8/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

CBDC Technology Considerations

WHITE PAPER

NOVEMBER 2021

Images: Getty Images

Contents

This white paper is part of the Digital Currency Governance Consortium White Paper Series. Its authors, contributors and acknowledgements can be found in that compendium report.

Preface

This white paper presents information for policy-makers to help inform their choices around the technical design requirements and security features for an effective central bank digital currency (CBDC).

Given the rapid pace of technological experimentation and development, and the multitude of variables at play, it can be challenging to assess the best technology choices for a new CBDC. This white paper is intended to guide central banks and other decision-makers through major technology considerations. It is divided into three chapters, as follows:

1. CBDC policy goals and technical design considerations

2. Trade-offs for CBDC based on distributed ledger technology (DLT)

3. Cybersecurity considerations

Our goal with this white paper is to help central banks build a potential CBDC based on a holistic approach, as well as to facilitate conversations between public and private stakeholders around CBDC requirements. Furthermore, this paper can be approached as an extension of section 10 ("Technology choices, considerations and risks") of the World Economic Forum's *Central Bank Digital Currency Policy-Maker Toolkit*, published in January 2020.[1]

This paper assumes the decision-maker has first identified a favourable value proposition for CBDC (an issue that is under investigation in most jurisdictions) and clarified the specific policy goals that the CBDC seeks to achieve. Put another way, sound CBDC technology decisions can only be made following a rigorous evaluation of CBDC's value in delivering a clear set of policy goals within a specific country's context. Technology decisions must follow from economic and policy decisions.

1 CBDC policy goals and technical design considerations

Numerous research reports describe the various policy goals that CBDC can help achieve.[2] This chapter delineates eight distinct (yet related) policy goals for CBDC, alongside the critical technical design considerations for achieving each goal.[3] It provides a starting point for understanding how CBDC can be technically designed and implemented to meet various policy goals.

The content of this chapter is not intended to prescribe certain technology decisions. Each central bank must closely consider the unique conditions of its jurisdiction and make well-informed technology decisions for CBDC that are in line with its own distinct goals, conditions and constraints. It should further be noted that, in many cases, CBDC implementation alone will not achieve policy goals – regulatory and policy changes are often necessary to comprehensively meet such goals.[4]

This chapter addresses each of the following distinct goals for CBDC in detail (listed below in no particular order):

1. Continued access to central bank money
2. Financial inclusion
3. Payment system efficiency (domestic or cross-border)
4. Payment system safety and resilience
5. Mitigation of currency substitution risk
6. Improvement of payments and banking competitiveness
7. Monetary policy implementation
8. Household fiscal transfers

Regardless of the policy goal CBDC is aiming to support, critical technical considerations for any CBDC deployment include:

– Strong cybersecurity, technical stability and resilience

– Sound technical governance

Without meeting these requirements, the technical foundation of the CBDC is unlikely to be suitable for public use, and the risks associated with CBDC deployment are high.

These risks could include technical failure, loss of user funds, breach of confidential user data and central bank reputational risk.

Sound technical governance includes consideration of CBDC network and infrastructure management, data hosting, privileges of law enforcement and other issues. Safe and reliable custody is also critical for CBDC. For instance, users should not lose access to their funds if their mobile phone or any other physical storage device is lost, stolen or damaged. Additional technical governance considerations should include compatibility with existing legal frameworks and the abilities to audit transactions and upgrade software to remain compliant with evolving legal frameworks. Finally, the CBDC system should maintain flexibility to update software for future needs and changes to functional, regulatory, cybersecurity and other requirements.

The Bank of England, the Bank for International Settlements (BIS) and a group of seven monetary authorities with the BIS have produced valuable research on technical and policy requirements for effective CBDC that targets various goals:[5]

- Bank of England, *Central Bank Digital Currency: Opportunities, challenges and design*, March 2020
- Bank for International Settlements, *The technology of retail central bank digital currency*, March 2020
- Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, 2020

Lastly, as part of this white paper, the World Economic Forum has worked with industry experts to co-create a visual mapping of important technology design considerations for technologists creating CBDC.[6]

1.1 Continued access to central bank money

Background

Continued access to central bank money (money that is a direct claim on the central bank) is one of the most popular policy goals for potential CBDC in developed economies.[7] The BIS describes this goal as the following: "In jurisdictions where access to cash is in decline, there is a danger that households and businesses will no longer have access to risk-free central bank money. Some central banks consider it an obligation to provide public access and that this access could be crucial for confidence in a currency. A CBDC could act like a 'digital banknote' and could fulfil this obligation."[8]

Such ongoing access to central bank money can provide a variety of benefits to citizens and end-users. As one example, it can support the availability of a stable, safe and reliable public option for savings and payments in case of a credit crisis, a loss of confidence or a collapse in the capabilities of private-sector options.[9] For instance, where electronic retail money consists only of options provided by private-sector intermediaries, problems with those providers such as insolvency, illiquidity, fraud or technical outages could jeopardize users' access to their funds.[10]

Technology considerations

The following technology considerations stand out for this policy goal:

- "Cash-like" features for CBDC, such as very wide acceptance and convenience, instant settlement, continuous 24/7/365 availability and offline capabilities.
- Compatibility with prevalent point-of-sale hardware to stimulate adoption and merchant acceptance. Policy-makers may consider subsidizing merchant acquisition of necessary technology upgrades.
- Related to privacy, physical cash is highly private to all parties except the payee who sees the payer's identity in many cases; the privacy considerations for the CBDC can take note of the privacy profiles of different payment technologies in the Bank of Canada's staff note "Privacy in CBDC technology".[11]

> **In jurisdictions where access to cash is in decline, there is a danger that households and businesses will no longer have access to risk-free central bank money. Some central banks consider it an obligation to provide public access and that this access could be crucial for confidence in a currency. A CBDC could act like a "digital banknote" and could fulfil this obligation.**
>
> Bank for International Settlements

1.2 Financial inclusion

Background

Financial inclusion is one of the most important and widely cited policy goals for CBDC, particularly in emerging economies where central banks rank it as the most important motivation alongside domestic payment efficiency.[12] Whether CBDC can meaningfully address financial inclusion across most economies is not yet fully evidenced,[13] but common arguments for how it could do so centre on the following two points:

1. Because CBDC can reduce complexity and reliance on intermediaries in payments, it can facilitate time-saving and cost-saving gains for consumers. Lower costs enable wider access.

2. CBDC can fill a gap for low-cost, convenient and reliable savings, deposits and payment services that the private sector has not yet provided. It can offer wider access than pre-existing services with lower fees or compliance requirements.

The challenge of financial inclusion relates to situations in which there is demand for a service that is unmet by the private sector, where the public sector has the capability and willingness to step in and provide it. These occasions may be rare, given the private sector's generally greater competence for innovation in providing financial products to the public.

Overall, it is necessary to avoid simply considering ways in which CBDC can support financial inclusion that are equally feasible for the private sector to deliver (e.g. the creation of an open-loop, interoperable payment system) or that can be enabled with public policy (e.g. limits on bank fees, deposit insurance requirements, or financial education and literacy campaigns). The question to ask is this:

Where does CBDC enable a capability or service that –

a. *cannot realistically occur only through private sector or public policy initiatives,*

b. *the private sector lacks the incentives to deliver,*

c. *involves fewer risks or expenditures of economic or political capital than would be incurred with other policy instruments?*

Furthermore, it is critical to have a clear definition of financial inclusion goals, a detailed analysis of the barriers to inclusion that exist in the jurisdiction, and an understanding of how CBDC will be able to address those barriers in the specific context.

It is critical to have a clear definition of financial inclusion goals, a detailed analysis of the barriers to inclusion that exist in the jurisdiction, and an understanding of how CBDC will be able to address those barriers in the specific context

Technology considerations

The technology considerations that stand out for this policy goal are detailed below.

Low cost

CBDC should aim to be zero- or very low-cost. Total costs to consider include the cost of acquiring the application and/or device for transacting, the costs to link and activate accounts, and ongoing costs such as transaction and data usage fees. Costs related to telecom and mobile phone usage should be transparent and low.

The public sector could potentially support low costs through multiple channels. It may cover costs through central bank seigniorage.[14] Among other activities, the central bank could do the following:

– Provide CBDC devices or applications for free

– Subsidize specific costs, such as the data for users transacting with CBDCs

– Form partnerships with certain private sector firms, such as telecommunication providers, to provide additional benefits or affordable services to users

The private sector could also help drive down costs by stimulating competition. For instance, licensed entities could potentially offer CBDC payment applications and services, competing for market share by offering value-add feature sets and products and providing top-tier customer service with very low fees.[15]

Accessibility and convenience

From a compliance perspective, accessibility can be widened by enabling the use of CBDC with varying or tiered Know Your Customer (KYC) requirements, depending on transaction or account sizes. Pairing CBDC development with an improved domestic digital identity programme can also widen access (globally, 20% of unbanked populations lack the appropriate ID to meet KYC rules imposed by financial institutions).[16] Governments can also provide financial and digital literacy programmes.

Policy-makers should "meet users where they are", by providing CBDC in a way that works with the tools and technology already widely available and accessible to citizens, for example:

- Service availability on multiple devices used by citizens (e.g. smart phones and feature mobile phones, personal computers, pre-paid cards etc.)
- Applications made available through the most popular application stores
- Very strong ease-of-use, with clear and intuitive UI/UX and simple base-layer features that instil confidence in users
- Ability to perform some actions successfully in offline or low-connectivity environments, and potentially on feature phones[17]

Finally, the interoperability of CBDC with the relevant payment infrastructure, including mobile money, and its wide acceptance within the jurisdiction would increase both the convenience and the value that CBDC could provide to citizens. These factors could also increase the efficiency of domestic remittances. For cross-border remittances, interoperability with the relevant payment infrastructure of exchanged currencies may be valuable or necessary.

Additional resources on this topic

- Bank of Canada (2020): "Designing a CBDC for universal access"[18]
- GSMA (2020): "The State of Mobile Internet Connectivity 2020"[19]
- Federal Reserve Bank of Kansas City (2020): "Motives Matter: Examining Potential Tension in Central Bank Digital Currency Designs"[20]
- Federal Reserve Bank of Kansas City (2020): "Inclusion by Design: Crafting a Central Bank Digital Currency to Reach All Americans"[21]
- Harvard Kennedy School, Belfer Center (2020): "Central Bank Digital Currencies: Tools for an Inclusive Future?"[22]
- Atlantic Council GeoTech Center (2020): "Central bank digital currency can contribute to financial inclusion but cannot solve its root causes"[23]

> **Policy-makers should "meet users where they are", by providing CBDC in a way that works with the tools and technology already widely available and accessible to citizens**

1.3 Payment system efficiency (domestic or cross-border)

Background

One of the most valuable contributions CBDC could potentially make is towards greater domestic and/or cross-border payment efficiency. For domestic payment efficiency, in most cases alternatives such as the implementation of a fast payment system without the use of CBDC should be considered. Notwithstanding this, CBDC can improve payment efficiency for both domestic and cross-border payments in the ways described below.

Domestic payments

CBDC could increase payment efficiency of domestic payments chiefly through the reduction of intermediaries in favour of central bank transaction settlement and clearing. This is particularly the case if the country lacks an efficient domestic interbank system (such as a real-time gross settlement or deferred net settlement system) or a fast payment system that offers near-immediate 24/7/365 retail payment settlement.[24]

Cross-border payments

CBDC could increase payment efficiency of cross-border payments in the following ways:

- If domestically issued CBDC were compatible with foreign CBDC (in bilateral or "multi-CBDC arrangements") or foreign payment systems, then retail payments would no longer need to go through the international interbank systems and could settle more directly
- If a CBDC were accessible to foreign entities, that would enable both foreign and domestic entities to transact more efficiently through clearing and settlement at the domestic central bank[25]

Technology considerations

The technology considerations that stand out for this policy goal are detailed below.

Cross-border payment efficiency

For cross-border payment efficiency with CBDC, the jurisdiction will need to do at least one of the following:

1. Open access to foreign entities to hold accounts or otherwise transact in the CBDC. This may require the central bank to support and enable potentially millions more accounts owned by foreign entities. It may also require close consideration of technical scalability and throughput, security, and regulatory and compliance issues related to overseas accounts.[26] In addition, policy-makers may need to give special consideration to any domestic capital controls, capital flows or foreign exchange policies and compliance.

2. Allow for domestic citizens to hold accounts or otherwise transact in another country's CBDC.

3. Allow transactions to occur between domestic and foreign CBDCs, which could involve enhancing the compatibility of the CBDCs, interlinking them, or integrating them into a single "mCBDC" (multi-CBDC) arrangement.[27] For this, technical interoperability is necessary in various ways, including: common messaging and data standards, legal and regulatory compatibility, overlapping operating times, integration through an interoperable link where CBDC infrastructures combine their functions, and more.[28]

Additional technology considerations

- Continuous 24/7/365 functionality with proven operational resilience (to address barriers to efficiency related to limitations across operating hours or lack of continuous service)
- Instant or near-instant final transaction settlement
- High transaction throughput and scalability
- High interoperability (to improve efficiency through greater interconnectedness with domestic and foreign payment systems)
- CBDCs that seek to improve efficiency may require new payments infrastructure – distributed ledger technology (DLT) may be used, although it is not fundamentally required or axiomatically beneficial[29]

Technical trade-offs for this policy goal

Cross-border payments generally involve higher compliance and regulatory standards and requirements (including those that relate to anti-money laundering, capital controls, sanctions and foreign exchange controls). One trade-off will be regulatory and policy compliance versus cross-border payment efficiency (in terms of speed and cost). For example, it may be hard to conduct real-time transaction settlement in cross-border payments or high-value domestic payments, when various important compliance checks and procedures must be conducted.

The presence of privacy-enhancing techniques that mask end-user transaction details can also interrupt efficiency, as they may involve high computational requirements that can slow down transactions.

"The presence of privacy-enhancing techniques that mask end-user transaction details can also interrupt efficiency, as they may involve high computational requirements that can slow down transactions

1.4 Payment system safety and resilience

Background

A technically robust CBDC system can support payment system resilience by virtue of serving as a primary, back-up or additional payment method, assuming other payment methods and instruments remain available. CBDC may become even more valuable as a back-up payment method if access to cash (which otherwise serves as a back-up) is very low. It is also important to note that defending against cyber-attacks is likely to be more difficult in a retail CBDC system as the quantity of endpoints and users can be very large.[30]

Some open questions about safety and resilience in CBDC include the following, listed by the BIS:[31]

- What lessons can be drawn from other domains such as safety-critical and fault-tolerant systems to create high resilience?
- What is the balance of device cost versus the risk and severity of the breach?
- Can tamper-resistant devices survive un-breached for long periods of non-connectivity?
- Can users truly settle device-to-device or only clear the transaction locally and settle when reconnected to the network?

Technology considerations

The following technology considerations stand out for this policy goal:

- Very strong cybersecurity standards and features, including practices such as ongoing cybersecurity monitoring and upgrades that address vulnerabilities and threats (this is generally a priority for all CBDC implementations)
- Data and hardware redundancy and continuous or frequent data syncing
- Consideration of potential vulnerabilities of physical devices providing access to CBDC, such as stored-value cards
- Very strong anti-counterfeiting measures and practices, for the CBDC to serve as a safe and reliable system that instils high confidence (also a priority for all CBDC implementations)
- Continuous service and availability, including offline functionality, to serve as an adequate back-up system in the event of electricity, telecom or internet network failures
- Interoperability with relevant payment systems to improve the likelihood of serving as an effective substitute where other systems fail[32]
- Resilience of any interdependency or integration with other systems. As stated by the BIS, "if a critical function is provided to a CBDC system by another system or supporting infrastructure, its unavailability could negatively impact the CBDC system".[33]

While offline capabilities improve resilience to power or connectivity outages, they may also increase vulnerability to fraud in transactions, as fewer security features and centralized controls can mitigate fraudulent behaviour. These include locking stolen funds, querying suspicious transactions, or freezing breached accounts.

The architectural design of the CBDC will also influence its technical resilience. A two-tiered CBDC may provide greater resilience than a single-tier or "direct" CBDC, as both the central bank and private payment providers are running and updating payment infrastructures.[35] Then again, a two-tiered CBDC could also increase dependencies, where resilience could be affected by failure at a private sector entity (this would interfere with the purpose of CBDC to serve as an effective back-up or alternative in the case of private-sector payment failures).

The use of blockchain or DLT can improve resilience in some ways but not others, so it is not evident that it is strongly preferable to further this policy goal of payment system resilience.[36] The use of DLT provides for strong hardware fault tolerance, continuous syncing of data and reduced reliance on a single node or operator. That said, this can also be achieved with traditional technology through multiple data centres and frequent database syncing. DLT might also introduce vulnerabilities related to newer and more complex architectures and potentially harmful activity by non-central bank nodes that have the ability to access or update records, or to validate transactions.

1.5 Mitigation of currency substitution risk

Background

CBDC could support monetary sovereignty and continued use of the domestic currency, in the event that currency substitution risks arise from various sources, such as high adoption of foreign CBDC or high adoption of stablecoins or other forms of digital currency denominated in and/or backed by foreign currency. CBDCs can help mitigate currency substitution if they are used rather than other digital currencies.[37] As with all other policy goals, the feasibility and suitability of alternative solutions such as regulatory action should also be considered.

Technology considerations

> To improve the likelihood of a CBDC's adoption... the central bank could consider efforts including researching the user's perspective and taking a user-centric design approach to developing CBDC that provides a strong value proposition

The following technology considerations related to supporting high adoption stand out for this policy goal:

- Very low or no cost
- Wide CBDC accessibility, including to citizens who can use various technologies, such as mobile phones, personal computers and pre-paid cards
- For convenience, the CBDC should be employable in various payment scenarios, including point-of-sale, e-commerce, person-to-person (including with QR codes or NFC) and online. Interoperability with other payment systems will enable a variety of payment configurations, including those already in use in the market, resulting in greater convenience and merchant acceptance.
- Functionality to pay interest to CBDC accounts, for the purposes of stimulating adoption
- High transaction capacity and scalability to support potentially high adoption
- The CBDC must be perceived to be trustworthy; for this, its implementation could be coupled with a public education or marketing campaign. Policy-makers can also instil trust and confidence through data privacy measures and strategies such as transparent accountability mechanisms that could provide proof-of-privacy for all users, within the bounds of anti-money laundering (AML) and other compliance requirements. For instance, transaction data-access logs could be established that record when user transaction data is accessed and by whom.

Adoptability can be one of the most challenging parts of CBDC deployment. To improve the likelihood of a CBDC's adoption beyond the factors listed, the central bank could consider efforts including researching the user's perspective and taking a user-centric design approach to developing CBDC that provides a strong value proposition.[38]

1.6 Improvement of payments and banking competitiveness

Background

The ability to employ CBDC to challenge the monopoly power of private-sector payment providers, or of deposit and savings account providers, can be an important goal for policy-makers. CBDC could serve as a counterweight to the market power of these entities and increase competition in payments and deposits. This can lead to a greater variety of high-quality and affordable payment options and higher deposit rates for citizens, which can increase welfare.[39] As always, policy-makers should also consider alternative solutions to this challenge, including pro-competition policies.

Technology considerations

Key considerations for CBDC issued in pursuit of this policy goal are those that make the CBDC competitive for payments and deposits, such as:

- Low cost to users
- High usability and accessibility
- High convenience, including interoperability with relevant payment systems and widespread acceptance by merchants and vendors
- Strong reliability, stability and security practices to instil trust among users
- Value-add capabilities and features that meet the needs of users in a manner that is competitive with pre-existing payment and deposit services
- Ability to pay a positive interest rate (remuneration on CBDC accounts could help push bank deposit rates upwards)

Policy-makers should also consider designing CBDC according to open-source principles, thereby inviting more involvement and innovation from the private sector to the CBDC system.

All else being equal, it is likely that if CBDC is implemented in a two-tiered structure where the same banks or payment service providers (PSPs) with monopoly power take custody of and distribute the CBDC to users – and where users can very easily move funds between the CBDC and deposit accounts operated by that provider – then the ability for the CBDC to challenge the monopoly power of those entities would likely be weaker. The CBDC accounts would still exist as an alternative option for users, creating some competitive threat to the bank deposit and PSP accounts, but users may not meaningfully hold balances in the CBDC unless it offered superior functionalities, capabilities or remuneration.

1.7 Monetary policy implementation

Background

“CBDC might be able to support some monetary policy implementation. Most economists have not expressed much conviction in this opportunity, owing to limitations or policy complexities.

CBDC might be able to support some monetary policy implementation. Most economists have not expressed much conviction in this opportunity, owing to limitations or policy complexities. Because of these factors, implementing CBDC for this policy goal alone may not be worthwhile.[40] This goal closely relates to goal #5 (“Mitigation of currency substitution risk”), yet it focuses on opportunities for stronger monetary policy implementation rather than mitigating challenges to monetary sovereignty specifically.

Key channels in which CBDC could help with monetary policy implementation are listed below, along with limitations.

1. **Interest-bearing CBDC** can enable a direct mechanism for policy-rate changes to impact households and firms (this is also called “transmission of interest rate policies”). Interest-bearing CBDC could also encourage banks to pass on policy-rate changes to their deposit and lending interest rates.[41]

   For this activity, CBDC would need to pay competitive interest rates and allow large account balances, which could lead to banking disintermediation and financial stability risks if not managed (e.g. through a tiered remuneration system, or account or transaction limits).[42] A large percentage of citizens and firms would also need to open CBDC accounts for this policy to be effective, a condition which is likely to be challenging.

2. **Breaking through effective lower bound** (ELB) in nominal interest rates: if physical cash is abolished or generally unavailable (particularly large-denomination bills), then CBDC could arguably be used to impose negative interest rates on households and firms. The existence of cash as an alternative for storing money, especially large denomination bills, dampens this opportunity today.

   Negative nominal interest rates can discourage the use of CBDC in the first place, potentially in favour of other alternatives that weaken monetary sovereignty. They can also be very difficult to implement on a social or political level. Lastly, of utmost importance, the presence of cash in an economy is critical for financial inclusion and resilience, so actions that limit its availability are not advisable.

Technology considerations

The following technology considerations stand out for this policy goal:

- The CBDC must be capable of having an interest rate that could be positive or negative
- The CBDC needs to be easily accessible and widely held among households and firms. As discussed in prior sections, to achieve this requires certain preconditions: it should be low- or no-cost, trustworthy, convenient and easy to use, accessible from technological and compliance standpoints, and it should involve attractive privacy capabilities.
- For CBDC to have wider adoption, policy-makers can also consider enacting government identity programmes and/or financial and digital education and literacy campaigns

1.8 Household fiscal transfers

Background

CBDC could be employed for fiscal transfers to households or firms, such as relief or stimulus payments. Such helicopter drops or subsidies would potentially become easier when there is widespread adoption of CBDC accounts. The transfer payments could also be "programmable", with conditions such as expiration upon a certain date or a requirement to spend the funds at certain vendors.

This activity has multiple challenges, including:

- Requirement for a very high or complete rate of adoption of CBDC accounts
- Blurring of lines between fiscal and monetary policy, if the programme were overseen by the monetary authority
- Lack of clarity over the benefits of using CBDC rather than providing stimulus payments through commercial bank accounts

It is not immediately evident that CBDC is useful for this purpose, as commercial bank accounts could also support it. Both channels are subject to challenges related to the identification of and adoption by the full set of end-recipients who would be entitled to such transfer payments.

Technology considerations

Technical considerations for this goal centre on wide accessibility (as described in prior sections), so that the widest population that may be entitled to fiscal transfers can receive the CBDC.

2 Trade-offs for blockchain-based CBDC

Several central banks that are interested in CBDC are currently evaluating the pros and cons of employing blockchain or DLT as a core part of their technology infrastructure. Using Table 1 below, this section highlights the major trade-offs, in terms of benefits and downsides, of this opportunity.

2.1 The benefits and downsides of DLT-based CBDC

In many cases, central bank exploration of DLT for CBDC is in research and experimental phases, and the extent to which central banks will choose to employ DLT in full-scale implementations is not yet clear.[43] The content in Table 1 is not intended to be a final or complete list of the benefits and downsides of DLT-based CBDC. Instead it highlights apparent opportunities, trade-offs and considerations for policy-makers and technologists considering the suitability of DLT for CBDC. The table is based on CBDC research conducted thus far, while noting there is currently a limited set of CBDC experiments or deployments to learn from. *The table's contents relate to both "permissioned" and "permissionless" DLT relative to centralized technology architecture, all else equal and unless otherwise noted.*

A permissioned blockchain or DLT for CBDC can refer to a variety of configurations and must be clearly defined for each instance proposed. It often involves non-central bank parties who operate as "nodes" with various powers related to a country's CBDC transactions, potentially including updating the record of transactions.

Hyperledger Fabric or Iroha, Corda and Quorum are all examples of software frameworks and platforms that can operate permissioned DLT for CBDC.[44]

A permissionless DLT is meant to represent those with public transaction visibility and fully permissionless or open participation in initiating and validating transactions and updating the record of transactions. Cryptocurrencies such as bitcoin and ether operate on permissionless DLT.

To frame the topic, the report by Raphael Auer and Rainer Böhme entitled *The technology of retail central bank digital currency*, published in March 2020 by BIS, states: "Overall, one needs to carefully weigh the costs and benefits of using DLT. This technology essentially outsources to external validators the authority to adjust claims on the central bank balance sheet, which is advantageous only if one trusts this network to operate more reliably than the central bank."[45] Given the heightened complexity and issues at stake, there should be clear motivation for decentralization of certain functions to justify the use of DLT in a CBDC system.

> **One needs to carefully weigh the costs and benefits of using DLT**
>
> Raphael Auer and Rainer Böhme

TABLE 1 | **Benefits and downsides of DLT-based CBDC**

Note: the benefits and downsides listed below relate to both permissioned and permissionless DLT, unless stated otherwise. They are stated in terms relative to and "all else equal" with respect to fully centralized technology infrastructure. Also, the benefits in the left column do not necessarily relate to the downsides in the right column – and vice versa.

Benefits of DLT-based CBDC	Downsides of DLT-based CBDC
Potential to bypass central bank or other authorities in transaction validation, clearing and/or settlement. This could increase speed and alleviate operational or technical challenges related to dependency on the central bank to validate transactions where those challenges cannot be solved by other means.[46]	Where validation of CBDC transactions is influenced by or deferred to parties beyond monetary authorities, there may be greater risk of digital counterfeiting (including "double spending" activity) or harmful interference with CBDC operations, as well as potential loss of monetary sovereignty or independence.[47,48]
Potential for higher hardware fault tolerance, data redundancy from continuous syncing, and continuous service during extended periods of internet connectivity loss.[49] These features generally increase as the quantity of geographically diverse nodes increases.	Higher complexity with respect to governance as entities beyond the central bank and traditional authorities may have powers and permissions related to the CBDC network and its transactions. More difficulty implementing protocol-level governance decisions or security fixes.[50,51]
Potential for greater transparency in the account balances of participants and in the software code employed to execute conditional transactions, as account balances and software may be publicly visible.	Higher overall privacy costs and more difficulty maintaining data confidentiality and preventing unwanted data dissemination, as more parties have access to transaction and account information.[52]
Potential to reduce need for trusted intermediaries (e.g. clearing houses or custodians) and counterparties in interbank payments (such as in DvP or PvP[53] transactions), as software enabling conditional transactions can be programmed in a manner that is difficult for individual entities to tamper with or alter.[54]	Higher overall security costs from greater system openness and wider "attack surface", if nodes beyond the central bank and public authorities have various permissions and powers in the CBDC network, and if software code for the CBDC network's operations is transparent (i.e. publicly visible).[55] As with other software, if smart contracts are coded improperly, they can create errors in the programme or be exploited. The decentralized and "immutable" nature of blockchain generally increases the difficulty of correcting software "bugs" or faulty transactions. These challenges are higher as the blockchain is more public and open.
If permissioned DLT: For cross-border CBDC arrangements, through shared ledger, potential to: 1. provide economies of scale in technology development and maintenance, 2. provide an alternative solution for cases where involved jurisdictions cannot agree on common governance arrangements unless ownership and management of the ledger is shared, 3. provide other new benefits with respect to greater integration, interoperability and the ability to settle international currencies (multiple foreign CBDCs) on a single distributed ledger.[56]	Lower transaction speed and scalability, depending on implementation.[57] Transaction throughput and scalability are generally inversely related to the degree of decentralization (or positively related to the degree of centralization). Relevant implementation factors affecting this issue include consensus algorithm, quantity of nodes, and the various powers and permissions of nodes.
If permissioned DLT: Ability to implement alternative governance structures that might be valuable in the CBDC context (e.g. to implement "checks and balances" and reduce dependency on one department or institution for sound governance). Namely, central banks can distribute certain responsibilities across different in-house departments or external organizations. Nodes (internal or external to the central bank) could perform functionality that is specific to the mandate of that entity.	Greater operational complexity and likelihood for operational risks.[58] Challenges to overall technical resilience, continuous operation and cybersecurity, given newness of DLT infrastructure with lower testing and track record at scale coupled with greater operational complexity. DLT arguably presents a higher degree of uncertainty and potential for new or different forms of cybersecurity challenges, risks and attack vectors, as distinct parties are linked in a more complex network with a higher variety and quantity of participants.[59]

TABLE 1 **Benefits and downsides of DLT-based CBDC** *(continued)*

Benefits of DLT-based CBDC	Downsides of DLT-based CBDC
If permissionless DLT: Potential for lower-cost and more rapid deployment, as the CBDC operates on a pre-existing network and the monetary authority does not need to design, implement and manage the technology infrastructure itself. That said, the total cost of operating the CBDC must be considered, and it may not be lower in permissionless blockchain given the presence of transaction fees and potential for higher security and privacy costs (see right-hand column).	*If permissionless DLT:* Leaves operation of the CBDC subject to the security, transaction throughput, governance rules, transaction fees and smooth functioning of the DLT network, which includes up to thousands of non-central bank parties and activities outside the central bank's control.[60,61] Higher total cost of transaction validation and updating transaction records.[62] Presence of transaction fees, which fluctuate and may be high at times.[63] Potential legal and compliance challenges with the transaction network and database operating across borders and in a manner that is generally outside any jurisdiction's control or liability.

The following issues are included for completeness but have been left out of Table 1 for two reasons: first, the unique value-add of DLT must be investigated further or is not yet fully evident; second, they may provide potential benefits or downsides depending on the situation.

- Permissioned DLT may present in some cases the potential for lower implementation cost and faster deployment, as DLT payment networks can be set up quickly with support from outside parties acting as nodes or plugging into the system.[64] This may benefit economies where the central bank's resources are limited. In many cases for a central bank with adequate resources and human capital, a centralized system can be developed equally or more quickly. Moreover, beyond initial implementation and deployment costs, the ongoing maintenance and operating costs of a permissioned DLT-based CBDC are not necessarily lower than for a CBDC operating on centralized infrastructure.

- Permissionless DLT may offer lower-cost integration and interconnectivity into the CBDC payment network by private retail payment and infrastructure providers, stimulating competition, as participation in the network and access to its data may be fully public.[65] That said, this feature is rendered moot as central banks are extremely likely to limit participation by private firms, restricting access to the CBDC network to those who are licensed, regulated and have a track record of stability, rather than fully allowing public access.[66] Moreover, the value-add of DLT is unclear as the central bank could equally enable open access to the CBDC network and data (e.g. via APIs), if desired, with centralized technology infrastructure.

- The use of self-custody or "non-custodial" digital currency wallets in DLT can enable end-users to privately store and manage their private keys (the access information that allows for the transfer of funds), empowering them to fully control the movement of their funds in the distributed ledger. This can be seen as a benefit. However, it may also be seen as a downside, as it implies higher responsibility on the part of retail users with regards to maintaining the security and access of their funds. Namely, the loss or theft of the private keys, if not managed by an intermediary, could lead to an irreversible loss of funds for the user.[67]

Central banks are extremely likely to limit participation by private firms, restricting access to the CBDC network to those who are licensed, regulated and have a track record of stability, rather than fully allowing public access

2.2 Examples of nodes in DLT-based CBDC

This section provides additional discussion and illustrative examples of a decentralized approach for CBDC that involves permissioned DLT. Such an approach may enable checks and balances on operators of the system, as well as the avoidance of "all-in risk" where there is dependency on one institution to successfully operate.[68]

The examples below are not a complete list, nor are they meant to endorse the various roles or involvement of non-central bank parties, or of DLT, in a CBDC system. Each central bank must closely consider its own needs, priorities and constraints and how these inform CBDC technology and governance, along with the presence of non-central bank parties on the CBDC platform. There must be a clearly understood value proposition, with a careful consideration of complexities and risks, for decentralizing certain roles and operations with non-central bank and non-regulatory parties.

The Linux Foundation's Hyperledger Fabric technology divides blockchain management responsibilities across several components or "nodes", as described in the following list. Each node can be operated by a separate firm, meaning each firm would manage the hosting of their particular node software, either using hardware on their premises or a cloud service provider. For illustrative purposes only, some examples of potential node operators and roles that can be enabled using permissioned DLT are listed in Table 2.

TABLE 2 **Examples of potential node operators using permissioned DLT**

Certificate authority
– A node that authorizes users to join the network by issuing them a valid cryptographic certificate for node identity and role definition – Node operator candidates: identification or licensing authority, AML compliance regulator, licensed financial institution(s)
Transaction endorser or validator
– A node that receives transaction proposals and verifies them according to the rules of the network, authenticating as many necessary elements as are required, including sufficiency of the sender's account balance, ownership of the CBDC by the sender (to prevent "double spend" and digital counterfeiting etc.) – Node operator candidates: central bank, licensed financial institution(s), regulatory body
Transaction orderer
– A node responsible for ordering incoming transactions in a specific, repeatable manner – order is relevant as network delays may cause transaction requests to appear in an unpredictable order – Node operator candidates: central bank, licensed financial institution(s)
Anchor peer
– A node that submits transaction-invocation calls to the transaction endorser nodes and broadcasts transaction proposals to the transaction orderer nodes – Node operator candidates: payment services providers, financial institutions, telecom firms

Nodes could be run by more than one department within each of the listed node operators, to provide further data integrity and redundancy. Furthermore, in certain circumstances two or more firms could create private transaction channels that enable transactions and communication between a limited number of counterparties. In these cases, the firms involved may need to run a defined combination of nodes to achieve the desired functionality. For example, the Saudi Central Bank and Central Bank of the United Arab Emirates utilized channels extensively to achieve various privacy and economic objectives.[69]

3 Cybersecurity considerations for CBDC systems

Cybersecurity is one of the main concerns regarding CBDC systems. There are many actors with different roles and the incentives for malicious entities to attack such systems can be significant. Research shows payment services are common targets for cyber-attacks.[70] Depending on the design, building a CBDC constitutes a major technology and infrastructure endeavour, likely involving new software, that can expose a central bank to a host of cybersecurity risks that it may not have practical experience of mitigating.

This chapter aims to provide a technical overview of some of the possible security threats and existing mitigations for such threats. It is not a comprehensive list, nor a checklist of cybersecurity practices for CBDC. The assumption is that cybersecurity best practices such as those published by the US National Institute of Standards and Technology (NIST) or the "STRIDE" model would be applied for general security hygiene.[71] Moreover, this chapter discusses CBDC developed with or without distributed ledger technology (without recommending one or the other be used). It strictly represents technology issues and does not consider issues related to economic and monetary policy. Furthermore, issues related to privacy are out-of-scope for this chapter but are covered in the white paper in this series entitled *Privacy and Confidentiality Options for Central Bank Digital Currency*.

3.1 Credential theft and loss

Access credentials for CBDC may come in different forms, depending on CBDC implementation. They could be given in the form of a passphrase that could be easily communicated even on paper, or they could come in the form of a hardware token which stores the private keys. Regardless of the form in which access credentials are provided, the threat of theft and loss of such credentials is significant. The impact of credential theft and loss could be extremely damaging to an individual's or entity's savings held in CBDC, and it could also damage the central bank's reputation.

> Techniques such as social engineering, side-channel attacks and malware could be used to extract credentials from a CBDC user's device

Clearly, the risk is not limited to physical theft, especially in the case of passphrases. Given the arsenal of modern attacks, techniques such as social engineering, side-channel attacks and malware could be used to extract credentials from a CBDC user's device. Moreover, if passphrases or hardware tokens are lost or damaged due to fire, water or natural hazards, it is not reasonable for CBDC users to simply lose all their funds and data. Therefore, the CBDC system should have built-in recovery mechanisms for such credentials.[72]

Credential recovery mechanisms are common in non-DLT computer systems offering an interface to large customer bases, as loss and theft events can occur frequently. The key differences between credential loss and theft mitigations for non-DLT- and DLT-based CBDCs are as follows:

- For non-DLT-based CBDC, a privileged authority can simply update a database entry with the new credentials
- For DLT-based CBDC, in addition to the method above, two or more independent parties could recover and replace the old credentials

It could be advisable for a DLT-based CBDC to use a multi-signature wallet, also known as a "social recovery" wallet. In addition to the credentials held by the owner of the wallet, there would be at least two other trusted parties who hold credentials to the same wallet (this could be the central bank itself, family members or other contacts of the end-user). Such multi-signature wallets enable the removal of a compromised or lost credential or key and the addition of new credentials.

3.2 Users with privileged roles

> As with other types of information security, the central bank – and any intermediaries involved – should have in place a cybersecurity risk management plan to cover such privileges

One concern of CBDC users is that government institutions, law enforcement and other entities may have roles which allow privileged actions, such as the freezing or withdrawal of funds in CBDC accounts without the user's consent. These capabilities are in line with today's compliance procedures in regulated payment systems. Although such roles are likely to be a functional requirement of a CBDC, they could lead to the threat of malicious insiders abusing the CBDC system. As with other types of information security, the central bank – and any intermediaries involved – should have in place a cybersecurity risk management plan to cover such privileges.

Malicious insiders could be employees of entities within the CBDC system who have privileged roles. Not all insiders pose the same level of risk to the security of the CBDC. Insiders at the central bank could have greater access to CBDC transaction data and funds, which they could accidentally or deliberately steal. To mitigate this threat, multi-party mechanisms such as those employed by multi-signature wallets, or other protections, could increase the difficulty of such attacks. In terms of the actual number of parties involved in such a multi-signature wallet, there is a trade-off between the security and usability of the system. As more parties are required to sign-off on transactions, the security level becomes higher, yet convenience decreases due to human delay and coordination.

If the CBDC operates on DLT, malicious validator nodes[73] operated by non-central bank entities could present several serious threats – in addition to undermining the central bank's monetary authority and independence by virtue of accepting or rejecting transactions contrary to the central bank's intention.

In a DLT-based system, depending on the consensus protocol used, nodes could declare transactions as invalid, essentially blocking them from being accepted by the network and creating a denial-of-service attack for CBDC users and censorship of their transactions. Collusion by non-central bank nodes could also enable double-spending attacks, a form of counterfeiting where the CBDC is spent multiple times illegitimately. The nodes may also decide to fork the distributed ledger, creating a different track and view of the ledger of transactions that disagrees with that of the central bank.

3.3 Denial of service

In addition to the potential denial-of-service attack that could be caused by validators described in the previous section, the threat of malicious CBDC end-users issuing too many transactions simultaneously is important to consider. If a very large number of CBDC users (possibly controlled by the same organization) were to issue transactions simultaneously, the CBDC system could become overloaded and stop serving legitimate users, potentially losing benign transactions. This may occur with CBDC operating on DLT or on centralized technology infrastructure. Another threat which could lead to such a denial of service is a natural or technological calamity (e.g. flood, fire, power-outage etc.) close to the infrastructure on which the CBDC system is running.

One way to mitigate this threat could be to use a highly distributed system with sufficient redundant machines on different cloud platforms (e.g. AWS, Azure, GCloud, Salesforce, "on-premise" or private cloud etc.) in different physical locations. This mitigation is more naturally applicable to DLT-based CBDC systems, where computing resources may be more distributed across various cloud platforms and locations. Moreover, this mitigation also solves the threat of malicious cloud or system administrators who could single-handedly cause a denial of service or even of privileged actions, by tampering with the software stored on the systems under their control. Leveraging public cloud infrastructure would also benefit from the robust security that such organizations have built up over time.

3.4 Double spending

As introduced above, CBDC end-users could try to spend funds from their wallets in multiple places, constituting a form of digital counterfeiting.[74] The risk of double spending is higher if the CBDC has an offline capability, depending on the technology with which it operates. Double-spend transactions could be sent to entities that are offline without the high-security validation process that would normally occur online.

For instance, a malicious actor could repeatedly transfer funds to entities which are all offline and cannot notify the CBDC system that they have received a transfer from the attacker. By imposing spending and transaction frequency limits when the CBDC user is offline, the impact of such attacks can be reduced. Furthermore, once a device that is conducting transactions comes back "online", compliance software could sync with any transactions that have concurred during the offline period.

Anonymity in CBDC accounts aggravates double-spend risk in offline payments, as the central bank or authorities may have greater difficulty identifying the attackers or blacklisting wallets that are used on a one-time or ephemeral basis.

3.5 Quantum computers

Regardless of whether the implementation of the CBDC system will be using a DLT- or non-DLT-based solution, it will involve cryptographic primitives for protecting the confidentiality and integrity of the data being stored and transmitted. Therefore, the threat of emerging quantum computers should be taken into account when choosing the cryptographic techniques used in the CBDC system. Moreover, quantum computers developed in the future may be able to break current cryptography without detection. Quantum computing will ultimately impact all financial services, as it compromises major data encryption methodologies used today.

> **Quantum computing will ultimately impact all financial services, as it compromises major data encryption methodologies used today**

Conclusion

As central banks research the technology that may support CBDC issued in the future, they must consider numerous technology choices, trade-offs and platforms, as well as security and technical issues. This white paper provides guidance in three priority areas:

1. It describes key technology considerations and choices for CBDC to meet various policy goals

2. It analyses a set of pros and cons for the use of distributed ledger technology as a primary part of CBDC technology infrastructure

3. It presents some key cybersecurity vulnerabilities for CBDC

Ultimately, this white paper aims to assist central banks and other decision-makers in understanding the critical technology issues at stake as they consider developing CBDC.

Endnotes

1. World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, 2020, https://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf.
2. Boar, Codruta and Wehrli, Andreas, *Ready, steady, go? - Results of the third BIS survey on central bank digital currency*, Bank for International Settlements (BIS), January 2021, https://www.bis.org/publ/bppdf/bispap114.htm.
3. Other policy goals that, for the purposes of brevity, are not included in this chapter include the ability of CBDC to reduce costs associated with the distribution, management, storage and transportation of physical cash, or the ability of CBDC to potentially help reduce tax evasion and the corrupt or illicit activity that can arise through using cash.
4. Fatás, Antonio, "The conflict between CBDC goals and design choices", *VoxEU*, 3 May 2021, https://voxeu.org/article/conflict-between-cbdc-goals-and-design-choices.
5. See:

   1) Bank of England, *Central Bank Digital Currency: Opportunities, challenges and design*, March 2020, https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593.

   2) Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

   3) Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, https://www.bis.org/publ/othp33.pdf.

   4) Group of Central Banks, *Central bank digital currencies – executive summary*, BIS, September 2021, https://www.bis.org/publ/othp42.htm.
6. "CBDC Technology Considerations Mind Map" [Flow chart], *Bitt and World Economic Forum*, https://www.bitt.com/solutions/mindmap.
7. See:

   1) The ECB's reference to this policy goal in its recently announced digital euro project: "Eurosystem launches digital euro project" [Press release], *European Central Bank*, 14 July 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html.

   2) Boar, Codruta and Wehrli, Andreas, *Ready, steady, go? - Results of the third BIS survey on central bank digital currency*, BIS, January 2021, https://www.bis.org/publ/bppdf/bispap114.htm.
8. Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, p.5, BIS, 2020, https://www.bis.org/publ/othp33.pdf.
9. The CBDC design can include several limitations or controls on end-user holdings. For instance, account or transaction sizes can be limited (with a purpose to limit risks, such as financial disintermediation or illicit activity). Thus, the citizen or business may have a constrained ability to hold funds in the CBDC account.
10. Auer, Raphael and Böhme, Rainer, "CBDC architectures, the financial system, and the central bank of the future", *VoxEU*, 29 October 2020, https://voxeu.org/article/cbdc-architectures-financial-system-and-central-bank-future.
11. Darbha, Sriram and Arora, Rakesh, "Privacy in CBDC technology", *Bank of Canada Staff Analytical Note*, June 2020, https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/.
12. Boar, Codruta and Wehrli, Andreas, *Ready, steady, go? - Results of the third BIS survey on central bank digital currency*, BIS, January 2021, https://www.bis.org/publ/bppdf/bispap114.htm.
13. For one example of an analytical report about financial inclusion and CBDC, see: Cenfri, *The Use Cases of Central Bank Digital Currency for Financial Inclusion: A Case for Mobile Money*, 2019, https://cenfri.org/wp-content/uploads/2019/06/CBDC-and-financial-inclusion_A-case-for-mobile-money.pdf.
14. "Seigniorage" means "profit made by a government by issuing currency, especially the difference between the face value of coins and their production costs". Source: Oxford Languages.
15. Policy-makers should consider the need for engagement and proactive cooperation with the private sector on CBDC topics. They may also consider clarifying the potential benefits of cooperation on CBDC work with private sector entities. For further discussion on this topic, see the white paper in this series, *The Role of the Private Sector and Public-Private Cooperation in the Era of Digital Currency Growth*.
16. World Bank Group, *The Global Findex Database* 2017, 2018, https://globalfindex.worldbank.org/.
17. For a discussion of offline capabilities and CBDC design, see Auer, Raphael and Böhme, Rainer, *Central bank digital currency: the quest for minimally invasive technology*, BIS, June 2021, https://www.bis.org/publ/work948.pdf.
18. Miedema, John et al., "Designing a CBDC for universal access", *Bank of Canada Staff Analytical Note*, June 2020, https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-10/?utm_source=linkedin&utm_medium=social&utm_campaign=SANH200624.

19. GSMA, *The State of Mobile Internet Connectivity 2020*, September 2020, https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf.

20. Maniff, Jesse Leigh, "Motives Matter: Examining Potential Tension in Central Bank Digital Currency Designs", *Federal Reserve Bank of Kansas City, Payments System Research Briefing*, 1 July 2020, https://www.kansascityfed.org/research/payments-system-research-briefings/motives-matter-examining-potential-tension/.

21. Maniff, Jesse Leigh, "Inclusion by Design: Crafting a Central Bank Digital Currency to Reach All Americans", *Federal Reserve Bank of Kansas City Payments System Research Briefing*, 2 December 2020, https://www.kansascityfed.org/research/payments-system-research-briefings/inclusion-by-design-crafting-central-bank-digital-currency/.

22. Lee, Eve, "Central Bank Digital Currencies: Tools for an Inclusive Future?", *Harvard Kennedy School, Belfer Center for Science and International Affairs*, September 2020, https://www.belfercenter.org/publication/central-bank-digital-currencies-tools-inclusive-future.

23. Raghuveera, Nikhil, "Central bank digital currency can contribute to financial inclusion but cannot solve its root causes", *Atlantic Council GeoTech Center*, 10 June 2020, https://www.atlanticcouncil.org/blogs/geotech-cues/central-bank-digital-currency-can-contribute-to-financial-inclusion-but-cannot-solve-its-root-causes/.

24. According to the BIS, about 55 jurisdictions had fast payment systems as of March 2020. For additional information, see Bech, Morten Linnemann et al., *Fast retail payment systems*, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003x.htm.

25. Cross-border CBDC involves several "spillover risks" and other complexities related to its impact on other economies. These topics are beyond the scope of this paper, but additional information can be found in the white paper in this series entitled: *The Role of the Private Sector and Public-Private Cooperation in the Era of Digital Currency Growth*.

26. The exact structure of the CBDC can vary and some of these issues can be addressed by the central bank designing a "two-tiered" intermediated architecture where private providers distribute and take custody of the CBDC for end retail users. Various reports on CBDC discuss this concept. See for example: Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review, BIS, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

27. Auer, Raphael et al., *Multi-CBDC arrangements and the future of cross-border payments*, BIS Papers No. 115, March 2021, https://www.bis.org/publ/bppdf/bispap115.pdf.

28. See:

    1) Auer, Raphael et al., *Multi-CBDC arrangements and the future of cross-border payments*, BIS Papers No. 115, March 2021, https://www.bis.org/publ/bppdf/bispap115.pdf.

    2) Group of Central Banks, *Central bank digital currencies: system design and interoperability*, BIS, September 2021, https://www.bis.org/publ/othp42_system_design.pdf.

29. See:

    1) Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

    2) Chapman, James et al., "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?", *Bank of Canada, Financial System Review*, June 2017, p.59, https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.

30. Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p.5, https://www.bis.org/publ/othp33.pdf.

31. Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p.19, https://www.bis.org/publ/othp33.pdf.

32. Group of Central Banks, *Central bank digital currencies: system design and interoperability*, BIS, September 2021, p.6, https://www.bis.org/publ/othp42_system_design.pdf.

33. Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p.15, https://www.bis.org/publ/othp33.pdf.

34. Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p.15, https://www.bis.org/publ/othp33.pdf.

35. Auer, Raphael and Rainer Böhme, *Central bank digital currency: the quest for minimally invasive technology*, BIS, June 2021, https://www.bis.org/publ/work948.pdf.

36. Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review, March 2020, pp.91-93, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

37. According to the BIS, "Even in a case where a stablecoin is denominated in the domestic currency of a jurisdiction, there is a risk that the payment system and the data that comes along with operating the payment system will be in foreign hands and beyond the control of domestic institutions." Source: Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p.9, https://www.bis.org/publ/othp33.pdf.

38. For further discussion on this topic, see Group of Central Banks, *Central bank digital currencies: system design and interoperability*, BIS, September 2021, https://www.bis.org/publ/othp42_system_design.pdf.

39. See:

1) Usher, Andrew et al., "The Positive Case for a CBDC", *Bank of Canada Staff Discussion Paper*, July 2021, https://www.bankofcanada.ca/2021/07/staff-discussion-paper-2021-11/.

2) Andolfatto, David, "Assessing the Impact of Central Bank Digital Currency on Private Banks", *The Economic Journal*, vol. 131, issue 634, February 2021, pp.525-540, https://academic.oup.com/ej/article-abstract/131/634/525/5900973?redirectedFrom=fulltext.

3) Chiu, Jonathan et al., "Bank Market Power and Central Bank Digital Currency: Theory and Quantitative Assessment", *Bank of Canada Staff Working Paper*, May 2019, https://www.bankofcanada.ca/2019/05/staff-working-paper-2019-20/.

40. For further discussion on this topic, see:

1) World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit – Appendices*, January 2020, p.6, https://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit_Appendices.pdf.

2) Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p.8, https://www.bis.org/publ/othp33.pdf.

41. For an interesting exploratory discussion of the use of stablecoin-based CBDC to support monetary policy transmission, see: Copic, Ezechiel and Franke, Markus, *Influencing the Velocity of Central Bank Digital Currencies*, cLabs, 2020, https://celo.org/papers/cbdc-velocity.

42. Bindseil, Ulrich, *Tiered CBDC and the financial system*, European Central Bank, Working Paper Series No 2351, January 2020, https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf.

43. According to researchers, "This [CBDC] can be based on a conventional centralised database or on distributed ledger technology (DLT). These technologies differ in their efficiency and degree of protection from single points of failure. DLT often aims to replace trust in intermediaries with trust in an underlying technology. Yet no central bank we examined aims to rely on permissionless DLT, as used for Bitcoin and many other private cryptocurrencies. We find six central banks running prototypes on DLT, two with conventional technology, and two considering both. Yet these infrastructure choices are often for first proofs of concept and pilots. Only time will tell if the same choices are made for large-scale designs." Source: Auer, Raphael et al., "Central bank digital currencies: Drivers, approaches, and technologies", *VoxEU*, 28 October 2020, https://voxeu.org/article/central-bank-digital-currencies-drivers-approaches-and-technologies.

44. See:

1) Hyperledger [Homepage], 2021, https://www.hyperledger.org/.

2) "Latest research on Central Bank Digital Currencies (CBDC)", *R3*, 2021, https://www.r3.com/cbdc-research/.

3) Consensys Quorum [Homepage], 2021, https://consensys.net/quorum/.

45. Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review, March 2020, p.93, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

46. Note that by decentralizing this activity, transaction validation, clearing and settlement would become dependent on a set of nodes operating in a functional and honest manner. Dependency is not eliminated; instead, it is *decentralized*.

47. All forms of digital and physical currency are subject to "double spending" risk or counterfeiting, where genuinely issued money is spent multiple times. For CBDC, counterfeiting occurs as follows: a) the double spending or copying of genuine central bank-issued currency, b) the spending of fake money that was not issued by the central bank but appears to be. To prevent the former (a) requires the ownership of the CBDC – as it changes hands – to be tracked and updated on a centralized or decentralized ledger.

For further discussion, see:

Armelius, Hanna et al., *On the possibility of a cash-like CBDC*, Sveriges Riksbank, February 2021, https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf.

The party or parties updating the CBDC ownership history on the (centralized or decentralized) ledger must act honestly to ensure this reconciliation is accurate and that double spending activity does not occur. With domestic interbank payments, the monetary authority and other public authorities currently conduct this activity. It is arguably very difficult to imagine situations in which a monetary authority would double spend its own currency (considering several issues including the fact that it can "print" money if desired). As a result, by decentralizing transaction validation to parties that are not the monetary authority, the risk of digital-money counterfeiting is likely to increase. Such a deferral of transaction approval for sovereign money might also raise concerns with respect to monetary authority and independence, if there are situations in which non-central bank parties would approve of or reject sovereign currency transactions where the central bank would decide otherwise.

48. With DLT, the participating nodes that conduct transaction verification update the ledger of transactions and the mechanism of a "double-spend attack" varies according to the distributed consensus mechanism used. For the proof-of-work consensus mechanism used by Bitcoin, Ethereum and many major blockchains, the cost of performing a "51% attack" – where a majority of dishonest nodes validate the spending of genuine digital money twice – varies according to the current "hash rate", or total processing power, of the network across its participating nodes. Estimated costs of such an attack vary (across protocols and across time for a given protocol as its hash rate changes), and they can be found on this website: Crypto51, https://www.crypto51.app/.

49. In terms of resilience overall, DLT presents advantages related to avoiding vulnerability to one node or a single source of failure. However, DLT also suffers other vulnerabilities that relate to resilience. For this reason, it is not accurate to describe DLT as offering higher overall technical resilience (see corresponding resilience issue in right-hand column of Table 1). For instance, vulnerabilities related to the consensus mechanism can include dishonest behaviour by the node or denial-of-service attacks.

    For further discussion, see:

    Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review, March 2020, p.93, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

    Separately, it is feasible and relatively easy today to achieve adequate redundancy and data or service back-ups with traditional and centralized technologies in many cases. Today's centralized technology systems and databases generally have strong hardware fault tolerance, redundancies and failover mechanisms.

50. Technical governance for CBDC includes consideration of CBDC network and infrastructure management, transaction approvals, software upgrades, liability for cybersecurity problems, data-hosting location and activity, privileges of law enforcement and others to access account data and/or freeze or suspend accounts, and other issues.

51. For public-permissionless DLT, complexity and ability to implement protocol-level governance decisions and software fixes can arguably be considered very high (and higher than those for permissioned DLT). Governance decisions are made using a variety of voting or agreement mechanisms and typically entail approval or agreement by a portion of the nodes participating in transaction validation, which can number in the hundreds or thousands depending on the size of the network.

52. Privacy-enhancing techniques can help address this issue, although usually at the cost of system performance and scalability. Moreover, blockchain technology is relatively new, and research continuously advances with regards to privacy and scalability possibilities. That said, an issuing authority may need to dedicate resources to continuously upgrade and maintain technology systems.

53. DvP means Delivery versus Payment; PvP means Payment versus Payment.

54. DLT is not generally required for programmable payments, including "hash time-locked contracts" and "atomic swap" transactions (which employ pre-existing conditional programming and hash functions). However, DLT can enable transparency in software code and account balances, and confidence that specific entities will not be able to unilaterally alter the software code.

    For further discussion, see:

    Albers, Todd et al., "Ten troublesome blockchain terms: What's accurate, what's not?", *Federal Reserve Bank of Minneapolis*, 22 February 2019, https://www.minneapolisfed.org/article/2019/ten-troublesome-blockchain-terms-whats-accurate-whats-not.

55. Software code in public, permissionless blockchains is transparent and publicly visible, and the ability to interact with smart contracts where present may also be public. In one respect, the public nature of the code allows for bugs to be visible and reported by more people, improving security. In another respect, it enables people to see and exploit vulnerabilities. Separately, in permissioned blockchains, the transparency of the software code is up to the discretion of the designer (monetary and public authorities for CBDC) and the code may not be transparent. Similarly, the degree of system "openness" and the quantity of nodes with various permissions can be constrained in a permissioned blockchain, likely reducing overall security risk relative to permissionless blockchains.

    Related to higher security costs, see:

    Auer, Raphael et al., *Permissioned distributed ledgers and the governance of money*, BIS, January 2021, https://www.bis.org/publ/work924.pdf.

56. These types of arrangements also introduce policy challenges with respect to shared governance, relinquishing some system control and monitoring to another operator or group of operators, and other issues. Depending on the software developer for the ledger, there may also be issues that arise with respect to trusting a record-keeping ledger and system designed by a second party (e.g. another central bank) or third party (e.g. an external privately owned software development firm). It can also be difficult to enable interoperability between different CBDCs without international standards for various data (e.g. identity credentials) and operations. These challenges are not resolved using a shared blockchain ledger alone.

    See:

    1) Auer, Raphael et al., *Permissioned distributed ledgers and the governance of money*, BIS, January 2021, https://www.bis.org/publ/work924.pdf.

    2) Auer, Raphael et al., *Multi-CBDC arrangements and the future of cross-border payments*, BIS, March 2021, p.8, https://www.bis.org/publ/bppdf/bispap115.pdf.

57. See also: Didenko, A and Buckley, R., *Central Bank Digital Currencies: A Potential Response to the Financial Inclusion Challenges of the Pacific*, Asian Development Bank, August 2021, pp.18-19, https://www.adb.org/sites/default/files/publication/720016/central-bank-digital-currencies-pacific.pdf.

58. See:

1) Chapman, James et al., "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?", *Bank of Canada, Financial System Review*, June 2017, p.68, https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.

2) Ali, Robleh and Narula, Neha, *Redesigning digital money: What can we learn from a decade of cryptocurrencies?*, MIT Media Lab, October 2019, https://dci.mit.edu/research/2020/1/22/redesigning-digital-money-what-can-we-learn-from-a-decade-of-cryptocurrencies-by-robleh-ali-and-neha-narula-of-the-digital-currency-inititaive.

59. Ali, Robleh and Narula, Neha, *Redesigning digital money: What can we learn from a decade of cryptocurrencies?*, MIT Media Lab, October 2019, https://dci.mit.edu/research/2020/1/22/redesigning-digital-money-what-can-we-learn-from-a-decade-of-cryptocurrencies-by-robleh-ali-and-neha-narula-of-the-digital-currency-inititaive.

Importantly, some forms of attacks to the network as a whole or to individuals within the network will look different depending on the governance model and powers of the nodes participating in the network. Special care must be taken with respect to the governance rules of any DLT-based CBDC system.

60. Public blockchain networks such as Bitcoin and Ethereum have operated successfully for years, but their continued operational success and security depend on continued involvement by many validators. Validators (also called "miners" in proof-of-work blockchains such as Bitcoin) may choose to stop validating transactions for a variety of reasons, including loss of confidence or a decline in the remuneration they receive for such activity.

See:

1) Lee, Alexander, "What is programmable money?", *Board of Governors of the Federal Reserve System, FEDS Notes*, 23 June 2021, https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.htm.

2) Carlsten, Miles et al., *On the Instability of Bitcoin Without the Block Reward*, 2016, https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf.

61. See also: Narula, Neha, "The Technology Underlying Stablecoins", *Neha's Writings*, 23 September 2021, https://nehanarula.org/2021/09/23/stablecoins.html.

62. Second-layer solutions (e.g. The Lightning Network) reduce transaction validation costs but at the expense of technical resilience (certain nodes need to remain online) and locked-up capital. They also tend towards centralization, potentially mimicking today's existing financial system.

See:

1) Auer, Raphael, *Beyond the doomsday economics of "proof-of-work" in cryptocurrencies*, BIS, January 2019, p.20 https://www.bis.org/publ/work765.htm.

For additional discussion on cost, see:

2) Budish, Eric, *The Economic Limits of Bitcoin and the Blockchain*, National Bureau of Economic Research, June 2018, https://www.nber.org/papers/w24717.

3) Catalini, Christian and Gans, Joshua, *Some Simple Economics of the Blockchain*, National Bureau of Economic Research, 2016 (revised 2019), https://www.nber.org/papers/w22952.

4) Gans, Joshua and Gandal, Neil, *More (or Less) Economic Limits of the Blockchain*, SSRN, December 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3494434.

63. While it is possible for the monetary or state authorities to subsidize transaction fees for end-users, the presence of transaction fees is generally unavoidable in public, permissionless blockchains.

64. Chapman, James et al., "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?", *Bank of Canada, Financial System Review*, June 2017, p.68, https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.

65. Catalini and Gans (2019) argue that the fully open ability for entrepreneurs to access a public blockchain network and its data lowers the barriers to entry and stimulates competition. They continue that the overall costs of networking in a marketplace based on a public, permissionless DLT can be lower as rents from network effects are shared more widely among participants rather than owned by one firm, and no single firm has full control over the underlying digital assets. See: Catalini, Christian and Joshua Gans, *Some Simple Economics of the Blockchain*, National Bureau of Economic Research, 2016 (revised 2019), https://www.nber.org/papers/w22952.

66. "For CBDC... it is unimaginable that a central bank would allow unidentified or unvetted parties to manage critical records. If a CBDC architecture uses designated intermediaries, they would be composed of licensed and supervised banks, established payment service providers, or technology companies if they undergo supervision." Source: Auer, Raphael a nd Rainer Böhme, *Central bank digital currency: the quest for minimally invasive technology*, BIS, June 2021, p.14, https://www.bis.org/publ/work948.pdf.

67. A DLT-based currency system does not need to require user self-custody and private key management. The private keys could be managed, stored or backed up by solely the user or the payment provider, or other services. Moreover, a CBDC developed in a "two-tiered" structure can help address this issue, as the financial intermediaries who distribute and take custody of CBDC for end retail users could back up and recover records of private keys, or generate new private keys for customers, especially those who have known identities (e.g. if they have undergone a full KYC process, where their identity and account ownership is known to the intermediary).

68. Auer, Raphael et al., *Permissioned distributed ledgers and the governance of money*, Bank for International Settlements, January 2021, https://www.bis.org/publ/work924.pdf.

    For various roles the private sector can play in a CBDC system (whether DLT-operated or not), see:
    Group of Central Banks, *Central bank digital currencies: system design and interoperability*, BIS, September 2021, https://www.bis.org/publ/othp42_system_design.pdf.

69. Central Bank of the UAE and Saudi Central Bank, *Project Aber: Saudi Central Bank and Central Bank of the U.A.E. Joint Digital Currency and Distributed Ledger Project*, 2020, https://www.centralbank.ae/sites/default/files/2020-11/Aber%20Report%202020%20-%20EN_4.pdf.

70. Aldasoro, Iñaki et al., *Covid-19 and cyber risk in the financial sector*, BIS Bulletin No 37, January 2021, p.6, https://www.bis.org/publ/bisbull37.pdf.

71. See:

    1) "Cybersecurity Framework", *NIST (US National Institute of Standards and Technology)*, https://www.nist.gov/cyberframework.

    2) "The STRIDE Threat Model", *Microsoft*, 2009, https://www.microsoft.com/security/blog/2007/09/11/stride-chart/.

72. In a two-tiered CBDC structure, this responsibility might be taken on by the distributor (e.g. a commercial bank or private payment service provider). The central bank may then insure or guarantee the funds and it is likely to impose requirements that strengthen the cybersecurity of the CBDC.

73. Validator nodes are nodes with privileges to validate transactions.

74. For a detailed discussion of the counterfeiting of digital money and CBDC, see:

    Armelius, Hanna et al., *On the possibility of a cash-like CBDC*, Sveriges Riksbank, February 2021, https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf.

    Additional experimental efforts are also underway exploring the ability to safely conduct temporary offline transactions in CBDC, such as: Christodorescu, Mihai et al., *Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies*, December 2020, https://arxiv.org/abs/2012.08003.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org