limitations. Extended offline models, where funds are stored on the device, allow for real-time settlement and ownership transfer without online synchronization, thereby enabling transitivity over prolonged offline periods (Minwalla and others 2023).

<sup>83</sup> This Note focuses on settlement finality as protection in payment and settlement systems, which is generally addressed in public law. There are other types of areas, mainly related to private laws discussed in Bechara and others (2025), which should also be first addressed as to achieve the settlement finality (for example, perfection of transfer or the impact of general rules such as “nemo dat” rule) that could apply to rCBDCs (the nemo dat rule is the general rule that a person who does not have adequate ownership of goods or property cannot transfer good ownership to someone else).

<sup>84</sup> See discussion under Section V-B (Insolvency Protection, Payment System Settlement Finality, and Transfers of Token-Based CBDC) of Bechara and others (2025).

the transaction and the reconciliation with the core CBDC ledger (if and when required). Although there can be various technological offline models, from a legal perspective, it is important that, in any solution, legislative clarity regarding the finality moment is ensured. One solution, as proposed in the draft digital euro regulation, is that the law explicitly provides that final settlement occurs at the moment of updating the records of relevant digital euro holdings in the local storage devices of, respectively, the payer and the payee, irrespective of whether digital euros are recorded as holding balances or units of value, or regardless of the technology used.<sup>85</sup>

Legal provisions may be needed to maintain the singleness of money in the context of offline rCBDC. The law might explicitly state that both offline and online rCBDC have legal tender status. The legal framework might also allow payees to refuse an offline rCBDC payment in good faith because of reasons beyond their control (for example, a malfunctioning device). Furthermore, to ensure the singleness of money, the law could guarantee full convertibility at par between offline and online rCBDC.

Clear compensation rules are needed for losses related to offline rCBDC use. Offline users face risks that online users do not. For example, depending on the system design, losing an offline device (or having it stolen) could mean losing the rCBDC stored on it—unlike online wallets which could be cloud-backed. Also, since rCBDC intermediaries cannot monitor or block offline transactions in real time, an offline user defrauded by a rogue transaction might not be compensated (Bank of Israel 2025). Therefore, jurisdictions should assess if specific compensation rules for offline rCBDC losses are necessary or if general rules suffice. In any event, roles and liabilities in offline payments must be clearly defined (for example, who is liable for double-spending). Intermediaries should be obliged to disclose to users the risk of loss if an offline device is lost or stolen (Bank of Israel 2025). Cybercrime risks, in addition to all other types of frauds, require prudence with risk reduction measures being taken by central banks, and potentially adapting laws on counterfeiting to fit this new type of risk.

Finally, the legal framework should ensure certainty about the validity of transferring ownership rights in offline rCBDC transactions. The law should be clear that an offline transaction can legally occur and be perfected (that is, meet all requirements for transfer of ownership). This includes clarifying the roles of offline rCBDC wallets and any transaction registries.<sup>86</sup> Depending on its system design, an additional challenge is how the “good faith purchaser” rule applies if an offline wallet device is lost or stolen. Legislators may need to address whether, for example, someone who unknowingly receives stolen offline rCBDC could obtain a good title.

<sup>85</sup> Bechara and others (2025) discusses the private law implications and risks related to the perfection of rCBDC transfers including the risk of double-spending in Box 4 (“The Legal Challenges of Offline Transactions”).

<sup>86</sup> See Bechara and others (2025) for further details.

## VI. Selected Legal Aspects of wCBDC

### Definition and Scope

For the purposes of this Note, wCBDC refers to a tokenized form of central bank money accessible only to a predefined entity group, typically financial institutions. This section analyzes wCBDC designed for a prominent use case: the facilitation of payments (that is, wCBDC serving as money and a settlement asset). We focus on models where issuing and operating wCBDC is not expected to economically change the central bank balance sheet, and wCBDC is intended to be fully fungible with reserves held at the central bank. This means that wCBDC would be treated economically the same as reserves (for example, it might be remunerated similarly, qualify as high-quality liquid assets, and be accounted for like reserves). Also, this Note generally focuses on wCBDC models that result in the creation of an instrument not clearly covered by existing legal classification. Notably, it is important to distinguish between (i) wCBDC not legally classified as current account deposits and (ii) tokenized current account deposits that are legally identical to existing current account deposits and do not require amendments or new legal interpretations.

### Legal Aspects<sup>87</sup>

#### ***Legal Certainty over the Nature and Validity of Operations of Tokens***

As a tokenized form of central bank reserves, wCBDC raises legal challenges inherent to tokenization. Tokenization involves creating digital representations of assets, and legal intervention is essential to ensure alignment between tokens and the underlying assets they represent. In the case of wCBDC, tokens would typically reflect a financial institution's rights vis-à-vis the central bank. A common model is linking tokens to financial institutions' accounts in the RTGS system. In this model, wCBDC tokens represent contractual rights mediated through the RTGS accounts. A key legal risk is desynchronization between token ledgers and RTGS systems, potentially enabling double spending or circulation of unbacked tokens. Legal frameworks must thus ensure real-time reconciliation and enforceable backing mechanisms. As the legal framework for wCBDC evolves, clear definitions of token types and robust mechanisms for legal enforceability are critical to maintaining trust, transparency, and systemic integrity.

The nature and extent of wCBDC user's rights can vary depending on how wCBDC is legally linked to central bank reserves. Although credit risk might not be a concern (since reserves are at the central bank), other risks (like operational risk) exist. Ideally, this link to the reserves needs to be enshrined in the law, unless legal frameworks allow for contractual arrangements. Fundamental legal rules are needed to ensure certainty for token operations. Beyond rules linking tokens to assets, the law should address rules governing issues such as transferring tokens (including loss, illegal transfers, or good-faith acquisition) and effects of counterparty insolvency (Garrido 2023). Jurisdictions should strive for legal certainty on these issues through legal reforms or contracts where appropriate.<sup>88</sup> In addition, they should

<sup>87</sup> This section focuses on the distinguishing challenges of wCBDC as opposed to rCBDC. Nevertheless, some of the legal challenges raised in the context of rCBDC in the previous sections could also be relevant in the context of wCBDC such as the challenge brought by programmability, the use of smart contract, or the general rules related to the governance of central banks.

<sup>88</sup> Another relevant legal area that would need legal certainty is whether wCBDC could be used as a collateral and what would be the implications for insolvency and priority claims. The issues are discussed in detail in Bechara and others (2025).



carefully consider whether to give wCBDC currency status (given its limited scope) or to rely on contractual arrangements instead.

### ***Mandate of the Central Bank to Issue wCBDC***

A key question is whether central banks have legal authority to issue this tokenized form of central bank money. Several legal areas are typically explored to assess this power:

- *Issuance of central bank liabilities:* In most jurisdictions, central bank laws explicitly authorize two main forms of central bank liabilities that could be used as money: currency (that is, physical banknotes and coins) and balances (reserves) in accounts at the central banks.<sup>89</sup> Each jurisdiction should determine if wCBDC issuance is legally allowed. If wCBDC is seen as functionally equivalent to reserves, existing authority of the central bank might suffice.<sup>90</sup> If wCBDC is considered a new type of liability, for instance, in the context of tokenization, current powers might not allow such an issuance, thereby raising the risk that the central bank could act *ultra vires*—beyond the scope of its legal mandate. Relevant elements for this classification process depend on legal traditions including private law classification of properties as new and on accounting treatment of wCBDC as a new type of liability. In jurisdictions where the law does not grant the central bank the requisite competence to issue this new type of liability, legislative changes are a precondition.
- *Opening of accounts at the central bank:* Jurisdictions should check whether existing legal provisions on central bank accounts suffice for issuing wCBDC. Legal reform may be needed to allow wCBDC issuance in a token form recorded separately on the balance sheet.
- *Payment system mandate:* Depending on wCBDC's design and domestic legal interpretation, the general mandate to promote efficient payment systems might or might not allow setting up a wCBDC platform. To avoid legal and reputational risk, authorities should ensure that both central bank law and payments law clearly permit establishing a wCBDC system.
- *Extended access:* If wCBDC access is extended to non-bank institutions not currently eligible for central bank accounts, legal reforms might be required. Authorities should assess necessary adjustments (and accompanying regulation/supervision of those entities) to safely broaden the wCBDC access.

### ***Central Bank Operation and Control of the wCBDC Platform***

If a wCBDC platform is designated as a systemically important one, PFMI standards apply. Most wCBDC designs target large-value interbank payments or securities settlements, which could qualify them as systemically important because of the market risks involved under payment and settlement systems laws. If so, observance of PFMI standards should be ensured (for example, PFMI Principle 1 requires a well-founded, clear, and enforceable legal framework for all material activities of an FMI, as discussed in Box 2).

<sup>89</sup> Central bank laws also typically grant central banks the power to issue other types of liabilities not meant to be used as means of payment such as certificate of deposits that are meant to serve primarily for monetary policy purposes.

<sup>90</sup> This might not be enough as wCBDC could be classified as new type of property that will require legal reform in private law to achieve its full purposes.



A central bank should have statutory authority to own and operate a wCBDC platform: If a central bank outsources wCBDC platform operation, it must have legal permission and retain control. Legal reform may be needed to ensure the central bank is empowered to own and operate the wCBDC platform, or to outsource operations to third parties. In some jurisdictions (for example, Switzerland), the law permits the central bank to issue wCBDC on a platform operated by a third party (private company) and outsource tasks to that operator (as demonstrated in Project Helvetia under Swiss law). An additional relevant question is whether such an outsource could also extend to the operation of settlement accounts held at the central bank. Since the central bank remains ultimately responsible for a wCBDC platform in outsourcing its operation, it must retain control and oversight through technical and contractual means. Such arrangements might include identifying weaknesses and risks, powers to require changes, authority to suspend specific participants, and ability to block transactions if suspicious or risky. Consequently, if the central bank exercises such control, the law should address its corresponding responsibility for potential losses.

### ***Legal Relationship between Central Bank and wCBDC Users***

#### ***Asset Link***

There may be two parallel legal relationships between the central bank and wCBDC users regarding the wCBDC holding, and legal certainty is needed for both. In the model where no intermediary is involved, the central bank–user relationship can be direct in terms of the asset link:

- *Reserves relationship*: If wCBDC is essentially tokenized central bank reserves, there is a foundational layer where an account is recorded on the central bank's books for the user. Central bank laws and payment laws governing central bank accounts apply, as well as any typical contractual arrangements, and the account holder has, at minimum, a monetary claim against the central bank for repayment.
- *Token relationship*: In parallel, there is a relationship concerning the token that represents those reserves. Central banks should carefully assess how the law classifies this relationship and the nature of the token. This would determine the nature and extent of the obligations the central bank has to wCBDC users. The classification of the token—whether it is just evidence of the reserves or a property of its own—and the legal relationship or role of the central bank—whether it is just a recordkeeping relationship or a safekeeping of assets—would depend on the wCBDC design and legal framework in every jurisdiction.

Contractual arrangements could be explored to govern the rights of wCBDC users, although they might not be sufficient. For example, wCBDC users might agree in advance that what is recorded on the platform—the wCBDC balance—represents a claim on the central bank reserves held thereto in connection with the wCBDC user. However, such contractual arrangements alone may not be sufficient under the existing legal rules on finality and insolvency. Legal reform might still be needed to address scenarios like a payer's insolvency in the gap between a wCBDC transfer and reconciliation of the reserves balances at the central bank.

#### ***Technological Link***

Effective governance of the technological link in the wCBDC landscape may require legal reform and suitable contractual arrangements based on the central bank's role. This reform and contractual

arrangements should address the following areas in relation to the various technological services offered by the central bank to wCBDC users (for example, platform access, operation, maintenance):

- *Nature of the relationship*: The nature of this relationship for the provision of these services could be comparable to the one in case of rCBDC (as discussed in the paragraphs of “Technological Link” in Section IV) where general liability rules could hold the central bank liable. It is likely that central banks will formalize this through contractual arrangements (rulebooks), such as in the context of RTGS. In theory, unlike rCBDC rulebooks where third parties’ rights such as the end-users will be affected and could be issued in the form of regulation, that might not necessarily be the case for wCBDC rulebooks.
- *Third-party platforms*: Alternatively, the central bank might use a third-party front-end platform for wCBDC, not directly providing technological services to users (for example, the role of the central bank could be limited to providing the asset by the tokenization of the reserves and would end once it is released on the platform operated by the third party). In that case, the central bank’s responsibilities on the technological level might be limited to maintaining the integrity of its own internal system linked to the third-party platform. Legal reform could be necessary to allow central banks to issue wCBDC on a privately-operated platform (as discussed in the paragraphs of “Central Bank Operation and Control of the wCBDC Platform” in Section VI). It should be noted that if the third party operates the platform on the central bank’s behalf, the central bank’s responsibility should remain.

## Settlement Finality

Legal frameworks should recognize settlement finality for wCBDC transactions. Settlement finality is achieved when the settlement of an obligation becomes legally irrevocable and unconditional.

Jurisdictions should make sure that solutions considered for various challenges can be implemented by legal reforms unless contractually possible:

- *Finality of transfer*: A significant legal issue for wCBDCs is determining when a token transfer is considered final under the law—identifying the single finality moment of transfer of wCBDC units, from the transferor to the transferee.<sup>91</sup>
- *Impact of insolvency regimes*: Insolvency laws might affect the finality of wCBDC transfers already perfected, for instance, for prevention of fraud purposes. The main question is whether a wCBDC platform would get protection under the existing settlement finality laws.
- *Consensus mechanisms*: In addition, legal complexities may appear around identifying the exact moment of the transfer in some system designs. For wCBDC designs with probabilistic settlement, finality could be defined as after a certain percentage of validators confirm a transaction or several blocks are added to the chain.

---

<sup>91</sup> Bechara and others (2025) delves into this extensively.

## VII. Conclusion

This Note aims to assist policymakers in identifying and addressing key legal issues relevant to the issuance of CBDCs, with a primary focus on rCBDC and a separate analysis of wCBDC. It is not intended to constitute, and should not be construed as, a recommendation for member jurisdictions to issue CBDCs—its purpose is rather to navigate the authorities on the key legal considerations guiding their decision-making process. As set out in the Introduction (Section I), this Note builds on prior IMF legal work and draws from enacted laws, regulations, and public drafts in order to support jurisdictions in evaluating the adequacy of their legal frameworks. This concluding section recaps the principal legal findings and implications for rCBDC—particularly regarding its legal nature under public law, issuance mandate, and legal relationships in its landscape—before turning to the distinct legal aspects associated with wCBDC.

Analyzing rCBDC begins with its public law nature as a central bank liability and whether it should be granted currency status. rCBDC is a central bank liability—a new form of central bank money. As such, it carries the key attribute of being credit risk-free, unlike privately issued instruments. rCBDC's availability to the general public is its distinguishing feature among other digital central bank liabilities. Consequently, many jurisdictions could view rCBDC as “digital cash,” granting it currency status. This implies that the monetary authority holds the exclusive issuance right, rCBDC payments honor the face (nominal) value, and there is a 1:1 convertibility with other central bank money and with commercial bank money to support the singleness of money. Jurisdictions can also extend administrative and criminal protections to rCBDC's issuance monopoly and legal tender status, and penalize rCBDC cybercrime and fraud.

The legal mandate for rCBDC issuance requires clear central bank authority to issue it, alongside legally sound, well-regulated rCBDC payment platforms and intermediaries. An explicit statutory mandate for rCBDC issuance reduces legal risks and challenges. Given rCBDC's novelty, central bank laws often need updating to confirm issuance authority, with a preference observed for two-tier models (public–private partnership) over direct public accounts at central banks. Legal reforms may also be needed to affirm central banks' authority to own/operate rCBDC payment platforms if not already within their remit. When rCBDC platform operations (including technology aspects) are outsourced, the central bank must retain full control legally and contractually. If a central bank–operated rCBDC payment platform is systemically important, it should align with PFMI standards, and governance mechanisms must address the conflicts of interest (self-regulation) concerns. The central bank's mandate might extend to providing front-end rCBDC access tools (software/hardware), which require clear legal authorization. A comprehensive legal framework is also needed to license, regulate, and supervise intermediaries offering rCBDC services such as wallets and service accounts. Depending on jurisdictions' policy choices, this may entail mandating participation by key intermediaries in the rCBDC payment platform to serve public interest objectives—designed in a proportional way. Finally, authorities should carefully consider empowering the imposition of rCBDC wallet or service account portability in exceptional cases, with appropriate safeguards.

Legal relationships within an rCBDC landscape must be carefully assessed to identify and mitigate potential risks. Three types of relationships should be carefully assessed. First, the legal relationship

between issuing central bank and rCBDC users which is two folded: (i) There is the “asset link” on one hand that is related to the link that would exist between users and central bank revolving around the rCBDC being a monetary instrument, and (ii) there is the “technological link” that would relate to the technological service that the central bank would provide to users, directly or indirectly, to allow access and use of the rCBDC. Second, the legal relationship between the central bank and intermediaries also has a double dimension: (i) On the one hand, intermediaries offering rCBDC services appear as regulated payment service providers and would probably be captured under existing legal and regulatory payment regimes. Nevertheless, updating of these existing regimes may be needed to better govern rCBDC intermediaries and services. (ii) On the other hand, intermediaries stand as participants in the rCBDC platform deployed by the central bank. If qualified as a payment system, those intermediaries, as participants, will have to adhere to standardized terms and conditions of the system that will take the form of a rulebook. Third, the legal relationship between intermediaries and users covers the offering of rCBDC services. Such services can be classified as regulated payment services, and this relationship will be primarily based on the law. However, contractual arrangements could also complement.

rCBDC specifications, including limits on holding, transaction amounts, and fees, as well as interest accrual, programmability, and offline payment must all be grounded in law. Although rCBDC, to serve as money, should function as both a medium of exchange and a store of value, jurisdictions may impose legal limits on its use in either capacity for policy reasons (for example, capping holdings or transactions). The majority of current rCBDC projects envisage no interest on rCBDC. In addition, programmable (conditional) payments could encourage rCBDC usage by allowing automatic transfers when predetermined conditions are met. Although such functionality is not new, implementing it in publicly available central bank money is novel, and legal challenges may appear. Finally, providing an offline payments option for rCBDC can help central banks achieve a broad set of public policy objectives, including greater payment resilience and support for financial inclusion, but a sound legal foundation must be explored for such offline payments.

Issuing wCBDC requires careful consideration of multiple legal aspects: its legal nature, the central bank’s mandate to issue wCBDC and operate (or outsource) its platform, the legal rules for tokens and their operation, and settlement finality. In this Note, wCBDC refers to a tokenized form of central bank money accessible only to selected financial institutions. The central bank–user (institution) relationship in wCBDC raises specific issues related to the asset link and technological link. It is essential that the central bank’s mandate clearly covers issuing wCBDC and either operating the wCBDC platform or outsourcing some operations with maintaining control—these are foundational legal elements regardless of technical model. Moreover, laws must address fundamental issues such as the legal rules for token transfers (including loss, illegal transfers, good-faith acquisition) and the precise moment when wCBDC settlement is irrevocable and final.

## Annex: Key Legal Considerations with Practical Approaches<sup>92</sup>

<i>The Legal Nature of Retail Central Bank Digital Currency (rCBDC) in Public Law</i>		
1	rCBDC: a digital form of central bank money available to the general public	<p><b>Jurisdictions should qualify rCBDC—a digital form of central bank money available to the general public—as a liability of the central bank in their legal frameworks.</b></p> <p>The Bank of Jamaica Act 2022 provides that its “monetary liabilities” include notes, coins and central bank digital currency. Regulatory Guidelines on the eNaira 2021 state that the eNaira is a direct liability of the Central Bank of Nigeria. The Reserve Bank of India Act, 1934, as amended, explicitly disappplies certain sections relevant only to physical currency (such as those dealing with denominations, physical form, or acts of mutilation of currency) to banknotes issued in a digital form.</p>
2	rCBDC: intermediary insolvency remote	<p><b>rCBDC should remain a central bank liability in any architecture: rCBDC users should be legally protected from the insolvency of intermediaries in a two-tier system (public–private partnership).</b></p> <p>China’s rCBDC (e-CNY) is a direct liability of the People’s Bank of China (PBOC). In that vein, the e-CNY uses a two-tier architecture: the PBOC handles issuance and redemption, whereas intermediaries provide e-CNY services. Because such rCBDC is a liability of the central bank, not of the intermediaries, their insolvency would not affect the value of e-CNY held by rCBDC users.</p>
3	rCBDC: currency status	<p><b>If rCBDC is meant to be the digital form of cash, the law should recognize it as currency: jurisdictions should assess the need for legal reforms to apply key currency features to rCBDC.</b></p> <p>The Bank of Jamaica Act 2022 grants the central bank exclusive rights to issue rCBDC (<i>monopoly of issuance</i>). The EU draft digital euro regulation mandates acceptance at full face value (<i>cours forcé</i>). Ukraine has amended its central bank law to recognize digital currency as legal tender (<i>legal tender</i>). The Bahamas’ Central Bank Act 2020 criminalizes counterfeiting of electronic money designated as legal tender (<i>criminal law protection</i>).</p>
<i>Retail CBDC Implications on the Legal Mandate of Central Banks</i>		
4	Legal mandate to issue rCBDC	<p><b>Jurisdictions should consider vesting the rCBDC issuance function in the central bank, preferably through clear statutory language. It should be noted that launching certain rCBDC pilots might require such legal amendments.</b></p> <p>The Bank of Jamaica Act 2022 was amended to define rCBDC as a digital form of currency, clearly empowering the central bank to issue digital currency. The Eastern Caribbean Central Bank (ECCB) Agreement was amended to include digital currency in the definition of currency when launching the “DCash” pilot.</p>
5	Authority to own and operate an rCBDC platform	<p><b>Central banks should have statutory authority to own and operate rCBDC payment platforms as part of their public mandates. Any front-end involvement, including providing public access to rCBDC, should also be consistent with those mandates.</b></p> <p>The Law of the People’s Republic of China on the People’s Bank of China tasks the PBOC with ensuring the normal operation of payment, clearing, and settlement systems. The Central Bank of Malaysia Act authorizes the central bank, its affiliates, or authorized persons to establish and operate systems—electronic or otherwise—for transferring, clearing, and settling funds and debt securities. The draft digital euro regulation recognizes the central bank’s competence to provide front-end services as public options within a competitive payments market.</p>

<sup>92</sup> As mentioned in Section I (Introduction) and Section VII (Conclusion), this table is not intended to constitute and should not be construed as, a recommendation for member jurisdictions to issue CBDCs. Its purpose is rather to navigate the authorities on the key legal considerations guiding their decision-making process.

6	Principles for Financial Market Infrastructures (PFMI) standards for an rCBDC platform	<p><b>If an rCBDC payment platform is designated systemically important, the central bank should review compliance with the PFMI to ensure it is legally sound and robustly regulated.</b></p> <p>For instance, (i) FMIs must ensure a well-founded, enforceable legal framework for all material activities (Principle 1); (ii) settlement finality must be legally clarified to provide irrevocable and unconditional payments (Principle 8); (iii) FMIs need transparent governance that promotes safety, efficiency, and supports financial system stability as well as public and stakeholder interests (Principle 2); and (iv) FMIs should identify and mitigate operational risks, including business continuity and security, through appropriate measures (Principle 17).</p>
7	Outsourcing of rCBDC platform operations	<p><b>When a central bank outsources operation of its rCBDC platform to a third party, it should ensure the outsourcing is legally permissible and maintain full control through appropriate legal and contractual arrangements.</b></p> <p>The central bank must ensure—through regulation and/or contractual arrangements—that any third-party operator complies with its security standards, provides ongoing audit and inspection access (including regular reporting), and maintains robust business continuity and contingency plans. Legal and regulatory frameworks should reinforce the central bank's authority to intervene in cases of material operational failure and require operators to design systems that are open and interoperable to enable seamless transition.</p>
8	Dual central bank roles as operator and regulator of an rCBDC platform	<p><b>In case a central bank serves as both operator of an rCBDC platform and regulator/overseer of payment systems, governance mechanisms should address the conflicts of interest (self-regulation) concerns.</b></p> <p>Traditional risk mitigation measures include: (i) establishing an independent oversight board or committee for rCBDC policy with external members; (ii) ensuring transparency through clear rule-making and regular audits by independent auditors; (iii) maintaining internal separation between the rCBDC operational team and the regulatory oversight function; and (iv) mandating periodic public reporting on the rCBDC platform's performance and its interaction with the broader retail payment market.</p>
9	Regulation/supervision of rCBDC intermediaries	<p><b>rCBDC service intermediaries should be regulated under a sound legal framework, either through adapted existing categories or a tailored regime. Any mandatory participation requirements to intermediaries must serve the public interest and observe proportionality.</b></p> <p>The Bahamian Dollar Digital Currency (BDDC) Regulations, 2021, establish a bespoke licensing regime under which only Central Bank-registered wallet providers may offer BDDC services. The draft digital euro regulation mandates that credit institutions offering certain payment services must provide basic digital euro services upon client request. The Central Bank of Nigeria's Regulatory Guidelines require all licensed financial institutions to act as eNaira intermediaries.</p>
10	rCBDC wallet/service account portability in exceptional cases	<p><b>To ensure continuity of users' access to rCBDC, legal authority should be established to transfer users' rCBDC wallets or accounts to an alternative provider if the incumbent cannot maintain services.</b></p> <p>Depending on rCBDC system design, the draft digital euro regulation, for instance, provides that, in exceptional circumstances—such as when a provider loses access to essential account data—the European Central Bank may authorize the transfer of digital euro payment accounts. This enables a new provider, selected by the rCBDC user, to access the user's holdings and complete the transfer without reliance on the original provider.</p>
<b>Legal Relationships in a Retail CBDC Landscape</b>		
11	Clarification of relationships in the rCBDC landscape	<p><b>Central banks must analyze the key legal relationships in the rCBDC landscape to effectively identify and mitigate potential risks.</b></p> <p>The legal characterization of relationships in an rCBDC landscape—whether legal or contractual—directly influences central bank responsibilities and risk exposure. A well-defined legal framework enhances enforceability, mitigates systemic risk, and supports public confidence—essential for effective rCBDC adoption.</p>



12	Central bank–users relationship	<p><b>Central banks must carefully evaluate their obligations arising from both the Asset and Technological Links with the users, ensuring that these responsibilities are clearly articulated in law and, where applicable, in user agreements.</b></p> <p>The central bank's role in rCBDC operations extends beyond physical cash issuance, potentially creating more direct legal obligations with users. These would arise from the asset link, where rCBDC is a central bank liability issued by and held on its platform, and the technological link centered around the central bank's obligation to provide a secure and continuous technological access. Without a clear legal classification of those relationships, central banks might fail to correctly assess their potential responsibilities and risks.</p>
13	Central bank–intermediaries relationship	<p><b>Existing legal payment regimes should be assessed and updated to explicitly cover rCBDC service providers and platform participants, ensuring legal clarity over their roles, responsibilities, and enforceability mechanisms.</b></p> <p>Intermediaries act toward the central bank as both rCBDC service providers and rCBDC platform participants, creating legal ties under legal and contractual arrangements. Although existing payment laws may apply, they often fall short in addressing novel services like programmability or offline use. Legal frameworks should be updated to clarify supervisory mandates, tailor licensing, oversee mixed-activity entities, and establish enforceable platform rulebooks that also protect user rights.</p>
14	Intermediaries–users relationship	<p><b>The legal relationship between rCBDC users and intermediaries should ensure that users' holdings are protected and remain legally distinct from the intermediaries' assets, guaranteeing user rights even in the event of intermediary failure.</b></p> <p>To preserve the credit risk-free nature of rCBDC, the user–intermediary relationship must establish that rCBDC users maintain proprietary rights and such holdings are ring-fenced through legal frameworks or tools such as custody or trust. Legal frameworks should also provide for contingency access—for example, rCBDC wallet portability or central bank intervention—and clearly allocate liability and indemnification procedures, particularly in cases of the shared responsibility between the central bank and the intermediary.</p>
15	Applicable general legal principles in the rCBDC landscape	<p><b>Legal frameworks should align with general legal principles—such as non-discrimination, proportionality, access to justice, and protection of property rights—with clarifying the scope of central bank immunities and liabilities.</b></p> <p>Any rCBDC system design must comply with fundamental rights. Legal frameworks should ensure non-discriminatory access, proportionate restrictions, and remedies for rCBDC users affected by central bank actions. They must also safeguard property rights, define the scope of central bank immunity and legal protection if any. Where functions are outsourced, agency principles may apply.</p>
<i>Specific Functionalities of Retail CBDC: Limits, Interest, Programmability, and Offline Transactions</i>		
16	Limits on rCBDC holdings/ transactions and fee caps for rCBDC services	<p><b>Jurisdictions should ensure a clear legal basis for setting rCBDC holding or transaction limits and for any limitations on fees charged for rCBDC services.</b></p> <p>As per the draft digital euro regulation, the European Central Bank would be empowered to set limits on the use of the digital euro as a store of value (<i>holding limit</i>). In Russia, the central bank law states that the Bank of Russia shall determine the maximum amounts of transactions with digital rubles (<i>transaction limit</i>). The effective use of the digital euro as a legal tender means of payment would be preserved through limits on inter-PSP or merchant fees (<i>limitation on fees</i>).</p>
17	rCBDC: programmability	<p><b>Authorities should carefully assess the legal implications of designing rCBDC that can be used for programmable payments.</b></p> <p>Existing legal frameworks may require revision to accommodate smart contracts in rCBDC-based programmable payments. These self-executing codes raise legal issues of enforceability and interpretation. Jurisdictions should clarify their legal status and evaluate associated regulatory risks. Regulators should have explicit authority to supervise programmable payment services and mitigate risks to financial stability and consumer protection. Legal regimes should also delineate liability for losses stemming from technical failures or misuse of programmable features.</p>

18	rCBDC: offline functionality	<p><b>Where offline payment functionality is envisaged, the legal framework should clearly address settlement finality, legal tender status, convertibility, compensation rules, and the validity of ownership transfers.</b></p> <p>Although various technological models for offline rCBDC exist, legal clarity on the moment of settlement finality is essential. Legislation should confirm that both offline and online rCBDC constitute legal tender. To preserve the singleness of money, the law should ensure full convertibility at par between the two forms. Jurisdictions should determine whether specific compensation rules for offline rCBDC losses are required or if general provisions suffice. The legal framework should also recognize the validity and perfection of offline rCBDC transactions.</p>
<i>Selected Legal Aspects of Wholesale Central Bank Digital Currency (wCBDC)</i>		
19	Legal mandate to issue wCBDC	<p><b>Jurisdictions should ensure a sound and robust legal basis for the issuance of wCBDC—a tokenized form of central bank reserves—to mitigate legal uncertainty and associated risks.</b></p> <p>Each jurisdiction should determine whether wCBDC issuance is allowed under its legal framework. Where wCBDC is deemed functionally equivalent to existing reserves, the current authority of the central bank might suffice. However, if wCBDC constitutes a novel form of liability, particularly in the context of tokenization, existing mandates might not allow such an issuance, thereby raising the risk that the central bank could act ultra vires—beyond the scope of its legal mandate.</p>
20	wCBDC: a tokenized form of central bank reserves	<p><b>Authorities should assess the need for legal reforms to ensure legal certainty in the conduct of wCBDC token operations.</b></p> <p>Since wCBDC is a tokenized form of central bank reserves, jurisdictions should anticipate legal challenges commonly associated with tokenization. In addition to establishing robust legal links between tokens and underlying assets, the law should address core issues, including rules for transferring tokens (for example, loss, unauthorized transfers, or good-faith acquisition) and effects of counterparty insolvency. Legal certainty on these issues should be pursued through legislative reforms or contracts where appropriate.</p>
21	Operation/ outsource of wCBDC platforms	<p><b>Central bank powers to own and operate wCBDC platforms—directly or through outsource—may require legal reforms.</b></p> <p>A central bank should have clear statutory authority to own and operate a wCBDC platform (if it is systemically important, PFMI standards apply). Where operations are outsourced, legal provisions must permit such outsource with ensuring the central bank retains control. Legislative reform may be required to establish or clarify this authority. In certain jurisdictions, such as Switzerland, the legal framework allows issuance of wCBDC through platforms operated by private entities, with operational tasks outsourced accordingly (for example, Project Helvetia under Swiss law).</p>
22	wCBDC: settlement finality	<p><b>Legal frameworks should explicitly recognize settlement finality for wCBDC transactions.</b></p> <p>Settlement finality in wCBDC transactions is essential. Legal frameworks should specify exactly when ownership of wCBDC transfers, taking insolvency laws into account, especially regarding fraud or platform protections. In probabilistic settlement systems, finality may hinge on validator confirmations or new ledger blocks. Jurisdictions should ensure solutions to these issues are legally enforceable.</p>

## References

Bains, Parma, Nobuyasu Sugimoto, and Christopher Wilson. 2022. “BigTech in Financial Services: Regulatory Approaches and Architecture.” IMF Fintech Note 2022/002, International Monetary Fund, Washington, DC.

Bank of Canada, Swiss National Bank, European Central Bank, Bank of England, Bank of Japan, Board of Governors of the Federal Reserve System, Sveriges Riksbank, and Bank for International Settlements. 2024. “Legal aspects of retail CBDCs.” Bank for International Settlements, Basel, November.

Bank of England. 2020. “Central Bank Digital Currency: Opportunities, challenges and design.” Discussion Paper, Bank of England, London, March.

Bank of England. 2025. “Digital pound experiment report: Offline payments.” Bank of England, London, April.

Bank of England and HM Treasury. 2024. “Response to the Bank of England and HM Treasury Consultation Paper: The digital pound: a new form of money for households and businesses?” Bank of England and HM Treasury, London, January.

Bank of Ghana. 2022. “Design paper of the digital Cedi (eCedi).” Bank of Ghana, Accra, March.

Bank of Israel. 2025. “Preliminary Design for the Digital Shekel System.” Bank of Israel, Jerusalem, March.

Bechara, Marianne, Wouter Bossu, Yan Liu, and Arthur Rossi. 2021. “The Impact of Fintech on Central Bank Governance: Key Legal Issues.” IMF Fintech Note 2021/001, International Monetary Fund, Washington, DC.

Bechara, Marianne, Wouter Bossu, Amira Rasekh, Chia Yi Tan, and Akihiro Yoshinaga. 2025. “Private Law Aspects of Token-Based Central Bank Digital Currencies.” IMF Fintech Note 2025/003, International Monetary Fund, Washington, DC.

BIS Innovation Hub. 2023a. “Project Polaris—Part 1: A handbook for offline payments with CBDC.” Bank for International Settlements, Basel, May.

BIS Innovation Hub. 2023b. “Project Polaris—Part 4: A high-level design guide for offline payments with CBDC.” Bank for International Settlements, Basel, October.

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.

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO). 2015. “Application of the Principles for financial market infrastructures to central bank FMs.” Bank for International Settlements, Basel, August.

Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO). 2022. “Application of the Principles for Financial Market Infrastructures to stablecoin arrangements.” Bank for International Settlements, Basel, July.

Committee on Payment and Settlement Systems (CPSS) and International Organization of Securities Commissions (IOSCO). 2012. “Principles for financial market infrastructures.” Bank for International Settlements, Basel, April.

Das, Mitali, Tommaso Mancini-Grieffoli, Fumitaka Nakamura, Julia Otten, Gabriel Söderberg, Juan Sole, and Brandon Tan. 2023. “Implications of Central Bank Digital Currencies for Monetary Policy Transmission.” IMF Fintech Note 2023/010, International Monetary Fund, Washington, DC.

European Central Bank. 2020. “Report on a digital euro.” European Central Bank, Frankfurt, October.

European Central Bank. 2024. “Update on the work of the digital euro scheme’s Rulebook Development Group.” European Central Bank, Frankfurt, January.

Garrido, José M. 2023. “Digital Tokens: A Legal Perspective.” IMF Working Paper 23/151, International Monetary Fund, Washington, DC.

International Institute for the Unification of Private Law (UNIDROIT). 2023. “UNIDROIT Principles on Digital Assets and Private Law.” UNIDROIT, Rome.

Minwalla, Cyrus, John Miedema, Sebastian Hernandez, and Alexandra Sutton-Lalani. 2023. “A Central Bank Digital Currency for Offline Payments.” Staff Analytical Note 2023-2, Bank of Canada, Ottawa, February.

Murphy, Kieran, Tao Sun, Yong Sarah Zhou, Natsuki Tsuda, Nicolas Zhang, Victor Budau, Frankosiligi Solomon, Kathleen Kao, Morana Vucinic, and Kristina Miggiani. 2024. “Central Bank Digital Currency Data Use and Privacy Protection.” IMF Fintech Note 2024/004, International Monetary Fund, Washington, DC.

Relevant Ministries and the Bank of Japan Liaison Meeting on Central Bank Digital Currency (CBDC). 2024. “Interim Report.” Relevant Ministries and the Bank of Japan Liaison Meeting on CBDC, Tokyo, April.

Tourpe, Herve, John Kiff, Majid Malaika, and Chris Ostrowski. 2025. “Technology Solutions to Support Central Bank Digital Currency with Limited Connectivity: Review of Existing Approaches.” IMF Fintech Note 2025/005, International Monetary Fund, Washington, DC.



## PUBLICATIONS

**Selected Legal Considerations for Central Bank Digital Currencies**  
NOTE/2025/006