# Design Handbook for Central Bank Digital Currencies

Jeremy Clark
j.clark@concordia.ca
Concordia University

## ABSTRACT

Central banks around the world are evaluating the option of issuing a centrally banked digital currency (CBDC). There are a number of policy objectives attributed to offering a CBDC. Curiously, some of the stated objectives are contradictory. This confusion is a consequence of a very broad design landscape, which runs contrary to the conventional wisdom that suggests CBDCs can be broken into 2 or 4 main categories. In this paper, we systematically iterate through 8 key design decisions, most of which have 3 or more possible designs. Our design landscape is based on dozens of whitepapers and technical reports issued by central banks, international financial institutions, and technology firms.[1] By laying out a comprehensive set of options, we offer central banks a finer grained approach to tailoring a design that meets their specific objectives—objectives that will change from country to country.

## CCS CONCEPTS

• **Information systems → Digital cash**.

## 1 INTRODUCTORY REMARKS

Central banks have weighed the benefits of offering a central bank digital currency (CBDC) since the 1990s [6]. In recent years, interest has increased materially with 80% of surveyed central banks reporting engagement in CBDC work [17]. This seems due to (1) the emergence of Bitcoin and other blockchain-based financial technologies, (2) the declining use of banknotes, and (3) interest in direct stimulus policies. As an example of the latter, lawmakers in the US in early 2020 proposed a digital US dollar (months after scrutinizing Facebook's intentions for the Libra cryptocurrency) in draft legislation—a CBDC intended to directly distribute stimulus payments to US residents during the COVID-19 pandemic [20].

The purpose of this paper is to comprehensively explore the design landscape of a CBDC, showcasing the many possible configurations. This study does not take a normative position that a CBDC ought to be deployed in a modern economy, nor does it argue for a particular design, but rather provides a positive iteration of the design possibilities. We also briefly discuss the link between designs and their policy implications, outline some new issues for CBDC designers (such as a usability trilemma), and how design decisions can influence the potential impact of CBDCs on commercial banks.

### 1.1 Existing CBDC Categorizations

Early classifications of CBDCs were proposed by CPMI [7] and Bjerg [16], and subsequently merged by Bech and Garrett [14] to produce a Venn diagram of money and payment systems (called the 'money flower') with four sets: *electronic*, *universally accessible*, *issued by a central bank*, and *peer-to-peer*. Note that Bech and Garrett study central bank *cryptocurrencies* (as opposed to *digital currencies*) where the former are peer-to-peer by definition. Consequently they find two designs: both are centrally banked, electronic, peer-to-peer money but they differ in whether the currency is offered only to firms that are members of the central bank (*wholesale*) or to all participants in the economy (*retail*).

A second CBDC distinction was popularized by the central bank of Sweden, which was working through an actual design [72, 73]. It split CBDCs into designs that maintain account balances in online databases, and ones that enable offline transfers of units of value. The wording for these two designs evolved over time—respectively from *register-based* to *account-based* for the first; and from *value-based* and *prepaid* to *token-based* for the second [34, 55, 72]. Contemporary reports consider combinations of retail/wholesale and account-/token-based (*e.g.*, [11, 12]). Recently, the central bank of Lithuania suggests a third addition: *interest-bearing* [45].

While these classifications provide granularity, independent design decisions are still bundled together. To illustrate, a *token-based* design often presumes retail services to the public with anonymous cash-like payments via offline secure hardware, while a *account-based* design might consider an online distributed ledger systems for a member bank's interest-bearing reserve accounts. In actuality, the choice between a centralized or distributed ledger can be combined with different levels of anonymity, with different technical deployments, the choice of interest payments, and the choice of who the central bank offers accounts to.

Concurrently to writing this paper, Auer and Böhme provide an approach much closer to our own contribution. They consider CBDC designs in four levels of a pyramid: starting at the base, the *architecture*, the *infrastructure*, *account-/token-based*, and *support for international payments*. This presentation still bundles together issues we believe should be separated (for example, their *architecture* level combines three of our design parameters: unit of value, distribution structures, onboarding) however they do identify all significant categories of CBDCs that we found (with one notable exception: they do not discuss if designs are *interest-bearing* or not, which is important for a number of policy reasons we will describe). We would highly recommend their paper to a general readership and policy makers, while maintaining that our paper is still useful

[1] URL omitted: categorized Zotero library


*Working Draft, 2020, Concordia*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

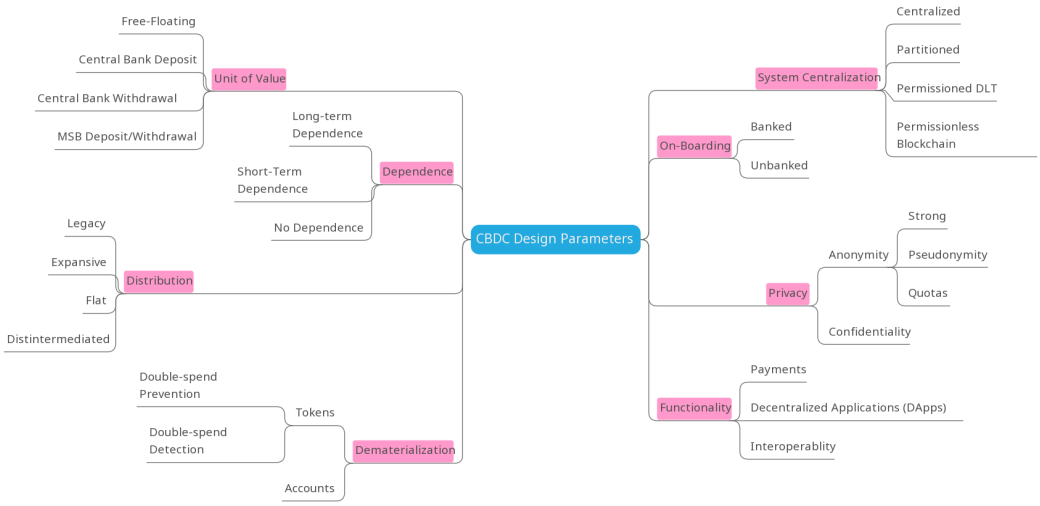



**Figure 1: An overview of the CBDC design landscape**

for even further detail and design parameters,[2] and perhaps better suited for a technical audience.

## 1.2 Misconceptions

CBDC commentary is hindered by design presumptions. Our work reiterates the important point that CBDCs have a broad design landscape, and there is not much that can be assumed beyond what the name CBDC itself already implies: it is digital and the central bank plays a role. Everything else, including the examples below, cannot be assumed:

(1) **Retail Service**: A CBDC could result in the central bank offering accounts to the general public or it could maintain closed membership or somewhere in between.
(2) **Banknotes**: A CBDC might compete with (and possibly replace) banknotes or it might compliment banknotes by appealing to a different set of customer needs.
(3) **Privacy**: A CBDC could be as private as banknotes or a traceable as commercial bank payment systems or somewhere in between.
(4) **Negative Interest Rates**: A CBDC could be interest bearing which would affirm a negative interest rate policy (NIRP) or it could be drawn down like a banknote and provide a low-friction safe haven from negative interest rates, directly impeding NIRP.
(5) **Blockchain**: A CBDC could be decentralized using distributed ledger (DLT) or blockchain technology, or it could be run on a centralized datacenter overseen by the central bank.

To illustrate this with an example, economist Lawrence H. Wight argues in the Washington Post that a CBDC is not in the public interest [59]. However he presumes the CBDC is interest bearing (and NIRP-affirming), offered directly to the public, and has no privacy. His real argument is that a CBDC of this particular design is not in the public interest, but the reader is unsure of his expert opinion on a CBDC of any different design (*e.g.,* a privacy-enhanced CBDC distributed indirectly to the public through commercial banks). A secondary intention for this paper is to nudge experts to argue directly about the design parameters. Which, if any, are required for a CBDC to be acceptable? Which, maybe all, result in a CBDC that is unacceptable?

[2]For the reviewer's consideration (and not to be included in the final paper), some specific inclusions found in our paper include interest-bearing CBDCs, negative interest rates, blockchain scalability solutions, enabling DApps, expanding central bank membership, impact on open market operations, and impact on the future of banknotes.

## 1.3 Preliminaries

*Central Banks.* For historic reasons, the services provided by a typical central bank has expanded and evolved. Among these services, they provide reserve accounts to commercial banks and other members (including the government) which are paid interest at the deposit rate. The bank will also typically facilitate Inter-bank payments and lending, using these accounts for final settlement. In this paper, we will discuss the reserve accounts of *commercial banks*, as well as considering the broader set of financial and technical institutes as *money service businesses (MSBs)* which could hypothetically become members of the central bank or find themselves regulated by the central bank.

*Physical and Digital Currency.* We assume the central bank issues and manages a fiat governmental currency, such as the US Dollar: USD. Like any sovereign currency, USD can exist in different forms. To keep the discussion simple, we consider two forms of USD: (1) banknotes and coins that are in circulation; and (2) USD that is deposited at the central bank by commercial banks. The first form is physical and the second is already effectively a digital currency.

# 2 UNIT OF VALUE

In this and the following sections, we break down the key design parameters of a CBDC (an overview is given in Figure 1), while considering the relative strengths and weaknesses of each. The first

design parameter is a foundational one from a finance perspective: what does a unit of a CBDC (which we will call dUSD for digital USD) actually represent? Among all the options, we highlight 4 key approaches, summarized in Table 1.

## 2.1 Free-floating

A central bank could maintain dUSD as an independent currency from USD allowing the exchange rate to float. If dUSD is managed with similar operational targets (*e.g.,* short-term market interest rates), they might maintain relative parity. However if material differences emerge between how and when dUSD is used by firms and consumers, as opposed to USD, their values are likely to diverge (this can arise under other circumstances as well; *e.g.,* quantitative limits on dUSD [31]). Further, commercial banks might opt to never loan dUSD, nullifying interest-rate targeting as a monetary policy.

A central bank deploying a free-floating design would have to be confident it could manage the currency even if it was restricted to only managing the currency by setting the quantity of money. Unfortunately this operational approach—using quantitative targets—has been tried historically by central banks and has been largely abandoned across the world for several decades [53]. On the positive side, managing two distinct currencies used for different purposes within the same market provides the central bank with another degree of flexibility. A central bank wanting to target efforts at easing credit to specific sectors might to choose to act within only one of its two currencies, USD or dUSD.

The Marshall Islands, which has no central bank and uses USD, is developing a free-floating sovereign digital currency (on the Algorand [42] DLT) to temper USD usage [69]. RSCoin is a technical proposal for a DLT-based CBDC that enables central banks to issue free-floating independent digital currencies [33].[3]

## 2.2 Central Bank Deposit & Withdrawal

In the next two designs, any member of the central bank can exchange USD deposits with dUSD (and vice-versa) on demand. This low-friction convertibility between dUSD and USD, guaranteed by the central bank, results in parity between the value of dUSD and USD. The difference between these two designs is a philosophical one: (1) should the dUSD be treated like it is still on deposit at the central bank where it earns interest (which we call the *central bank deposit* design), or (2) or should dUSD be like treated like a digital banknote that has been drawn down from the account and does not earn interest (which we call the *central bank withdrawal* design).

A deposit design requires interest payments on dUSD at the reserve rate (or another rate [36]). Since a CBDC is likely to operate as a 24/7 payment system (no overnight holding) with real-time settlement (dUSD can change hands many times over a period of time), when and to whom an interest payment is made will need careful specification, as well as the conduit for the payment itself: in dUSD, in USD, from capital, or through money creation.

It appears on first glance that a deposit design implies that dUSD can only be held by members of the central bank, and raises the question of whether the central bank should offer membership to the general public. We address this in section 4. For now, we point out that all customers could accept and transact in dUSD even without an account at the central bank, knowing that the dUSD will eventually flow back to an entity with an account.

Consider if Alice (with no central bank membership) is given dUSD by AB&C Bank (with central bank membership). Trivially, she can hold it on deposit at AB&C—as a consequence, the dUSD is a liability of AB&C not the central bank. However if the CBDC system allows anyone to create a bank number (or blockchain address), Alice could hold dUSD as a liability of the central bank without having the full member services of the central bank. The central bank could send dUSD interest payments directly to any holder of dUSD even if it knows nothing beyond the account number/address (this style of payment is called an *airdrop* by cryptocurrency enthusiasts). This challenges the notion of what it means to 'have an account' at the central bank. It is possible for the central bank to onboard users who have registered with its members and not provide any service beyond that (discussed further in section 7).

One of the earliest CBDC proposals, FedCoin [49], proposes the deposit design. Broadbent argues the more a CBDC resembles a deposit, the greater the competition with commercial bank deposits (and conversely with banknotes) [21]. Sweden's Riksbank e-krona concept discusses the option of interest at length, outlining expected impacts on the commercial banking sector [72, 73]. Engert and Fung distinguish the withdrawal model (called the benchmark CBDC) from the deposit model (called I-CBDC) and discuss interest rate policies for I-CBDC [36].

## 2.3 MSB Issuance

In the fourth unit of account type, dUSD is issued by a commercial bank or MSB instead of the central bank. While such dUSD is a claim on the commercial bank instead of the central bank (and arguably not a **CB**DC), the central bank could still play a key role. For example, the central bank could provide regulatory oversight and require authorization to issue dUSD. With lighter regulation, dUSD could be converted to/from commercial bank deposits. With stronger regulation, dUSD would only be issued if the commercial bank increases their balance in a segregated reserve account (*cf.* DDR [62]) at the central bank—the commercial bank would operate as a full reserve (or narrow) bank with respect to their dUSD issuance. While not technically a liability of the central bank, such dUSD would be isolated from any liquidity or solvency issues at the commercial bank.

dUSD would be redeemable at the issuing bank and the system could be regulated so that dUSD is redeemable at any bank. Operationally, it could be that Bob redeems his dUSD (originally issued by AB&C to Alice) for a USD deposit at his own bank XY&Z, and XY&Z either holds the dUSD, or exchanges the dUSD with AB&C for the equivalent central bank reserves using an interbank payment. Ideally the exchange of dUSD and reserves could happen atomically (delivery on payment) which is possible given that both are digital forms of money.

In its least regulated form, MSB issuance does not rely on the central bank at all. Thus, there is no technical barrier (only regulatory barriers [38]) to a commercial bank or MSB implementing it at any time. The earliest experiments with digital cash, such as

[3] We note that RSCoin is a general framework that could implement any of the designs in this section and that the authors only briefly discuss how currency is issued, however a free-floating CBDC seems to be the design intent.

| Unit of Value | Enactable by | Description | CB Role: System provider | CB Role: Issuer | CB Role: Oversight |
|---|---|---|---|---|---|
| Free-Floating | RSCoin [33] | The digital currency is managed by the central bank but is not directly tied to the governmental currency | • | • | • |
| Central Bank Deposit | Fedcoin [49], DDR [62], Account-based e-krona [72, 73] | 1 dUSD is equivalent in value to 1 USD that is currently deposited in an account with the central bank. An owner of 1 dUSD is entitled to the interest that would be paid at the bank's deposit rate. An owner of 1 dUSD can redeem it for a deposit of 1 USD into their reserve account at the central bank. | • | • | • |
| Central Bank Withdrawal | Value-based e-krona [72, 73] | 1 dUSD is equivalent in value to 1 USD that has been withdrawn from an account with the central bank. An owner of 1 dUSD can redeem it for a deposit of 1 USD into their reserve account at the central bank. | | • | • |
| MSB Issuance | Digicash [28], Liberty Reserve [65], 'Stablecoins' [30], JPM Coin [44] | The same as *central bank deposit/withdrawal* above except that the CBDC is issued by member banks or MSBs instead of the central bank. The central bank does not play an active role. It only provides regulatory oversight. | | | • |

**Table 1: Summary of a variety of approaches to defining the unit of value in a CBDC and the role of the central bank under each definition. Provided examples are (past and present) technologies well-suited for each.**

DigiCash's cyberbucks in the mid-1990s (offered legally in the US by a single bank in St. Louis) follow this design [65], as did a number of unregulated digital currencies like Liberty Reserve (although Liberty Reserve used a decentralized network of "exchangers" to interface with customers and merchants). In the post-Bitcoin era of cryptocurrencies, a number of MSB projects (including Tether and the proposal Libra) are pursuing this design under the moniker of stablecoins [30], as are some banks (including JP Morgan [44]).

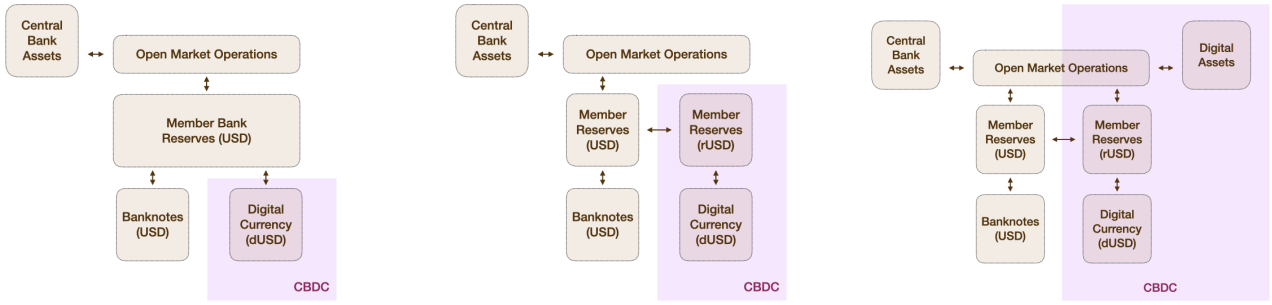
## 2.4 Discussion

Based on the commercial bank literature, a *free-floating* CBDC appears unpopular with countries with their own established currencies. For a central bank that wants a digital currency in circulation but also wants to minimize changes to itself, an *MSB-issued* digital currency that is fully backed by segregated central bank reserves offloads nearly all the technical challenges to commercial banks and MSBs. The central bank expands its oversight, and perhaps membership to other financial, technology or retail firms (see section 4), but otherwise incurs minimal changes.

The most popular option is either the *central bank deposit* or *central bank withdrawal* design. In fact, these are not mutually exclusive. A hybrid design could enable both an interest-bearing deposit-like currency (to avoid overloading terminology, call this rUSD for reserves) and a cash-like currency (dUSD). It could be that rUSD is on the same CBDC technological system as dUSD but is otherwise no different from current reserve accounts: rUSD is interest-bearing, ledger-based, and can only be transferred between members of the central bank (we revisit this in section 4). From the perspective of the central bank's balance sheet, reserves, banknotes, rUSD, and dUSD are all listed as liabilities, and conversions do not grow or shrink the balance sheet.

In a hybrid model, commercial banks with rUSD reserves can autonomously convert and withdraw it as dUSD. The bank's customers can hold dUSD directly (as a liability of the central bank) or keep it on deposit with the commercial bank (as a liability of the commercial bank) to earn interest. The commercial bank can recursively apply the same hybrid design by issuing a new interest-earning rUSD-esque token (say AB&C-rUSD) to its customer. This allows the commercial bank to operate fractionally by using the dUSD (*e.g.,* for lending) while giving the customer a digital representation of their dUSD that can be used for payments without 'withdrawing' the dUSD. This approach is used by decentralized finance (DeFi) services on Ethereum such as Compound [54]. The advantage for the central bank in such a system is real-time data for the composition of the (digital) money in the economy (*i.e.,* MB, M0 and M1 for the CBDC including commercial bank deposits).

Central banks generate significant income from money creation (*seigniorage*). Creating new reserves has negligible marginal cost but offering an interest rate offsets the income. Banknotes have a production cost but it is smaller than the face value of the bill and banknotes do not incur interest—generally, they produce greater seigniorage [66]. A CBDC will have a high overhead cost to deploy the system, but the marginal cost of producing money will be negligible. For a central bank withdrawal design, dUSD is cheaper to produce than a banknote and does not pay interest, so a positive impact on seigniorage is expected [31, 55]. For a central bank deposit design, seigniorage will be similar to reserves (neutral impact on seigniorage) but may draw customers away from banknotes (negative impact).




**(a) Long-term dependence** **(b) Short-term dependence** **(c) Futuristic**

**Figure 2: Dependence models illustrated with a hybrid (central bank deposit and withdrawal) unit of account.**

## 3 FUTURE DEPENDENCE

The next design parameter considers whether the CBDC should be a sub-component of the bank's existing operations or if it should be an alternative implementation. This is closely related to the unit of value illustrated in the previous section. As of 2020, a quarter of surveyed central banks have or are in the process of being granted legal authority to issue a CBDC [17].

In an *independent design*, dUSD (and possibly rUSD) are issued independently of how the central bank creates USD reserves. In a *long-term dependent* design, dUSD is issued from USD reserves (see figure 2). A withdrawal design leads to long-term dependence. A hybrid design is also dependent on USD reserves initially for issuing rUSD and dUSD however it is *short-term dependent* as USD reserves could be completely phased out in favour of rUSD. It becomes possible that the bank's asset purchases and sales could be conducted directly with the CBDC, as well as its lending facilities. It is even possible (*futuristic*) that the assets themselves could be tokenized within the CBDC system, offering atomic delivery of the asset on payment, both for the central bank and its members, for use in open market operations and in accepting collateral for rUSD loans (*i.e.,* through a reverse repurchase agreement).

### 3.1 Discussion

A central bank interested in issuing a CBDC itself, but otherwise incurring minimal technological changes should opt for long-term dependence. However for greater flexibility moving forward, short-term dependence allows the CBDC to be gracefully degraded if it does not prove useful over time, while also allowing the CBDC to gracefully overtake the current system and replace it with an alternative technological stack. Further, providing a common technical environment for digital assets, collateral, reserves, and currency can allow efficient financial operations for the central bank and its members.

For advocates of banknotes, dependence might sound like a pledge for the continuing issuance of banknotes and coins. However as seen in Figure 2, dUSD and banknotes are always substitutable, regardless of dependence.

The third phase of the Bank of Canada's Project Jasper considers the delivery of securities within a blockchain-based payment system, settled with member's reserves at the central bank [74]. This design is long-term dependent as payments require pledged reserves, but it is technically similar to the upper (rUSD and digital asset) portion of the futuristic design—although designed for member banks to purchase securities rather than the central bank, which tends to purchase bonds.

## 4 DISTRIBUTION STRUCTURES

The next design parameter is how to distribute the CBDC to those allowed to hold it. The options are provided in Figure 3.

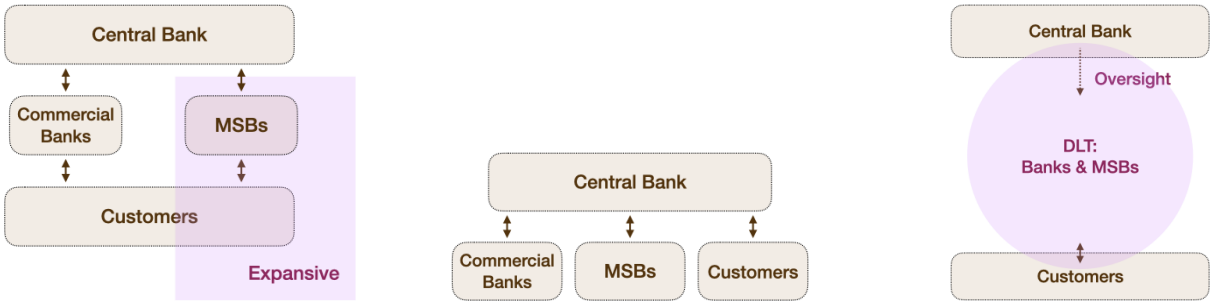
### 4.1 Legacy / Expansive Hierarchy

In the *legacy hierarchy*, dUSD (or rUSD) would be distributed in the same way as banknotes. Membership in the central bank would not change, and members could exchange reserve dollars and dUSD with the central bank. dUSD would be distributed from the members (*e.g.,* commercial banks) to its customers. The CBDC might require *tiered payments* between customers (routed from the sender's commercial bank to the receiver's via the central bank [2]) or the CBDC might allow *bilateral payments* between dUSD holders. A legacy hierarchy is appears in Engert and Fung's benchmark CBDC [36], as well as in the ensuing literature.

In an *expansive* variant, the central bank would expand its members to a broader assortment of firms: fintech, web, technology (an early suggestion by Broadbent [21]). These firms would meet the basic requirements of being registered money service businesses (MSBs) and would compete with commercial banks in providing public-facing dUSD financial services. In both cases, a *wholesale* variant is possible where dUSD (or more likely rUSD in a hybrid system) is distributed to the central bank members and can only be transferred between members.

### 4.2 Flat Hierarchy

In a *flat hierarchy*, residents or the general public would be able to open accounts with the central bank (initially proposed by Tobin [75] years before CBDCs as a safer alternative to commercial bank accounts). With a CBDC, customers would receive dUSD (and/or rUSD). From the customer's perspective, rUSD is preferable when interest rates are positive and dUSD if interest rates were ever negative. To prevent mass conversions between them during financial crises, it seems prudent that a central bank would offer only one to the general public.




(a) Legacy / Expansive (b) Flat (c) Disintermediated

**Figure 3: Distribution structures**

It is important distinguish between being able to: (a) hold CBDC without a central bank account, (b) have an account and basic services of the central bank, and (c) being a full-fledged member of the central bank. The term *retail CBDC* is often used interchangeably for any, while *general purpose* is used for (a) [17]. Note that only (b) and (c) imply a flat hierarchy, while (a) can be accomplished with any distribution method.

### 4.3 Disintermediated Hierarchy

In the *disintermediated hierarchy*, banks and MSB would run distributed ledger technology (DLT), or blockchain technology, between themselves, disintermediating the central bank from digital money creation (except for regulatory oversight). The central bank could continue to offer reserve accounts, banknotes, and payments. Money creation, on the CBDC side, would be done by the banks and MSBs (using an MSB issuance design) and dUSD would be backed by USD held in deposits (long-term dependence). This could form a strongly regulated version of what has become the status quo in blockchain technology where directly-backed stablecoins are offered by MSBs that are not always regulated, and backing funds are generally held in commercial banks or with other custodians.

### 4.4 Discussion

The expansive hierarchy seems to strike a balance between fostering innovation within digital currency services while maintaining a largely traditional role for the central bank. Note that DLT/blockchain technology can be used for payments, even if distribution is centralized (see Section 6) within an expansive hierarchy. A flat hierarchy introduces a massive expansion of central bank services to service customers across the country, and authorize new accounts, in a regulatory compliant way (respecting financial reporting and KYC/AML provisions) that is already largely solved by commercial banks [36].

Where a disintermediated hierarchy attracts attention is one level higher—in international finance. Central banks could form an interoperable decentralized ledger for international payments between central banks (and thus indirectly between the central bank's member banks) using their own nationally-issued digital currencies as the unit of account. This was termed a synthetic hegemonic currency (SHC) by then governor of the Bank of England [26]. The Fnality consortium (*née* Utility Settlement Coin), currently consisting of many large international financial institutions, is also pursuing disintermediated international payments, only bilaterally without central banks.

## 5 DEMATERIALIZATION

The next design parameter considers the format of the digital currency. Among the options, two basic categories are *token-based* and *account-based*. In the token-based design, dUSD is held like a digital banknote by the customers themselves, requiring some sort of secure electronic device. In the account-based design, dUSD balances are recorded in an online database (or ledger, whether centralized or decentralized—see section 6) and payments require a connection to the database.

### 5.1 Tokens

A token-based design tries to digitally replicate a banknote. In its purest form, tokens can be transferred electronically from customer to customer without any third party involvement. The challenge of any token-based design is solving the *double-spend problem* where a customer sends the same token over and over to multiple recipients.

To prevent double-spending, a token-based CBDC requires tamper-resistant memory. This could be specialized hardware—*e.g.,* smart cards and readers—or it could be situated in common digital devices—*e.g.,* phones and computers with security augmentation. A lightweight mitigation of double-spending is to not *prevent* it but just *detect* it (after the fact) and then use legal penalties for the perpetrator. Bank cheques operate under the principle of detection rather than prevention. Detection can be used alone, or as a fallback mechanism for a prevention-based approach. With double-spend prevention, transactions can be conducted offline assuming both the sender and receiver have compatible secure hardware. With detection, generally offline transactions require a later online reconciliation.

### 5.2 Accounts

In an account-based system, balances and transactions are recorded in a database or ledger. Transactions are conducted online with the sender (and potentially the receiver) forming an authenticated connection to the database and authorizing the payment. Transactions

that do not span multiple databases or authorities can generally be validated and finalization near-instantenously.

### 5.3 Discussion

To a certain extent, the difference between tokens and accounts is a spectrum not a binary choice. Coins are pure tokens. Banknotes are tokens but have serial numbers that correspond to ledger entries. A gift card can be given from Alice to Bob like a token but it requires online activation, pre-payment, and Bob can never be sure Alice does not know the secret required to spend it (*e.g.,* scratch-offs can be removed and reapplied). Cryptocurrencies (*e.g.,* Bitcoin) are account-based but can support offline transactions for pre-paid payments (*e.g.,* the Lightning Network).

Tokens have intrinsic advantages. They can operate in an offline world and have no limit (other than physical limits) on the number of transactions per second. If there is no reconciliation of transactions, they enable strong privacy.

The core issue with tokens is security. Can hardware be hardened enough to be truly uncloneable and tamperproof? The common answer from decades of cybersecurity research on e-cash pilots to metro cards is no [3, 22, 39, 40, 48, 68]. Tampering attacks have largely relegated token-based public payment systems to deployments with low value or pre-paid transactions. The technology is not suitable for a widely-held currency with large value transactions.

It is also important to consider the consequences of a security breach of the customer's card or device. In a token-based design, an adversary could print unlimited amounts of currency—a *wholesale attack* that compromises the entire currency. In an account-based system, if hardware is used to authenticate the user, the breach only effects the victim (a *retail attack*). Of course, there is a wholesale attack on account-based systems too: attacking the database. But the design does not put this critical aspect of the system into everyone's hands the way a token-based system does.

## 6 SYSTEM CENTRALIZATION

The next design parameter addresses system architecture with a focus on account-based designs. In table 2, we compare various security and scalability properties. Before our paper, these issues were scattered throughout dozens of whitepapers and technical reports on CBDCs but have never been systematized.

With an account-based design, the CBDC is essentially a database of users and account balances with routines for validating payments and incrementing/decrementing balances. As the authority over money creation, the central bank's participation in the system will be necessary. If the central bank maintains the entire system internally, we say it is *centralized*.

In contrast to a centralized system, the data and/or routines could be tasked to other participants. The literature uses inconsistent and evolving terminology (*e.g.,* distributed, decentralized, peer-to-peer, *etc.*) for such a system. We will examine two basic approaches. First, a *partitioned* design is where different participants each maintain a portion of the data independently. The second approach is a *distributed ledger (DLT)* design where all of the data is maintained together but multiple participants independently validate the data.

A DLT design can be subdivided according to who the participants are and what they can and cannot do (*i.e.,* their permissions) within the system. While DLT is a slightly more general term than a blockchain, they are largely interchangeable. We use the term DLT for a *permissioned* (or private, consortium) system and blockchain for a *permissionless* (or public) system.

*Illustration.* Before explaining each design, let us illustrate the design differences (especially between partitioned and DLT) with an example. Consider the account balances in deposit accounts (savings and chequing) across a country. This system is partitioned. The central bank maintains balances for and facilitates payments between commercial banks, while commercial banks internally manage their own balances and payments for their own customers. A customer-to-customer payment, for customers of different commercial banks, is not possible with a single transaction on a single ledger but routes through the systems of the sender's commercial bank, the central bank, and the recipient's commercial bank. A financial tracking agent authorized to obtain the full details of the transaction would have to obtain data from multiple sources.

By contrast, if account balances were centralized, the central bank would maintain all balances of all customers and settle all the payments between accounts. Commercial banks could continue to operate as today but they would forward all transactions to the central bank for execution, including simple transactions like a customer moving money from their chequing account to their savings account within the same commercial bank. Financial tracking could be initiated at the central bank alone. The central bank system would be a single point of failure should it ever become non-responsive or have its security breached.

In a blockchain design, the data is not partitioned and all balances of all commercial banks are stored on a common ledger, as in the centralized design. However the common data is shared amongst all participants (we set aside the privacy considerations of this for section 8). Payments can be proposed by any participant, including the customers themselves, and if enough participants agree that the payment is valid, everyone will update their copy of the shared database synchronously. Financial tracking agents can be participants and obtain transctional data directly (for identities, see section 7), it takes just one responsive participant to ensure the data is available, and certain cybersecurity attacks (such of processing invalid transactions) require many participants to be simultaneously compromised.

### 6.1 Centralized

In a *centralized* design, the central bank would maintain the CBDC database and use an internet-facing server to receive payment requests. In order for a customer to obtain dUSD, they would undergo an on-boarding process. We discuss the possible designs for this further in section 7. Assume the central bank maintains a list of customers permitted to send and receive payments. Once customers have payment permissions, they can receive dUSD from a bank, an MSB, or from another customer.

With reference to table 2, a centralized design enables the central bank to use technology that underlies the majority of the current financial market. Since the servers will be maintained internally within the bank, standard cybersecurity measures can be used to

| Architecture | Mature technology | Public transparency | Financial gain from a single breach is limited | Private data gained from a single breach is limited | Resistant to foreign influence | On-boarding of users can be load-balanced | Payment processing can be load-balanced | Law enforcement requests can be load-balanced | Resilient against server downtime | Does not require clients to reconcile data |
|---|---|---|---|---|---|---|---|---|---|---|
| | **Security** | | | | | **Scalability** | | | | |
| Centralized | ● | | | | ● | | ○ | | | |
| Partitioned | ● | | ○ | ○ | ● | ● | ● | ● | | |
| Permissioned DLT | | | ● | | ● | ● | ○ | ● | ● | ● |
| Permissionless Blockchain | | ● | ● | | | ● | ○ | ● | ● | ● |

**Table 2: An evaluation framework for the security and scalability properties of different centralization options for a CBDC. Precise evaluations depend on exact implementations, while this chart only makes generalized, 'out of the box' assumptions about each architecture. A ● symbol implies the property is fully satisfied, ○ implies it is partially satisfied, and while an empty space implies it is not satisfied. An ideal system would fully satisfy every property.**

maintain privacy and standard load-balancing techniques can be used to mitigate the high amounts of traffic. However since every payment is processed centrally, critical attention to reliability is necessary. Further, in the case of a breach, whether for financial gain or for obtaining private information (many examples of both kinds in the banking sector over decades), the attacker has access to a system of high value with a very broad dataset. Since the central bank maintains the data, they also are trusted with its integrity. Central banks are generally institutions of high public trust and leveraging this trust to simplify the technical aspects of the system might make centralization suitable. Member banks and customers will have to continue performing reconciliation of their records with the CBDC system.

In a centralized design, the bank will also have to handle inquiries from law enforcement, financial tracking, and other enforcement agencies for all customers, even the ones that are not actual members of the bank. As a digital system, access can be facilitated by an online request system (used by many web technology firms that collect personally identifiable information) but it is a new burden for central banks that needs to be weighed against the considerations of other possible system architectures.

## 6.2 Partitioned

In a *partitioned* design, the central bank would maintain balances and enable payments for its members only. Once dUSD was drawn down by a commercial bank or MSB, this member would take over large aspects of the technical system. A partitioned design can be accomplished today with minimal changes to the central bank under an MSB issuance design. The key challenge of a partitioned system is how much control does the central bank retain over dUSD once it has left he central bank.

In a token-based model, the central bank can distribute dUSD and be certain (within the security of the tokens) that all dUSD returning to the central bank is legitimate. In an account-based design, counterfeiting currency is as simple as increasing a balance in an account and so the central bank must perform a certain amount of tracking.

In an account-based partitioned design, the central bank maintains dUSD balances for commercial banks and MSBs, while these banks and MSBs maintain balances for their customers. If a customer of AB&C Bank sends dUSD to a customer of XY&Z Bank, the dUSD balances of AB&C and XY&Z would change on the central bank ledger, as well as the customers' balances on each commercial bank's ledger.

Partitioned designs use time-tested database technology where financial and privacy breaches and server downtime is limited to each commercial bank. Since commercial banks are authoritative over their records, and the central bank knows nothing beyond the total amount of dUSD their members hold, the burden of on-boarding users, processing intra-bank payments, and assisting authorized enforcement agencies can be spread out amongst the banks and MSBs. However since records are spread out and inter-bank payments involve different ledgers, records require reconciliation.

The defining feature of a partitioned system is that dUSD held by customers is a liability of their commercial bank, not the central bank. In order for dUSD to be a claim on the central bank, the central bank must maintain the balance for ever customer. This implies either a centralized design, or a design where *both* the commercial bank and the central bank maintain the data—a DLT design.

## 6.3 Permissioned DLT

In a *distributed ledger technology (DLT)* design, the central bank maintains the CBDC system jointly with other participants through

a network. Participation can be by invitation (*permissioned*) or open to anyone online (*permissionless blockchain*). The central bank can track every dUSD transaction, enabling dUSD to be a liability of the central bank—however the bank must validate every payment. As invited participants, member banks and MSBs can on-board users and address authorized law enforcement inquiries. Their participation also eases their reconciliation procedures. The network is resilient to disruptions and many wholesale financial attacks as long as the adversary cannot overtake a majority of network participants. One exception that is difficult to capture with the coarse-grained evaluation in table 2 is a breach of the permission list itself—an adversary could grant itself new network nodes until it reaches a majority. A mitigation is to require changes to be staged for a certain number of days before taking effect; if caught, the breach can be rolled back.

While a blockchain might sound like an ideal balance between a centralized and partitioned system, it has two primary drawbacks. The first is privacy: out-of-the-box, every participant of a blockchain sees every transaction. The second is performance: every transaction needs to be replicated across all participants. Techniques for improving the privacy and performance of blockchain technology is highly active in academia. In a permissioned setting, one of the most costly operations, forming consensus on the validity of each transaction, is much more efficient than the proof of work protocols used in permissionless blockchains (*e.g.,* Bitcoin and Ethereum).

There are many ways to define permissions but here is one example. The central bank retains central authority over the permission list itself, as well as sole permission to create and destroy dUSD. Commercial banks and MSBs are permitted to validate transactions along with the central bank, permitted to on-board users (details of this left to section 7), and permitted to transfer dUSD. Customers that have been on-boarded by at least one permitted bank or MSB can transfer dUSD to other permitted users. All participants are permitted to read all transactions, although participants will be identified with random-looking numbers. Only the commercial bank or MSB who on-boarded the user will know their true identity (even this is inadequate privacy protection, see section 8).

While blockchain technologies are not as mature as standard databases, pilot studies of permissioned blockchain technology have been conducted within banking and finance in areas beyond (retail) CBDC. This includes implementations of large value transfer systems from the Bank of Canada using Ethereum and R3's Corda [8, 9, 27, 62], the Monetary Authority of Singapore using Corda, Hyperledger Fabric, and J.P. Morgan's Quorum [8, 9, 35], and academic proposals using Hyperledger Fabric [25, 76]. Securities issuance has also been piloted by NASDAQ using Chain [60], TMX Group using Corda [74], and the World Bank using Ethereum [61].

## 6.4 Permissionless Blockchain

In a permissionless blockchain design, the central bank would deploy the CBDC in on a public blockchain platform where anyone can validate transactions. Otherwise, the design would largely mirror a permissioned DLT design.

The benefit of a permissionless design is a very low barrier to entry for central banks as the technical infrastructure is already in place and operational. By deploying on an existing blockchain (*e.g.,* as an ERC20 token on Ethereum), dUSD would be available for use in other applications running on Ethereum and a central bank could potentially capture part of the market currently relying on stablecoins. The drawbacks of permissionless design include a low transaction throughput capacity, which is on the order of thousands per second for wide deployments like the current version of Ethereum (Istanbul) although this is subject to on-going improvements and research. Also Ethereum relies on customers holding ETH (Ethereum's internal currency) for processing transactions which complicates its usage (a central bank could design around this through *meta-transactions*).

The final questionable design parameter of a permissionless system is that it leaves the operational details to a global network of participants. While this can offer protection against internal participants, it also leaves the network vulnerable to foreign influence, at least theoretically. A CBDC is likely to be considered critical financial market infrastructure for regulatory reasons, and the possibility that foreign actors could collude to censor and disrupt dUSD transactions is a legal challenge. Some consideration has been given to geographically restricted blockchain networks (*e.g.,* GovChain [1]) however this is subject to on-going research.

## 6.5 Scaling & Hybrid Architectures

Active research on scaling blockchain technology focuses on two basic designs: first, *sharding* where a single primary blockchain spawns many secondary blockchains that work independently, in parallel, and infrequently sync to the primary blockchain [32]; and second, *sidechains* where a primary blockchain spawns secondary blockchains that run independently but can swap assets with the primary chain [5]. As one example, Libra's FastPay proposal uses both in a permissioned setting to break the 80,000 transactions/second barrier (a common benchmark for global credit card payment authorizations) [13].

A central server could run like a single-node blockchain with integrity on all transactions, and selective disclosure of transactions or properties of transactions, along with proof that they are integrated correctly into a blockchain structure that is never publicly revealed in its entirety. Similar selective disclosure is possible with the inverse architecture: a blockchain as the primary system but private enclaves or consortiums that operate off-chain [29, 46].

## 6.6 Discussion

Choosing the correct system architecture is a question of priorities. For a central bank offering a CBDC with full retail service (*i.e.,* a flat hierarchy), a centralized system is a strong fit. For a central bank that wants to hand off as much of the system as possible, to the extent that the CBDC is a liability of the commercial banks, a partitioned design is a strong fit. For a middle position where a central bank wants to off-load retail responsibilities to commercial banks, but still offer the CBDC as a liability of the central bank, a blockchain or blockchain hybrid design enables overlapping collaboration. A blockchain can also serve as a common environment for other financial services (section 9) but it requires some mitigations for its privacy issues (section 8).

# 7 ON-BOARDING

First-time dUSD customers need to be on-boarded to the system. For end-users, this includes installing a suitable application, registering for a web-service, or obtaining the required smart card or hardware. Depending on regulation, the customer may also need to identify themselves to a registrar, who may perform a background check. If the CBDC can only be held by customers of a commercial bank or MSB, we say it is a *banked* design. If the CBDC can be held by anyone with the technical capabilities, we say it is *unbanked*.

## 7.1 Banked

In a banked design, customers (individuals and companies) will register for a CBDC account through a commercial bank or MSB. The bank complies with financial tracking regulations such as requiring proof of identity and other know your client (KYC) requirements, as well as transaction reporting, data retention, and other responsibilities. Once on-boarded, customers can hold dUSD themselves individually, but their account information will be persistently known to the MSB that on-boarded them and subject to court-authorized enforcement requests. MSBs could also rely on a third party identity providers in on-boarding users.

## 7.2 Unbanked

A banked design is a departure from banknotes which can be held by anyone: foreign nationals, tourists, residents without government identification or home addresses, children. In an unbanked (or underbanked [10]) design, customers will create CBDC accounts for themselves that can immediately receive and then transact dUSD. Cryptocurrencies like Bitcoin have this property. Unbanked customers become banked when they want to deposit dUSD with a bank or exchange dUSD through an MSB.

## 7.3 Discussion

A banked design has a straightforward path to regulatory compliance. From within it, some measures can help expand banking services (*financial inclusion*) to the unbanked. The first is an expansive hierarchy: MSBs outside of financial services might offer lightweight services with low-fee accounts and no minimum balances (*cf.* M-Pesa [55]). Even still, the limitations of a banked system is a compelling argument for preserving the use of banknotes alongside a CBDC [10, 52].

To some extent, small amounts of dUSD could be issued to unbanked individuals. First consider if there could be a cap on how much dUSD an unbanked account could hold before requiring KYC [18, 31]. This control is not sufficient—a single individual can effortlessly create many digital accounts. Instead, a control could be on the currency flow (our suggestion). An MSB could apply for special permission to distribute dUSD to unidentified individuals. At a technical level, the CBDC would otherwise deny such transactions. Once distributed, this dUSD could only be paid to a banked customer authorized to receive it. It could not circulate peer-to-peer amongst the unbanked.

Finally, we note that the banked/unbanked distinction is related but not equivalent to identified/anonymous (discussed next). As mentioned above, identity is one reason to be unbanked but not the only one. Additionally, being banked does not prevent anonymity. As discussed in the next section, a middle position on anonymity could require all users to be identified (banked) but their identities are kept confidential (cryptographically) until regulation requires disclosure [77].

# 8 PRIVACY

Financial privacy is a very complicated design parameter for a CBDC and many different designs are possible. For CBDCs using a centralized or partitioned system architecture, the relevant bank keeps all records internally using traditional cybersecurity protections. In a DLT/blockchain design, all transactions are known to all participants validating transactions and potentially known publicly. In this section, we concentrate on DLT-based designs.

It is important to distinguish between *anonymity* and *confidentiality*. A system that has neither might record a transaction as: Alice sends Bob $500. With confidentiality: Alice sends Bob $Z. With anonymity: X sends Y $500. With both: X sends Y $Z. If Alice is involved in multiple transactions and the same pseudonym X is used in each, the system offers *pseudonymity*. If Alice is identified with different, unlinkable identifiers each time she transacts, the system offers true anonymity. Blockchain-based cryptocurrencies like Bitcoin and Ethereum are pseudonymous by default.

## 8.1 Anonymity

In traditional banking, the traceability of transactions is an important deterrent to financial crime. By contrast, banknotes offer strong anonymity. A CBDC that is token-based could also offer cash-like anonymity. At least, if the design is transparent—the 1990s e-cash pilot Mondex used stored value smartcards but was still beseeched with privacy concerns [71]. Blockchain-based CBDDs require further consideration.

Traditional cryptocurrencies offered strong anonymity comparable to banknotes [57], but these systems rely on, and are claims on, commercial banks. Bitcoin succeeded by avoiding all banks and intermediaries allowing anyone to transact using one or more randomly generated pseudonyms. While initially represented in the media as being anonymous, the specifics of Bitcoin often result in the same pseudonym being used across multiple transactions in a way that can be clustered [4, 56, 63], as well as being vulnerable to other metadata leaks [41, 50].

A followup generation of privacy-enhanced cryptocurrencies include Monero and zcash. In lay terms, they use extra cryptography to allow users to form 'crowds' where someone in the crowd sent a transaction. While stronger, these systems have their own quirks that can lead to poor anonymity [47, 51].

## 8.2 Confidentiality

In a permissioned blockchain design, confidentiality ensures the amount of a transaction is hidden from the participants. Logistically, the sender and receiver know the amount but instead of revealing it, they cryptographically prove that the transaction does not create new money. While confidential transactions have been proposed for Bitcoin, they are not currently implemented. They can be found in privacy-enhanced cryptocurrencies like Monero and Mimblewimble [23], and in payment systems like ZKLedger [58].

### 8.3 Discussion

Providing traceability of transactions is the most straight-forward path to regulatory compliance. While centralized systems allow selective traceability, disclosures happen unscrutinized behind closed doors. While a public blockchain is a challenging environment to establish privacy, its transparency allows users to see and evaluate the solution for themselves.

The baseline pseudonymity in blockchain technology is too strong for traceability (identities can only be inferred heuristically) and too weak for financial privacy (material amounts of partial information is leaked publicly). Typically this is resolved through role-based access control, which enhances traceability toward authorized entities and enhances anonymity toward the public.

If strong digital identities for all users were established (implying a banked design), cryptographic proofs of identity could be anonymous [19, 24] while allowing disclosure to authorized enforcement agencies when amounts exceed a regulatory limit [15, 77]. Such traceable credentials require extensive key management by a broad set of authorities (enforcement is split between many different agencies and jurisdictions, as is the court system that provides warrants) and suffers from a *key escrow* problem where breached keys could cause massive leakage of private personal and corporate financial transactions. A different system (our suggestion) could allow the MSBs that on-boarded a user to link that user's (otherwise anonymous appearing) activities to her identity (information subject to lawful enforcement requests), but every user would have an *anonymity quota* for anonymizing currency up to a certain amount (*e.g.,* $10K every month) that could not be traced by anyone. Disregarding the exact solution, balancing privacy and transparency for a CBDC continues to be an interesting and largely unresolved research question.

## 9 FUNCTIONALITY

The next design parameter considers how feature-rich (or *programmable* [70]) the CBDC system will be. At a minimum, it could offer only *payments*. Alternatively it could be *interoperable* by design to enable easy integration with other financial systems. Finally, it could allow other financial technologies, developed outside of the central bank, to run as *applications* on the CBDC environment. In the context of a DLT/blockchain design, smart contracts or decentralized applications (DApps) would be supported.

### 9.1 Payments

A central bank interested in a minimal design could offer a narrow payments-only system. Many central banks already offer digital payment systems for their members, and a CBDC could be built with overlapping experience, which might lower the technical burden and chance of error.

### 9.2 Interoperability

To allow more expressive financial technologies to emerge without taking on the risk of widely expanding its functionality, the CBDC system could offer services to external systems for interoperability. For a centralized system, this could consist of APIs to initiate payments. For a decentralized system, this could consist of a small number of verbose payment types—*e.g.,* hashed time-locked contracts (HTLC) can allow atomic swapping of assets on different decentralized systems. HTLC was used in a piloted study by two central banks to swap currency [8, 9]. HTLC is a basic building block for many advanced *layer 2* interoperability solutions [43].

### 9.3 Applications

While centralized systems are efficient, a financial arrangement that involves multiple independent systems can introduce latency and complexity. A feature of a DLT/blockchain system is that many systems can be brought onto a shared digital environment, enabling native interoperability and allowing the system providers to maintain authority—*i.e.,* they own their own decentralized applications (DApps) and participate in the underlying consensus system [67]. This allows other authorities (with permission) to issue financial instruments (*e.g.,* securities, government bonds, commercial paper, *etc.*) on the same blockchain, while enabling delivery-vs-payment and elaborate arrangements (*e.g.,* contingent payments, contracts, financial infrastructure, markets, *etc.*). Non-financial DApps, such as identity systems (national or otherwise) are also useful.

### 9.4 Discussion

There are clear benefits to allowing interoperability and external applications on the CBDC system. A first drawback is the increased complexity as securing app/DApp hosting is difficult. It could also result in a concentration of critical services in a one environment. Finally, privacy enhancements are already difficult for payments, but they becomes much more complicated for DApps. It would be prudent for a central bank to start narrowly with payments and basic interoperability before expanding functionality over time.

Interoperability also presents a regulatory risk, as dUSD (or its value) could effectively be transferred onto different systems in different jurisdictions with differing levels of restrictions, compliance, and anonymity. This is a deeper issue than CBDCs. Commercial bank deposits already accomplish the same thing: *e.g.,* Liberty Reserve [65] or stablecoins that can be deployed any blockchain [30].

## 10 FURTHER CONSIDERATIONS

*Institutional Risks.* A CBDC has the potential to reshape aspects of the banking sector. It provides customers with a liquid, safe-haven asset. Demand for dUSD might be counter-cyclical with customers fleeing bank deposits during financial crises, which could have a destabilizing effect on banks' liquidity and the economy [21, 55]. Even in a strong economy, commercial banks might need to increase services and interest rates to retain customers [55]. Broadbent argues that a cash-like CBDC would complete more directly with banknotes than commercial bank deposits and that an expansive hierarchy (as opposed to flat) would temper its impact [21]. Some central banks (*e.g.,* ECB and others) have 'reportedly' abandoned CBDCs citing risk to commercial banks [55].

A CBDC is not the only source of competition for commercial banks. Digital payment services from technology firms (*e.g.,* Alipay, WeChat, Venmo), FinTech offerings, cryptocurrencies (stabilized or not), and decentralized finance (DeFi) will also provide competition [55]. Banks could have a larger role in a CBDC than in a Libra-esque privatized cryptocurrency from a technology firm.

Another important impact is on central bank policy. If excess reserves can be instantly and frictionlessly drawn down as dUSD at any time of the day, this would open up new outlets for commercial banks to invest their excess reserves instead of lending them overnight. This might destabilizing the key policy target of many central banks.

*Negative Interest Rate Policy (NIRP).* A policy tool used by some central banks, generally to counteract recessions, is to target a negative interest rate where members of the central bank must make (instead of receive) interest payments on their reserves. While banks must hold some level of reserves due indirectly to capital requirements (and, in some countries, directly due to reserve requirements), banks often have excess reserves. Banks can draw down excess reserves in banknotes to avoid this payment but securely storing cash is not free. If the cost of the deposit is less than the (marginal) carrying costs of cash, commercial banks will accept the payment.

A CBDC design might allow instantaneous exchange of reserves for dUSD, where the carrying cost of dUSD is fixed and negligible relative to banknotes. A CBDC of this design removes negative interest rates from the central bank's policy options. However in a CBDC design might implement interest-bearing rUSD. and negative interest rates could be directly implemented on all rUSD held by members of the central bank, or in fact, on all rUSD held by anyone.

*Unconventional monetary policies.* Certain CBDC designs affirm monetary policies that are generally consider 'unconventional.' Quantitative easing is where central banks purchase assets from open markets. As a central bank has no direct payment method to non-members, payments are tiered through a member bank. If a CBDC leads to a flat hierarchy where the general public hold accounts, this also enables the public to sell assets directly the central bank for dUSD (increasing dUSD circulation) [16]. Retail accounts also enable direct stimulus payments to anyone—an unconventional policy commonly known as helicopter money [36].

*Future of banknotes.* As the use of banknotes diminishes in many countries in favour of retail payment systems, some concern has been raised over the increasing proportion of illicit banknote transactions (*e.g.,* for criminal enterprise or tax evasion). This has led to policy discussions around phasing out large denomination banknotes or even phasing cash out completely [64]. This discussion also overlaps with negative interest rates as it removes a bank's ability to drawdown excess reserves into banknotes.

A CBDC does not intrinsically affirm or deny this policy, it depends on how it is designed. Customers seeking strong anonymity could move from banknotes to a CBDC if it provided similar transactional privacy to banknotes. Customers forgoing the convenience of retail payments systems in favour of safe government assets might also move from banknotes to a CBDC. The unbanked, including those unable or unwilling to receive government identification, would continue to rely on banknotes.

*Usability.* In blockchain systems, transactions are validated with digital signatures which requires the signee to securely store and manage private signing keys. Generally, these systems are unforgiving if a key is lost or stolen, and transactions are irreversible. Additionally, the mental model for securing a cryptographic key is different than securing cash or cash-like material objects [37]. It is common for users of cryptocurrencies to deposit them with third parties. Similarly, commercial banks and MSBs can compete on providing services for holding a customer's dUSD (*e.g.,* in a full reserve custodianship). This service would compliment the option of depositing dUSD where the customer would earn interest but the dUSD would enter a fractional reserve. While in theory, dUSD is a claim on the central bank, such behaviour means in practice, customer-held dUSD might end up as a liability of the commercial banks and MSBs providing the wallet software.

We briefly propose an *DLT-based CBDC usability trilemma* for further study. Any DLT design appears to only support two of the following three desirable properties: (1) users can entrust dUSD to a custodian, (2) dUSD is a claim on the central bank, and (3) the central bank does not offer retail service to the general public. Note that the trilemma is sidestepped by a token-based design (and banknotes).

*Sanctions and censorship.* If a CBDC incorporates a 'banked design' and banknotes are phased out, it is technically feasible for a nation-state to comprehensively deny an individual or organization access to its currency. This raises civil liberty issues that warrant consideration and debate.

*Data Tracking.* In some designs, such as a DLT-based CBDC, even if consumer transactions are sharded or somehow protected from all the nodes on the network, the commercial bank or MSB that on-boards a customer can potentially trace their users' transactions. This is an old issue, one found in early attempts at digital cash (including a controversial aspect of the token-based Mondex [71] system) and reemerged with Facebook's involvement with Libra [70]. The exposure of financial data to commercial banks is not new, but it might be unacceptable to customers for a currency that is ultimately a liability of the central bank, as could expanding this purview to new MSBs, who might undergo corporate acquisitions for their customer records. These concerns affirm a centralized CBDC design.

## 11 CONCLUDING REMARKS

Designing a CBDC is complex and 'design matters [70]' for achieving the policy objectives of the central bank. Central banks wanting to take a conservative but meaningful first step toward a retail CBDC could consider: CB withdrawal, long-term dependence, legacy distribution, account-based, centralized, banked, private server, and payments-only. This is a very conservative CBDC that we anticipate seeing in the short term (at the time of writing, China is piloting such a design), however it is a design that also leaves a lot of room to incrementally add bolder features, ones that empower money users and could reshape financial markets.

*Acknowledgements.* The author is grateful for feedback on this work from Rakesh Arora, Sriram Darbha, Fahad Saleh, Mehdi Salehi, and Dinesh Shah.

## REFERENCES

[1] Moe Adham. 2017. *GovChain: An approach to a distributed, equitable government ledger secured by its constituents.* Technical Report. BitAccess.
[2] Robleh Ali, John Barrdear, Roger Clews, and James Southgate. 2014. *Innovations in Payment Technologies and the Emergence of Digital Currencies.* Quarterly Bulletin. Bank of England.

[3] Ross Anderson and Markus Kuhn. 1996. Tamper Resistance: A Cautionary Note. In *Proceedings of the 2nd Conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2*. 1.

[4] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. Evaluating User Privacy in Bitcoin. In *Financial Cryptography*.

[5] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. 2014. *Enabling Blockchain Innovations with Pegged Sidechains*. Technical Report.

[6] Bank for International Settlement 1996. *Implications for central banks of the development of electronic money*. Technical Report. Bank for International Settlements.

[7] Bank for International Settlement 2015. *Digital currencies*. Technical Report. Bank for International Settlements and Committee on Payments and Market Infrastructures.

[8] Bank of Canada 2018. *Cross-border Interbank Payments and Settlements*. Technical Report. Bank of Canada, Bank of England, and Monetary Authority of Singapore. 68 pages.

[9] Bank of Canada 2019. *Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies*. Technical Report. Bank of Canada, Monetary Authority of Singapore, Accenture, and J.P. Morgan.

[10] Bank of Canada 2020. *Contingency Planning for a Central Bank Digital Currency*. Technical Report. Bank of Canada.

[11] Bank of England 2020. *Central Bank Digital Currency: Opportunities, challenges and design*. Discussion Paper. Bank of England.

[12] Christian Barontini and Henry Holden. 2019. *Proceeding with Caution: A Survey on Central Bank Digital Currency*. Technical Report. Bank for International Settlements.

[13] Mathieu Baudet, George Danezis, and Alberto Sonnino. 2020. FastPay: High-Performance Byzantine Fault Tolerant Settlement. *arXiv:2003.11506 [cs]* (2020).

[14] Morten L. Bech and Rodney Garratt. 2017. Central Bank Cryptocurrencies. *BIS Quarterly Review* (September 2017).

[15] Alex Biryukov, Dmitry Khovratovich, and Sergei Tikhomirov. 2018. Privacy-preserving KYC on Ethereum. In *ERCIM Blockchain Workshop*.

[16] Ole Bjerg. 2017. *Designing New Money - The Policy Trilemma of Central Bank Digital Currency*. Technical Report. Copenhagen Business School, CBS.

[17] Codruta Boar, Henry Holden, and Amber Wadsworth. 2020. *Impending arrival – a sequel to the survey on central bank digital currency*. BIS Papers 107. Bank for International Settlements.

[18] Matthieu Bouchaud, Tom Lyons, Matthieu Saint Olive, and Ken Timsit. 2020. *Central banks and the future of digital money*. Technical Report. ConsenSys Solutions.

[19] Stefan Brands. 1997. Rapid demonstration of linear relations connected by boolean operators. In *EUROCRYPT*.

[20] Jason Brett. 2020. How Project Libra And COVID-19 Drove Digital Dollar Idea In Congress. *Forbes* (2020).

[21] Ben Broadbent. 2016. *Central banks and digital currencies*. Speech. Bank of England.

[22] Russell Brown. 1997. Anderson: The unmaking of Mondex. *Computerworld News Wire* (1997).

[23] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell. 2018. Bulletproofs: Short Proofs for Confidential Transactions and More. In *IEEE Symposium on Security and Privacy*.

[24] Jan Camenisch and Anna Lysyanskaya. 2004. Signature Schemes and Anonymous Credentials from Bilinear Maps. In *CRYPTO*.

[25] Shengjiao Cao, Yuan Yuan, Angelo De Caro, Karthik Nandakumar, Kaoutar Elkhiyaoui, and Yanyan Hu. 2020. Decentralized Privacy-Preserving Netting Protocol on Blockchain for Payment Systems. In *Financial Cryptography*.

[26] Mark Carney. 2019. The Growing Challenges for Monetary Policy in the current International Monetary and Financial System. Speach.

[27] James Chapman, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon. 2017. *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?* Financial Systems Review. Bank of Canada.

[28] David Chaum. 1982. Blind signatures for untraceable payments. In *CRYPTO*.

[29] Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah M. Johnson, Ari Juels, Andrew Miller, and Dawn Song. 2018. *Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution*. Technical Report. CoRR.

[30] Jeremy Clark, Didem Demirag, and Seyedehmahsa Moosavi. 2020. Demystifying Stablecoins. *Commun. ACM* (2020).

[31] Benoît Cœ uré and Jacqueline Loh. 2018. *Central Bank Digital Currencies*. Technical Report. Bank for International Settlements and Committee on Payments and Market Infrastructures. 34 pages.

[32] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, and Roger Wattenhofer. 2016. On Scaling Decentralized Blockchains. In *Bitcoin Workshop*.

[33] George Danezis and Sarah Meiklejohn. 2016. Centrally Banked Cryptocurrencies. In *NDSS*.

[34] Danmarks Nationalbank 2017. *Central bank digital currency in Denmark?* Technical Report. Danmarks Nationalbank.

[35] Deloitte 2017. *The future is here Project Ubin: SGD on Distributed Ledger*. Technical Report. Deloitte and Monetary Authority of Singapore.

[36] Walter Engert and Ben S. C. Fung. 2017. *Central Bank Digital Currency: Motivations and Implications*. Technical Report. Bank of Canada.

[37] S Eskandari, D Barrera, E Stobert, and J Clark. 2015. A first look at the usability of Bitcoin key management. In *USEC*.

[38] Financial Stability Board 2020. *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements*. Technical Report. Financial Stability Board.

[39] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. 2008. Dismantling MIFARE Classic. In *ESORICS*.

[40] F. D. Garcia, P. v. Rossum, R. Verdult, and R. W. Schreur. 2009. Wirelessly Pickpocketing a Mifare Classic Card. In *IEEE Symposium on Security and Privacy*.

[41] Arthur Gervais, Srdjan Capkun, Ghassan O Karame, and Damian Gruber. 2014. On the privacy provisions of bloom filters in lightweight bitcoin clients. In *ACSAC*.

[42] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. In *SOSP*. 51–68.

[43] Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. 2020. SoK: Layer-Two Blockchain Protocols. In *Financial Cryptography*.

[44] J.P. Morgan 2019. *J.P. Morgan Creates Digital Coin for Payments*. Technical Report. J.P. Morgan.

[45] Aistė Juškaitė, Sigitas Šiaudinis, and Tomas Reichenbachas. 2019. *CBDC — in a whirlpool of discussion*. Occasional Paper Series. Lietuvos bankas.

[46] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S. Matthew Weinberg, and Edward W. Felten. 2018. Arbitrum: Scalable, private smart contracts. In *USENIX Security*.

[47] George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. 2018. An Empirical Analysis of Anonymity in Zcash. In *USENIX Security*. https://www.usenix.org/conference/usenixsecurity18/presentation/kappos

[48] Timo Kasper, Michael Silbermann, and Christof Paar. 2010. All You Can Eat or Breaking a Real-World Contactless Payment System. In *Financial Cryptography*.

[49] JP Koning. 2016. *Fedcoin: A Central Bankissued Cryptocurrency*. Technical Report. R3 Reports.

[50] Philip Koshy, Diana Koshy, and Patrick McDaniel. 2014. An analysis of anonymity in bitcoin using p2p network traffic. In *Financial Cryptography*.

[51] Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. 2017. A Traceability Analysis of Monero's Blockchain. In *ESORICS*.

[52] Timothy Lane. 2020. *Money and Payments in the Digital Age*. Technical Report. Bank of Canada.

[53] Tony Latter. 1996. *The Choice of Exchange Rate Regime*. Handbooks in Central Banking. Centre for Central Banking Studies, Bank of England.

[54] Robert Leshner and Geoffrey Hayes. 2018. *Compound: The Money Market Protocol*. Technical Report. Compound Finance.

[55] Tommaso Mancini Griffoli, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu, and Celine Rochon. 2018. *Casting Light on Central Bank Digital Currencies*. IMF Staff Discussion Notes 18/08. International Monetary Fund.

[56] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. In *IMC*.

[57] A Narayanan and J Clark. 2017. Bitcoin's academic pedigree. *Commun. ACM* 60, 12 (2017).

[58] Neha Narula, Willy Vasquez, and Madars Virza. 2018. zkLedger: Privacy-Preserving Auditing for Distributed Ledgers. In *USENIX NSDI*.

[59] Neha Narula and Lawrence H. White. 2020. Does the U.S. Need a National Digital Currency? *Washington Post* (2020).

[60] NASDAQ 2015. *Nasdaq linq enables first-ever private securities issuance documented with blockchain technology*. Technical Report. NASDAQ.

[61] Mike Orcutt. 2019. The World Bank is still loving its blockchain-powered bonds. *MIT Technology Review* (2019).

[62] Payments Canada and Bank of Canada and R3 2017. *Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement*. Technical Report. Payments Canada, Bank of Canada and R3.

[63] Fergal Reid and Martin Harrigan. 2011. An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*.

[64] Kenneth S Rogoff. 2017. *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*. Princeton University Press.

[65] Burton Rosenberg (Ed.). 2010. *Handbook of Financial Cryptography and Security*. Chapman and Hall/CRC.

[66] Garreth Rule. 2015. *Understanding the central bank balance sheet*. Handbooks in Central Banking 32. Centre for Central Banking Studies.

[67] Scott Ruoti, Ben Kaiser, Arkady Yerukhimovich, Jeremy Clark, and Robert Cunningham. 2020. Blockchain Technology: What is It Good For? *Commun. ACM* 63, 1 (2020), 46–53.
[68] R. Ryan, Z. Anderson, and A. Cheisa. 2008. Anatomy of a Subway Hack. In *DEFCON*.
[69] SFB Technologies 2020. *Marshall Islands to Power World's First National Digital Currency with Algorand and SFB Technologies'a.* Technical Report. SFB Technologies.
[70] Saket Sinha, Nitin Gaur, Mollie Martin, Mark Perelman, Bhavin Patel, Philip Middleton, Pierre Ortlieb, Konrad Lucke, William Coningsby-Brown, Julian Frazer, and Jamie Bulgin. 2020. *Retail CBDCs: the next payments frontier.* Technical Report. OMFIF and IBM.
[71] Felix Stalder and Andrew Clement. 1999. Exploring Policy Issues of Electronic Cash: The Mondex Case. *Canadian Journal of Communication* 24, 2 (1999).
[72] Sveriges Riksbank 2017. *The Riksbank's e-krona project: Report 1.* Technical Report. Sveriges Riksbank.
[73] Sveriges Riksbank 2018. *The Riksbank's e-krona project: Report 2.* Technical Report. Sveriges Riksbank.
[74] TMX 2018. *Jasper Phase III: Securities Settlement using Distributed Ledger Technology.* Technical Report. TMX, R3, Payments Canada, Bank of Canada and Accenture.
[75] James Tobin. 1987. A Case for Preserving Regulatory Distinctions. *Challenge* 30, 5 (1987), 10–17. http://www.jstor.org/stable/40720529
[76] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, and W. Zhao. 2018. Inter-Bank Payment System on Enterprise Blockchain Platform. In *CLOUD*.
[77] Karl Wüst, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun. 2018. PRCash: Fast, Private and Regulated Transactions for Digital Currencies. Cryptology ePrint Archive, Report 2018/412. In *Financial Cryptography*. https://eprint.iacr.org/2018/412.