WP/20/104

IMF Working Paper

A Survey of Research on Retail Central Bank Digital Currency

by John Kiff, Jihad Alwazir, Sonja Davidovic, Aquiles Farias,
Ashraf Khan, Tanai Khiaonarong, Majid Malaika,
Hunter Monroe, Nobu Sugimoto,
Hervé Tourpe, and Peter Zhou

IMF Working Papers **describe research in progress by the author(s) and are published to elicit comments and to encourage debate.** The views expressed in IMF Working Papers are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

INTERNATIONAL MONETARY FUND

WP/20/104

IMF Working Paper

Monetary and Capitals Markets Department, Information Technology Department, and the World Bank

A Survey of Research on Retail Central Bank Digital Currency

Prepared by John Kiff,[1] Jihad Alwazir, Sonja Davidovic, Aquiles Farias, Ashraf Khan, Tanai Khiaonarong, Majid Malaika, Hunter Monroe, Nobu Sugimoto, Hervé Tourpe, and Peter Zhou[2]

Authorized for distribution by Jihad Alwazir

June 2020

***IMF Working Papers* describe research in progress by the author(s) and are published to elicit comments and to encourage debate.** The views expressed in IMF Working Papers are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

This paper examines key considerations around central bank digital currency (CBDC) for use by the general public, based on a comprehensive review of recent research, central bank experiments, and ongoing discussions among stakeholders. It looks at the reasons why central banks are exploring retail CBDC issuance, policy and design considerations; legal, governance and regulatory perspectives; plus cybersecurity and other risk considerations. This paper makes a contribution to the CBDC literature by suggesting a structured framework to organize discussions on whether or not to issue CBDC, with an operational focus and a project management perspective.

JEL Classification Numbers: E51, E58, E52

Keywords: money, central bank digital currencies, monetary policy

Author's E-Mail Address: JKiff@imf.org; JAlwazir@imf.org; SDavidovic@imf.org; AFarias@imf.org; AKhan4@imf.org; TKhiaonarong@imf.org; MMalaika@imf.org; HMonroe@imf.org; NSugimoto@imf.org; HTourpe@imf.org; ZZhou1@worldbankgroup.org

[1] Corresponding author

[2] The paper also benefited from comments and contributions from Tobias Adrian, Chris Erceg, Dong He, Tommaso Mancini-Griffoli, Wouter Bossu, Tamas Gaidosch, Dirk Jan Grolleman, Vikram Haksar, Nigel Jenkinson, Elias Kazarian, Marcello Miccoli, Mwanza Nkusu, Jan Nolte, Manasa Patnam, Nadine Schwarz, Tao Sun, Zhibo Tan, Itaru Yamamoto, David Andolfatto, Ahmed Faragallah, Michael Kumhof, David Mills, Harish Natarajan, Oya Pinar Ardic, Jorge Ponce, Adolfo Sarmiento, Cecilia Skingsley, Gynedi Srinivas, and Martin Summer. Donna Tomas provided excellent editorial assistance.

TABLE OF CONTENTS

Tables

Figures

Boxes

Annexes

EXECUTIVE SUMMARY

Central bank digital currency (CBDC) is a digital representation of sovereign currency that is issued by a jurisdiction's monetary authority and appears on the liability side of the monetary authority's balance sheet. By surveying published research, this paper examines in detail the issuance considerations, focusing solely on retail CBDC for use by the general public.[3] This paper focuses mainly on CBDC issued directly by the central bank, as opposed to "synthetic" CBDC (sCBDC) which is privately-issued digital money backed by central bank reserves, regulated and supervised by the central bank (Adrian and Mancini-Griffoli, 2019a). The intention of the paper is not to advocate for retail CBDC issuance, but to take stock of recent research, central bank experiments, and ongoing discussions among stakeholders on the topic. It also intends to summarize existing literature, providing central bankers and researchers with a deep dive into the complex interrelated policy issues beyond just whether to issue retail CBDC, including operating models, design considerations and risk management issues. Given the limited practical experience with the topic, these are just initial observations and are not meant to be prescriptive, exhaustive, or universal.

At the conceptual level, most of the major central banks and monetary authorities considering CBDC issuance are following similar workflows that start with clearly identifying objectives and then thoroughly assessing expected benefits, costs, and risks. The authorities exploring CBDC issuance cite different objectives, two primary ones being to improve financial inclusion and to maintain the central bank's relevance in the monetary system. Other objectives include reducing costs associated with physical cash, increasing payment system efficiency, improving monetary policy formulation and implementation, strengthening financial integrity, addressing potential issues related to private payment systems such as privacy or monopolistic power, and more recently following the COVID-19 global crisis, to expedite stimulus payments and to make payment systems more resilient against shocks.

On the other hand, some observers have highlighted significant potential risks with CBDC issuance. These include hampering monetary policy transmission, competing with bank deposits and undermining bank intermediation, and facilitating runs from bank deposits to CBDC during banking crises. Operational risks include issues relating to cyber-resilience, misdirection of funds, data loss or leakage, outsourcing/third-party dependency, and reputational risks. These can also lead to serious financial stability risks.

Central banks exploring CBDC issuance are considering different business models based on issuance, distribution, and transfer of CBDC to execute payments. All are thinking to retain the issuance function, but most are planning to outsource the distribution and payments components to private financial institutions. Some are focusing on running on a traditional centralized ledger, and some on a distributed ledger technology (DLT) platform in which the ledger is replicated and shared across several trusted participants within a private permissioned network. Balancing the need to ensure privacy of user identity and transaction

[3] This paper does not cover wholesale CBDC (W-CBDC). W-CBDC is limited to a set of predefined user groups, typically banks and other members of national payment systems, whereas a retail CBDC is widely accessible to the public. See WEF (2020) for a broader analysis of CBDC issuance considerations that includes W-CBDC. See BIS (2019) for an extensive discussion of W-CBDC.

data while meeting financial integrity standards is also an important design challenge. Some academic research advocates paying variable interest rates to CBDC holders to modulate demand or provide a new monetary policy instrument, but few central banks are considering doing so at the outset.

This paper also reviews some of the processes, roles, and responsibilities that would need to be defined for creating, issuing, distributing, freezing, deactivating, and destroying CBDC. Central banks considering issuing CBDC are also discussing how to address up-front cybersecurity risks at the business, process, and infrastructure layers.

Central banks considering moving beyond the pilot stage are deliberating whether to spell out the status of CBDC as legal tender in the appropriate laws and regulations. Some central banks may find that their governance frameworks need amending to accommodate CBDC issuance (addressing objectives and functions, technical requirements, internal organization requirements, and arrangements for transparency and accountability). Regulatory and supervisory frameworks may also need amending to cover new roles and players.

A decision to issue CBDC will stretch the technical capacity and resources of even the best-equipped central banks, in an environment where technology and risks are evolving rapidly. At the same time, outsourcing vital central bank functions to external vendors calls for great care and vigilance, given the functions’ systemic importance and significant financial, operational, and reputational risks to the central bank. Based on a comprehensive survey of published research, this paper aims to suggest general foundations for discussions on whether to issue CBDC, and if the decision is made to go ahead, present concrete operational considerations.

I. Introduction: Retail CBDC

In addition to monetary and financial stability roles, central banks play a core public sector role in the economy to provide a safe, efficient, and inclusive payment system. As technology, user needs, and regulation change, the payment system may have to adapt. In some economies, cash is disappearing as a means of payment, and new digital payment systems are challenging central bank roles. In other countries, the private sector lags in improving financial inclusion and reducing the operational costs and risks associated with the management of physical currency. To address these challenges, some central banks are exploring issuing retail CBDC—a widely accessible digital form of fiat money (available to the public) that could be legal tender. Such CBDC would be a central bank liability and form part of the base money supply.

IMF staff have proposed a conceptual framework to assess the case for retail CBDC issuance from the perspectives of users and central banks (Mancini Griffoli and others, 2018). This assessment concluded that the impact of CBDC introduction will hinge on its design and country-specific characteristics. Overall, the note found no universal case for CBDC adoption yet, and that demand for CBDC will depend on the attractiveness of alternative forms of money. Some concerns have been expressed that CBDC issuance could hamper monetary policy transmission, but the paper concluded that this is unlikely, and it may even strengthen it through greater financial inclusion. A well-designed CBDC could enhance financial integrity compared to cash, but a poorly designed one could undermine the authorities' compliance with financial integrity standards. Also, while CBDC could increase deposit-taking institutions' funding costs, impact the funding structure of deposit-taking institutions, and intensify "run" risk, design choices such as tiered CBDC remuneration and various policy measures can help ease such concerns.

Building on those conclusions, this paper takes a closer look at the design, risk, and operational considerations of issuing retail CBDC, based on published research, central bank experiments, and ongoing discussions among stakeholders. There are many papers that provide high-level overviews of CBDC implications for payments, monetary policy, and financial stability (BIS, 2018) or their effects on monetary policy instruments (European Money and Finance Forum, 2018 and Lariccia, 2018). There are general evaluations of CBDC models and their main attributes (Norges Bank, 2018) and considerations on how to design CBDC to ensure financial stability by pre-empting liquidity squeezes and system-wide run from bank deposits (Kumhof and Noone, 2018).

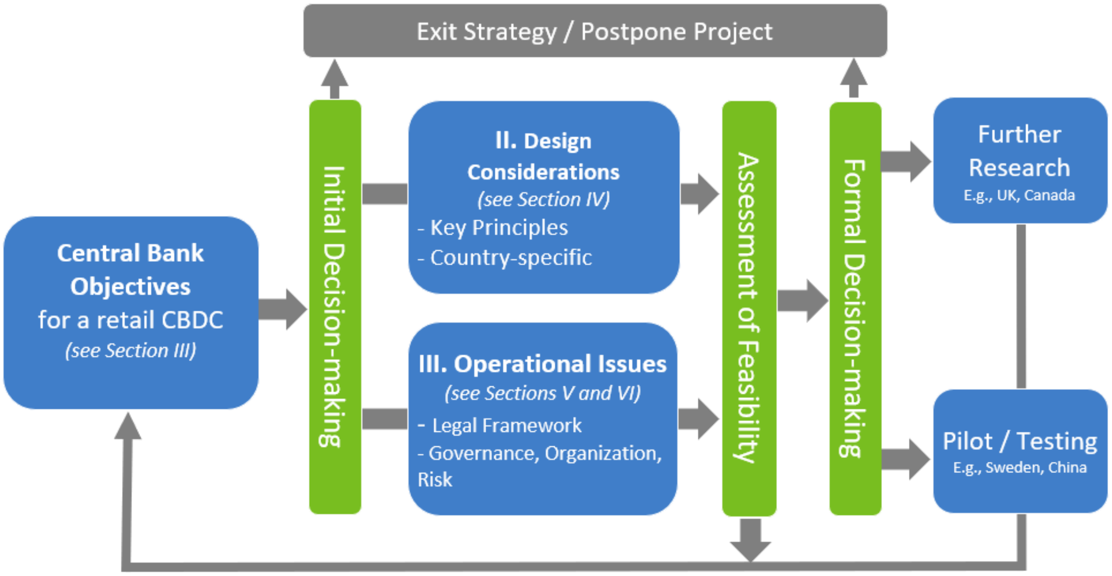
This paper also builds on the recent literature that discusses detailed CBDC design considerations and technological solutions. Auer and Böhme (2020) provide an overview of underlying trade-offs and the related hierarchy of technical design choices, while others explore options and describe potential limits that the underlying technology may impose on the mix of policy objectives (e.g., Shah and others, 2020). There are proposals on platform models to provide a fast, highly secure, and resilient technology infrastructure that would provide the minimum necessary functionality for CBDC payments (BoE, 2020) and a two-tier remuneration of CBDC as a solution to the risk of structural disintermediation of banks risk and facilitation of systemic runs on banks in crisis situations (Bindseil, 2020).

This paper focuses on CBDC intended to be used only within the borders of the issuing central bank. It lays out some of the most relevant elements being considered for keeping usage within those borders, including ensuring that foreign visitors have at least limited access. However, interoperability and standardization across national or international digital payment systems are important considerations to keep cross-border options open for future evolution. To this end, it would seem prudent for central banks to consider coordinating their CBDC efforts closely and introducing sufficient flexibility into their CBDC designs to facilitate cross-border interoperability and standardization across CBDC implementations. Cross-border and financial integrity issues will be addressed in separate papers.

Figure 1 shows the main elements that will be covered in the paper. It opens with a basic definition of CBDC (Section II) before reviewing the main issuance objectives and risks (Section III). Next, Section IV discusses key design features, such as the business model, technology, degree of anonymity/transparency, offline functionality, and whether it should bear interest. This is followed by a detailed review of governance, legal, and regulatory requirements (Section V), concluding with cybersecurity considerations (Section VI). This sequence does not necessarily reflect the workflow of the CBDC issuance decision-making process because some choices are inter-related, and there may be feedback from one decision to another. For example, a product design decision may impact on factors considered in the decision as to whether to issue CBDC. Similarly, lessons learned during a pilot phase may impact product design and/or regulatory considerations. In other words, the CBDC decision-making process should be viewed as dynamic and iterative with possibly multiple feedback loops. Depending on capacity, some of the workflow elements can be tackled in parallel. For example, one team could be working on the regulatory aspects while another could be devising core design principles.

This paper aims to provide a comprehensive review of the published research and suggest general considerations for discussions on whether to issue CBDC, and if the decision is made to go ahead, present concrete operational considerations.

Figure 1. Main Elements of the Paper


Exit Strategy / Postpone Project
Central Bank Objectives for a retail CBDC (see Section III)
Initial Decision-making
II. Design Considerations (see Section IV)
- Key Principles
- Country-specific
III. Operational Issues (see Sections V and VI)
- Legal Framework
- Governance, Organization, Risk
Assessment of Feasibility
Formal Decision-making
Further Research E.g., UK, Canada
Pilot / Testing E.g., Sweden, China

KEY QUESTIONS

* What is/are the objectives of issuing CBDC's? Have all other options been considered? Interaction with existing objectives?
* Is the legal/regulatory/supervisory framework supportive? Is the relevant infrastructure available?
* Are all risks (e.g., macroeconomic, monetary policy implementation, financial stability, cyber security) identified and addressed?
* Are key stakeholders involved? Are proper project management principles and practices being followed?

Source: Authors.

II. CBDC Definition

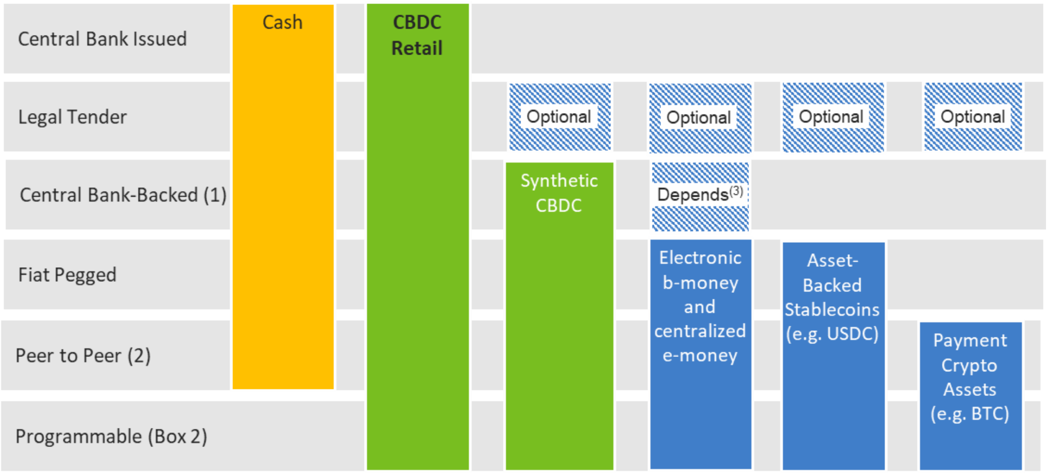
This paper will define CBDC as a digital representation of a sovereign currency issued by and as a liability of a jurisdiction's central bank or other monetary authority. However, the taxonomy of digital representations of money is still evolving, and there are no universally accepted CBDC definitions.[4] Figure 2 presents the taxonomy that will guide the discussion in this paper, comparing physical cash to four types of digital currency (CBDC, sCBDC, stablecoins, and crypto-assets) based on whether it is (i) issued by a central bank, (ii) deemed legal tender, (iii) central bank backed, (iv) pegged to a fiat currency, (v) allows for peer-to-peer transfers, and (vi) can be programmed.[5] For example, sCBDC is backed by, but not issued by or a direct claim on, a central bank, but can be deemed legal tender. The concept of legal tender, which is discussed in more detail in Section V.A., varies slightly

[4] There are other digital forms of money backed by fiat currency but not issued by the monetary authority and are therefore not considered CBDC. These could include various forms of "b-money" such as credit and debit cards, and "e-money" like stored-value facilities (M-Pesa, AliPay and WeChat Pay). For a fuller discussion of digital money, see Adrian and Mancini-Griffoli (2019a).

[5] Stablecoins are crypto-assets pegged to fiat currency. Crypto-assets are privately issued tokens that are digital representations of value that are not denominated in fiat currency, that depend primarily on cryptography and distributed ledger technology as part of their perceived or inherent value. Many asset-backed stablecoins have been launched. The biggest by far is Tether ($9.2 billion market capitalization on June 8, 2020), followed by USD Coin ($725 million), Paxos ($245 million), BinanceUSD ($170 million) TrueUSD ($140 million).

across jurisdictions, but basically it defines the forms of money that are legally recognized as satisfactory mediums of exchange to pay for goods or services and discharge financial obligations. Also, all digital currencies can be programmed. Programmability, which is discussed in more detail in Section IV.F, is achieved via smart contracts that encode the terms of traditional contracts into computer programs and executes them automatically.[6]

Figure 2. Retail Money Key Attributes



(1) Backed by deposits at the central bank
(2) Person to person, bank to bank, merchant to merchant, person to merchant etc.
(3) B-money is typically fractionally backed by central bank reserves, whereas centralized e-money may or may not be. For example, Kenya's M-Pesa is not, but China's AliPay and WeChat Pay are fully central bank-backed.

Source: Authors.

Many central banks are considering the pros and cons of issuing retail CBDC. Annex 1 tabulates the jurisdictions in which central banks are (or have been) actively exploring CBDC for retail use based on publicly available information.[7] At least four central banks (Bahamas, Ecuador, Ukraine, and Uruguay) are conducting, or have already conducted, limited-scale pilot issuance, and others are making plans, such as the Eastern Caribbean Central Bank (Kotaro and others, 2020).

Some countries are exploring retail crypto-assets which are used as a medium of exchange to pay for goods or services and discharge financial obligations. These are not CBDC, because they are not digital representations of the countries' central bank-issued fiat currency and they are issued by the countries' finance ministries and not their central banks. For example, the government of the Marshall Islands is planning to launch the SOV, a crypto-asset that will become legal tender along with the U.S. dollar, with the motivation to raise funds for the

[6] A smart contract encodes the terms of a traditional contract into a computer program and executes them automatically (BoE, 2020, and Box 3 in He and others, 2017).

[7] By "active" is meant central banks which have convened projects to seriously explore retail CBDC or have undertaken pilots.

government.[8] Similarly, Venezuela has launched the Petro, a commodity-backed crypto-asset, in an attempt to skirt U.S. and EU sanctions (Berman, 2018).

III. Motivations and Policy Considerations for Issuing CBDC

This section examines the motivations that central banks have identified for issuing, or not issuing CBDC and factors influencing this decision. Clarifying objectives provides a framework for balancing pros and cons of CBDC issuance and guiding design options in the context of country-specific circumstances.

A. Why Central Banks are Exploring CBDC Issuance[9]

Central banks are considering a wide range of objectives for issuing retail CBDC. These are summarized below and reviewed more deeply in the rest of this subsection:

- CBDC could enhance payment system competition, efficiency, and resilience in the face of increasing concentration in the hands of few very large companies.
- CBDC may be a means to support financial digitization, reduce costs associated with issuing and managing physical cash, and improve financial inclusion, especially in countries with underdeveloped financial systems and many unbanked citizens.
- CBDC could improve monetary policy effectiveness to implement targeted policy, or to tap more granular payment flow data to enhance macroeconomic projections.
- An interest-bearing CBDC could enhance the transmission of monetary policy, by increasing the economy’s response to changes in the policy rate. Such a CBDC could be used to break the “zero lower bound” on policy rates to the extent cash were made costly.
- CBDC would also help reduce or prevent the adoption of privately issued currencies, which may threaten monetary sovereignty and financial stability, and be difficult to supervise and regulate.
- CBDC could help improve traction of local currency as means of payments in jurisdictions attempting to reduce dollarization.
- CBDC could play a role in distributing fiscal stimulus to unbanked and other recipients.

CBDC may be aimed at mitigating the market dominance of private payment systems or reducing concentration risk in such payment systems. Payment systems may tend to become natural monopolies, reflecting strong network externalities (the value of using a given payment network is greater the larger the user community, including savings from netting

[8] IMF staff have assessed that the potential benefits from revenue gains appear considerably smaller than the potential costs arising from economic, financial integrity, reputational, governance and legal risks. Given this, and in the absence of adequate measures to mitigate potential costs and risks, staff recommended that the Marshall Island authorities seriously reconsider the issuance of the SOV as legal tender (IMF, 2018).

[9] This section draws heavily from Mancini-Griffoli and others (2018) and Adrian and Mancini-Griffoli (2019b), plus Barontini and Holden (2019), Boar and others (2020) and King (2020).

transactions), economies of scale (decreasing average costs, including high fixed development and maintenance costs), and economies of scope, (gains from aggregating data to provide additional services - Bolt, 2005, and Gowrisankaran and Stavins, 2004). However, some private money issuers may not internalize the social cost of possible systemic disruptions from operational failure, including cyberattacks, and thus may underinvest in security. Also, monopolistic private issuers may abuse that power and lead to inefficiency by offering partial, inadequate and expensive services. They could also commercialize collected user data, although these could also invite competition, depending on the barriers to entry. These arguments might justify CBDC issuance or some jurisdictions' decision to deploy fast payment systems, which also gives them control over an essential piece of the payment architecture. If monopolistic distortions raise concerns, antitrust regulations and data protection legislation could be a response (CGAP, 2019).

CBDC could improve financial inclusion in countries with underdeveloped financial systems and low financial penetration. In countries with large remote or rural areas, or more of the population shifting to digital forms of money, the infrastructure for distributing cash may not be available or has deteriorated, and businesses may resist dealing with it. Their commercial banks and other deposit-taking institutions might be financially constrained or not highly incentivized to offer banking services to some segments of the population. One policy solution may involve subsidizing the distribution of cash to remote areas and/or provision of banking services through alternative solutions to those underserved populations such as mobile money (e.g., M-Pesa in Kenya and PayTM in India). However, the lack of digital financial services could relate to weak digital communications infrastructure calling for the prioritization of efforts to improve it. However, if barriers to financial inclusion stem from an aversion to or difficulties in achieving formalization, neither CBDC nor other digital initiatives would prove sufficient.

Issuing CBDC and pushing financial services digitization may reduce costs associated with issuing and managing physical cash. Alvez and others (2019) estimated that the private costs of using cash in Uruguay were about 0.6 percent of GDP. In a review of the relevant literature, they found that such private costs ranged from 0.2 percent (Norway) to 0.6 percent (Belgium). Kosse and others (2017) came up with similar numbers for cash usage in Canada (0.5 percent of GDP), but Banka (2018) reported much higher costs for Albania (1.0 percent) and Guyana (2.5 percent). Costs fall mostly on banks, firms, and households. Although introducing and maintaining CBDC would probably entail substantial fixed costs, marginal operational costs would likely be low, despite the need for customer service. On this basis, the cost efficiency case to adopt CBDC may be better for larger jurisdictions able to absorb the fixed costs. Also, considering that managing digital cash is comparatively as complex as managing physical cash (Annex 2), it should not be assumed that digitalization will necessarily lead to cost reduction. For example, some of the fixed costs to the central bank and commercial banks associated with physical cash will remain. Finally, there are additional development and operational costs associated with CBDC as illustrated in Table 1.

Table 1: Costs Associated with Developing and Operating CBDC

Cost Category	Examples
Labor	IT consulting firm; developers; user experience specialist; wallet maintenance costs, etc.
Infrastructure	Cloud or on-premise servers
Software	Licenses; service fees
Cyber Security	Threat modeling; protection; identification; response management; penetration tests. Etc.
Support	Help desk; training; communication

Source: Authors.

CBDC issuance could improve monetary policy effectiveness. Interest-bearing CBDC could allow for deeply negative policy rates, although only if cash were prohibited as argued in Rogoff (2014), made costly to hold as suggested in Bordo and Levin (2018), or made to depreciate against CBDC, which would become the sole legal tender (Agarwal and Kimball, 2015). However, deeply negative rates could generate criticism from the public and substantially undermine public confidence in the central bank (Mersch, 2020). CBDC could also allow for the implementation of non-linear transfers based on user account balances (Davoodalhosseini and others, 2020) or "helicopter drop" monetary stimulus to alleviate adverse impacts arising from natural disasters or public health crisis or facilitate other "unprecedented policies," bordering on fiscal policy, such as those proposed by Boivin and others (2019). CBDC could also be designed to amplify money velocity by incentivizing specific types of consumer consumption (Copic and Franke, 2020). For example, "cash back" payments could be made on purchases from local merchants and/or certain industries, or

CBDC holdings could incur a fee to incentivize people to quickly spend it. The central bank would credit citizens' CBDC accounts or wallets holding CBDC tokens. However, doing so would not necessarily reach all citizens, and the central bank would have to decide how much to transfer to each household, a thorny issue given the distributional consequences. Finally, more innovative monetary policy could discourage innovation in existing payment systems (BoE, 2020), lead to a disproportionate concentration of power in the central bank, and be at odds with the concepts of separating monetary from fiscal policy and central bank independence (Mersch, 2020).

Central banks could use CBDC for targeted monetary policy formulation and conduct. Central banks could tap real-time and more granular contextual payment metadata to enhance monetary policy formulation and macroeconomic projections (Bergara and Ponce, 2018). Access to historical transaction data and the ability to observe the economy's response to shocks or policy measures in near real-time and more accurately would be valuable from a financial and macroeconomic stability perspective (Burgos and Batvia, 2018). This micro-level view of payment flow data would help policymakers recognize the macro-financial effects of seasonality, natural disasters or consumer behavior.[10] Central banks could use that

[10] For example, if there is an explicitly defined numerical inflation target, CBDC could be designed to notify when the inflation forecast is converging (or not) with the target (Sarwat, 2012).

collected data in machine learning and other advanced quantitative models to inform macro-economic projections, manage liquidity and reserves, or determine the true velocity of money. Machine learning models based on pattern recognition could help forecast demand for CBDC by designated regions or sectors. Before collecting and using micro-level consumer data, it would be necessary to implement adequate data protection and cyber-resilience measures to avoid theft or misuse of that data (see section VI). Without these measures in place, central banks risk high reputational damage, which would outweigh any potential benefits from CBDC.[11]

CBDC would help preserve monetary central banks' monetary sovereignty. Stablecoin-based payment systems like Facebook's Libra could gain a substantial share of payments markets. Particularly in emerging market and developing economies (EMDEs) they could threaten monetary sovereignty by accelerating currency substitution (e.g., dollarization) and undermine financial stability (Diez de los Rios and Zhu, 2020; FSB, 2020). Widespread migration into stablecoins could reduce commercial bank deposits which could shrink their sources of stable funding, as well as their visibility into transactions data, and hinder credit provision to the economy (Brainard, 2020). Global stablecoins that are adopted across multiple jurisdictions could be difficult to supervise and/or regulate, particularly for EMDEs likely acting as hosts to most entities in a stablecoin system, which may be headquartered elsewhere (Feyen and others, 2020). A well-designed CBDC or sCBDC might ensure that public money remains a relevant unit of account (Brunnermeier and others, 2019).

CBDC could help improve traction of local currency as means of payments in jurisdictions attempting to reduce dollarization. However, CBDC would not by itself address causes of dollarization or alter the attractiveness of foreign currency as store of value, particularly where residents have lost trust in the local currency due to unsound domestic policies and macro instability (current instability or episodes of past instability). CBDC could also foster financial inclusion, increasing use of local currency in payments, and possibly contribute to de-dollarization as part of a comprehensive strategy that addresses the fundamental causes of dollarization through consistent fiscal, monetary, and financial policy mix that stabilizes the macroeconomic framework, lowers inflation, ensures a healthy financial system, and develops local currency denominated instruments (such as a local bond market and availability of hedging instruments against foreign exchange rate exposures).

CBDC could be used as a payment rail for stimulus and other government-to-peer (G2P) direct payments to households. For example, a March 22, 2020 draft of a U.S. House emergency COVID-19 stimulus bill referred to the creation of a "digital dollar" to get

[11] Also, advanced data analytics involves a high degree of complexity that requires adequate resources, time and data. Setting up, training, testing and maintaining machine learning models demand substantive time commitment by subject matter experts (financial sector and monetary policy experts), data scientists, and possibly back-end developers. Vast amounts of data points are required for the model to be trained and tested. Hence data analytics will only be an option once a CBDC becomes fully operational and sufficient data has been generated. Unanticipated biases might occur in using machine learning techniques that could adversely affect segments of financial market actors. Also, strong cybersecurity will be necessary since security breaches could wreak havoc in the financial system.

stimulus payments to unbanked Americans.[12] Under the proposal, the U.S. Treasury, acting through the Internal Revenue Service (IRS), would have the option of making payments by direct deposit to recipient bank accounts or "digital dollar wallets" if the IRS has enough information (otherwise by check). Digital dollar wallets ("FedAccounts") would be offered directly by Federal Reserve Banks (FRBs), or indirectly by FRB-member banks through pass-through FedAccounts. Pass-through FedAccounts would entitle individual wallet holders to a pro rata share of a pooled reserve balance held in master accounts at FRBs. Each bank would have to set up a separate legal entity for the sole purpose of holding all assets (exclusively central bank reserves) and maintaining all liabilities associated with pass-through FedAccounts. Digital dollars would be remunerated at an interest rate that is the greater of the interest rate on required reserves and that on excess reserves. It was ultimately pulled from the final legislation, but the idea came back into play as a standalone Senate bill.[13] However, there are many other ways of directly transferring funds to households that could be considered alongside CBDC issuance (Rutkowski and others, 2020).

B. The Risk of Issuing CBDC

The introduction of CBDC could affect the transmission of monetary policy. For example, CBDC would change the demand for base money and its composition in unpredictable ways and might also modify the sensitivity of the demand for money to changes in interest rates (Carstens, 2019). However, Mancini-Griffoli and others (2018) argue that this impact is unlikely to be significant under plausible CBDC designs. In fact, monetary policy transmission could strengthen if CBDC increases financial inclusion and, therefore, exposes more households and firms to interest-sensitive instruments. The exchange rate transmission channel may be altered by the introduction of CBDC because it would facilitate more active currency management which could lead to stronger/faster exchange rate movements for given market rate changes (Armelius and others, 2018). The bank lending transmission channel, by which monetary policy affects bank creditworthiness and cost of funding could also be maintained if central banks provide stable funding by recycling deposits back into the banking system.

Depending on design, CBDC could affect financial stability and banking intermediation if it competes with bank deposits (Fernández-Villaverde and others, 2020). The extent to which CBDC will compete with commercial bank deposits will depend in part on interest rates paid on CBDC, if at all. A non-interest bearing CBDC would come closest to mimicking cash. Banks with a larger share of retail deposits will face competition from CBDC, particularly an interest-bearing CBDC, and they may have to raise deposit rates to remain competitive. Such higher deposit rates would reduce interest margins, and banks could attempt to increase lending rates, though at the cost of loan demand.[14] The ability of banks to respond and

[12] https://assets.documentcloud.org/documents/6817441/House-Democrats-Counterproposal-For-Stimulus.pdf

[13] https://www.banking.senate.gov/imo/media/doc/SIL203681.pdf

[14] In addition, central banks could lower policy rates to counter the tighter financial conditions stemming from banks' higher lending rates, so that the banks' response to CBDC would be less contractionary for the economy. Moreover, the net impact of CBDC adoption on interest rates will depend on how the central banks introduce

preserve profitability will depend on their power in loan markets (Agur and others, 2019). Deposit insurance allows banks to fund themselves with deposits at lower cost than with other instruments. CBDC issuance could reduce market discipline, if banks lose more uninsured than insured deposits, which could lead to banks taking on more risk.

Banks could also increase their reliance on wholesale funding, with implications for funding cost and stability, and market discipline. However, under current regulatory liquidity requirements, they may have to reduce lending or corporate bond holdings (BIS, 2013 and 2014). Also, it would not be a viable option in countries with less developed capital markets. But even when and where switching from deposit to wholesale funding is feasible, it could result in lower bank profits or higher lending rates to preserve margins. Bank funding could also become more volatile.[15] In that case, banks might have to hold more liquid assets to meet regulatory requirements or cut back on lending possibly at the expense of financial inclusion or growth-enhancing policy measures.

CBDC issuance could have important impacts on central bank balance sheets, depending on the CBDC conversion modality. If disintermediation materializes, the central bank could lend the funds diverted from commercial bank deposits back to those banks so they can keep on lending (Brunnermeier and Niepelt, 2019). However, this implies a drastic step away from typical central bank mandates, and they would have to decide how to allocate funds across banks, opening the door to political interference. CBDC is least disruptive if issued only against existing physical cash, as it merely results in a switch on the liability side of the central bank balance sheet from cash to CBDC. However, the impact is more ambiguous when CBDC is issued against central bank reserves, which will be the case if users convert from commercial bank deposits. More specifically, to the extent that CBDC are paid for with reserves, the size of the central bank balance sheet will remain unchanged, as reserves and currency are both liabilities, although there will be a shrinkage of commercial bank balance sheets.

Several suggestions have been put forward to control the potential resulting banking sector disintermediation that could result from this balance sheet shrinkage. Panetta (2018) suggests imposing holding limits, but that could limit the number or size of payments, as user CBDC holdings would have to be known in order to finalize the payment. Bindseil (2020) suggests a way around the payment finality issue would be for CBDC users to designate a “waterfall” account to which payments that push holdings over the cap would be automatically transferred. This is the approach adopted in the Central Bank of Bahamas CBDC pilot (CBOB, 2019). Kumhof and Noone (2018) propose a more radical approach that would limit commercial banks’ ability to provide on-demand convertibility of deposits into CBDC.[16]

the CBDC, where an injection of CBDC via the sale of government bonds could, under specific circumstances, lead to lower rates (Barrdear and Kumhof, 2016).

[15] Retail depositors are more stable sources of funding than wholesale depositors (see Huang and Ratnovski 2011; Gertler and others 2016).

[16] Kumhof and Noone (2018) suggest four design features to mitigate potential disintermediation risk and ensure parity between CBDC and bank deposits by (i) paying an adjustable interest rate to modulate demand, (ii) blocking conversions from reserves to CBDC, (iii) removing any guarantees of on-demand convertibility of

Bindseil (2020) argues that it is unnecessary to introduce such far reaching, albeit conditional, changes banking and central banking core principles relating to convertibility.[17] He proposes instead to control the quantity of CBDC through a tiered remuneration system with a relatively attractive rate applied up to some holding ceiling, while a lower interest rate would be applied to amounts beyond the threshold.

A poorly designed CBDC may accelerate bank runs by offering a readily available, safe, and liquid alternative to deposits. However, Mancini-Griffoli and others (2018) argue that the increase in run-risk will depend on whether bank deposits are covered by credible deposit insurance, and the type of crisis. In many jurisdictions, credible deposit insurance should continue to dissuade runs.[18] In addition, safe and relatively liquid assets already exist in many countries, such as government bond funds, or state banks. In cases of individual bank insolvency, running from one bank to another bank is already technically possible with the click of a button in most jurisdictions, so having CBDC is not likely to affect the likelihood of runs in that scenario. However, depending on the design of the CBDC and its ecosystem, including potential convertibility limits, CBDC could increase the risk of generalized runs out of the banking sector. On the other hand, in the event of such a run, CBDC could allow the central bank to offer liquidity faster to distressed commercial banks to avoid the first-come-first-serve dynamics that fuel runs to begin with. Moreover, CBDC is unlikely to increase generalized run risk in a currency or sovereign crisis, because depositors would typically run from all local assets.

CBDC of reserve currency countries available across borders could increase currency substitution (“dollarization”) in countries with high inflation and volatile exchange rates. These prospects need to be studied further, along with implications for the international financial system.

C. The Preconditions for Issuing CBDC

Before even thinking about issuing CBDC, advanced economy central banks are carefully reviewing the legal and institutional preconditions. These would include robust national data privacy protection legislation and regulations, strong central bank cyber resilience and national payment system regulations that comply with pertinent international standards. Another important precondition is having sufficient central bank resources to devote to the decision-making process.

bank deposits into CBDC, and (iv) permitting CBDC issuance only against eligible securities (government securities). However, in addition to the critique of Bindseil (2020), Bjerg (2017) questions whether the principles will actually ensure parity between CBDC and bank deposits.

[17] However, Barrdear and Kumhof (2016) apply a theoretical model to suggest that permitting CBDC issuance only against government securities (one of the four Kumhof and Noone (2018) conditions) could lead to higher economic output. This would result from a fall in interest rates due to a combination of replacing high-interest debt with low-interest CBDC, and lower government debt default risk due to a partial replacement of defaultable debt with non-defaultable CBDC.

[18] According to the International Association of Deposit Insurers, there are 146 countries worldwide with credible deposit insurance in place. (https://www.iadi.org/en/deposit-insurance-systems/dis-worldwide/)

Figure 3 suggests foundational issues that could help determine whether a country's circumstances are appropriate for CBDC issuance. There are no universally applicable best practices or prescribed rules that will guarantee the ultimate success of CBDC issuance, but this maturity assessment could facilitate the decision-making process and also help policymakers identify and address any gaps or deficiencies in their infrastructure, regulatory and supervisory framework, governance and risk management, and central bank legislation. Coordinating with other line ministries and government agencies will ensure that foundational elements outside the central bank purview are given attention.

Issuing CBDC is a complex national project that will involve multiple stakeholders beyond the traditional central bank counterparts (such as the Ministry of Finance). Interest in and impact of the CBDC extends also to the legal framework. For example, depending on the existing legal framework, CBDC might require changes in the governing, accounting and financial reporting standards to recognize the CBDC. It will also affect multiple public agencies, such as financial intelligence units, tax, capital market, and statistical agencies, plus supervisors, consumer protection agencies and private sector stakeholders, including merchants and users. Depending on the local circumstances, the central bank might consider the establishment of a national consultative committee of stakeholders to facilitate communication and engagement with various stakeholders, including via surveys and focus groups. Clear mandates and effective collaboration among stakeholders can help prioritize tasks and maximize resource efficiency (Taylor, 2019).

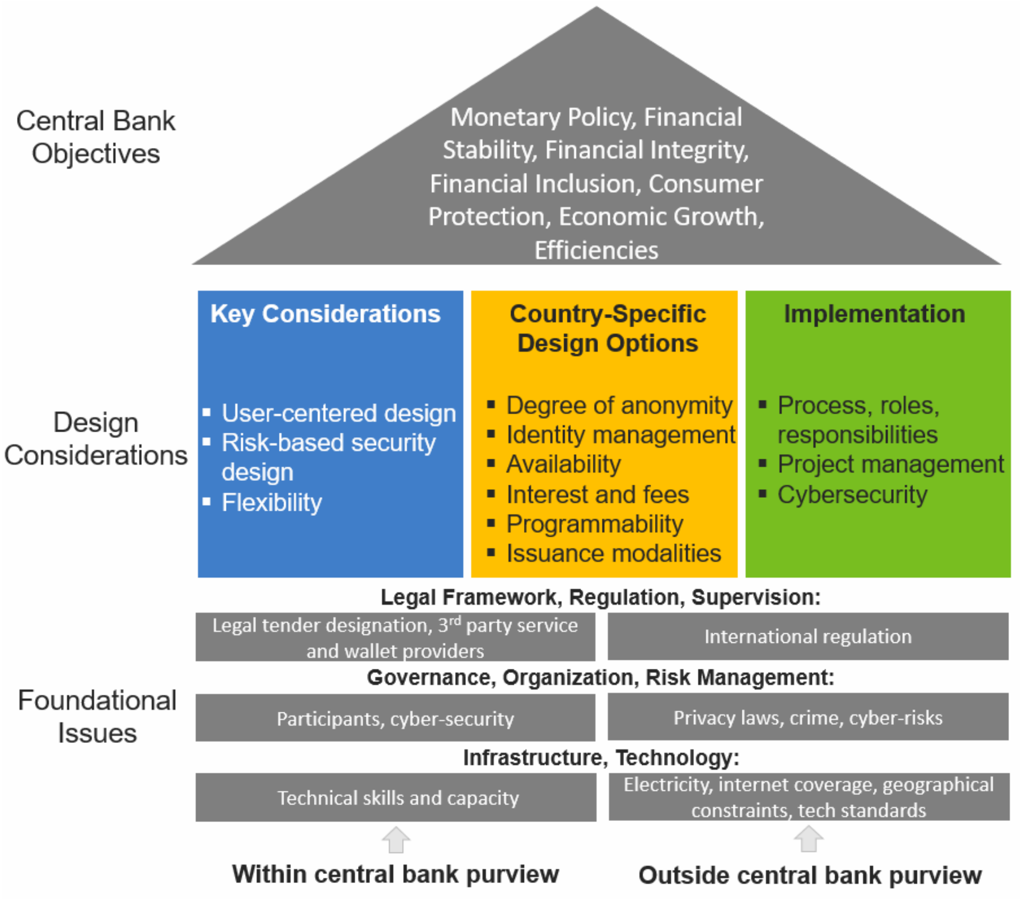
Issuing CBDC requires an adequately developed technological infrastructure. Developing the needed infrastructure to support CBDC includes insuring a high level of availability and resilience of the general infrastructure such as electricity grids, mobile network and internet coverage. Depending on their circumstances, countries may opt for a combination of submarine fiber optic cables, landlines, and satellite connections. Investments in cable and satellite can be balanced based on the need for greater bandwidth in high-density areas and the reliability of satellite in remote areas or as backup in case of outages (George, 2018). In some circumstances, strong motivations to issue CBDC might accelerate a country's infrastructure investment and the digitalization of the financial system.

CBDC issuance is best considered in the broader context of national payment systems development, and driven by needs, objectives, and capacity rather than technology.[19] A payment is the process by which monetary instruments, typically cash and deposit claims, are transferred between two parties (payer, payee) to finalize a transaction. A national payment system is the configuration of diverse institutional arrangements and infrastructures that facilitates the transfer of monetary value between parties. As part of international guidance, the identification of all user needs in the national payments system are critical for guiding development (BIS, 2016). CBDC implementation calls for an analysis of business and resource requirements, and capabilities, which are drawn from stocktaking exercises and

[19] See Brainard (2019) for the case of the United States, which will continue to analyze the potential benefits and costs of CBDC given the demand for physical currency, the role of the U.S. dollar as a reserve currency, the robust banking system that meets the needs for consumers, and the existence of widely available and expanding variety of digital payment options that build on existing institutional framework and applicable safeguards.

stakeholder consultations. The development of skilled and knowledgeable human resources is equally critical to the development of physical infrastructure, including training personnel in developing, operating and managing CBDC arrangements and supporting education programs for users as well as service providers.

Figure 3. Overview of the Main Elements Covered in the Paper


Central Bank Objectives
Monetary Policy, Financial Stability, Financial Integrity, Financial Inclusion, Consumer Protection, Economic Growth, Efficiencies
Design Considerations
Key Considerations
▪ User-centered design
▪ Risk-based security design
▪ Flexibility
Country-Specific Design Options
▪ Degree of anonymity
▪ Identity management
▪ Availability
▪ Interest and fees
▪ Programmability
▪ Issuance modalities
Implementation
▪ Process, roles, responsibilities
▪ Project management
▪ Cybersecurity
Foundational Issues
Legal Framework, Regulation, Supervision:
Legal tender designation, 3rd party service and wallet providers
International regulation
Governance, Organization, Risk Management:
Participants, cyber-security
Privacy laws, crime, cyber-risks
Infrastructure, Technology:
Technical skills and capacity
Electricity, internet coverage, geographical constraints, tech standards
Within central bank purview
Outside central bank purview

Source: Authors.

Launching a CBDC is a multidimensional undertaking that extends beyond the central bank's normal information technology project management frameworks. Issuing a CBDC will require political support, extensive senior management commitment, and focus on detailed product design choices and operational processes. The new currency could lead to major disruptions affecting monetary policy transmission, financial stability, financial sector intermediation, the exchange rate channel, and the operation of the payment system. The issuing central bank will need to consider the existing operating environment and the impact of the CBDC issuance including the degree of public acceptance, use, the nature of financial sector response, and consumer dynamics. The central bank will also have to weigh the availability of in-house capacity against options to outsource selected operations to handle this expanded role.

Since CBDC involves many aspects of central bank operations, the impact of its issuance on central bank internal operations will need to be considered. The real-time nature of CBDC will require adequately skilled resources and quick decision-making structures and response time within the central bank to address urgent issues, ensure business continuity and operational resilience. Even for operations that the central bank outsources, it will need to develop monitoring, oversight and risk management functions, evaluate vendor and third-party risks, and establish systems to respond to potential CBDC disruptions that could result from operational failures, cyber breaches, or mistakes in execution. For the operations that the central bank does not outsource, redundant systems and business continuity will need to be established. It is important to factor in the impact of a 24/7/365 CBDC environment into the cost analysis including its implication for staffing, support for CBDC life cycle, and cyber-security.

A strong commitment to the CBDC by the issuing central bank and government and trust in the currency will be critical for its acceptance. Just like with the issuance of regular physical currency, the central bank and the government will have to show strong commitment and readiness to take the steps needed to ensure that the CBDC is perceived as no less viable and stable than the physical currency by companies and the general public. Public confidence in economic and financial stability, in the value of the digital currency, and the central bank itself is essential. Real or perceived macro-economic or central bank related challenges that might undermine public confidence in the country's currency or the central bank, require a mix of different macro-economic policy measures and adjustments. Given the importance of underlying trust in a currency (analog or digital), policymakers efforts are better spent on trust-building policy measures before considering CBDC issuance.

D. Weighing the Alternatives, Costs and Benefits of CBDC

The ultimate decision as to whether to issue CBDC will come down to weighing the costs and benefits of CBDC issuance against those of the alternatives. Figure 1 proposes a model to assess the feasibility, and to validate initial assumptions. The initial decision-making process starts with understanding thoroughly the problem to be solved and the full array of solutions. Central banks in several countries are working on improving existing payment systems to match the speed and convenience of digital currencies. For example, the U.S. Federal Reserve is developing so-called fast payments, allowing nearly instantaneous and low-cost settlement of inter-bank retail payments (U.S. Federal Board, 2019). In some instances, deploying fast payments would offer enhanced control over essential payment systems without issuing CBDC. In other countries, similar systems have improved payment services and injected competition in payments, especially if paired with other reforms, such as public digital identities, common communication standards, open application programming interfaces (APIs, which allow banking applications to interoperate and to be extended by third-party developers), and data portability and protection standards (Cœuré, 2019). If the objective for considering issuing CBDC is to expand financial inclusion or react to dwindling cash usage, other options could include promoting mobile money, incentivizing private-sector financial institutions to improve their product offerings or changing or instituting relevant legislation to ensure merchants accept cash.

After reviewing all the alternatives and coming to the conclusion that CBDC issuance is a potentially cost-effective and safe of meeting the objectives, weighing CBDC costs and benefits is likely to be iterative (Figure 1).[20] For example, the potential cost savings and financial inclusion benefits could be offset by infrastructure upgrade costs. For countries where cash usage is plummeting, if reducing monopoly distortions is the rationale for exploring CBDC issuance, the absence of robust cyber-security resilience might introduce vulnerabilities with adverse impacts on consumer protection and financial stability. The potential impacts to monetary policy implementation and financial intermediation may also counter the other perceived CBDC benefits. Furthermore, as discussed below, choices of operating model and design features can change the mix of CBDC issuance pros and cons. For example, if the central bank does not have the capacity to directly issue CBDC, sCBDC may be worth considering.

IV. CBDC DESIGN CONSIDERATIONS

Central banks that have made the decision to more seriously explore CBDC issuance are focusing on a common set of key design choices. These include the operating model, the platform (centralized versus decentralized database technology, or token-based), degree of anonymity/privacy, availability/limitations, and whether to pay interest. These design decisions, which will be discussed in more detail below, are driven by country-specific factors and balance the need to achieve the policy objectives that launched the exploration process and be attractive to users and merchants.

CBDC demand will ultimately be shaped by the level and trend in cash usage in a specific country, and incentives for stakeholders, including end-users and merchants. While access to CBDC might become more convenient than withdrawing cash from an automatic teller machines (ATM), it could only make CBDC like a bank debit card (Khiaonarong and Humphrey, 2019). If the CBDC is not interest-bearing, the only incentive to use CBDC is related to convenience of access and ease-of-use compared to cash. Cost-sharing and interoperability arrangements for point-of sale terminals could incentivize merchants to accept CBDC for the purchase of their products or services. Hence, CBDC demand may be weak in countries where cash usage is already very low, due to a preference for cash substitutes (cards, electronic money, mobile phone payments). Where cash usage is high, demand for CBDC could be stronger, due to a lack of cash substitutes.

The design thinking may also have to consider scenarios in which CBDC and other retail digital payment platforms drive cash out of common usage. There may be some people who cannot afford the necessary hardware and those with limited internet connectivity. For example, a survey found that 17 percent of the U.K. population would struggle to cope in a cashless society, comprised mostly of the poor and elderly (Access to Cash Review, 2019). Sweden dealt with this issue by passing legislation that came into effect January 1, 2020 that requires banks to provide adequate cash services, although it does not oblige merchants to

[20] In that iterative process, cost considerations would be balanced against appropriate standards of safety and security. Best practice would also be for the CBDC arrangement to establish mechanisms for the regular review of its efficiency, including its costs and pricing structure. This could include an evaluation of both the productivity of operational processes and the relative benefits of the processing method given the corresponding costs (BIS, 2012).

accept cash (Sveriges Riksbank, 2020). Some of the ways for CBDC design features to accommodate some of these special needs are discussed below.

Central banks that are seriously exploring CBDC are using various techniques to weigh user perspectives into the design process. Optimal user satisfaction and usability can also be achieved through best practices in the product design processes such as user-centered design and user experience analysis. For the Bank of Canada, this has included basing analysis on surveys and focus groups of potential users (Bank of Canada, 2020, Huynh and others, 2020). For example, Huynh and others (2020) and Sun (2020) find that the most important features are low transaction costs, ease-of-use, affordability, and security perceptions, in order of decreasing importance. Involving users (including merchants) throughout the iterative design process promotes highly usable and accessible products that promote adoption, enhance robustness and may instill trust (Interaction Design Foundation, 2019).

According to the BoE (2020), there are a number of attributes that are key to CBDC success. The CBDC system should provide 24/7 payments, including offline under certain conditions, with no planned downtime and be able to recover quickly from operational disruption. It should be able to handle increased volumes if demand for CBDC payments increases significantly. The payment process should complete as quickly as possible, with certainty over completion. Users should be able to make real-time peer-to-peer payments, and the process should be intuitive, involving the minimum number of steps and required level of technical literacy. The CBDC payment system should be designed to minimize barriers to use from disabilities, and hardware or mobile data network access. In addition, users should expect privacy in lawful transactions, and the system should conform with all relevant privacy laws and regulations. The costs of making payments in CBDC should be clear to all users.

More broadly, the design decision-making process starts with a comprehensive review of the financial integrity, cyber-security, and privacy risks. Key issues like mitigation of the financial integrity and cyber-security risks are not after-thoughts. Instead they are drivers of architecture design decisions. The effective implementation of financial integrity measures is important in all cases. This entails ensuring compliance with the Financial Action Task Force (FATF) standard and taking effective action to mitigate money laundering and terrorist financing risks.[21] Some aspects of the financial integrity considerations driving the design of CBDC are mentioned below. Cyber-security across different product layers forms the basis for a reliable and resilient CBDC payment system that is resistant to fraud and cyber-attacks as reviewed in-depth in Section

Incorporating flexibility into the architecture can support future-proofing the CBDC to account for changing user needs, regulations, and technology. A flexible design could reduce costs associated with required re-works or upgrades of the operating model or design features

[21] The FATF is an independent inter-governmental body that develops and promotes policies (the “FATF Recommendations”) to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The IMF Executive Board has endorsed the FATF Recommendations as the international anti-money laundering and countering financing of terrorism (AML/CFT) standard for the purposes of its work.

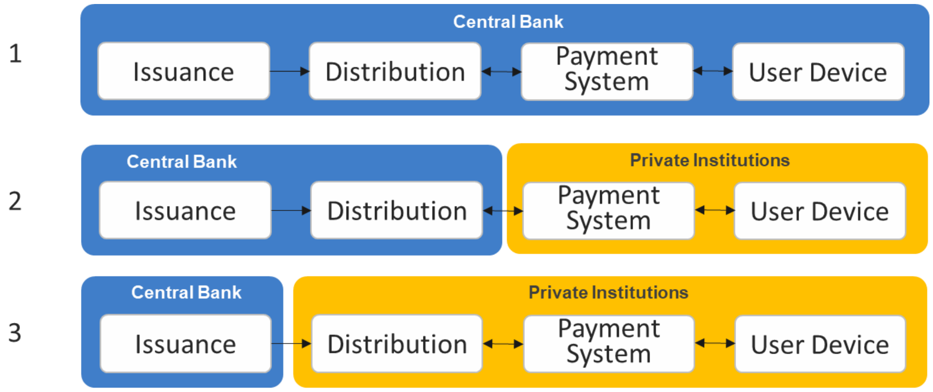
the central bank chooses or needs to adopt. This type of architecture could allow a controlled open architecture enabling third parties, such as payment system providers, to integrate or build their own services on top of the CBDC platform. Such an open architecture could facilitate a competitive market for CBDC-related payment services, although its design should ensure that there are no structural factors that could lead to winner-take-all market dynamics for such provision (BoE, 2020). It would also be useful if such payment systems were interoperable with each other and enable prospective cross-border CBDC payments.[22]

The rest of this section will enumerate the design choices, and finish with some thoughts on project management and business partner selection.

A. CBDC Operating Model[23]

Central banks can adopt a tiered approach to the CBDC operational model (Figure 4). In broad terms, in a single-tier model the central bank would perform all the tasks involved, from issuing the CBDC to running user wallets (Figure 4, Panel 1). In a multi-tier model, the central bank issues and redeems CBDC, but distribution and payment services would be delegated to the private sector (Panels 2 and 3). The operating model serves as a conceptual framework, the ultimate decision as to which model to adopt in practice will depend on country-specific circumstances. These might be related to the breadth and depth of its financial sector, the robustness of its financial integrity, financial market infrastructure standards and supervision, and resource and capacity constraints.

Figure 4. Central Banks can Adopt Different Degrees of Responsibilities



Source: Roberto Giori Company.

In a single-tier model, a CBDC transaction would resemble transactions with commercial banks, except accounts would be held with the central bank. A payer would log in to an account at the central bank—for example, through a web or mobile application—and request

[22] An in-depth study of interoperability is outside the scope of this paper. However, at the architecture level, examples of interoperability work include (i) maximizing ability for cross-chain transfer in the case of a DLT infrastructure ("atomic swap"); (ii) adopting a common data standard such as ISO20022 to facilitate cross-systems payment; (iii) allowing cross-wallet transfer of value between different wallet providers.

[23] See also Dyson and Hodgson (2017), Kumhof and Noone (2018) and Meaning and others (2018)

a transfer of funds to a recipient’s account, also at the central bank. The central bank would ensure settlement by updating a master ledger, but only after verification of the payer’s authority to use the account, enough funds, and authenticity of the payee’s account. This mode gives central banks more control over the product design and implementation process. However, the central bank would need to assume a more active role in distribution and payment services, which may exceed the scope of its core mandate and capacity to manage the entire process. Moreover, central banks would directly compete with existing digital payment service providers aggravating disintermediation concerns. Conceptually, the single-tier model may be appropriate for a country with a well-resourced central bank in which the financial sector is extremely underdeveloped, so that there are no institutions to assume distribution and provision of payment services, as is the case in some low-income countries and small island states in the Pacific.

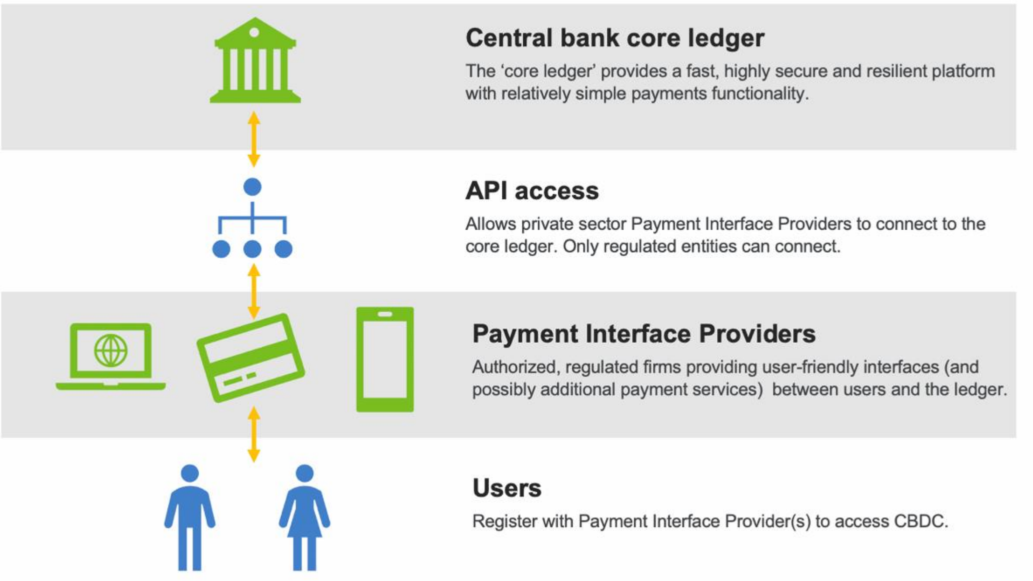
In a multi-tier or “platform” operating model the central bank issues the CBDC but outsources some or all the work of administering the accounts and payment services (Figure 5). However, CBDC remains the liability of the central bank and thus CBDC holders would not be exposed to default risk of the engaged payment service providers (PSPs). Auer and Böhme (2020) suggest that this risk can be mitigated by a legal framework that keeps user CBDC holdings segregated from PSP balance sheets so that the holdings are not considered part of a failed PSP’s estate available to creditors. They also suggest that the legal framework should also give the central bank the power to switch user accounts in bulk from a failed PSP to a functional one. They also point out that, in order to do this expeditiously, the central bank would have to retain a copy of all retail CBDC holdings.

The multi-tier model is less disruptive than the single-tier one as financial institutions play their traditional roles in distribution and payment services (Panels 2 and 3 of Figure 4). In addition, this layered approach facilitates the integration of new types of consumer electronic devices without the need to alter the core of the system, and it supports the ability for third parties to build on top of the core (Shah and others, 2020). So far, this has been the favored model in central bank CBDC pilots and ruminations. For example, the People’s Bank of China (PBOC) is proposing and piloting a “two-tier” model in which the central bank distributes CBDC to selected banks or payment platforms (distribution layer), who distribute CBDC to users through their payment system layers. (Fan, 2020).

Sun (2020) identifies the preconditions that could contribute to multi-tier CBDC model success based on an in-depth examination of Alipay’s experience. First, the ecosystem should create economic incentives for PSPs, whether they be commercial banks or fintech firms, to participate in ways that serve central bank interests (making the CBDC broadly available to the public, across regions, etc.). There should be a cost-effective business model for such PSPs with enough revenues from interest spreads, fees, and cross-subsidization, as well as controllable fixed and variable costs. Also, regulations should leave room for enough users to reach critical mass and incentivize network buildup while promoting PSP market competition. For example, regulations that encourage interoperability of competing payment systems to encourage new entrants and reduce concentration risk should take care not to adversely impact network build-up.[24]

An approach not included in Figure 4 is for the central bank to allow stablecoin issuers and/or private-sector PSPs access to their reserve accounts (Kumhof and Noone, 2018, Adrian and Mancini-Griffoli, 2019a).[25] Such stablecoin issuers and PSPs would have accounts at the central bank and cross-provider payments would be settled on the central bank's books. An sCBDC license would establish the conditions to widen access to central bank reserves. Such access would be given only under strict conditions and within the central bank's mandate, and appropriate regulations would protect reserve accounts in which the collateral is kept safe from issuer or other creditor bankruptcy. See Box 1 for a discussion of the pros and cons of sCBDC.

Figure 5. CBDC Platform Model


Central bank core ledger
The 'core ledger' provides a fast, highly secure and resilient platform with relatively simple payments functionality.
API access
Allows private sector Payment Interface Providers to connect to the core ledger. Only regulated entities can connect.
Payment Interface Providers
Authorized, regulated firms providing user-friendly interfaces (and possibly additional payment services) between users and the ledger.
Users
Register with Payment Interface Provider(s) to access CBDC.

Source: BoE, 2020[26]

[24] For a new PSP, interoperability across PSPs could diminish the incentive of a startup to innovate since it could lower the value of a privately developed network. It could also restrict competition by excluding certain technical innovations or restricting new business models and reduce the value and increase the costs to PSPs. In addition, interoperability might increase overall risks if an innovative service provider has a higher risk profile.

[25] The concept is not completely new. Some central banks, such as the Hong Kong Monetary Authority, and the Swiss National Bank already offer special purpose licenses that allow nonbank fintech firms to hold reserve balances, subject to an approval process. The Bank of England is discussing such prospects. The Peoples Bank of China requires the country's large payment providers, Alipay and WeChat Pay, to hold client funds at the central bank in the form of reserves.

[26] "In the 'platform' model, the [central bank] would provide a fast, highly secure and resilient technology infrastructure, which would sit alongside the [central bank's] RTGS service and provide the minimum necessary functionality for CBDC payments. This could serve as the platform to which private sector payment interface providers would connect in order to provide customer facing CBDC payment services. Payment interface providers could also build 'overlay services' — additional functionality that is not part of the [central bank's] core infrastructure, but which might be provided as a value-added service for some or all of their users. As well as providing more advanced functionality, these services might meet future payment needs by enabling

The choice of business model will also have important regulatory implications. In a one-tier ecosystem, the central bank alone would need to conform to any existing oversight and regulatory norms. In a multi-tier ecosystem, it would seem to be important that the engaged third parties are subjected to robust regulatory oversight and supervision, to protect customers and avoid risks to financial stability. Some aspects of these might bear some similarities to what crypto-asset and stablecoin operators, and custodians are subjected to. These would include market conduct, especially with respect to the entities that engage directly with customers. The detailed aspects of CBDC ecosystem regulation and supervision are discussed in more detail in Section V.

In the case of sCBDC central banks could establish clear conditions to grant licenses to sCBDC issuers. This would include strict supervision and oversight by the central bank or other authority. For instance, selected providers would be responsible for appropriate customer screening, transaction monitoring and reporting in accordance with know-your-customer and anti-money-laundering regulation, as well as security of wallets and customer data. Control over who can receive and hold sCBDC may also prove helpful to limit its spread beyond a country's borders, for instance.

B. Centralized Versus Decentralized Authority[27]

Most current CBDC experiments focus on centralized authority architectures. However, decentralized or hybrid architectures, or even ledger-less offline peer-to-peer stored value platforms are possible. In the digital asset world, "decentralization" usually refers to the decentralization of authority to verify and commit transactions to the ledger. In a traditional centralized ledger (client-server model with no distributed components) transaction processing would entail the payor connecting to the central ledger keeper and initiating a funds transfer to the recipient's account. The ledger would be updated after the payor has been confirmed as the account holder who has enough funds to carry out the transaction. In a partially-decentralized authority model, the central bank could issue tokens to selected financial institutions that act either to safeguard funds or act as intermediaries. Intermediaries that are banks or licensed deposit-taking institutions would have additional flexibility, due to the fractional reserve system, as they are not expected to deliver the exact number of tokens as deposited by payors.

Alternatively, the ledger could be run on a distributed ledger technology (DLT) platform, in which the ledger is replicated and shared across several participants (U.K., 2016). With a DLT platform the central bank could have a centralized, decentralized or partially-decentralized authority for verifying and/or committing transactions. The best-known public

programmable money, smart contracts and micropayments. Payment interface providers would be subject to appropriate regulation and supervision in line with any risks they might pose." (BoE, 2020)

[27] The terminology used here deviates from the "account-" versus "token-based" based payment systems taxonomy introduced by Khan and Roberds (2009). This is to more clearly distinguish this level of classification from the technology used and skirt the debate over whether DLT-based platforms should be labeled as account- or token-based (Milne, 2020, Shah and others, 2020).

and decentralized DLT implementation is the technology underlying Bitcoin (Nakamoto, 2008). DLT platforms can be "public" (accessible by anyone) or restricted to a group of selected participants ("consortium" or "private"). Ledger integrity can be managed by a selected group of users ("permissioned") or by all network participants ("permissionless") (See Annex 2 for details on DLT).

Box 1. Synthetic Central Bank Digital Currency[28]

sCBDC differs from other forms of money in two basic ways. First, it is a liability of private firms—the sCBDC issuers—rather than of the central bank. Second, sCBDC is backed with central bank reserves, and thus differs from privately issued digital currencies such as e-money, stablecoins, or crypto-assets that are not backed by any asset.[29] sCBDC thus requires central banks to widen access to their reserves to non-bank financial firms, BigTechs, and fintech startups.

The reserve backing allows sCBDC providers to offer a credible guarantee of redemption at face value. A similar guarantee is offered by e-money providers and banks relative to deposits. However, in both cases, the guarantee is not necessarily credible depending on the assets in which customer funds are invested and—for banks—the existence of deposit insurance and access to central bank liquidity.

Central banks could establish clear conditions to grant licenses to e-money providers, including strict supervision and oversight by the central bank or other authorities, though according to lighter regulation with respect to banks engaged in maturity transformation. For instance, selected providers would be responsible for appropriate customer screening, transaction monitoring and reporting in accordance with financial integrity regulation, as well as security of wallets and customer data.

For central banks, an advantage of sCBDC, over directly issued and managed CBDC, is that it is cheaper and less risky. It also fully preserves the comparative advantage of the private sector to innovate and interact with customers, and of the central bank to provide trust and efficiency. However, there is a risk that the public sees sCBDC as a central bank-branded product and does not fully understand the central bank's limited responsibility for it. However, as is true for commercial banks today, fraud or technical glitches related to a person's debit card, for instance, are not blamed on the central bank, even though commercial banks have access to its reserves.

Permissioned DLT-based platforms appear to be better suited for retail CBDC due to governance and oversight considerations. Thus far, DLT-based CBDC experiments have focused on private permissioned (centralized authority) platforms as these allow for control over platform participants and their access to the platform, and role-based oversight and visibility of transactions. Private permissioned platforms also ensure that the central bank retains full control over money issuance and monetary policy. Permissionless platforms (with decentralized authority), on the other hand, fall short on scalability, and settlement finality,

[28] For more detail on sCBDC concepts and considerations see Adrian and Mancini-Griffoli (2019a).

[29] The term "e-money" is also used in recent legislation (Adrian and Mancini-Griffoli, 2019). Singapore's 2019 Payment Services Act emphasizes that "e-money" is denominated in currency, "pegged" to a currency, and is intended to serve as a "medium of exchange." The European Commission's 2009 Directive on electronic money defines e-money in a somewhat more general way, referring to "a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions." According to this definition, even pre-paid cards (which were originally associated with e-money) must be redeemable.

and financial integrity risk management.[30] Box 2 summarizes some of the reasons why some central banks are considering DLT-based CBDC platforms.

The Committee on Payments and Market Infrastructures (CPMI) DLT analytical framework outlines key considerations for using such arrangements (BIS, 2017).[31] These include processing speed, processing costs, reconciliation speed and transparency, credit and liquidity management costs, and potential smart contract applications. Safety issues include operational and cybersecurity risks, data management and protection, and governance will require more attention since the usage of a DLT-based CBDC will possibly expose more of the system due to the distributed nature of the DLT architecture.

An offline peer-to-peer stored value CBDC platform would take the form of a card or a mobile wallet app on which prepaid values are stored locally. Such a CBDC platform could be of interest for countries where large population segments are excluded from the formal financial sector or internet access. However, attempts to implement such systems during the 1990s via rechargeable smart cards like MintChip, Mondex and VisaCash failed to develop enough customer acceptance to become viable (Matonis, 2012; Bátiz-Lazo and Moretta, 2016). Also, at the time, computer scientists argued that such smartcards could never be strong enough to support existing currency schemes (Stalder, 2002). However, rapid technological progress since then is likely to have addressed some of these security concerns, such as the complex offline capable dynamic data authentication/combined dynamic data authentication security features for stored value cards (Secure Technology Alliance, 2014).

C. Financial Integrity, Privacy and Transparency

FATF has issued a set of standards that countries should implement on a risk basis to prevent money laundering and terrorist financing that will impact CBDC design considerations. These include requirements on financial institutions, virtual asset service providers and designated non-financial businesses and professions to implement customer due diligence measures, monitor transactions and report suspicious transactions, amongst other obligations. In most instances, this means that some information on CBDC users would likely need to be collected, transmitted and, when necessary, made available to competent authorities. Some form of proportionality would likely be applied as well for instance in cases where the risk of money laundering and terrorist financing is low, such as in occasional, low value transactions.

Further guidance on the balance between digital developments and financial system integrity is to be expected. On November 4, 2019, the FATF published its draft guidance on digital identity (FATF, 2019). The document seeks input from the financial sector and other stakeholders on the FATF's guidance on determining "how digital ID systems can be used to conduct certain elements of customer due diligence (CDD) under FATF Recommendation 10." The FATF stresses that "the growth in digital financial transactions requires a better

[30] For example, Xiao (2019) show that all proof-of-work and chain-based proof-of-stake consensus protocols can only ensure probabilistic finality.

[31] The CPMI, previously the Committee on Payment and Settlement Systems, was renamed in June 2014.

understanding of how individuals are being identified and verified in the world of digital financial services."

Box 2. DLT-Basked vs Traditional Centralized Ledger Approaches

A key CBDC platform implementation decision is whether to run it on a decentralized (DLT) platform, rather than on a traditional centralized database. Central banks are still debating the advantages and disadvantages of each approach, assessing parameters such as security, resilience, performance or long-term tokenization strategy.

Centralized vs decentralized authority: The key question for central banks considering DLT-based CBDC, is whether the purported benefits of partially- or fully decentralizing the authority to adjust claims on their balance sheets outweigh the risks. These risks are discussed below, along with some of the ways that they can be mitigated. However, DLT-based ledger keeping was developed mainly to overcome a lack of trust in a central authority, so there may be a tension between the idea of DLT-based CBDC and some of the central tenets of central banking and central bank money.

Security: Most central banks already have a mature security posture to manage centralized databases. Their internal systems are typically secured via multiple protection layers, such as audits, middle-tier services, authentication/authorization and firewalls.[32] CBDC projects would open up these centralized databases, which brings new security concerns. DLT-based platforms keep multiple copies of databases across a number of participants or "nodes" which makes it more difficult for malicious attempts to alter the data. Most central banks considering issuing DLT-based CBDC are opting for "permissioned" platform, which limit the ability to update databases to themselves and selected financial institutions.

Resilience: Neither centralized platforms nor DLT-based CBDC offer complete resilience. Both face cybersecurity risks, hardware issues, power or network outages or cloud service interruptions. The DLT architecture may offer enhanced resiliency by reducing single points of failure. Furthermore, potential data loss at one node can be recovered through replication of the ledger from other nodes when it comes back online. Despite their resilience, DLT-based platforms may experience attacks against the network or applications layer which includes the consensus mechanism by which database updates are approved (Auer and Böhme, 2020).

Performance: Centralized platforms usually process transactions more quickly. For reference, the VISA network can theoretically handle up to 65,000 transactions per second (TPS), while private DLT platforms are slower at around 20 TPS.[33] Rapid technological progress is expected to address this issue with networks provided by new entrants achieving up to 10,000 TPS (Mearian, 2019).

Tokenization in this context involves the recording of assets, properties, rights or currencies on a DLT platform. Financial ecosystems are expected to use asset tokenization to facilitate delivery versus payment (Accenture, 2019). It may be complicated to implement digital assets, with properties such as double-spending prevention or immutability, on "legacy" centralized systems without essentially recreating the equivalent of a DLT architecture.

Central banks have been exploring different options to strike the right balance between financial integrity, privacy and transparency requirements in their CBDC design thinking. Financial integrity could be maintained if strict limits are placed on the size of anonymous CBDC transactions and holdings. The European Central Bank (ECB) tested out "anonymity

[32] Middle-tier services are comprised of the processing that takes place in an application server that sits between the user's machine and the database server. A firewall allows or blocks traffic into and out of a network.

[33] Based on the South African Reserve Bank tests several of the most popular private blockchain platforms (SARB, 2018).

vouchers" in a Proof of Concept (PoC). These vouchers allow users to anonymously transfer a limited amount of CBDC over a defined period whereby a user's identity and transaction history cannot be seen by the central bank or intermediaries other than those chosen by the user. The enforcement of limits on anonymous electronic transactions is automated, and additional checks are delegated to a financial integrity authority (ECB, 2019). China's Digital Currency Electronic Payment (DCEP) platform is expected to include "controllable or voluntary anonymity" in its design. Although the PBOC will be privy to the identity of its users as they are required to provide their real identities when they first sign up to preempt tax evasion and money laundering, users will have the ability to control what information they expose to counterparties that they are dealing with (Qian, 2018). Complete third-party anonymity would jeopardize financial integrity, so the PBOC's proposed solution aims to keep the degree of anonymity within a controllable range by requiring the disclosure of transaction data only to the central bank (Fan, 2020). Some stablecoin solutions, which could be applied to CBDC as well, require compliance with Know-Your-Customer (KYC) requirements notably at the point when coins are exchanged for bank account holdings or vice versa. Intermediate users in peer-to-peer transactions of CBDC, on the other hand, would not need to be identified (Lewis, 2019). However, in the case of a successful CBDC implementation, the frequency of exchanges would be low as most transactions are expected to be peer-to-peer. DLT-based CBDC could include other privacy enhancing capabilities such rotating public keys, zero-knowledge proof and enclave computing (ECB, 2019).

Whatever design is chosen, an important consideration is how to accommodate the implementation of effective financial integrity measures. Allowing some level of anonymity in the CBDC design would foster usability, provide a more ubiquitous access to CBDC, and assuage data privacy concerns. However, true anonymity for any digital form of money will be very difficult to achieve and most of the existing CBDC solutions could be regarded "pseudo-anonymous" at best. Even when no identification is required at registration, such is the case for ECB anonymity vouchers, transactional metadata can be used to devise user identities based on knowledge graphs. Ensuring adequate data privacy protection and compliance with financial integrity standards is a delicate political decision that involves a collaborative approach by legislators, regulators as well as policy and decision-makers across different line ministries.

There are trade-offs between satisfying legitimate user preferences for privacy and mitigating risks to financial integrity for policymakers. A fully transparent CBDC, where information on its users and all their transactions is accessible by relevant authorities, has oversight benefits (as it would likely facilitate detection, supervision, monitoring and law enforcement efforts), but could be less appealing to legitimate users as an alternative to the anonymity of cash. CBDC that are subject to full identity authentication might disadvantage citizens without access to identification, which could impair financial inclusion efforts. The complete lack of anonymity in financial transactions could potentially infringe on the right to be forgotten stipulated in legislation such as the European Union General Data Protection Regulation (GDPR). Moreover, it could aggravate privacy advocates' concerns of digital surveillance and CBDC being used to carry out sanctioning measures against citizens, especially in cases of already low trust in public institutions. Conversely, a CBDC that is fully opaque regarding transactions and users could infringe on financial system integrity and consumer protection, introducing significant money laundering and terrorist financing risks, as illicit transactions and fraud would go undetected. This risk would likely be greater than in the case of cash, notably due to the ease and speed with which transactions can be performed and their potential global reach.

The current financial privacy debate spans across those in favor of full anonymity to safeguard citizens' rights to privacy and those in favor of fully transparent financial transactions and stringent identification requirements. Reasons for anonymity include reducing the risk of identity theft and spamming, and of being stalked or robbed (Kahn and others, 2005). A low-cost privacy-preserving method of payment could also reduce the impact of negative externalities involved with sharing payments data as data revealed by one person can be used to make interference about the purchasing habits of others (Garratt and others, 2019). Bech and Garratt (2017) specify two types of financial anonymity – counterparty and third-party anonymity. Counterparty anonymity means that a payor initiating a payment need not reveal their identity to the recipient. The more stringent third-party anonymity means that the payor is invisible to all other parties, including the entity that is running the payment system. Some argue that, because third-party anonymity facilitates criminal activity, terrorist financing or money laundering, it should not be allowed (Bech and Garratt, 2017). However, some users may regard a lack of third-party anonymity as revealing too much information about users' private activities (Chaum, 1983), while other studies cast doubt on how highly consumers value anonymity (Bech and Garratt, 2017).

D. Availability and Limitations

Recent CBDC pilots have imposed limits on holdings and transaction sizes, on the need to make the currency as cash-like as possible and reduce disintermediation risk. For example, The Bahamas "Sand Dollar" pilot imposes holding limits "so that it does not operate in practice as a substitute for traditional banking deposits" (CBOB, 2019). Also, in order to enable higher-value transactions, Sand Dollar wallets must be linked to domestic financial institution deposit accounts into which excess holdings have to be deposited, as suggested by the Bindseil (2020) "waterfall" concept discussed above. BoE (2020) points out that if users can hold multiple CBDC accounts with multiple payment service providers, there would need to consolidate user holdings to enforce limits. To achieve its goal of financial inclusion and serving the unbanked, the Sand Dollar pilot allows individuals to have wallets without the need for a bank account, but with less functional capabilities. BoE (2002) also suggests that limits could change over time based on observed CBDC demand and its determinants.[34]

Some central banks are looking at introducing CBDC with offline capabilities to provide the same 24/7 availability as cash. This would be useful when temporary electricity or infrastructure outages occur, or to cover areas without network access. Offline capabilities are important considerations as any digital system, including digital currencies, are

[34] For more on the challenges of limit setting, including avoiding breakdowns in parity between different forms of money, see Subsection III.B.

potentially exposed to outages or catastrophic events.[35] Such designs include rechargeable cards, quick response (QR) code based prepaid cards and smart chip enabled banknotes.[36] Sveriges Riksbank (2018) suggests that a centralized ledger-based CBDC could offer offline functionality with a "regulatory framework that defines how the risks are divided between different agents, how many payments can be made offline and in what amount." If physical cash has not been terminated with the introduction of CBDC, that can always be a fallback, although producing and distributing cash could be equally challenging in the wake of the kind of crises being discussed here. Plus, in the world of mobile payment usage that CBDC will promote, people may no longer be holding cash. However, some of the ideas discussed above may also alleviate the problems of those who cannot afford the necessary hardware or with limited internet connectivity, such as prepaid and rechargeable cards.

Another key design question is whether the CBDC is freely convertible for other forms of central bank money and bank deposits. The aim of this convertibility restriction is to limit potential banking sector disintermediation risk and ensure parity between CBDC and bank deposits (see above). However, on-demand convertibility is likely to be a key user demand criterion, and restricting it violates core central banking principles (Bindseil, 2020).[37] Plus there are other less intrusive ways of mitigating disintermediation risk, such as the holding limits and/or tiered renumeration (see above).

There are special cases where the CBDC may have to be accessible by foreigners. Foreign holdings could be blocked by limiting wallet holders to residents, and this could be enforced with strong KYC requirements. However, it may be necessary to allow foreign tourists access to the CBDC so they can make payments to counterparties that do not accept physical cash or credit/debit cards. Sveriges Riksbank (2018) floats the idea of providing tourists with special wallets with limitations on holdings and/or top-ups that conform to the minimum requirements of the country's financial integrity legislation. Bindseil (2020) suggests that offline stored value cards could be enough.

However, allowing CBDC to be used across borders opens complications that are beyond the scope of this paper. Would access to a reserve currency CBDC facilitate currency substitution in countries that have weak institutions and currencies? And to what extent might safe-haven flows be encouraged, potentially draining resources from countries that face banking, sovereign, or currency crises? Finally, if CBDC were used for cross-border transactions, how might central banks be required to cooperate? Would they absorb some of the functions of correspondent banks and thus take on additional liquidity, credit, and foreign

[35] A recurrence of the 1859 Carrington Event could knock out communications and power for up to a year, and potentially render any digital systems unusable (Lovett, 2011).

[36] For example, a "smart banknote" that combines blockchain with smart chip and near-field communication (NFC) technology could be used just like cash (Stewart, 2018). The smart banknote could have a tamper proof chip securing a private key, the balance could be verified by any NFC enabled smartphone, settlement could be instantaneous, and anonymity could be preserved.

[37] A survey of about 1,200 participants during an April 7, 2020 Bank of England CBDC webinar (see https://youtu.be/EM7NB1_NtC4) found that 35 percent believed that convertibility was the most important design choice influencing CBDC demand, versus access restrictions (32 percent), renumeration (25 percent) and limits (8 percent).

exchange rate risk, or might tokens be created for cross-border payments among particular central banks, commercial banks, or firms? These are deep and difficult questions with far-reaching implications that deserve further research.

E. Interest and Transaction Fees

Interest payments on CBDC could be used to modulate demand (see above). Also, an interest-bearing CBDC would eliminate the effective lower bound on interest-rate policy, but only with constraints on cash availability. However, paying interest would have an adverse impact on the anonymity due to tax reporting requirements and bring operational challenges related to interest calculation. It may be straightforward in ledger-based systems where transaction times and interest rates are known, but they may not always be readily available if offline peer-to-peer transactions are permitted, which would be the case with offline stored value devices (Shah and others, 2020).

Shah and others (2020) suggest several solutions for dealing with these interest calculation challenges. The time of the transaction could be determined according to the user devices onboard clocks, updating the interest rate when the device is connected to the network, although this may not work for stored value devices that only connect when they are being topped up. Another is to cap the allowable amount on the device under which interest is not calculated or require occasional connection to the network.

Transaction fees may also be needed to make CBDC cost-effective for payment service providers (PSPs). They could be fixed amounts, percentage or volume based and could vary depending on types of transactions or tiered by transaction volumes. For example, business-to-business (B2B) and person-to-business (P2B) transactions might draw higher fees than person-to-person (P2P) transactions. In the National Bank of Ukraine (2019) pilot project, P2P transactions were free of charge, but PSPs were able to charge up to one percent of the transaction amount on P2B and B2B transactions, which is slightly less than what is charged on other digital payment instruments and payment cards. Also, eliminating interchange fees on CBDC transactions, along with a reduction/ elimination in the cost of handling cash, would incentivize some retailers to encourage consumers to adopt and use CBDC as a more convenient payment instrument, assuming the foregone fees are not passed on to users.[38] However, using tax revenues to finance central bank competition with private banks could raise political issues in some countries. Also, transaction fees could mitigate the risk of denial-of-service attacks shutting down the system (Eyers, 2019).[39]

Even if there are no immediate needs for an interest or transaction fee bearing CBDC, adding such capabilities might be a prudent part of contingency plans and design flexibility. As the implications of CBDC mass adoption are still untested, including the capability will provide

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

[39] Denial of Service (DoS) attacks are designed to overload application programming interfaces (APIs) with a massive number of requests until the service stops responding.

tools for the central bank to utilize in cases of unintended consequences and CBDC behaviors that are negatively impacting intermediation. Sweden's eKrona thinking includes a built-in ability to pay interest if the central bank ever opted to introduce this feature.[40]

CBDC costs and fees would also need to be considered relative to central bank policy approaches. If CBDC substituted for physical currency, the expense of printing currency, maintaining its fitness, building vaults and storage depots, and distributing cash would be markedly reduced. Nevertheless, there would also be costs that need to be recovered through fees.[41] Such cost considerations are relevant for CBDC services. For example, central bank spending on the operation of inter-bank funds transfer systems could be significant in some countries and need to be recovered through appropriate pricing policies. Although policy approaches could vary from adopting a minimalist, competitive or public service focus, subsidization that distorts incentives and misallocates resources is best avoided (Khiaonarong, 2003).

F. Smart Contracts and Programmability

A smart contract encodes the terms of a traditional contract into a computer program and executes them automatically (BoE, 2020, and Box 3 in He and others, 2017). Smart contracts can be coded on top of any technology stack and range from simple to highly complex executable commands. These commands can relate to an automatic transfer of value or any other conditional function that the protocol allows. On a DLT-based platform smart contracts can in principle be self-executing and self-enforcing, without the need for intermediaries. BoE (2020) runs through several potential applications of this functionality, including paying sales taxes directly to tax authorities at point of sale, and integration with physical devices or Internet-of-Things (IoT) applications.[42] Also smart contracts could be used to automate the distribution of economic relief based on specific demographic or other characteristics. Another possibility, with the appropriate device management controls, could be to leverage smart contracts to ensure that wallets or point-of-sale devices are using the most up-to-date versions of the software, by blocking or limiting transaction or holding amounts until they are updated. However, smart contracts introduce new risks. Fan (2020) suggests that smart contracts could undermine the CBDC's legal tender status, and, in the worst case, reduce the CBDC to a form of negotiable security that may affect its free usability. Also, smart contracts

[40] Agur and others (2019) argues that making CBDC interest-bearing would avoid the welfare losses that might be created by non-interest bearing CBDCs. An interest-bearing CBDC that closely competes with deposits depresses bank credit and output, while a cash-like CBDC may lead to the disappearance of cash. The paper finds that the optimal CBDC design trades off bank intermediation against the social value of maintaining diverse payment instruments. When network effects matter, an interest-bearing CBDC alleviates the central bank's tradeoff.

[41] For illustration, the U.S. Federal Reserve Board currency budget for 2019 was $955 million. This covered currency printing by the Bureau of Engraving and Printing, maintaining currency fitness, vault costs, protection, plus some transportation by Federal Reserve Banks, along with counterfeit deterrence. U.S. Federal Reserve Financial Service fees help recover the associate costs. The FedCash Services fee schedule, for example, includes uniform cash access policy for order and deposits and currency recirculation charges to depository institutions.

[42] Embedded smart contracts might also be useful in implementing other monetary policy rules, such as the Taylor Rule (Constâncio, 2017).

could compromise user privacy, slow down the velocity of currency circulation, hamper monetary policy transmission and execution of macro-prudential policy (Fan, 2020).

BoE (2020) discusses three broad approaches to implementing smart contracting in a CBDC payment system. The first involves building programmable money functionality on the core ledger. The paper opines that this may be necessary to realize the full extent of the benefits associated with programmable money, although it could undermine the ledger's overall performance and scalability. The second approach is to run the smart contracts on a module separate from the core ledger that would process the code and instruct the core ledger when an action is needed would solve the performance problem. This would require careful consideration around such aspects as the process for user authentication and control of this extra functionality. The third option involves restricting smart contract functionality on the core to the minimum necessary to enable payment service providers to provide a more complete range of programmable functionality to users, with the central bank setting standards for security and smart contract interoperability between providers.

G. Technology Selection and Project Management

Applying selection and procurement best practices will ensure the adequacy and robustness of a technological solution. Large technology projects with high impact and long-term consequences are typically managed by outside consultants, often selected through a request for proposal (RFP) to ensure stringent project management principles. Another RFP may be issued to identify best-suited technology service partners. Selection criteria may include, but are not limited to, previous experience, size and financial strength of the company, cybersecurity expertise, the network of implementation and support partners. If the central bank is unsure about the adequacy of a company's technological solutions, it may decide to evaluate those solutions first through a series of proof of concepts (PoCs) against the central bank's design, risks and adoption criteria.[43]

Prior to full-blown implementation, conducting pilots to test public acceptance, impacts and use cases is a key success factor of CBDC projects. After having selected a technological solution and vendor companies, central banks typically explore how a CBDC might work in real life through a pilot program. Exploring the effects of CBDC in a controlled environment could help the central bank to explore CBDC use cases, and to test public acceptance and impact, based on data and knowledge acquired during pilot. Instead of testing out all CBDC functions and design features in one single pilot program, they could be separated into multiple distinct programs. For example, one pilot could test cybersecurity resilience, while others could check financial integrity and financial stability implications. Determining success criteria, key performance indicators and expected outcomes could help central banks

[43] The central bank's risk management, legal, procurement and communication teams may be engaged upfront to help safeguard against reputational risks. Regardless of the project stage, the central bank may decide to sign non-disclosure agreements (NDA), as any technical and non-technical partner may knowingly or unknowingly put the central bank in a defensive position. The central bank could maintain control of communication by being the sole party authorized to communicate on progress of the project.

understand whether the design of the experiment itself or the outcomes themselves need re-alignment. The pilots can also help inform true implementation and maintenance costs. Laying out a data collection framework before the experiment with clearly defined target variables and frequency, will help the central bank evaluate the achievement of the policy outcomes.[44] Independent analysis and evaluation by third parties could be considered to obtain unbiased analysis.

Central banks may benefit from introducing and testing contingency and business continuity plans that would support the pilot in case of serious operational disruptions, instances of financial system instability or inadequacy to meet regulatory requirements. To improve crisis response time and help reduce uncertainty, the central bank could consider running crisis scenario planning and developing crisis playbooks, specifically involving CBDC. This will add flexibility to central bank response in dealing with expected and unexpected scenarios such as technical glitches, cyber breaches, misuses, and possible infringements of financial integrity standards. Also, running a CBDC crisis scenario will sensitize central bank staff to emerging risks that may reduce response time to address such risks.

Full implementation of the project could benefit from an agile, iterative approach. The key benefits of this method are the ability to address gaps and deficiencies as they arise, and to rapidly test assumptions and react accordingly. The project team, or project management partners could apply agile and design thinking methodologies, allowing the development of the CBDC in an incremental and iterative approach with the participation and feedback of representative key project stakeholders, including the end-users (Naybour, 2015). Including the end-user in CBDC development fosters usability, which will help promote user adoption and build trust. Maximizing user adoption is critical for the success of any CBDC, particularly to foster financial inclusion and to build trust in countries with low confidence in public institutions.

In addition to a user-centric approach, CBDC issuance calls for a well-designed public education campaign, change management plan, and communication strategy. Ideally, the public outreach effort would involve central banks other pertinent public agencies, financial sector representatives, merchants, and the general public. The campaign could be like those used for the introduction of new currencies such as the introduction of the Euro in Eastern European with the accession to the European Monetary Union. For example, starter wallets like the Euro starter packs introduced at the introduction of the Euro. A robust change management and communications strategy is necessary will support adoption of the currency among the general population.

V. Legal, Governance, and Regulatory Perspectives

This section will discuss legal, governance, and regulatory challenges faced by central banks considering CBDC. In order to issue CBDC some may need to amend their legal

[44] Collected data could include (anonymized) data on initial individual/businesses bank deposit holdings and substitution into digital currency, to evaluate degree of substitution with bank deposits. Average daily balances, fraction of transactions conducted in CBDC, as well as average transaction values, for instance, are all useful metrics to evaluate the uptake and success of the experiment.

frameworks, including for issues relating to legal tender, central bank governance, internal organization, and risk management. As Lönnberg (2013) puts it: "Strengthening the institutional capacity of the central bank and ensuring it has the resources needed are critical preconditions for currency reform." Regulations related to user-facing financial institutions such as digital wallet providers and other engaged third parties, may need to be revamped.

The legal framework for CBDC includes the body of law which determines the rights and obligations of parties in the system. The legal framework involves laws of general applicability that affect the payment system (property and contract, banking and finance, insolvency, credit and collateral, electronic documents and digital signatures), as well as those that are specific to it (payment instruments, including currency, bills of exchange, check, electronic payments) (BIS, 2006).[45]

A. Central Bank Legislation and Legal Tender

Central bank legal frameworks need to be examined closely to assess the possibilities and constraints for issuing CBDC. Legislation governing central banks forms the framework within which a central bank can operate, including the constitution, central bank law, as well as, for instance, criminal law, banking/financial institutions law, consumer protection law, financial integrity, and budget laws.

Central banks will need to assess to what extent and under what conditions their legal framework allows CBDC issuance. Relevant aspects relate directly to the designation of banknotes (and coins) as legal tender, the central bank's cash currency management function, and accounting requirements (for instance, International Financial Reporting Standards or local Generally Accepted Accounting Principles). Indirect legal aspects could include requirements for procurement, data security, external audit / oversight, the need to consult with government on specific issues, and/or the right of government to issue directives to the central bank (see Table 2 for a structured list of questions to be addressed).

Change in legislation may be needed for CBDC to be legal tender (Mancini-Griffoli and others, 2018). The definition of legal tender—usually applied to banknotes and coins issued by central banks—varies slightly across jurisdictions. For instance, a creditor is not obligated to accept payment in legal tender in all jurisdictions. The legal concept of currency is associated with the power of the sovereign to establish a legal framework providing for central issuance of banknotes and coins (He and others, 2016). Currency refers to the unit of account and the medium of exchange denominated by reference to that unit of account, prescribed by law. In the strict sense, currency refers to the banknotes and coins that are issued by a central authority (for example, the central bank or Ministry of Finance in some jurisdictions) that has the exclusive right to do so. Currencies are given the status of legal tender under the state's legal framework, which generally entitles the debtor to discharge monetary obligations with the currency through its mandatory acceptance within the relevant

[45] This list of laws is not exhaustive and could vary by jurisdiction.

jurisdiction.[46] As such, the value and credibility of a sovereign currency are intrinsically linked with the ability of the state to support that currency.

The legal concept of money is also based on the power of the state to regulate the monetary system. As a legal matter, the concept of money is broader than the concept of currency and includes not only banknotes and coins but also certain types of assets or instruments that are readily convertible into such banknotes and coins (for example, demand deposits). While money can be created by private parties (for example, banks) as well as central banks, it must generally be denominated in a currency issued by a sovereign authority and must be intended to serve as a generally accepted medium of exchange within that state (Procter 2012).

The concept of legal tender creates two relevant questions for central banks. First, the *application* of this definition of legal tender to retail CBDC is a specific issue that central banks would need to examine further. If, for instance, a retail CBDC would be denominated in the existing domestic currency (as is currently the case with the Swedish pilot project of the "e-Krona"), it would likely not imply any consequences for this retail CBDC as legal tender in Sweden (that is, from the moment of creation, the retail CBDC would be legal tender).[47] If, for instance, a retail CBDC would be denominated in anything other than the currency that the state has decreed must be accepted in payments of debts, the central bank would need to ascertain if this would require changes to that designation.

Additionally, the concept of "legal tender" on its own might need to be subjected to further scrutiny. Some central banks, such as the Swedish Riksbank, are suggesting a review of the concept itself: what does "legal tender" in a digitalized economy imply and does require possible legal amendments to the central bank law as the outcome (Sveriges Riksbank, 2019). Central banks should therefore also consider examining whether the existing legal provisions on legal tender would or should include possibly planned retail CBDC.

[46] It should be noted that the definition of legal tender varies slightly among jurisdictions (He and others, 2016). For example, in some countries, legal tender rules allow the debtor to make a valid "tender"—that is, to take the necessary steps to complete a payment—but there is no obligation on the side of the creditor to accept the tender. A creditor, however, would be barred from recovering the debt in court, if he has refused to accept a valid tender. On the other hand, in other countries, it is unlawful to refuse legal tender in payment. In light of the differences in the definition of legal tender in the euro area, the European Commission adopted a recommendation in 2010 that the concept of legal tender should rely on three main elements: (i) a mandatory acceptance of banknotes and coins; (ii) for their full face value; and (iii) with a power to discharge debt.

[47] Note that the existence of a retail CBDC as legal tender is different from it becoming currency-in-circulation. As noted in the previous sections, a retail CBDC – even if denominated in the domestic currency – would only become currency-in-circulation the moment the central bank decides to issue it.

Table 2. CBDC Legal Framework Analysis

Question	Examples	Comments
What are the relevant **domestic laws** and regulations?	Constitution, Central Bank Law (and central bank by-laws, and/or regulations), Banking Law, Criminal Law, Budget Law, Tax Law, financial integrity regulation, etc.	Ensure a complete overview of relevant legislation, including possible pending amendments.
What are specific **legal requirements** and limitations to CBDC?	Monetary policy instruments, payment system aspects, cash currency management requirements, financial supervision instruments, accounting requirements, government consultation requirements, as well as internal organization requirements (such as procurement, data security, external audit).	Ensure a complete overview of specific legal requirements and limitations, their interactions, as well as possible judicial interpretations.
What are **potential needs** to be captured in legal considerations?	Input/comments from government and public sector at large (finance, economics, telecom, taxation, police, financial intelligence unit, as well as the attorney-general), industry consultation: commercial sector (bank, insurance, pension fund, money exchangers' representatives, chamber of commerce, telco operators, other fintech companies).	Ensure a near-to complete overview of input and views from relevant stakeholders regarding legal considerations to a possible CBDC.
What could be the limitations **of CBDC** within the current legal framework?	Provide a gap analysis of the scope, nature and intent of CBDC as is possible within the existing legal framework, and identify, if any, what kind of legal changes are necessary.	Conduct a feasibility analysis for issuing CBDC within the current legal framework.

Source: Authors.

B. Central Bank Governance and Risk Management

Central banks are considering their governance, internal organization, and risk management when examining the pros and cons of issuing CBDC. CBDC would require the Board's and operational-level staff's clear understanding of key issues regarding initial CBDC considerations, and implementation once a decision to issue CBDC has been made. These can possibly include:

- CBDC objectives (see section III);
- Policy consequences, for instance, relating to the position of CBDC within governmental policies (such as those relating to a cashless society); or, as cash will remain in existence for most scenarios, relating to the coexistence of physical and digital currencies; as well as the effects on liquidity management and operational cash currency management;
- Technical requirements;
- Effects on the internal organization (for instance, capacity and expertise development), risk management (third-party involvement / procurement and

outsourcing risk, cyber security, and other operational, legal and reputational risks for the central bank), data collection and management; and

- Transparency and accountability requirements, for instance, relating to internal audit findings, accounting mechanisms, and internal and external communication.

On CBDC accounting, further clarification might be needed. For instance, in July 2018 the International Accounting Standards Board (IASB) issued a Staff Paper on digital currencies (IASB, 2018). In it the IASB explores various accounting options relating to digital currencies. It notes that digital currencies are: (i) not cash under International Accounting Standards (IAS) 7, given that they are no real means of exchange, and are not issued by a central bank – note that this could be possibly different for CBDC); (ii) not a financial instrument under IAS32, given that there is no contractual relationship; and (iii) possibly an intangible asset under IAS38, given that they could be seen as an identifiable nonmonetary asset without physical substance. Table 3 below provides a structured list of questions to be addressed.

Integrated central bank risk management analysis would be needed to assess what risks the central bank might face when exploring CBDC. CBDC-related cybersecurity issues, as identified in more detail in Section VI, can create operational risks for the central bank. However, a central bank might also run strategy and policy risks, and a variety of other operational risks – including those pertaining to fraud or inadequate project management, outsourcing/third-party risk (when cloud computing solutions are involved), legal risks, and institutional culture, governance and decision-making risks. This could also include lacking skills, expertise, and understanding among central bank key decision-makers and/or staff.[48]

Policy (or strategy) risk results from the key areas in which the central bank is active, such as monetary policy-related risks. With the expanding mandates of central banks this might also involve risks related to policy making in other areas, most notably financial stability (macro prudential oversight, microprudential supervision, ELA/LOLR, and resolution). It could also include issues relating to financial integrity, financial inclusion, consumer protection, and other possible objectives of central banks. Increasingly, fintech is also discussed in the context of central bank mandates.[49] According to the Bank for International Settlements (BIS), most central banks see at least the monetary policy risks as part of decision-making process in the monetary policy committee (BIS, 2009). Some central banks include policy risk management in their general risk management, working on the thought that all risks to the central bank should be approached from a single framework. Risks relating to monetary policy operations are kept under particular scrutiny by central banks by incorporating strict risk control criteria to collateral in case of lending to commercial banks.

Transparency is also an important component of CBDC policies. Given the abovementioned expansion of central bank mandates, transparency by central banks over their policies and

[48] See also Khan (2016) for more guidance on central bank risk management in general.

[49] For example, see the Mexican Fintech Law, approved in March 2018, and the United Arab Emirates Law regarding the Central Bank and Organization of Financial Institutions and Activities, in particular regarding digital money and stored value facilities.

actions is needed. This holds for fintech-related activities as well, including any CBDC-related policy. Given the breadth of topics and central banking areas that these could expand into—a lack of transparency would amount to policy risk for the central bank. The IMF has started work on a Central Bank Transparency Code, that would cover the "broader set of activities undertaken by many central banks since the Global Financial Crisis" (IMF, 2019).

An example of CBDC-related policy risk can be found in Financial Market Infrastructures (FMIs)**.**[50] FMIs play an important role in a country's financial system at large. The 2012 CPMI Principles for Financial Markets Infrastructures (PFMIs) were drafted precisely to help identify and mitigate risks related to this systemic nature of FMIs. FMIs "facilitate the clearing, settlement, and recording of monetary and other financial transactions [which] can strengthen the markets they serve and play a critical role in fostering financial stability." Given this role, they could also "pose significant risks to the financial system and be a potential source of contagion, particularly in periods of market stress." (BIS, 2012)

In addition to policy risk, CBDC can also lead to significant operational risk. Alwazir and Khan, 2020 explores in more detail what possible fintech-related risks are for central banks, including examples of how selected central banks try to mitigate these risks within their internal organization. In addition to policy-related risk (such as the FMI example noted above) and financial risk, the central bank will predominantly run operational risk related to outsourcing / third party involvement, the IT infrastructure in general, cyber security, as well as legal risks related to, i.e., ownership and accountability. As the BoE (2020) notes: "There should be clear policies about who is responsible for redress in the case of fraudulent payments." Figure 6 below offers a schematic overview of the central bank risk universe for considering CBDC.

C. Regulatory Considerations and Pre-Requisites

It would need to be determined whether the CBDC arrangements can be characterized as a payment system and, if so, whether it is systemically important. It could be characterized as a payment system if the arrangement features a "set of instruments, procedures, and rules for the transfer of funds between or among participants, including the participants and the entity operating the arrangement" (BIS, 2012). Determining systemic importance would also be critical given its likely role in the financial system. Key criteria could be like those for private payment systems, including the number and value of transactions processed, the number and type of participants, the markets served, interconnectedness, and any available alternatives. However, given the high expectation from the public from CBDC, it is very likely that the CBDC arrangement is deemed systemically important regardless of its current and potential size. As such, once the CBDC arrangement is identified as a systemically important payment system, then it should be subject to more stringent regulation, supervision, and oversight as a central bank operated FMI. Although systemic importance is largely focused on large-value payment systems, retail payment systems could fall into that category. This would also be relevant for CBDC arrangements.

[50] Which includes payment systems, Central Securities Depositories, Securities Settlement Systems, Central Counterparties, and Trade Repositories.

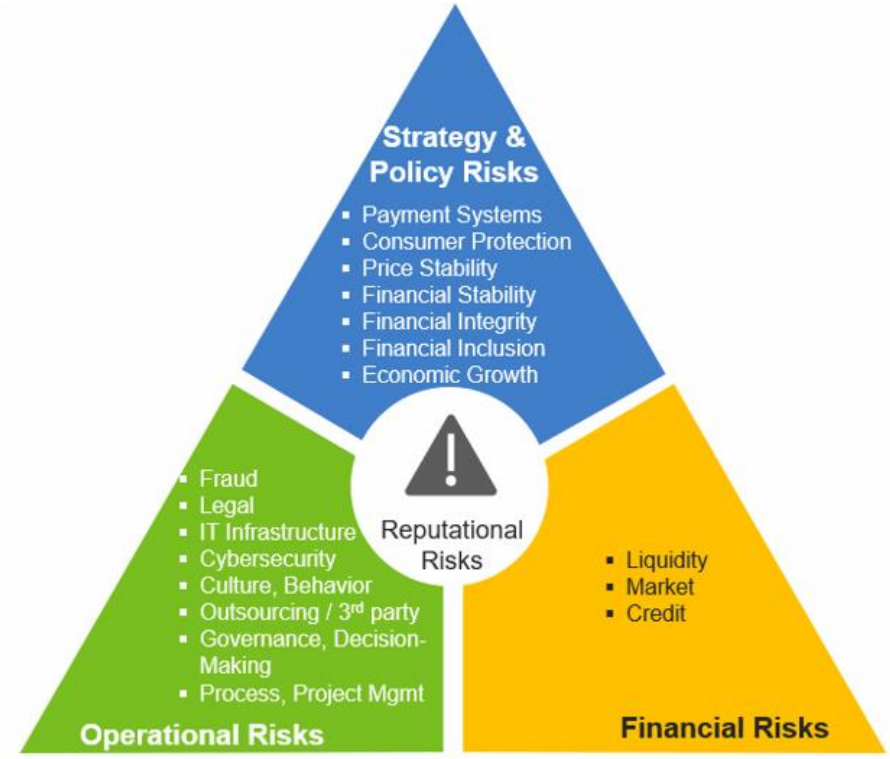
Table 3: CBDB Central Bank Internal Organization Analysis

Question	Examples	Comments
What central bank **objectives** and/or functions will the CBDC serve?	For instance, payment system stability, price stability, financial stability (macro prudential oversight, micro prudential supervision, ELA/LOLR, resolution), financial integrity, financial inclusion, consumer protection, economic growth. Possible links / interaction with the central bank's strategy plan.	CBDC can serve multiple central bank objectives. However, like existing central bank instruments, the central bank needs to be aware of and balance potential conflicts between objectives and therefore the use of CBDC.
What are the **technical requirements** for CBDC?	For instance, a gap analysis of existing infrastructural and technological requirements for and limitations to setting-up and issuing CBDC. See previous subsection on technological infrastructure, and cyber-security.	Identified technological limitations should be assessed from a risk perspective and a financial perspective (see next point), to ensure a realistic overview of what CBDC possibilities the central bank could explore.
What are the **internal organization requirements**?	For instance, building up of expertise and training of staff, risk management (third-party involvement / procurement and outsourcing risk, contractual arrangements, cyber security, and other operational, legal and reputational risks for the central bank), budget requirements and restrictions, data collection and data management requirements.	A complete overview of internal organization requirements (which could also be in part based on internal and external audit findings, and internal and external organization assessments) would help to identify the relevant contextual issues for setting-up and issuing CBDC.
How will **transparency and accountability** over the CBDC be shaped?	For instance, internal audit findings, accounting mechanisms, and internal and external communication.	Transparency by the central bank on CBDC developments will allow for proper accountability to its stakeholders (parliament / society), which on its turn could lead to strengthening / clarifying the central bank's mandate and legal framework (see previous subsection).

Source: Authors.

CBDC arrangements that have been identified as payment systems would also need to observe the public policy objectives of safety and efficiency. The CPSS/IOSCO PFMIs establish the principles aimed at enhancing the safety and efficiency of payment, clearing, settlement, and recording arrangements, and more broadly, limiting systemic risk and fostering transparency and financial stability (BIS, 2012). There are 18 applicable principles for payment systems.[51] The PFMIs also set forth five major responsibilities for authorities, where the central bank oversight and operational responsibilities in CBDC arrangements should warrant authorities' attention.[52]

Figure 6. CBDC Risk Landscape



Source: Alwazir and Khan (2020).

Supervisory Considerations

Gradual development of CBDC through pilot projects or regulatory sandboxes, would help the authorities learn both benefits and risks and help build internal capacity. They may need to hire and retain experts in relevant areas, such as operational, cyber, payment, and settlement risks. It is advisable that the central bank and financial sector regulators keep up with the new technologies and risks. Pilots and sandboxes will be most relevant in indirect

[51] The applicable principles for payment systems are: legal basis, governance, framework for the comprehensive management of risks, credit risk, collateral, liquidity risk, settlement finality, money settlements, exchange-of-value settlement systems, participant-default rules and procedures, general business risk, custody and investment risks, operational risk, access and participation requirements, tiered participation requirements, efficiency and effectiveness, communication procedures and standards, and disclosure of rules, key procedures, and market data.

[52] The responsibilities are: regulation, supervision, and oversight of FMIs; regulatory, supervisory, and oversight powers and resources; disclosure of policies with respect to FMIs; application of the principles for FMIs; and cooperation with other authorities.

operating models, to ensure that legislation, regulations and supervision covers the new activities and institutions (e.g., BigTech firms).

CBDC users could be exposed to additional risks of participating third parties such as default risk of distributors, exchanges and wallet service providers. Distributors and exchanges would accept fiat money from the clients and provide CBDC in exchange. Wallet service providers may hold their clients' private keys and may commingle their clients' CBDC with their own assets. Therefore, depending on the implementation model, the end users may be subject to default risk of distributors and exchanges. Existing financial regulation and supervision, such as e-money regulations, have addressed those risks (such as commingling of assets in case of bankruptcy of a wallet service provider, etc.) of fiat currencies. If those risks in CBDC related entities would not be fully addressed by financial regulation and supervision, the adaptation of CBDC would likely be only limited to small holdings and transactions to avoid the risk of default of their service providers.

CBDC arrangements would also need to manage the potential risks arising from critical third-party service providers (CSPs). Such CSPs are critical to the operational function of an FMI and typically include information technology and messaging providers. As CBDC arrangements could depend on specialized software vendors (for software development and maintenance) and cloud service providers, the associated risks would need to be managed. Authorities' CSP oversight expectations within the PFMI focus on 5 major areas, including risk identification and management, information security, reliability and resilience, technology planning, and communication with users (BIS, 2012). Where permitted under the applicable legal framework, a regulator, supervisor or overseer of an FMI may choose to assess an FMI's CSP against these expectations to promote their robustness (BIS, 2014).

CBDC arrangements that involve the creation of digital tokens to settle retail transactions would also raise similar issues to those that settle wholesale transactions. Despite their different categorization, their design choices could have implications on the safety and efficiency of the arrangement. This includes availability, issuance and redemption process, access, underlying assets/funds and claims, transfer mechanisms, privacy and regulatory compliance, and interoperability (BIS, 2019). Strong legal underpinnings that previously existed for traditional payment, clearing and settlement arrangements also may not necessarily unambiguously extend to CBDC arrangements, and require greater legal certainty to mitigate potential risks. As such, if CBDC arrangements were identified as a payment system, and considered systemically important, it would be expected to observe the PFMI. Further, developers could consider achieving greater consistency with respect to international standards in their design of CBDC arrangements.

More generally, to achieve the trust of the end users, proper regulation and supervision would be needed to the engaged third parties. A recent IMF Fintech Note on regulation and supervision of crypto assets discusses private crypto-asset regulatory frameworks, including how to regulate offering, trading, custody of private crypto assets (Cuervo and others, 2019). While many risks such as market risk are lower for CBDC than private crypto assets, other risks might be similar, such as operational and default risk of service providers. Existing e-money regulations in many countries would also provide useful reference to appropriate regulations of entities engaging with CBDC. Applying proper regulation and supervision to the engaged third parties would help to achieve the social trust of CBDC ecosystem. In addition, the transparency of CBDC itself (such as important product features) is also important, especially when fees or negative interest rates could be imposed on users.

VI. Cybersecurity Considerations

Ever-changing sophisticated cybersecurity threats endanger CBDC at various components or levels, with lucrative rewards for malicious users. Cybersecurity is a persistent and significant risk to any payment infrastructure (BIS, 2016). This emphasizes the importance for central banks to design, build, and run a secure and resilient CBDC ecosystem in its entirety and throughout all components and integrations of the underlining systems. This will require central banks to concentrate on two main information technology (IT) security components:

- Reviewing and strengthening the central bank's IT operational resilience and security posture. The main components are the central bank internal IT processes, technologies and skills needed to maintain the highest-level assurance of the central bank's networks, integrated systems, applications, and data. The internal IT processes should align with best practices (e.g., U.S. DHS, 2016), and strengthen key roles such as the Security Operations Center, whether operated internally by the central bank or delegated to a third party.
- Strengthening *s*ecurity activities around the CBDC design, implementation and deployment of its components and the security decisions impacting the overall CBDC ecosystem (see below).

A typical two-layer approach to strengthening the CBDC design, implementation and deployment is presented below. Each layer requires the appropriate security controls and practices. The main goal is to design the CBDC in a "defense-in-depth" fashion and to consider security during the initial phases of the project rather than later in the process.

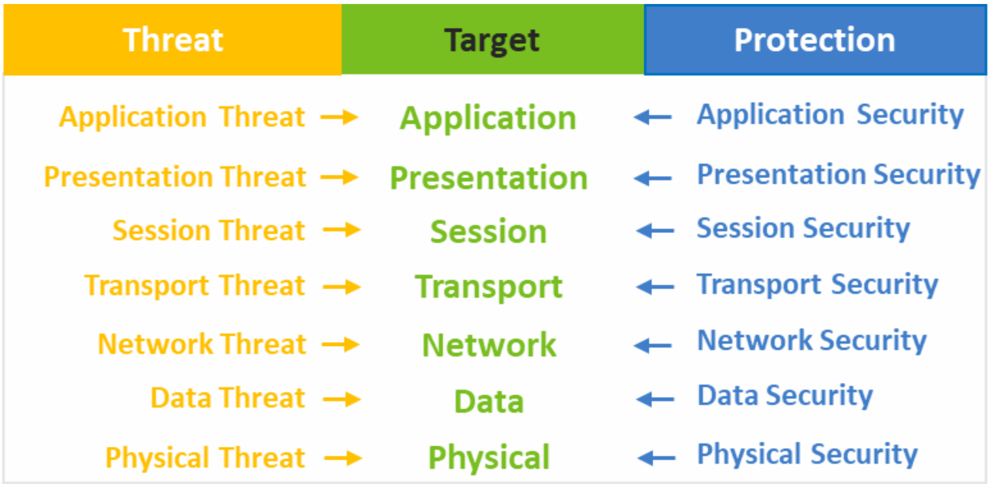
- Business and process layer. This layer relies on the early decisions and the central bank's security work practices to manage people, processes and technologies. The security of this layer is only as good as the central bank's operational resilience and security posture mentioned above. The goal is to be able to continuously reduce risks such as weak access model, privilege escalation,[53] abuse of privileged functionalities, excessive permissions, lack of protections around the source-code, flaws within the coin issuance or decommissioning processes. It is preferable for central banks to verify their operational resilience and security posture through a specialized independent third party. Appendix 2 discusses some of these layer concerns in more detail.

[53] Privilege escalation is the act of exploiting a vulnerability or misconfiguration within an application/system to elevate a restricted and limited access to a privileged access to perform an unauthorized functionality or gain unauthorized access to sensitive data.

- Infrastructure and application layer. This layer can leverage well established frameworks such as the open systems interconnections (OSI, 1994) model to perform threat modeling and architecture risk analysis with the right level of granularity. ITU (2019) introduced a useful unified security model (USM) to link *Targets* to corresponding *Threats*, to identify a set of specific *Protection* schemes. Models such as OSI or USM, sometimes used together, can help perform systemic security threat modeling, reducing significantly the chances of missing important risks at the infrastructure and application layer of CBDC (Figure 7).

As with any critical system susceptible to malicious or non-malicious events that can lead to disruptions, rigorous security activities and appropriate prevention controls are implemented during the design phase (NIST, 2020). These security threat preventions include (i) *CBDC architecture risk analysis* to identify any security design flaws, including for smart contracts design and integration with the CBDC ledger, whether it is DLT or non-DLT based; (ii) *security threat modeling* of the design, integrations and data flows to identify the overall CBDC targets, threats, and countermeasures; (iii) *manual and* automated *security code-review* to verify the CBDC critical components – including smart contracts – and identify and remediate any vulnerabilities in the source-code; and (iv) *manual and automated penetration testing* to examine the exposed components and to reach the highest-level of assurance of the CBDC ecosystem. These activities should be performed by an independent cybersecurity assurance specialist and should be repeated on a regular basis to maintain the highest-level of assurance of the entire CBDC ecosystem (Annex 2).

Figure 7: OSI Threat, Target, Protection Model



Threat		Target		Protection
Application Threat	→	Application	←	Application Security
Presentation Threat	→	Presentation	←	Presentation Security
Session Threat	→	Session	←	Session Security
Transport Threat	→	Transport	←	Transport Security
Network Threat	→	Network	←	Network Security
Data Threat	→	Data	←	Data Security
Physical Threat	→	Physical	←	Physical Security

Source: ITU, 2019.

VII. Conclusion and Summary

As new forms of digital money emerge, central banks have started exploring retail CBDC issuance. In some economies, retail CBDC are expected to serve as a tool to tackle the dwindling use of cash, while other economies seek innovative methods to expand financial inclusion. The underlying rationale for CBDC issuance may vary based on the central banks mandate, macro-financial circumstances or market and regulatory environment.

Based on a comprehensive survey of published research, this paper is intended to provide policymakers with a structured framework to organize decisions on CBDC issuance. These decisions range from whether and under what circumstances to issue, to selecting the right operating model, design features and the project management approach, ending with a holistic discussion of the cybersecurity risks and regulatory and legal framework considerations. It acknowledges that there is no one-size-fits-all approach as central banks may be at different stages in their CBDC thinking or might approach the question from different angles.

The decision-making process starts with understanding thoroughly the problem to be solved and the full array of solutions. In some instances, deploying fast payments would offer enhanced control over essential payment systems without issuing CBDC. On the other hand, expanding financial inclusion or reacting to dwindling cash usage could be compelling reasons for CBDC issuance. However, other options could include promoting mobile money or incentivizing private-sector financial institutions to improve their product offerings. A solid use case and rationale for retail CBDC issuance is critical as it will inform the design and implementation process.

In terms of technology development best practices, an agile project management approach can optimize development costs, reduce project risks and facilitate gradual user adoption and trust. The iterative nature of an agile approach will support a non-linear decision- making flow and ensure that any deficiencies or gaps in the design or implementation can be addressed immediately. Involving key stakeholders, such as end-users, into the implementation process will ensure CBDC usefulness and contribute to building adoption and trust.

The operating model determines the degree of central bank hands-on involvement in CBDC distribution and user engagement. For example, a single-tier direct-access account-based approach would have users holding accounts directly at the central bank that also provides and manages users’ digital wallets. Under a two-tier indirect approach, the central bank would issue CBDC, but private institutions would carry out the work of administering accounts and providing user payment services, perhaps mitigating financial disintermediation risk. Under an sCBDC approach CBDC issuance is effectively outsourced to private digital money issuers by giving them access to central bank reserves in exchange for submitting to strict supervision and oversight by the central bank or other authorities.

Design features depend on CBDC policy objectives and country circumstances, while key design principles are foundational and independent. Key design principles like cybersecurity, user-centricity, flexibility, and financial integrity provide the foundation for the specific design features such as the technology platform, the degree of transparency, availability, usage limits, whether it will be interest bearing, and usage fees.

Cyber risk management capacity becomes critical in a digital currency world. It covers the business and/or the infrastructure layers, each requiring unique and appropriate security controls and practices to mitigate malicious attacks and breaches. Business layer risks revolve around people, processes and technology, while the infrastructure layer risks are concerned with high-level threat modeling and an architecture risk analysis. A big decision is whether to outsource the running of the CBDC network to third-party cloud providers and how to manage any associated risks.

Legal, governance, internal organization, and risk management issues are all key constraints and decision factors. Does CBDC fall under the existing legal tender definition, and does existing legislation allow the central bank to issue CBDC and/or does it limit design choices? Is CBDC issuance feasible within the central bank's currency management mandate and function? Pertinent accounting standards and indirect legal aspects such as procurement, data security, and external audit requirements also need to be considered, along with internal governance and capacity, and transparency and accountability requirements.

A central bank's decision to issue CBDC and, if yes, how, involves a holistic assessment of policy considerations and risks, product design, cybersecurity, operational, technical, legal and regulatory requirements. Options can be tested in a closed and controlled environment such as an innovation hub or regulatory sandbox using an agile approach to help gain a more practical understanding of the implications and risks the choices might introduce. This approach would also help build capacity among central bank staff.

Table 4 provides a summarized overview of the retail CBDC considerations listed above, including possible components of IMF technical assistance.

Table 4. Summary of Retail CBDC Implementation Considerations

	Considerations	Description	Technical Assistance Components
1.	**Objectives**	Central bank identifies the needs and problem(s) that a retail CBDC would address, and the full array of possible (other) solutions. Central bank assesses cash and non-cash use and trends	Policy frameworks Central bank law Payments and Financial Market Infrastructures
2.	**Implementation & Infrastructure**	Central bank identifies project management approach and involves key stakeholders. Central bank assesses CBDC design features based on policy objectives (point 1) and country circumstances, including aspects of cybersecurity, user-centricity, flexibility, and financial integrity.	Central bank project management Central bank cyber-security Payments and Financial Market Infrastructures
3.	**Legal Framework**	Central bank identifies constraints posed by legal framework, including legal tender definition.	Central bank law
4.	**Governance, Organization, Risk Management**	Central bank identifies decision-making structure relevant for CBDC, organization structure (including innovation hub and/or sandbox), and operational risks (including outsourcing/cloud computing).	Central bank governance, organization, risk management, accounting. internal audit

Source: Authors.

References

Accenture. 2019. “The (R)evolution of Money II.

Access to Cash Review. 2019. “Access to Cash Review: Final Report.”

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

----. 2019b. “Central Bank Digital Currencies: 4 Questions and Answers,” International Monetary Fund Blog, December 12.

Agarwal, R., and M. Kimball. 2016. “Breaking through the Zero Lower Bound,” IMF Working Paper 15/224, International Monetary Fund, Washington, DC.

Agur, I., A. Ari, and G. Dell’Ariccia. 2019. “Designing Central Bank Digital Currencies,” IMF Working Paper WP/19/252, International Monetary Fund, Washington, DC.

Alvez, M., R. Lluberas and J. Ponce. 2019. “The Cost of Using Cash and Checks in Uruguay,” Documento de trabajo del Banco Central del Uruguay 004-2019.

Alwazir, J., and Khan, A. 2020. “Fintech and Central Bank Risk Management,” IMF Working Paper (forthcoming).

Armelius, H., P. Boel, C.A. Claussen and M. Nessén. 2018. “The e-Krona and the Macroeconomy,” Sveriges Riksbank Economic Review, Third Quarter.

Auer, R. and R. Boehme. 2020. “The Technology of Retail Central Bank Digital Currency,” Bank for International Settlements Quarterly Review, March.

Bank of Canada. 2020. “Contingency Planning for a Central Bank Digital Currency,” February 25.

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

Bank for International Settlements. 2006. “General Guidance for National Payment System Development,” Committee on Payment and Settlement Systems, Basel: Bank for International Settlements.

----. 2009. “Issues in the Governance of Central Banks – A Report from the Central Bank Governance Group,” Basel: Bank for International Settlements.

----. 2012. “Principles for Financial Markets Infrastructures,” Committee on Payment and Settlement Systems and International Organization of Securities Commissions, Basel: Bank for International Settlements.

----. 2013. “Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools,” Basel Committee on Banking Supervision, Basel: Bank for International Settlements.

----. 2014. “Basel III: The Net Stable Funding Ratio,” Basel Committee on Banking Supervision, Basel: Bank for International Settlements.

----. 2014. "Principles for Financial Market Infrastructures: Assessment Methodology for the Oversight Expectations Applicable to Critical Service Providers," Committee on Payment and Settlement Systems and International Organization of Securities Commissions, Basel: Bank for International Settlements.

----. 2016. "Guidance on Cyber-Resilience for Financial Market Infrastructures," Committee on Payments and Market Infrastructures and International Organization of Securities Commissions.

----. 2017. "Distributed Ledger Technology in Payment, Clearing and Settlement—An Analytical Framework," Committee on Payment and Settlement Systems, Basel: Bank for International Settlements.

----. 2018. "Central Bank Digital Currencies," Committee on Payments and Market Infrastructures, Basel: Bank for International Settlements.

----. 2019.. "Wholesale Digital Tokens," Committee on Payments and Market Infrastructures, Basel: Bank for International Settlements.

----. 2020. "Payment Aspects of Financial Inclusion in the Fintech Era," Committee on Payments and Market Infrastructures and World Bank Group.

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

Bank of Japan and European Central Bank (BoJ/ECB). 2017. "Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment."

Banka, H. 2018. "Initial findings from the implementation of the Practical Guide for Measuring Retail Payment Costs," World Bank Private Sector Development Blog, May 28. https://blogs.worldbank.org/psd/initial-findings-implementation-practical-guide-measuring-retail-payment-costs

Barrdear, J. and M. Kumhof. 2016. "The Macroeconomics of Central Bank Issued Digital Currencies," Bank of England Working Paper 605, Bank of England, London.

Barontini, C., and C. Holden. 2019. "Proceeding with Caution – A Survey on Central Bank Digital Currency," Bank for International Settlements Papers No. 101, January.

Bátiz-Lazo, B., and Moretta, T. 2016. "Mondex and VisaCash: The First (Failed) Attempt at an Electronic Purse," in B. Bátiz-Lazo and L. Efthymiou (eds.) *The Book of Payments: Historical and Contemporary Views on the Cashless Economy*, London: Palgrave-Macmillan (Springer Nature), pp. 177-186.

Bech, M. and R. Garratt. 2017. "Central Bank Cryptocurrencies," *BIS Quarterly Review*, Basel: Bank for International Settlements, September.

Bech, M., Y. Shimizu and P. Wong. 2017. "The Quest for Speed in Payments," *BIS Quarterly Review*, Basel: Bank for International Settlements, March.

Bergara, M. and J. Ponce. 2018. "Central Bank Digital Currency: The Uruguayan E-Peso Case," in Gnan, E. and D. Masciandro. 2018. *Do We Need Central Bank Currency? Economics, Technology and Institutions*, Société Universitaire Européenne de Recherches Financières.

Berman, A. 2018. "Venezuela Officially Launches Sale of Controversial Petro Coin for Fiat, Crypto," Coin Telegraph, October 30.

Bernhardt, C. 2019. "Quantum Computing for Everyone," The MIT Press.

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

Bjerg, O. 2018. "Breaking the Gilt Standard: The Problem of Parity in Kumhof and Noone's Design Principles for Central Bank Digital Currencies," Copenhagen Business School Working Paper, August.

Boivin, J., E. Bartsch, S. Fischer, P. Hildebrand. 2019. "Dealing with the Next Downturn," Blackrock Investment Institute.

Boar, C., H. Holden and A. Wadsworth, 2020, "Impending Arrival - A Sequel to the Survey on Central Bank Digital Currency," Bank for International Settlements Paper No. 107.

Bolt, W. and D. Humphrey. 2005. "Public Good Issues in TARGET: Natural Monopoly, Scale Economies, Network Effects and Cost Allocation," European Central Bank Working Paper 505, July. https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp505.pdf

Bordo, M., and A. Levin. 2018. "Central Bank Digital Currency and The Future of Monetary Policy," *Monetary Policy and Payments*, Vol. 3, pp. 143-178.

Bouvier, J. 1852. *Law Dictionary, Vol. II (Adapted to the Constitution and Laws of the United States of America And of the Several States of the American Union).*

Bradbury, D.. 2013. "Hackers Hit Bitcoin Central Exchange," Coindesk, April 29.

Brainard, L. 2019. "Digital Currencies, Stablecoins, and the Evolving Payments Landscape," Speech at the Future of Money in the Digital Age, Peterson Institute for International Economics and Princeton University's Bendheim Center for Finance, Washington, D.C.

----. 2020. "The Digitalization of Payments and Currency: Some Issues for Consideration," Speech at the Symposium on the Future of Payments, Stanford, California, February 5.

Breckinridge, S.P. 1903. *Legal Tender – A Study in English and American Monetary History*, Chicago: The University of Chicago Press.

Brunnermeier, M.K., H. James and J.-P. Landau. 2019. "The Digitalization of Money," National Bureau of Economics Research Working Paper 26300, September.

Brunnermeier, M.K. and D. Niepelt. 2019. "On the Equivalence of Private and Public Money," *Journal of Monetary Economics*, Vol. 106, October.

Bullmann, D., J. Klemm, and A. Pinna. 2019. "In search for stability in crypto-assets: are stablecoins the solution?" European Central Bank, Occasional Paper Series No. 230.

Burgos, A. and B. Batavia. 2018. "Currency in the Digital Era," Banco Central do Brasil Working Paper, July.

Carstens, A.. 2019. "The Future of Money and Payments," Speech at the Central Bank of Ireland. March 22.

Casey, M., J. Crane, G. Gensler, S. Johnson, and N. Narula. 2018. "The Impact of Blockchain Technology on Finance: A Catalyst for Change," Geneva Reports on the World Economy 21, International Center for Monetary and Banking Studies, Geneva.

Central Bank of the Bahamas (CBOB). 2019. "Project Sand Dollar: A Bahamas Payments System Modernisation Initiative."

Chaum, D. 1983. "Blind Signatures for Untraceable Payments," *Advances in Cryptology, Proceedings of Crypto '82*, pp 199–203.

Cheng, R. 2016. "By 2020, More People Will Own a Phone Than Have Electricity," CNET, February 3.

Constancio, V. 2017. "The future of monetary policy frameworks," Lecture at the Instituto Superior de Economia e Gestro, Lisbon, May 25.

Consultative Group to Assist the Poorest (CGAP). 2019. "Fair Play: Ensuring Competition in Digital Financial Services."

Cœuré, B. 2019. "Towards the Retail Payments of Tomorrow: A European Strategy," Speech at the Joint Conference of the ECB and the National Bank of Belgium on "Crossing the chasm to the retail payments of tomorrow," November 26.

Copic, E. and M. Franke. 2020. "Influencing the Velocity of Central Bank Digital Currencies," Unpublished manuscript.

Cuervo, C., A. Morozova and N. Sugimoto, 2020, "Regulation of Crypto-Assets," IMF Fintech Note No. 19/03.

Davoodalhosseini, M., F. Rivadeneyra, Y. Zhu. 2020. "CBDC and Monetary Policy," Bank of Canada Staff Analytical Note 2020-04, February.

Deloitte. 2016. "Bitcoin, Blockchain, and Distributed Ledgers: Caught Between Promise and Reality," Melbourne.

Diez de los Rios, A. and Y. Zhu. 2020. "CBDC and Monetary Sovereignty," Bank of Canada Staff Analytical Note 2020-5, February.

Dyson, B., and G. Hodgson. 2017. "Digital Cash: Why Central Banks Should Start Issuing Electronic Money."

European Central Bank (ECB). 2016. "Distributed Ledger Technology."

----. 2018. "What is TARGET Instant Payment Settlement (TIPS)?"

----. 2019. "Exploring Anonymity in Central Bank Digital Currencies," ECB In Focus, December.

European Money and Finance Forum. 2018. "Do We Need Central Bank Digital Currency?" Economics, Technology and Institutions, SUERF Conference Proceedings 2018/2.

Eyers, J. 2019. "Facebook to Man Barricades Against Libra Hackers," *Financial Review*, June 20.

Fan Y. 2020. "Some Thoughts on CBDC Operations in China," *Central Banking*, April 1.

Financial Action Task Force (FATF). 2019. "Public Consultation on FATF Draft Guidance on Digital Identity," Paris: FATF.

Federal Reserve Board (FRB). 2019. Is it Legal for a Business in the United States to Refuse Cash as a Form of Payment? Board of Governors of the Federal Reserve Board. (Retrieved April 18, 2019)

Fernández-Villaverde, J., D. Sanches, L. Schilling, H. Uhlig. 2020. "Central Bank Digital Currency: Central Banking for All?" Federal Reserve Bank of Philadelphia Working Paper WP 20-19, June.

Feyen, E., J. Frost and H. Natarajan. 2020. "Digital Money: Implications for Emerging Market and Developing Economies," VoxEU, January 16.

Financial Stability Board (FSB). 2020. "Addressing the Regulatory, Supervisory and Oversight Challenges Raised by Global Stablecoin Arrangements," FSB Consultative Document, April 14.

Garratt, R. and M. van Oordt. 2020. "Privacy as a Public Good: A Case for Electronic Cash," Bank of Canada Staff Working Paper 2019-24, July.

George, A. 2018. "How Satellite Internet Could Provide Disaster-Proof Coverage," *Popular Mechanics*, February 19.

Gertler, M., N. Kiyotaki, and A. Prestipino. 2017. "A Macroeconomic Model with Financial Panics," International Finance Discussion Paper 1219, Federal Reserve Board, Washington, DC.

Gowrisankaran, G. and J. Stavins. 2004. "Network Externalities and Technology Adoption: Lessons from Electronic Payments," *RAND Journal of Economics* 35 (2): 260–276.

He, D., K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, T. Saadi Sedik, N. Stetsenko, and C. Verdugo-Yepes. 2016. "Virtual Currencies and Beyond: Initial Considerations," IMF Staff Discussion Note 16/03.

He, D., R. Leckow, V. Haksar, T. Mancini-Griffoli, N. Jenkinson, M. Kashima, T. Khiaonarong, C. Rochon, and H. Tourpe. 2017. "Fintech and Financial Services: Initial Considerations," IMF Staff Discussion Note SDN/17/05.

Huang, R., and L. Ratnovski. 2011. "The Dark Side of Bank Wholesale Funding," *Journal of Financial Intermediation.* 20 (2): 248–63.

Huynh, K., J. Molnar, O. Shcherbakov and J. Yu. 2020. "Demand for Payment Services and Consumer Welfare: The Introduction of a Central Bank Digital Currency," Bank of Canada Staff Working Paper 2020-7.

Interaction Design Foundation. "User Centered Design."

International Accounting Standards Board (IASB). 2018. *Transactions Involving Commodities and Cryptocurrencies*, Staff Paper. London: IFRS Foundation, July.

International Monetary Fund (IMF). 2018. "Republic of the Marshall Islands: Selected Issues," Washington, D.C.: International Monetary Fund, September.

----. 2019. "Staff Proposal to Update the Monetary and Financial Policies Transparency Code," Washington, D.C.: International Monetary Fund, May.

International Organization for Standardization (ISO). 1994. "Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model."

International Telecommunication Union (ITU). 2019. "Protection Assurance for Digital Currencies," ITU Digital Fiat Currency Focus Group Security Working Group Deliverable, June 2019.

Jenks, T. 2018. "Pros and Cons of Different Blockchain Consensus Protocols."

Kahn, C., J. McAndrews and W. Roberds. 2005. "Money is privacy," *International Economic Review*, vol. 46, no. 2, pp 377–99.

Kahn, C., and W. Roberds. 2009. "Why Pay? An Introduction to Payments Economics," *Journal of Financial Intermediation*, 18 (1): 1–23.

Kahn, C. M., F. Rivadeneyra and T.-N. Wong. 2018. "Should the Central Bank Issue E-Money?" Bank of Canada Staff Working Paper 2018-58., December.

Khan, A. 2016. "Central Bank Governance and the Role of Nonfinancial Risk Management," IMF Working Paper 16/32. Washington, D.C.: International Monetary Fund.

Khiaonarong, T. 2003. "Payment Systems Efficiency, Policy Approaches, and the Role of the Central Bank," Bank of Finland Discussion Paper 1/2003, Helsinki.

Khiaonarong, T. and D. Humphrey. 2019. "Cash Use Across Countries and the Demand for Central Bank Digital Currency," IMF Working Paper WP/19/46, Washington, D.C.

King, R. 2020. "The Central Bank Digital Currency Survey 2020 – Debunking Some Myths," *Central Banking*, May 7.

Kolisko, L. 2018. "In-depth on Differences between Public, Private and Permissioned Blockchains."

Koning, J.P.. 2019. "Controllable Anonymity."

Kosse, A., H. Chen, M.-H. Felt, V. D. Jiongo, K. Nield, and A. Welte. 2017. "The Costs of Point-of-Sale Payments in Canada," Bank of Canada Staff Discussion Paper 2017-4, Ottawa.

Kotaro, I., H. Wang, W. Mitchell and M. Malaika. 2020. "A Central Bank Digital Currency in the ECCU," in IMF. 2020. "Eastern Caribbean Currency Union Selected Issues," Country Report No. 20/71, March.

Kumhof, M., and C. Noone. 2018. "Central Bank Digital Currencies - Design Principles and Balance Sheet Implications," Bank of England Staff Working Paper No. 725.

Lariccia, F. 2018. "Central Bank Digital Currency: A Macro-Financial Perspective."

Lönnberg, A. 2013. "New Money," *Finance & Development*, Washington, D.C.: International Monetary Fund, December.

Lovett, R. A. 2011. "What If the Biggest Solar Storm on Record Happened Today?" *National Geographic News*, March 4.

Mancini-Griffoli, T., M.S. Martinez Peria, I. Agur, A. Ari, J. Kiff, A. Popescu, and C. Rochon. 2018. "Casting Light on Central Bank Digital Currency," IMF Staff Discussion Note SDN/18/08.

Mantini, N. 2018. "Design Thinking, Lean Startup and Agile: What is the difference?" *Medium*, December 28.

Matonis, J. 2012. "MintChip Misses the Point of Digital Currency," *Forbes*, April 12.

Meaning, J., B. Dyson, J. Barker and E. Clayton, 2018. "Broadening Narrow Money: Monetary Policy with a Central Bank Digital Currency," Bank of England Staff Working Paper No. 724, May.

Mearian, L. 2019. "Hedera Hashgraph Launches Mainnet, Hopes to Compete with Global Business Networks," *Computerworld*, August 29.

Mersch, Y. 2020. "An ECB digital currency – a flight of fancy?" Speech at the Consensus 2020 Virtual Conference, May 11.

Middlebrook, S.T., and S.J. Hughes. 2016. "Substitutes for Legal Tender: Lessons from History for the Regulation of Virtual Currencies," Indiana University Legal Studies Research Paper. Bloomington: Indiana University.

Mills, D., K. Wang, B. Malone, A. Ravi, J. Marquardt, C. Chen, A. Badev, T. Brezinski, L. Fahy, K. Liao, V. Kargenian, M. Ellithorpe, W. Ng, and M. Baird. 2016. "Distributed Ledger Technology in Payments, Clearing, and Settlement," Finance and Economics Discussion Series 2016-095. Washington: Board of Governors of the Federal Reserve System.

Milne, A.. 2020. "Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money," SSRN Electronic Journal.

Murphy, S. 2014. "Proof of Concept versus Pilot Program."

Nakamoto, S. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

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

National Institute of Standards and Technology (NIST). 2020. "SP 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

----. 2019. "NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto Semifinals."

Naybour, P. 2015. "Agile Project Management – the What and the Why," Association for Project Management.

Norges Bank. 2018. "Central Bank Digital Currencies," Norges Bank Paper 1, Oslo.

Official Monetary and Financial Institutions Forum (OMFIF). 2019. "Retail CBDCs: The next payments frontier."

Panetta, F. 2018. "21st Century Cash: Central Banking, Technological Innovation and Digital Currency," SUERF SUERF Policy Note, Issue No 40.

Prince, M. 2017. "Quantifying the Impact of Cloudbleed," he Cloudflare Blog, March 1.

Procter, C., 2012, *Mann's Legal Aspect of Money*, Oxford University Press.

Reserve Bank of India (RBI). 2018. "Reserve Bank of India releases Dissent Note on Inter-Ministerial Committee for finalization of Amendments to PSS Act," RBI Press Release, October 19.

Reuters. 2018. "The Coincheck Cryptocurrency Hack: Everything You Need to Know," *Fortune*, January 29.

Rogoff, K. 2014. "Costs and Benefits to Phasing Out Paper Currency," NBER Working Paper 20126, National Bureau of Economic Research, Cambridge, MA.

Rutkowski, M., A. Garcia Mora, G.L. Bull, B. Guermazi, C. Grown. 2020. "Responding to crisis with digital payments for social protection: Short-term measures with long-term benefits," World Bank Blog, March 31.

Sarwat, J. 2012. "Inflation Targeting: Holding the Line," *Finance & Development*. International Monetary Fund.

Schneier, B. 2018a. "Spectre and Meltdown Attacks Against Microprocessors," *Schneier on Security*, January 5.

----. 2018b. "Quantum Computing and Cryptography," *Schneier on Security*, September 14.

Schwartz, M. J. 2017. "NotPetya Patient Zero: Ukrainian Accounting Software Vendor Backdoored Software Facilitated Malware Attack, ESET Finds." *BankInfoSecurity*, July 4.

Secure Technology Alliance. 2014. "Giesecke & Devrient Offers the Most Advanced U.S. Debit EMV Solution."

Shabsigh, G., T. Khiaonarong., and H. Leinonen. 2020. "Distributed Ledger Technology Experiments in Payments and Settlements," IMF Fintech Note, forthcoming.

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

Siegel, D. 2016. "Understanding the DAO Attack," *Coindesk*, June 25.

Sirer, E. G. 2016. "The ShapeShift Hack: Simply Incredible," *Hacking, Distributed*, April 12.

South African Reserve Bank (SARB). 2018. "Project Khoka."

Sveriges Riksbank. 2018. *The Riksbank E-Krona Project: Report 2*.

Sveriges Riksbank, 2019. "The Riksbank Proposes a Review of the Concept of Legal Tender," Press Release, April 29.

Sveriges Riksbank. 2020. "Do We Have the Right to Pay in Cash?" in *Payments in Sweden 2019*.

Stalder, F.. 2002. "Failures and Successes: Notes on the Development of Electronic Cash," *The Information Society*, 18 (3).

Stewart, J. 2018. "Developers Work to Combine NFC With Blockchain for POS Transactions," *Digital Transactions*, April 17.

Sun, T. 2020. "Preconditions for Digital Money Adoption − What Can we Learn from Alipay?" IMF Working Paper, forthcoming.

SwiftSafe. 2018. "Trade.io Cold Wallet Hacked Losing 50 Million TIO Tokens—TIO Coin to Be Forked," Medium, November 2.

Taylor, C., Wilson, C., Holttinen, E., Morozova, A. 2019. "Institutional Arrangements for Fintech Regulation and Supervision," IMF Fintech Note 19/02.

Torode, C., and M. Pratt. 2018. "Agile Project Management."

United Kingdom Government Office for Science. 2016. "Distributed Ledger Technology: Beyond Block Chain," London.

United States Department of Homeland Security (U.S. DHS). 2016. "Cyber Resilience Review (CRR) Method Description and Self-Assessment User Guide."

United States Federal Reserve Board. 2019. "Federal Reserve Announces Plan to Develop a New Round-the-Clock Real-Time Payment and Settlement Service to Support Faster Payments," Press Release, August 5.

VISA. 2018. "VISA Fact Sheet."

World Economic Forum (WEF). 2020. Central Bank Digital Currency Policy- Maker Toolkit.

Zhang, T. 2020. "Central Bank Digital Currency," Keynote Address at the London School of Economics, February 28.

Xiao, Y., N. Zhang, J. Li, W. Lou, and Y.T. Hou. 2019. "Distributed Consensus Protocols and Algorithms," in *Blockchain for Distributed Systems Security*, First Edition, Wiley & Sons, 2019.

Yao, Q. 2018. "Technical Aspects of CBDC in a Two-Tiered System," Institute of Digital Money, People's Bank of China.

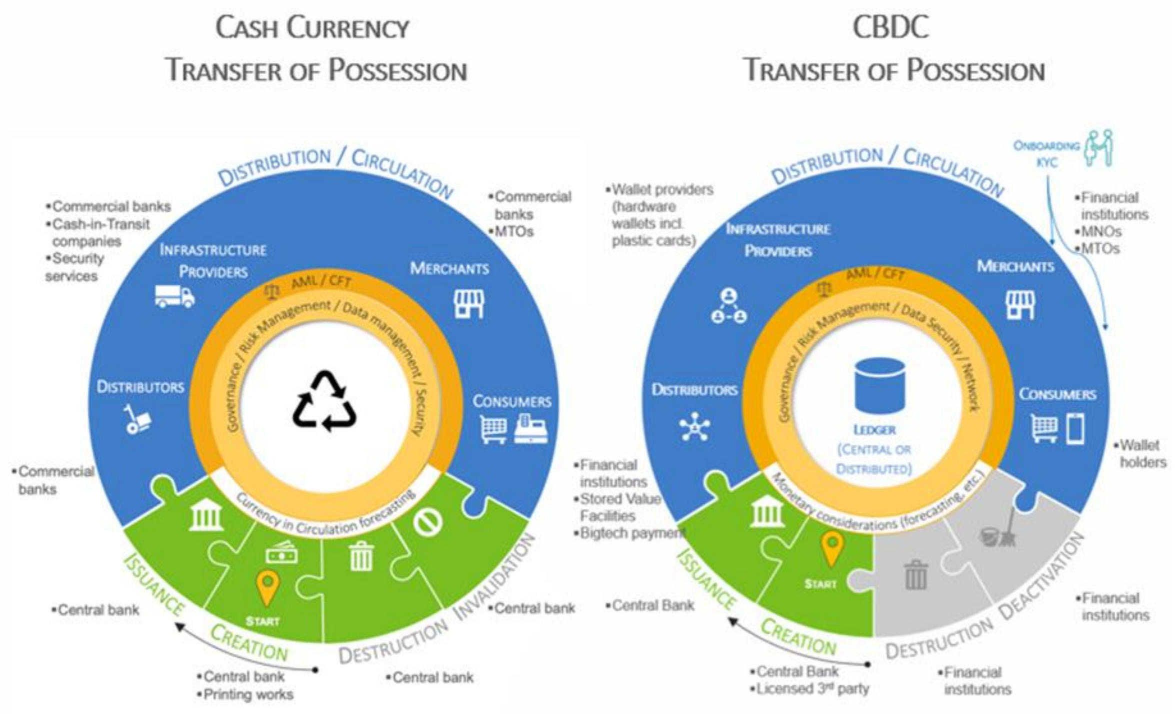
Annex 1. Countries Where Retail CBDC is Being Explored[54]

Jurisdictions Where Retail CBDC Is Being Explored (as of May 27, 2020)	
Where central banks are in the advanced stages of retail CBDC exploration	
Bahamas (pilot launched)	Sweden (proof of concept started)
China (pilot launched)	Ukraine (pilot completed)
Eastern Caribbean (pilot launched)	Uruguay (pilot completed)
South Africa	
Where central banks have explored or are exploring issuing retail CBDC	
Australia	Jamaica
Brazil	Japan
Canada	Korea (proof of concept started)
Chile	Mauritius
Curaçao en Sint Maarten	Morocco
Denmark	New Zealand
Ecuador (completed pilot & project discontinued)	Norway
Euro Area	Russia
Finland	Switzerland
Ghana	Trinidad and Tobago
Hong Kong SAR	Tunisia
Iceland	Turkey
India	United Kingdom
Indonesia	United States
Israel	
Where central banks have explored or are exploring issuing retail CBDC (unconfirmed)	
Bahrain	*Lebanon*
Egypt	*Pakistan*
Haiti	*Palestine*
Iran	*Philippines*
Kazakhstan	*Rwanda*
Sources: Central banks or various news sources per hyperlinks above. *Italicized* entries are sourced from news articles. Information has not been verified through official channels.	

[54] Each country listed in the table embeds a hyper-link to the sources of the information regarding that country's CBDC work.

ANNEX 2. PROCESS, ROLES, AND RESPONSIBILITIES

The CBDC life cycle is likely to resemble at least parts of that of physical cash currency (see figure). In the case of the physical version, the first part of the cycle is to forecast the demand for cash currency, based on relevant economic data, including cyclical demand. These could be related, for instance, to national holidays, reasonably predictable shocks, such as inclement weather or even natural disasters, and agricultural cycles. This is particularly relevant for those countries where agriculture is still largely cash based.



The design of the notes would need to account for optical and security-related features. Following the forecast, the second part of the cycle is to design bank notes and/or coins. This includes optical designs (often reflecting symbols of national identity) as well as security aspects to prevent or significantly limit counterfeiting. The design of the Uruguayan e-Peso digital notes included a series ID number so the notes can be traced back to a specific user through their wallet.

CBDC, as a digital representation of the fiat currency created through an entry in a database or through token creation for the CBDC counterpart, is somewhat like the minting of coins and printing of bank notes. The creation of the CBDC could be done by the monetary authority, or, as with physical currency, outsourced following adequate governance and cybersecurity measures. Most central bank pilots are outsourcing this step, though this entails several operational risks that the central bank needs to identify, mitigate, and monitor (see Section V.B). After the creation process has been completed, the monetary authority will issue the CBDC. Since the process of creation can be almost instantaneous, issuance and creation could be linked. Although creation could be outsourced, issuance will remain a prerogative of the monetary authority (see Section V.A).

Independent of the operating model, the onboarding and identification procedures, responsibilities and costs should be thoroughly analyzed. It is still hard to implement it using a straight through process, and the ECCB pilot, for example, relies on a two-tier system to reduce costs and risk. The Uruguay e-Peso pilot fully outsourced compliance with identification requirements to the user-facing payment system providers. There are several digital identity solutions that central banks could leverage to strengthen the implementation of identification requirements in the context of CBDC.

Central banks need to discuss scenarios under which invalidation and destruction would be required as the last two possible steps of the CBDC cycle (see above figure). For instance, court orders or suspicious activities may require temporary deactivation of CBDC user accounts or tokens that could be reactivated later, without necessarily going through destruction and recreation. It should be noted that some freezing measures could be mandatory and/or permanent for financial integrity purposes.[55]

Anticipating the possibility of destruction may support more profound changes to the CBDC. One example relates to changes of the technology underlying the CBDC should it become obsolete and require replacement. Another similar example may occur when a third-party provider with proprietary technology compromises the security or robustness of the CBDC, which would require switching the implementation partner. In both cases, a predictable process for CBDC destruction helps ensure business continuity and address unexpected challenges. This could be implemented in the database level, with a status indicator, or in the context of DLT-based systems, the destruction could also be implemented through transferring CBDCs into a wallet that nobody has the private key and thus no possibility to transfer them out of it.

[55] For example, under UN Security Council Resolution 1373.

ANNEX 3. ADDITIONAL CYBERSECURITY CONSIDERATIONS

The business and process layer

Security risks within the business layer could result in vulnerabilities and design flaws which could lead to security breaches and loss of trust. Key concerns include node protection, brute-force and availability disruption. To mitigate such risks, stakeholders - business and IT - should analyze each process/use-case to design the CBDC ecosystem with the mindset of defense-in-depth; while defining precisely each participant's role and activities and applying security methodologies like least-privilege and need-to-know bases accordingly. A retail CBDC's wide availability makes it more exposed to abuse of privileged access to the backend systems, if poorly designed.

The development, update and maintenance process of the CBDC platform carries a different set of security concerns. Failure to protect and monitor the source-code could lead to the injection of malicious code into the backend or interfaces of the CBDC systems.[56] It is important that the source-code for the backend and interfaces applications be monitored and protected, and access and modifications be restricted through proper process and security controls. In addition, third-party libraries should systematically be examined for malicious code or vulnerabilities before integration, and before applying updates.

Cyber sovereignty risk should also be considered during the design and planning phases where the IT infrastructure of the entire country could be attacked and brought down by external actors; as a result, any CBDC could be brought down or rendered partially dysfunctional.

The infrastructure and application layer

A key decision is whether the CBDC network, servers, databases and data should be deployed within their own datacenter or a cloud/third party provider's network. In the case of an external-hosted CBDC model, the CBDC will have to be planned and designed around some model-specific security risks. For example, the insider threat is a risk to both deployment methods, but it may be more prominent with an externally-hosted CBDC.[57]

Data sovereignty should also be considered during the design and planning phases of CBDC. This is because sensitive, and possibly personal data processed/stored within a foreign cloud provider could likely end up outside the central bank's country borders. In consequence, this data may be subject to the laws and legal jurisdiction of other countries and could be summoned and disclosed to other governments without the issuing central bank's approval or knowledge.

[56] An example of such a breach was the "NotPetya" outbreak in which malicious hackers gained access to the source-code repository of a software product widely used by financial institutions (Schwartz, 2017). The hackers injected malicious code to implement a backdoor within the application to access it remotely and infiltrate the banks' networks.

[57] Trade.io occurred when an insider stole their private keys to the hot and cold wallets where $7.5 million were stolen (SwiftSafe, 2018). Another example is Shapeshifter.io where an insider in collaboration with an external group stole 315 Bitcoins (Sirer, 2016).

Cloud-hosted CBDC can suffer from shared vulnerabilities within the cloud provider's systems, services and network components. These shared vulnerabilities can seriously undermine the integrity of the ledger and could lead to major CBDC disruptions or theft. One prominent example is the Cloudbleed vulnerability discovered in 2017 within Cloudflare, a widely used cloud provider (Prince, 2017). Cloudbleed impacted many customers and was a serious security risk to Cloudflare's customers and their sensitive data.

CBDC's physical layer, regardless of the hosting model, can suffer from hardware vulnerabilities. Although hardware vulnerabilities are rare; they tend to be severe and very difficult and costly to fix. Recent examples, discovered in early 2018, were the meltdown and spectre vulnerabilities in Intel x86 microprocessors (Schneier, 2018a).

The application layer is where most of the digital currency functions and processing take place. CBDC security concerns are focused around the exposed components like websites or web services etc. These interfaces are an attractive target for malicious users, especially administrative and privileged interfaces. Bitcoin Central reported a breach within their web interface where a malicious user was able to reset the privileged account password of their hosting provider and lock the exchange out of their website (Bradbury, 2013).

CBDC storage/backup and access of the encryption keys, or the authentication/ authorization secrets, are attractive targets for attackers. Most of the recent reported digital currency exchange breaches were due to improper storage and processing of private keys combined with poor system design. In the Coincheck 2018 breach, improper private key security processes resulted in more than $400 million in losses (Reuters, 2018). Risks of such breaches can be mitigated by emphasizing properly handling encryption keys during the CBDC design phase and giving appropriate guidance to end-users on how to protect and access their encryption keys or authentication/ authorization secrets.

Quantum computing is an evolving field and could pose a direct threat to encryption in general.[58] However, the threat is more prominent with asymmetric encryption algorithms, which is the core component for authentication and authorization in DLT-based platforms (Schneier, 2018b). Although quantum computing is in its early stages it is advancing rapidly so DLT-based platform encryption algorithms should be designed for future flexibility for when quantum computing becomes a threat. Research initiatives are already ongoing to develop *"post-quantum"* or *"quantum-safe"* cryptographic algorithms. The U.S. National Institute of Standards and Technology (NIST) has already short-listed 26 out of 69 candidates to the semifinals; a selection is expected to take place by 2024 (NIST, 2019).

[58] Quantum computing is based on the science of quantum physics; it introduces quantum bits (Qubits) instead of the conventional computing bits (0 and 1). Quantum computers operates by controlling the behavior of atoms (photons and electrons) and a Qubit can exist in a superposition between 0 and 1 which have the potential to enable tremendous efficiencies over conventional computers (Bernhardt, 2019).

ANNEX 4. BLOCKCHAIN PRIMER

Blockchain describes the format of a computerized ledger, in which valid transactions are organized in blocks. The blocks are cryptographically linked to each other in a chronological chain to ensure integrity even in an environment that the participants do not know each other (Mills and others, 2016). Only new blocks can be added to the chain, and as a verified block has been added it cannot be changed or deleted, rendering the chain immutable. Transactions are broadcast real-time across the network of participants, which eliminates the need for reconciliation or intermediation. This can reduce settlement time, lower back-office costs, and secure data transmission (Casey, 2018).

Broadly speaking, blockchain networks can be categorized along two dimensions; who can access the network and who validates transactions.

- On a *public* blockchain access and interaction with the network is unrestricted and the identity of its participants is semi-anonymous. (Although the identity of network participants is not disclosed it can be ascertained based on a participant's internet protocol (IP) address, location, and other identifying meta data.[59]) *Consortium* blockchain access, on the other hand, is granted only to selected participants. *Private* blockchains keep write permissions to one entity, although read permissions may be more open.
- In a *permissionless* network anyone can participate in validating transactions in contrast to only selected participants within a *permissioned* network. Validation is the process that ensures that all participating nodes[60] are synchronized and in agreement on the legitimacy of added transaction blocks. Consensus must be reached after each new block is added, and only after that can the block be considered immutable. Depending on the design, this could lead to finality uncertainty in the meantime (U.K. 2016; Mills and others, 2016; ECB 2016; Deloitte 2016).

The more restricted the network (private, permissioned) the more it looks like traditional centralized systems. The choice between permissionless and permissioned networks center around the ability to create trust among network participants and the ability to scale.

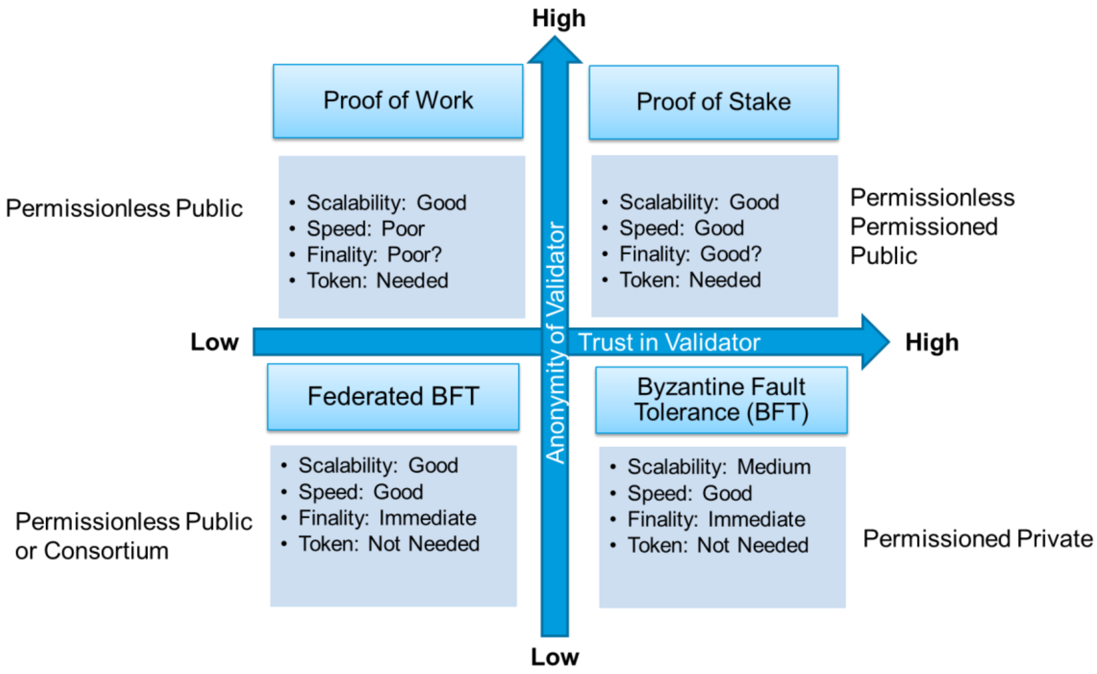
- Permissionless platforms offer opportunities for full disintermediation but creating trust among network participants through cryptographic verification and synchronization can require high computational power. The increased computational power translates into higher energy consumption and lower throughput, which inhibits the ability to scale.
- Permissioned platforms are based on relatively simple consensus mechanisms, since only approved participants can update the ledger. However, they are more susceptible to cyber-attacks than permissionless platforms, because it takes the compromise of

[59] Meta data is set of data that describes or gives information about other data.

[60] A node can be any active electronic device, including a computer, phone or even a printer, as long as it is connected to the internet and has an IP address. The role of a node is to support the network by maintaining a copy of a blockchain and, in some cases, to process and validate transactions.

only one trusted node were to bring down the network. Also, a centralized authority must determine which consensus to use, how many nodes should participate in the network and who authorizes new nodes. In addition, someone must (determine and) validate cybersecurity requirements, and decide when to upgrade and validate the code.

Public, Private and Permissioned Blockchains



Source: Kalisko 2018.

The type of consensus mechanism will depend on whether a permissioned or permission less blockchain platform is chosen.

- *Practical Byzantine Fault Tolerance (PBFT)* is the most popular permissioned blockchain consensus protocol. It can reach a consensus on the validation of transactions despite the potential existence of malicious nodes in the system that are failing or propagating incorrect information to the network. A consensus decision is determined based on a majority vote submitted by all participating nodes. The objective is to defend against system failures by mitigating the malicious activities by hostile nodes that aim at impeding the correct functioning of the network. However, the PBFT protocol works only on a permissioned blockchain because there is no anonymity.
- *Proof of Work (PoW)* protocol is the most common consensus mechanism among permissionless blockchains like Bitcoin. “Miners” compete to solve a cryptographic puzzle to add the next block to the chain. The first miner to solve the puzzle, receives a transaction fee and rewards in the form of newly minted crypto assets. This consensus mechanism requires high amounts of energy consumption. Another

challenge is the lengthy time it takes for transaction confirmation ("finality") which for Bitcoin can be up to 60 minutes.

- *Proof of Stake (PoS)* consensus mechanisms were designed for public blockchains with a view to overcoming the challenges of PoW, particularly regarding the high energy consumption. Rather than competing through their computational power, miners buy stakes in coins at inception. The probability of being selected to validate the next block depends on the number of coins at stake. The validating node receives a processing fee, but no new coins are created. Although the PoS is more energy efficient and provides better finality, only the nodes with the highest stakes are permitted to have control of consensus. This can lead to centralization of consensus power, which promotes inequality among participants and exposes the network to vulnerabilities - one single malicious node with enough stake needs to use only financial means to potentially destroy the network (Jenks, 2018).

Several DLT wholesale CBDC implementations have been tested by central banks on payments and settlements systems (see table).[61] The main DLT implementations are Hyperledger Fabric, Quorum and R3 Corda. Compared to public ones such as Bitcoin or Ethereum, they are designed for financial services or cross-industry use with features such as transaction confidentiality, high scalability and governance, etc. Among them, the differences are mainly in the implementations of the data privacy, smart contract languages, consensus rules and cross-ledger interoperability such as Hashed Time-Locked Contracts.[62]

[61] See also Shabsigh and others (2020) for a review of DLT experiments in payments and settlements systems.

[62] "Hashed Time-Locked Contracts synchronize all the actions making up a payment, so that either they all happen, or none happen. This is achieved through the use of smart contracts on the two DLT platforms to lock or encumber the assets to be transferred, complete transactions on both platforms when a common secret is used or release the locked or encumbered asset on both platforms back to their original owners if the common secret is not used within the pre-agreed time period, i.e., upon timeout… Smart contracts are self-executing computer programs that perform predefined tasks based on a predefined set of criteria or conditions. Smart contracts cannot be altered once deployed, which ensures the faithful completion of contractual terms" (BoC/MAS, 2019).

Central Bank Payment System Experiments with Wholesale CBDC

Central Bank	Project	Platform
Bank of Canada	Project Jasper Phase 1	Ethereum
	Project Jasper Phase 2	R3 Corda
	Project Jasper Phase 3	R3 Corda
	Project Jasper-Ubin	R3 Corda & Quorum
Banque de France	n/a	n/a
European Central Bank (ECB) & Bank of Japan (BoJ)	Project Stella Phase 1	Hyperledger Fabric
	Project Stella Phase 2	R3 Corda Elements Hyperledger Fabric
	Project Stella Phase 3	Hyperledger Fabric
Hong Kong Monetary Authority (HKMA) & Bank of Thailand (BoT)	Project Inthanon-LionRock	R3 Corda
Saudi Arabian Monetary Authority and the United Arab Emirates Central Bank	Project Aber	Hyperledger Fabric
Monetary Authority of Singapore	Project Ubin Phase 1	R3 Corda
	Project Ubin Phase 2	Hyperledger Fabric & Quorum
South Africa Reserve Bank	Project Khokha	Quorum
Bank of Thailand	Project Inthanon Phase 1	R3 Corda
	Project Inthanon Phase 1	R3 Corda

Sources:
Bank of Canada. 2017. “Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement.”
----. 2017. “Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement.”
----. 2018. “Jasper Phase III: Securities Settlement Using Distributed Ledger Technology.”
Bank of Canada and Monetary Authority of Singapore. 2019. “Jasper-Ubin Design Paper : Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies.”
Banque de France. 2020. “Central Bank Digital Currency Experiments with the Banque de France: Call for Applications.”
ECB-BoJ. 2017. "Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment."
---. 2018. “Securities Settlement Systems: Delivery-versus-Payment in a Distributed Ledger Environment.”
---. 2019. “Synchronized Cross-Border Payment.”
HKMA-BoT. 2020. “Project Inthanon-LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments.”
Saudi Arabian Monetary Authority. 2019. “A Statement on Launching “Aber” Project, the Common Digital Currency between Saudi Arabian Monetary Authority (SAMA) and United Arab Emirates Central Bank (UAECB).”
Monetary Authority of Singapore. 2017. Project Ubin: SGD on Distributed Ledger.
South African Reserve Bank. 2018. “Project Khokha: Exploring the Use of Distributed Ledger Technology for Interbank Payments Settlement in South Africa.”
Bank of Thailand. 2019. “Project Inthanon: An application of Distributed Ledger Technology for a Decentralised Real Time Gross Settlement system using Wholesale Central Bank Digital Currency.”
Bank of Thailand. 2019. “Project Inthanon: Enhancing Bond Lifecycle Functionalities & Programmable Compliance Using Distributed Ledger Technology.”