



TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

CENTRAL BANK DIGITAL CURRENCIES: IMPLICATIONS FOR SUPERVISORS

MAY 2023

CENTRAL BANK DIGITAL CURRENCIES: IMPLICATIONS FOR SUPERVISORS

TABLE OF CONTENTS

Introduction	2
Why introduce a CBDC?	2
Decline in cash usage	3
Crypto-assets	3
Payment system developments	3
Speed, efficiency and cost of retail payments	4
Encourage innovation.....	4
Financial inclusion	5
Facilitate fiscal transfers.....	6
Cross-border payments.....	6
Design of a CBDC.....	7
Where are retail CBDC accounts held?	7
Centralized database or distributed ledger technology?	10
Account or token?	11
Cross-border payments.....	12
Risks to supervisory objectives and supervisory responses.....	12
Legal basis	12
Consumer protection	13
AML and CFT	19
The safety and soundness of financial institutions: Deposit substitution.....	21
Financial stability	22
Supervisory approach	23
Conclusion	25
References.....	26

Copyright © Toronto Centre. All rights reserved.

Toronto Centre permits you to download, print, and use the content of this TC Note provided that: (i) such usage is not for any commercial purpose; (ii) you do not modify the content of this material; and (iii) you clearly and directly cite the content as belonging to Toronto Centre.

Except as provided above, the contents of this TC Note may not be transmitted, transcribed, reproduced, stored or translated into any other form without the prior written permission of Toronto Centre.

The information in this TC Note has been summarized and should not be regarded as complete or accurate in every detail.

CENTRAL BANK DIGITAL CURRENCIES: IMPLICATIONS FOR SUPERVISORS

Introduction¹

A central bank digital currency (CBDC) is a new form of central bank money, issued digitally by a central bank, denominated in an existing unit of account, and intended to serve as legal tender, a medium of exchange, and a store of value.²

Interest in CBDCs has grown rapidly in recent years – most central banks have a CBDC project underway, and a small number have already issued retail CBDCs.³ The Bahamas launched a live retail CBDC (the Sand Dollar) in October 2020; Nigeria issued the eNaira in October 2021; and Jamaica issued the JAM-DEX in July 2022. Pilot versions were released for public testing by China (e-CNY) in April 2020, the Eastern Caribbean (DCash) in March 2021, and India (Digital Rupee) in December 2022.⁴

Since some emerging markets and developing economies have already issued a retail CBDC, and many other countries are considering doing so, it is important for supervisory authorities to consider the possible implications for their supervisory objectives. The precise nature of these implications will depend on the design of a retail CBDC, but they may affect the safety and soundness of banks, financial stability, financial inclusion, consumer protection and data privacy, anti-money laundering, and cross-border remittances.

The focus of this Toronto Centre Note is on retail (not wholesale) CBDCs, because this is of more interest to most supervisory authorities. The Note reviews briefly the reasons for introducing a retail CBDC and the key choices in its design; then considers the risks arising from retail CBDCs and how these risks might be addressed by financial supervisors.

Why introduce a CBDC?

Central banks have offered various reasons for introducing a retail CBDC.

Some of these are reactive – to developments such as the decline in the use of cash, the emergence of crypto-assets, and the growth of digital payments (which was accelerated as a result of the COVID-19 pandemic).

¹ This Toronto Centre Note was prepared by Clive Briault. Please address any questions about this Note to publications@torontocentre.org.

² See International Monetary Fund (2020).

³ Bank for International Settlements (2020a and 2022b) outline the history of central bank retail CBDC projects, while Bank for International Settlements (2022a and 2022d) survey CBDC developments in Latin America and the Caribbean, and Africa. The latest developments are tracked by Atlantic Council (2023), the Bank for International Settlements (2023) and cbdctracker.org (2023).

⁴ For more details, see Central Bank of The Bahamas (2023), Central Bank of Nigeria (2021), Bank of Jamaica (2021), People's Bank of China (2021), Eastern Caribbean Central Bank (2021) and Reserve Bank of India (2022).

Others are more proactive – to improve the efficiency of payments systems, encourage innovation, enhance financial inclusion, facilitate fiscal transfers, and underpin cheaper and more secure cross-border payments.⁵

Decline in cash usage

The use of cash has been declining in many economies. If this trend continues, there is a risk that individuals and businesses will no longer have access to, or be able to make payments with, central bank money.

Central banks have committed to continuing to provide cash in response to public demand for it. But a retail CBDC could preserve many of the functions of cash, and could provide access to central bank money, by acting as a “digital banknote”. CBDC transactions would need to be final and completed in real time, allowing users to make payments to one another using a risk-free asset. Individuals, businesses, and governments could use a CBDC to buy goods and services or pay bills, and governments could use a CBDC to collect taxes or make benefit payments.

Cash also serves as a backup payment method to electronic systems if those networks cease to function. However, as the use of cash declines, it will be less useful as a backup method. A retail CBDC system could act as an additional payment method, improving operational resilience.

In some countries where the use of cash remains high, the opportunities are different. The attraction of a retail CBDC in these countries is to introduce a form of central bank money that is cheaper to produce than bank notes; less subject to counterfeiting; less able to be used for money laundering, tax evasion, and other financial crimes; and more likely to encourage people to enter and use the formal financial system. For example, a main purpose of the JAM-DEX retail CBDC in Jamaica is to provide a replacement for cash.

Crypto-assets

Central banks have become concerned that the use of crypto-assets, and in particular stablecoins linked to the value of a currency (or basket of currencies), could impair monetary policy. It could also undermine confidence in the value or operational continuity of currencies, which could threaten financial stability.

One motivation for issuing a CBDC is to address the threat from crypto-assets by providing digital central bank money.

Payment system developments

Digital retail payment systems have expanded rapidly in many countries.⁶ In some cases, this has fragmented these systems, increasing the cost and complexity of interoperability between these systems and leaving users and merchants with higher costs and difficulties paying users of other systems.

⁵ The potential benefits of a retail CBDC are discussed in Bank for International Settlements (2020a, 2020b, 2021b and 2022b) and Board of Governors of the Federal Reserve System (2022).

⁶ Retail payment systems and their supervision are discussed in Toronto Centre (2023).

This is inconvenient and socially inefficient. A retail CBDC could provide a common means to transfer funds between fragmented digital retail payment systems.⁷

Alternatively, retail payment systems can become heavily concentrated, posing a risk to competition and innovation. In this case, a retail CBDC could support a more diverse retail payment system.

Speed, efficiency and cost of retail payments

Individuals and businesses may face relatively high costs and delays in making payments through private sector retail payment systems. These costs and delays could be reduced if individuals and businesses have access to, and can transfer, a retail CBDC to facilitate the sale of goods and services. The ability to transfer value seamlessly between individuals and businesses through a convenient, electronic form of central bank money, with the safety, liquidity, finality, and integrity that would entail, could make the retail payment system more efficient and allow money to move more freely throughout the economy.

In other countries, where retail payment systems are less well developed, the introduction of a retail CBDC could lead to the adoption of a CBDC arrangement as the core element of retail payment systems. This could create an opportunity for individuals and households to connect to an inclusive, safe, and efficient payment system.

Encourage innovation

The provision of a retail CBDC can offer non-bank payment system providers direct access to an alternative payment infrastructure in which they can offer payment services to their customers. Such providers could then develop new and innovative financial products and services. A retail CBDC could therefore promote competition and underpin a diverse and innovative monetary system.

Encouraging innovation was a key consideration in the introduction of The Bahamas Sand Dollar. Central Bank of The Bahamas (2023) states:

“... the Bank wants to foster the creativity of local fin-tech firms, developers and start-ups. It is hoped that Sand Dollar will be a catalyst for front-end, customer-facing services and solutions not yet imagined. [With] one of the first CBDCs in the world, local fin-tech developers are encouraged not to limit their vision to the local market, but to think globally when designing and developing their solutions.”

⁷ As with many of the reasons for introducing a retail CBDC, there are also other means of delivering similar benefits. For example, an accessible central bank-operated retail fast payment system could also reduce the costs of fragmentation.

Financial inclusion

A retail CBDC could enhance financial inclusion, because individuals who do not currently have traditional bank accounts would be able to access CBDC accounts.⁸ Retail CBDC accounts could offer lower costs and transaction fees, and be accessible through less onerous proof of identification, thereby providing a fast, secure, and cheap way to make and receive payments. Using only cash to make and receive payments leaves the unbanked outside the formal financial system and without the data and transaction trails needed to more readily access financial services such as credit and insurance.

There is also the advantage to individuals that a retail CBDC should be more secure than cash. If you lose your physical wallet, or misplace cash, you lose your money. But in a CBDC system, if you lose your phone or other access device, your digital wallet or your access to an account can be reinstalled and the money can be recovered.

To maximize the opportunities to enhance financial inclusion by encouraging adoption and accessibility, a retail CBDC should be:

- Trusted by users, in particular those currently excluded from the financial system.
- Based on a sound and robust legal framework.
- As easy to use as cash, tapping with a card, or scanning a mobile phone, and usable in many of the same types of transactions as cash, including point of sale and person-to-person.
- Provided at very low or no cost to end users, with minimal requirements for users to make a technological investment.
- Available 24/7 every day of the year.
- Highly resilient to operational failure and disruptions, cyberattacks, natural disasters, electrical outages and other issues. There should be some ability for end users to make offline payments if network connections are unavailable.
- Robust in terms of data privacy and fraud protection.
- Scalable, to accommodate the potential for large future volumes.
- Interactive with private sector digital payment systems and arrangements to allow easy flows of funds between systems.

However, to increase financial inclusion, a retail CBDC would need to address the barriers to inclusion, which can be difficult to surmount and which vary across countries. For example, Financial Stability Institute (2022) lists six barriers to financial inclusion, relating to geographic barriers such as vast territories and remote locations; the absence of identity credentials and a lack of consumer protection; inefficiency in the financial sector and a lack of profitability of serving excluded groups; vulnerabilities such as age, gender, income, or disability; a lack of education and financial literacy; and low trust in existing financial services.

⁸ The benefits of a retail CBDC for financial inclusion are discussed in Financial Stability Institute (2022) and Carstens and H.M. Queen Máxima of the Netherlands (2022).

Retail CBDCs are not the only way to overcome these barriers, but they could be part of the solution, along with the financial inclusion initiatives countries already have in place, including those focusing on digital financial inclusion. For example, a retail CBDC could add value by promoting and facilitating innovation and competition and the entry of non-bank entities; offering robust and low-cost technology; integrating a CBDC with existing payment systems and instruments; and enabling individuals and businesses in more remote geographical areas to use CBDCs for their savings and payments.⁹

However, introducing a retail CBDC may not make any difference to financial exclusion arising from a digital divide. Increasing digitalization could leave some sections of society behind due to barriers such as a lack of trust in financial institutions, a lack of digital literacy, an inability to access IT and smart phones, and data privacy concerns.¹⁰

Facilitate fiscal transfers

In some countries, the COVID-19 pandemic illustrated the benefits of governments using digital payment facilities to transfer funds to individuals and businesses in a crisis. A retail CBDC system with identified users (for example, a system linked to a national digital identity system) could also be used for such payments, and could extend the reach of these payments beyond individuals and businesses with traditional bank accounts.

Compared to cash, a retail CBDC system might also provide a better means to distribute funds in geographically remote locations or during natural disasters, and to increase the resilience of payments in the face of natural disasters, when other channels might be unavailable. However, significant offline capabilities would probably need to be developed, both for the CBDC system and any dependencies (for example, the availability of electricity for mobile devices).

Cross-border payments

Cross-border retail payments and transfers are often expensive and slow. This leaves scope for interoperable CBDCs to make cross-border payments cheaper and faster, while also making them safer and more secure.

The Financial Stability Board (2020) road map to enhance cross-border payments includes a focus area on the potential for new infrastructures and arrangements for cross-border payments. This is based on recent advances in technology and innovation, including multi-CBDC arrangement designs and interoperability, and experiments with arrangements that enable access and interlinking and facilitate efficient cross-currency retail CBDC payments.

⁹ For example, in Nigeria, some government ministries use the eNaira to make fiscal transfers to individuals in remote areas as part of the country's financial inclusion objectives. This has contributed to a rapid expansion in the number of eNaira wallets held by households.

¹⁰ Digital Currency Initiative (2023) discusses why a retail CBDC may have only a limited impact on financial inclusion.

Design of a CBDC

A retail CBDC can take many different forms.¹¹ This is important for the extent to which a retail CBDC can deliver the benefits listed above, and for the risks that a CBDC might pose to the objectives of a supervisory authority. Various trade-offs inevitably arise.

This section explores the choices around where retail CBDC accounts are held, whether transaction ledgers are held centrally or in a distributed manner, and whether a retail CBDC is held as an account or a token.

Where are retail CBDC accounts held?

A retail CBDC requires a system to provide and distribute it to individuals, businesses, and the government. However, this system could take different forms, depending on the roles of the central bank, commercial banks, and other payment system service providers and operators. This is summarized in Table 1 below. These roles could then be supported by a wider system, including data service providers, applications, and point of sale devices to initiate and accept payments.

Table 1: Retail CBDC models

Retail CBDC model	Who is the retail CBDC issued to?	Who holds the payment records?	Who undertakes account (wallet) management?	Who is responsible for money laundering and other due diligence checks?
Direct	Directly to end-users	Central bank	Central bank	Central bank
Intermediated	Intermediaries	Intermediaries	Intermediaries	Intermediaries
Hybrid	Intermediaries	Intermediaries and central bank (directly or indirectly)	Intermediaries	Intermediaries
Synthetic	No one	Intermediaries	Intermediaries	Intermediaries

Direct CBDC

A direct retail CBDC is conceptually the most straightforward payment system. The system would be operated by the central bank, which would offer accounts directly to individuals, businesses, and the government. The central bank would handle and execute all payments in real time, maintain a record of all retail holdings, and maintain the ledger of all transactions. There would be no need for intermediaries.

¹¹ Auer and Bohme (2020) set out these design choices using a “CBDC pyramid”, which also maps the design choices into delivering benefits. See also Bank for International Settlements (2022b).

However, a direct retail CBDC would require the central bank to build massive technological capabilities to process and record all retail CBDC transactions and to handle a large volume of payments traffic. It would also require the central bank to take responsibility for “know-your-customer” (KYC) and customer due diligence, which would take a central bank way beyond its current responsibilities. The central bank would also bear all the risks relating to operational resilience (and to offline payments if this capability was offered), and would have to provide a dispute resolution service.

For these reasons, no central bank has yet issued a direct CBDC.

Intermediated CBDCs

Under an intermediated system, a CBDC would remain a claim on the central bank. However, private sector intermediaries would offer accounts or digital wallets to manage holdings of the retail CBDC, execute payments, undertake identity verification, handle all communication with retail clients, and be subject to dispute resolution procedures. A user’s CBDC holdings would be held in an individual retail CBDC account (or wallet). A user may (or may not) also have a traditional deposit account with a bank.

Intermediaries could include commercial banks and other regulated non-bank financial service providers. They would be required to back each outstanding indirect CBDC liability to the customer through their holdings of actual CBDCs (or other central bank money) deposited at the central bank. Intermediaries would net payments and send payment messages to other intermediaries and send (net) wholesale payment instructions to the central bank.

The central bank would settle the wholesale CBDC accounts with finality. The central bank would maintain only a wholesale ledger, not a central ledger of all retail transactions. Because the central bank would not keep a record of individual claims (only the intermediaries keep these records), there is no cash-like direct proof of a customer’s retail CBDC claim. The central bank cannot honour claims from consumers without information from the intermediary.

If an intermediary cannot – for whatever reason – access its own records, determining the legitimate owner of CBDC might involve a potentially lengthy and costly legal process with an uncertain outcome. However, this risk could be reduced by the central bank requiring that all intermediaries be able to provide the necessary information to the central bank in the event of any failure, so the central bank could transfer retail CBDC holdings to a different provider, or indeed pay holders in cash.

The eNaira is an account-based retail CBDC system operated through commercial banks (Central Bank of Nigeria (2021)).

Financial institutions are intermediaries between the Central Bank of Nigeria (CBN) and their customers. These intermediaries facilitate customer (individuals and businesses) access to eNaira speed wallets; integrate the eNaira speed wallet feature into their electronic banking channels; request eNaira from the CBN for themselves and on behalf of their customers; manage eNaira across their branches; develop internal frameworks to ensure compliance with KYC and AML/CFT requirements; receive and resolve customers’ complaints on eNaira; and report eNaira enquiries and complaints periodically to the CBN.

Hybrid CBDCs

Some central banks favour a hybrid solution, incorporating some elements of the direct and intermediated models. Intermediaries would handle retail payments, but the retail CBDC is a direct claim on the central bank. The central bank would also keep a central ledger of all transactions and operate a backup technical infrastructure, allowing it to transfer holdings from one payment service provider to another in the event of a technical failure, and to restart the payment system if intermediaries fail.

Since the retail CBDC is a direct claim on the central bank, each customer's claim would have to be segregated from the balance sheets of the payments service providers (PSPs). If a PSP fails, holdings of the CBDC are not considered part of the PSP's assets available to creditors.

The hybrid model would be more complex for a central bank to operate than the intermediated model, but it should be possible using available technology. The central bank would not interact directly with retail customers, but it would have to keep a central ledger of all transactions.

The Central Bank of The Bahamas (2023) plays a multi-purpose role, including issuing the Sand Dollar and monitoring holdings. The Bank maintains the ledger of all individual holdings of the digital currency, but does not provide a front-end customer service, nor directly sponsor digital wallets.

All payments services firms have access to the digital currency. They are able to use the Sand Dollar Network to settle retail Bahamian dollar payments, thereby promoting interoperability among existing and new channels for the provision of payments services.

Supervised financial institutions are authorised Sand Dollar agents and can enrol customers through their tailored applications (digital wallets). This creates a fiduciary relationship between the provider and the wallet holder. Sand Dollars can be accessed flexibly with either a mobile phone application (iOS and Android) or using a physical payment card to access a digital wallet. Transactions and real-time transactions processing are near instantaneous.

There is a fully auditable (non-anonymous) transactions trail, with user confidentiality protected by strict regulatory standards around access. Transactions are monitored for fraud protection.

For individuals, the Sand Dollar provides a record of income and spending. This can be used as supporting data for micro-loan applications; zero transaction fees (but also no payment of interest); and offline functionality that allows users to make a pre-set dollar value of payments when communications access to the Sand Dollar Network is disrupted, with wallets updated once communications are re-established.

Businesses receive point of sale support for accepting payments, and can process payments with modern credit and debit card machines or mobile phone apps.

The Sand Dollar is restricted to domestic use.

In an alternative hybrid model, the central bank would not maintain a current ledger of transactions. Instead, it would have powers to access the ledgers of any intermediary and therefore to be able to step in to transfer holdings from one provider intermediary to another. This would also require intermediaries to satisfy record-keeping requirements as part of their authorization or permission to offer retail CBDC accounts or wallets.

The Bank of Jamaica (2021) uses the alternative hybrid model for issuing its retail CBDC, the JAM-DEX. It issues JAM-DEX to commercial banks and other deposit-taking institutions – building societies, merchant banks and authorized payment service providers - licensed or authorized by the bank of Jamaica. These intermediaries distribute JAM-DEX to the retail market.

To use the JAM-DEX, consumers need a CBDC account, which is different from a regular bank account and much easier and simpler to obtain, with streamlined and simplified Know Your Customer requirements. Individuals who already have bank accounts can automatically obtain a CBDC account. Customers can transfer and convert funds seamlessly between regular and CBDC accounts.

To carry out CBDC transactions anywhere and at any time, consumers can access, download, and deploy a mobile wallet app on any smart phone, tablet or similar compatible device using the networks of both major telecom service providers.

Indirect or Synthetic CBDCs

In this model, an intermediary would, in effect, create a synthetic CBDC by operating as a “narrow bank.” Customers would have a claim on these intermediaries (not on the central bank), which would operate retail payments and would fully back all their liabilities to retail customers with claims on the central bank.

It can be argued that this synthetic model does not represent a CBDC, because the central bank does not issue a retail CBDC.

Centralized database or distributed ledger technology?

Central banks are considering whether retail CBDC transfers should be recorded and settled in a centralized or decentralized manner. In a direct retail CBDC model (as described in the previous section), this would involve settling each individual transaction across end-user accounts at the central bank. In an intermediated model, the settlement would be more like a wholesale settlement process across accounts held by the intermediaries at the central bank.

A conventional centralized database is controlled by a single authority (here it would be the central bank), albeit with the data stored in multiple locations to provide resilience. In a direct retail CBDC model, the database could simply record retail CBDC transactions, or provide additional functionality such as the ability to synchronize payments.

A decentralized database could use distributed ledger technology (DLT), in which the ledger is jointly managed by different entities in a decentralized manner without a single authority. Each update of the ledger has to be harmonized between the entities (for example, using “consensus mechanisms”). A transaction can only be added to the ledger with finality once this validation process has taken place. This could be on a “permissionless” basis (as used for Bitcoin and many other private crypto-assets), or – more likely for a CBDC – a “permissioned” basis, where transactions can only be validated by trusted parties who are admitted to the network by the central bank.

It would also be possible to use a combination of centralized and decentralized databases. For example, in The Bahamas, the Sand Dollar uses a centralized ledger to settle transactions and a DLT layer where all transactions are recorded.

The main practical (and cost) issue with DLT is operating the consensus mechanism, which would limit the number of transactions it is capable of handling. It could not therefore be used for a direct retail CBDC system, except in a small economy.

The key vulnerability of a centralized database is that it could be subject to a cyberattack. In principle, DLT should offer greater resilience because it is decentralized, although the consensus mechanism could be subject to a denial-of-service type of attack. DLT could also provide greater interoperability with private sector solutions based on similar technologies.

Account or token?

Another design consideration is whether retail CBDC is held as an account, or as a token. In an account-based CBDC, the currency represents an electronically registered claim against the central bank, held either directly at the central bank or held through a bank or another financial institution. A CBDC transaction involves a book entry that debits the account of the payor and credits that amount to the payee’s account. The identity of the account holder allows the holder to access the funds: “I am therefore I own.”

In a token-based CBDC, the currency represents tokens (digital banknotes) issued by the central bank, each with a specific denomination. The ledger for a token-based CBDC identifies currency transfers that transfer ownership of tokens from the payor to the payee. The holder of a token transfers funds by using a password (private key): “I know therefore I own.”

The Eastern Caribbean Central Bank (ECCB) DCash digital currency is a token-based system.

The conventional account model, with CBDC ownership linked to an identity, has the advantages of familiarity, a clear and well-established legal status, lower operating costs (the security required for a token-based model could be expensive), and a well-established link to KYC and AML procedures.

A token-based system could be more effective in providing universal access to a retail CBDC, because individuals and small businesses without bank accounts (and possibly without the identification required to open an account) would only need to obtain a digital signature. And it could offer a higher level of privacy, closer to the use of cash, and potentially a stronger interface with other token-based payment systems.

However, because it is closer to the use of cash, a token-based system poses challenges in designing an effective AML framework, because it would be difficult to identify the owners of tokens and to follow the flow of money through the system. In addition, the legal status of tokens under public and private law may not be clear in all countries.

Cross-border payments

As noted above, there is scope for retail CBDCs to reduce at least some of the high costs of cross-border retail payments. In theory, account-based direct retail CBDCs could operate the same way in which cross-border wholesale digital currency payments are currently made.

In theory, central banks could work together to design seamless and inexpensive cross-border retail payments using CBDCs. In practice, however, most central bank retail CBDC projects have a national focus, with little progress being made – at least so far – towards multi-national arrangements to improve cross-border payments. Central banks may therefore be building national design features into their retail CBDC that will make it difficult to deliver the hoped-for benefits of cross-border payments.

Risks to supervisory objectives and supervisory responses

The introduction of a retail CBDC could pose risks to supervisory objectives. These will depend to some extent on the design features of a retail CBDC, as discussed above, but are likely to include risks in the following areas:

- The legal basis of a retail CBDC, from operational and design perspectives.
- Consumer protection, including risk of loss, operational resilience, and data privacy.
- Money laundering and terrorist financing.
- The safety and soundness of financial institutions.
- Financial stability.

This section outlines these risks¹² and discusses possible supervisory responses to them. It also considers how supervisory authorities can engage with central banks to ensure that any concerns of a supervisory authority are properly considered.

Legal basis

A retail CBDC raises legal issues relating to whether a central bank has a clear mandate and the necessary powers to issue a retail CBDC to individuals and businesses; whether a retail CBDC can be legal tender; and whether any changes are required to the legal framework governing existing retail payment systems. For example, International Monetary Fund (2020) highlights two relevant types of central bank powers for both account and token-based retail CBDCs: the power to issue certain types of currency and the power to open accounts in the central bank's books.¹³

¹² The risks arising from retail CBDC are discussed in Bank for International Settlements (2020b).

¹³ The legal basis of retail CBDC is discussed in International Monetary Fund (2020) and Schwarcz (2021).

A robust legal framework is therefore required to cover both issuing a retail CBDC and the wider payment system that uses this CBDC. The absence of a sound and robust legal framework would give rise to risks not only for the central bank but also for all users of a retail CBDC, including financial intermediaries and their customers. Moreover, any concerns about legality could limit the uptake of a retail CBDC and therefore its ability to deliver the benefits discussed above.

Consumer protection

There are three main concerns for consumers:

- The risk of loss of retail CBDC holdings.
- The operational resilience (access to and availability) of a retail CBDC.
- Data privacy.

Risk of loss

Consumers could lose money if (i) funds are removed fraudulently from their retail CBDC account; (ii) they mistakenly transfer funds to the wrong person; or (iii) expected funds do not arrive in their account. To the extent an account-based retail CBDC makes use of existing banking technology and systems, these risks should be comparable to the risks of using a digital commercial bank account.

In a token-based system, consumers could lose money if their passwords are accessed fraudulently, or they could lose access to their money, at least temporarily, if they have lost their password.

Supervisory response: risk of loss

Since the risk of loss is very similar to the risks inherent in digital bank accounts and all digital token-based systems, the supervisory responses will also be similar. This may take the form of some combination of:

Disclosure and transparency – supervisors should place requirements on retail CBDC issuers and intermediaries to provide consumers with clear, understandable information about the risks, benefits, customer privacy and security of retail CBDC and related products and services before they open a CBDC account or download a CBDC wallet.

Consumer liabilities and rights – supervisors can set limits on the monetary value of losses that consumers might suffer when using a retail CBDC, and place obligations on banks and other service providers to have security procedures and transaction checks in place to protect consumers. In effect, supervisors can establish where consumer responsibilities begin and end for losses arising from the use of retail CBDCs.

Consumers should be informed clearly and precisely about their rights, obligations, and responsibilities related to unauthorized or erroneous transactions, other losses, or unavailability, processing errors, security breaches and other problems.

Security – consumers should be made aware of commonly known threats to the safety and security of their CDBC holdings, and should be advised on how to safeguard their account details, identity credentials, passwords, etc.

Complaints handling – providers of retail CDBC should be clear about how a consumer can file a complaint, how a complaint will be handled, and the timeline that a provider has for responding to and resolving a complaint. The responsibilities of existing dispute resolution schemes could be extended to cover complaints relating to retail CBDCs.

For example, for the eNaira in Nigeria, banks and other intermediaries must meet all the requirements on them set out in the Regulatory Guidelines,¹⁴ and in particular:

- ensure that eNaira users have access to an array of channels (live messaging, internet banking platforms, customer service centres, and in-branch customer care) to report the loss or theft of a device or a compromise of their eNaira speed wallet;
- develop a system to validate the identity of complainants; and
- facilitate prompt restrictions on eNaira speed wallets where a valid report of loss/theft of device or compromise of user eNaira speed wallet is made.

Consumers have an obligation to protecting their eNaira speed wallet login credentials and devices to prevent disclosure to third parties. They must also report promptly to their provider or the eNaira Helpdesk where there has been a loss/theft of device or compromise of user eNaira speed wallet, or any other suspected fraud.

Consumer complaints in relation to the usage of the eNaira should be referred to the provider and resolved within two working days. If the complaint remains unresolved, it can be escalated to the eNaira Helpdesk. Where one or both parties remain unsatisfied with the resolution, the issue shall be referred to an arbitration panel as provided under the Arbitration and Conciliation Act of Nigeria.

Operational resilience

As an alternative central bank liability to cash, a retail CBDC system would need to be extremely resilient, providing access and availability 24/7 every day of the year.

A retail CBDC system may be an attractive target for cyberattacks, in an attempt to steal money, access confidential information, disrupt services, or cause reputational damage to a highly visible national system operated by the central bank of a country.

A retail CBDC system could be vulnerable because it could have more entry points than existing wholesale and retail payment systems. A successful attack would not only cause inconvenience and possible substantial losses for a large number of individuals and businesses, but it could also damage confidence in the central bank and in the financial system.

¹⁴ See Central Bank of Nigeria (2021).

Meanwhile, a retail CBDC could enhance the operational resilience of the payment system if it were designed with offline capability, allowing some payments to be made without internet access. Many digital payment systems cannot operate during natural disasters or other large disruptions, so users have to rely on in-person cash transactions.

In the Eastern Caribbean, the DCash CBDC suffered a lengthy loss of service of almost two months, from 14 January to 9 March 2022.

On 14 January 2022, the ECCB announced that:¹⁵

“... the DCash platform has experienced an interruption in service that has affected all users. This break in service has been caused by a technical issue and the subsequent necessity for additional upgrades. Therefore, DCash transactions are not being processed at this time.”

The ECCB notified users that:

“A report has been made and logged of all failed transactions. These transactions will be honoured as soon as full DCash service is restored. You have our assurance that while DCash service has been interrupted, all DCash wallet balances remain secure and unaffected.

“The ECCB is fully aware of the impact of this service interruption to all of our DCash partners. We are actively and diligently working with our service provider, technical partner and specialists to bring the platform back online.”

The ECCB explained that cause of the loss of service was an expired certificate for the third-party network that hosted DCash’s distributed ledger.

On 3 March 2022 the ECCB issued an update:¹⁶

“The ECCB is completing the final testing and assurance exercises following the system upgrades and will make the DCash platform available for public use next week.

“The security and integrity of all DCash data, applications and architecture, including all central bank, financial institutions, merchant and wallet apps remain secure and intact.

¹⁵ <https://www.eccb-centralbank.org/news/view/region-wide-service-interruption-of-dcash-platform>

¹⁶ <https://www.eccb-centralbank.org/news/view/dcash-service-to-resume-next-week>

“Following the interruption, the ECCB took the opportunity to undertake several upgrades to the DCash platform.... These upgrades have further strengthened the robust security mechanisms which ultimately underpin the DCash technology, resulting in a more resilient product.

“Several new features will be added to the list of DCash functionalities and tested as part of the pilot. These include the introduction of an e-commerce function, which will allow business owners to accept DCash via their websites; government-to-consumer payments; and the rollout of the pilot to the final ECCB member country, Anguilla.”

On 9 March the ECCB announced that:¹⁷

“ full functionality of the DCash digital payments platform has been restored effective Wednesday, 9 March.

“As part of the restoration, the platform now benefits from several upgrades including an enhanced certificate management process and an updated version of the software which provides the foundation for the DCash system. Extensive testing and assurance exercises were conducted prior to restoration of the platform to ensure full functionality of the service in accordance with quality assurance specifications.”

Supervisory response: operational resilience

Financial supervisors have become more focused on operational resilience in recent years. This is in part due to concerns about cyber security, and in part because of the potential impact on consumers and investors of the loss of critical services, whatever the cause of the disruption.

Supervisors have therefore placed more emphasis on the ability of financial institutions not only to prevent operational disruptions from occurring, but also to recover rapidly and securely from any such disruptions when they do occur.

In the case of a retail CBDC, supervisors should focus on the operational resilience of all parties involved in providing the retail CBDC system. These include the central bank, financial intermediaries and other service providers, mobile phone operators, and merchants. A retail CBDC should be subject to at least the same resilience expectations as other critical financial market infrastructures. This should cover both the systems and controls in place to prevent service disruptions and the procedures in place to restore services should a disruption occur. This should include – but not be limited to – effective cyber resilience.

¹⁷ <https://www.eccb-centralbank.org/news/view/dcash-service-resumes>

Where a central bank provides a retail CBDC directly to consumers, it can be argued that it should be subject to the same requirements as are applied to commercial banks offering deposit accounts, on the basis of “same activity, same risks, same regulation.” Where a CBDC is provided through regulated intermediaries, and those intermediaries rely in part on the operational resilience of the central bank for their own operational resilience (for example, where the central bank issues new retail CBDC to an intermediary, or redeems existing retail CBDC from an intermediary), then a supervisor should expect these intermediaries to be able to demonstrate that this reliance has a sufficiently solid basis.

Data privacy

Protecting consumer privacy is critical, both to protect data and to maintain trust. Depending on its design, a retail CBDC raises a number of issues around data privacy.

At one extreme, in a direct (or hybrid) account-based retail CBDC system with the central bank operating a centralized database of transactions, the central bank would hold information on this database on all transactions using the retail CBDC. There is an argument that governments (and perhaps even more so central banks) should protect the privacy of data more effectively than commercial entities. However, there may be concerns that:

- A centralized database means that any security breach will be systemic, because the transaction and account holding records of all users of the retail CBDC would be compromised.
- Public authorities could use a retail CBDC system for surveillance and control. Transactions data could allow public authorities to track individuals, monitor their income and expenditures, and block their accounts (or simply close them without compensation) or their access to CBDC payments. Whether or not this concern was warranted, it could undermine public trust and confidence in a retail CBDC and therefore limit its adoption.

An intermediated retail CBDC system might give rise to less severe concerns about data privacy. Each intermediary or other payment service provider would see and keep records of only a subset of the overall picture, and would address privacy concerns in much the same way they do for existing deposit accounts and private retail payment systems. But two concerns remain.

First, as with a direct or hybrid retail CBDC, there is the risk of large-scale breaches of data held by the system operator or intermediaries. This may be less pronounced in an intermediated retail CBDC because the intermediaries use different security measures, so a vulnerability at one bank or other service provider would not necessarily be present at other banks or service providers. There may also be other opportunities to spread data across entities and across digital storage systems and locations.

An additional protection would be to minimize data storage. This might be achieved by restricting data collection by front-end payment applications, or through the deletion of old transactions after a minimum storage period.

Second, even in the absence of any data breaches, there is a question about the amount of personal information contained within any retail payment system. Data collection and storage for a retail CBDC would involve multiple participants, including the central bank, consumers, financial service providers, data service providers, and government entities.

An alternative approach to data privacy would be to introduce design features and other measures that maximize the anonymity of data, thereby closely replicating the key feature of cash that no centralized records of holdings or transactions exist. There is scope to engineer data privacy by design, by separating individual transaction data from information about identity. For example, information on user identities could be gathered and stored only by payment service providers, with the central bank having no information on the identity of users in any specific transaction. If there were a need to collect such information, for example for law enforcement purposes or to transfer information and account balances to a different provider when a service provider failed, there would need to be clear procedures for doing so, similar to today's bank secrecy laws.

However, as with cash transactions, this could create opportunities for money laundering, the financing of terrorism, and tax evasion. Any retail CBDC would need to strike an appropriate balance between safeguarding the privacy rights of consumers and providing the transparency necessary to deter criminal activity.

Supervisory response: data privacy

Credible privacy and data governance frameworks can create greater trust in a retail CBDC and encourage its adoption. Rules governing the storage, ownership, and sharing of data need to be defined and established. Legal and regulatory reforms could further protect CBDC end users and combat money laundering and the financing of terrorism by specifying the conditions under which information could be used.

As in other retail payment systems, these rules could enhance data privacy by separating payment services from control over the resulting data. Such designs could allow anonymity with respect to specific parties, such as payment service providers, businesses, or public agencies. Consumers can also be given some control over their payments data, leaving them to decide what data they share with payment system providers and third parties.

Concerns regarding end users' privacy within a retail CBDC system, and the trade-off with financial integrity, could be addressed through legal, regulatory and technical choices. Separating identity information from transaction information may enhance data privacy, but this may also require some adjustments in AML/CFT requirements.

As an example, the e-CNY has a tiered wallet design where the lowest category wallets can be anonymous with only phone numbers required. The personal information of these users is not shared with commercial banks or the central bank by the telecom operators. Moreover, payments can be made with tokenized “sub-wallets” pushed to e-commerce and other online-to-offline platforms, while ensuring these platforms have no access to personal information.

In addition, the People’s Bank of China has set up an information firewall and strictly implements information security and privacy protocols. These include appointing responsible persons for maintenance, establishing internal barriers to data use, applying a tiered authorization system, putting in place checks and balances, and conducting internal audits. These are designed to prevent arbitrary information requests and use.

AML and CFT

Financial institutions should be subject to robust rules that are designed to combat money laundering and the financing of terrorism. These rules include customer due diligence, record-keeping, and reporting requirements. A retail CBDC needs to be designed to comply with these rules.

In a direct retail CBDC system, this means imposing these rules on the central bank operating the system. In an intermediated system, the intermediaries need to verify the identity of a person accessing a retail CBDC, just as banks and other financial institutions currently verify the identities of their customers.

However, if customer due diligence was applied to every retail transaction using a CBDC, this would impose high transaction costs because of the large volume of those transactions. To reduce these costs, AML requirements could place a floor on the value of transfers that would trigger the need for customer due diligence.

Similarly, simplified due diligence processes could be applied to the enrolment of customers with small balances into a retail CBDC system, combined where possible with digital identity checks.

Supervisory response: AML and CFT

Many supervisory authorities already impose “tiered” AML and CFT requirements based on the size of transactions or account balances. This approach has been carried across to retail CBDCs, using either the existing thresholds or a new set of thresholds designed specifically for retail CBDCs.

In addition, where central banks issue a retail CBDC directly to end-users, this can be linked to a digital centralized KYC and identity register.

As an example, two tiers of individual wallets are available for The Bahamas Sand Dollar:

Tier I

- \$500 eWallet holding limit, with a \$1,500 monthly transaction limit.
- Government-issued identification is not an enrolment requirement.
- Cannot link to a bank account.

Tier II

- \$8,000 eWallet holding limit, with a \$10,000 monthly transaction limit.
- Government-issued identification is required for enrolment.
- Can be linked to a bank account.

Users of retail CBDCs in other countries are also subject to a tiered structure with transaction and balance limits.

The Central Bank of The Bahamas is developing a centralized KYC register to maintain identification and profile data that would either mandate or allow individuals who do not maintain such information within banks or licensed intermediaries to supply the data for the register. The register would be maintained to be compliant with AML/CFT standards, to enable other financial relationships to be established by Central Bank-supervised financial institutions. The register would draw on data in government-maintained systems, once statutory provisions are enabled or consent-enabled access frameworks are established.

In Nigeria, four tiers of individual wallets are available for the eNaira:

Category	Daily Transaction Limit	Balance/eNaira Speed Wallet Limit
Tier 0 Phone number without verified National Identification Number (NIN)	N20,000	N120,000
Tier 1 Phone number with verified NIN	N50,000	N300,000
Tier 2 Bank Verification Number (BVN) Evidence of basic customer information, and identification and monitoring by financial institutions	N200,000	N500,000
Tier 3 Bank Verification Number (BVN) Customers with Tier 2 accounts can upgrade to Tier 3 by visiting a branch of their bank and providing some required details for the upgrade in line with AML/CFT regulations Banks are required to obtain, verify, and maintain copies of all the required documents for account opening	N1,000,000	N5,000,000

The safety and soundness of financial institutions: Deposit substitution

The introduction of a retail CBDC could lead to a substitution from deposits held with commercial banks, money market funds, or other savings entities into retail CBDC accounts (or retail CBDC tokens). This substitution could occur because of the attractiveness of a retail CBDC in terms of its:

- safety – as a liability of the central bank, as compared with deposits held in commercial banks and other entities;
- remuneration – retail CBDCs could be remunerated by adding interest to CBDCs held either in accounts or as tokens¹⁸;
- cost of use – charges on CBDC accounts could be less than the charges on bank accounts;
- ease of access and ease of making digital payments; and
- privacy and anonymity.

Deposit substitution could have an adverse impact on the deposit base of specific banks and similar entities perceived to be particularly risky, or which offered a relatively poor deal to depositors in terms of remuneration, charges, and ease of access and use.

In response, these banks and similar entities might have to pay a higher cost for their funding; become more reliant on wholesale funding, which may be less stable than retail deposits; increase their risk-taking to restore margins; reduce their lending or increase their lending rates, thereby reducing credit availability or raising credit costs for individuals and businesses; or increase fees and commissions on other products and services.

Some banks or similar entities could therefore become less safe and sound, or offer a less attractive service to their customers, both of which would be a concern for their supervisors.

In addition to this potential impact even in normal circumstances, the existence of a retail CBDC as a safe haven, and the liquidity of and ease of access to retail CBDCs, could make deposits held in banks and similar entities even more “flighty” and therefore increase the probability, speed, and potential severity of a run on a bank.

¹⁸ Although not discussed in this Note, one potential advantage of retail CBDCs for monetary policy would be for a central bank to be able to pass changes in official interest rates – potentially including the imposition of both positive and negative interest rates – directly onto holders of retail CBDC.

Supervisory response: deposit substitution

Supervisory authorities have already taken some steps following the 2007-2009 Global Financial Crisis ahead of any introduction of retail CBDCs. These should limit the extent of deposit substitution, including higher regulatory requirements on banks and other deposit-taking entities; more intensive and intrusive supervision; more generous deposit insurance; and additional powers and tools (such as the Financial Stability Board resolution framework¹⁹) that should protect retail depositors if a financial institution fails.

However, none of these makes a deposit held with a commercial bank or similar entity completely safe. Even deposit insurance has coverage limits and there may be a delay before full access to deposits is restored.

Additional measures can be taken to make a retail CBDC less attractive to individuals and businesses. These could include not offering any remuneration on a retail CBDC, or reducing the rate of remuneration for larger holdings; or limiting the amount of a retail CBDC that could be held by an individual or business, or the size of any transaction using a retail CBDC.

However, if the absence of remuneration and transaction and holding limits make a retail CBDC less attractive, this could also reduce the extent to which a retail CBDC delivers the benefits discussed earlier in this Note, including financial inclusion.

To limit competition with bank deposits, the Bahamas Sand Dollar and the Eastern Caribbean DCash retail CBDCs are non-interest-bearing, with both transaction and holding limits on retail CBDC accounts. In the Bahamas, these limits depend on whether the account holder is a business or an individual and whether the individual is banked or not. In the Eastern Caribbean, transaction and holding limits vary according to the risk profile of each client.

Financial stability

The deposit substitution effects discussed above could also have an adverse impact on financial stability and on the wider economy.²⁰ This could take various forms, including:

- A reduction in retail deposits, which reduces the aggregate amount and stability, or increases the cost, of deposits in the banking system. This could be passed on as a reduction in the availability or increase in the cost of credit (and possibly of other products and services) to individuals and businesses. This could have a negative impact on economic growth and development, especially if the disintermediation was rapid and substantial.
- The failure of a systemically important bank or similar entity.

¹⁹ Toronto Centre (2020) discusses the Financial Stability Board's recommendations for the effective resolution of failing systemically important financial institutions.

²⁰ The potential financial stability implications of retail CBDC are discussed in Bank for International Settlements (2021a).

- A greater probability of a system-wide run on banks, notwithstanding effective banking regulation and supervision, deposit insurance, resolution frameworks, and the availability of central bank liquidity facilities. A widely available and accessible retail CBDC would make it easier for deposits to leave the commercial banking system, making bank runs potentially more frequent and severe during periods of financial panic. During the global financial crisis, there were large-scale outflows from some money market funds to banks. The concern is that similar flows could occur from banks or non-banks to a retail CBDC.

Supervisory response: financial stability

Many of the considerations in the previous sub-section also apply here.

Regulation, supervision, and deposit insurance may make a system-wide reduction in retail deposits less likely, both in normal times and during a financial crisis.

Lower or zero remuneration and limits on retail CBDC holdings or transactions may make a retail CBDC less attractive and less easy to switch into. Such measures could be valuable in managing risks when a retail CBDC is introduced, and could potentially have a longer-term role in some countries.

However, these measures would have to be balanced against policy objectives such as financial inclusion, which can only be achieved through a significant uptake of a retail CBDC.

As with all aspects of financial stability, careful analysis and close monitoring is required to assess the extent of the risks in an individual country. Scenario analysis, stress testing, and sensitivity analysis could all be used to gain a better understanding of the risks to financial stability from the introduction of a retail CBDC.

Supervisory approach

Supervisory authorities have a close and legitimate interest in the design, development, and introduction of a retail CBDC because of the risks to supervisory objectives and the opportunities to enhance financial inclusion. What does this imply for a supervisory authority?

First, a supervisory authority should be involved in the design and development of a retail CBDC if it has responsibility for supervising banks and similar entities or other payment service providers; financial stability; financial inclusion; consumer protection; or anti-money laundering.

The introduction of a retail CBDC will create risks and opportunities for supervisory objectives, and the various design choices will create trade-offs across different supervisory objectives. For example, there may be a trade-off between achieving financial inclusion and maintaining protections against money laundering.

The design of a retail CBDC may have implications for the risks to regulated entities, financial stability, consumer protection, financial inclusion, and money laundering.

Although the central bank may oversee the retail CBDC system, a supervisory authority (including supervisory departments within the central bank) should have a “seat at the table” during the design and development of a retail CBDC. This includes when a central bank decides to change a design feature after a retail CBDC has been introduced.²¹

Second, once the design of a retail CBDC is decided, a supervisory authority should consider what this implies for its regulation and supervision of existing supervised entities, and for the authorization of potential new entrants.

For example, an account-based retail CBDC could operate through the same entities, infrastructure and technologies that are already in place for other digital retail payment systems. Regulated intermediaries will need to conform to the same (or at least very similar) regulatory standards when providing the transfer, storage or custody of retail CBDCs as when providing similar services for other types of digital money and payment services.

This should include requirements on the governance of regulated intermediaries (proportionate to their risk, size, complexity, and systemic importance, and to the financial stability risk that may be posed by the activity or market in which the providers are participating). Other requirements should cover lines of responsibility and accountability; risk management framework; operational resilience; robust frameworks for collecting, storing, safeguarding, and the timely and accurate reporting of data; cyber security; anti-money laundering and countering terrorist financing controls; and other relevant policies, procedures, and infrastructures.²² Supervisory authorities should have access to the data and information as necessary and appropriate to fulfil their mandates.

Supervisory authorities can use standard supervisory techniques – including off-site and on-site supervision and the use of reports – to assess whether intermediaries are meeting these requirements.

Third, a retail CBDC may require enacting new laws and regulations or revising existing laws to enable the effective supervision of regulated retail CBDC participants, whether existing or new players undertaking similar or novel roles under the CBDC system. This may include laws and regulations governing data privacy, AML/CFT, and the transfer of data and assets in the event of a failure of a service provider. This would provide a “rulebook” setting out the roles and responsibilities of the operator(s), participants, and potentially other service providers in a retail CBDC system.

Fourth, and in particular if a retail CBDC does encourage innovation, supervisory authorities must remain alert to the possible need to adjust the regulatory perimeter to bring new types of entity (or existing entities undertaking new activities) within the regulatory and supervisory net.

²¹ For example, in Nigeria, three supervisory departments within the Central Bank of Nigeria and other financial sector regulatory agencies were part of the team established to consider all aspects of the eNaira and to write the Regulatory Guidelines on the eNaira. [Source: discussion with the Central Bank of Nigeria.]

²² Financial Stability Board (2022) discusses these issues in the broader context of crypto assets.

Fifth, a supervisory authority should consider whether a central bank activity might fall within the regulatory perimeter, in particular where a direct retail CBDC design is implemented. The principle of “same activities, same risks, same regulation” might apply to a central bank offering CBDC accounts directly to individuals and businesses; to a central bank holding data on individuals and their activities; and to a central bank handling complaints from retail customers.

A central bank providing these direct services to end-users should be subject to some oversight to assess whether it is treating its retail customers fairly, has adequate operational resilience (including the ability to covert retail CBDC claims into cash if necessary), and is applying appropriate customer due diligence. This could be delivered through some form of self-regulation, public procurement rules, and independent third-party reviews. However, this cannot remove entirely the conflict of interest that could arise if a central bank is supervising itself, or if one part of a central bank is being supervised by a supervisory department within the central bank.

Conclusion

Since some emerging markets and developing economies have already issued a retail CBDC, and many other countries are considering doing so, it is important for supervisory authorities to consider the possible implications for their supervisory objectives.

It is not the purpose of this Note to recommend any specific design features of a retail CBDC. However, these design features will have implications for consumer protection and data privacy, the safety and soundness of banks, financial stability, financial inclusion, anti-money laundering, and cross-border remittances.

There are therefore difficult balances to be drawn when designing a retail CBDC. Since most countries are still at this design stage, it is important that supervisory authorities have a “seat at the table” so supervisory objectives can be properly considered in the design.

References

- Atlantic Council. [Central Bank Digital Currency Tracker](#). 2023.
- Auer, R. and Böhme, R. [The technology of retail central bank digital currency](#). BIS Quarterly Review. March 2020.
- Bank of Jamaica. [BoJ prepares for central bank digital currency](#). March 2021.
- Bank for International Settlements. [Rise of the central bank digital currencies: drivers, approaches and technologies](#). BIS Working Paper 880. August 2020a.
- Bank for International Settlements. [Central bank digital currencies: foundational principles and core features](#). October 2020b.
- Bank for International Settlements. [Central bank digital currencies: financial stability implications](#). September 2021a.
- Bank for International Settlements. [Central bank digital currencies: motives, economic implications and the research frontier](#). BIS Working Papers 976. November 2021b.
- Bank for International Settlements. [Central bank digital currencies \(CBDCs\) in Latin America and the Caribbean](#). BIS Working Papers 989. January 2022a.
- Bank for International Settlements. [CBDCs in emerging market economies](#). BIS Papers 123. April 2022b.
- Bank for International Settlements. [Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies](#). BIS Papers 125. May 2022c.
- Bank for International Settlements. [Central bank digital currencies in Africa](#). BIS Papers 128. November 2022d.
- Bank for International Settlements. [Rise of the central bank digital currencies: drivers, approaches and technologies. Updated data set](#). January 2023.
- Board of Governors of the Federal Reserve System. [Money and Payments: The U.S. Dollar in the Age of Digital Transformation](#). January 2022.
- Carstens, A. and H.M. Queen Máxima of the Netherlands. [CBDCs for the People](#). April 2022.
- CBDC Tracker. [cbdctracker.org](#). 2023.
- Central Bank of The Bahamas. [Digital Bahamian Dollar](#). 2023.
- Central Bank of Nigeria. [Regulatory Guidelines on the eNAIRA](#). October 2021.
- Digital Currency Initiative. [CBDC: Expanding Financial Inclusion or Deepening the Divide?](#) January 2023.
- Eastern Caribbean Central Bank. [ECCB Governor Announces DCash Public Launch](#). March 2021.
- Financial Stability Board. [Enhancing Cross-border Payments. Stage 3 roadmap](#). October 2020.

Financial Stability Board. [Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets](#). Consultative document. October 2022.

Financial Stability Institute. [Central bank digital currencies: a new tool in the financial inclusion toolkit?](#) FSI Insights 41. April 2022.

International Monetary Fund. [Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations](#). IMF Working Paper 2020/254. November 2020.

People's Bank of China. [Progress of Research and Development of E-CNY in China](#). July 2021.

Reserve Bank of India. [Concept Note on Central Bank Digital Currency](#). October 2022.

Steven L. Schwarcz. [Regulating digital currencies: towards an analytical framework](#). CPMI Conference on Pushing the frontiers of payments: towards faster, cheaper, more transparent and more inclusive cross-border payments. March 2021.

Toronto Centre. [Operational resilience: The Next Frontier for Supervisors?](#) April 2021.

Toronto Centre. [Resolution: Implications for supervisors](#). August 2020.

Toronto Centre. [Regulation and Supervision of Retail Payment Systems](#). January 2023.