THE CBDC THINK TANK

CBDC WORKSHOP

3-Day Intensive

Student Pack

http://cbdctt.com

> “(CBDC) is a technical endeavor as well as a fundamental change.
>
> We need to make sure that we’re not going to break any system, but to enhance the system.
>
> - ***Christine Lagarde***, European Central Bank President
> Interview with Francine Lacqua / Bloomberg on 31/03/2021

Contents

Welcome

Welcome to the CBDC Think Tank Workshop!

The fervor behind central bank digital currency space has markedly accelerated in the past 18 months, both in the messaging central banks are projecting into the market and the interest in adoption. A concoction of several factors drives this acceleration including, but not limited to, the popularity and growing retail and institutional comfort with Bitcoin and cryptocurrencies, Facebook's Libra / Diem project and pandemic-friendly contactless payment mechanisms. However, the messaging does not appear to be consistent. For example, Bank of Canada's Timothy Lane stated only last week that he sees "no strong case for issuing" retail CBDCs, yet the bank is actively hiring for it.

What this means is there is a need for education and information sharing. Because there is so much at stake with a CBDC and it touches upon a number of complex topics including financial inclusion, blockchain, payments and devices, the path forward can be daunting.

It is in this vein we launched the Central Bank Digital Currency Think Tank, an attempt at pulling together academics, researchers, and current and retired IEI/NGO staffers to help disseminate unbiased information and knowledge related to CBDCs. Although there has been a deluge of papers written on the topic, what is not certain is how much of that content is being distilled and absorbed by decision makers and practitioners. Since the CBDCTT's inception in January 2021, we deliver two formats of education. The first is a monthly community meeting where a central bank delivers an intimate talk on their position and view on CBDCs and answers questions. This has been incredibly successful, and we've heard from the central banks of Switzerland, Uruguay and have booked Riksbank, Banks of England, France, Norway and Canada for the coming months. All sessions are heavily attended by other central banks, regulatory bodies, and NGOs.

- Jamiel Sheikh, Founder CBDC TT, Adviser

It is with great pleasure that I greet the participants of our workshop! I am very excited to see a large number of central banks join us in our work to move the CBDC conversation forward for all of us.

During my tenure at the IMF I worked on a number of initiatives that helped central banks better understand CBDCs. This included being part of the teams that wrote several influential papers on the practical aspects of issuing CBDC, and launching the IMFs CBDC technical assistance program. Also, via these works and at various conferences and seminars I've worked to help facilitate a common understanding and induce collaboration and cooperation between the central banks as they engage in the complex topic of CBDCs.

Along with my colleagues at the IMF and various central banks, I've heavily advocated the idea that central banks facing similar challenges should work together and share information. Also, along with the Bank of Canada and the Riksbank , I organized semi-annual CBDC roundtables for such information sharing. After retiring from the IMF, I have continued my information sharing efforts through social media and webinars, including my Kiffmeister Chronicles blog and via Twitter.

The CBDC Think Tank shares my vision of central banks working together and benefiting from the information shared by academics, intellectuals, practitioners and policymakers, and I am proud to assist in its efforts.

- John Kiff, Retired International Monetary Fund Senior Financial Sector Expert

The CBDC Think Tank was founded out of a genuine belief that the peculiar acronym deserved to be more than a cryptic crypto development.

We all realized that the future of payments was bound to be fundamentally altered when Facebook unveiled in 2019 its "global currency and financial infrastructure" Libra, now Diem. And consequently, we all noticed the sudden urge for Central Banks to delve into technology and to research if and how their national banknotes could become digital.

CBDCTT.com recognizes that when – not if – digital currencies will be issued, they will represent a systemic change in the way countries consider their payments services. CBDCs have a potential to reduce the cost of banking services, to help the unbanked rejoin the financial community and to greatly facilitate cross-border transactions.

But our think tank also understands that they also have the capacity to fundamentally reshape the banking system. Issuing a digital currency is not a decision that financial authorities around the world can take lightly. The consequences of a failing, or poorly documented experiment would be disastrous with unconceivable repercussions. A risk no central bank would or should take.

In a matter of months, discussions around CBDCs have intensified and are no longer the prerogative of financial geeks. At the Think Tank, we are determined to take part in these discussions and to contribute to the ongoing research and analysis on this issue. Our monthly sessions now allow individual central banks to present in front of a growing audience their view on this issue, and our CBDCinsider.com site offers relevant info about the latest technical, legal or political news in the CBDC sphere.

But we also felt the time had come to be more proactive on the tutoring front. This seminar is the first in a series of upcoming events with a view to explain, decrypt and figure out what is the current CBDC situation, what are the various options under consideration and the hurdles to be avoided. We know you won't mind being our beta group and rest assured that our lecturers are determined to make these 3 days insightful, memorable… and fun.

- Bruno Silvestre, CBDC TT Advisor

Course Agenda

But also the leap into electronic typesetting remaining essentially unchanged popularised in asthe 1960s with the looked up one of the more obscure latin words release.But also the leap It was popularised in the 1960s with the release of Letraset sheets containing.

Current Retail CBDC Landscape
John Kiff

To CBDC or not to CBDC?
Ashley Lannquist

Financial Stability Considerations
David Andolfatto

CBDC Design Considerations
Sonja Davidovic

Technology Platforms & Considerations
Jamiel Sheikh

Legal and Regulatory Readiness
Arthur Rossi

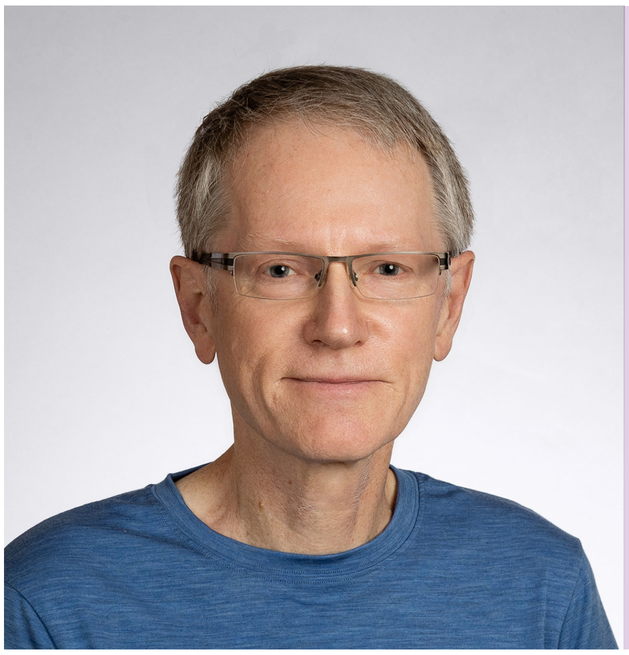
Security and Assurance Validation
Jacques Francoeur

CBDC Think Tank Bios

JAMIEL SHEIKH

Founder CBDC TT, Adviser

Jamiel is Founder & CEO of Chainhaus, a digital assets advisory and education company focused on decentralized finance and artificial intelligence. He has over 20 years of experience in technology, capital markets, real estate and management. Prior to Chainhaus, Jamiel worked for organizations like Lehman Brothers, JPMorgan, Bank of America, Sun Microsystems, SONY and Citigroup. Jamiel is an adjunct professor at Columbia Business School, NYU and CUNY teaching graduate-level blockchain, AI and data science subjects.



JOHN KIFF

Retired International Monetary Fund Senior Financial Sector Expert

John was a Senior Financial Sector Expert at the IMF from 2005 until he retired in April 2021. Prior to that, he worked at the Bank of Canada for 25 years, where he spent most of his time managing the funding and investment of the government's foreign exchange reserves, including running its large interest rate and currency swap book. At the IMF he was part of the team that produces the semi-annual Global Financial Stability Report. More recently he has been focusing on fintech issues, in particular on digital currency, publishing papers, blogging and speaking on the topic. His Kiffmeister Chronicles blog is a widely followed fintech web resource, and he actively Tweets on these topics as @Kiffmeister.

BRUNO SILVESTRE

CBDC TT Advisor

Bruno is has been a trusted name in the television news business for 28 years before becoming a communications eminence grise. He worked in foreign bureaux of the 3 leading network news channels before starting a new career as media counsel and strategic advisor for national firms and international organizations. After graduating from Columbia University, Bruno joined ABC News where he became Pierre Salinger's right-hand man. He ended his career at ABC News as Paris Bureau chief before joining CBS first, and then NBC.

In 2008, Bruno left journalism behind and became a member of the private staff of the French Economy and Finance Minister Christine Lagarde at the height of the financial crisis in charge of communications, media and strategy. After having been a key part of the team who ran her election campaign, Bruno followed Christine Lagarde to Washington when she was appointed Managing Director of the IMF.

He is now capitalizing on these years of experience and distinctive qualifications by working with domestic or international authorities as well as private companies to help them elaborate a targeted communications strategy and/or a proper media response in times of crisis. He lives between Paris, Washington and southern Maryland.

Instructor Bios

JOHN KIFF

Retired International Monetary Fund Senior Financial Sector Expert

John was a Senior Financial Sector Expert at the IMF from 2005 until he retired in April 2021. Prior to that, he worked at the Bank of Canada for 25 years, where he spent most of his time managing the funding and investment of the government's foreign exchange reserves, including running its large interest rate and currency swap book. At the IMF he was part of the team that produces the semi-annual Global Financial Stability Report. More recently he has been focusing on fintech issues, in particular on digital currency, publishing papers, blogging and speaking on the topic. His Kiffmeister Chronicles blog is a widely followed fintech web resource, and he actively Tweets on these topics as @Kiffmeister.

ASHLEY LANNQUIST

Project Lead, Blockchain & Digital Currency at World Economic Forum

Ashley is the Project Lead for Blockchain and Digital Currency at the World Economic Forum. She is based in San Francisco and leads the Forum's work on CBDC, as well as blockchain for financial inclusion and anti-corruption. Ashley is the lead author of the World Economic Forum's 2020 "CBDC Policy-Maker Toolkit." She previously worked in fixed income investment management at BNY Mellon. Ashley has an MBA from UC Berkeley's Haas School of Business, where she started and led the FinTech Club, and a Bachelor of Arts with honors in Economics and European Studies from Barnard College of Columbia University. She is also a Chartered Alternative Investment Analyst (CAIA).

Instructor Bios

DAVID ANDOLFATTO

SVP Research at Federal Reserve Bank of St. Louis

David is a Senior Vice President in the Research Department at the Federal Reserve Bank of St. Louis. He was a professor of economics at the University of Waterloo (1991-2000) and Simon Fraser University (2000-2009), before joining the Fed in July 2009. Mr. Andolfatto has published several articles in the profession's leading economic journals, including the American Economic Review, the Journal of Political Economy, and the Journal of Economic Theory. In 2009, he was awarded the Bank of Canada Fellowship Award for his contributions in the area of money, banking, and monetary policy. Mr. Andolfatto is a native of Vancouver, Canada and received his Ph.D. in economics from the University of Western Ontario in 1994.

SONJA DAVIDOVIC

Economist/Digital Expert at International Monetary Fund

Sonja is an economist and digital expert on transformative technologies in the IMF's Monetary and Capital Markets and Information Technology Departments. In this role, she provides policy recommendations and technical advice to member countries on fintech, private and central bank digital currencies, and national digital strategies. Sonja also works across departments on macroeconomic surveillance missions, including several assignments in the Asia-Pacific region, research projects, and internal and external capacity building efforts. Most recently, Sonja has worked on the Financial Stability Board roadmap to enhance cross-border payments. She helped guide development, operations, and governance of the IMF Innovation Lab, as one of the as one of the Lab's founding Advisory Board members. Sonja holds an MSc from Georgetown University and an MA from Bonn University.

Instructor Bios

ARTHUR ROSSI

Financial Regulation Expert, Bank of France

Until very recently, **Arthur** was a Research Officer in the IMF Legal Department's Financial and Fiscal Law unit, providing legal analysis on public financial management, financial law frameworks and fintech issues, for the IMF's financial assistance programs, surveillance activity and technical assistance. Before joining the IMF in 2017, he worked for the European Central Bank advising staff, academics and Members of the European Parliament on institutional and financial law questions such as the prohibition of monetary financing or the governance of payments and securities settlement systems including Target 2 and Target 2 securities. Arthur holds a Juris Doctor in Business Law at Jean Moulin University in Lyon and a Masters degree in Financial and Tax Law from La Sorbonne University in Paris.

JACQUES FRANCOEUR

CEO & Founder

Jacques is a 30-year industry and thought leader in cybersecurity and audit/compliance. His current focus is on CBDC modelling and security and assurance standards development with the International Telecommunication Union (ITU) and International Standards Organization (ISO). He is also collaborating with the World Economic Forum on solutions to emerging Fintech industry security and compliance challenges. He worked with the Canadian space program before moving to enterprise cyber risk management, the last two decades in Silicon Valley, including as a risk, security and compliance advisory consultant with the Big-4 accounting firms, and the Science Application International Corporation. In his current work as Team Lead of the ITU's Security and Assurance Working Group of the Digital Currency Global Initiative, and as a Liaison to the ISO work on CBDC Security, Jacques is at the nexus of influence and activity for the creation of standards which will become regulatory requirements. Jacques has a B.A.Sc and M.A.Sc in Aerospace Engineering from the University of Toronto, and an MBA from Concordia University.

Instructor Bios

JAMIEL SHEIKH

Founder CBDC TT, Adviser

Jamiel is Founder & CEO of Chainhaus, a digital assets advisory and education company focused on decentralized finance and artificial intelligence. He has over 20 years of experience in technology, capital markets, real estate and management. Prior to Chainhaus, Jamiel worked for organizations like Lehman Brothers, JPMorgan, Bank of America, Sun Microsystems, SONY and Citigroup. Jamiel is an adjunct professor at Columbia Business School, NYU and CUNY teaching graduate-level blockchain, AI and data science subjects.

Jamiel is currently authoring a book on decentralized finance and the author of Amazon 100 bestselling Mastering Corda. He runs the Central Bank Digital Currency Think Tank which consists of central bank, academics and IEIs, and Blockchain NYC largest blockchain and digital assets Meetups in NYC consisting of over 10K+ local members and holds marquee conferences like the DEFiiCON, NFT WORLDS, CBDC Summit and DLT Summit. He is board member of the Society of Women Coders, a group that seeks to help young females in underprivileged societies better engage in technology, a cause he is deeply passionate about, and sits on board of advisors of several startups while also mentoring startups in the IBM / Columbia LAUNCH accelerator program and is Innovation Fellow at Columbia Business School's Lang Center for Entrepreneurship.

Jamiel holds an MBA from Columbia University's Business School and BBA from Baruch College and is completing his second Masters in Artificial Intelligence from Georgia Institute of Technology.

Jamiel enjoys cooking, coding, reading dry & boring whitepapers, dastardly excessive travel, the elegant nuances of MMA and is an active contributor in several Java, Kotlin, Python and Rust open source projects.

Course Schedule

DAY 1, JUNE 15TH

10:00 AM
Welcome & Logistics
Presented by: Bruno Silvestre

10:10 AM
Opening Remarks
Presented by: Jamiel Sheikh

10:20 AM
Opening Remarks
Presented by: John Kiff

10:30 AM
Current Retail CBDC Landscape
Presented by: John Kiff

11:00 AM
To CBDC or not to CBDC?
Presented by: Ashley Lannquist

12:00 NN
BREAK

12:15 PM
GROUPTHINK - What are your obstacles to CBDC?
Presented by: Jamiel Sheikh

12:45 PM
Financial Stability Considerations
Presented by: David Andolfatto

01:45 PM
Memo to Governor
Presented by: John Kiff

02:15 PM
Wrap Up
Presented by: Bruno Silvestre

Course Schedule

DAY 2, JUNE 22ND

10:00 AM
Welcome & Logistics
Presented by: Bruno Silvestre

10:15 AM
CBDC Design Considerations
Presented by: Sonja Davidovic

11:15 AM
Technology Platforms & Considerations
Presented by: Jamiel Sheikh

12:15 PM
BREAK

12:30 PM
Legal & Regulatory Readiness
Presented by: Arthur Rossi

01:30 PM
Memo Status
Presented by: John Kiff

02:00 PM
Wrap Up
Presented by: Bruno Silvestre

Course Schedule

DAY 3, JUNE 29TH

10:00 AM
Welcome & Logistics
Presented by: Bruno Silvestre

10:15 AM
Security and Assurance Validation of CBDC Systems
Presented by: Jacques Francoeur

11:15 AM
Memo Presentation (Interactive)

12:15 PM
BREAK

12:30 PM
Memo Presentation resume

01:30 PM
Wrap Up, Graduation Ceremonies
Presented by: Bruno Silvestre

Hands-on Exercises

The workshop consists of several hands-on exercises to promote networking, collaboration, knowledge share and interactivity.

1

Whiteboard Session: What are the challenges to CBDC adoption?

In this session we will work together to discuss what you believe are the challenges to adopting a retail CBDC in your country, region or just in general. This is a group, hands-on exercise that will require participation from all parties!

2

Memo to the Governor

All participants will be broken into teams and each team will write a brief memo to the governor of their central bank outlining, advocating and justifying their position for or against a retail CBDC. This memo will be due at the last session of the course and each team will present their memo for 10 minutes.

Reading Materials

Central Bank Digital Currency Policy-Maker Toolkit

WORLD ECONOMIC FORUM

COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Insight Report

Central Bank Digital Currency Policy-Maker Toolkit

Centre for the Fourth Industrial Revolution

January 2020

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

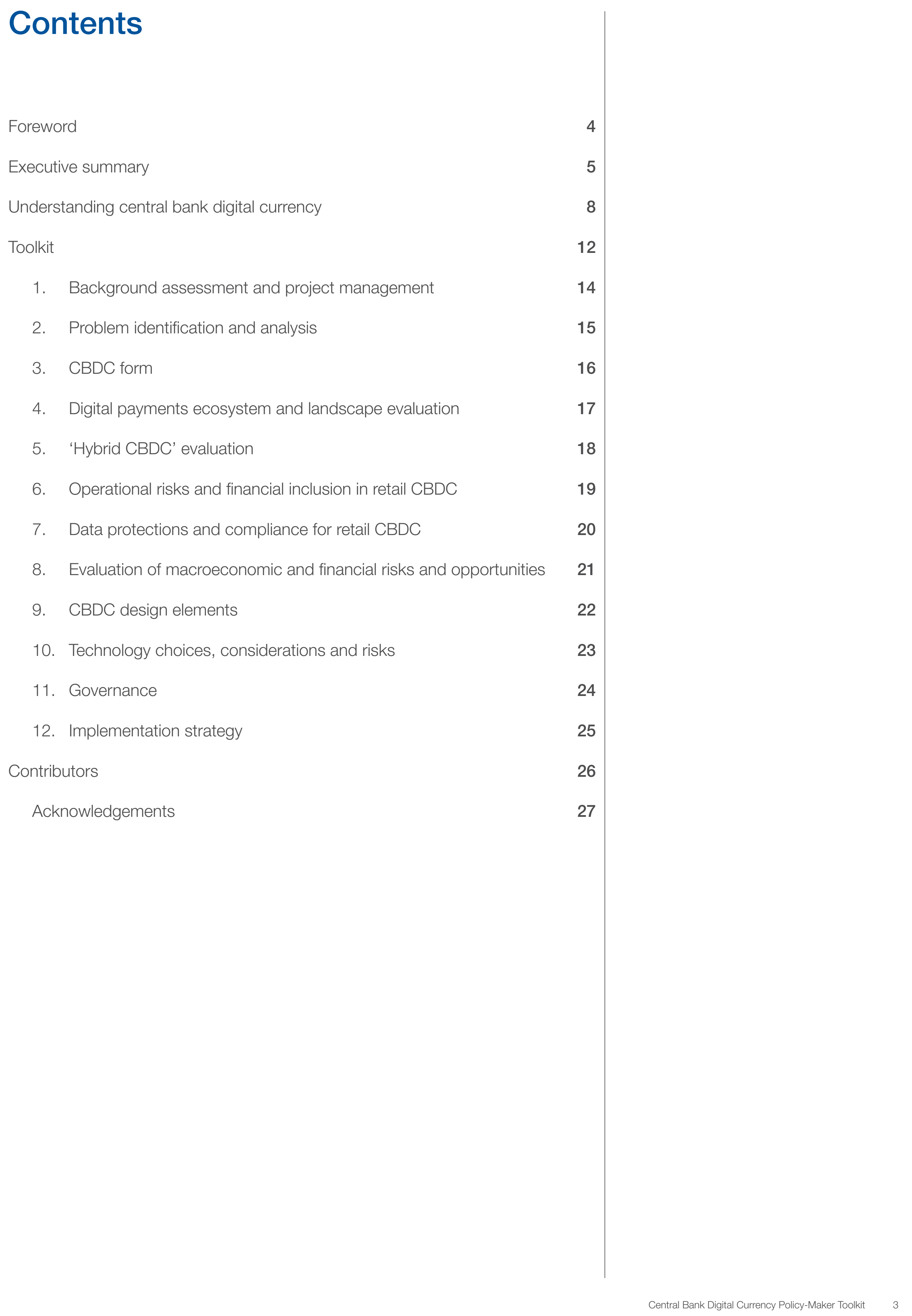
World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

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

www.weforum.org

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



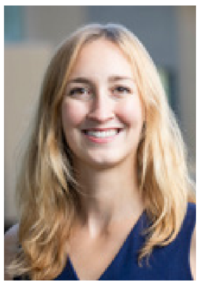
Contents

Central Bank Digital Currency Policy-Maker Toolkit 3

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Foreword



Ashley Lannquist, Project Lead – Blockchain and Distributed Ledger Technology, World Economic Forum, USA

Sheila Warren, Platform Head – Blockchain and Distributed Ledger Technology, World Economic Forum, USA

Richard Samans, Managing Director, World Economic Forum, USA

In recent years, central bank digital currency (CBDC) has risen to prominence as a policy and operational consideration for central banks, ministries of finance and other institutions because of its potential to address both long-standing and new challenges such as financial inclusion and payment-system stability. CBDC is a digitized version of sovereign currency, created and issued by, and a liability of, the country's monetary authority.

CBDC differs from other forms of digital or virtual currencies, including cryptocurrencies such as bitcoin and "stablecoins", which are not issued by central banks or typically considered legal tender. Notably, CBDC may use centralized or decentralized technology systems, and policy-makers should evaluate trade-offs between technology choices before any CBDC issuance.

Academic and policy research on CBDC has proliferated since 2014, as has technological experimentation. More recently, numerous central banks have been actively evaluating CBDC, spanning continents and economies both large and small, developed and emerging. The motivations for CBDC vary between countries, as does its relevance and potential for creating value. The "case for CBDC" is unresolved, with research and experiments from central banks and academic researchers indicating different assessments of a CBDC's value after considering costs and risks. Ultimately, countries should assess the value of CBDC on a case-by-case basis, evaluating trade-offs and carefully considering risks and design choices. Given the potentially far-reaching consequences of CBDC, policy-makers must apply the utmost prudence.

While many central bank researchers and policy-makers have developed an interest in CBDC over the past few years, most are not yet subject-matter experts. Many research reports on CBDC provide in-depth information and analysis of issues such as macroeconomic impact, financial stability, market infrastructure and design without providing as much information about social risks, governance or implementation strategies. Coupled with the ever-growing body of CBDC research from all corners of the world and the rapid speed of technological developments that relate to CBDC, researchers and policy-makers stand to benefit from a concise framework that can help inform their exploration.

The World Economic Forum's *CBDC Policy-Maker Toolkit* seeks to address the need for a concise, high-level CBDC decision framework that provides comprehensive and risk-aware information to policy-makers. The document serves as a guide to ensure that any CBDC deployment is cautious and fully considers alternative solutions, risks, deployment and governance strategies, multistakeholder input and other salient factors. Notably, it is intended to serve as a complement to additional research that any policy-maker considering CBDC should conduct.

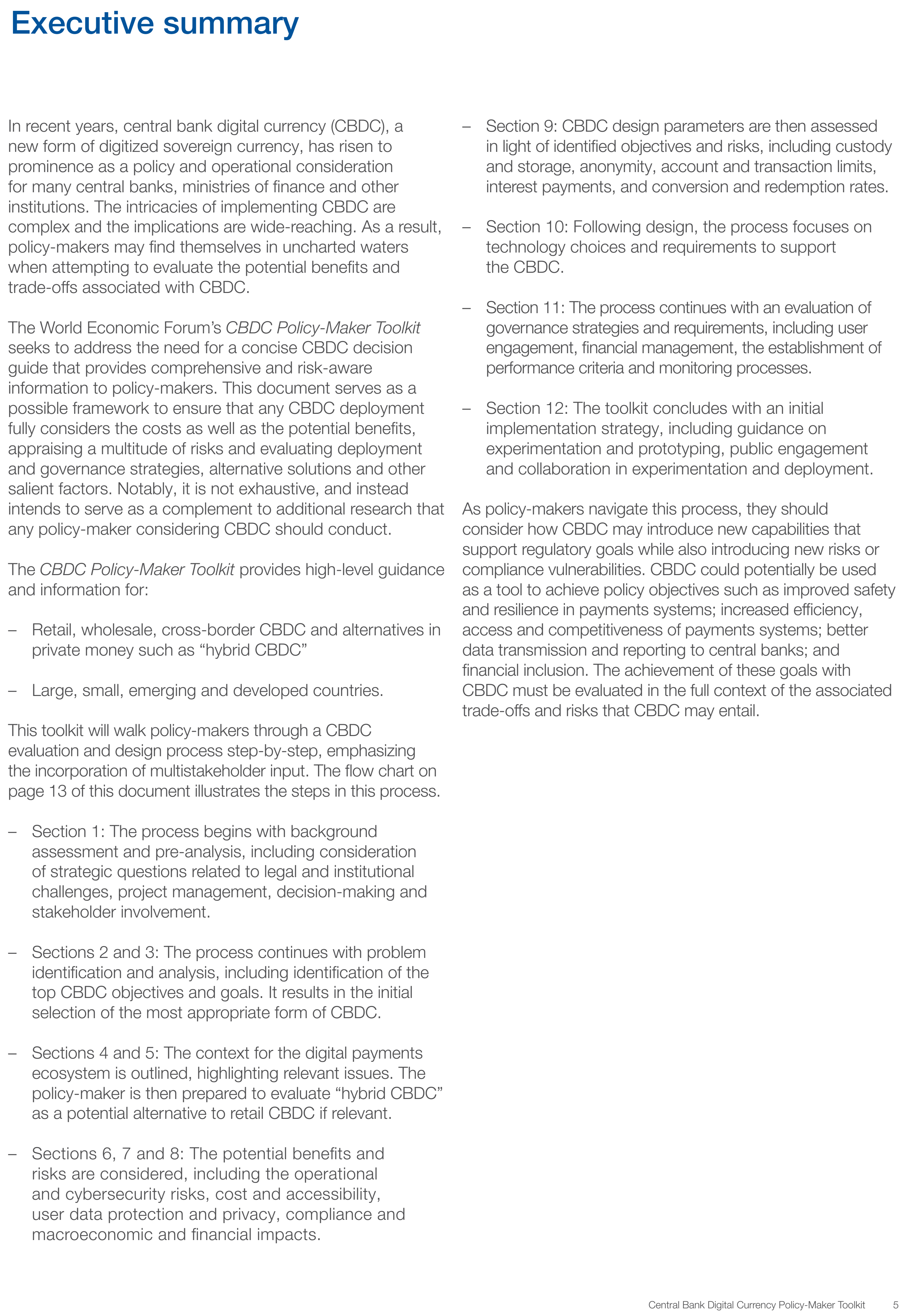
In the development of this framework, the Forum has taken a global and multisector view, drawing input from its unique global community of CBDC experts and researchers, and developing an approach that is equally suitable for policy-makers in developed or emerging economies. Furthermore, the toolkit can serve as a springboard to a community of practice and experience exchange within the World Economic Forum network as central banks progress with their CBDC investigation and development.

Prior to crafting the *CBDC Policy-Maker Toolkit*, the Forum convened central bank researchers and policy-makers from more than 45 countries to guide its project work related to central banks, CBDC and distributed ledger technology. It is from this input, as well as extensive discussion with additional experts, that the toolkit draws its motivation and content. Succinctly, this framework helps policy-makers within central banks to confidently evaluate whether CBDC is appropriate for their economy.

The *CBDC Policy-Maker Toolkit* is developed within the Centre for the Fourth Industrial Revolution's Blockchain and Distributed Ledger Technology Platform. It builds upon the platform's March 2019 white paper, which highlights central bank activity with blockchain technology as well as the platform's globally unique, curated list of more than 60 reports on CBDC research and experiments. Notably, the World Economic Forum does not advocate for or against the implementation of CBDC in any country.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



Executive summary

In recent years, central bank digital currency (CBDC), a new form of digitized sovereign currency, has risen to prominence as a policy and operational consideration for many central banks, ministries of finance and other institutions. The intricacies of implementing CBDC are complex and the implications are wide-reaching. As a result, policy-makers may find themselves in uncharted waters when attempting to evaluate the potential benefits and trade-offs associated with CBDC.

The World Economic Forum's *CBDC Policy-Maker Toolkit* seeks to address the need for a concise CBDC decision guide that provides comprehensive and risk-aware information to policy-makers. This document serves as a possible framework to ensure that any CBDC deployment fully considers the costs as well as the potential benefits, appraising a multitude of risks and evaluating deployment and governance strategies, alternative solutions and other salient factors. Notably, it is not exhaustive, and instead intends to serve as a complement to additional research that any policy-maker considering CBDC should conduct.

The *CBDC Policy-Maker Toolkit* provides high-level guidance and information for:

- Retail, wholesale, cross-border CBDC and alternatives in private money such as "hybrid CBDC"
- Large, small, emerging and developed countries.

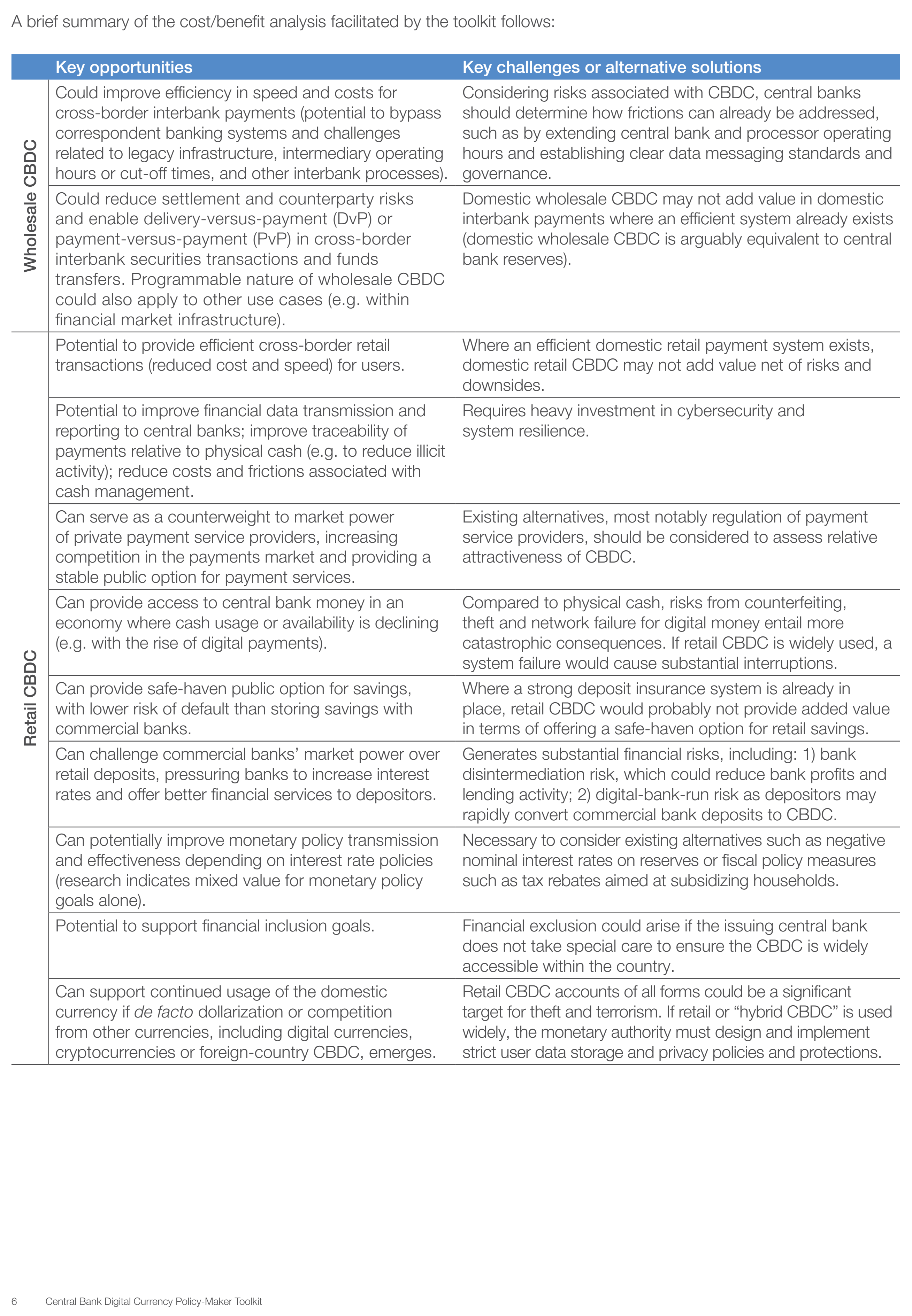
This toolkit will walk policy-makers through a CBDC evaluation and design process step-by-step, emphasizing the incorporation of multistakeholder input. The flow chart on page 13 of this document illustrates the steps in this process.

- Section 1: The process begins with background assessment and pre-analysis, including consideration of strategic questions related to legal and institutional challenges, project management, decision-making and stakeholder involvement.
- Sections 2 and 3: The process continues with problem identification and analysis, including identification of the top CBDC objectives and goals. It results in the initial selection of the most appropriate form of CBDC.
- Sections 4 and 5: The context for the digital payments ecosystem is outlined, highlighting relevant issues. The policy-maker is then prepared to evaluate "hybrid CBDC" as a potential alternative to retail CBDC if relevant.
- Sections 6, 7 and 8: The potential benefits and risks are considered, including the operational and cybersecurity risks, cost and accessibility, user data protection and privacy, compliance and macroeconomic and financial impacts.
- Section 9: CBDC design parameters are then assessed in light of identified objectives and risks, including custody and storage, anonymity, account and transaction limits, interest payments, and conversion and redemption rates.
- Section 10: Following design, the process focuses on technology choices and requirements to support the CBDC.
- Section 11: The process continues with an evaluation of governance strategies and requirements, including user engagement, financial management, the establishment of performance criteria and monitoring processes.
- Section 12: The toolkit concludes with an initial implementation strategy, including guidance on experimentation and prototyping, public engagement and collaboration in experimentation and deployment.

As policy-makers navigate this process, they should consider how CBDC may introduce new capabilities that support regulatory goals while also introducing new risks or compliance vulnerabilities. CBDC could potentially be used as a tool to achieve policy objectives such as improved safety and resilience in payments systems; increased efficiency, access and competitiveness of payments systems; better data transmission and reporting to central banks; and financial inclusion. The achievement of these goals with CBDC must be evaluated in the full context of the associated trade-offs and risks that CBDC may entail.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

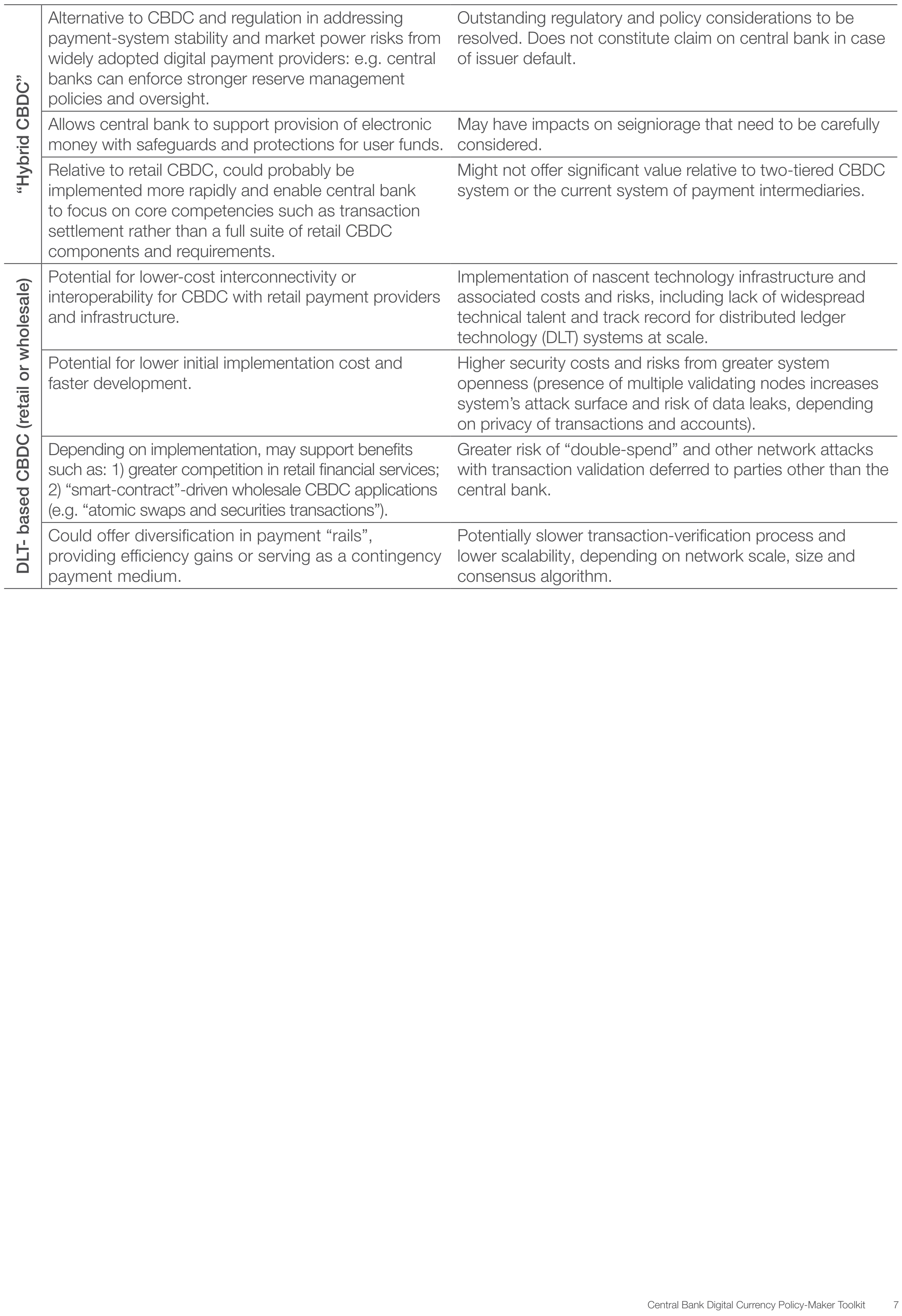


A brief summary of the cost/benefit analysis facilitated by the toolkit follows:

	Key opportunities	Key challenges or alternative solutions
Wholesale CBDC	Could improve efficiency in speed and costs for cross-border interbank payments (potential to bypass correspondent banking systems and challenges related to legacy infrastructure, intermediary operating hours or cut-off times, and other interbank processes).	Considering risks associated with CBDC, central banks should determine how frictions can already be addressed, such as by extending central bank and processor operating hours and establishing clear data messaging standards and governance.
	Could reduce settlement and counterparty risks and enable delivery-versus-payment (DvP) or payment-versus-payment (PvP) in cross-border interbank securities transactions and funds transfers. Programmable nature of wholesale CBDC could also apply to other use cases (e.g. within financial market infrastructure).	Domestic wholesale CBDC may not add value in domestic interbank payments where an efficient system already exists (domestic wholesale CBDC is arguably equivalent to central bank reserves).
Retail CBDC	Potential to provide efficient cross-border retail transactions (reduced cost and speed) for users.	Where an efficient domestic retail payment system exists, domestic retail CBDC may not add value net of risks and downsides.
	Potential to improve financial data transmission and reporting to central banks; improve traceability of payments relative to physical cash (e.g. to reduce illicit activity); reduce costs and frictions associated with cash management.	Requires heavy investment in cybersecurity and system resilience.
	Can serve as a counterweight to market power of private payment service providers, increasing competition in the payments market and providing a stable public option for payment services.	Existing alternatives, most notably regulation of payment service providers, should be considered to assess relative attractiveness of CBDC.
	Can provide access to central bank money in an economy where cash usage or availability is declining (e.g. with the rise of digital payments).	Compared to physical cash, risks from counterfeiting, theft and network failure for digital money entail more catastrophic consequences. If retail CBDC is widely used, a system failure would cause substantial interruptions.
	Can provide safe-haven public option for savings, with lower risk of default than storing savings with commercial banks.	Where a strong deposit insurance system is already in place, retail CBDC would probably not provide added value in terms of offering a safe-haven option for retail savings.
	Can challenge commercial banks' market power over retail deposits, pressuring banks to increase interest rates and offer better financial services to depositors.	Generates substantial financial risks, including: 1) bank disintermediation risk, which could reduce bank profits and lending activity; 2) digital-bank-run risk as depositors may rapidly convert commercial bank deposits to CBDC.
	Can potentially improve monetary policy transmission and effectiveness depending on interest rate policies (research indicates mixed value for monetary policy goals alone).	Necessary to consider existing alternatives such as negative nominal interest rates on reserves or fiscal policy measures such as tax rebates aimed at subsidizing households.
	Potential to support financial inclusion goals.	Financial exclusion could arise if the issuing central bank does not take special care to ensure the CBDC is widely accessible within the country.
	Can support continued usage of the domestic currency if *de facto* dollarization or competition from other currencies, including digital currencies, cryptocurrencies or foreign-country CBDC, emerges.	Retail CBDC accounts of all forms could be a significant target for theft and terrorism. If retail or "hybrid CBDC" is used widely, the monetary authority must design and implement strict user data storage and privacy policies and protections.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



"Hybrid CBDC"	Alternative to CBDC and regulation in addressing payment-system stability and market power risks from widely adopted digital payment providers: e.g. central banks can enforce stronger reserve management policies and oversight.	Outstanding regulatory and policy considerations to be resolved. Does not constitute claim on central bank in case of issuer default.
	Allows central bank to support provision of electronic money with safeguards and protections for user funds.	May have impacts on seigniorage that need to be carefully considered.
	Relative to retail CBDC, could probably be implemented more rapidly and enable central bank to focus on core competencies such as transaction settlement rather than a full suite of retail CBDC components and requirements.	Might not offer significant value relative to two-tiered CBDC system or the current system of payment intermediaries.
DLT- based CBDC (retail or wholesale)	Potential for lower-cost interconnectivity or interoperability for CBDC with retail payment providers and infrastructure.	Implementation of nascent technology infrastructure and associated costs and risks, including lack of widespread technical talent and track record for distributed ledger technology (DLT) systems at scale.
	Potential for lower initial implementation cost and faster development.	Higher security costs and risks from greater system openness (presence of multiple validating nodes increases system's attack surface and risk of data leaks, depending on privacy of transactions and accounts).
	Depending on implementation, may support benefits such as: 1) greater competition in retail financial services; 2) "smart-contract"-driven wholesale CBDC applications (e.g. "atomic swaps and securities transactions").	Greater risk of "double-spend" and other network attacks with transaction validation deferred to parties other than the central bank.
	Could offer diversification in payment "rails", providing efficiency gains or serving as a contingency payment medium.	Potentially slower transaction-verification process and lower scalability, depending on network scale, size and consensus algorithm.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Understanding central bank digital currency

CBDC is a new form of digitized sovereign currency, generally conceived to be equal to physical cash or reserves held at the central bank. It is central bank money, or a component of the monetary base and a direct liability of the central bank.

Currently, central bank money is composed of physical cash (coins and bills) and reserves held at the central bank by financial institutions with access to the central bank's deposit facility. CBDC would constitute a third form of central bank money.

	Coins and bills (physical cash)	Reserves	CBDC
Retail uses	√	X	√
Wholesale uses	√	√	√
Digital form	X	√	√

Retail CBDC

Today, the general public holds central bank money in the form of physical cash. For a given country, retail CBDC, which can also be called "general-purpose" CBDC, would constitute the first digitized form of central bank money and liability the general public could own. The public could have accounts of the digitized fiat currency with the central bank, or hold CBDC on mobile devices, prepaid cards or other forms of digital wallets. While the central bank issues and manages retail CBDC, several ecosystem participants, such as commercial banks and payment service providers, may be involved in the system through a two-tiered structure, introduced further below, or by offering interoperable payments and services.

Wholesale CBDC

Wholesale CBDC could be issued by central banks to commercial banks and potentially other financial institutions for use in interbank payments and securities transactions. These institutions could hold wholesale CBDC accounts with the central bank, akin to the reserve accounts they keep today (it could be argued that wholesale CBDC already exists today in many countries in the form of reserves).

Wholesale CBDC for domestic use may not provide additional interbank payment functionality to an economy that already has a well-functioning commercial banking sector and interbank payment system, such as a real-time gross settlements (RTGS) system. Such banks can already efficiently transact with one another using reserves held at the central bank in the manner they would with CBDC. Wholesale CBDC for use in domestic interbank payments may be most relevant for developing economies that need a more efficient interbank system and prefer an alternative to today's standard systems, such as a traditional RTGS system.

Beyond interbank payments, wholesale CBDC could be applied in various countries to interbank securities transactions or financial market infrastructure applications (domestic or cross-border), discussed at the end of this section.

Cross-border CBDC (retail or wholesale)

The value that a cross-border CBDC provides depends on the economy's unique payments infrastructure and starting point. Cross-border wholesale CBDC may be valuable across economies to enable more efficient cross-border interbank payments. As foreign banks and financial institutions today are generally unable to hold reserve accounts with the central banks of other countries, they must conduct cross-border payments in a much less efficient manner. Rather than transacting and settling through a common central bank in which both parties hold reserve accounts, they route payments through correspondent and other interbank payment networks, entailing extra time, costs and risks.

Generally, a cross-border form of wholesale CBDC in which foreign institutions might own and transact in CBDC could potentially unlock efficiencies related to more direct cross-border interbank payments. For a given economy, the CBDC would constitute the first form of digitized central bank money that could be held and sent directly overseas, where transactions could be made without the need for today's cross-border interbank payment networks.

Likewise, cross-border retail CBDC could allow retail users to send payments, including remittances, across borders in a manner that reduces the need for intermediaries. Importantly, for this to occur, the central bank must allow foreign entities to hold the CBDC. Accordingly, it may raise complex legal or financial integrity questions.

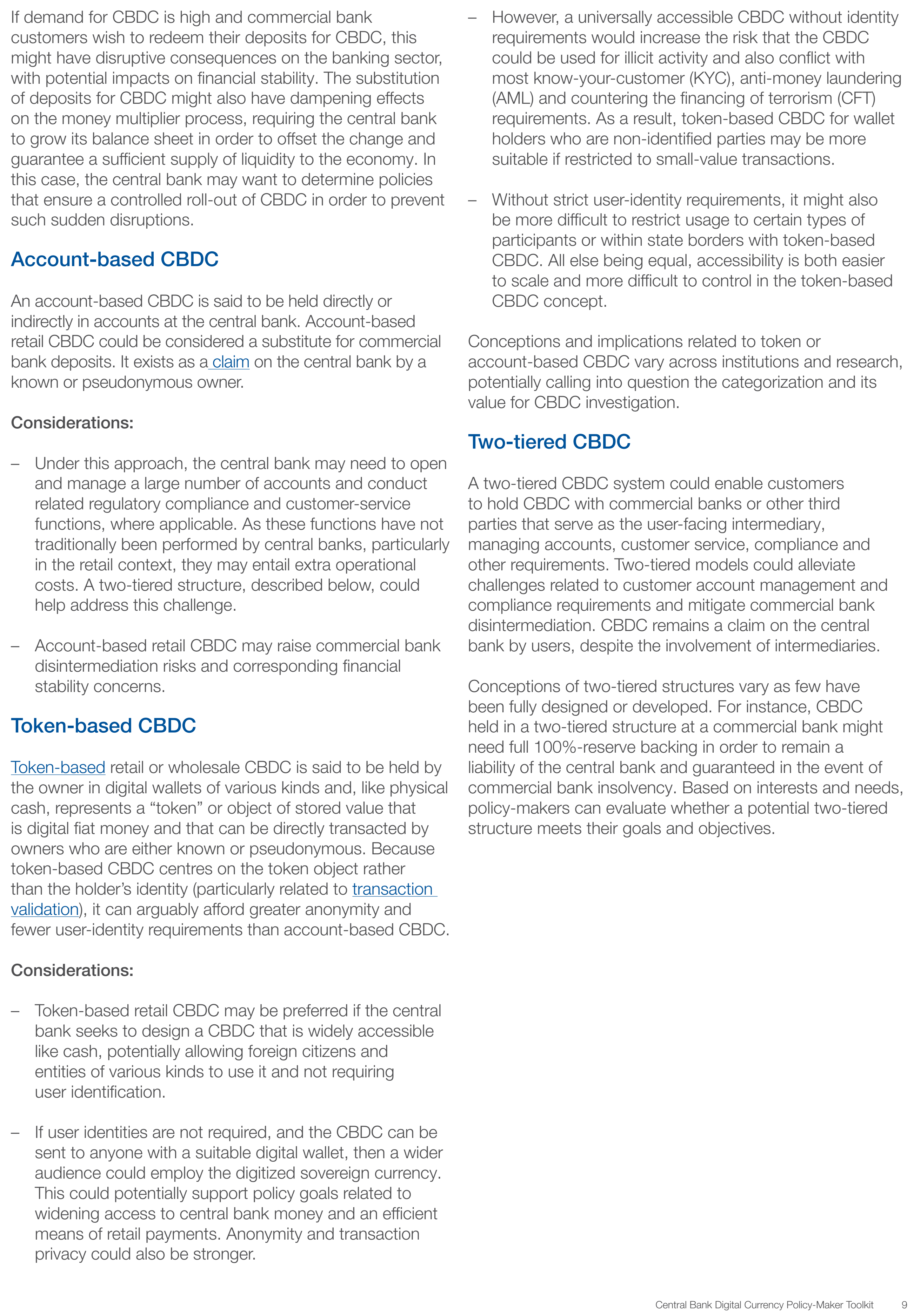
Where cross-border payments involve a foreign-exchange transaction from a domestic CBDC to another country's CBDC, present-day currency conversion frictions remain. The system requires either that a foreign-exchange market-making intermediary is willing to assume foreign-exchange risk or that the transacting commercial banks hold accounts in foreign CBDC.

CBDC and the central bank balance sheet

When central banks issue CBDC, they may substitute an existing liability, namely physical cash or commercial bank reserves at the central bank, for the CBDC. In this scheme, the composition of central bank liabilities changes, but the size of the balance sheet generally does not change. Alternatively, the central bank could issue CBDC as a new liability in exchange for bonds or other assets, increasing the total size of the balance sheet (i.e. both assets and liabilities increase).

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



If demand for CBDC is high and commercial bank customers wish to redeem their deposits for CBDC, this might have disruptive consequences on the banking sector, with potential impacts on financial stability. The substitution of deposits for CBDC might also have dampening effects on the money multiplier process, requiring the central bank to grow its balance sheet in order to offset the change and guarantee a sufficient supply of liquidity to the economy. In this case, the central bank may want to determine policies that ensure a controlled roll-out of CBDC in order to prevent such sudden disruptions.

Account-based CBDC

An account-based CBDC is said to be held directly or indirectly in accounts at the central bank. Account-based retail CBDC could be considered a substitute for commercial bank deposits. It exists as a claim on the central bank by a known or pseudonymous owner.

Considerations:

- Under this approach, the central bank may need to open and manage a large number of accounts and conduct related regulatory compliance and customer-service functions, where applicable. As these functions have not traditionally been performed by central banks, particularly in the retail context, they may entail extra operational costs. A two-tiered structure, described below, could help address this challenge.

- Account-based retail CBDC may raise commercial bank disintermediation risks and corresponding financial stability concerns.

Token-based CBDC

Token-based retail or wholesale CBDC is said to be held by the owner in digital wallets of various kinds and, like physical cash, represents a “token” or object of stored value that is digital fiat money and that can be directly transacted by owners who are either known or pseudonymous. Because token-based CBDC centres on the token object rather than the holder’s identity (particularly related to transaction validation), it can arguably afford greater anonymity and fewer user-identity requirements than account-based CBDC.

Considerations:

- Token-based retail CBDC may be preferred if the central bank seeks to design a CBDC that is widely accessible like cash, potentially allowing foreign citizens and entities of various kinds to use it and not requiring user identification.

- If user identities are not required, and the CBDC can be sent to anyone with a suitable digital wallet, then a wider audience could employ the digitized sovereign currency. This could potentially support policy goals related to widening access to central bank money and an efficient means of retail payments. Anonymity and transaction privacy could also be stronger.

- However, a universally accessible CBDC without identity requirements would increase the risk that the CBDC could be used for illicit activity and also conflict with most know-your-customer (KYC), anti-money laundering (AML) and countering the financing of terrorism (CFT) requirements. As a result, token-based CBDC for wallet holders who are non-identified parties may be more suitable if restricted to small-value transactions.

- Without strict user-identity requirements, it might also be more difficult to restrict usage to certain types of participants or within state borders with token-based CBDC. All else being equal, accessibility is both easier to scale and more difficult to control in the token-based CBDC concept.

Conceptions and implications related to token or account-based CBDC vary across institutions and research, potentially calling into question the categorization and its value for CBDC investigation.

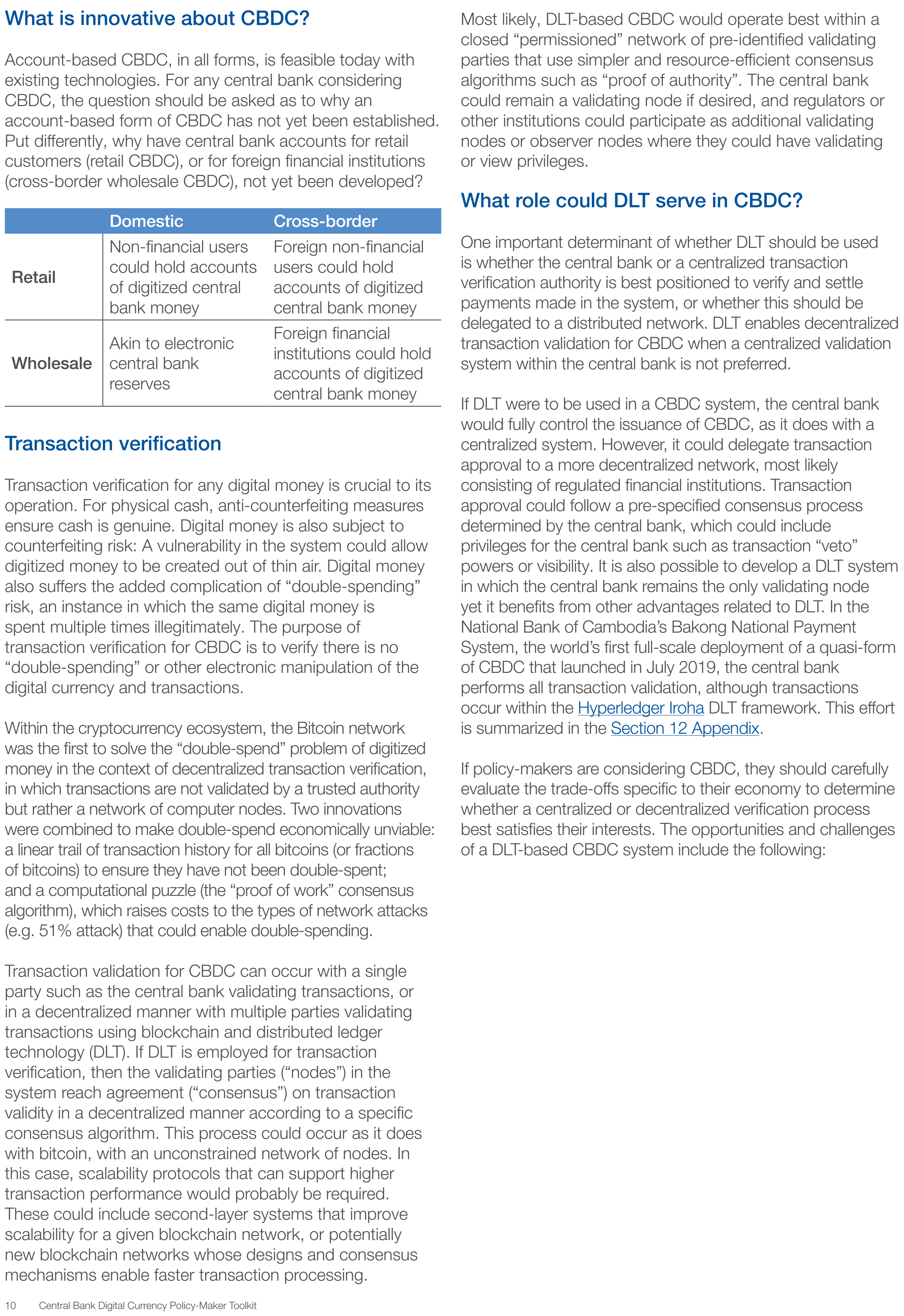
Two-tiered CBDC

A two-tiered CBDC system could enable customers to hold CBDC with commercial banks or other third parties that serve as the user-facing intermediary, managing accounts, customer service, compliance and other requirements. Two-tiered models could alleviate challenges related to customer account management and compliance requirements and mitigate commercial bank disintermediation. CBDC remains a claim on the central bank by users, despite the involvement of intermediaries.

Conceptions of two-tiered structures vary as few have been fully designed or developed. For instance, CBDC held in a two-tiered structure at a commercial bank might need full 100%-reserve backing in order to remain a liability of the central bank and guaranteed in the event of commercial bank insolvency. Based on interests and needs, policy-makers can evaluate whether a potential two-tiered structure meets their goals and objectives.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



What is innovative about CBDC?

Account-based CBDC, in all forms, is feasible today with existing technologies. For any central bank considering CBDC, the question should be asked as to why an account-based form of CBDC has not yet been established. Put differently, why have central bank accounts for retail customers (retail CBDC), or for foreign financial institutions (cross-border wholesale CBDC), not yet been developed?

	Domestic	Cross-border
Retail	Non-financial users could hold accounts of digitized central bank money	Foreign non-financial users could hold accounts of digitized central bank money
Wholesale	Akin to electronic central bank reserves	Foreign financial institutions could hold accounts of digitized central bank money

Transaction verification

Transaction verification for any digital money is crucial to its operation. For physical cash, anti-counterfeiting measures ensure cash is genuine. Digital money is also subject to counterfeiting risk: A vulnerability in the system could allow digitized money to be created out of thin air. Digital money also suffers the added complication of "double-spending" risk, an instance in which the same digital money is spent multiple times illegitimately. The purpose of transaction verification for CBDC is to verify there is no "double-spending" or other electronic manipulation of the digital currency and transactions.

Within the cryptocurrency ecosystem, the Bitcoin network was the first to solve the "double-spend" problem of digitized money in the context of decentralized transaction verification, in which transactions are not validated by a trusted authority but rather a network of computer nodes. Two innovations were combined to make double-spend economically unviable: a linear trail of transaction history for all bitcoins (or fractions of bitcoins) to ensure they have not been double-spent; and a computational puzzle (the "proof of work" consensus algorithm), which raises costs to the types of network attacks (e.g. 51% attack) that could enable double-spending.

Transaction validation for CBDC can occur with a single party such as the central bank validating transactions, or in a decentralized manner with multiple parties validating transactions using blockchain and distributed ledger technology (DLT). If DLT is employed for transaction verification, then the validating parties ("nodes") in the system reach agreement ("consensus") on transaction validity in a decentralized manner according to a specific consensus algorithm. This process could occur as it does with bitcoin, with an unconstrained network of nodes. In this case, scalability protocols that can support higher transaction performance would probably be required. These could include second-layer systems that improve scalability for a given blockchain network, or potentially new blockchain networks whose designs and consensus mechanisms enable faster transaction processing.

Most likely, DLT-based CBDC would operate best within a closed "permissioned" network of pre-identified validating parties that use simpler and resource-efficient consensus algorithms such as "proof of authority". The central bank could remain a validating node if desired, and regulators or other institutions could participate as additional validating nodes or observer nodes where they could have validating or view privileges.

What role could DLT serve in CBDC?

One important determinant of whether DLT should be used is whether the central bank or a centralized transaction verification authority is best positioned to verify and settle payments made in the system, or whether this should be delegated to a distributed network. DLT enables decentralized transaction validation for CBDC when a centralized validation system within the central bank is not preferred.

If DLT were to be used in a CBDC system, the central bank would fully control the issuance of CBDC, as it does with a centralized system. However, it could delegate transaction approval to a more decentralized network, most likely consisting of regulated financial institutions. Transaction approval could follow a pre-specified consensus process determined by the central bank, which could include privileges for the central bank such as transaction "veto" powers or visibility. It is also possible to develop a DLT system in which the central bank remains the only validating node yet it benefits from other advantages related to DLT. In the National Bank of Cambodia's Bakong National Payment System, the world's first full-scale deployment of a quasi-form of CBDC that launched in July 2019, the central bank performs all transaction validation, although transactions occur within the Hyperledger Iroha DLT framework. This effort is summarized in the Section 12 Appendix.

If policy-makers are considering CBDC, they should carefully evaluate the trade-offs specific to their economy to determine whether a centralized or decentralized verification process best satisfies their interests. The opportunities and challenges of a DLT-based CBDC system include the following:

Opportunities with DLT-based CBDC	Challenges with DLT-based CBDC
– Potential to bypass central bank or other central authority to validate transactions. (This could alleviate operational or technical frictions where they exist, such as central bank operating-hour limitations, and where they are difficult to solve directly.) – Potential for lower implementation cost and faster deployment, as DLT payment networks can be set up quickly with support from third parties acting as nodes. – Potential for lower-cost interconnectivity for CBDC with retail payment providers and infrastructure, if DLT network enables easier and more open API connectivity. This capability may support competition in retail financial services.	– Potential for high security costs and risks from greater system openness (presence of multiple validating nodes increases the system's attack surface and risk of data leaks, depending on privacy of transactions and accounts). – Greater potential risk of "double-spend" and other network attacks with transaction validation deferred to parties other than the central bank. – Implementation of nascent technology infrastructure and associated costs and risks, including lack of widespread technical talent and track record for DLT systems at scale. Linking distinct institutions and parties across complex financial systems through distributed networks probably creates new cybersecurity challenges. – Potential for slower transaction verification processes and lower scalability, depending on network scale, size and consensus algorithm.

Some argue that DLT-based CBDC transaction verification could support greater transparency in CBDC payment processes or better preserve the anonymity of senders and receivers. However, both a DLT-based and traditional central bank-managed system could make transaction records publicly visible in real time if needed or support pseudonymous accounts or obfuscated transaction information. All else being equal, the narrower set of validators within a central banking system, potentially only the central bank, preserves confidentiality to a greater degree.

It might be argued that a DLT-based system could provide greater resilience and continuous functionality from the participation of multiple nodes in the transaction validation process. However, DLT systems are largely untested at scale and involve new or different security vulnerabilities and complexities. Compared with time-tested software systems, they may not increase overall system resilience.

Wholesale CBDC in cross-border interbank securities transactions and funds transfers

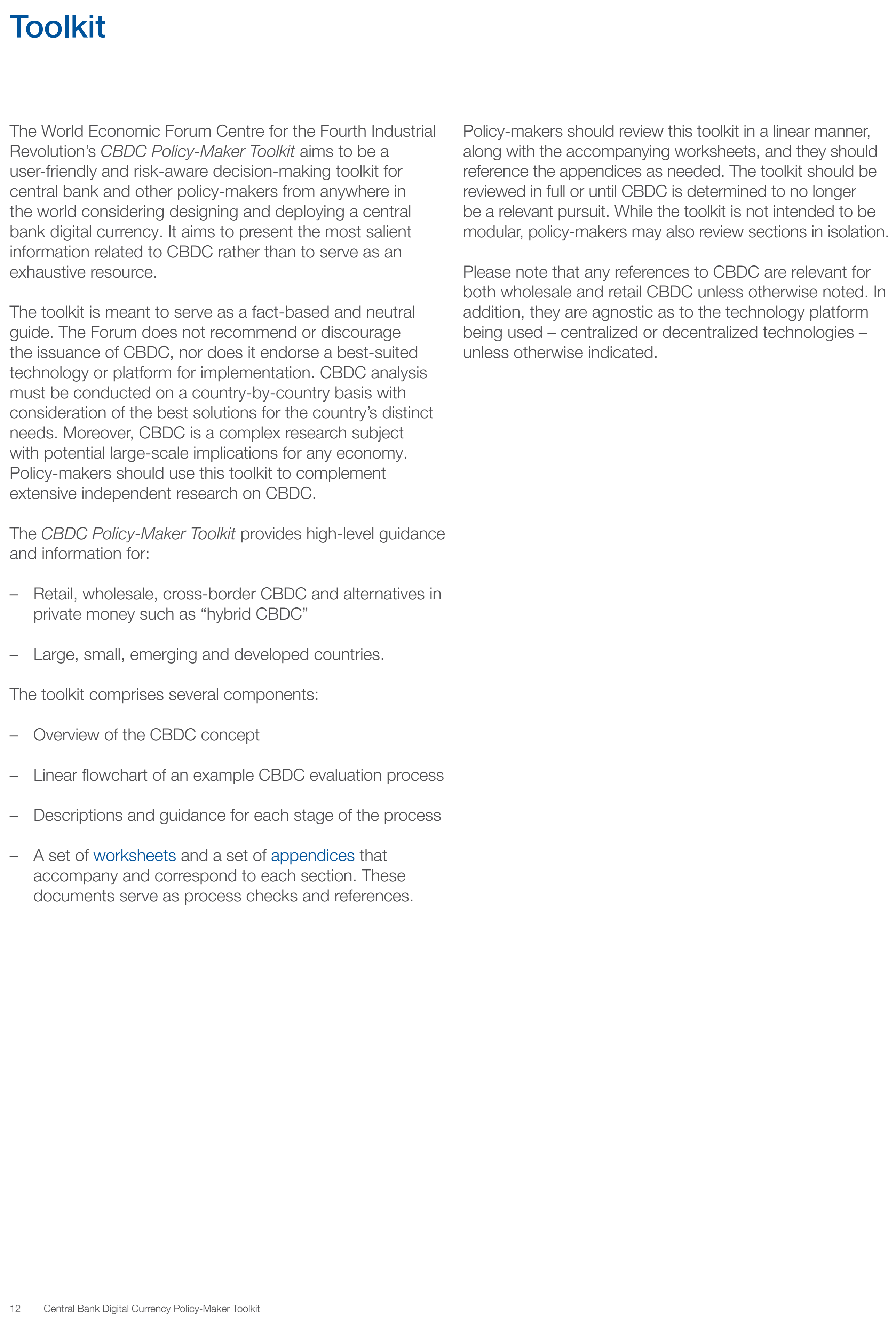
The programmable nature of wholesale CBDC can support interbank securities and derivatives transactions, including cross-border "atomic" swap transactions. Collaborative research published in 2019 by the Monetary Authority of Singapore and the Bank of4 Canada and by the European Central Bank and the Bank of Japan investigates DLT for enabling rapid and complete cross-border interbank securities transactions using a blockchain-based wholesale CBDC. Using conditional programming and cryptographic hash functions in a process called "hash time-locked contracts", the full and final payment and settlement for a trade occurs at the same time the asset is fully (or "atomically") delivered to the buyer. Both the asset and currency are located on the distributed ledger and they are traded simultaneously (this capability supports delivery-versus-payment goals). The nature of the "atomic" transaction is such that either both delivery and payment happen simultaneously or neither occurs. The result is greater operational efficiency and reduced settlement and counterparty risk.

While both research projects mentioned in the previous paragraph employ blockchain technology, the functionality for "atomic" swap transactions does not depend on DLT but rather on conditional programming and general-purpose hash functions. However, using "smart contracts" with blockchain technology could enable certain benefits such as automated and transparent escrow accounts for participants that reduce the need for intermediaries such as clearing houses or custodians to guarantee and deliver funds in exchange for assets. Depending on implementation, this capability may constitute another benefit of employing DLT.

Wholesale CBDC could also be applied to use cases and applications in cross-border fund transfers and financial market infrastructure, where it could provide benefits such as improved efficiencies through reduced settlement layers, better foreign exchange liquidity management and streamlined regulatory compliance. For instance, the Bank of Thailand and Hong Kong Monetary Authority's Project LionRock-Inthanon experiments with creating a DLT-based corridor network that allows banks in two jurisdictions to conduct instantaneous peer-to-peer transactions using wholesale CBDC across borders. Using smart contracts, cross-border fund transfers can be embedded with foreign-exchange transactions so that on-demand foreign-exchange liquidity management can be achieved.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



Toolkit

The World Economic Forum Centre for the Fourth Industrial Revolution's *CBDC Policy-Maker Toolkit* aims to be a user-friendly and risk-aware decision-making toolkit for central bank and other policy-makers from anywhere in the world considering designing and deploying a central bank digital currency. It aims to present the most salient information related to CBDC rather than to serve as an exhaustive resource.

The toolkit is meant to serve as a fact-based and neutral guide. The Forum does not recommend or discourage the issuance of CBDC, nor does it endorse a best-suited technology or platform for implementation. CBDC analysis must be conducted on a country-by-country basis with consideration of the best solutions for the country's distinct needs. Moreover, CBDC is a complex research subject with potential large-scale implications for any economy. Policy-makers should use this toolkit to complement extensive independent research on CBDC.

The *CBDC Policy-Maker Toolkit* provides high-level guidance and information for:

- Retail, wholesale, cross-border CBDC and alternatives in private money such as "hybrid CBDC"
- Large, small, emerging and developed countries.

The toolkit comprises several components:

- Overview of the CBDC concept
- Linear flowchart of an example CBDC evaluation process
- Descriptions and guidance for each stage of the process
- A set of worksheets and a set of appendices that accompany and correspond to each section. These documents serve as process checks and references.

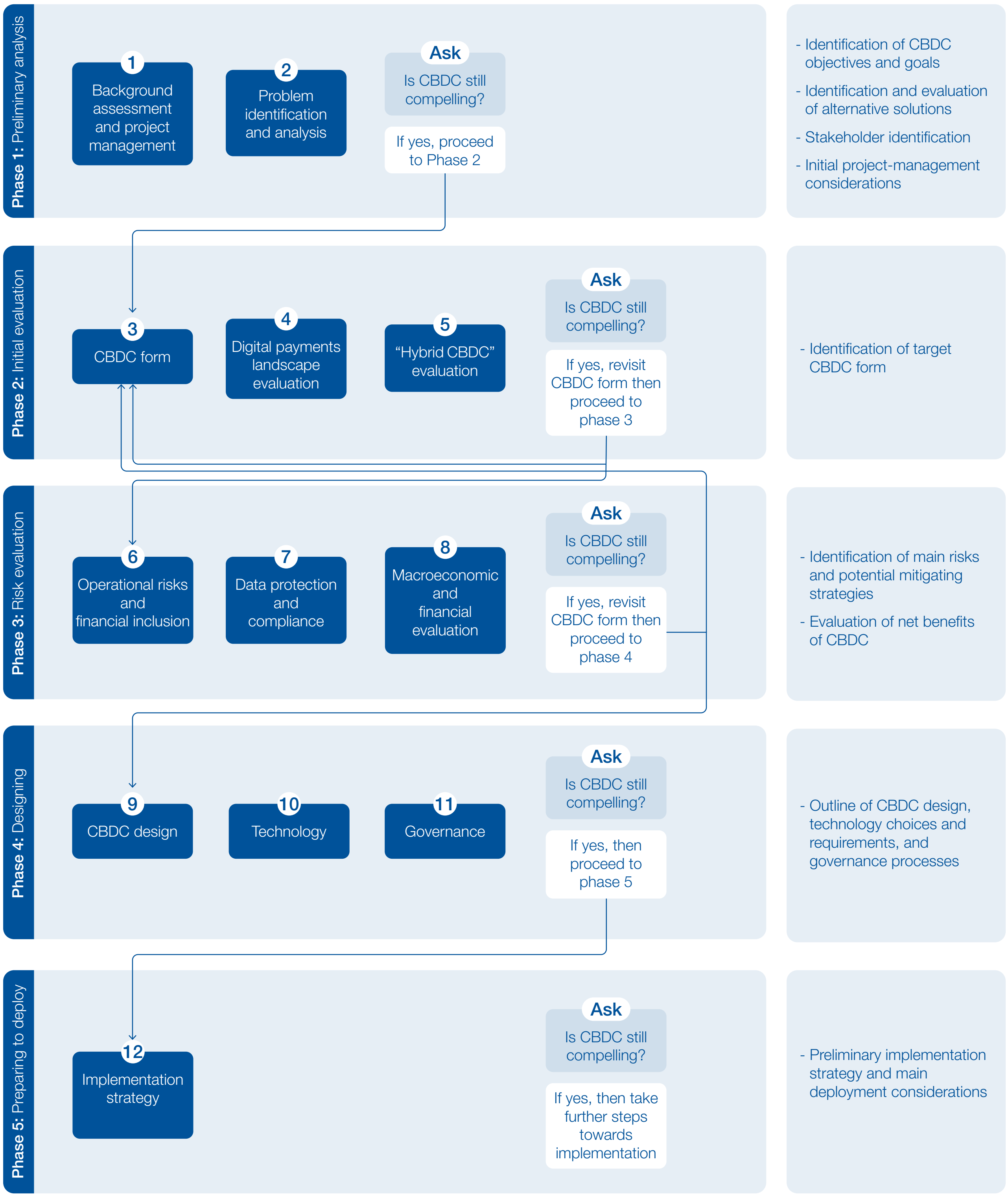
Policy-makers should review this toolkit in a linear manner, along with the accompanying worksheets, and they should reference the appendices as needed. The toolkit should be reviewed in full or until CBDC is determined to no longer be a relevant pursuit. While the toolkit is not intended to be modular, policy-makers may also review sections in isolation.

Please note that any references to CBDC are relevant for both wholesale and retail CBDC unless otherwise noted. In addition, they are agnostic as to the technology platform being used – centralized or decentralized technologies – unless otherwise indicated.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

The graphic below illustrates the CBDC decision flow chart:



Phase 1: Preliminary analysis

1 Background assessment and project management

2 Problem identification and analysis

Ask: Is CBDC still compelling?

If yes, proceed to Phase 2

- Identification of CBDC objectives and goals
- Identification and evaluation of alternative solutions
- Stakeholder identification
- Initial project-management considerations

Phase 2: Initial evaluation

3 CBDC form

4 Digital payments landscape evaluation

5 "Hybrid CBDC" evaluation

Ask: Is CBDC still compelling?

If yes, revisit CBDC form then proceed to phase 3

- Identification of target CBDC form

Phase 3: Risk evaluation

6 Operational risks and financial inclusion

7 Data protection and compliance

8 Macroeconomic and financial evaluation

Ask: Is CBDC still compelling?

If yes, revisit CBDC form then proceed to phase 4

- Identification of main risks and potential mitigating strategies
- Evaluation of net benefits of CBDC

Phase 4: Designing

9 CBDC design

10 Technology

11 Governance

Ask: Is CBDC still compelling?

If yes, then proceed to phase 5

- Outline of CBDC design, technology choices and requirements, and governance processes

Phase 5: Preparing to deploy

12 Implementation strategy

Ask: Is CBDC still compelling?

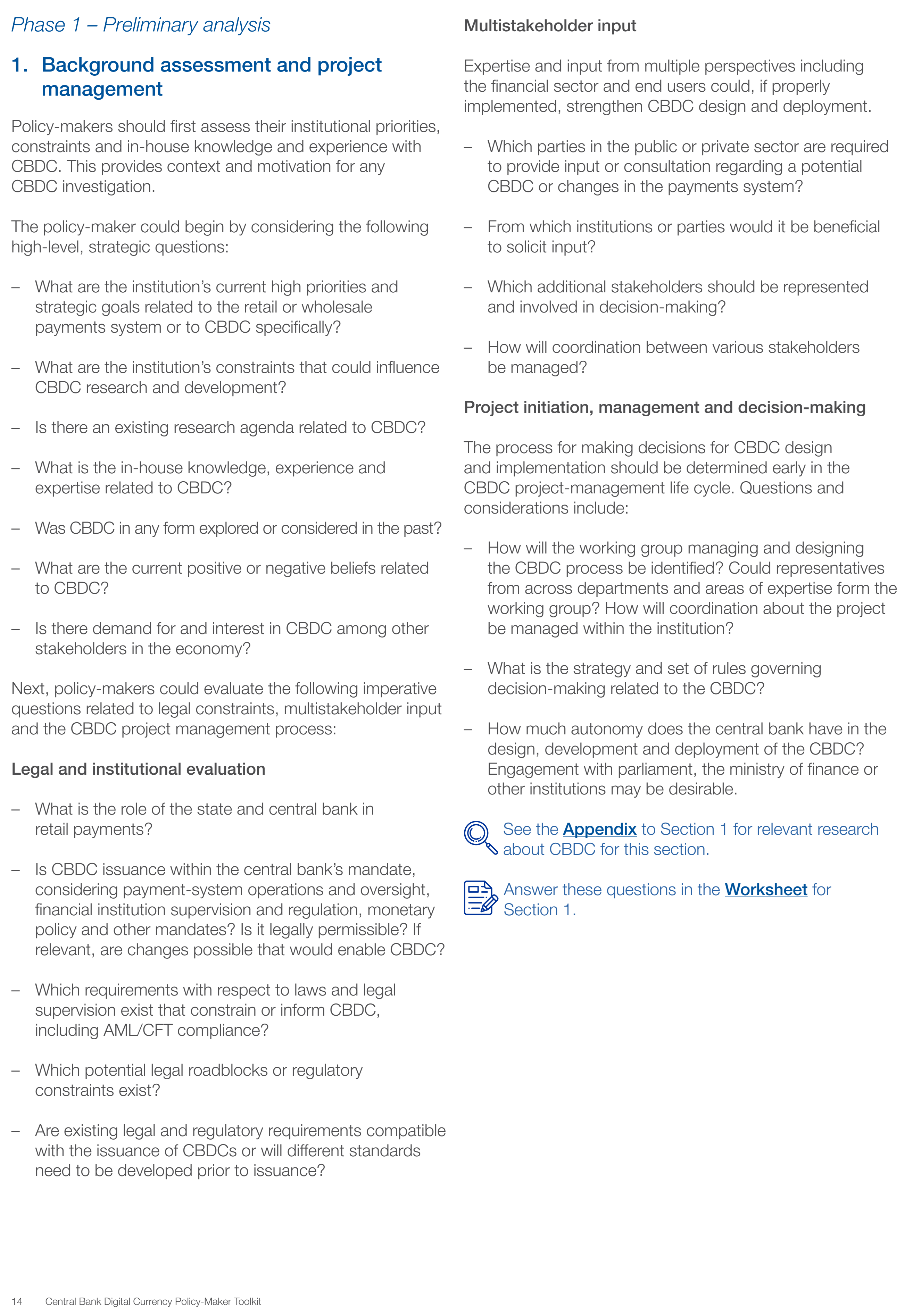
If yes, then take further steps towards implementation

- Preliminary implementation strategy and main deployment considerations

The flowchart above serves as an example of a CBDC evaluation and design process. Each country's approach to evaluating CBDC will be unique and should follow its needs and interests. For instance, CBDC evaluation may take a more dynamic or cyclical form, where issues are continually re-evaluated.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



Phase 1 – Preliminary analysis

1. Background assessment and project management

Policy-makers should first assess their institutional priorities, constraints and in-house knowledge and experience with CBDC. This provides context and motivation for any CBDC investigation.

The policy-maker could begin by considering the following high-level, strategic questions:

- What are the institution's current high priorities and strategic goals related to the retail or wholesale payments system or to CBDC specifically?
- What are the institution's constraints that could influence CBDC research and development?
- Is there an existing research agenda related to CBDC?
- What is the in-house knowledge, experience and expertise related to CBDC?
- Was CBDC in any form explored or considered in the past?
- What are the current positive or negative beliefs related to CBDC?
- Is there demand for and interest in CBDC among other stakeholders in the economy?

Next, policy-makers could evaluate the following imperative questions related to legal constraints, multistakeholder input and the CBDC project management process:

Legal and institutional evaluation

- What is the role of the state and central bank in retail payments?
- Is CBDC issuance within the central bank's mandate, considering payment-system operations and oversight, financial institution supervision and regulation, monetary policy and other mandates? Is it legally permissible? If relevant, are changes possible that would enable CBDC?
- Which requirements with respect to laws and legal supervision exist that constrain or inform CBDC, including AML/CFT compliance?
- Which potential legal roadblocks or regulatory constraints exist?
- Are existing legal and regulatory requirements compatible with the issuance of CBDCs or will different standards need to be developed prior to issuance?

Multistakeholder input

Expertise and input from multiple perspectives including the financial sector and end users could, if properly implemented, strengthen CBDC design and deployment.

- Which parties in the public or private sector are required to provide input or consultation regarding a potential CBDC or changes in the payments system?
- From which institutions or parties would it be beneficial to solicit input?
- Which additional stakeholders should be represented and involved in decision-making?
- How will coordination between various stakeholders be managed?

Project initiation, management and decision-making

The process for making decisions for CBDC design and implementation should be determined early in the CBDC project-management life cycle. Questions and considerations include:

- How will the working group managing and designing the CBDC process be identified? Could representatives from across departments and areas of expertise form the working group? How will coordination about the project be managed within the institution?
- What is the strategy and set of rules governing decision-making related to the CBDC?
- How much autonomy does the central bank have in the design, development and deployment of the CBDC? Engagement with parliament, the ministry of finance or other institutions may be desirable.

See the **Appendix** to Section 1 for relevant research about CBDC for this section.

Answer these questions in the **Worksheet** for Section 1.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

2. Problem identification and analysis

In this stage, the policy-maker identifies the various challenges that a CBDC could potentially help address. He or she also conducts a preliminary analysis of the feasibility and suitability of CBDC to address these problems relative to high-potential alternative solutions. While the answers to these questions may change as the policy-maker proceeds through the toolkit, they are an essential first step to critically review CBDC and understand its potential role in the economy.

To begin, list the major country-specific geographic, political, economic and technological conditions that could affect the usefulness or desirability of CBDC:

Examples:

- **Geographic:** A country with many small islands or severe weather seasons may have cash distribution, availability and security challenges and benefit from CBDC.

- **Political:** A democratic country may want multistakeholder involvement in decisions about issuing retail CBDC and cash policies.

- **Economic:** A dollarized economy may benefit from CBDC if it has a shortage of small currency; a country with a fragmented payments system or low financial inclusion could benefit from a retail CBDC that harmonizes existing payment systems and connects citizens to bank accounts.

- **Technological:** A country with high internet connectivity and mobile phone penetration could have greater adoption of retail CBDC. A country with rapidly declining cash usage could benefit from the availability of a retail CBDC as a public option for digital payments.

Start by identifying the problems that CBDC could address, examining how viable and feasible CBDC is in addressing these problems and the viability of alternative solutions.

- What are the most important problems or challenges that a CBDC could potentially address, considering both retail and wholesale payments?

- How valuable or important is it to address these problems?

- How feasible and suitable is CBDC to solve these specific problems?

- What is the highest-potential corresponding alternative solution that could also address these problems?

After the preliminary analysis above, could CBDC potentially effectively address high-priority problems or challenges? Which ones?

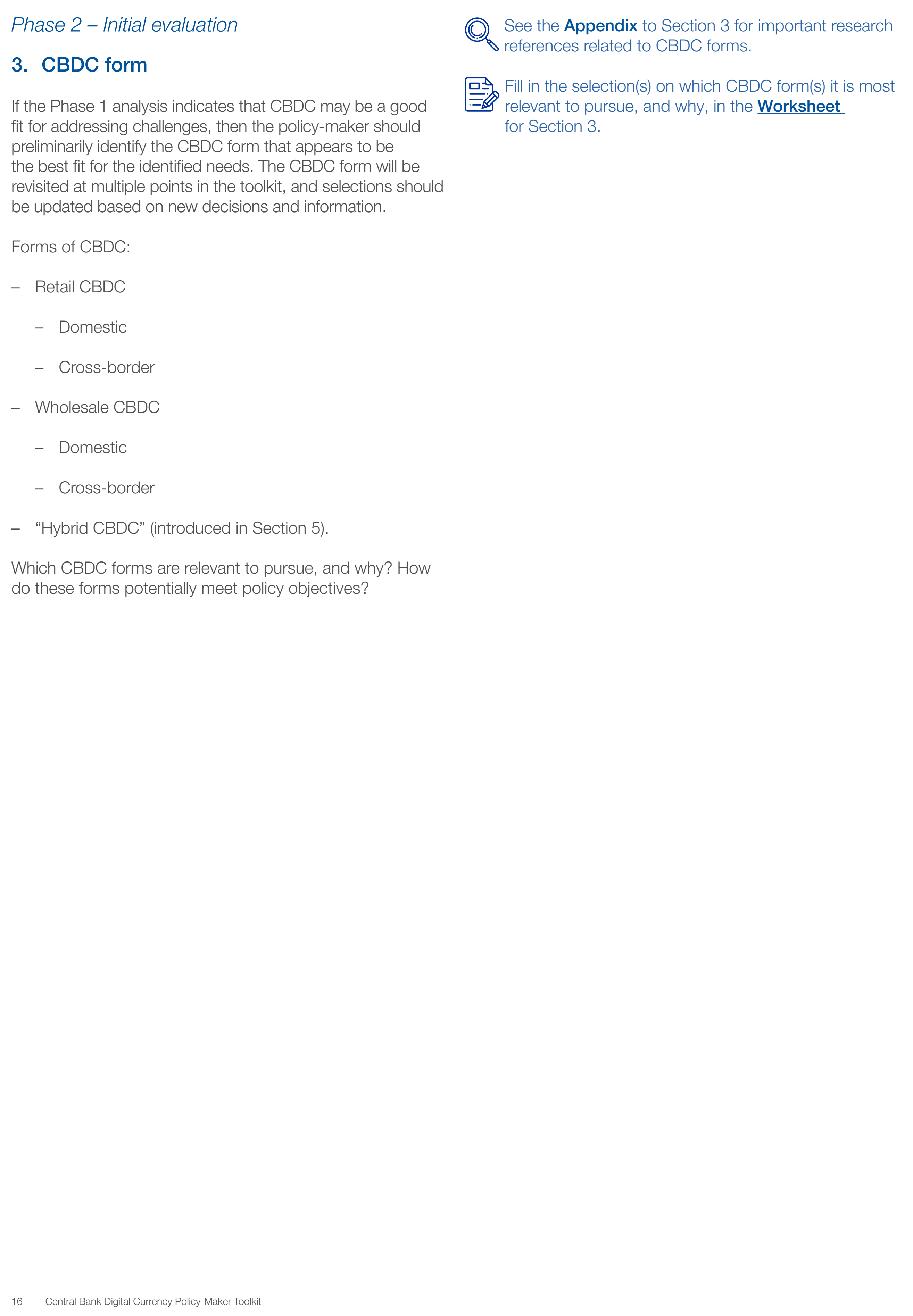
See the **Appendix** to Section 2 for information that can inform answers to the questions.

Answer the questions for this section in the **Worksheet** for Section 2.

If there are no relevant objectives or high-potential CBDC applications identified, consider pausing evaluation of CBDC.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



Phase 2 – Initial evaluation

3. CBDC form

If the Phase 1 analysis indicates that CBDC may be a good fit for addressing challenges, then the policy-maker should preliminarily identify the CBDC form that appears to be the best fit for the identified needs. The CBDC form will be revisited at multiple points in the toolkit, and selections should be updated based on new decisions and information.

Forms of CBDC:

- Retail CBDC
  - Domestic
  - Cross-border
- Wholesale CBDC
  - Domestic
  - Cross-border
- "Hybrid CBDC" (introduced in Section 5).

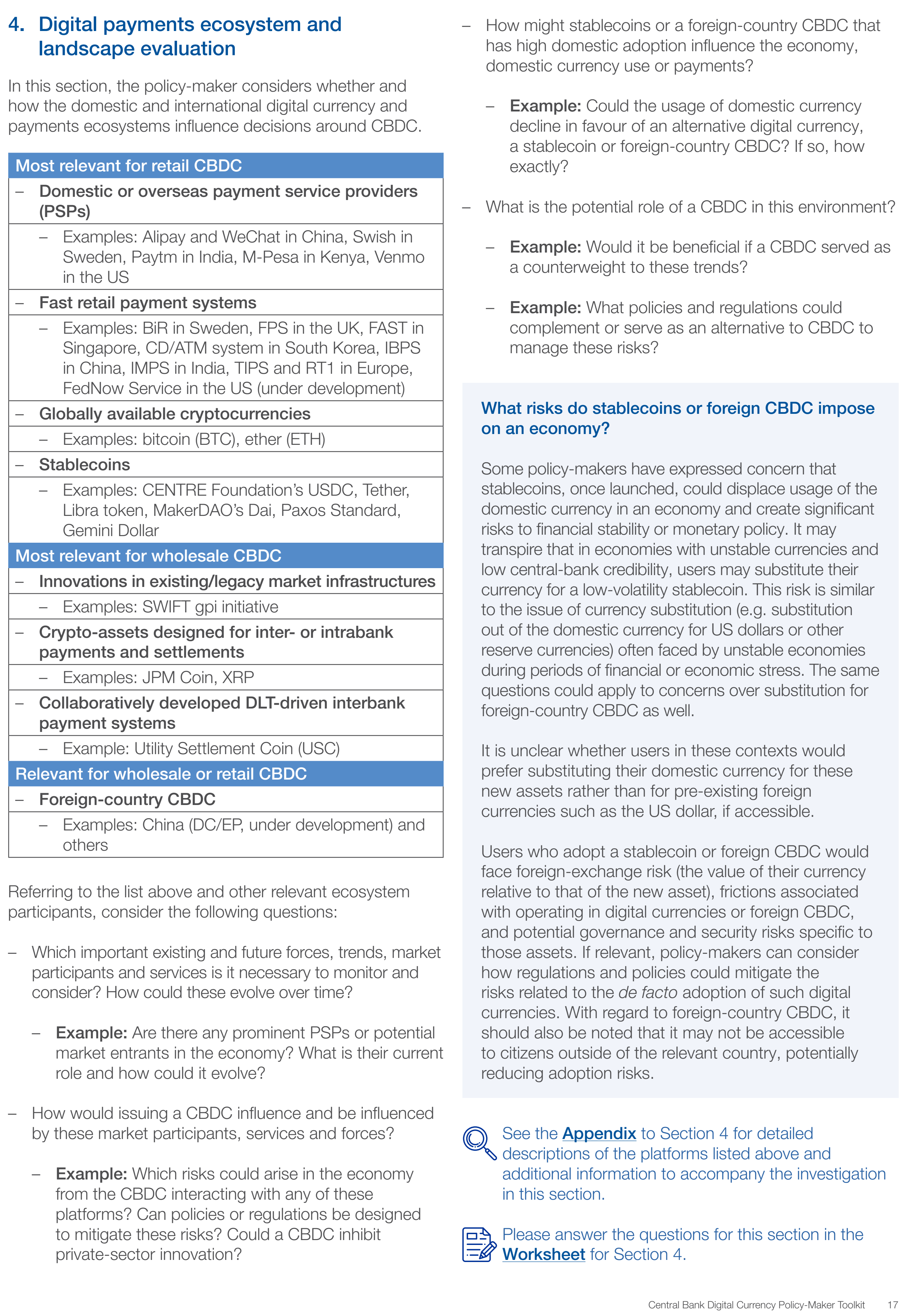
Which CBDC forms are relevant to pursue, and why? How do these forms potentially meet policy objectives?

See the **Appendix** to Section 3 for important research references related to CBDC forms.

Fill in the selection(s) on which CBDC form(s) it is most relevant to pursue, and why, in the **Worksheet** for Section 3.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**



4. Digital payments ecosystem and landscape evaluation

In this section, the policy-maker considers whether and how the domestic and international digital currency and payments ecosystems influence decisions around CBDC.

Most relevant for retail CBDC
– **Domestic or overseas payment service providers (PSPs)**
– Examples: Alipay and WeChat in China, Swish in Sweden, Paytm in India, M-Pesa in Kenya, Venmo in the US
– **Fast retail payment systems**
– Examples: BiR in Sweden, FPS in the UK, FAST in Singapore, CD/ATM system in South Korea, IBPS in China, IMPS in India, TIPS and RT1 in Europe, FedNow Service in the US (under development)
– **Globally available cryptocurrencies**
– Examples: bitcoin (BTC), ether (ETH)
– **Stablecoins**
– Examples: CENTRE Foundation's USDC, Tether, Libra token, MakerDAO's Dai, Paxos Standard, Gemini Dollar
Most relevant for wholesale CBDC
– **Innovations in existing/legacy market infrastructures**
– Examples: SWIFT gpi initiative
– **Crypto-assets designed for inter- or intrabank payments and settlements**
– Examples: JPM Coin, XRP
– **Collaboratively developed DLT-driven interbank payment systems**
– Example: Utility Settlement Coin (USC)
Relevant for wholesale or retail CBDC
– **Foreign-country CBDC**
– Examples: China (DC/EP, under development) and others

Referring to the list above and other relevant ecosystem participants, consider the following questions:

- Which important existing and future forces, trends, market participants and services is it necessary to monitor and consider? How could these evolve over time?
  - **Example:** Are there any prominent PSPs or potential market entrants in the economy? What is their current role and how could it evolve?
- How would issuing a CBDC influence and be influenced by these market participants, services and forces?
  - **Example:** Which risks could arise in the economy from the CBDC interacting with any of these platforms? Can policies or regulations be designed to mitigate these risks? Could a CBDC inhibit private-sector innovation?
- How might stablecoins or a foreign-country CBDC that has high domestic adoption influence the economy, domestic currency use or payments?
  - **Example:** Could the usage of domestic currency decline in favour of an alternative digital currency, a stablecoin or foreign-country CBDC? If so, how exactly?
- What is the potential role of a CBDC in this environment?
  - **Example:** Would it be beneficial if a CBDC served as a counterweight to these trends?
  - **Example:** What policies and regulations could complement or serve as an alternative to CBDC to manage these risks?

What risks do stablecoins or foreign CBDC impose on an economy?

Some policy-makers have expressed concern that stablecoins, once launched, could displace usage of the domestic currency in an economy and create significant risks to financial stability or monetary policy. It may transpire that in economies with unstable currencies and low central-bank credibility, users may substitute their currency for a low-volatility stablecoin. This risk is similar to the issue of currency substitution (e.g. substitution out of the domestic currency for US dollars or other reserve currencies) often faced by unstable economies during periods of financial or economic stress. The same questions could apply to concerns over substitution for foreign-country CBDC as well.

It is unclear whether users in these contexts would prefer substituting their domestic currency for these new assets rather than for pre-existing foreign currencies such as the US dollar, if accessible.

Users who adopt a stablecoin or foreign CBDC would face foreign-exchange risk (the value of their currency relative to that of the new asset), frictions associated with operating in digital currencies or foreign CBDC, and potential governance and security risks specific to those assets. If relevant, policy-makers can consider how regulations and policies could mitigate the risks related to the *de facto* adoption of such digital currencies. With regard to foreign-country CBDC, it should also be noted that it may not be accessible to citizens outside of the relevant country, potentially reducing adoption risks.

See the **Appendix** to Section 4 for detailed descriptions of the platforms listed above and additional information to accompany the investigation in this section.

Please answer the questions for this section in the **Worksheet** for Section 4.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

5. ‘Hybrid CBDC’ evaluation

In July 2019, authors at the International Monetary Fund (IMF) proposed the concept of a “synthetic CBDC”, which could also be called “reserve-backed private tokens” or “hybrid CBDC”. Policy-makers considering retail CBDC could review the IMF’s paper, *The Rise of Digital Money*, and the briefer blog post, *From Stablecoins to Central Bank Digital Currencies*, to learn more about this concept.

In this alternative to CBDC, the central bank allows financial institutions such as electronic money or payment service providers (PSP) that do not typically have access to the central bank’s deposit facility to hold reserves at the central bank, enabling stronger safeguards and monitoring of these organizations as well as potentially improving interoperability between different payment systems. For instance, conditions could be included in payment providers’ charters establishing that users of the payment system would have the first *lien* on the provider’s reserves or other assets in the event of bankruptcy. It is important to note that, unlike CBDC, “hybrid CBDC” is not a claim on the central bank in the case of issuer default.

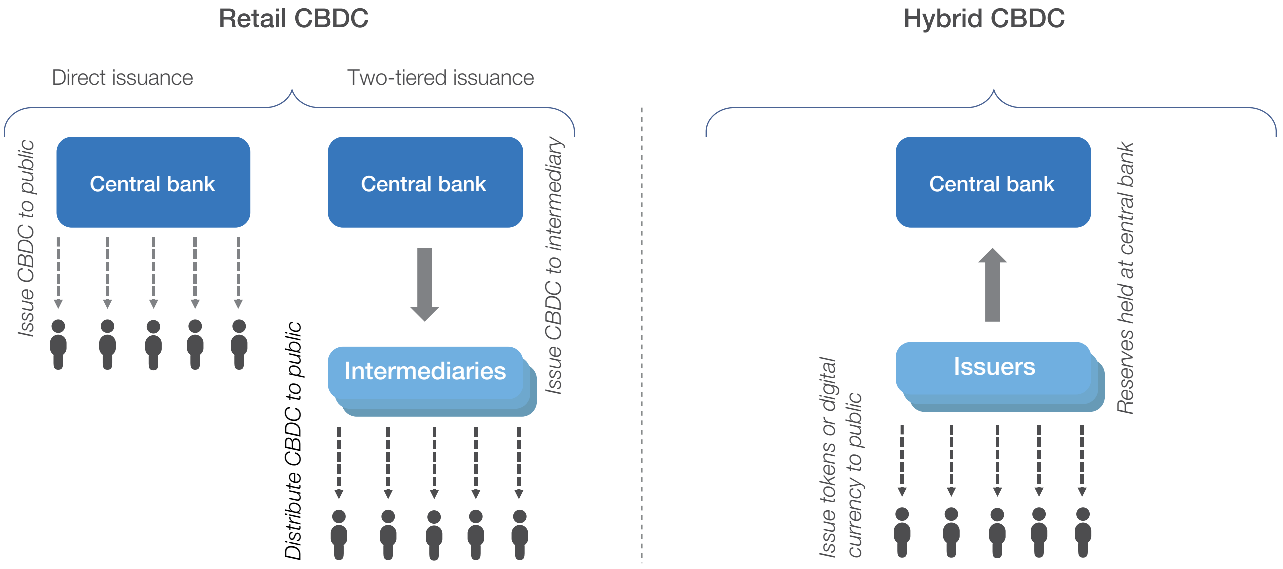
The value proposition of “hybrid CBDC” includes the following:

- It allows the central bank to support provision of stable and liquid electronic money by private institutions with safeguards and protections for user funds.
- It represents an alternative to regulation or retail CBDC in addressing payment-system stability and market power risks from widely adopted digital payment providers (including stablecoin providers).
- It could probably be implemented more rapidly than retail CBDC.
- In place of retail CBDC, it would allow central banks to focus on core competencies such as transaction settlement rather than a full suite of retail CBDC components and requirements (two-tiered CBDC also partly addresses this challenge).

Policy-makers who identified retail CBDC as an area of exploration should consider the following questions:

- Is “hybrid CBDC” a potential avenue for the institution? If so, which policy goals or objectives could it help deliver?
- What value does “hybrid CBDC” offer relative to retail CBDC (including retail CBDC issued via intermediaries in a two-tiered structure)?
- Are there statutory or policy constraints that might prevent the central bank from giving access to non-bank institutions?
- What could “hybrid CBDC” in the country look like? Are there specific types of financial institutions it could make sense to include or not include? What types of oversight regimes could be appropriate?

The graphic below portrays retail and “hybrid CBDC”:



See the **Appendix** to Section 5 for additional information to accompany your investigation of this section.

Please answer the questions for this section in the **Worksheet** for Section 5.

In the **Worksheet** to Complete Phase 2, re-evaluate at this stage whether CBDC remains a compelling value proposition. If not, consider pausing analysis of CBDC. It may also be relevant to revisit Section 3, CBDC form, after having evaluated “hybrid CBDC”.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Phase 3 – Risks evaluation

6. Operational risks and financial inclusion in retail CBDC

When considering the introduction of a retail CBDC, the issuing central bank must evaluate the technological and operational risks that can negatively affect users, along with accessibility and financial inclusion. The central bank should, in all cases, set and enforce strong policies that reduce the risks to the general public, ensuring constant CBDC availability and designing back-up strategies and systems.

What are the technological risks that must be considered prior to CBDC implementation?

Network failure and operational risks – For all forms of CBDC, as payments are integral to the economy, the central bank and policy-makers must seek to enable the greatest degree of system availability possible, implementing safeguards and contingency plans that reduce risks to system interruption. CBDC system availability and continuous 24/7 access should be designed to consider people living beyond the reach of the internet or who do not have regular internet access; this is essential for refugees and people living in remote settings. The system must also protect the availability of CBDC from physical disruption of systems or infrastructure (e.g. large-scale electricity interruptions from storms).

Cybersecurity risks – Central banks must create precautions and robust cyber-resiliency policies to reduce risks from cyberattacks. They should operate under the assumption that a cyberattacker has unlimited resources, as it is not unthinkable that the attacker could be a foreign government. Contingency systems such as available sources of physical cash (for a retail CBDC system shutdown) should be put in place to maintain necessary liquidity in the event of an interruption of digital systems.

How can a retail CBDC be designed to enable greater financial inclusion?

Accessibility and financial inclusion – New CBDC implementation should strive to maximize participation in financial systems and not reinforce existing barriers or erect new barriers to inclusion for vulnerable populations.

- According to the World Bank, 1.7 billion people live without access to any form of identification and are therefore typically excluded from regulated financial services. Without proper design and customer identification policies, populations that do not have access to traditional forms of government-recognized identification may be excluded from CBDC.

- Elderly people are also at risk of exclusion from participation due to their lower than average willingness or ability to engage with technology.

- Those with disabilities such as blindness should be accounted for in CBDC design and development.

Tourists may struggle to make payments in an economy heavily reliant on retail CBDC if ownership is limited to residents and domestic institutions. Accessibility considerations should also include CBDC interoperability with existing payment systems, such as debit or credit cards.

A CBDC should have no or very limited cost to users. Costs related to telecommunications and mobile phones involved in CBDC must be transparent and low to support inclusion (and to increase the value of the CBDC in general). CBDC custody should not rest fully within the mobile phone, so that a customer who loses his or her phone does not lose his or her CBDC holdings.

It may be worth considering whether CBDC accessibility can be improved with technology. It could be possible to meet KYC/AML/CFT goals without mandating the requirement of government-issued identity documents, opening participation to a wider audience and supporting financial-inclusion goals. New digital identity capabilities, such as biometrics or other non-traditional mechanisms, could potentially validate a user's identity. However, policy-makers should be aware that people may be hesitant to use biometrics as identity verification. The security of alternative identity approaches must also be strongly considered.

The importance of cash

Physical cash, particularly small banknotes, guarantees financial inclusion more than any other means of payment. Cash serves as a last-resort means of payment and store of value in the event of payment-system shocks and failures. For many, it is also their primary means of payment and savings. The central bank should not develop policies that remove small banknotes from retail use until a fully reliable alternative is available to all members of the population, which may not be possible.

See the **Appendix** to Section 6 for additional information to accompany this section.

Please answer the questions for this section in the **Worksheet** for Section 6.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

7. Data protections and compliance for retail CBDC

Upon issuance of a retail CBDC, the central bank is extending its involvement in the retail payment system, and as a result is also extending its responsibility. It must balance user data privacy goals with AML/CFT requirements and the need to limit illicit activity within the CBDC system.

What are the main issues related to data privacy for CBDC?

Data privacy risks – User privacy is one of the most important considerations for CBDC. Access to a user's transaction history not only allows for tracking spending habits but can also enable location tracking and identification of sensitive personal data. If retail CBDC is used widely, the monetary authority must design and implement strict user data storage and privacy policies and protections. For instance, protections could ensure users are not unlawfully discriminated against because of their spending habits or targeted for data privacy abuses based on membership of certain subpopulations.

The system must have safeguards to reasonably ensure the security, privacy and confidentiality of transaction and identity data while protecting against unauthorized access, acquisition, alteration, disclosure or destruction of that data. User data privacy should be a priority, not only to protect citizens from the risks of potential state-level surveillance but also to reduce vulnerabilities to external cyberattacks by domestic or foreign parties. Accordingly, CBDC should be designed with as much anonymity as possible, taking into consideration AML/CFT regulations and security policies.

Another potential issue related to user data privacy arises if retail users can employ the retail CBDC of other countries. If foreign-country CBDC has different customer data privacy policies and safeguards, then user data may be vulnerable when people use those CBDCs. Policy-makers may need to consider regulating foreign-country CBDCs to protect the public from data privacy abuses.

Customer data policy

It might be prudent to develop a user data policy that clearly articulates the rules for data management, access, privacy and custody. It should reduce any applicable conflicts of interest and be clearly connected to governance processes with strict requirements and penalties for violations.

As part of the policy, citizens should receive an understandable explanation of when, how, by whom and for what purposes their data is being collected, used, shared and retained.

Data access and portability – New CBDC implementation should strive to maximize user agency and trust. Users should have a right to access and share their data as they choose in a structured and standardized format. They must also have the right to dispute the accuracy of their data and to have erroneous data promptly corrected, updated or deleted.

See the **Appendix** to Section 7 for information about modern cryptography techniques that can provide transaction privacy and confidentiality while meeting regulatory and other goals.

Please answer the questions for this section in the **Worksheet** for Section 7.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

8. Evaluation of macroeconomic and financial risks and opportunities

The policy-maker should next evaluate the main macroeconomic and financial risks and opportunities that a CBDC presents. Several points within this section correspond with issues identified in other sections of this toolkit; where relevant, these concepts can be revisited or revised.

- What important macroeconomic and financial goals or opportunities could this form of CBDC enable in the economy?
- Which macroeconomic and financial risks is it important to consider? Which solutions or strategies can mitigate risks?
- Who will have access to the CBDC, in terms of domestic and foreign citizens and financial institutions?
- What is the anticipated effect on banks? How are the roles and business models of banks expected to change after CBDC is deployed?
- Which additional types of firms would be positively or negatively affected by CBDC?
- What are the effects of CBDC (interest-bearing or not) on monetary policy?
- What would be the implications of CBDC for the domestic political environment, government institutions and geopolitics?
- Which macroeconomic policy decisions should be made with respect to CBDC?
  - Will CBDC be used to implement monetary policy goals and, if so, how? Will a CBDC be allowed to implement negative interest rates?
  - Will there be any significant cash policies implemented alongside CBDC?
  - Will there be lending activity associated with a retail CBDC? Why or why not?
  - Would a CBDC interact with existing policies related to international capital mobility?

Revisit the **Appendix** to Section 2 for information about the main macroeconomic and financial issues related to CBDC that can inform the answers to the questions in this section. See the Appendix to Section 8 for research references to accompany this section.

Please answer the questions for this section in the **Worksheet** for Section 8.

In the **Worksheet** to Complete Phase 3, list the top benefits of the CBDC envisioned, as well as the main risks and downsides. Do the benefits outweigh the identified risks and downsides? If not, consider pausing or stopping the evaluation of the CBDC. If they do, consider revisiting Step 3, CBDC form, if relevant. Once this is complete, proceed to Phase 4, Designing CBDC.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Phase 4 – Designing

9. CBDC design elements

In this phase, the policy-maker considers how the CBDC should be designed in order to achieve the target outcomes and mitigate the risks identified in the preceding sections of this toolkit.

- *Availability/access* – For which entities should the CBDC be available? For retail CBDC, will foreign citizens, tourists or other parties have access? For wholesale CBDC, will foreign commercial or central banks, non-bank corporates, investment funds, stablecoin providers or systemically important financial institutions have access?

- *Custody and storage* – Where will the CBDC be held? Will it be held with accounts directly or indirectly at the central bank or in digital wallets of various forms? Will a two-tiered system be used?

- *Anonymity* – To what degree is the user, account balance and transaction information private or pseudonymous? Which regulatory, legal or compliance policies constrain anonymity? What are the goals of the CBDC with respect to transaction tracing, monitoring or anonymity? Does the degree of anonymity correspond with the transaction sizes?

- *Account and transaction limits* – Should there be limits or constraints on transaction size or total account balance?

- *Interest payments* – What is the interest rate policy for the CBDC? Should a retail or wholesale CBDC pay interest (including, possibly, a negative one)? How do monetary policy and financial stability goals and risks determine the appropriate interest rate policy?

- *Conversions and redemption rates* – What are the conversion or redemption policies related to a retail CBDC with respect to bank deposits or cash? For a wholesale CBDC?

- *Settlement times and finality* – Should settlement be near-immediate and available 24/7/365 (more “cash-like”), periodic or delayed in order to allow more time for recourse and compliance requirements? Which compliance and other laws constrain settlement and finality options?

- *Programmability features* – For what purposes and capabilities should the CBDC be potentially programmable, if any? (For instance, cross-border “atomic” interbank transactions.)

- *Lending activity* – Should central banks or intermediaries conduct lending activity on CBDC?

See the **Appendix** to Section 9 for information and research references to accompany this section.

Please answer the questions for this section in the **Worksheet** for Section 9.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

10. Technology choices, considerations and risks

After the target CBDC design is fully defined, the policy-maker can then investigate and identify the most suitable technology to deliver the CBDC. It is valuable to wait until as late in the process as possible to identify the target technology solution, suspending preconceived notions in order to allow for more flexibility and informed technology decisions. CBDC issuance and design is largely a technology-agnostic decision. Importantly, policy-makers should conduct their own research and fully evaluate technology solutions and providers, and they should be wary of simply selecting a convenient technology solution. Given the target CBDC identified in the preceding sections of the toolkit, evaluate the following:

Core functionalities

Which characteristics are priorities?

- Transaction scalability and performance
- Privacy and confidentiality of transaction information
- Transaction finality
- Interoperability with existing payment systems and infrastructure.

Technology assessment

- What are the trade-offs, pros and cons associated with various technology options?
- If DLT is considered, who would serve as validating nodes? Which platform and consensus algorithm may be relevant to employ and why?
- Which technology providers, services or experts can support implementation?
- Which technologies may be best suited, and why?

Cost assessment

- What cost constraints exist for the CBDC implementation?
- How much will it cost to implement this target technology?
- How much maintenance will be needed with this technology and what are the associated costs?

Cybersecurity and resilience

- How cyber resilient is the platform, and why? What are the CBDC's cybersecurity vulnerabilities or "attack surfaces"?
- What are the appropriate cyber-resilience requirements? How can the system's cyber resilience be studied?
- Which cybersecurity standards and techniques must be identified to reduce cyber risks?
- What are the ongoing cybersecurity monitoring requirements for this technology implementation? How will monitoring and upgrades be conducted so as to be minimally disruptive?

Additional considerations

- How can vendor lock-in be avoided?
- How much has this technology been deployed and tested in the world? Is there sufficient software-developer availability and expertise to support the platform?
- How will this technology integrate with legacy systems and processes?
- How will this technology interoperate with existing and future financial systems?
- What are the ongoing monitoring requirements of this technology?
- How will the CBDC be minted (digitally created)?

Interoperability and integration

Interoperability with existing and future systems is critical to ensure the adoption and longevity of CBDC. If multiple central banks issue CBDC, there may be an opportunity for the coordination of international standards to ensure technical interoperability between a CBDC infrastructure and payment and banking systems, and between cross-border CBDCs. Policy-makers should also consider the technology infrastructure that would support cross-border CBDC and currency-exchange operations, and retail CBDC for tourists, if relevant.

See the **Appendix** to Section 10 for information and research references to accompany this section.

Please answer the questions for this section in the **Worksheet** for Section 10.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

11. Governance

Governance entails the rules and practices that govern the life cycle of the CBDC, from co-design to issuance. Good governance is a crucial ingredient of a successful deployment and should not be overlooked. Policy-makers should use the list below as a starting point to define governance with the appropriate stakeholders.

Legal evaluation

- Which requirements exist with respect to laws and legal supervision?
- Would a retail CBDC be politically feasible? How might political limitations affect CBDC design? (For instance, would a negative interest rate on retail CBDC be politically tenable?)
- How will public interest in CBDC be determined?
- Should there be any special consideration if there is an upcoming election cycle?
- Are CBDCs compatible with existing financial market infrastructure (e.g. the rulebooks of payment and settlement systems) and what legal validation needs to take place to ensure that transactions on financial market infrastructure are legally enforceable?
- Are there additional requirements and standards that custodians and intermediaries would need to comply with in relation to CBDCs (e.g. with respect to standards around safeguarding private keys, secure storage etc.)?
- How would CBDC be treated from a prudential regulation or regulatory capital perspective? Are there prudential risks over and above those relating to traditional fiat currencies that must be considered?

User engagement

- User engagement and consultation are critical for effective CBDC design; users should be engaged as early in the CBDC process as feasible.
- How can end users (the public, commercial banks etc.) be consulted on the CBDC concept and provide input to the design and testing process?
- Which solution requirements exist for usability, user interfaces, identity and key management, privacy and security?
- It could be valuable to provide a user guide or FAQs to various classifications of participants, with educational resources and background information on how to successfully engage with the CBDC.

Financial management

- How will project financial management and monitoring occur?
- Which, if any costs might private entities have in providing the CBDC, and who is responsible for managing those costs?

Identification of performance criteria

Performance criteria should be identified before the launch of the CBDC in order to: 1) establish relevant targets and goals; 2) measure success and identify areas of improvement; 3) instil accountability in the programme; and 4) ensure success in meeting risk management and security requirements. A specific evaluation frequency (e.g. weekly or monthly) should be determined.

CBDC termination

A termination plan could be identified before project deployment. The plan might include the following considerations:

- What conditions would indicate that the CBDC programme should be terminated?
- Which obligations would need to be met before termination in order to reduce disruption and risks to users?
- How can the safety of public CBDC savings be ensured?
- How would CBDC be destroyed?

Additional considerations

- How will the environmental impact and footprint of the CBDC be monitored, evaluated and controlled?
- Can a third party such as a law-enforcement institution freeze CBDC account assets, and under what circumstances?
- What other deployment risks and unintended consequences must be considered?

See the **Appendix** to Section 11 for additional information to accompany this section.

Please answer the questions for this section in the **Worksheet** for Section 11.

By the end of Phase 4, the policy-maker should have a clear outline of the CBDC design, technology choices and requirements, and governance processes. Consider whether this formulation corresponds with the goals and constraints identified in Phase 1 (preliminary analysis). If not, revisit the appropriate sections of the toolkit. When ready, fill in the **Worksheet** to Complete Phase 4 before proceeding to Phase 5.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Phase 5 – Preparing to deploy

12. Implementation strategy

The purpose of this section is to inform vital considerations and requirements before implementing the CBDC solution envisioned in the toolkit.

Policy-makers should consider the following issues, among others, as part of a CBDC implementation strategy:

Experiments and prototyping

The CBDC solution may need to be tested or introduced on a trial basis prior to full deployment. For example, the policy-maker could engage in experimentation such as a proof-of-concept (PoC) or pilot, which can test against defined research goals and provide valuable insight into a potential CBDC deployment. For both experimentation and deployment, the central bank should work collaboratively with the stakeholders identified in Section 1, including relevant public-sector, regulatory, private-sector, civil society and technology parties.

Methodology

Furthermore, the CBDC design and development process should take an agile and flexible approach, adjusting according to testing, feedback and new research. For user-facing components, it should involve user input, testing and interviews to inform effective user-interface (UI) and user-experience (UX), taking a "user-centric" approach where possible. This methodology will strengthen adoption and usability.

Public engagement for retail CBDC

For retail CBDC, a strong public-engagement effort is imperative. Further, education and informational programmes should be created so that users can understand the advantages and risks related to the CBDC. One example of an important risk consideration for users is password or key management; teaching safe use of passwords and private keys is critical. The central bank could also provide user guides or FAQs about the CBDC to the public. The central bank should also consider a public communication strategy that could include town halls and live engagement.

Collaborative experimentation and deployment

Policy-makers could consider whether to cooperate with other central banks, international organizations, commercial banks or other governmental or financial institutions in the development of CBDC. Collaboration can strengthen knowledge-building and inform effective CBDC design and deployment, potentially leading to greater adoption and deployment success. International organizations that conduct research or other efforts related to CBDC include the IMF, the Inter-American Development Bank and the Bank for International Settlements, among others. Further, engagement with commercial banks may be beneficial or necessary for retail or wholesale CBDC development. Many experiments have involved commercial banks, strengthening cooperation with the private sector and the financial system.

Introduction plan

Lastly, the central bank should develop a CBDC introduction plan that considers vital factors such as:

- The scope, nature and specific deployment strategy for a PoC, pilot or full deployment
- The timeline of CBDC introduction
- A strategy to introduce and monitor the CBDC roll-out, following the appropriate governance policies identified in Section 11
- Policies the central bank will put into place to ensure a controlled roll-out of CBDC that does not have negative impacts on financial stability.

See the **Appendix** to Section 12 for additional information to accompany this section.

Please answer the questions for this section in the **Worksheet** for Section 12.

By the end of Phase 5, the policy-maker should have a clear vision of the target CBDC, along with governance policies and an implementation plan. The policy-maker should also re-evaluate the costs and risks associated with CBDC against the objectives and advantages, confirming whether CBDC remains compelling. If so, the next steps towards development can be taken.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Contributors

Lead author

Ashley Lannquist, Project Lead, Blockchain and Distributed Ledger Technology, World Economic Forum, USA

Content contributors

Jeremy Allaire, Co-Founder and Chief Executive Officer, Circle, USA

Jorge Barrera Vivero, Oversight and Surveillance of Payment Systems, Banco Central del Ecuador, Ecuador

Lisseth Barzallo, Oversight and Surveillance of Payment Systems, Banco Central del Ecuador, Ecuador

Harro Boven, Policy Advisor, De Nederlandsche Bank, Netherlands

Frederick Cheung, Manager, Hong Kong Monetary Authority, Hong Kong

Carlo Cocuzzo, Economist, Digital Finance, ING, UK

Stuart Davis, Partner, Latham & Watkins, UK

Sumedha Deshmukh, Project Specialist, World Economic Forum, USA

Erin English, Director, Thought Leadership and Policy Research, Visa, USA

Eric Groothedde, Senior Compliance Expert, ING, Netherlands

Jonas Gross, Research Assistant, Frankfurt School Blockchain Center, Germany

Simon Hawkins, Counsel, Latham & Watkins, Hong Kong

Justine Humenansky, Research Fellow, World Economic Forum, USA

Jan Lebbe, Initiative Lead for Blockchain and International Payments, ING, Netherlands

Lawrence Lundy-Bryan, Head of Research, Outlier Ventures, UK

Ousmène Mandeng, Senior Advisor, Global Blockchain Technology, Accenture, UK

Andrew Moyle, Partner, Latham & Watkins, UK

Miguel Musa, Technological Observatory, Banco Central de Chile, Chile

Leon Sanz Bunster, Technological Observatory, Banco Central de Chile, Chile

Jonathan Schiller, Research Assistant, Universität Bayreuth, Germany

Cuy Sheffield, Head of Cryptocurrency, Visa, USA

Alpen Sheth, Senior Technologist, Blockchain, Mercy Corps, USA

Kasidit Tansanguan, Deputy Director of Corporate Strategy, Bank of Thailand, Thailand

Content reviewers

Robleh Ali, Research Scientist, MIT Digital Currency Initiative, USA

Central Bank of Chile staff, Monetary Policy Division, Financial Policy Division, Operations Division and Legal Services: Jorge Lorca, Carlos Madeira, Maximiliano Concha, Ignacio Araya and others

Serey Chea, Director General, National Bank of Cambodia, Cambodia

Francis Jee, Fellow, Blockchain and Distributed Ledger Technology, World Economic Forum, USA

Raúl Morales Reséndiz, Fintech Forum Secretariat, Center for Latin American Monetary Studies (CEMLA)

Neha Narula, Director, MIT Digital Currency Initiative, USA

Andrea Pinna, Market Infrastructure and Payments, European Central Bank

Drew Propson, Project Lead, Financial Services, World Economic Forum, USA

Mariana Rojas-Breu, Associate Professor, University of Paris Dauphine PSL, France

Richard Samans, Managing Director, World Economic Forum, USA

Gabriel Söderberg, Associate Professor, Uppsala University and Senior Economist, Sveriges Riksbank, Sweden

Sheila Warren, Platform Head – Blockchain and Distributed Ledger Technology, World Economic Forum, USA

Ben Weisman, Project Lead, Financial Services, World Economic Forum, USA

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

Acknowledgements

Many thanks to those who contributed to the toolkit through their participation in the workshops held alongside the Singapore Fintech Festival, the World Bank and IMF Spring Meetings, Money 20/20 Europe and a meeting of the OECD Committee on Financial Markets and to our dedicated partners in those events. Sincere appreciation is also extended to Mauricio Ulate, Sumedha Deshmukh, Jesse McWaters, Herve Tourpe, John Kiff, Sonja Davidovic, Francisco Rivadeneyra and Zvika Krieger.

Reading Materials

Source: **World Economic Forum. 2020. Central Bank Digital Currency Policy-Maker Toolkit.**

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.

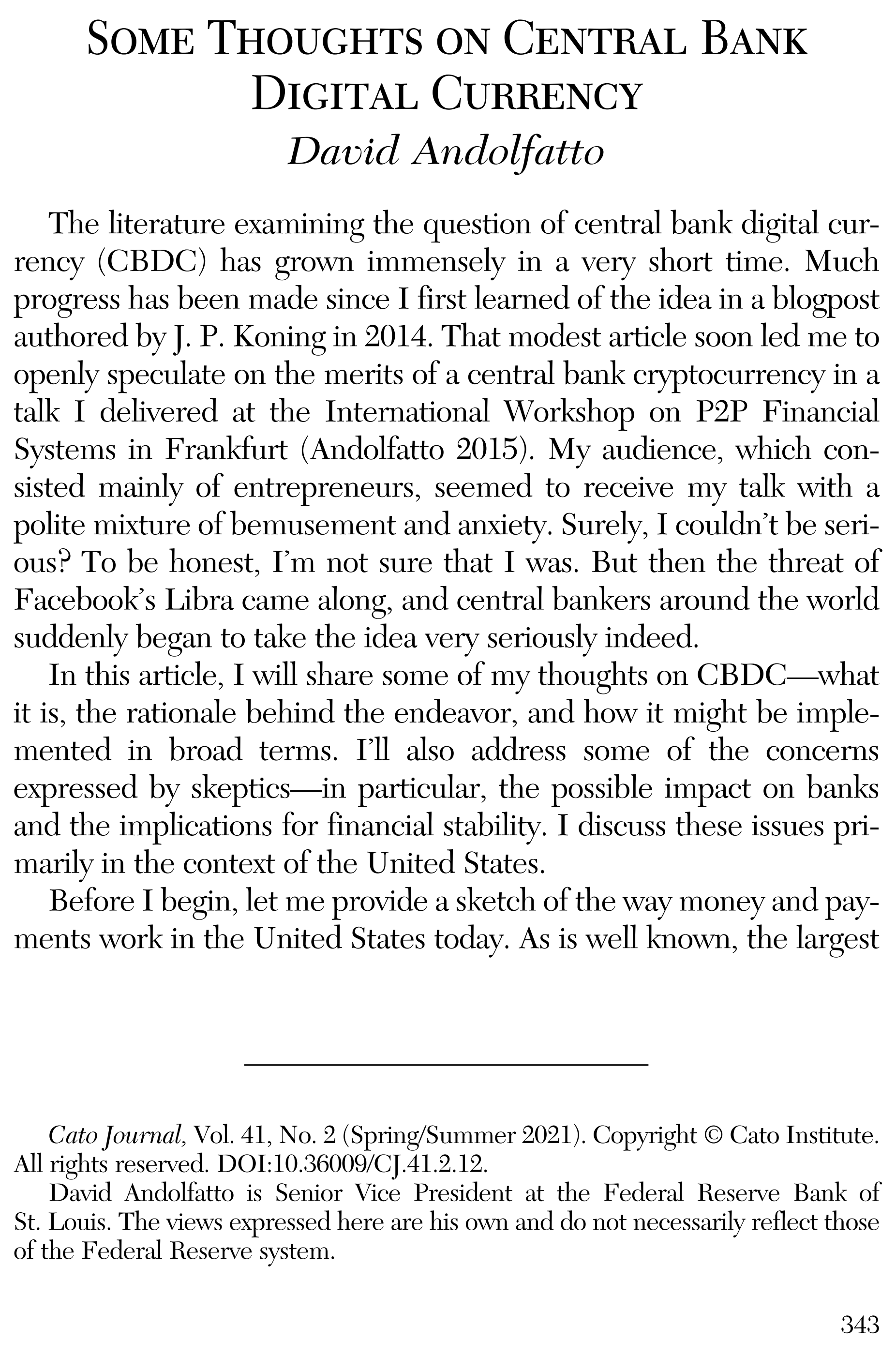
The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

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

Reading Materials

Some Thoughts on Central Bank Digital Currency



Some Thoughts on Central Bank Digital Currency

David Andolfatto

The literature examining the question of central bank digital currency (CBDC) has grown immensely in a very short time. Much progress has been made since I first learned of the idea in a blogpost authored by J. P. Koning in 2014. That modest article soon led me to openly speculate on the merits of a central bank cryptocurrency in a talk I delivered at the International Workshop on P2P Financial Systems in Frankfurt (Andolfatto 2015). My audience, which consisted mainly of entrepreneurs, seemed to receive my talk with a polite mixture of bemusement and anxiety. Surely, I couldn't be serious? To be honest, I'm not sure that I was. But then the threat of Facebook's Libra came along, and central bankers around the world suddenly began to take the idea very seriously indeed.

In this article, I will share some of my thoughts on CBDC—what it is, the rationale behind the endeavor, and how it might be implemented in broad terms. I'll also address some of the concerns expressed by skeptics—in particular, the possible impact on banks and the implications for financial stability. I discuss these issues primarily in the context of the United States.

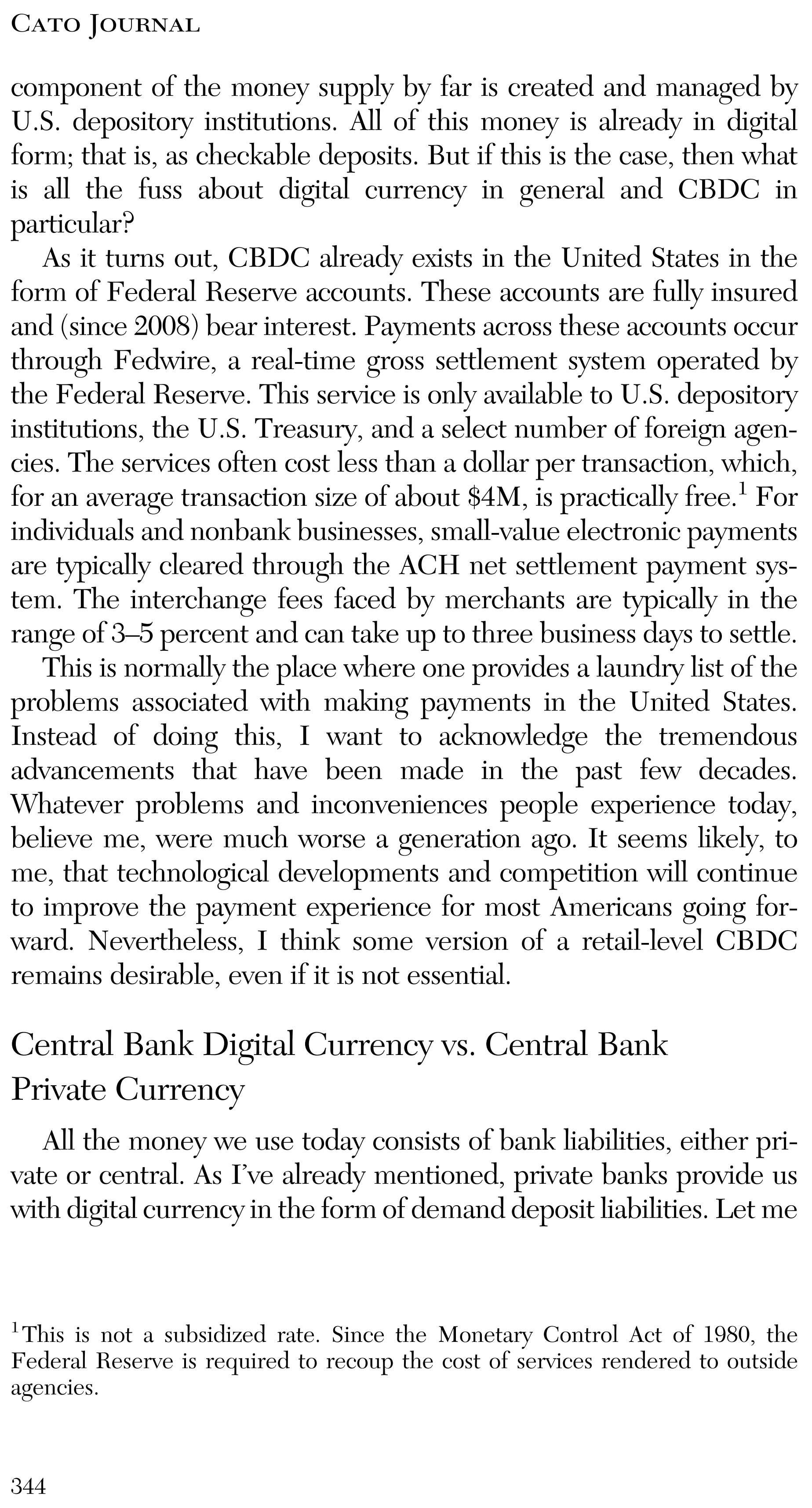
Before I begin, let me provide a sketch of the way money and payments work in the United States today. As is well known, the largest

Cato Journal, Vol. 41, No. 2 (Spring/Summer 2021). Copyright © Cato Institute. All rights reserved. DOI:10.36009/CJ.41.2.12.

David Andolfatto is Senior Vice President at the Federal Reserve Bank of St. Louis. The views expressed here are his own and do not necessarily reflect those of the Federal Reserve system.

Reading Materials

Source: **Andolfatto, D. 2021. "Some Thoughts on Central Bank Digital Currency," Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



component of the money supply by far is created and managed by U.S. depository institutions. All of this money is already in digital form; that is, as checkable deposits. But if this is the case, then what is all the fuss about digital currency in general and CBDC in particular?

As it turns out, CBDC already exists in the United States in the form of Federal Reserve accounts. These accounts are fully insured and (since 2008) bear interest. Payments across these accounts occur through Fedwire, a real-time gross settlement system operated by the Federal Reserve. This service is only available to U.S. depository institutions, the U.S. Treasury, and a select number of foreign agencies. The services often cost less than a dollar per transaction, which, for an average transaction size of about $4M, is practically free.[1] For individuals and nonbank businesses, small-value electronic payments are typically cleared through the ACH net settlement payment system. The interchange fees faced by merchants are typically in the range of 3–5 percent and can take up to three business days to settle.

This is normally the place where one provides a laundry list of the problems associated with making payments in the United States. Instead of doing this, I want to acknowledge the tremendous advancements that have been made in the past few decades. Whatever problems and inconveniences people experience today, believe me, were much worse a generation ago. It seems likely, to me, that technological developments and competition will continue to improve the payment experience for most Americans going forward. Nevertheless, I think some version of a retail-level CBDC remains desirable, even if it is not essential.

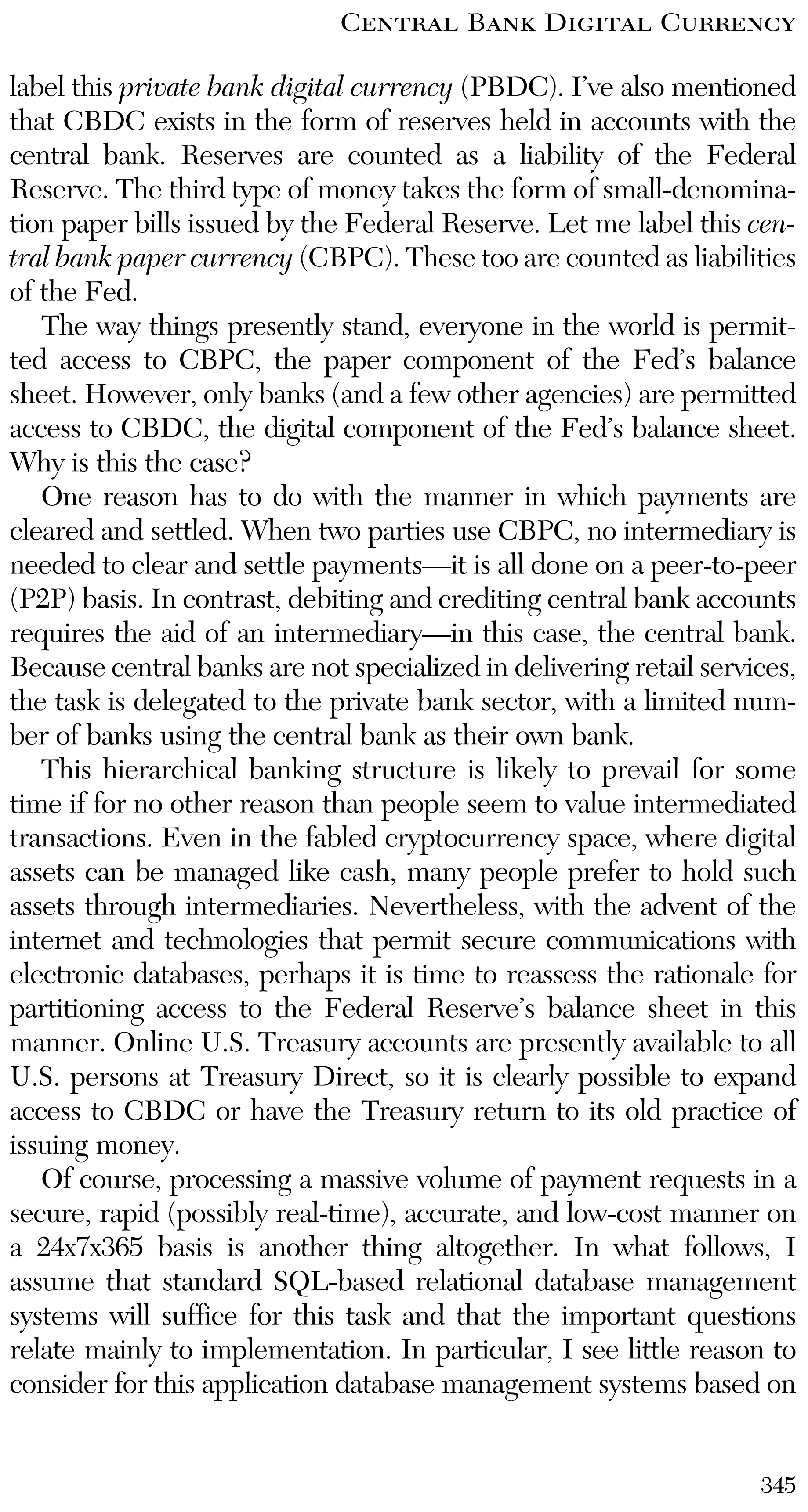
Central Bank Digital Currency vs. Central Bank Private Currency

All the money we use today consists of bank liabilities, either private or central. As I've already mentioned, private banks provide us with digital currency in the form of demand deposit liabilities. Let me

[1] This is not a subsidized rate. Since the Monetary Control Act of 1980, the Federal Reserve is required to recoup the cost of services rendered to outside agencies.

Reading Materials

Source: **Andolfatto, D. 2021. "Some Thoughts on Central Bank Digital Currency," Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



label this *private bank digital currency* (PBDC). I've also mentioned that CBDC exists in the form of reserves held in accounts with the central bank. Reserves are counted as a liability of the Federal Reserve. The third type of money takes the form of small-denomination paper bills issued by the Federal Reserve. Let me label this *central bank paper currency* (CBPC). These too are counted as liabilities of the Fed.

The way things presently stand, everyone in the world is permitted access to CBPC, the paper component of the Fed's balance sheet. However, only banks (and a few other agencies) are permitted access to CBDC, the digital component of the Fed's balance sheet. Why is this the case?

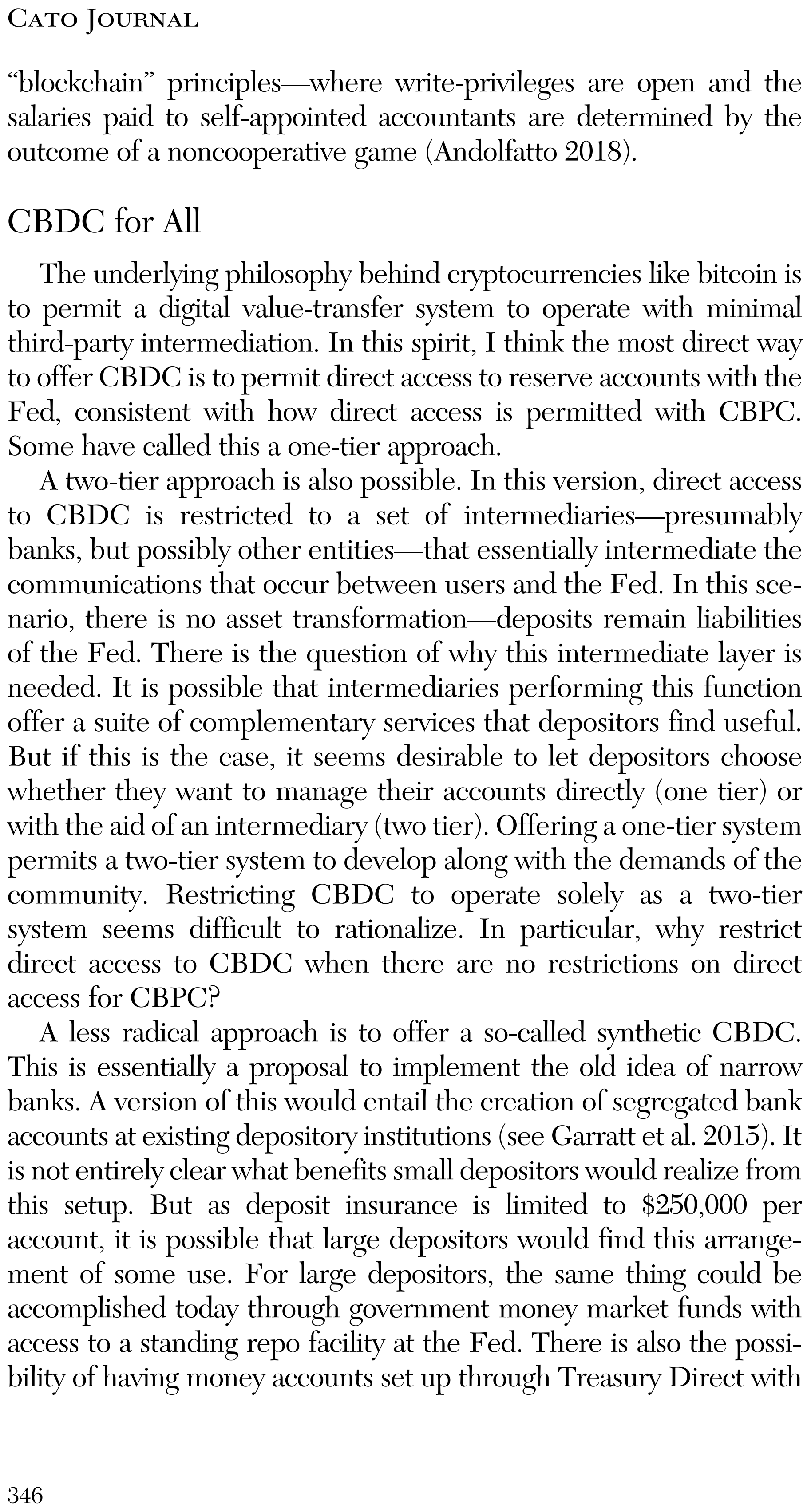
One reason has to do with the manner in which payments are cleared and settled. When two parties use CBPC, no intermediary is needed to clear and settle payments—it is all done on a peer-to-peer (P2P) basis. In contrast, debiting and crediting central bank accounts requires the aid of an intermediary—in this case, the central bank. Because central banks are not specialized in delivering retail services, the task is delegated to the private bank sector, with a limited number of banks using the central bank as their own bank.

This hierarchical banking structure is likely to prevail for some time if for no other reason than people seem to value intermediated transactions. Even in the fabled cryptocurrency space, where digital assets can be managed like cash, many people prefer to hold such assets through intermediaries. Nevertheless, with the advent of the internet and technologies that permit secure communications with electronic databases, perhaps it is time to reassess the rationale for partitioning access to the Federal Reserve's balance sheet in this manner. Online U.S. Treasury accounts are presently available to all U.S. persons at Treasury Direct, so it is clearly possible to expand access to CBDC or have the Treasury return to its old practice of issuing money.

Of course, processing a massive volume of payment requests in a secure, rapid (possibly real-time), accurate, and low-cost manner on a 24x7x365 basis is another thing altogether. In what follows, I assume that standard SQL-based relational database management systems will suffice for this task and that the important questions relate mainly to implementation. In particular, I see little reason to consider for this application database management systems based on

Reading Materials

Source: **Andolfatto, D. 2021. "Some Thoughts on Central Bank Digital Currency," Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



"blockchain" principles—where write-privileges are open and the salaries paid to self-appointed accountants are determined by the outcome of a noncooperative game (Andolfatto 2018).

CBDC for All

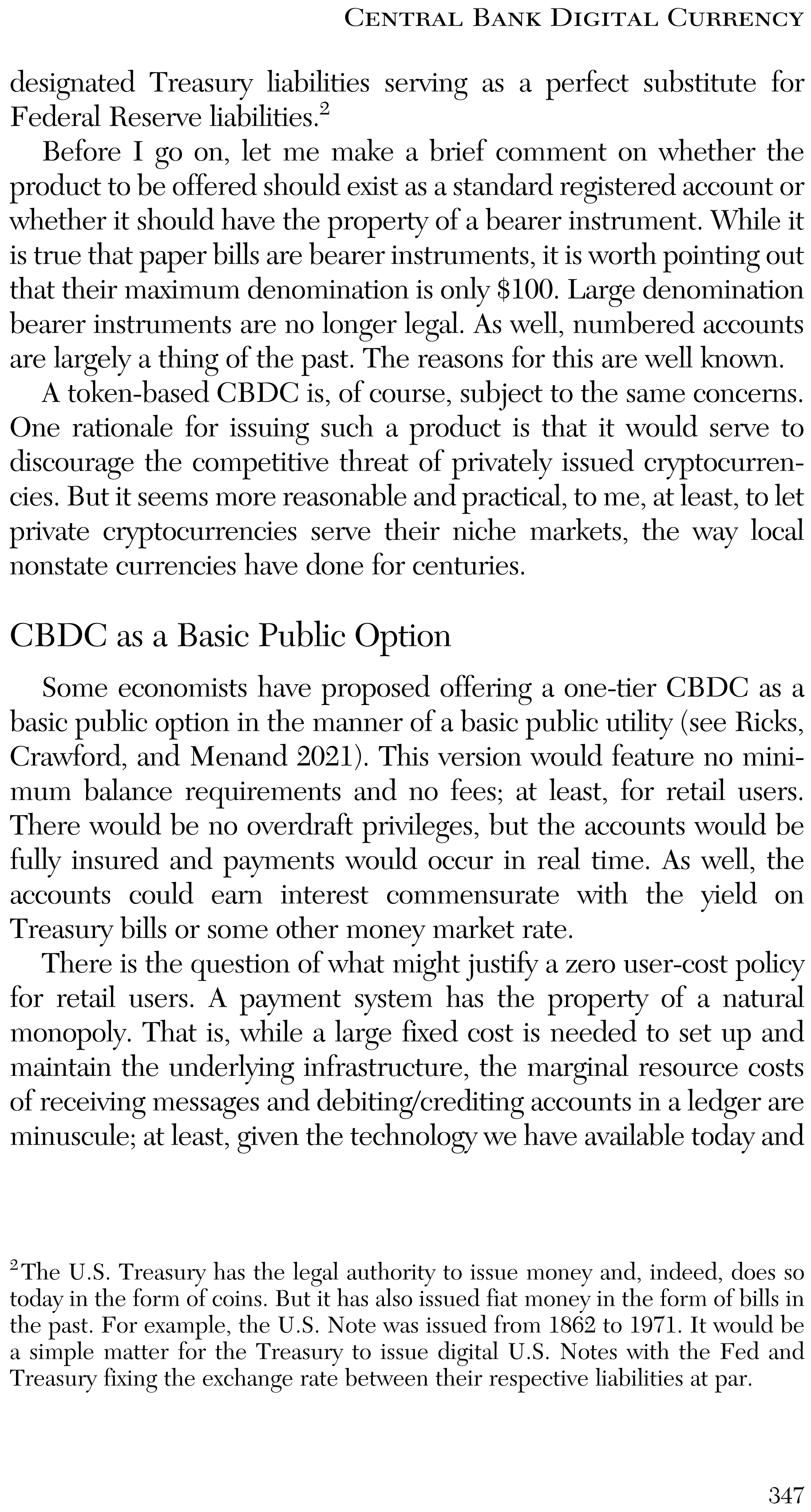
The underlying philosophy behind cryptocurrencies like bitcoin is to permit a digital value-transfer system to operate with minimal third-party intermediation. In this spirit, I think the most direct way to offer CBDC is to permit direct access to reserve accounts with the Fed, consistent with how direct access is permitted with CBPC. Some have called this a one-tier approach.

A two-tier approach is also possible. In this version, direct access to CBDC is restricted to a set of intermediaries—presumably banks, but possibly other entities—that essentially intermediate the communications that occur between users and the Fed. In this scenario, there is no asset transformation—deposits remain liabilities of the Fed. There is the question of why this intermediate layer is needed. It is possible that intermediaries performing this function offer a suite of complementary services that depositors find useful. But if this is the case, it seems desirable to let depositors choose whether they want to manage their accounts directly (one tier) or with the aid of an intermediary (two tier). Offering a one-tier system permits a two-tier system to develop along with the demands of the community. Restricting CBDC to operate solely as a two-tier system seems difficult to rationalize. In particular, why restrict direct access to CBDC when there are no restrictions on direct access for CBPC?

A less radical approach is to offer a so-called synthetic CBDC. This is essentially a proposal to implement the old idea of narrow banks. A version of this would entail the creation of segregated bank accounts at existing depository institutions (see Garratt et al. 2015). It is not entirely clear what benefits small depositors would realize from this setup. But as deposit insurance is limited to $250,000 per account, it is possible that large depositors would find this arrangement of some use. For large depositors, the same thing could be accomplished today through government money market funds with access to a standing repo facility at the Fed. There is also the possibility of having money accounts set up through Treasury Direct with

Reading Materials

Source: **Andolfatto, D. 2021. "Some Thoughts on Central Bank Digital Currency," Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



designated Treasury liabilities serving as a perfect substitute for Federal Reserve liabilities.[2]

Before I go on, let me make a brief comment on whether the product to be offered should exist as a standard registered account or whether it should have the property of a bearer instrument. While it is true that paper bills are bearer instruments, it is worth pointing out that their maximum denomination is only $100. Large denomination bearer instruments are no longer legal. As well, numbered accounts are largely a thing of the past. The reasons for this are well known.

A token-based CBDC is, of course, subject to the same concerns. One rationale for issuing such a product is that it would serve to discourage the competitive threat of privately issued cryptocurrencies. But it seems more reasonable and practical, to me, at least, to let private cryptocurrencies serve their niche markets, the way local nonstate currencies have done for centuries.

CBDC as a Basic Public Option

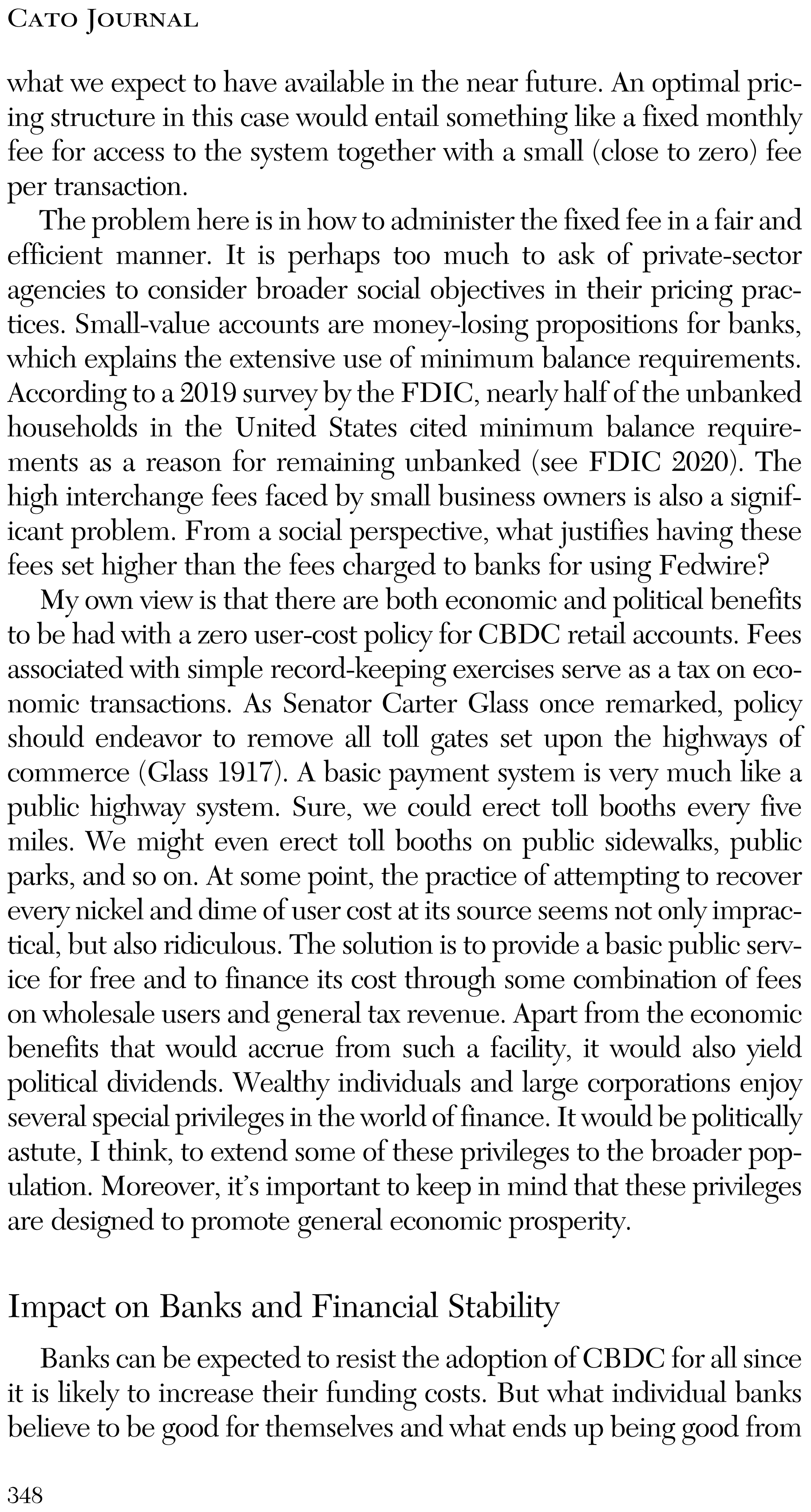
Some economists have proposed offering a one-tier CBDC as a basic public option in the manner of a basic public utility (see Ricks, Crawford, and Menand 2021). This version would feature no minimum balance requirements and no fees; at least, for retail users. There would be no overdraft privileges, but the accounts would be fully insured and payments would occur in real time. As well, the accounts could earn interest commensurate with the yield on Treasury bills or some other money market rate.

There is the question of what might justify a zero user-cost policy for retail users. A payment system has the property of a natural monopoly. That is, while a large fixed cost is needed to set up and maintain the underlying infrastructure, the marginal resource costs of receiving messages and debiting/crediting accounts in a ledger are minuscule; at least, given the technology we have available today and

[2] The U.S. Treasury has the legal authority to issue money and, indeed, does so today in the form of coins. But it has also issued fiat money in the form of bills in the past. For example, the U.S. Note was issued from 1862 to 1971. It would be a simple matter for the Treasury to issue digital U.S. Notes with the Fed and Treasury fixing the exchange rate between their respective liabilities at par.

Reading Materials

Source: **Andolfatto, D. 2021. "Some Thoughts on Central Bank Digital Currency," Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



what we expect to have available in the near future. An optimal pricing structure in this case would entail something like a fixed monthly fee for access to the system together with a small (close to zero) fee per transaction.

The problem here is in how to administer the fixed fee in a fair and efficient manner. It is perhaps too much to ask of private-sector agencies to consider broader social objectives in their pricing practices. Small-value accounts are money-losing propositions for banks, which explains the extensive use of minimum balance requirements. According to a 2019 survey by the FDIC, nearly half of the unbanked households in the United States cited minimum balance requirements as a reason for remaining unbanked (see FDIC 2020). The high interchange fees faced by small business owners is also a significant problem. From a social perspective, what justifies having these fees set higher than the fees charged to banks for using Fedwire?

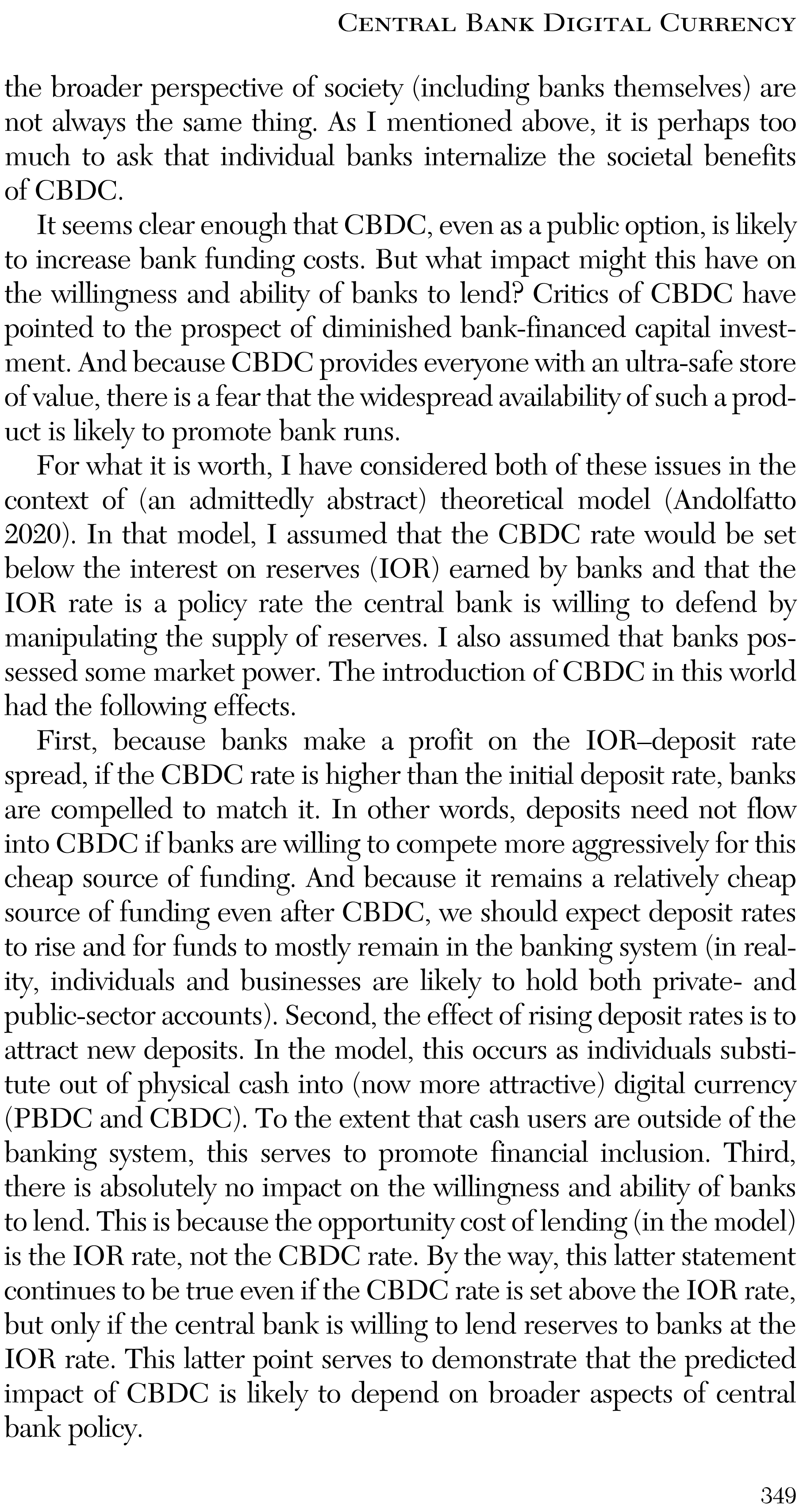
My own view is that there are both economic and political benefits to be had with a zero user-cost policy for CBDC retail accounts. Fees associated with simple record-keeping exercises serve as a tax on economic transactions. As Senator Carter Glass once remarked, policy should endeavor to remove all toll gates set upon the highways of commerce (Glass 1917). A basic payment system is very much like a public highway system. Sure, we could erect toll booths every five miles. We might even erect toll booths on public sidewalks, public parks, and so on. At some point, the practice of attempting to recover every nickel and dime of user cost at its source seems not only impractical, but also ridiculous. The solution is to provide a basic public service for free and to finance its cost through some combination of fees on wholesale users and general tax revenue. Apart from the economic benefits that would accrue from such a facility, it would also yield political dividends. Wealthy individuals and large corporations enjoy several special privileges in the world of finance. It would be politically astute, I think, to extend some of these privileges to the broader population. Moreover, it's important to keep in mind that these privileges are designed to promote general economic prosperity.

Impact on Banks and Financial Stability

Banks can be expected to resist the adoption of CBDC for all since it is likely to increase their funding costs. But what individual banks believe to be good for themselves and what ends up being good from

Reading Materials

Source: **Andolfatto, D. 2021. “Some Thoughts on Central Bank Digital Currency,” Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



the broader perspective of society (including banks themselves) are not always the same thing. As I mentioned above, it is perhaps too much to ask that individual banks internalize the societal benefits of CBDC.

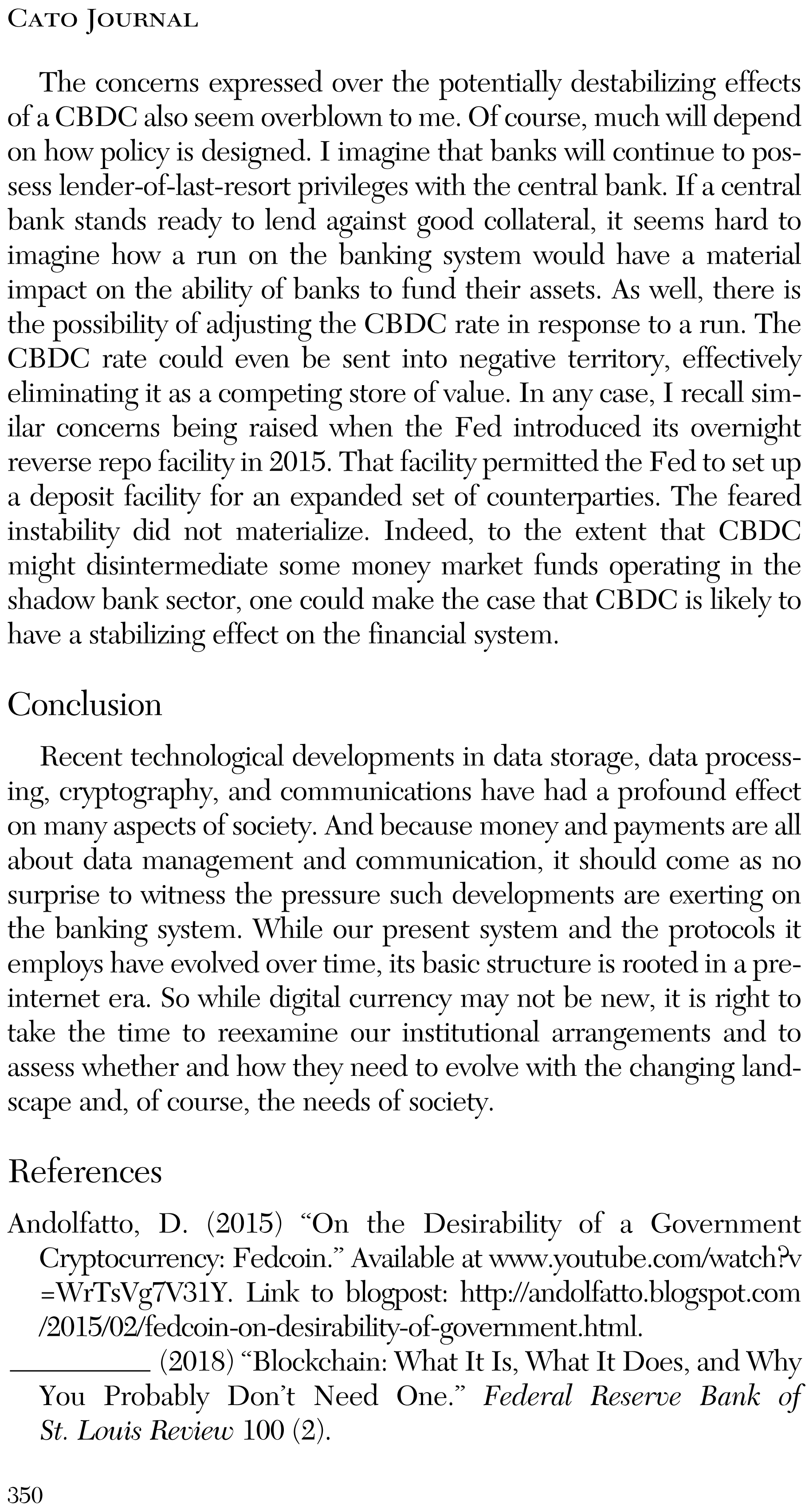
It seems clear enough that CBDC, even as a public option, is likely to increase bank funding costs. But what impact might this have on the willingness and ability of banks to lend? Critics of CBDC have pointed to the prospect of diminished bank-financed capital investment. And because CBDC provides everyone with an ultra-safe store of value, there is a fear that the widespread availability of such a product is likely to promote bank runs.

For what it is worth, I have considered both of these issues in the context of (an admittedly abstract) theoretical model (Andolfatto 2020). In that model, I assumed that the CBDC rate would be set below the interest on reserves (IOR) earned by banks and that the IOR rate is a policy rate the central bank is willing to defend by manipulating the supply of reserves. I also assumed that banks possessed some market power. The introduction of CBDC in this world had the following effects.

First, because banks make a profit on the IOR–deposit rate spread, if the CBDC rate is higher than the initial deposit rate, banks are compelled to match it. In other words, deposits need not flow into CBDC if banks are willing to compete more aggressively for this cheap source of funding. And because it remains a relatively cheap source of funding even after CBDC, we should expect deposit rates to rise and for funds to mostly remain in the banking system (in reality, individuals and businesses are likely to hold both private- and public-sector accounts). Second, the effect of rising deposit rates is to attract new deposits. In the model, this occurs as individuals substitute out of physical cash into (now more attractive) digital currency (PBDC and CBDC). To the extent that cash users are outside of the banking system, this serves to promote financial inclusion. Third, there is absolutely no impact on the willingness and ability of banks to lend. This is because the opportunity cost of lending (in the model) is the IOR rate, not the CBDC rate. By the way, this latter statement continues to be true even if the CBDC rate is set above the IOR rate, but only if the central bank is willing to lend reserves to banks at the IOR rate. This latter point serves to demonstrate that the predicted impact of CBDC is likely to depend on broader aspects of central bank policy.

Reading Materials

Source: **Andolfatto, D. 2021. “Some Thoughts on Central Bank Digital Currency,” Cato Journal, Vol. 41, No. 2. DOI:10.36009/CJ.41.2.12.**



The concerns expressed over the potentially destabilizing effects of a CBDC also seem overblown to me. Of course, much will depend on how policy is designed. I imagine that banks will continue to possess lender-of-last-resort privileges with the central bank. If a central bank stands ready to lend against good collateral, it seems hard to imagine how a run on the banking system would have a material impact on the ability of banks to fund their assets. As well, there is the possibility of adjusting the CBDC rate in response to a run. The CBDC rate could even be sent into negative territory, effectively eliminating it as a competing store of value. In any case, I recall similar concerns being raised when the Fed introduced its overnight reverse repo facility in 2015. That facility permitted the Fed to set up a deposit facility for an expanded set of counterparties. The feared instability did not materialize. Indeed, to the extent that CBDC might disintermediate some money market funds operating in the shadow bank sector, one could make the case that CBDC is likely to have a stabilizing effect on the financial system.

Conclusion

Recent technological developments in data storage, data processing, cryptography, and communications have had a profound effect on many aspects of society. And because money and payments are all about data management and communication, it should come as no surprise to witness the pressure such developments are exerting on the banking system. While our present system and the protocols it employs have evolved over time, its basic structure is rooted in a pre-internet era. So while digital currency may not be new, it is right to take the time to reexamine our institutional arrangements and to assess whether and how they need to evolve with the changing landscape and, of course, the needs of society.

References

Andolfatto, D. (2015) “On the Desirability of a Government Cryptocurrency: Fedcoin.” Available at www.youtube.com/watch?v=WrTsVg7V31Y. Link to blogpost: http://andolfatto.blogspot.com/2015/02/fedcoin-on-desirability-of-government.html.

__________ (2018) “Blockchain: What It Is, What It Does, and Why You Probably Don’t Need One.” *Federal Reserve Bank of St. Louis Review* 100 (2).

__________ (2020) "Assessing the Impact of Central Bank Digital Currency on Private Banks." *The Economic Journal* (forthcoming). See https://doi.org/10.1093/ej/ueaa073.

Federal Deposit Insurance Corporation (2020) "FDIC Survey Shows 95 Percent of U.S. Households Were Banked in 2019." FDIC Press Release (October 19). Available at www.fdic.gov/news/press-releases/2020/pr20113.html.

Garratt, R.; Martin, A.; McAndrews, J.; and Nosal, E. (2015) "Segregated Balance Accounts." Federal Reserve Bank of New York Staff Report No. 730.

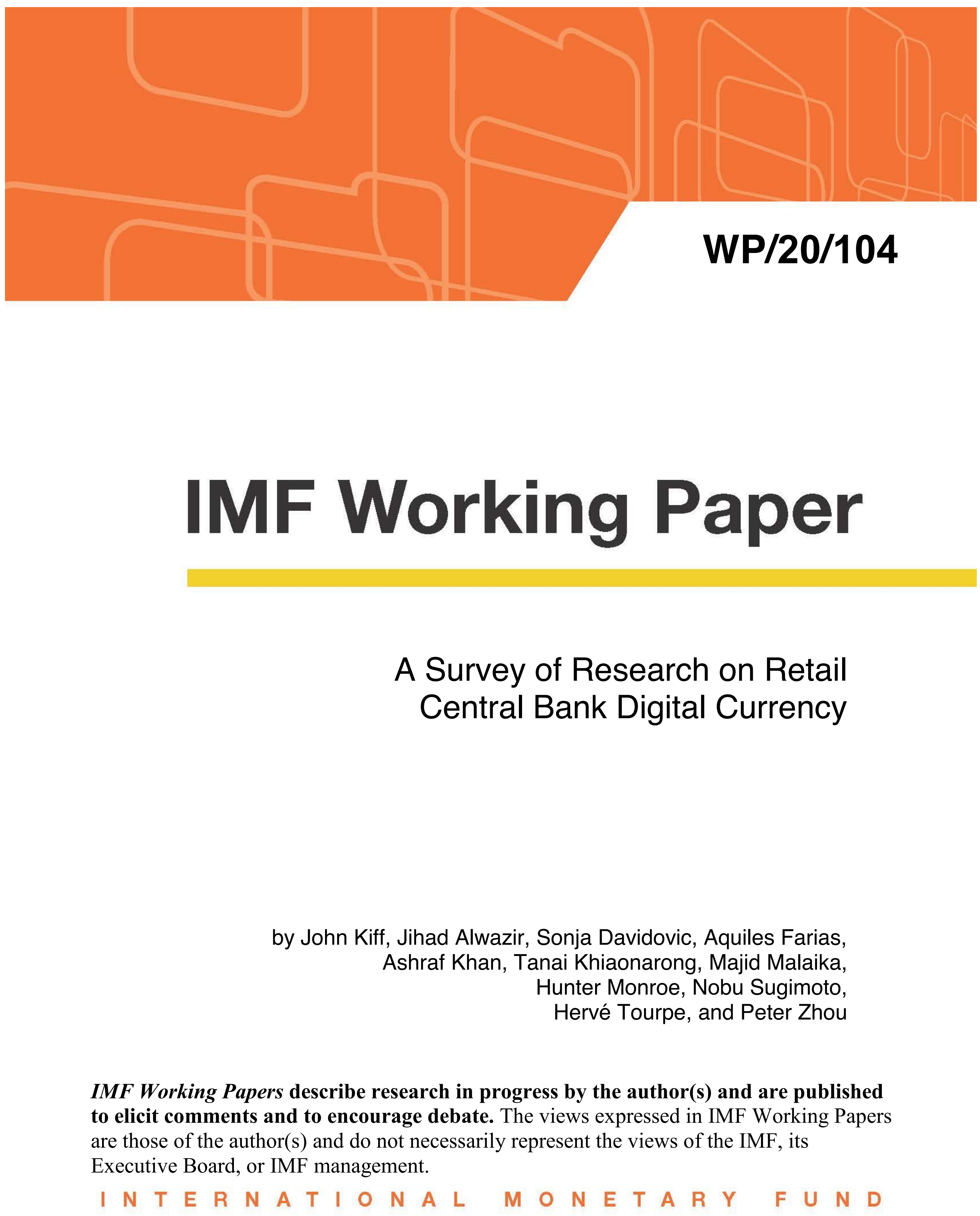
Glass, C. (1917) "Amending the Federal Reserve Act: Speech in the House of Representatives" (June 14). Available at https://fraser.stlouisfed.org/title/statements-speeches-carter-glass-3773/amending-federal-reserve-act-475386.

Koning, J. P. (2014) "Fedcoin." *Moneyness* (October 19). Available at http://jpkoning.blogspot.com/2014/10/fedcoin.html.

Ricks, M.; Crawford, J.; and Menand, L. (2021) "FedAccounts: Digital Dollars." *George Washington Law Review* 89 (1): 113–72.

Reading Materials

A Survey of Research on Retail Central Bank Digital Currency



WP/20/104

IMF Working Paper

A Survey of Research on Retail Central Bank Digital Currency

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

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

INTERNATIONAL MONETARY FUND

Reading Materials

Source: **Kiff, J., J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H.K. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. 2020. "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper No. 20/104.**

WP/20/104

IMF Working Paper

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

A Survey of Research on Retail Central Bank Digital Currency

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

Authorized for distribution by Jihad Alwazir

June 2020

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

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

JEL Classification Numbers: E51, E58, E52

Keywords: money, central bank digital currencies, monetary policy

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

[1] Corresponding author

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

Reading Materials

Source: **Kiff, J., J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H.K. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. 2020. "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper No. 20/104.**

TABLE OF CONTENTS

Tables

Figures

Boxes

Annexes

Reading Materials

Source: **Kiff, J., J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H.K. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. 2020. "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper No. 20/104.**

Executive Summary

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

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

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

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

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

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

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

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

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

Source: **Kiff, J., J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H.K. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. 2020. "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper No. 20/104.**

I. Introduction: Retail CBDC

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

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

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

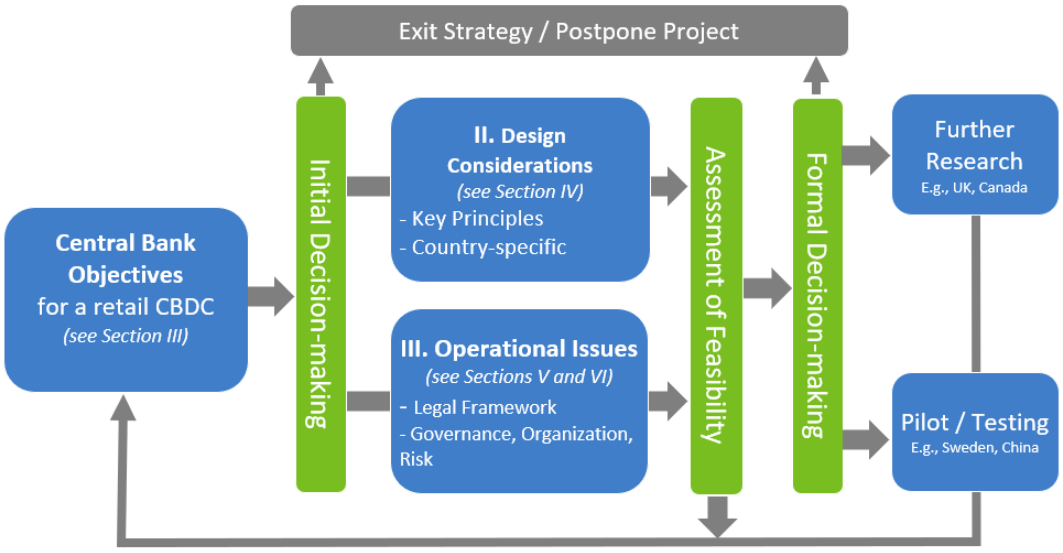
This paper also builds on the recent literature that discusses detailed CBDC design considerations and technological solutions. Auer and Böhme (2020) provide an overview of underlying trade-offs and the related hierarchy of technical design choices, while others explore options and describe potential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

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

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

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

Figure 1. Main Elements of the Paper


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

KEY QUESTIONS

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

Source: Authors.

II. CBDC Definition

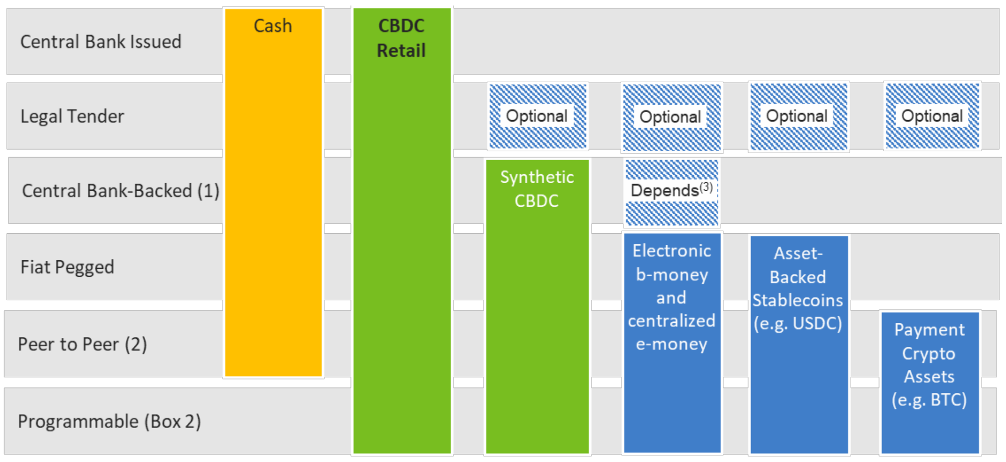
This paper will define CBDC as a digital representation of a sovereign currency issued by and as a liability of a jurisdiction's central bank or other monetary authority. However, the taxonomy of digital representations of money is still evolving, and there are no universally accepted CBDC definitions.[4]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

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

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

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

Figure 2. Retail Money Key Attributes



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

Source: Authors.

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

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

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

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

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

III. Motivations and Policy Considerations for Issuing CBDC

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

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

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

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

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

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

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

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

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

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

Table 1: Costs Associated with Developing and Operating CBDC

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

Source: Authors.

CBDC issuance could improve monetary policy effectiveness. Interest-bearing CBDC could allow for deeply negative policy rates, although only if cash were prohibited as argued in Rogoff (2014), made costly to hold as suggested in Bordo and Levin (2018), or made to depreciate against CBDC, which would become the sole legal tender (Agarwal and Kimball, 2015). However, deeply negative rates could generate criticism from the public and substantially undermine public confidence in the central bank (Mersch, 2020). CBDC could also allow for the implementation of non-linear transfers based on user account balances (Davoodalhosseini and others, 2020) or "helicopter drop" monetary stimulus to alleviate adverse impacts arising from natural disasters or public health crisis or facilitate other "unprecedented policies," bordering on fiscal policy, such as those proposed by Boivin and others (2019). CBDC could also be designed to amplify money velocity by incentivizing specific types of consumer consumption (Copic and Franke, 2020). For example, "cash back" payments could be made on purchases from local merchants and/or certain industries, or CBDC holdings could incur a fee to incentivize people to quickly spend it. The central bank would credit citizens' CBDC accounts or wallets holding CBDC tokens. However, doing so would not necessarily reach all citizens, and the central bank would have to decide how much to transfer to each household, a thorny issue given the distributional consequences. Finally, more innovative monetary policy could discourage innovation in existing payment systems (BoE, 2020), lead to a disproportionate concentration of power in the central bank, and be at odds with the concepts of separating monetary from fiscal policy and central bank independence (Mersch, 2020).

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

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

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

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

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

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

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

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

B. The Risk of Issuing CBDC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. The Preconditions for Issuing CBDC

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

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

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

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

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

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

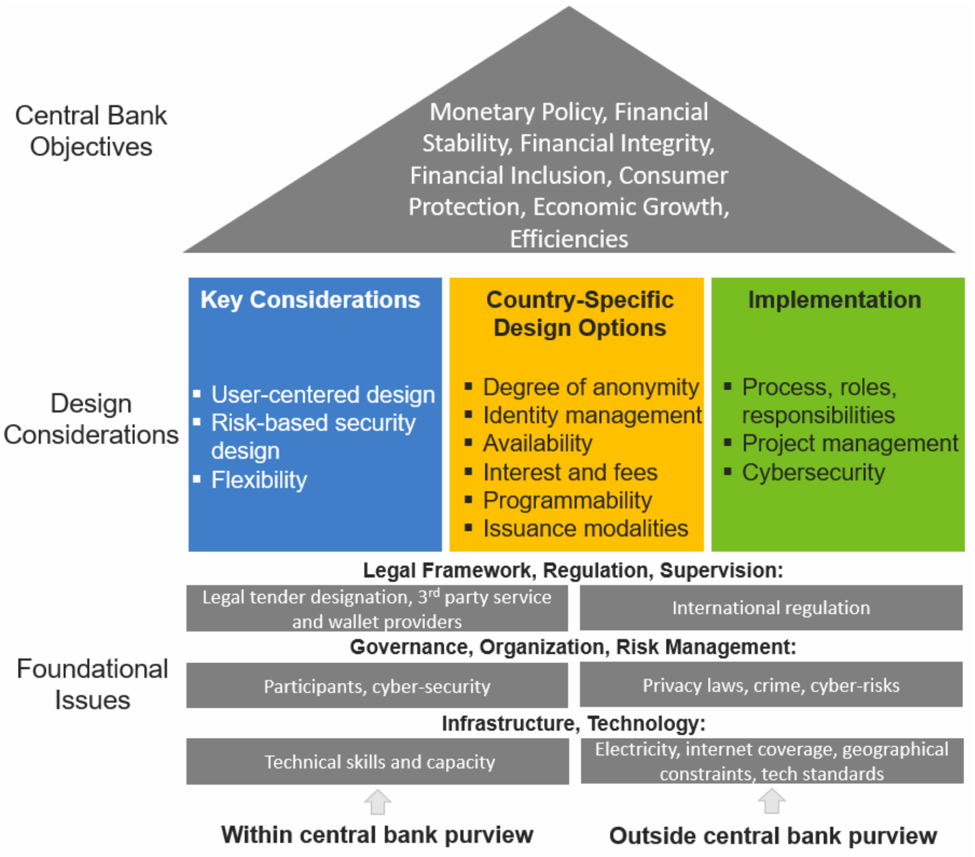
Issuing CBDC requires an adequately developed technological infrastructure. Developing the needed infrastructure to support CBDC includes insuring a high level of availability and resilience of the general infrastructure such as electricity grids, mobile network and internet coverage. Depending on their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

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

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

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

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


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

Source: Authors.

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

Since CBDC involves many aspects of central bank operations, the impact of its issuance on central bank internal operations will need to be considered. The real-time nature of CBDC

Source: **Kiff, J., J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H.K. Monroe, N. Sugimoto, H. Tourpe, and P. Zhou. 2020. "A Survey of Research on Retail Central Bank Digital Currency," IMF Working Paper No. 20/104.**

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

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

D. Weighing the Alternatives, Costs and Benefits of CBDC

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

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

IV. CBDC Design Considerations

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

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

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

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

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

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

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

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

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

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

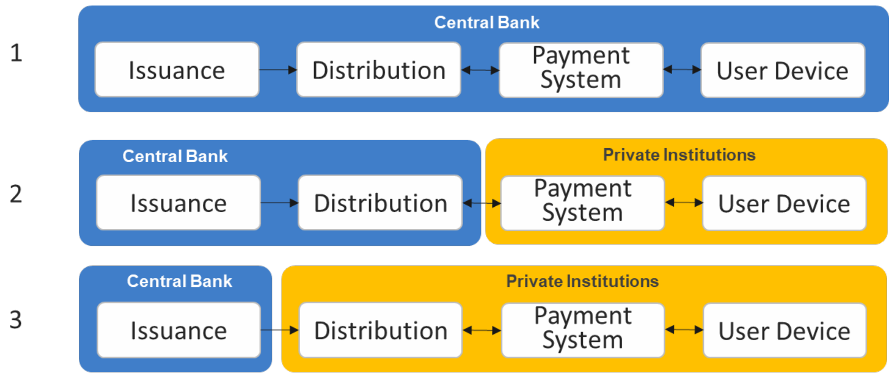
the central bank chooses or needs to adopt. This type of architecture could allow a controlled open architecture enabling third parties, such as payment system providers, to integrate or build their own services on top of the CBDC platform. Such an open architecture could facilitate a competitive market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

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

A. CBDC Operating Model[23]

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

Figure 4. Central Banks can Adopt Different Degrees of Responsibilities



Source: Roberto Giori Company.

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

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

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

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

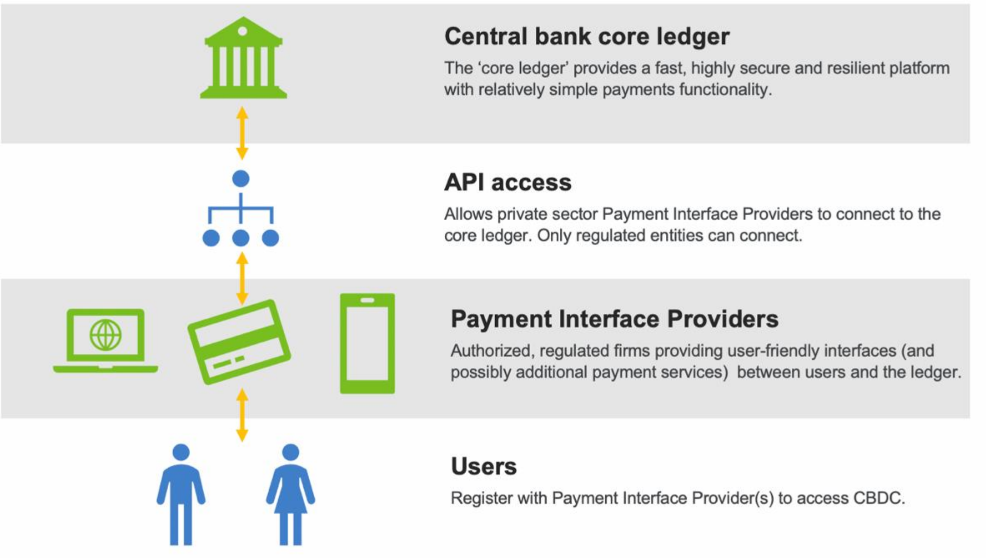
In a multi-tier or "platform" operating model the central bank issues the CBDC but outsources some or all the work of administering the accounts and payment services (Figure 5). However, CBDC remains the liability of the central bank and thus CBDC holders would not be exposed to default risk of the engaged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

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

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

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

Figure 5. CBDC Platform Model


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

Source: BoE, 2020[26]

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

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

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

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

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

B. Centralized Versus Decentralized Authority[27]

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

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

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

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

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

Box 1. Synthetic Central Bank Digital Currency[28]

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

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

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

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

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

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

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

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

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

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

C. Financial Integrity, Privacy and Transparency

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

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

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

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

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

Box 2. DLT-Basked vs Traditional Centralized Ledger Approaches

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

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

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

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

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

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

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

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

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

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

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

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

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

D. Availability and Limitations

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

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

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

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

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

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

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

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

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

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

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

E. Interest and Transaction Fees

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

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

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

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

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

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

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

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

F. Smart Contracts and Programmability

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

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

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

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

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

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

G. Technology Selection and Project Management

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

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

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

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

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

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

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

V. Legal, Governance, and Regulatory Perspectives

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

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

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

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

A. Central Bank Legislation and Legal Tender

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

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

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

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

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

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

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

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

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

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

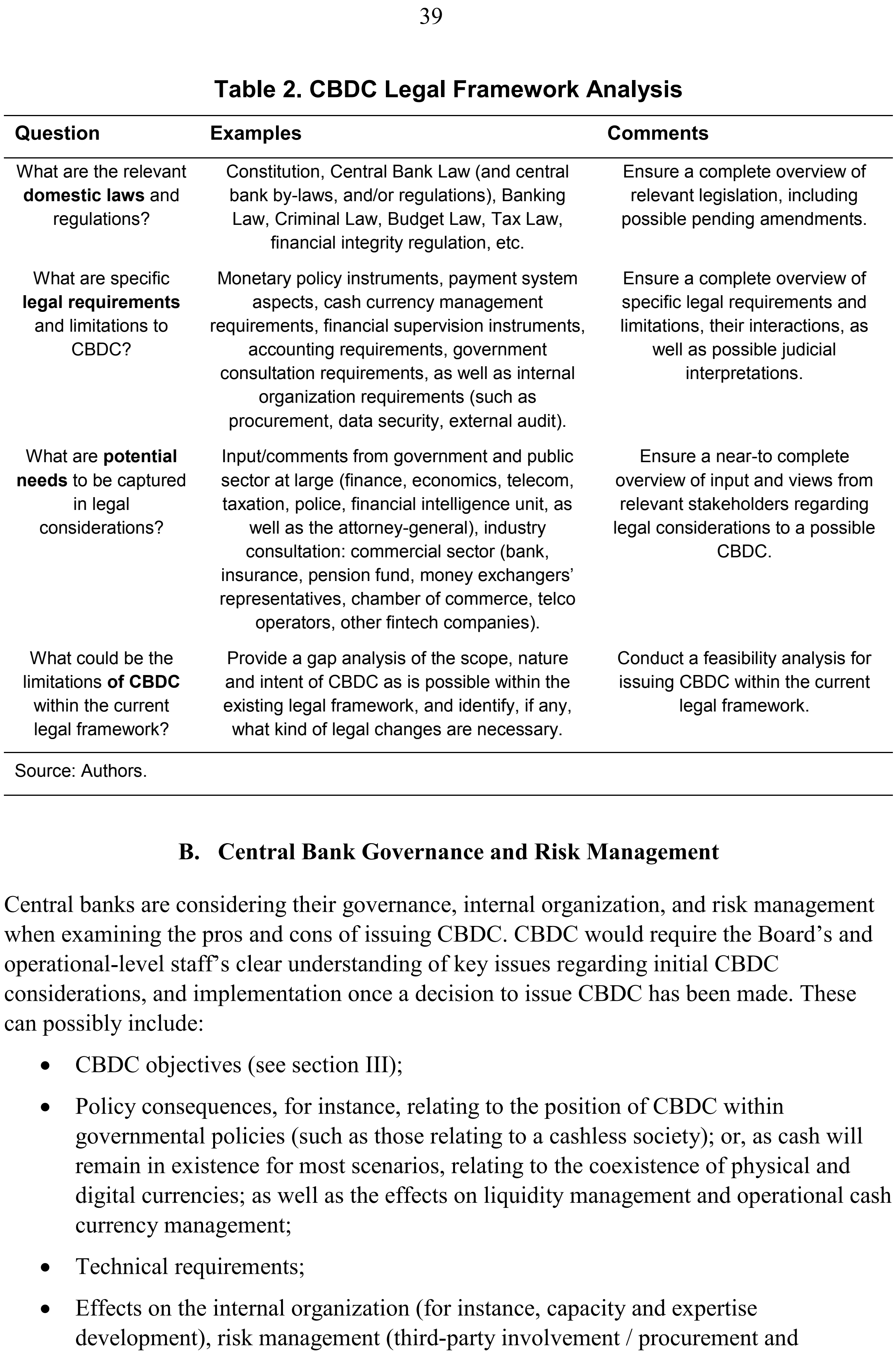


Table 2. CBDC Legal Framework Analysis

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

Source: Authors.

B. Central Bank Governance and Risk Management

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Regulatory Considerations and Pre-Requisites

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

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

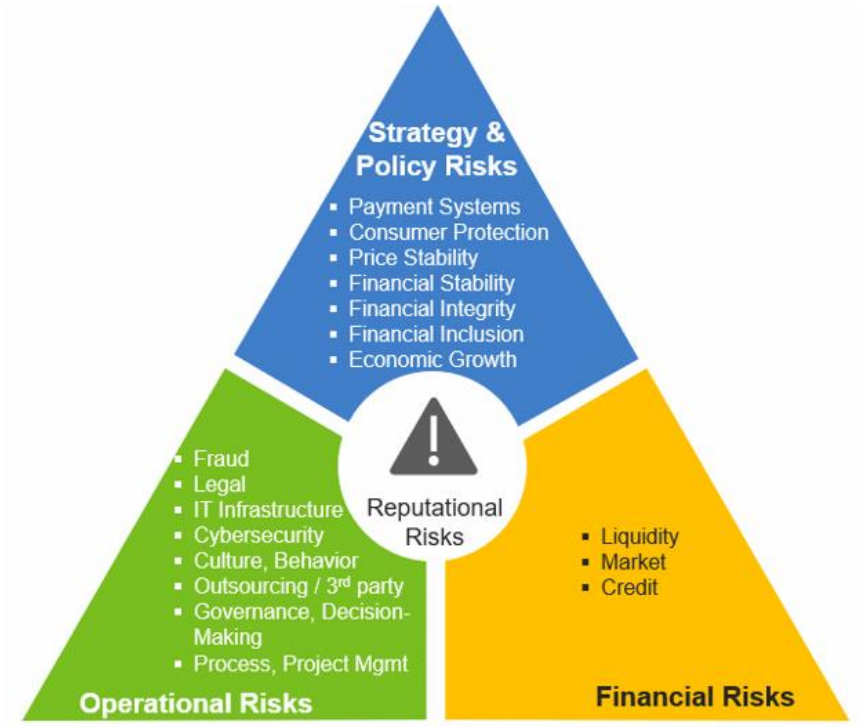
Table 3: CBDB Central Bank Internal Organization Analysis

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

Source: Authors.

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

Figure 6. CBDC Risk Landscape



Source: Alwazir and Khan (2020).

Supervisory Considerations

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

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

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

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

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

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

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

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

VI. Cybersecurity Considerations

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

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

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

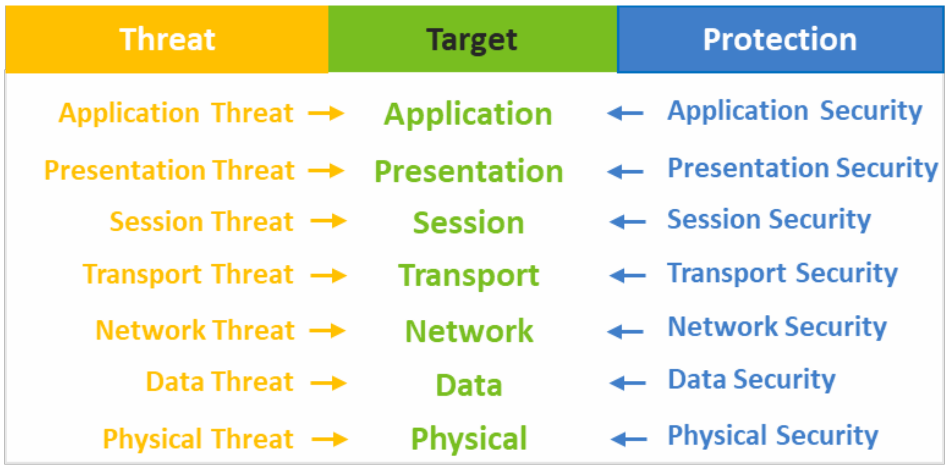
- Business and process layer. This layer relies on the early decisions and the central bank's security work practices to manage people, processes and technologies. The security of this layer is only as good as the central bank's operational resilience and security posture mentioned above. The goal is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

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

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

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

Figure 7: OSI Threat, Target, Protection Model



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

Source: ITU, 2019.

VII. Conclusion and Summary

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

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

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

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

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

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

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

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

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

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

Table 4. Summary of Retail CBDC Implementation Considerations

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

Source: Authors.

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Interaction Design Foundation. "User Centered Design."

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VISA. 2018. "VISA Fact Sheet."

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

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

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

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

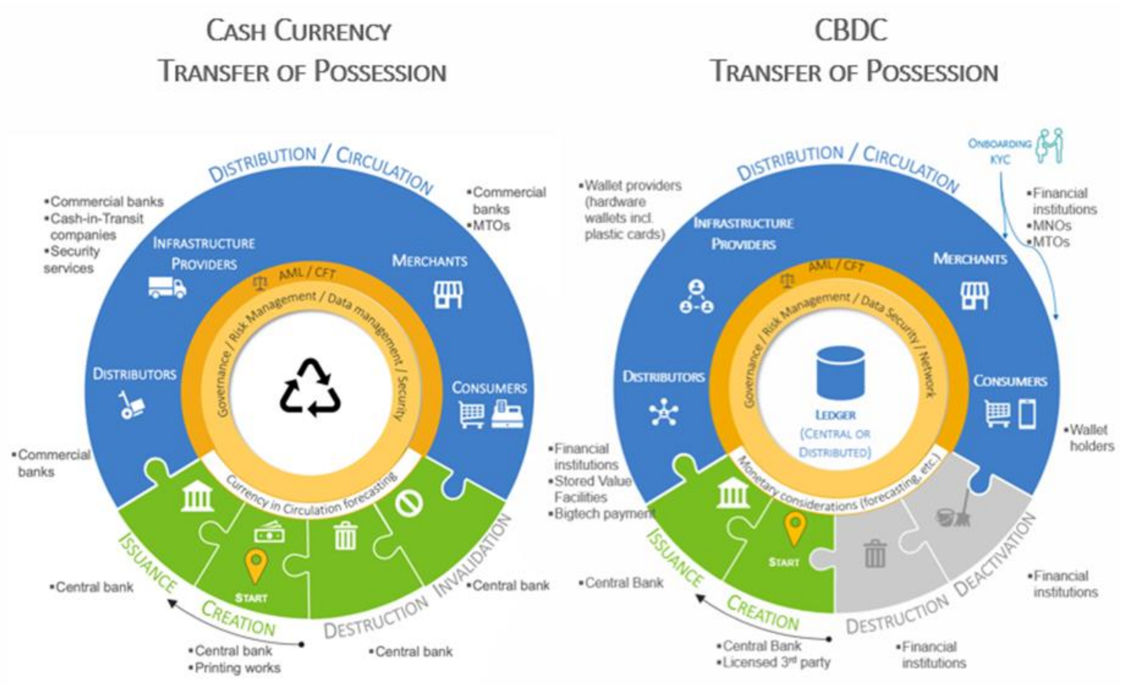
Annex 1. Countries Where Retail CBDC is Being Explored[54]

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

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

Annex 2. Process, Roles, and Responsibilities

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



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

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

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

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

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

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

ANNEX 3. ADDITIONAL CYBERSECURITY CONSIDERATIONS

The business and process layer

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

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

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

The infrastructure and application layer

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

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

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

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

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

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

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

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

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

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

Annex 4. Blockchain Primer

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

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

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

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

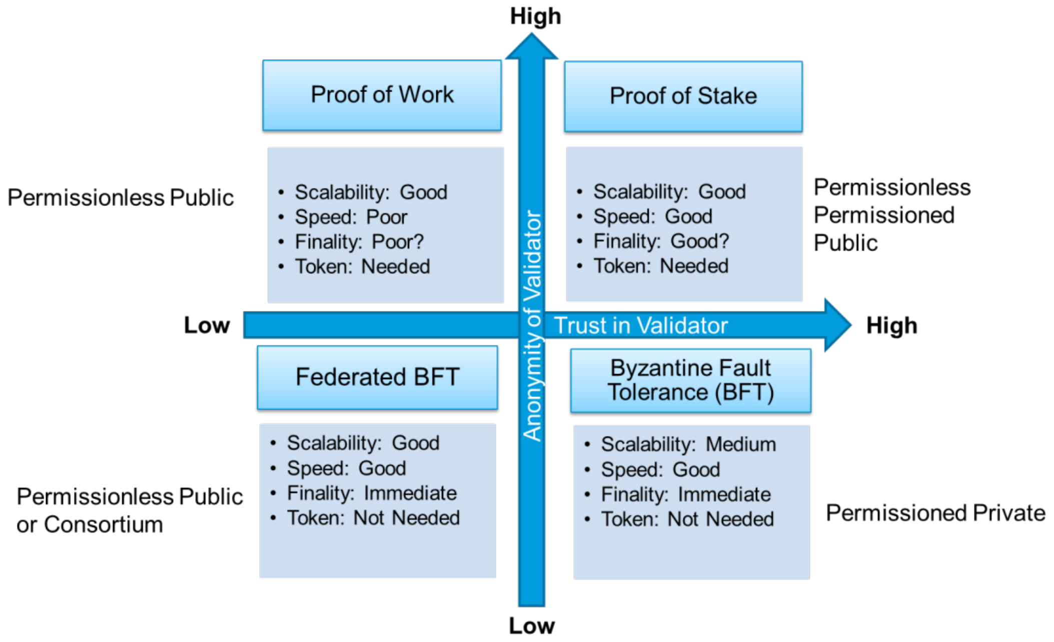
- Permissionless platforms offer opportunities for full disintermediation but creating trust among network participants through cryptographic verification and synchronization can require high computational power. The increased computational power translates into higher energy consumption and lower throughput,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

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

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

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

Public, Private and Permissioned Blockchains



Source: Kalisko 2018.

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

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

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

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

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

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

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

Central Bank Payment System Experiments with Wholesale CBDC

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

Sources:

Bank of Canada. 2017. "Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement."

----. 2017. "Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement."

----. 2018. "Jasper Phase III: Securities Settlement Using Distributed Ledger Technology."

Bank of Canada and Monetary Authority of Singapore. 2019. "Jasper-Ubin Design Paper : Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies."

Banque de France. 2020. "Central Bank Digital Currency Experiments with the Banque de France: Call for Applications."

ECB-BoJ. 2017. "Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment."

---. 2018. "Securities Settlement Systems: Delivery-versus-Payment in a Distributed Ledger Environment."

---. 2019. "Synchronized Cross-Border Payment."

HKMA-BoT. 2020. "Project Inthanon-LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments."

Saudi Arabian Monetary Authority. 2019. "A Statement on Launching "Aber" Project, the Common Digital Currency between Saudi Arabian Monetary Authority (SAMA) and United Arab Emirates Central Bank (UAECB)."

Monetary Authority of Singapore. 2017. Project Ubin: SGD on Distributed Ledger.

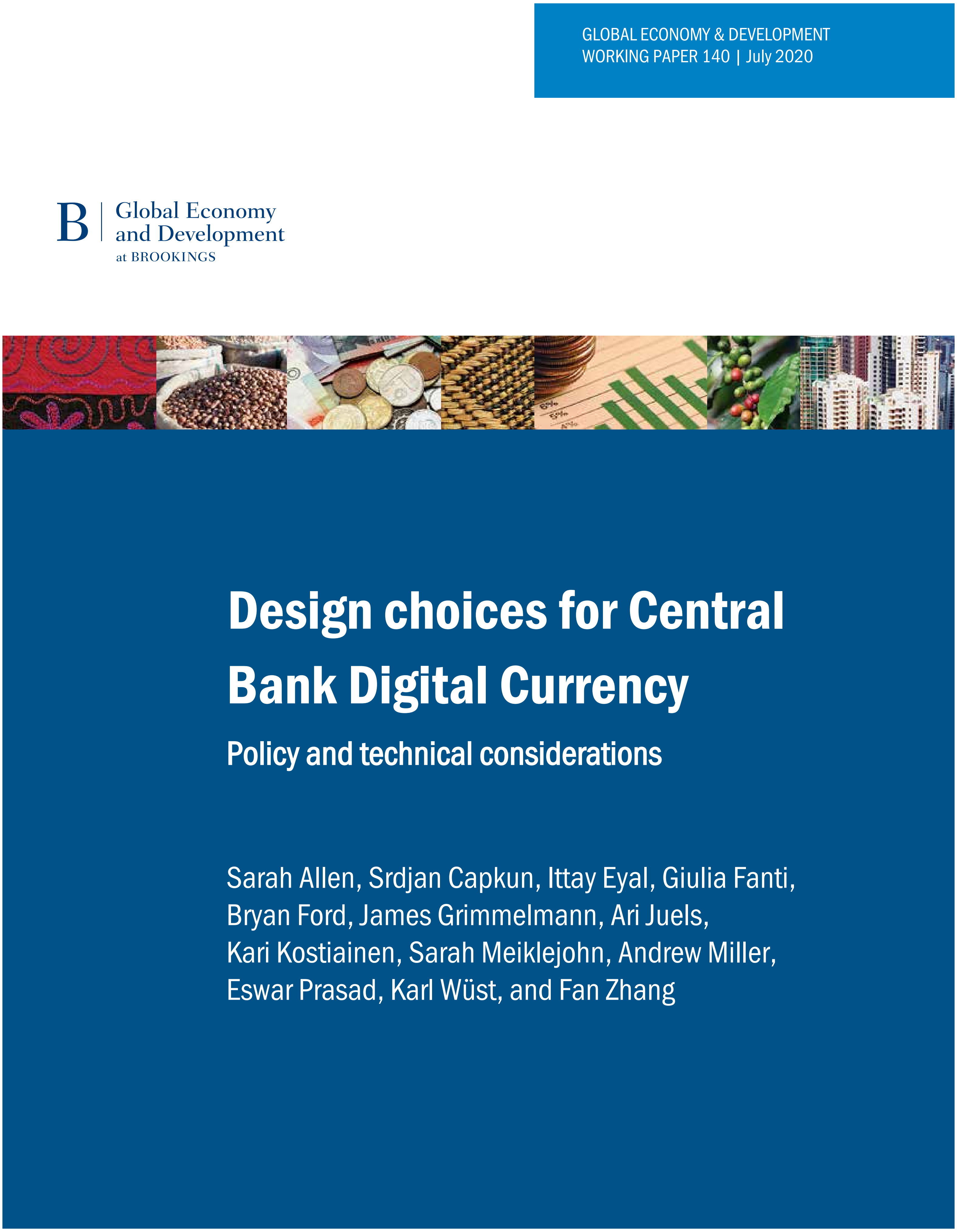
South African Reserve Bank. 2018. "Project Khokha: Exploring the Use of Distributed Ledger Technology for Interbank Payments Settlement in South Africa."

Bank of Thailand. 2019. "Project Inthanon: An application of Distributed Ledger Technology for a Decentralised Real Time Gross Settlement system using Wholesale Central Bank Digital Currency."

Bank of Thailand. 2019. "Project Inthanon: Enhancing Bond Lifecycle Functionalities & Programmable Compliance Using Distributed Ledger Technology."

Reading Materials

Design Choices for Central Bank Digital Currency: Policy and Technical Considerations



GLOBAL ECONOMY & DEVELOPMENT
WORKING PAPER 140 | July 2020

B | Global Economy and Development at BROOKINGS

Design choices for Central Bank Digital Currency

Policy and technical considerations

Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, and Fan Zhang

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

Design Choices for Central Bank Digital Currency: Policy and Technical Considerations

Sarah Allen[1], Srdjan Capkun[2,1], Ittay Eyal[3,1], Giulia Fanti[4,1], Bryan Ford[5,1], James Grimmelmann[6,1], Ari Juels[10,1], Kari Kostiainen[2,1], Sarah Meiklejohn[7,1], Andrew Miller[8,1], Eswar Prasad[9], Karl Wüst[2,1], and Fan Zhang[10,1]

[1]Initiative for CryptoCurrencies and Contracts (IC3)
[2]Swiss Federal Institute of Technology in Zürich (ETH Zürich)
[3]Israel Institute of Technology (Technion)
[4]Carnegie Mellon University (CMU)
[5]Swiss Federal Institute of Technology in Lausanne (EPFL)
[6]Cornell Tech and Cornell Law School
[7]University College London (UCL)
[8]University of Illinois at Urbana-Champaign (UIUC)
[9]Cornell University and Brookings Institution
[10]Cornell Tech

July 23, 2020
v1.0

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

Abstract

Central banks around the world are exploring and in some cases even piloting Central Bank Digital Currencies (CBDCs). CBDCs promise to realize a broad range of new capabilities, including direct government disbursements to citizens, frictionless consumer payment and money-transfer systems, and a range of new financial instruments and monetary policy levers.

CBDCs also give rise, however, to a host of challenging technical goals and design questions that are qualitatively and quantitatively different from those in existing government and consumer payment systems. A well-functioning CBDC will require an extremely resilient, secure, and performant new infrastructure, with the ability to onboard, authenticate, and support users on a massive scale. It will necessitate an architecture simple enough to support modular design and rigorous security analysis, but flexible enough to accommodate current and future functional requirements and use cases. A CBDC will also in some way need to address an innate tension between privacy and transparency, protecting user data from abuse while selectively permitting data mining for end-user services, policymakers, and law enforcement investigations and interventions.

In this paper, we enumerate the fundamental technical design challenges facing CBDC designers, with a particular focus on performance, privacy, and security. Through a survey of relevant academic and industry research and deployed systems, we discuss the state of the art in technologies that can address the challenges involved in successful CBDC deployment. We also present a vision of the rich range of functionalities and use cases that a well-designed CBDC platform could ultimately offer users.

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

Contents

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

1 Introduction

Central Bank Digital Currency (CBDC)—fiat currency issued by central banks in digital form—has progressed in the past few years from a bold speculative concept to a seeming inevitability.

More than 80% of central bank respondents to a Bank for International Settlements survey in 2019 reported engagement in CBDC projects [1]. One in ten of these banks, representing approximately one-fifth of the world's population, deemed it likely that they would offer CBDCs within the next three years. The People's Bank of China, whose plans are well in advance of that of other major economic powers, has begun to pilot a digital yuan [2]. Hearings on CBDC have taken place this year in the U.S. House Committee on Financial Services [3]. The European Central Bank has initiated a project to explore CBDC development [4] while Sweden (an E.U. but not Eurozone member), has begun testing a CBDC known as the e-krona [5].

At the same time, a Facebook-initiated fiat-backed cryptocurrency called Libra has raised the prospect of an industry alternative. Regulator concerns about the project [6] and (perhaps incorrect) speculation that it has catalyzed CBDC development [7] highlight Libra's overlap in goals with CBDC.

Various forms of CBDC have in a sense existed for years, but as wholesale facilities available exclusively to financial institutions [8]. What is striking and potentially transformative about many recent CBDC initiatives is their retail focus, that is, their aim of democratizing central bank account holdings to individual consumers or, at a minimum, making digital central bank liabilities available to households and businesses. Our focus in this paper is on retail CBDCs.

While the goals of cryptocurrencies such as Bitcoin differ dramatically from that of CBDC, they offer evidence of feasibility and technical idea for retail deployment of digital currency. Their technical foundations underpin Libra, have to some extent influenced CBDC design plans, and strongly inform the findings and recommendations of this paper.

Paper scope: This position paper investigates and explains the design choices, mainly technical, but also financial and legal, that central banks will unavoidably encounter in their exploration of CBDCs. Contributing authors include experts in computer science, economics, and law whose research and practical experience has a strong bearing on the design of digital currencies. We highlight not just choices, but challenges that we believe will constitute the main impediments to CBDC deployment or define the main limiting factors in CBDC realization.

This work is geared toward readers who may be only lightly conversant with the technical concepts behind digital currencies. It does not assume specialized technical knowledge. It can also serve as a reference work, as individual sections are largely self-contained.

At a minimum, we suggest reading section 2 for background on CBDC from a banking perspective and basic terminology and section 12 for a summary position of the authors of this work. In this introductory section, we briefly review the main benefits and risks of CBDC (section 1.1) and present a roadmap of the paper (section 1.2).

1.1 Benefits and risks

Among the main potential benefits spurring central bank exploration are:

- *Efficiency:* CBDC can reduce friction in existing payment systems, potentially lowering the monetary cost and increasing the speed of transactions while ensuring finality. The prospect of instantaneous payments has proven attractive in the U.S., for instance, in view of the challenges of disbursing financial aid during the current pandemic [9].
- *Broader tax base:* CBDC can potentially bring more economic activity into the tax net, limiting tax evasion and boosting tax revenues. Moreover, the traceability of digital transactions would inhibit the use of CBDC for illicit purposes such as money laundering and terrorism financing.
- *Flexible monetary policy:* The zero lower-bound constraint on monetary policy (interest rates set by central banks) could in principle be relaxed, with a central bank instituting a negative nominal interest rate by reducing CBDC account balances at a pre-announced rate. Similarly, CBDC would ease the implementation of non-distortionary helicopter drops or withdrawals of central bank money (without relying on fiscal transfers).
- *Payment backstop:* CBDC could act as a backstop to private sector managed payment systems, avoiding breakdown of payments systems in times of crisis of confidence and rise in counterparty risk.
- *Financial inclusion:* CBDC could serve as a gateway for unbanked and underbanked individuals to have access to electronic payment systems and, potentially, to other financial products and services as well.

We highlight an additional benefit in this paper, namely opportunities for novel financial technologies, particularly for regulators.

The many potential benefits of CBDC should be weighed against a number of potential risks, both financial and technical. They include:

- *Disintermediation of the banking system:* Many CBDC plans seem to be gravitating toward a two-layer architecture (see, e.g., [10]), in which the CBDC itself serves as a basic functional layer, while existing non-governmental financial institutions interface manage a second layer that interfaces with users. Nonetheless, by reducing transaction frictions and possibly even providing interest-bearing accounts [8], CBDCs could disintermediate significant swaths of the banking system.

- *Miscalibration of government involvement:* One acknowledged benefit of a two-layer architecture is the opportunity for financial institutions to innovate on top of a CBDC [10]. A CBDC design that arrogates to a central bank activities such as payments that can be cheaply and efficiently be managed by the private sector could limit innovation. At the same time, systemic risks and incompatibilities could arise without adequate central bank involvement.

- *Financial risks due to lack of regulatory expertise and capacity:* With increased speed and efficiency—and especially financial innovation—come new risks, financial and technical, many enumerated above. Regulators may struggle to develop the tools and expertise to address these risks in the face of a dramatic change in the basic operation of the financial system.

- *Loss of privacy:* Given the complexity and performance limitations of current privacy-enhancing technologies, it seems likely that a true retail CBDC will expose new forms of sensitive information to its operators. CBDC designers should consider legal and technical mitigations from the outset.

- *Technological vulnerabilities or entrenched design mistakes:* Even with conservative design, CBDCs will represent a technical experiment, whose risks of information security failures and fundamental design mistakes should not be underestimated.

Our focus in this paper on the technical choices and risks involved in CBDC deployment, as well as key financial and legal considerations, emphasizes exploration of the last two of these risks.

1.2 Paper roadmap

The foundation of a digital currency is a digital record of all of the transactions that have taken place in the system. Such a record is often referred to as a *digital ledger*, and may be viewed abstractly as a digital bulletin board to which all transactions in the currency system are posted. The set of transactions in the ledger cumulatively determine the *account balances* in the system. The set of all account balances at a given time may be regarded as a snapshot of what is sometimes called the *state* of the ledger.

To ensure against ambiguity in account balances at a given time, the ledger must also include a *sequencing* of transactions—generally based on their time of receipt—that determines their order of execution. In the view of a ledger as a bulletin board, new transactions may be thought of as appended to an ever-growing, ordered transaction list.[1] See fig. 1 for a conceptual diagram.[2]

[1] A ledger may be thought of as a database with an append-only structure, i.e., in which no transactions are deleted. Most databases, however, allow records to be deletes, and are thus not digital ledgers in sense that the term is currently used. Such databases, despite their weaker data-integrity assurances, could be used to realize a CBDC. Many of the findings in this paper would still

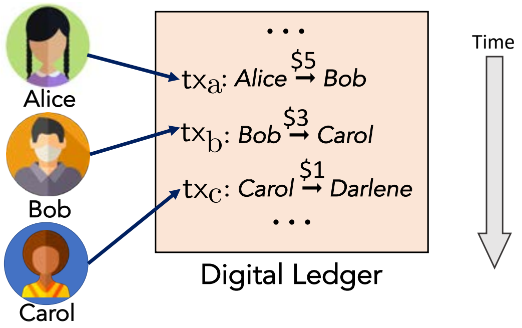

Alice
Bob
Carol
. . .
tx_a: Alice $\xrightarrow{\$5}$ Bob
tx_b: Bob $\xrightarrow{\$3}$ Carol
tx_c: Carol $\xrightarrow{\$1}$ Darlene
. . .
Digital Ledger
Time

Figure 1: Conceptual diagram of a digital ledger with a sequence of three of its posted transactions. (Clipart attribution: flaticon.com.)

In section 3 ("Ledger Infrastructure"), we describe the various types of digital ledgers in common use today and their underlying technologies, classifying them broadly according to their degree of *centralization* or *decentralization*, i.e., the diversity of the set of entities in which system control is vested. We discuss the security and privacy features offered by different types of digital ledgers.

A retail CBDC assigns account balances to individual users, necessitating a regime for *account management*, with a supporting notion of *identity*, concepts treated in section 4 ("Account and Identity Management"). Critical design elements include the choice of entities to verify users' real-world identities and translate them into digital form and the mechanisms by which the system *authenticates* enrolled users, i.e., permits use of an account only by its assigned users. To access the CBDC system, users need specialized applications, typically referred to as *digital wallets*, and discussed in section 5 ("Digital Wallets"). Wallets serve as the endpoints for user authentication, and provide *user interfaces* that guide users in their interaction with the CBDC and allow them to initiate transactions, view account balances, etc. Wallets may also perform *transaction authentication* facilitating the CBDC's verification of the validity of submitted transactions.

The term "bulletin board" suggests a publicly visible medium. Indeed transactions in cryptocurrencies such as Bitcoin are readable by any user, resulting in strong *transparency*. Central banks, however, may have more stringent requirements for the *privacy* of users transactions, and are unlikely to embrace a fully public model. Digital ledgers can be designed to reveal information selectively and/or only to authorized entities.

The tension between transparency and privacy is the focus of section 6 ("Privacy and Transparency"), which discusses how privacy relates to *identities* and *transactions*. That section explains limitations in the widely embraced privacy model of

be relevant in this case.

[2] The diagram in fig. 1 also illustrates the significance of transaction ordering and why unambiguous ordering is important. Suppose that balances prior to tx_a are: Alice: \$5; Bob: \$0; Carol: \$0. If processed in the displayed order, all transactions are valid, i.e., have adequate balances in originating users' accounts. Were tx_a processed *after* tx_b, however, then both tx_b and tx_c would be invalid.

pseudonymous accounts, discusses techniques for enforcing strong privacy, and addresses issues of privacy as it relates to regulatory compliance.

The transactions recorded on digital ledgers can transfer money between accounts, but can also perform more complex actions. *Smart contracts*, discussed in section 7 ("Smart Contracts"), are computer applications that execute on top of and can greatly expand the capabilities of digital ledgers and thus CBDCs. We explain how the history of smart contracts in cryptocurrencies illuminates potential benefits, including the opportunities to create powerful, novel financial instruments, but also highlights the potential pitfalls of enriched CBDC capabilities.

We discuss *secure hardware* in section 8 ("Secure Hardware"), specifically a powerful new set of security features available in recent-model computer chips. Little known outside information security circles, secure hardware can serve as a powerful addition to the security architecture of a variety of high-trust systems, including CBDCs. We discuss the limitations and recognized vulnerabilities of secure hardware and consequently where it is and is not appropriate to incorporate it into CBDC architectures.

The transaction information in a CBDC could offer unprecedented visibility into monetary flows, given financial regulators new insights into the functioning of a national economy. We discuss such opportunities in section 9 ("Opportunities for Novel Financial Technology"), as well as ways that enhancements to CBDC systems, such as non-fungible tokens (e.g., currency with attached spending conditions) and smart contracts can serve as vehicles for innovative financial interventions.

A number of legal considerations will have a significant bearing on CBDC design choices, as discussed in section 10 ("Legal Considerations"). Existing laws, particularly in the U.S., would seem to offer fairly wide latitude in the degree of privacy afforded by a CBDC. Legal requirements for remediating erroneous or fraudulent transactions and enforcing liens will require careful consideration of appropriate technical provisions in a CBDC and may motivate the enactment of supporting legislation.

While still in their infancy, given their maturity by comparison with related projects, study of the digital yuan and Libra can help elucidate critical design choices. We outline what is known publicly about their technical designs in section 11 ("Overview of Libra and Digital Yuan"), and also discuss hypothetical capabilities revealed in published patent applications relating to the digital yuan.

2 Overview from a Banking Perspective

The basic functions of money are that it serves as a unit of account, medium of exchange, and store of value. While money is associated in the popular mind with physical cash issued by central banks, broader monetary aggregates that serve some of these functions include bank deposits created by commercial banks when they make loans. Thus, while currency banknotes and coins are physical forms of money, much of the stock of money in modern economies is already in digital form. Even digital central bank money has already existed for a long time. Electronic balances held by commercial banks (and, occasionally, other financial institutions) at central banks, referred to as reserves, are used to facilitate payments and settlement through interbank payment systems managed by the central bank.

The specific innovation that we consider in this paper is the replacement of central bank issued money that can be used for retail transactions with their digital counterparts, which have come to be referred to as CBDC. In short, CBDC are fiat currencies issued by central banks in digital form in place of, or as a complement to, physical currency (banknotes and coins).

One simple form of CBDC is e-money. This can take the form of specific amounts downloaded to a mobile phone app by designated financial institutions (in exchange for cash or transfers from bank accounts) and that can be used for making payments at approved businesses. In an alternative formulation, all agents in an economy would have access to central bank accounts, where the balances could in principle be interest-bearing. The central bank would in effect become the manager of a sophisticated payments system that would also allow it, depending on the structure of this CBDC, to implement conventional and unconventional monetary policy in nonstandard ways and, in some respects, more effectively.

The first option is easiest to implement and, in combination with mobile phones that have become ubiquitous even in low-income economies, has significant potential to improve financial inclusion and reduce dependence on cash. The second option is technologically and conceptually more complicated but has greater potential to be scaled up into a payments system that serves as a backup to the private payments infrastructure.

One concern about central bank deposit accounts is the possible disintermediation of the banking system–a subject that will be explored in more detail later in this paper. Recognizing this risk, some central banks that are experimenting with CBDC are taking a hybrid two-tier approach. Under this approach, central banks would disseminate CBDC to commercial banks–just as they now do with cash–and commercial banks would distribute these to individuals and businesses by setting up and managing digital wallets.

Some governments, such as those of the Marshall Islands and Venezuela, have ventured to develop what they refer to as *Official cryptocurrencies*. The Venezuelan government has created the Petro, a digital currency backed by the country's oil reserves, which is ostensibly a cryptocurrency that could help avoid financial sanctions imposed by the United States. It is far from clear whether such digital currencies can be considered the equivalent of fiat currency and how they would help get around international financial sanctions.

2.1 Technical definitions

Kumhof and Noone [11] provide a useful definition of CBDC to distinguish it from reserves and cash. They define CBDC as electronic central bank money that: (i) can be accessed more broadly than reserves, (ii) has functionality for retail transactions, (iii) can be interest bearing (with a rate different from that on reserves), and (iv) has a separate operational structure relative to other forms of central bank money.

Yao [12] offers a more technologically-oriented definition, positing that a CBDC is "a credit-based currency in terms of value, a crypto-currency from a technical perspective, an algorithm-based currency in terms of implementation, and a smart currency in application scenarios." He argues that cryptographic technology is essential for security and credibility of the DFC. He also notes that CBDC is not just a digital version of cash but has the potential to make money "smarter."

Bjerg [13] lays out a broad definition of CBDC as electronic, universally accepted, central bank issued money and discusses three possible scenarios. In the first one, the CBDC serves as electronic cash, complementing cash and bank deposits and, thus, fulfilling the role of medium of exchange. The central bank would maintain parity and free convertibility among CBDC, cash, and bank deposits. In a second scenario, the CBDC would serve as universal reserve and fulfill the role of store of value, replacing cash. The central bank would maintain parity but not free convertibility between CBDC and bank deposits. In a third design, CBDC serves as sovereign account money and as the unit of account, potentially replacing bank deposits. In this scenario, the central bank takes the sole responsibility of creating and issuing money in the economy, maintaining free convertibility between CBDC and bank deposits. The central bank could effectively use monetary policy to create or destroy liquidity in the system based on the state of the economy.

Bordo and Levin [14] present two designs for CBDC as a medium of exchange. In the first, the central bank circulates "CBDC tokens," supported by distributed ledger technology for ownership verification and payment transactions. In the second, the central bank maintains "CBDC accounts" that facilitate electronic holding of funds for individuals and follow a simple debiting and crediting transaction protocol that is instantaneous and costless. The authors then explore three alternatives for a secure store of value. First, similar to paper currency, the central bank would issue CBDC with "constant nominal value" and earning zero interest. This would constrain the central bank from implementing a negative nominal interest rate. Second, the central bank would retain "stable real value" of CBDC through price level indexation of CBDC, which would also constrain policy at the zero lower bound. Third, the central bank would provide an interest-bearing CBDC where the interest rate would be positive in a growing and stable price economy. The authors argue that such a CBDC would serve as a stable unit of account with the help of flexible price-level targeting monetary policy.

The sampling of definitions above suggests that there is no clear consensus yet on the definition of a CBDC, with both conceptual and technological issues still being sorted out. Both of these sets of issues are tied in to the motivation for a central bank to issue a CBDC.

2.2 Why issue a CBDC?

The key motives for issuing retail CBDC range from broadening financial inclusion to increasing the efficiency and stability of payment systems. In Sweden, an economy where the use of cash is fast disappearing, the central bank's consideration of retail CBDC, in the form of an e-krona, seems to be driven primarily by concerns about financial stability. The sharp decline in the use of cash for retail payments has occurred in tandem with a shift toward privately-managed payment systems and consolidation among a small number of commercial participants, payment services, and infrastructures.

The Riksbank notes than an e-krona could alleviate the problem of concentration of the payments infrastructure and also its potential vulnerability to loss of confidence. The digital currency would be based on a separate infrastructure that would also be open to private agents willing to offer payment services linked to the e-krona. The general public would have access to the e-krona with both payment suppliers and fintech companies having access to the network. Thus, an e-krona system would promote competition, innovation, and financial stability.

A primary motivation for emerging market economies to consider issuing CBDC seems to be related to financial inclusion. An app-based CBDC that takes advantage of mobile technologies can increase access to financial services for the poor, rural households, and other segments of the population that may be underserved by the banking system.

There are a number of ancillary benefits to a CBDC. Paper currency is vulnerable to counterfeiting. CBDCs could in principle reduce this risk, although the risk of electronic counterfeiting on an even more massive scale through hacking is a major concern for governments that intend to take this route.

Another potential advantage of a CBDC is that it would discourage illicit activity and rein in the shadow economy by reducing the anonymity of transactions now provided by the use of currency banknotes, a point made forcefully by Rogoff [15], especially in the context of high-denomination banknotes. This would also affect tax revenues, both by bringing more activities out of the shadows and into the tax net and also by enhancing the government's ability to collect tax revenues more efficiently.

Ensuring compliance with anti-money laundering/combating financing of terrorism (AML/CFT) regulations has been a major challenge for government authorities. The elimination of physical cash could assist in these efforts, although the likely shifting of illicit fund transfers to decentralized payment systems and intermediated through anonymous, decentralized cryptocurrencies could vitiate this progress. This is one reason why central banks might seriously consider issuing CBDCs so they can retain control of or at least oversight over payment systems that could as easily be used for illicit as for licit purposes.

These benefits come at the potential cost of loss of privacy in commercial transactions if these can be intermediated only through private or government-managed electronic payments systems. While various encryption technologies in principle allow users of retail CBDC to retain privacy, it is likely that these are subject to the same technological vulnerabilities as nonofficial cryptocurrencies, where privacy has been difficult to ensure.

Some of the trade-offs between physical and electronic forms of fiat currency issued by central banks are analyzed by Mishra and Prasad [16] in the context of a simple general equilibrium model. The key differences between these two forms of central bank-issued outside money include transaction costs (lower for CBDC), possibilities for tax evasion (higher for cash, but with a positive probability of being caught and penalized), and nominal rates of return (zero for cash; potentially positive or negative for CBDC). They show the conditions under which cash and CBDC can co-exist and also show how different combinations of government policies, such as the level of taxes and the penalty for being caught undertaking tax evasion, can influence the relative holdings of cash and CBDC. The model provides a framework that can eventually be extended to evaluate conditions under which different forms of government-backed and privately-issued currencies can coexist, conditional on the attributes of each of those currencies and also government policies.

2.3 Implications for the international monetary system

The advent of CBDC, cryptocurrencies, and other new financial technologies could have implications over the long run for certain aspects of the international monetary system. One of the major benefits of improved electronic payment and settlement systems that would go with the proliferation of digital currencies is the increase in speed and security of transactions, along with a reduction in their costs. This would mark a substantial improvement for settlement of trade-related transactions as well as remittances. Even cross-border settlement of other types of financial transactions could benefit from these developments. DLTs offer the potential for reliable tracking of different stages of trade and financial transactions, reducing one of the frictions associated with such transactions. Such changes might simply increase the efficiency and lower the cost of transactions routed through banks and other traditional financial institutions rather than displacing such institutions.

Both banks and nonbank financial institutions could expand the geographical scope of their operations across national borders using the new technologies. This creates new challenges for supervision and regulation. One complication is the lack of clarity about the domicile of informal financial institutions and the geographical locus of the supervisory authority of national regulators. The second is the potential accentuation of cross-border financial stability risks as more institutions operate across national borders. Some of these challenges could be overcome by the greater transparency of transactions if they are conducted using a public DLT or if the regulator has access to the relevant private ledgers.

For emerging market economies, the expansion of conduits for cross-border financial flows with greater efficiency and lower costs could be a double-edged sword, making it easier for them to integrate into global financial markets but at the risk of higher capital flow and exchange rate volatility. Such volatility, in part related to spillovers of monetary and other policies from the U.S. and other advanced economies, has often caused significant stresses for corporate and sovereign balance sheets in these economies. These challenges could become greater if new payments systems and digital currencies increase both the volumes and fluctuations in cross-border capital flows and make capital controls less potent, adding to such volatility. The intensification of global financial cycles would not only engender more capital flow and exchange rate volatility, but could also constrain monetary policy independence, even for central banks that practice inflation targeting backed up by flexible exchange rates. New channels for transmitting payments across borders more quickly and cheaply are likely to make it more difficult to regulate and control capital flows.

3 Ledger Infrastructure

The goal of a digital currency system is to track the balance of its users, allowing each to transact only her coins. One cannot map the technique of physical currency transaction to the digital world. A coin cannot be a simple file, and a transactions cannot be a transmission of the file from one user to another: Had it been done this way, the sender could have kept her copy, thus keeping the coin while also sending it.

Instead, contemporary digital currency systems maintain a global state, comprising the balances of all their users. This includes everything from banks' per-client balance tables to cryptocurrencies like Bitcoin [17] and Ethereum [18]. Updates to the state are called *transactions* – these could be simple transfers of funds or interaction with *smart contracts*. The transactions are serialized in a single *ledger*. The state of the system is the result of processing the transactions in the ledger according to their order. The transactions are typically aggregated into so-called *blocks*, each containing many transactions, and the blocks are linked to form a chain, imaginatively called a *blockchain* (Figure 2).

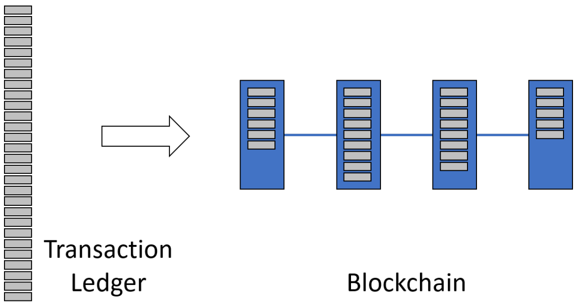


Figure 2: Each block contains transactions and the block order determines the global transaction order.

The system should allow participants to add blocks in a serial order, so the system progresses in a well defined manner. It should also allow all and only transactions that abide by its predefined rules, and prevent the removal of a block, which would have implied a reversal of history.

To avoid vulnerability to the crash or misbehavior of one or several machines, the blocks and state should be *replicated*, i.e., stored and processed concurrently by multiple machines. The challenge is thus to orchestrate these machines so they all agree on this order and behave like a single coherent machine, despite network latencies and arbitrary misbehavior by a subset of them. This is called *State Machine Replication* (*SMR*) in distributed systems literature. Even in a centralized setting, there are hardware failures, so it is prudent IT system design to incorporate multiple nodes for fault tolerance.

The design of the underlying SMR and networking layers affects the performance and the security of the system, but perhaps most significantly defines its ethos – how decentralized the system is. This choice determines how open the system is to participants, and how much it is in the control of one or a few entities, which can redefine its behavior, stop its operation, withhold certain transactions, etc.

There is a spectrum of decentralization designs, from bank balance tables, through semi-centralized systems like Ripple [19] and Libra [20], to cryptocurrencies, and there are clear trade-offs to be considered when designing a CBDC. The rise of cryptocurrencies since 2009 incited rapid advancement across this spectrum.

In the rest of this section, we first outline basic information security principles that are important in understanding and evaluating digital currency designs (§3.1), then refine the distinction between distribution and decentralization (§3.2), and proceed to review the design choices for the SMR mechanism (§3.3) and their trade-offs.

An independent challenge is to increase the system throughput beyond the capacity of a single machine. In order to accommodate the needs of a CBDC, the system should process a large number of transactions quickly. We briefly discuss approaches to scaling ledgers to large transaction volumes (§3.4), such as by *sharding* or partitioning of system state.

3.1 Information security foundations: The Confidentiality, Integrity, Availability (C-I-A) triad

No digital currency will remain operable and in use for long without satisfying certain fundamental *information security* properties. In particular, classical information security principles define three orthogonal and complimentary "dimensions" of information security: *confidentiality*, *integrity*, and *availability*, often collectively referred to as the *C-I-A triad*, illustrated in Figure 3.

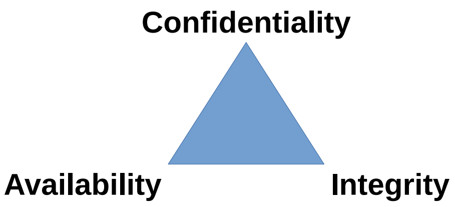


Figure 3: The three main protection goals of classic information security: Confidentiality, Availability, and Integrity.

In brief, confidentiality means that the information system does not leak information to those who should not have access to it. Integrity means that the system should store information correctly and produce correct results to computations, allowing neither to be tampered with maliciously for example. Availability means that the system should respond to users promptly when requested to retrieve data or perform some action, such as committing a digital currency transaction.

But how do we ensure that each of these dimensions of information is satisfied, and what types and degrees of costs are we willing to incur to guarantee these information security properties? This is where techniques for distribution and decentralization, fundamental to cryptocurrencies and CBDCs alike, come into play.

3.2 Distribution and decentralization

Distributed systems: A *distributed* system fundamentally consists of multiple devices communicating and coordinating over a network. There are innumerable varieties of distributed systems and countless functions they can perform. The most relevant type of distributed system for a CBDC is, of course, a *distributed ledger*, or group of devices cooperating to maintain a transaction history. Using *state-machine replication* or *consensus* algorithms as described below in Section 3.3, the devices comprising a digital ledger maintain copies or *replicas* of the transaction history and keep them synchronized. This replication protects the availability of the ledger by ensuring that even if some replicas fail, the other devices can continue servicing user transactions.

Traditional client/server and cloud computing infrastructures tend to use distribution in this way primarily to protect availability, and place the greatest investments toward this goal. Geographically distributed systems, for example, distribute the replicas of a service (such as a ledger) across data centers located in different cities or regions, so that a network or power outage affecting one entire data center does not make the entire service unavailable. Though widely distributed, cloud infrastructure is still typically highly *centralized* in that it is owned and controlled by one central authority (the cloud provider).

Decentralized systems: A *decentralized* system, in contrast, is a type of distributed system whose composite devices are *not* under control of a single, central authority. Decentralizing a system across independent authorities in principle reduces the amount of trust we must place in each, and similarly limits the damage any one authority can cause if it is compromised or misbehaves in some way.

There are many different and often-conflicting ways in which a system may be *decentralized*, however, and just as many fiercely-debated criteria for deciding whether and how much a system is actually "decentralized." In particular, decentralization often refers to some combination of *role separation*, *trust dispersal*, and/or *threshold trust*, as we outline below.

Role separation: Perhaps the weakest, but useful and ubiquitous, form of "decentralization" is the division of a process into multiple qualitatively-different functions carried out by multiple authorities serving in different roles. The corporate accounting practice of requiring one person to write checks, and another person sign them, is classic example of role separation within an organization. The division between the roles that central banks and commercial banks play in classical economics – the former managing the national money supply and the latter managing customer relationships – is a large-scale example of role separation. The Bank of England's CBDC proposal to delegate the account management role to a commercial Payment Interface Provider (PIP) [10] is an example of (limited) decentralization via role separation in a CBDC design.

Trust dispersal: When one role in a distributed system may be played by many independent authorities, each serving only a small subset of the total user population, trust is *dispersed* among these authorities. The dispersal of a nation's governmental powers across many regional and local governments, each having jurisdiction mainly only over its own residents and territorial domains, is a classic pre-digital example of this form of decentralization.

In a CBDC design in which many different companies implement the PIP role on behalf of their customers and *only* their customers, only those customers of a given PIP in principle need to trust that PIP. The trust that the entire system collectively places in the PIP role, therefore, is dispersed among the many companies serving that role, limiting the damage any single (smaller) compromised PIP can cause. Each individual user must fully trust their chosen PIP, however, and if one is compromised then the damage to that PIP's unlucky customers – in terms of confidentiality, integrity, and availability – may be severe and difficult to limit. Further, if one or more of the authorities playing such a role becomes "too big to fail" – e.g., serving too much of the user population – then even the global protection ensured by trust dispersal may be limited.

Threshold trust: Finally, systems may be decentralized such that users need not "choose" and then fully trust a single authority. Users instead individually or collectively split their trust across several authorities independently serving in the same role, so that no single authority or small coalition have unlimited power or authority over *any* user. A board of directors or parliament is a classic organizational embodiment of threshold trust, for example, whose members are collectively trusted but no single member can act alone. A distributed ledger, spread across a consensus group of servers operated by independent companies in a federation, provides threshold trust at least in terms of the ledger's availability, so that the ledger remains available to serve *all* users even if *any* one or a limited number of member servers go offline.

Consensus or state-machine replication of this form does *not* necessarily protect users from integrity or confidentiality failures in these servers, however. Any single compromised server may be able to fake or rewrite history, unless the consensus algorithm is also designed to tolerate malicious or *Byzantine* failures – a property that most public cryptocurrencies strive to provide but which many "permissioned" blockchains fail to ensure. Similarly, any single compromised server may leak any confidential data that server may have had access to, unless the confidential information is separately protected via *threshold cryptography* mechanisms, for example, as we discuss in Section 6.3. Therefore, it is important to understand *which* properties of the C-I-A triad discussed above a given ledger design protects with threshold trust, and which properties remain potentially vulnerable to "weakest-link" failures.

3.3 State machine replication for distributed ledgers

The level of decentralization of the ledger state-machine-replication infrastructure can be roughly divided into three categories. On one end there is the centralized option (§3.3.1), where the central bank runs the system itself. This is arguably a good

	Centralized	Semi-Decentralized	Decentralized
Archetypal Example	Amazon Quantum Ledger Database [21]	Libra [20]	Bitcoin [17]
Performance	Excellent, full control of infrastructure	Good, SMR with many participants	Challenging, active area of research
Censorship	Easy: single operator	Possible: particularly if operators are in the same jurisdiction	Hard: operators might not even be identified
Rewind	Easy: can be done quickly by single operator	Hard: takes longer for operators to agree, implying longer history to revert and worse violation	Extremely hard: requires cooperation by majority of possibly unidentified operators

Table 1: Centralized vs. Decentralized Infrastructure

starting point, as it is the easiest to manage and builds on classical system design. However, this design choice misses central goals of a CBDC. As the centralized CBDC can unilaterally withhold transactions or even change the rules or revert history, the users are not getting the same guarantees as in cash. Indeed, these aspects are closer to those of payment application.

As a first step, history revision can be prevented by providing users with commitments that their transactions are irrevocably committed in centralized but verifiable ledgers (§3.3.2). But one can do better.

In a semi-decentralized, or *permissioned* option (§3.3.3), a consortium of entities collaboratively runs the system. Such a design denies full control of the system from small subsets of the operators, but still allows for centrally-coordinated changes, which can be an advantage for legal purposes and is often desirable by customers.

Finally, a fully decentralized option (§3.3.4) would implement a CBDC on an infrastructure similar to that used by cryptocurrencies like Bitcoin – a design that has demonstrated unprecedented robustness in the wild. The decentralized option implies a lack of centralized control; this is arguably the goal of a CBDC, in contrast to payment applications and digital bank accounts, but due to legal and regulatory considerations it is not trivially acceptable in the CBDC context.

We review these options below, and summarize them in Table 1.

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

3.3.1 Centralized ledgers

The most straightforward approach to implement a CBDC ledger infrastructure is in a centralized fashion. For resilience the system should still be distributed, replicating the state among multiple servers. Classical solutions to this challenge have been studied for decades [22], providing protocols that overcome crashes of a subset of the servers, as well as unexpected behavior due to bugs or an attack [23]–[26].

Crash faults imply a danger only to availability (in the C-I-A triad). State machine replication (SMR) algorithms that protect against crash faults have well-understood solutions with mature, efficient implementations already widely-used in cloud computing environments for example (e.g., [27], [28]).

Servers that behave arbitrarily for whatever reason – such as by being hacked or under control of a compromised insider – can violate not only a ledger's availability but also its integrity. It is important to understand that mere replication does not protect a ledger's integrity against arbitrary *Byzantine* failures such as hacking or insider attacks. Even in a widely-replicated ledger, a single compromised server behaving maliciously might be able to rewrite history illegally, "print money" without detection, or trick a targeted victim into thinking a transaction has been committed while everyone else sees a conflicting transaction, or no transaction, on the ledger. State machine replication algorithms that protect against Byzantine failures, or *Byzantine fault tolerance* (BFT) mechanisms, have also received a great deal of research attention (e.g., [25], [28]). Byzantine fault tolerance mechanisms tend to be more complex and less mature than SMR algorithms tolerating only crash faults, however, in part because their development has not been driven by the already-ubiquitous cloud computing paradigm.

Challenges remain to avoid *common mode failures* among multiple system nodes (servers), such as a power or network outage affecting several (or all) nodes at once. The typical solution for geographically-localized common mode failures – such as outages caused by lightning strikes, floods or other natural disasters, or long-distance roadside cables accidentally cut by backhoe operators – is *geo-replication*: locating nodes in different data centers widely spread geographically.

Another type of common mode failure affecting Byzantine replication mechanisms is software bugs. If all replicas run the same implementation of the same algorithm and this implementation has an exploitable vulnerability, then a hacker or malicious insider could compromise all (or a threshold of) the nodes at once to compromise the ledger's integrity, despite its nominal protection against Byzantine failures. Using diverse software implementations on each server is one solution to this common mode failure risk, albeit one incurring considerable development cost [29], [30].

With centralized or semi-centralized ledger designs, a small number of servers is usually sufficient. This small number is relatively easy to coordinate and achieve good performance, as the machines can quickly propagate messages among each other. However, in a fully-centralized design in which the choice of nodes and their operation are all under direct control of one authority such as the central bank itself, that authority – or a malicious insider – can potentially change the rules at will, roll back system state or rewrite history, and censor or delay transactions. These capabilities

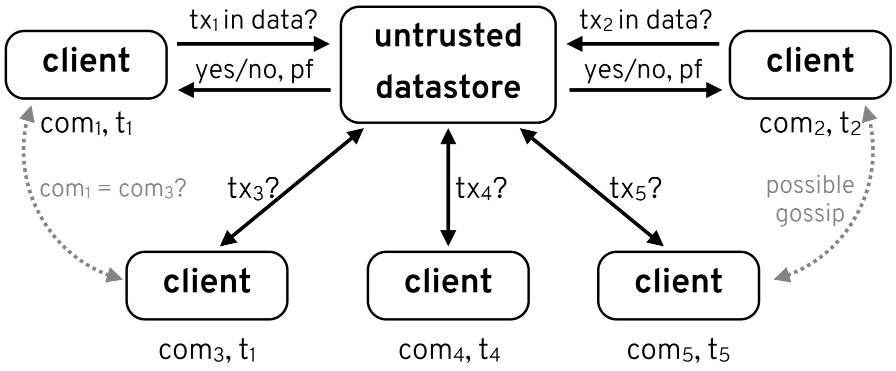


Figure 4: An overview of the interactions involved in an authenticated data structure. Clients do not trust the server in possession of the data. When the server tells a client whether or not a transaction is in the dataset, it provides a proof that this response is correct, which the client can check against a commitment to the data that it maintains and updates when needed. To ensure that the server is providing a consistent view of the dataset to all clients, a form of gossip is needed (which need not involve direct client-to-client communication). As one example (on the left), clients with commitments representing the same point in time (t_1) may want to check that these commitments are identical.

may be desirable from a management perspective, but may be undesirable from a perspective of robustness or public trust.

3.3.2 Centralized but verifiable ledgers

Even in a centralized setting, there are still ways to limit the trust that clients need to place in the servers maintaining the ledger. In particular, *authenticated data structures* [31]–[34] (ADSs) provide a method by which a server, in possession of some data, can prove things about that data to a client who does not necessarily trust the server to give accurate answers. For example, a client receiving money in a CBDC may want to ensure that the transaction in which they are being paid has gone through before providing any goods or service; i.e., they want to check for the inclusion of this transaction in the ledger. Rather than have the server simply tell the client if the transaction is included or not, in an ADS the server also provides a cryptographic proof of inclusion that the client can verify. The main guarantee of an ADS is that it should be impossible for a server to provide a valid proof for a response that does not accurately reflect the data it has stored.

To satisfy this requirement, clients must have some *commitment* to the data stored by the server, which the clients can then check the proof against. This commitment acts as a cryptographic fingerprint of the state of the entire dataset at a given point in time and is updated as the data changes; crucially, while it covers the entire dataset its size is a small constant that is independent of the size of the dataset. A central challenge of ADSs is that clients cannot be sure that their commitment is a canonical representation of the data stored by the server. In a *split-view attack*, for example, a malicious server may attempt to present different clients with commitments to different data, and thus make them believe that different transactions are or aren't included in the ledger. In the extreme case, a server could store completely different data for each client, and thus provide each one with a different commitment; this would not prevent them from providing valid proofs, but the results would be meaningless as there would be no global and unique representation of the server's state.

To prevent—or at least detect—split-view attacks, clients must typically engage in a *gossip* protocol [35], by which they can learn about the commitments held by other clients and thus ensure that they have the same view of the data. Options for gossip protocols range from client-to-client communication [36] to having the server post the commitment on a public blockchain [37], [38]. An alternative protection against split-view attacks is to employ a *witness cosigning* protocol [39], in which the primary server maintaining the ADS first obtains cryptographic co-signatures on each fingerprint commitment from a threshold of independent witness servers before publishing or returning that fingerprint to clients. The witness servers need not repeat or thoroughly check the primary server's work, but merely attest that they have witnessed and cosigned at most one cryptographic view for a given state version. Witness cosigning can eliminate the bandwidth, energy, and potential privacy costs to clients participating in gossip protocols, and can protect clients that are disconnected or whose network connectivity is under an adversary's control [40], [41]. The main cost is that the witness servers must be deployed and managed, introducing limited decentralization, and clients must trust a threshold of witnesses to behave correctly, rather than trusting only in each other and the network as with gossip.

It is also possible to use ADSs to create a more distributed ecosystem, as is perhaps best exemplified by the Certificate Transparency (CT) project.[3] In the CT ecosystem, a variety of organizations log certificates signed by a Certificate Authority, and clients ensure using the interaction described above that all the certificates they see appear in at least one of these logs. This is crucial due to the central role that certificates play in providing trust in the Internet ecosystem, in the form of underpinning encrypted communication (HTTPS), and due to the known cases in which CAs have misissued certificates [42], [43]. A decentralized network of auditors and monitors are then free to interact with these log servers to check, respectively, that they are properly storing the data (e.g., they are not carrying out split-view attacks) and that the certificates they are storing are valid according to some global set of rules (e.g., that a Certificate Authority has not misissued a certificate). This type of architecture may accommodate a CBDC [44], in which certificates are replaced with transactions and the role of log servers is played by commercial banks or other entities with an existing stake in the ecosystem.

3.3.3 Semi-centralized ledgers

To reduce centralization, the CBDC can instead be operated by a larger set of independent parties chosen or approved by the central bank. Superficially, the solution

[3] https://certificate.transparency.dev/

is similar to the centralized approach – instead of directly operating the different nodes, the central bank chooses the entities that run them. In practice, however, this approach is quite different, as the central bank forgoes its total control of the system. With dozens or even hundreds of independent operators and adequate technical protection against Byzantine faults in the state machine replication scheme, no single party or group of parties (below a certain size) can change the rules, perform censorship or roll back the system state. Nevertheless, since the operators are all chosen by the central bank, that central bank can facilitate an agreement of all parties to perform arbitrary changes. This allows the operators to comply with regulatory and legal requirements, as well as revert illegal operations due to attacks. Indeed, the central bank can deploy complex governance mechanisms, where different subsets of the operators can force a decision or exert veto power.

Therefore, despite the distribution of operation, the semi-decentralized approach lacks the true decentralization of physical cash. Users of a semi-centralized CBDC have less control over their funds than with cash. However, this control is an advantage in certain perspectives: Law enforcement agencies can compel the operators to enforce monetary controls, censor transactions, etc., particularly if they are all within the same jurisdiction.

The basic design considerations of protocols for semi-centralized systems are similar to the centralized case. Indeed, the distributed systems literature puts them in the same category, implementing a replicated state machine by a set of predefined nodes. However, the large number of nodes make classical solutions problematic – the amount of communication they require is typically quadratic in the number of nodes, making them prohibitively slow among many independent parties.

Building on ideas from cryptocurrencies, recent work [28], [45]–[47] proposes state machine replication solutions that reduce most communication to be linear in the number of nodes, and hence practical even with a large number of operators. This is the approach chosen by Facebook's Libra (§11).

3.3.4 Decentralized ledgers with central-bank monetary control

The most decentralized approach available is to use a blockchain infrastructure similar to that of cryptocurrencies. Unlike those cryptocurrencies, the CBDC is under centralized monetary control, but anyone can join and operate the system. This approach is called *permissionless*, as operators do not need permission from the central bank to join. Although the system operators can still change the system rules (known in Cryptocurrency as a *fork*), in a permissionless system a fork requires a wide agreement among independent parties. This makes controversial changes unlikely, but also takes away the control of the central bank.

On the positive side, decentralized blockchains demonstrate unprecedented robustness – Bitcoin has been running continuously without interruption[4] for over a

[4] In two famous events [48], [49] there have been issues with Bitcoin's blockchain layer. But, if anything, they demonstrated its robustness: although some operators significantly deviated from the prescribed protocol, the impact on the users has been inconsequential.

decade. A decentralized implementation also prevents monetary controls and transaction censorship – the open membership implies that the different operators are not subject to the decision of any central entity. This is a desirable property of an instrument that strives to replace physical cash.

However, this decentralization also implies no central control even when it is necessary, e.g., no reversal of transactions in case of mistakes, and no prevention of operator misbehavior like front-running [50], [51]. The setup would therefore have to include means aimed directly at these scenarios, which are active areas of research.

Finally, it is not immediately clear how to implement the decentralized approach in the context of a CBDC. To ensure the security of such an open system, incentives are used. System operators, often called miners as in Bitcoin, should receive rewards to incentivize them to follow the desired protocol. Unlike cryptocurrencies, here the central bank determines the inflation rate, and the rewards for the miners. Although it does not choose the miners in the open system, the central bank in this setup is still uniquely powerful, as it determines the reward rules.

The common technique for securing decentralized blockchains is Proof of Work [52], [53], as used in Bitcoin, Ethereum, etc. The idea is that miners expend physical resources, typically electricity, to participate in the protocol and receive rewards. A coalition that controls less than a threshold of the resources will maximize its revenue by following the rules [54]–[58]. Moreover, if the rewards are sufficient [59], an attacker cannot perform a Denial of Service (DoS) attack (i.e., stop the system) with less than 50% of the mining power.

Other alternatives have also been explored (e.g., [60], [61]), with *Proof of Stake* (*PoS*) [62], [63] gaining the most traction. In PoS, the operators are the system participants, i.e., they have a stake in the system. While there remain challenges in understanding the incentive mechanism of PoS and its security, PoS avoids the energy expenditure necessary in PoW [64], which is unacceptable for CBDC.

A decentralized cryptocurrency's openness to a large number of permissionless participants does not imply absolute protection against ledger manipulation or censorship. In practice the distribution of mining power in PoW cryptocurrencies, or the distribution of stake in PoS currencies, has often proven to be so concentrated that only the top 2, 3, or 4 miners or stakeholders account for a majority of voting power, and thus could in principle collude (perhaps secretly) to censor or manipulate the ledger.[5] Further, any permissionless cryptocurrency allowing open participation is potentially vulnerable to attacks by any adversary sufficiently resourceful and motivated to deploy large-scale computational or financial resources in an attack, even just temporarily. An attacker might short-sell a currency in other markets in order to "bet against" its value, for example, just before launching an attack that deliberately violates the system's economic rationality assumptions [65]. Many flavors of such attacks have been explored [66]–[69], and actual 51% attacks on real permissionless cryptocurrencies have become increasingly common in practice [70].

The openness of a permissionless system also typically implies slower performance, as it takes longer for the participants to realize who is actually participating. Nev-

[5] See for example https://bitcoinera.app/arewedecentralizedyet/.

ertheless, even in an open system it is possible to achieve throughput limited only by network properties [46], [71]–[74], and good latency with advanced block topologies [73], [75].

In conclusion, we believe a fully-open, permissionless design option is not at this point a natural choice for a CBDC, due to its extreme lack of central control. For example, Libra has recently stated [20] that "...a key concern expressed by regulators in a number of jurisdictions, including the Swiss Financial Market Supervisory Authority (FINMA), is that it would be challenging for the Association to guarantee that the compliance provisions of the network would be maintained if it were to transition to a permissionless network where, for example, no due diligence is performed on validators." We therefore believe that there remain technical, legal and regulatory questions to answer before this permissionless approach can be adopted in a CBDC.

3.4 Scalability to large transaction volumes

Whichever ledger design approach is taken, another element to address is how to scale performance beyond the capacity of a single server. While even in a fully decentralized architecture there are protocols that allow for arbitrarily high transaction throughput, all those transactions must be processed, and the workload can grow beyond the capacity of any one server. The openness of permissionless systems like Bitcoin does not help the system handle increased transaction load, because each miner is replicating, and hence repeating, all of the work of processing *all* transactions, leaving the maximum processing rate fixed regardless of participation.

There are several complementary approaches to this question. The first [76], [77] is to split the state into multiple parallel ledgers. Each ledger is operated by different servers, allowing the system capacity to grow by the number of parallel chains. However, special care must be taken when using this approach to make sure the security of each chain does not deteriorate compared to a single chain. Additionally, a split into parallel chains implies that special, often slow, protocols must be used when a transaction spans the state of multiple chains, e.g., making a payment from an account in one chain to an account on another. This approach applies when the state can be cleanly split into chains with little interaction, and the number of participants is large enough to allow splitting their roles among the different chains.

Another approach [78] is to operate a ledger with some arbitrary protocol, but rather than using a single machine per node, replace it with several interconnected servers that operate as a single high-performance node. This approach maintains the security properties of the original protocol and allows for scaling according to the resources available to the different nodes. It applies when it is acceptable to rely on more resources per node operator, which is likely the case in the CBDC setting.

We discuss in Section 7.2 methods to reduce ledger load by offloading transactions to direct peer-to-peer channels. These rely on an efficient underlying ledger and are independent of its implementation.

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

4 Account and Identity Management

Since a CBDC cannot achieve its maximum usefulness unless ordinary individuals can hold and use the digital currency, this raises the key question of who should be responsible for managing accounts and satisfying associated responsibilities such as identity-checking for "know your customer" (KYC) compliance. This section first explores the question of who should be responsible for account and identity management, then briefly surveys current and emerging approaches to digital identity and how they may (or may not) be relevant to CBDCs. The important topic of identity privacy will be covered later in Section 6.

4.1 Who manages accounts?

Central banks traditionally do not maintain accounts for or enter into business relationships with individuals, only with banks. In this way, central banks effectively delegate the task of managing individual accounts and customer relationships to the commercial banks. Allowing individuals to open and use CBDC accounts directly with the central bank, therefore, would be a "new business" for most central banks, bringing with it many account- and identity-management challenges and potential risks. Providing individual accounts directly with the central banks may be a concern for citizens as well: for example, many potential customers may be more inclined to entrust their personal and financial information to a local business than to a remote government agency that they can at best hope to contact by phone or online.

Accounts in cryptocurrencies: Most decentralized cryptocurrencies such as Bitcoin are technically designed to address – or perhaps to *avoid* – the account and identity management problem in a different way: by defining "accounts" not in terms of human identities but in terms of pseudonymous cryptographic key pairs. Bitcoin or Ethereum accounts are simply random-looking strings that represent cryptographic *public keys*. Anyone who knows the corresponding, mathematically-related *private key* associated with that account can spend the currency it holds. This property is what makes decentralized cryptocurrencies a cash-like character, with corresponding advantages and disadvantages. The cryptocurrency *miners* primarily responsible for maintaining and securing the ledger can avoid managing or checking traditional individual identities.

The perceived privacy that decentralized cryptocurrency accounts provide is attractive to many cryptocurrency holders, although the use of pseudonymous key pairs alone offers only weak privacy, due to the many available de-anonymization attacks discussed later in Section 6.1. On the other hand, this disconnect between purely cryptographic accounts and human identities has in part given cryptocurrencies a shady, "underground" character, making it difficult for individuals and businesses to use and convert cryptocurrencies directly while ensuring legal compliance. The irreversible character of cryptocurrency transactions also gives individuals no clear recourse path if their cryptocurrency is stolen, due to a hacked wallet for example – an important usability and security issue discussed further in Section 5.

Cryptocurrency exchanges: This gap between cryptographic keys and human identities has in part driven the development of centralized *exchanges* and related businesses intended to bridge this gap. A cryptocurrency exchange typically allows customers to trade one or more traditional currencies for one or more cryptocurrencies. To make this possible, exchanges typically maintain a traditional account and business relationship with each individual customer, and they either take on directly or further delegate the identity-checking tasks required to ensure compliance with the prevailing legal and financial policies.

On the positive side, exchanges can make the use of cryptocurrency more convenient to customers more familiar with traditional banks, and potentially more legitimate and compliant in reality and/or perception. On the negative side, in practice most exchanges are centralized third parties that must be trusted with the custody of users' cryptocurrency balances. Such centralized, custodial exchanges can potentially lose much or all of their customers' funds if they fail, are successfully hacked, or are internally compromised. Centralized exchange hacks have historically occurred numerous times, and at an accelerating rate [79], [80]. Non-custodial decentralized exchanges are possible and starting to appear, but currently tend to be less mature and usable, and more complex in operation.

Delegated account management in CBDCs: Much like central banks traditionally delegate the task of account management and identity checking to commercial banks, and like cryptocurrency miners have come to delegate this task implicitly to exchanges and other cryptocurrency holding and investment businesses, it may be natural for a CBDC to delegate this task similarly. This is one of the key roles of the Payment Interface Providers (PIPs) in the Bank of England's CBDC proposal, for example [10]. We believe this delegation approach is reasonable and in-line with historically-proven role separations, as it would avoid the need for the central bank to enter the unfamiliar business role of individual account management, and it would allow the Payment Interface Providers to innovate competitively in the way they provide these individual-facing services. The Digital Yuan also appears to be adopting this model, as discussed later in Section 11.2.

A possible downside of this delegation approach, however, is that many potential innovation opportunities may be left "on the table" and undeveloped, if the commercial Payment Interface Providers do not find it profitable or in their business interests to compete on the basis of certain aspects of account and identity management. Because banks generally avoid trying to "compete on security" or distinguish themselves from their competitors on grounds of security for fear of shaking customers' perceived trust in banks in general, for example, delegation of account management to commercial entities may in practice be ineffective at driving innovation in security-related areas. Similarly, the competitive pressure most high-tech businesses currently feel to collect and monetize data is likely to undermine competitive incentives for Payment Interface Providers to innovate in privacy-related areas. Thus, for some aspects of account and identity management especially including security and privacy, strong regulation and standards-setting – whether directed by a central bank or other government agencies or independent voluntary federations – may be necessary to ensure quality and innovation in these areas.

4.2 Approaches to digital identity verification

Beyond the issue of who manages individual accounts and identities, another question is how a customer's identity is verified for accuracy and legal compliance. There is a rich body of both academic literature and practice on the complex and challenging problem of digital identity verification. This complexity boils down to the fundamental problem that no known technology in our digital ecosystem – whether a device, algorithm, protocol, or service – can identify a particular "real human" with complete security. Instead, what we have is a plethora of mechanisms for associating digital accounts with imperfect *proxies* for individuals. Such proxies include information tokens such as cryptographic private keys, private information about the individual concerned (e.g., mother's maiden name, childhood pet, favorite film), hardware devices such as two-factor authentication (2FA) or multi-factor authentication (MFA) tokens [81], [82], traditional physical-world credentials such as ID cards and passports, other digital identity proxies such as E-mail addresses and phone numbers, biometric templates, or presence and interconnections in a social trust network. All of these identity proxies may work sometimes, but all have important costs, limitations, and critical failure modes. We briefly review a few of these approaches here and discuss their promise, trade-offs, and potential relevance to identity management for CBDCs.

In-person identity checking: Traditional banking has typically relied on in-person identity verification, requiring the customer to present a government-issued ID or passport at a branch office, often together with other evidence such as utility bills, in order to open an account. If banks or other financial institutions with local branches prove willing to play the role of PIPs for a CBDC, then they will be able to continue relying on in-person verification for CBDC accounts just as they do for traditional accounts. With both banks and their customers rapidly shifting towards mostly- or all-digital relationships, however, the days of in-person verification being the dominant approach may be numbered.

Online identity checking: To adapt to the demands of the digital age, numerous companies have started offering online *video identification* services.[6] These services typically ask customers to present themselves and one or more suitable forms of traditional ID over a video chat session. Using machine-learning and video face-recognition techniques [83], these services attempt to verify that the presented ID "looks" genuine and appears to match the face of the person holding it. These algorithms must also address challenges such as distinguishing between an actual, live person and a static image or video recording of one that an identity thief might be using to pose as the victim. When the algorithm cannot verify the ID with sufficient certainty, it may forward the video session to a human operator.

[6] Examples include IDnow, Fully-Verified, eID, and WebID.

This approach is attractive from a cost perspective as long as the algorithm can decide most cases automatically without requiring human involvement. The use of such algorithms presents many poorly-understood and underappreciated risks, however. Any complex algorithm such as this involving machine learning is almost certain to have a non-negligible false-positive rate, incorrectly accepting false ID cards as real, or accepting the wrong person holding it, or accepting a recorded image or algorithmically-generated *deep fake* [84], [85] of the victim supposedly presenting their ID. A determined and sophisticated fraudster is likely to be able to exploit even a small false-positive rate, through many automated attempts, while suffering little risk of getting caught or effectively punished – especially if they are launching their attack anonymously from a foreign country via a network proxy.

An important risk that tends to be underappreciated by the proponents of machine learning algorithms for identity verification is that the bad guys have artificial intelligence and machine learning algorithms too [86]. Whether in playing chess [87], Jeopardy [88], Go [89], [90], solving CAPTCHAs [91], [92] or creating deepfakes [84], [85], our consistent historical experience is that when we set up games between increasingly-sophisticated machine-learning attackers and increasingly-sophisticated machine-learning defenders, we find ourselves in an arms race in which the machine attacker sooner or later wins consistently over the real person. It may thus not be long before machine-learning identity checkers consistently accept sophisticated deepfakes while rejecting most real people, and an ever-larger percentage of online society – and perhaps even much of its commerce – is fake [93]–[95].

Weak digital identity proxies: Many non-financial applications in the online ecosystem rely on weaker identity proxies, such as E-mail addresses, phone numbers, IP addresses, or simply asking users to solve CAPTCHA puzzles [91], [96]. These weak identity proxies are rightfully not usually considered adequate for financial purposes, in part because they only rate-limit, rather than reliably deter, abuses such as the creation of false identities. All of these weak identity proxies can be faked or purchased by a determined and resourceful abuser at varying costs. E-mail addresses are practically free, for example, especially now that many E-mail account services, including Apple, allow their users to create effectively unlimited disposable E-mail pseudonyms for privacy and spam control.[7] CAPTCHAs can be broken via machine learning [91], [92] or social engineering [97], [98], or can be outsourced to countries with inexpensive labor [99].

Mobile phone numbers can be slightly stronger identity proxies, since many countries require customers to show ID when signing up for a calling plan, but anonymous prepaid plans still exist nevertheless. In any case, sophisticated hackers and identity thieves can exploit the weakly-protected SS7 signaling protocol to hijack a victim's phone number, together with the many digital services that use SMS challenges to reset account passwords [100], [101]. In summary, most of the identity proxies popular in the online ecosystem merely increase the cost of abuse somewhat without reliably

[7] See for example Hide My Email for Sign in with Apple, Temp Mail, Guerrilla Mail, FakeMail, ThrowAwayMail.

deterring it, and thus are inadequate for financial applications such as CBDCs.

Biometric identity: Biometrics are often proposed as a strong technology-based solution to digital identity challenges. India's Aadhaar program is both a showcase and testbed of this approach, having registered over a billion people via iris and fingerprints [102]–[104]. The use of biometrics for digital identity presents many challenges and risks that should not be underestimated, however. Biometrics are effectively "passwords you can't change" after something goes wrong [105], [106]. Biometric algorithms provide only approximate matches against biological characteristics that can change over time, be obscured, be destroyed accidentally or intentionally, and can be faked either physically or digitally in various ways [107], [108]. Even in the best circumstances, biometric matching algorithms inevitably exhibit both false-positive errors (incorrect acceptance of non-matches) and false-negative errors (incorrect rejection of true matches). Error rate estimates in the case of Aadhaar imply that hundreds of thousands of records could be duplicates [104]. Even the most precise and hence apparently-secure biometric, namely DNA, is already subvertible by an identical twin – and may soon be readily subvertible via increasingly-efficient synthesis of organoids [109], from stolen stem cells – or eventually, perhaps, the DNA residue we leave constantly in our physical environments.

The use of biometrics also presents profound privacy issues, especially when used for biometric *identity* as in India's Aadhaar program, as opposed to the biometric *authentication* features that have become commonplace in mobile personal devices. With biometric authentication, a device records one or at most a few biometric templates of authorized users, then later performs "one-to-one" or "one-to-a-few" matches against those stored templates when the user wishes to authenticate. The stored templates generally need not and should not ever leave the device, mitigating the most severe privacy concerns, and the common practice of disabling biometric authentication after a few failed attempts mitigates the risk of an attacker abusing the false-positive error rate through many brute-force attempts or other experimentation-based fakery.

In biometric *identity* systems like Aadhaar, in contrast, a registration service must not only record biometric templates for later authentication, but must also *compare* the templates against those of all the other – potentially billions of – already-registered individuals. Aadhaar requires this *deduplication* process in order to detect attempts by one person to register multiple identities and multiply the benefits they can obtain from the state's social "safety-net" services, for example. The need for users to be able to register on one device at one office and then authenticate to a different device at a different office, together with the need for detection of duplicates, fundamentally means that the biometric templates *must* be exported from the registering devices and be collected in a (typically centralized) database for later authentication and deduplication queries. This use of biometrics for identity thus raises much more serious security and privacy concerns [110], [111], as the biometric template database becomes an incredibly attractive target for hackers and foreign state adversaries alike. The need for a one-to-billions comparison in deduplication amplifies the effective false-positive rate correspondingly: a seemingly tiny Aadhaar-compliant false-positive rate of 0.01% for iris recognition actually means that each user might incorrectly match up to 100,000 others in the billion-user dataset. Finally, any single registration device that is hacked or under malicious control might be used to synthesize false biometric identities or impersonate real users. Most biometric templates previously thought to be irreversible have been proven otherwise [112], and cryptographic *secure sketch* algorithms have seen little adoption in part because they generally require the design of wholly new matching algorithms [113], [114].

In summary, while biometrics have legitimate uses when applied carefully in constrained applications such as mobile device authentication, we urge extreme caution in uses of biometrics for digital identity in security- and privacy-sensitive applications such as CBDCs.

Social trust networks: The basic human practice of "identifying" people – and deciding whether, how much, and for what to trust them – long predates modern government identity practices. Social or community trust remains an important identification factor in many parts of the world where government is weak or mistrusted, playing an important role in microfinance programs for example [115]. It should therefore be no surprise that social trust approaches to identity has long been of interest in the privacy-focused and often anti-government "cypherpunk" movement [116], [117], which first arose decades before but now overlaps heavily with the decentralized cryptocurrency community. The most well-known identity technology based on social trust is the "Web of Trust" concept introduced in the 1990s as part of the *Pretty Good Privacy* (PGP) encryption tool [118], [119]. Other social-trust identity technologies such as SPKI/SDSI [120], [121] were also proposed as public-key cryptography matured, but none proved usable enough to become widespread [122]. Web-based social media platforms such as Facebook and LinkedIn eventually popularized the social approach to identity [123], albeit with more emphasis on convenience and much less on privacy or strength of trust.

Identification based on social trust presents many practical issues. One principle challenge is that social identities tend to be easy and cheap to fake, especially for sophisticated automated algorithms, which has led to much of the social-identity ecosystem being essentially fraudulent [93]–[95]. While an important body of research has focused on algorithms for detecting or neutralizing false identities in social networks [124]–[127], it is not clear that actual trust networks have the properties needed for these algorithms to work [128], [129]. This is especially true when social media users are incentivized to inflate their "connectedness" or "follower counts" artificially through practices such as link farming [130], [131], and even to synthesize plausible content automatically [132]–[135]. For these and other reasons, social trust does not seem like a viable approach to identity for CBDCs – except perhaps in countries where existing government identification practices are weak or corrupt and *real-world* social trust may offer the only viable starting-point to identity.

Self-sovereign identity: One approach that has received significant attention recently, in the blockchain/cryptocurrency community especially, is the notion of *self-*

sovereign identity [136], [137]. In brief, the idea is to build a decentralized identity ecosystem allowing users to collect digital *attestations* of identity attributes from participating individuals or institutions, and then subsequently to reveal or *prove* those attributes selectively to other individuals or institutions demanding identification [138], [139]. Users might collect in their digital wallets attestations to attributes such as name, address, birthdate and other personal data, degrees and certificates earned, citizenships or memberships, etc. Institutions providing these attestations might include governments (for verifying government-issued identity attributes for example), academic institutions (for verifying grades and degrees earned), financial institutions (for verifying credit or other financial history), and so on. Ventures such as Sovrin are attempting to implement and build a self-sovereign identity ecosystem [140], [141], supported by some industry initiatives [142] and standardization efforts [143].

Self-sovereign identity is promising in that it allows many institutions beyond governments to assist with identity verification by issuing attestations, and because it in principle gives users control over how much and which specific attributes they're comfortable revealing to a particular relying party or to facilitate a particular transaction. The most commonly used illustration is that to enter a bar or nightclub, a user might need only to prove that they are above the legal drinking age, and not to reveal any other identity attributes. Self-sovereign identity is currently incomplete and immature, however, leaving many questions and concerns about how it will evolve in practice. For example, it remains unclear how many institutions (government or otherwise) will enter the business of providing attestations to users, how secure these attestations will be, or how widely they will be accepted. The privacy-enhancing "self-sovereign" principle could also be undermined if most relying parties demand that users reveal their real name and other personal information as a condition for doing business, as seems inevitable for financial use-cases. And if government-issued ID proves to be the most common or widely-trusted basis for users to obtain attestations to these personal attributes, then self-sovereign identity may prove to be mostly just a slightly-different technological mechanism for online identity-checking as discussed above. For these reasons, while self-sovereign identity approaches are worth watching, they currently appear to be neither mature enough, nor of sufficient value beyond that of standard identity-checking, to be a viable identity basis for CBDCs at the present time.

5 Digital Wallets

Digital wallets are the software applications through which users interact with a system of digital assets, such as currency. A digital wallet typically allows users to view their balance in one or more accounts, make payments, receive currency or digital assets from other users, and sometimes to trade assets or execute other financial transactions. The design and functionality of digital wallets are crucial not only for usability but also for security (users do not like to lose their money) and for privacy.

Popular money-transfer applications such as Venmo or Alipay may be viewed as digital wallets, and banking apps on mobile devices often include wallet-like functionality. These various applications, however, support user management of currency within existing financial infrastructure. They do not create or rely on fundamentally new representations of money such as CBDC. They do, however, provide a rough picture of the features and user experience that digital wallets for CBDCs would need to offer to see widespread adoption.

Software wallets for decentralized cryptocurrencies often resemble these money-transfer applications in terms of their user experience. Cryptocurrency wallets often differ in one essential respect, though: the cryptographic keys that authorize funds transfer may be stored *on the user's personal device itself* rather than being entrusted to a remote service. This property makes cryptocurrency wallets more cash-like, in principle eliminating the user's need to depend on and trust in a centralized financial provider. This dependence on the wallet device rather than a financial provider for key custody presents the similarly cash-like downside of exposing the user to the risk of unrecoverable financial loss if the wallet or device hosting it is compromised or lost. Motivated in part by the extreme security sensitivity of digital wallets, they also come in special-purpose hardware formats that function quite differently and take advantage of the hardware security practices discussed in Section 8.

In our discussion of digital wallets here, we assume for simplicity that the only digital asset the wallet manages is a CBDC, but note that digital wallets can in principle play a role in controlling a broad range of assets (cryptocurrency, digital tokens, smart contracts, digital cats [144], etc.). The capability of a digital wallet to hold many types of assets can itself present both significant opportunities and risks in its own right, as exemplified by the "ICO bubble" that was technologically enabled by Ethereum's ERC-20 standard [145], [146]. Thus, the question of whether a CBDC is typically held in and used via special-purpose wallets purpose-built to the CBDC, or generic wallets designed to manage a broader class of digital assets, presents important issues and questions to be considered carefully.

Digital wallets provide three main types of functionality: *user authentication*, *transaction authentication*, and a *user interface* for financial transactions. We explore each of these functionality areas in turn.

Figure fig. 5 shows the components and workflow of a digital wallet and can be referred to while reading this section.

5.1 User authentication

To ensure that access to digital wallet assets are limited to the authorized user or users, the wallet must *authenticate* a user. It must ensure that only the owner or a delegate acting on her behalf is able to operate the wallet or access the currency it controls.

Software wallets often use simple passwords or PINs for this purpose. With increasing reliance on mobile devices, though, it is common for wallets to authenticate users biometrically. Specifically, a user can gain access to her assets by possessing the particular device on which the wallet has been installed and successfully perform-

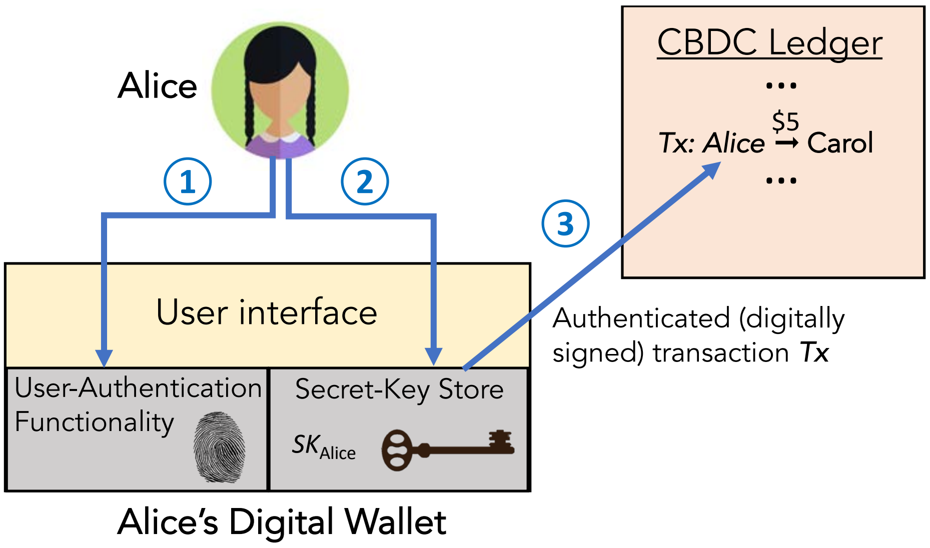


Figure 5: A digital wallet and example transaction workflow. In this example, a user Alice sends $5 to another user, Carol. Alice interacts with the wallet through its user interface. She first ① authenticates herself to the wallet. She then ② instructs the wallet to send $5 to Carol, whom she identifies by means of an account number or username. Her wallet ③ uses a secret key associated with Alice to digitally sign a transaction Tx specifying payment of the $5 and sends Tx to the CBDC system for inclusion on the CBDC ledger.
Note that this figure is strictly conceptual: To ensure privacy, users would be identified on the ledger by means of account numbers or pseudonyms, or for full anonymity might have their identities cryptographically concealed. (See section 6.1.) Additionally, Tx might be processed by a financial intermediary prior to transmission to the CBDC.

ing biometric authentication, e.g., fingerprint or face recognition.[8] Such biometric authentication is typically performed natively by mobile devices.

The goal of user authentication here overlaps with, but is slightly different than that of identity verification (see section 4.2), which generally aims to prove something about the the *real-world identity* of a user. Identity verification may be a precondition of wallet registration in some systems, but a wallet, once created, is in a sense agnostic to the user's identity: Securing the wallet requires only ensuring that the wallet is accessed by the original user (or a delegate).

In the loosest sense of the term, a "digital wallet" may be hosted by a *custody service*, meaning that it takes the form of an account with a service provider such as a financial institution, and need not be accessed through a particular device or instance of a software application. Custody services are used by many holders of cryptocurrency who wish to avoid the technical complexities – and potential security risks – of direct asset control.

[8] Such authentication schemes are sometimes called "two-factor" authentication: They involve a combination respectively of "something-you-have" and "something-you-know" factors [147].

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

5.2 Transaction authentication

Once authenticated, a user can cause her wallet to perform transactions on currency in her account(s), e.g., sending money to another person. Her wallet must then create and send a transaction message T to the CBDC system for processing—for example, for inclusion on the CBDC's digital ledger.

As a basic security requirement, the CBDC must ensure that transactions are issued authentically on behalf of the users upon whose assets they operate. If Alice issues a transaction T paying \$5 to Bob, the system must ensure that Alice herself authorized T.

In a typical online banking system, the processes of user authentication and transaction authentication are merged. If Alice logs into Piggy Bank, Ltd. (i.e., performs user authentication) and sends \$5 to Bob, the bank can identify the transaction as valid because it has already authenticated Alice. The setting here is simple: The entity that authenticates the user is identical with the one that manages the money she operates on.

A CBDC could operate in this way, requiring users to log onto a web platform to perform transactions. Alternatively, in a two-layer CBDC architecture in which financial intermediaries interface with users, an intermediary can submit transactions on behalf of users it has authenticated. Approaches of this kind where the CBDC operator and/or intermediaries vouch for the authenticity of users' transactions has the benefit of conceptual and design simplicity, but also has notable drawbacks.

The main drawback is the existence of a *single points of compromise* that is large and attractive to profit-motivated hackers. An adversary that compromises the infrastructure of any single financial intermediary can forge transactions from any of its users. Similarly, a financial institution could unilaterally freeze the funds of a user. Should the CBDC be able to confirm transactions unilaterally, then it would constitute a single point of compromise for the entire system.

Central to the design of cryptocurrencies is an alternative form of transaction authentication in which transactions are *digitally signed* in a cryptographic sense by the owners of the currency they transmit. In account-based cryptocurrencies (e.g., Ethereum), each account has an associated public key for verifying the validity of transactions signed by the account holder using a corresponding private key.[9] Only validly signed transactions are included on the blockchain / ledger.

If users manage their own private keys, then the use of digital signatures vests account control directly in the users' hands. Even if a financial intermediary is compromised, because it does not hold users' private keys, it cannot sign on their behalf, and thus cannot forge transactions from user accounts. Hybrid models are also possible (see, e.g., [148]) in which both a financial intermediary *and* a user must sign a transaction in order to authenticate it, helping ensure that compromise of either one does not enable transaction forgery.

In such a digital-signature based CBDC, digital wallets perform transaction authentication by digitally signing the transactions users initiate. They must also play

[9] See, e.g., the entry on Digital Signatures, for a primer on digital signatures and public-key cryptography.

the critical function of storing users' private keys for them. Secure and reliable storage of cryptographic keys has proven a serious challenge in cryptocurrencies, holding important lessons for similar CBDC designs. This challenge is often referred to as the problem of *key management*.

Key management: One statistic neatly sums up the intractability of the key management problem in practice: An estimated 4,000,000 Bitcoin, worth tens of billions of dollars at the time of writing, have disappeared forever because of lost private keys [149]. Key management is so daunting to users that many store their cryptocurrency with exchanges (custody services), such as Coinbase, paradoxically recentralizing systems whose main selling point is their decentralization.[10]

In an ideal world, a digital wallet might take the form of an app on a mobile device that secures a users' private keys effectively and makes them available for signing whenever the user needs them. But what happens if a user loses or breaks her phone? Or she wants to initiate a transaction from a different device? Or her phone is compromised by malicious software?

There is a fundamental tension between *security*, i.e., preventing theft of private keys, and *availability*, i.e., ensuring that keys aren't lost. Perfect security for a private key is easy: Just delete all copies of the key. So is perfect availability: Post the private key on a blockchain. Obviously neither of these solutions is useful. The challenge in building a workable system is striking a good balance between security and availability.

The cryptocurrency ecosystem has evolved various mechanisms in the quest for a good key management solution, with mixed success:

- *Secure hardware:* Most mobile devices contain what are often called *secure elements*, designed to store keys so that they can only be accessed upon successful user authentication.[11] A range of special purpose *hardware wallets* for cryptocurrency, usually in the form of USB devices, serve a similar purpose. Hardware wallets in principle reduce the risk of funds loss due to remote compromise (e.g., hacking) of the device holding the wallet, but they do not by themselves mitigate the risk of funds loss through the unavailability (loss or destruction) of the wallet device itself. The use of trusted hardware for wallets is further discussed in section 8.4.

- *Mnemonic seeds:* When a user initializes a software or hardware cryptocurrency wallet, she is typically presented with a list of words, known as a *mnemonic seed*, that encodes her private keys for the wallet. Users are encouraged to write down their mnemonic seeds and store them safely, e.g., in a safe deposit box, to enable recovery of lost private keys. This mechanism helps the user guard against loss of funds through the loss or destruction of the primary device containing the

[10] Coinbase alone reportedly holds some 10% of all Bitcoin in circulation [150].

[11] The iPhone has shown that this approach can be quite effective against even powerful adversaries, as shown for example by the difficulty that U.S. law enforcement authorities have encountered in recovering encrypted iPhone data [151].

(hardware or software) wallet, at the cost of introducing a new risk – namely that of the wrong person obtaining the mnemonic seed.

- *Threshold signing / multisig:* It is possible to split a private key into a set of n *shares*, as discussed in section 3.2, so that any k out of n shares (for $k \leq n$) can be used to reconstruct the private key. Advanced cryptographic protocols, e.g., [152], [153] enable generation of a signature from shares without explicit reconstruction. With this kind of setup, it is possible for n different entities (people or organizations) to exert joint control over a digital asset, with any k having signing authority.

  A popular feature of cryptocurrency wallets today is *multisig* (multiple signatures) transactions. Multisig transactions are similar in spirit to threshold signing and have the same goal of joint control. They require use of k-out-of-n distinct signing keys to validate a transaction, though, instead of shares. Both threshold signing and multisig transactions are different embodiments of the threshold trust approach to decentralization discussed earlier in Section 3.2.

  Multisig transactions are technically simpler to implement, because they do not require the signing keys to be generated cooperatively, or even to use the same cryptographic algorithm. They exhibit a subtle privacy-versus-transparency trade-off, however: a threshold signature does not reveal *which* particular k out of the n share-holders signed the transaction, whereas with multisig transactions the set of k signers authorizing the transaction is clearly visible on the ledger. Threshold signing may be preferable if stronger privacy or *group anonymity* of the signers is desired. Multisig may be preferable if it is considered important to make each signer individually accountable for the transactions they sign, and to deter attacks in which a threshold of k signers might secretly collude to authorize a transaction improperly.

  Both threshold signing and multisig mechanisms achieve a balance between security and availability that can be parameterized by varying k and n and various other enhancements [154], [155]. Its limitations, though, including a need for multiple participating users or devices, make it less readily suitable for the wallets of individual users. Threshold or multisig wallets might in principle enable individuals to recover their funds with the cooperation of some threshold of trusted friends – analogous to the "trusted friends" account recovery path that Facebook already supports – but such social recovery mechanisms have not yet seen widespread support in digital wallets.

Flexible key management in CBDCs: Key management is especially challenging in fully decentralized cryptocurrencies such as Bitcoin and Ethereum because there is no authority to intervene to remedy failures such as key loss. Erroneous transactions are irreversible; countless users have suffered losses as a result [50]. In CBDCs, however—or indeed, any permissioned currency system—more flexible key management regimes are possible.

One option is to empower the operator of the CBDC or some other authority to *revoke* the public key (and thus corresponding private key) associated with an account, and *authorize new keys*. Such a capability is analogous to the ability to rectify errors in the ledger, as discussed in section 10.4. In a digital-signature-based system, it will be equally essential. Loss and theft of keys is inevitable. A practically workable system must include mechanisms to remedy these eventualities.

This general key-registration capability amounts to near-total control of CBDC funds. By changing keys, it is possible to transfer control of accounts arbitrarily. Consequently, a key registration system would itself represent a critical point of system compromise. One way to mitigate the risk is to vest this capability in a *set* of authorities, of which an authorized subset must cooperate to make key registration changes. Cryptographic tools such as multisig or threshold signing can serve as a technical foundation for such joint control, another application of threshold trust.

A second and perhaps complementary risk mitigation approach relies on notification and time delays before transactions are executed or become irrevocable. Bitcoin vaults [154], for example, impose a time delay on moving funds out of "cold storage", giving the owner an opportunity to notice an unauthorized transaction and cancel it with a recovery key. Paralysis proofs [155] enable recovery of funds if too many signers in a threshold or multisig account become unavailable.

A key question that a CBDC design must answer is whether – and for how long – a transaction should be potentially reversible in some way if it is discovered and adequately proven to have been improper. The cash-like, irrevocable finality of cryptocurrency transfers may be attractive for small payments but undesirable for larger, high-stakes transactions in which certainty is more important than speed.

The policies governing conditions under which authorities can alter account access can be largely independent of the technical mechanisms for key registration. These policies can be designed to comply with legal frameworks for asset recovery and transfer, as discussed in section 10, and can involve a blend of automated tools as well as interventions dictated by conventional legal and regulatory institutions.

5.3 User interfaces

Just as important as the capabilities of a digital wallet is *how it presents these capabilities* to CBDC users. User interface design profoundly impacts not only the acceptance of a system by users, but also system security.

The history of Internet browsers abounds with cautionary tales. Hackers and researchers have shown repeatedly how misguided graphical design choices have caused users to misinterpret browser content. Users have as a result been vulnerable to deceptive attacks that cause them to navigate to unintended, malicious sites or click on malicious content even in the face of warnings [156].

USB-type hardware wallets for cryptocurrencies also underscore these challenges. Many include features to prevent malicious software from subverting digital wallets by displaying a valid-seeming cryptocurrency address (account number) to a user but instead generate transactions that send money to attackers. These devices include built-in displays that show the true destination address for a transaction. User studies, however, show that users derive only limited benefit from these cues [157].

Designers of CBDC wallets will have to contend with similar challenges. Happily, where wallets are managed by financial intermediaries (or a consumer-oriented CBDC platform), it is possible to leverage the array of sophisticated fraud-control mechanisms already prevalent in consumer payment platforms [158], and similarly to benefit from user interface design experience. These fraud-control mechanisms typically depend on some form of manual and/or automatic surveillance of transactions, however, exacerbating the privacy challenges discussed below in Section 6.

Some CBDC proposals, and CBDC-like systems such as Libra, envisage the possibility of sovereign control of wallets by users. Unless the CBDC takes on the task of fraud detection and remediation of transaction errors currently assumed by commercial banks, sovereign wallets will need to adhere to strict security requirements like those in cryptocurrency platforms, and fraud and error will be hard to detect or remediate.

6 Privacy and Transparency

In permissionless and decentralized cryptocurrencies like Bitcoin [17], regulatory oversight and compliance are generally an explicit non-goal: such systems are specifically designed *not* to be controlled by a state, a bank or any other central authority. In contrast, a CBDC likely needs to support mechanisms to enforce regulatory and compliance rules, as states want to detect and prevent criminal activities and ensure financial stability [10], [159].

At one extreme, we could imagine a CBDC in which transactions were made using real-world identities and were fully visible to an authority like the central bank or law enforcement in the clear. Oversight of compliance rules in such a CBDC, in terms of the detection and prosecution of violations, would be easy. Even if this oversight were done with good intentions, however, it would lay the foundations for large-scale abuse and human rights violations, enabling the government (and potentially private operators like banks) to track individuals with an unprecedented level of granularity.

At the other extreme, a CBDC that offers *full* privacy may not reveal any information about transactions to the operator(s)—a digital cash of sorts. This in turn would facilitate large-scale money laundering and make it near-impossible for law enforcement to track financial flows. Hence, we expect that most CBDCs will prefer to operate in a middle ground that offers some privacy protections to consumers, while also offering some visibility to auditors and law enforcement.

How to choose such a middle ground will reflect differences in individual or cultural values, likely related to the factors that make some individuals and some societies still prefer the relative anonymity of physical cash for everyday commerce, while others embrace the convenience of credit cards and willingly entrust their personal details and transaction histories to the card issuers. For this reason, it is critical for the identity-management approach a CBDC adopts to fit the cultural values and expectations of its intended user population, and these values may differ from one

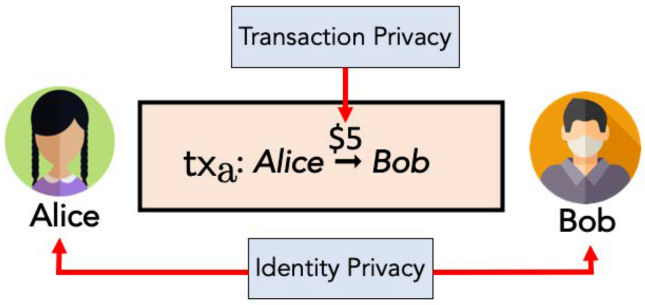


Figure 6: Two classes of privacy concerns arise: identity privacy, which concerns the participants in a transaction, and transaction privacy, which concerns the amount of the transaction (or the details of the contract in a smart contract).

country to another.

In addition to cultural considerations, choosing an appropriate middle ground will also depend on the technical limitations of existing tools. Indeed, there is a fundamental tension between transparency and privacy. On the one hand, transparency is essential to a digital currency because validators must be able to ascertain the correctness of transactions and their compliance with financial regulations. On the other hand, the more information we reveal to validators, the easier it is for those validators (and sometimes even outside observers) to learn information about individual transactions and the people executing them. This tension between privacy and transparency does not imply a "zero-sum" trade-off between the two, however: many privacy-enhancing technologies exist, outlined below, that can achieve privacy *together with* transparency in various forms.

We consider two types of privacy that a digital currency should consider (Figure 6). The first is identity privacy (Section 6.1), which describes the (in)ability to link transactions or activity to the sender or recipient of a given transaction. For example, we may wish to prevent an observer from learning that Alice sent money on Tuesday. The second is transaction privacy (Section 6.2), which describes the (in)ability to learn the nature of a given transaction. For example, we may wish to prevent an observer from learning that Alice paid $40 to the pharmacy. These categories of privacy require different tools, so we will separate them in the following discussion.

The trade-offs associated with identity and transaction privacy also have implications for decentralization of a CBDC (Section 6.3) and compliance (Section 6.4). Hence, we conclude the section by discussing some of these trade-offs.

6.1 Identity privacy

At the most basic level, a payment system can attempt to provide anonymity for its users by identifying them using *pseudonyms* rather than persistent identifiers. Such a system might label transactions performed by Alice with a numerical user identifier (e.g., 1234) instead of her real-world identity ("Alice"). This offers a very basic form of anonymity, often called *pseudonymity*, but pseudonymity is fragile. If Alice, for example, reveals her name to a merchant in the course of a transaction, the merchant learns that 1234 = "Alice". If the merchant's customer database is breached, then Alice's pseudonym could leak more broadly. It improves anonymity if Alice uses different pseudonyms to identify herself to different merchants, or more generally if she goes by a different pseudonym with every user with whom she transacts. In Bitcoin, which is perhaps the most prominent example of a pseudonymous currency deployed today, a pseudonym, also called an *address*, is the hash of the public key for a digital signature scheme. This means that it does not inherently reveal any information about the user to whom it is tied, and that two pseudonyms cannot inherently be linked together.

In practice, however, pseudonyms can leak information about the participants in a transaction. Indeed, there exist blockchain analytics companies whose entire business model is centered around de-anonymizing users (e.g., Chainalysis [160]). In Bitcoin, it is possible to *cluster* pseudonyms together according to common transaction patterns [161]–[164]. For example, an exchange may combine the addresses associated with its different users in ways that make it possible to identify that they are all part of the same exchange. An entity storing the ledger of transactions can even perform this clustering retrospectively as they discover new patterns. If they can further *tag* addresses by performing their own transactions within the network (e.g., depositing coins into and withdrawing coins from an account they create at an exchange), they can identify the real-world owners of not only the addresses they directly interact with but also the broader clusters that their tagged addresses are part of [163]. Even if we consider a completely passive attacker who does not perform their own transactions, lists of tagged Bitcoin addresses are readily available online (e.g., at `https://www.walletexplorer.com/`). These attacks are best suited to de-anonymizing services like exchanges rather than individuals, but within most cryptocurrencies these exchanges represent a large part of the ecosystem, and a chokepoint in terms of how users can get their money into and out of it.

This simple technique of using pseudonyms has been adopted by most other cryptocurrencies, meaning the de-anonymization attack described above works equally well for them. So-called "privacy coins" such as Zcash and Monero, however, have different ways of forming transactions that use more advanced cryptographic techniques to protect anonymity. Even within these cryptocurrencies though, it is still possible to identify patterns of usage and de-anonymize users and services accordingly [165]–[167]. In Zcash, for example, the main privacy feature is optional, and the majority of transactions do not take advantage of it.

The previous attacks rely solely on analyzing transaction patterns within the ledger itself. However, pseudonymous identifiers can also be used to link accounts to users by exploiting communication network infrastructure; i.e., the Internet. When a user initiates a transaction involving digital currency, they must send a message over the Internet to communicate this transaction to the CBDC validators. For example, the user might send the transaction to their bank, which may act as a validator and also forward the transaction to the remaining validators. A sophisticated attacker with access to Internet infrastructure (e.g., a nation-state or even a large Internet service provider) may be able to observe this message and identify its point of origination, i.e., IP address, even if the user encrypts their message. IP addresses can sometimes be linked to people, or at least to a person's hardware. If this same entity is also able to view the ledger, they may be able to link the IP address to an account. This again represents an attack on the anonymity of users, since an entity other than the user's bank can link financial accounts to a user's IP address.

Solutions: Prior experience suggests two main approaches for managing this class of attacks. The first approach is to eliminate pseudonymous identifiers. Cryptographic techniques can ensure that any two transactions by the same user cannot be linked together via the transaction contents, but can still be validated [168]. Although these techniques increase the complexity of implementation, they make it much harder for an adversary to link a user to their transactions.

Even without pseudonyms, it may still be able to link *individual* transactions to an IP address, using the previously described techniques. A common approach for addressing this concern is to alter the network relay dynamics. For example, instead of sending the transaction directly to a validator, the user may route her transaction through proxies using third-party services such as Tor [169]. However, this solution is not scalable to millions of people, nor is it usable by the average user due to high technical complexity. Additionally, it requires users to trust a third-party service, which may itself be vulnerable to attacks. Indeed, state-level adversaries have been known to break the anonymity of proxy services like Tor successfully [170], [171].

In general, there are no cryptocurrencies or privacy features today that make it impossible for attackers to learn information about the identity of senders and recipients in the network. This suggests that making the ledger of a CBDC globally visible would be undesirable, and that similarly it is not clear how to prevent validators (i.e., the organizations maintaining the ledger) from learning information. This further suggests that achieving similar anonymity guarantees to physical cash, at the same time as achieving forms of regulatory oversight (as we discuss in Section 6.4), is an open and challenging problem.

Active probing attacker: An average client does not typically meet the storage requirements needed to store something like the ledger of a cryptocurrency: e.g., the Bitcoin blockchain is currently on the order of hundreds of gigabytes. In a CBDC, clients may be unlikely to have direct access to the ledger anyway if it is centralized or permissioned, as discussed earlier in Section 3.3. As discussed above, this means that clients are likely to submit their transactions to the ledger through a validator, who will then be able to identify that client as the sender in the transaction.

Similarly, clients who receive a transaction may want to check with a validator if it is in the ledger or not. In Bitcoin, this is equivalent to a *lightweight* client, who stores only the headers of blocks, performing this check with a *full node*. Rather than completely trusting the full node to give the right answer, the client asks them for a proof that the transaction is included in a block, which the client can verify against the block header. Clients may be more willing to trust validators in a CBDC (although they should not have to), but the privacy issue remains that asking about the transaction directly is a clear signal that the client was a recipient in that transaction: there is no reason why they would know about or be interested in it otherwise.

Furthermore, some version of this attack could be carried out by a remote attacker who just observes the network connection between the client and the validator [172]. If the data is not encrypted in transit, for example, then they have the exact same information as the validator. Even if the data is encrypted, a remote attacker can learn information – for example, whether or not the client was interested in a transaction – based on the timing of its network traffic. It is thus important to protect these network connections by encrypting all traffic, and for all participants to use constant-time algorithms to avoid revealing information via timing channels.

In addition to the network-level anonymization techniques discussed above, it may be possible to run a type of *private set intersection* or *oblivious transfer* protocol instead, so that the client learns only whether or not the transaction is included and the validator learns nothing. This is an open research area, however, and furthermore one that typically involves the usage of advanced cryptographic techniques. Some approaches have instead relied on trusted hardware, as discussed in Section 8.

A more concrete approach is to design the ledger so that a client does not require active privacy-sensitive communication with anyone in order to check if a transaction is included in the ledger. In the SkipChain structure [173], [174], for example, all committed blocks are collectively signed by a rotating committee of signing trustees, whose evolution is similarly validated by collectively-signed "forward links." This structure enables any client to provide any other client with a direct cryptographic proof of a transaction's commitment to the ledger, without needing to make privacy-sensitive queries to full nodes or other third parties. While there are complexity costs and security trade-offs to be considered in this approach, the Libra blockchain has adopted it [175] and some variant may be appropriate for CBDCs more broadly.

6.2 Transaction privacy

Beyond identity, there are other aspects of blockchain computations that users might wish to keep private. First, they may wish to mask the *input data*. In a digital currency, this might correspond to transaction amounts. In a smart contract platform, this could include other metadata, such as private customer data. Second, users may wish to mask the *nature* of the computation being executed by a smart contract. As one example, a group of participants may want to compute a private algorithm for predicting the viability of a loan, without revealing the structure of that algorithm to other CBDC participants. These two challenges of *data privacy* and *program privacy*, respectively, are generally addressed by different technical approaches in practice.

Data privacy: The simplest form of data privacy is hiding the amount of a transaction. This typically involves the use of more advanced cryptographic techniques, such as encryption or commitments. Here, however, it is crucial to keep in mind the balance between privacy and verifiability: the amount that a user is sending can be hidden using encryption, but it is equally important that users cannot send more money than they actually possess. Validators must thus be able to check this property, at an absolute minimum, even without knowing the amount themselves. This is typically achieved using advanced cryptographic primitives known as *zero-knowledge proofs*. Such proofs allow the sender to prove that the amount they are sending does not exceed their current balance without revealing the amount or their balance.

To reap the benefits of zero-knowledge proofs, participants must be able to generate and validate transactions containing encrypted data. This design choice has trade-offs in terms of transaction efficiency. Zero-knowledge proofs typically take longer to generate and verify than a regular unencrypted transaction (on the order of seconds). While such a delay is negligible in blockchains with long confirmation times (e.g., Zcash), it could be a concern in a CBDC. A more significant concern is that validators likely want more than just this basic level of verifiability, in order to ensure compliance with financial regulations. This is a challenging problem that we discuss further in Section 6.4.

Another limitation of zero-knowledge proofs is that they can only prove facts about confidential data held *off* the ledger, but cannot ensure that the data is actually retained or disclosed when policy requires, as determined by a regulatory process or a smart contract for example. If policy allows transaction amounts and participant identities to be *normally* hidden but requires them to be disclosed if a relevant account comes under investigation, for example, then zero-knowledge proofs are inadequate by themselves because they can prove that the transaction amounts and identities are valid and *exist* but cannot ensure their retention and disclosure at investigation time. Some experimental ledger designs allow confidential data to be stored *on-chain* and collectively entrusted to the blockchain validators, which cooperate to control and record accesses, and to decrypt or transfer the confidential data when authorized [176], [177]. This design ensures that the ledger itself can retain and enforce selective disclosure or transfer of confidential transaction information on demand, at the cost of requiring users to place slightly higher privacy trust in the collective set of ledger validators.

Program privacy: Generalizing these ideas to smart contracts is challenging for two reasons. First, the inputs to a smart contract can be much more complex than inputs to a regular transaction. Second, the operations executed in smart contracts are also more complex. These issues make it difficult to extend zero-knowledge proof techniques for verifying encrypted transactions to arbitrary smart contracts. A common alternative is using *secure multiparty computation* (SMC). SMC is a class of techniques allowing multiple parties to compute a function of encrypted data without learning the function inputs. Although SMC is generally computationally inefficient, recent efforts have modified industrial blockchains like Hyperledger Fabric to support a curated class of SMC smart contracts optimized for performance, e.g., running private auctions [178].

Another possibility is for a subset of participants to perform the computation locally and report only a commitment to its new state to the ledger. Again, this raises the question of verifiability: how can validators be sure these *compute nodes* are not lying? One approach is to provide strong disincentives for dishonest behavior, by allowing other participants to challenge the results of a computation and have the network punish compute nodes who are caught lying [179]. Another is to have compute nodes run the computation inside of a trusted execution environment (TEE), or *enclave*, which guarantees that their reported results are correct and that all data inside the enclave is kept private [180]. Finally, compute nodes can provide a succinct zero-knowledge proof that they executed the computation correctly [181]. All of these approaches have trade-offs in terms of their functionality, efficiency, and required levels of trust (for example, in the compute nodes or the TEE manufacturer) that must be taken into account when considering their use in a deployed application like a CBDC.

6.3 Privacy and decentralization

Considerations of centralization versus decentralization, introduced earlier in Section 3 from a ledger infrastructure security and trust perspective, create similarly complex privacy considerations and tradeoffs that we briefly outline here.

One of the central questions is what the CBDC's threat model should be for privacy purposes: i.e., *from whom* should the CBDC protect sensitive identity and/or transaction data? If it is acceptable from a social, legal, and risk perspective to require users to place complete trust in the central bank to protect their privacy, for example, then a fully centralized design may be both simplest and most effective at protecting clients *from each other*. In such a design, however, a single bulk data breach of just one replica of the permissioned ledger or an associated sensitive database can expose the identities and financial histories of millions of users at once, as the Equifax breach affecting nearly half the US adult population amply demonstrated [182].

Many privacy and cryptocurrency advocates, therefore, favor more decentralized approaches to privacy protection, which a CBDC design should consider. The three main forms of decentralization introduced earlier in Section 3.2 – role separation, trust dispersal, and threshold trust – are all potentially useful to varying degrees in protecting user privacy against the compromise of any one server or authority.

Role separation: The Bank of England's proposed delegation of account and identity management to a Payment Interface Provider (PIP) [10], for example, makes it simple to give users a limited form of *accountable anonymity* [183] for identity privacy. If the central bank normally treats accounts as pseudonymous public keys, and only the PIPs verify and record the associated identity information, then individuals are at least pseudonymous with respect to the central bank and the ledger transactions it processes – provided, of course, the PIP adequately protects this identity information. The PIP can disclose the identity associated with an account under suspicion to the central bank or an independent investigator as appropriate, however, to address regulatory compliance and anti-money laundering considerations. In cultures where banking customers are more inclined to trust private companies than governments with their personal information, this form of role separation for privacy may be reasonable and useful, however limited.

Trust dispersal: The delegation of identity management to *multiple* commercial PIPs can similarly benefit privacy in terms of trust dispersal: the breach of a single PIP in principle affects only that PIP's customers, and not the CBDC's entire user population. While trust dispersal reduces the aggregate amount of trust placed in any one PIP, it does not necessarily do anything to improve the situation of – or perhaps to placate – each of those unlucky customers whose PIP has suffered a data breach. Further, the real possibility that the PIP service market could become dominated by a few large players – as in the case of credit rating services like Equifax in the US [182] – limits the privacy protection we can expect from decentralization via role separation and/or trust dispersal alone. Experience indicates that almost any centralized database of sensitive personal information inevitably becomes a prime target for hackers, identity thieves, industrial spies, or foreign adversaries. Therefore, while the two-level separation between central bank and multiple PIPs is a promising starting point already being embraced by multiple CBDC projects, including the digital yuan (Section 11.2) and the e-krona [5], we recommend that it be viewed merely as a starting point and not as a complete decentralized privacy solution.

Threshold trust: Analogous to the way that Byzantine state machine replication (SMR) protects the integrity of a ledger against any one compromised server (§3.3), *threshold cryptography* techniques such as Shamir secret sharing [184] protects the *privacy* of confidential information from any one compromised server holding a *share* of it. A threshold number of the parties holding shares must work together to decrypt or do anything with the threshold-encrypted data. With 3-of-5 secret sharing, for example, there are five independent trustees each holding one share, at least three of which must work together to decrypt the data. Threshold signing, discussed earlier in Section 5.2, is just one of numerous applications of threshold cryptography. Other applications include secure decentralized data deletion [185], or decentralized management of *on-chain secrets* entrusted to a ledger [176], [177]. Proper use of threshold cryptography could in principle address the tension between user identity privacy and the investigatory needs of law enforcement, as discussed below in Section 6.4.

To counter a common misunderstanding, a complete data breach in one of the five trustees in this example does not cause one-fifth of the data to be leaked. Instead, correctly-implemented threshold cryptography ensures that complete data breaches in one or even two of the trustees results in *no* data leakage. Only under a "full-threshold" breach, of three trustees simultaneously in this example, is any data leaked at all. At that point, *all* data may be leaked in bulk. Thus, in such systems it is critical that thresholds be chosen carefully to minimize the possibility of a full-threshold breach, while balancing this risk against data availability risks due to too many trustees failing or being affected simultaneously by network outages for example.

It is worth pointing out the cautionary note that a large number of projects and technologies claim to "use blockchain" to "secure" sensitive private data, but do not actually implement decentralized privacy protection. In particular, most blockchain-based systems designed to manage personal information actually entrust the *privacy* of the data either to a mobile device, which may be lost or stolen; to a cloud service, which is a central authority that may suffer a data breach; or to a hardware security module (HSM), which may have bugs or side-channel leaks. The "blockchain" in such designs typically only *records* uses of the private data that the centralized data trustee device *claims* to have performed. If the trustee device (mobile device, cloud service, or HSM) is compromised, however, it can readily leak the private data to an adversary without recording this fact on the blockchain. Referring back to the C-I-A triad (§3.1), even a blockchain that perfectly protects its integrity and availability cannot protect the *confidentiality* of a user's data if that data is held off-chain by a centralized trustee that might leak it without even recording that fact on the ledger.

6.4 Privacy and compliance

Today, most countries have compliance rules whose goal is to protect the economy against malicious activities like money laundering or tax evasion. (Specifics, such as the United States requirement that cash transactions exceeding 10,000 USD must be reported to the government, are discussed in Section 10.2.) If a central bank were to deploy a CBDC, most likely it would want to have mechanisms in place that allow it to detect or prevent large transactions that exceed such limits (or series of small transactions that exceed the limit combined). That is, the CBDC implementation should the support the enforcement of *pre-existing* compliance rules. We discuss anti-money-laundering (AML) laws in more detail in Section 10.2.

Additionally, the introduction of a CBDC might create the need to introduce and enforce *new* compliance rules. One particular threat is the implications of a CBDC for financial stability. During a financial crisis people might get worried about a bank run and want to move bank deposits into CBDC (which would be free of such risks by definition). This could, in turn, make the risk of bank run seem even more probable and create a vicious cycle. The potentially resulting massive shifting of funds might threaten the stability of the entire financial system. This threat is brought up in the CBDC discussion paper from the Bank of England [10] and also mentioned in the working paper of the European Central Bank (ECB) [159]. As a potential solution, both documents suggest limits of how much CBDC any individual can hold at a given time. Such a holding limit is an example of a new compliance rule that might be needed, if a CBDC were to be introduced.

Challenges: Recent research efforts have explored the question of how to combine anonymous payments with compliance and oversight. In the context of token-based digital currencies, Camenisch et al. designed a solution that allows users to make payments such that they remain anonymous but the bank who issued the coins can enforce simple compliance policies such as per-user payment limits [186]. The main problem with such solutions is that they do not provide recipient anonymity or hide payment amounts. In the context of ledger-based digital currencies, Garman et al. studied how similar compliance policies could be realized in payment systems like Zcash that provide strong privacy protection [187]. The drawback of such schemes is that they require expensive zero-knowledge proofs (SNARKs) and a trusted setup phase. Wüst et al. showed how simple payment limits can be combined with more lightweight anonymous payments that leverage cryptographic commitments [188]. One problem of such solutions is that transaction linking is still possible. Additionally, all above mentioned schemes require an enrollment phase where the identity of the user is verified by a trusted authority which may further complicate the adoption of a CBDC.

Recent work on privacy-preserving surveillance [189]–[194] may suggest CBDC designs that could provide strong privacy protection for transaction amounts and identities while ensuring not just proactive compliance (e.g., conformance with account balance or payment limits) but also retroactive compliance like retention and disclosure of confidential information in an investigation. An example privacy-preserving investigation process might require a "warrant" targeting a transaction or account of interest, even if the target's identity is as-yet unknown [190], [192]. Such a warrant, authorized by an independent judge and tallied in aggregate accountability mechanisms [193], [194], might authorize the transfer of encrypted on-chain secrets [176], [177] containing transaction amounts, identities, and other information to an investigator.

In general, the question of how to achieve payment privacy and enforcement of compliance rules with good performance, acceptable trust assumptions, and simple adoption is challenging. While the technological building blocks for such designs already exist, building them into operational, secure and privacy-preserving systems thus far remains an open challenge.

7 Smart Contracts

Many state-of-the-art digital assets feature a smart contract programming language. This is a way that independent third-party independent developers can extend the digital asset with new functionality. It is not necessary for a CBDC to provide smart contracts in order to fulfill its primary role as a digital currency, and some CBDCs (including the digital yuan, for example) are unlikely to do so. However, smart contracts can be an important way that a CBDC fosters innovation from other entities such as commercial banks and fintech providers.

There is a broad design space of smart contract languages for a CBDC to consider, and potentially many pitfalls. Notably, there have been many expensive losses in cryptocurrencies like Ethereum due to smart contract coding errors (known as "bugs") that have led to either to accidental losses or else made them vulnerable to deliberate attacks from opportunistic hackers. If a CBDC incorporates smart contract functionalities, then it will be important to consider safety and security when designing these.

Background: Smart contracts arise from the need to extend the spending limits and policies provided by digital assets, some of which are described in Section 5. For example, to help secure high-value accounts, it is considered a best practice to attach restrictions such as `"Funds from account A may only spent with authorization from any two out of Alice, Bob, and Carol"` or `"Only $1000 can be spent per day"`, as well as many other possible variations or combinations. Smart contracts provide a flexible way for users to define and customize such policies.

More generally, smart contracts can behave like trusted third parties, realized using software. Smart contracts can include conditional statements, for example, in very high level pseudocode,

```
Alice may choose before time T whether to receive either $10 or
10 TOK from Bob
```

or

```
"If the price of TOK tokens exceeds P, then transfer $X from Alice
to Bob".
```

These policies are codified into machine-readable programs that can be executed by the system operators. Alice’s choice in the above example, would be expressed through a digital signature, which is then checked by system operator according to the rules of the program.

In many applications, including the above examples, the correspondence with traditional legal contracts is fairly clear: The program code is available on-chain for both parties to see, hence it reflects the mutual agreement between them. The parties to the contract use digital signatures to express their intent to be bound by the contract and their acceptance of its terms. The contract may explicitly define the consideration to (automatically) transferred upon fulfilling the contract. Other applications of smart contracts do not as easily fit this pattern. For example, some of the most popular applications have included auctions, lottery games, and exchange services. Once funds are deposited into an account associated with a smart contract program, such funds are subject to those programmatic rules.

Smart contracts have emerged as an important tool for innovation in today’s digital assets. Many of the most widely used applications, such as auctions exchanges, as well as safety features like multi-signature wallets, have been written by independent developer teams separate from the core developers responsible for the platform. Since the developers of smart contracts are not explicitly trusted by the platform, the design of the smart contract language is essential in defining the boundary for untrusted developers. As one example, regardless of how a user customizes their smart contract, they should not be able to inflate or counterfeit the underlying digital currency. This is achieved in Ethereum by defining the programming language, known as the Ethereum Virtual Machine (EVM) so that upon encountering any instruction that makes an account balance go negative the entire transaction is reverted. Thus smart contracts can be thought of as defining the ground rules for a sandbox, within which developers are allowed to innovate.

7.1 Striking a balance between safety and extensibility

The need for program verification: Even in Ethereum's first few years of operation, we have seen numerous expensive disasters caused in part by smart contract "bugs", errors introduced when developing the smart contract programs. These have underscored the importance of program verification and other verification tools that can help identify such errors or correct for them. A few are especially instructive for illustrating some potential solutions: the 2016 theft of $50M USD worth of Ether from "The DAO" smart contract, the July 2017 theft of $30M USD worth of Ether from the Parity Wallet smart contract,[12] and the November 2017 accidental loss of $30M USD worth of Ether from the same Parity Wallet smart contract. In all three of these incidents, the underlying programming errors were subtle and were not found during security audits and code reviews. In the first two incidents, the vulnerabilities were deliberately exploited by hackers who aimed to profit from the theft, while in the third case the loss was triggered by accident — the funds were not stolen, they were simply made inaccessible. A CBDC should take efforts to prevent such disasters with forethought.

Support for verification and analysis: The expensive disasters mentioned above, as well as many others, have led to an active research effort in designing and applying program analysis and verification tools to smart contracts [195]. Program analysis tools aim to identify known classes of bugs, and rule out certain kinds of misbehavior. Program verification aims to provide a guarantee that the software satisfies certain requirements (e.g., that an account balance cannot go negative), or implements a formal specification. These tools can be used to help developers avoid bugs in the first place, and can also be employed by users performing due diligence to inform their decisions about whether to use the contract. Most smart contract language compilers and editors, such as the Remix IDE in Ethereum, contain some degree of ad-hoc bug and hazard detection — for example, warning users if a contract has code that resembles bugs that have occurred in the past. Complementary tools like Mythril, Oyente and others can also be used to evaluate smart contracts. Besides smart-contract specific tools, there are also generic frameworks for program analysis that can be adapted to this use. In particular, the K-Framework has been used to analyze a large number of Ethereum smart contracts [196].

Some program analysis tools can be directly built into the smart contract language, effectively preventing classes of bugs from appearing in the first place. For example, the information flow language[13] allows the programmer to annotate the smart contract with trust relationships, i.e. "Alice should not be able to affect Bob's outcome in this contract." The information flow type checker can catch errors where the smart contract implementation fails to enforce this constraint. As another example, some important invariants such as that digital assets should not be counterfeited, can be enforced through so-called "linear types" [197], [198] in essence, quantities of currency are annotated as "linear", which means they must behave like conserved quantities that

[12] https://hackingdistributed.com/2017/07/22/deep-dive-parity-bug

[13] https://github.com/Neroysq/VyperFlow

are exchanged, but not created or destroyed. Some languages, such as Michelson and Plutus, are based on functional (rather than stack- or register-based) programming models, which may make it easier to adapt new program analysis tools.

A CBDC could help avoid smart contract programming errors by developing program analysis tools alongside the CBDC platform itself. To the extent a CBDC must choose which existing smart contract technologies to co-opt from, it should take into consideration the maturity and effectiveness of available program analysis tools. A CBDC may choose to require mandatory requirements for some kinds of program analysis, which could be enforced automatically by the platform.

Expressiveness, restrictiveness, and domain-specific languages: None of the promising applications for a CBDC strictly require a smart contract programming language at all. Instead, capabilities anticipated by the CBDC platform designers can hardwired in. This would prevent bugs introduced by new smart contracts developed by third-party developers, but would also foreclose on their potential innovations.

Many smart contract systems in use today offer some compromise in between a fully general purpose smart contract language and hardwired applications. Some smart contract systems like Bitcoin script are based on a general purpose programming language but with many control-flow structures (like `for`-loops) removed. This can make programs easier to analyze, but also rules out many applications. Another approach, called "domain specific" languages (DSLs), which includes DAML, BitML, offer some flexibility to generalize, but are designed primarily around particular classes of applications such as auctions or bilateral agreements.

Support for upgrades, reversibility, and redactions: Even a language selected with security in mind will inevitably encounter bugs and mistakes. These bugs may arise through user error, creative development, or malicious intent. A CBDC may anticipate needing to employ a variety of mitigation and remediation strategies, which may include overwriting account balances, changing the code of a smart contract, or potentially other modifications. It is true that blockchains are "immutable" in the sense that the historical record of past transactions, since they are copied widely between the system operators as well as the users, are likely to remain available and may be difficult to suppress. However, the rules of a blockchain can be changed by the system operators, and in fact this has been an important way that many mistakes and disasters have been remediated in existing digital assets. As an example, the earlier-mentioned theft of $60 million USD worth of Ethereum cryptocurrency affecting The DAO in 2016 was addressed in such a way. A large segment of the Ethereum community agreed to a "hard fork," which effectively transferred coins from the thief's account back to the original participants of The DAO. Although the remediation in this case was successful, this has not always been the case. It took over a month to coordinate on the hard fork change, but in most cases an attacker would have been able to escape with the funds in a matter of hours, making such a hard fork ineffective. There have been several proposals from the research community, known as "reparable" or "redactable" blockchains [199], [200], that aim to simplify the process of applying such remediations so they can be applied more swiftly.

Even without relying on intervention from the platform itself, smart contract developers can build "upgradeability" features into their applications themselves. For example, OpenZeppelin, a popular library of smart contract templates, provides such a feature as a proxy layer. Essentially, the code for the outer layer, which indeed must be immutable, delegates its authority to a dynamically-named contract that can be updated by the original creator of the contract.[14] A CBDC may minimize the need to take platform-level remediations by encouraging smart contract administrators, such as fintech companies or commercial banks, to make use of such mechanisms.

Handling contention and concurrency in transactions: An important way in which smart contract languages have differed is in how they handle concurrent transactions and shared resources under contention. A benign example of a concurrent transactions is the following scenario, which is reminiscent of check floating in traditional (non-blockchain) banking.

1. Alice's account balance is initially \$10. She initiates a transaction T that sends \$20 to Bob - more than she has in her account.

2. Alice receives \$10 into her account because of a transfer on-chain, such as a withdrawal from an exchange. Alice's account now holds a \$20 credit.

3. Transaction T is committed on the blockchain, transferring her entire \$20 account balance to Bob.

Such "floating" transactions are supported in account-based cryptocurrencies such as Ethereum, just as they do with checks in the traditional banking system. It works because the identifier for Alice's account does not depend on its history of transfers. In contrast, with digital assets based on "Unspent Transaction Outputs" (UTXOs), such as Bitcoin, a transaction must refer not to the account identifier, but to the prior transfers that provide the source of funds. Hence in a UTXO-based digital asset, Alice could not initiate her transaction (Step 1) until after her withdrawal transaction is authorized (Step 2).

For other applications, such as auctions, this restriction on concurrent transactions makes the UTXO model far less flexible. Consider an auction, in which any member of the public can place a bid, and each bid is assigned a sequence number. The following example in pseudocode illustrates how such a mechanism could be implemented in an Ethereum-like digital asset:

```
memory cell BidCounter := 0;
    function PlaceBid() {
        ...
    BidCounter := BidCounter + 1;
...
}
```

[14] https://docs.openzeppelin.com/upgrades/2.8/writing-upgradeable

Suppose Alice and Bob each place a bid at roughly the same time — one or the other would be processed first, depending on network timing or potentially left to the choice of the system operator. However, this would be very difficult to implement in the UTXO model. One approach would be to represent the current value of `BidCounter` as a UTXO; a bid would need to "spend" the current value, and "create" a new UTXO for the updated value. If Alice and Bob place bids at roughly the same time, then only one of them would be committed, and the other would have to be resubmitted.

Besides account based and UTXO-based transaction models, other choices are possible as well. The Execute-Order-Validate model from Hyperledger Fabric lies somewhere in between. While account identifiers are used when initiating a transaction, the transactions are checked for "overlapping read/write sets" (such as the `BidCounter` in the above example), hence concurrently submitted bids may or may not need to be resubmitted, depending on the implementation of the system operator.

To summarize, the UTXO model can be seen as a restrictive case of the account model, which can avoid some potential hazards or delays (effectively preventing "check float"), but that also limit the ability to implement mechanisms like auctions through the smart contract system.

The potential of smart contracts to accelerate systemic risks: Even besides coding flaws, smart contracts may function exactly as intended by their creators, and yet when interacting together may lead to systemic hazards. Some set of smart contracts, such as stablecoins and other decentralized finance (DeFi) instruments, are highly interdependent, and rely on each other as collateral. It can be difficult to identify when the conditions are ripe for cascading "bank runs" on these instruments.

A fascinating recent example of systemic risks brought about by smart contracts has been the use of "flash loans" in price manipulation attacks. Flash loans are a particular kind of smart-contact enabled loan, for which there is no clear analog in traditional finance. In a flash loan, a user offers up their digital assets for a limited range of "zero counterparty risk" uses. Essentially, the rules of the smart contract guarantee that the funds that must be borrowed and repaid all within the timespan of a single transaction. This condition is automatically enforced by the smart contract code, which checks the account balance at the beginning and end of the transaction, and invalidates the entire transaction if these do not match. An example of a legitimate use of such a loan is an arbitrage opportunity across on-chain exchanges. If the currency can be traded in a cycle across multiple exchanges, all within a single atomically-executed (all-or-nothing) transaction, then a flash loan can enable both the arbitrageur as well as the lender to earn a profit. However, flash loans can also be used to manipulate market mechanisms whose "price estimate" can be temporarily affected by the movement of the flash-lent funds.

Limitations of enforcing policies through restrictions at the CBDC platform level: It may be tempting to think that a CBDC can limit the unsafe use of digital assets simply by restricting the expressiveness of the smart contract language. However, we have seen that even simple smart contract languages can be extended to new features by sufficiently clever developers, even in ways that are not intentionally supported. For example, even basic digital assets with only a plain digital signature can be enhanced with "threshold signing" functionality (as described in Section 5) without any explicit support from the platform. A CBDC may collaborate with regulators to restrict such uses, but enforcing them may be outside of what can be automatically enforced within the system.

At an extreme, desirable smart contract features that are not provided by the CBDC platform itself, may be achieved by relying on third party custodians. This is already the case, for example, with stablecoins such as Coinbase's USDC. This is backed by deposits of dollars custodied by Coinbase itself as a third party, hence relies in trust in them as an administrator. It is possible that limiting the extensibility of the CBDC in an attempt to improve safety may have the unintended effect of driving more users to services outside the sphere of influence of the central bank. This may be an argument in favor of the CDBC providing smart contract features.

7.2 Off-chain protocols and advanced cryptography

While the focus of most program analysis and safety features for smart-contract based applications have focused on the smart contracts themselves, smart contracts are only one of several software components making up the entire application. Other software, such as the (often web-based) user interfaces can potentially contain bugs and lead to dangers as well. It will be important for the CBDC to consider safety features and analysis standards for these software components as well.

As one example, in order to support rapid micropayments, faster than what can be provided directly by the platform, smart contracts can enable "off-chain" payment channels, which involves a smart contract acting in concert with digitally signed messages exchanged between parties as well. These off-chain messages and digital signatures should be scrutinized to the same degree as the smart contract. In general, to improve performance and reduce execution (i.e., gas) costs, smart contract developers have found ways to make use of complex arrangements involving cryptographic evidence and minimally-trusted third parties. These includes "roll-ups", or verifiable computing, which can accelerate the task of validating a blockchain.

7.3 Smart contracts as a two-layer architecture

It may be most effective for a CBDC to function as a two-layered system, where the central bank issues digital tokens to commercial banks that in turn maintain the digital wallets and define the smart contract languages. The central bank could focus on defining a minimal set of features, just what is necessary to support the flow of funds between the layers, while the innovation and customization is developed by the commercial banks at the second layer.

One approach is to consider each of the commercial banks, as well as the central bank, to maintain its own instance of a blockchain. The challenge then is to provide a way to manage the transfer of assets from one chain to another. There has been significant research and development work on defining protocols for interoperability across independent blockchains, such as HyperService, Aspen, Interledger, Cosmos, Protean, and sidechains [177], [201]–[203]. The basic idea of interoperability is that digital assets defined on Blockchain A can serve as a backing store for "shadow assets" defined on Blockchain B. The backing assets retain the security and monetary policy properties of Blockchain A, while the shadow assets can be traded and used in smart contracts according to the functionality defined by Blockchain B. This two-tier structure could function quite similar to how central banks currently provide reserve accounts that commercial banks must use as backing assets. The main challenge in interoperability is to ensure that the operators of the backing blockchain do not need to be aware of all the details of all the other blockchains, as otherwise this would undermine the extensibility and scalability benefits of point of independent operation. The minimal requirements to support such operation are that the backing Blockchain A can recognize a limited number of transactions (e.g., withdraw and deposit) on the shadow Blockchain B. In the simplest case, Blockchain B is identified simply by the public key of a fixed service provider responsible for it. The operators of Blockchain A can identify valid transactions on Blockchain B from these signatures. Other cases are more challenging. A research focus has been to define interoperability between public blockchains based on proof-of-work [53] and proof-of-stake [62], [204], which pose several challenges due to the design of their consensus protocols. If the CBDC is based on a permissioned blockchain architecture, it may be much simpler to define interoperability using simple digital signatures.

8 Secure Hardware

The role of secure hardware in digital currencies is a controversial and often misunderstood topic. The goal of this section is to provide non-expert readers a brief introduction to secure hardware technology and discuss both the main benefits and the limitations of the currently available secure hardware variants. We explain the problems of simple digital currency schemes that rely on secure hardware and discuss better ways to leverage secure hardware. Finally, we provide recommendations regarding the use of secure hardware for organizations like central banks that are currently investigating CBDC deployments.

8.1 Brief introduction to secure hardware

The term "secure hardware" commonly refers to a computing environment whose goal is to protect data and computation. Secure hardware can be used to execute security-critical applications such that their data and execution is protected and isolated from the rest of the computing platform that can be untrusted.

The use of secure hardware can enable significant security improvements compared application execution on standard computing platforms such as PCs and smartphones. In standard computing platforms, the security of any executed application relies on the trustworthiness of a very large software stack that includes the entire operating system (OS) and thus millions of lines of code, and also the trustworthiness of the

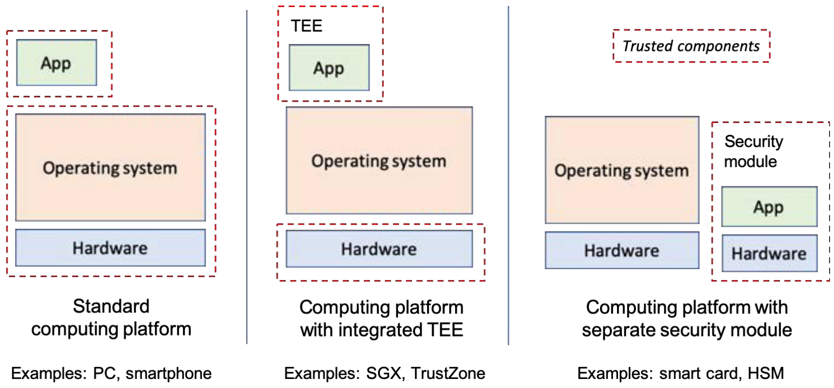


Figure 7: In standard computing platforms, shown on the left, the entire OS must be trusted for secure execution of security-critical applications. In computing platforms with TEE capabilities, shown in the middle, it is sufficient to trust the application’s code and the underlying hardware. In systems with dedicated security modules are used, shown on the right, the additional hardware and the application code must be trusted. The trusted components in all three models are shown surrounded by a dashed red border.

entity who operates the computing platform like an administrator. This standard trust model is illustrated in Figure 7, on the left. In comparison, when the same application is executed inside secure hardware, its security relies only on the correctness of the application code itself (e.g., few hundred lines), and the assumption that the protections of the secure hardware technology itself cannot be circumvented.

Secure hardware variants: Secure hardware can be realized in two main ways. The first common approach is a separate module or a chip that is connected to the rest of the computing platform over an interconnect. This approach is shown in Figure 7, on the right. The second common option, and one that has gained popularity recently, is to enhance the general-purpose CPU such that it provides a “trusted execution environment”, also known as TEE. The code that is executed inside the TEE is protected, with hardware and software enforcement, from other untrusted code that runs on the same platform. This approach is shown in Figure 7, in the middle.

On commodity computing platforms, such as PCs, the prime example of currently widely available secure hardware technology is Intel’s SGX [205]. SGX creates a TEE where applications, called *enclaves*, are protected from other code running on the same platform. SGX enclaves are supported by practically all latest Intel CPUs and the SGX architecture is open in the sense that it allows third parties to develop their own enclaves.

Most modern smartphones support two types of secure hardware. First, smartphones are typically equipped with a smart card (SIM card). Most smart cards are closed systems, as installing new code inside them requires permission from its issuer (e.g., mobile network operator). Second, many smartphones support the ARM

TrustZone [206] architecture which realizes a TEE on the main CPU of the mobile device. Permission from the mobile device manufacturer is typically needed to run new applications inside a TrustZone TEE, and thus TrustZone can be considered a closed platform as well.

Security-critical server platforms often use external hardware secure hardware modules (HSMs). Compared to the previously listed commodity secure hardware variants, modern HSMs are specialized and expensive hardware equipment that typically provide various protections against physical tampering and other attacks [207].

Other secure hardware variants exist too. For example, portable standalone devices can be used to store cryptographic keys for use cases such as two-factor authentication [82] and cryptocurrency client credential storage [208]. For the latter, see more details from Section 5 where digital wallets are discussed.

Security properties: Most secure hardware designs, whether realized as a separate chip or integrated in the main CPU, have two main security properties. The first is *data confidentiality*, which means that secrets like cryptographic keys that are stored and processed inside the secure hardware should be protected from unauthorized access. The second is *execution integrity*, which means that external parties that communicate with the secure hardware can be guaranteed that the intended code was executed correctly inside the secure hardware.

One simple approach to realize execution integrity is to rely on a closed secure hardware platform where only pre-vetted code can be executed. In such systems the code correctness is based on *whitelisting* by a trusted authority like the secure hardware vendor. Another, typically more flexible approach is to allow execution of any code inside the secure hardware, and to let other parties verify the correctness of the code through a process called *remote attestation* [209]. Remote attestation is an interactive protocol that can be executed between the secure hardware and a remote verifier who wants to examine which code is run inside the secure hardware. The secure hardware is trusted to execute the examined (attested) code faithfully, and thus ensure its execution integrity.

8.2 Limitations of secure hardware technology

Secure hardware can enable significant security benefits, as long as the protections of the secure hardware itself hold. In this section we discuss possible ways that adversaries can attempt to break secure hardware protections and the estimated feasibility of such attacks.

Software-based side channels: One common way to attack secure hardware is through side channels. TEEs like Intel SGX and ARM TrustZone share their hardware with the rest of the computing platform, which creates a potential susceptibility to side-channel attacks, where malicious software on the same CPU attempts to infer secrets that are processed inside the TEE based on utilization of shared physical resources like caches. Researchers have recently demonstrated the possibility of such information leakage from SGX enclaves [210], [211]. In addition, subtle side effects of transient execution can leak secrets to untrusted software on the same platform [212], [213].

One possible defense against side-channel attacks is to write code that includes defensive measures such as elimination of secret-dependent branching. Automated tools that help the developer to harden enclave code against side-channel attacks are an active area of research [214], [215]. While perfect elimination of all possible sources of leakage is difficult, code hardening can be an effective defense against most known software-based side-channels.

Physical tampering: In scenarios where the adversary has physical access to the secure hardware, physical attacks become another relevant concern. Modern TEE architectures like SGX and TrustZone store and process secrets inside the main CPU package. Physical attacks that attempt to extract secrets like cryptographic keys from the CPU package are generally considered difficult and expensive. Physical side-channels (e.g., ones that monitor the power consumption of the secure hardware during its processing of secrets and thus attempt to infer the value of the secret) are another and less invasive potential attack vector. Full elimination of all possible forms of physical side-channel leakage is considered difficult [216].

Most smart card manufacturers consider simple physical key extraction and side-channel attacks as part of their threat model and include protections against them. Researchers have shown that well-resourced adversaries (e.g., ones equipped with sophisticated laboratory equipment) may be able to extract secrets from smart cards [217]–[219]. Such attacks are likely to be infeasible to many adversaries. HSMs include sophisticated and expensive physical protections in their manufacturing process and are considered difficult to tamper with.

Trust concerns: Besides the above discussed attack vectors, another common concern for the use of secure hardware technology is the trust model, where the hardware vendor must be implicitly trusted. The TEE architectures that are widely available in commodity computing platforms today come from few vendors (mainly Intel and ARM). Thus, system designers have little choice in terms or which secure hardware to use and which vendor to trust. Such trust issues are emphasized by the fact that the designs details of TEEs are not entirely public. For example, many aspects of the Intel SGX’s design remain undisclosed.

This situation may improve. The computing platform and chip manufacturing landscape is getting more diverse, and in near future system designers may have more hardware and chip vendors to choose from. Also open-source initiatives such as the Keystone TEE [220] architecture on the RISC-V platform may enable secure hardware variants where the entire design is public.

Another trust concern is related to the supply chain. If the adversary manages to tamper with the secure hardware after its manufacturing and before it reaches the customer, the protections provided by the secure hardware may be weakened or circumvented. Such supply chain attacks require sophisticated hardware tampering skills and access to the logistics process, and thus such attacks are considered feasible only for the most resourceful adversaries (e.g., nation states).

8.3 Problems of simple use

Now, that we have explained the main benefits and limitations of secure hardware technology, we proceed to discussing its use in digital currencies. We start with a simple but commonly suggested example that is also one of the digital currency implementation approaches mentioned in a recent patent by People's Bank of China [221], as discussed in more detail in Section 11.3.

Simple design: Consider a token-based digital currency system where a trusted bank issues signed coins to users. One user, say Alice, can perform a payment by passing the sufficient number of coins (tokens) to another user, Bob. Bob accepts the coins by checking the bank's signature on each coin, but Bob does not contact the bank. The attractive aspect of such a design is that payments can take place entirely offline, as they require no communication with the bank, and payments enjoy strong privacy guarantees, as no third party is involved in the payment.

The main issue with any token-based design is the possibility of *double spending*. If Alice is able to spend the same coins twice, the whole digital currency system is obviously broken. The problem of double spending could, in principle, be addressed by using secure hardware on each user's device. During payments, the coins could be transferred from one (attested) secure environment to another, and the secure environments could enforce that each coin is spent at most once.

Main problems: Unfortunately, such simple use of secure hardware technology has serious problems. The first major problem is that it creates *economic incentives* for users to attack their own secure hardware. When the adversary is the owner of the computing platform, the adversary typically has significant control over other software that is running on the same platform and permanent physical access to the secure hardware. Such aspects may make the above discussed attack vectors easier to exploit. Attacks against secure hardware become economically viable if the adversary gains a larger benefit (in terms of double spent coins) compared to the time and equipment investment needed to attack the secure hardware.

The second problem with such simple design is that it does not support *graceful degradation*. Even if only one secure hardware environment gets compromised, the adversary is able to spend the same tokens an unlimited number of times and thus break the digital currency system completely. Alternatively, if the secure hardware vendor turns out to be malicious, if the attestation mechanism gets compromised, or if an attacker can infiltrate a link on the supply chain and change the hardware, double spending of coins without restrictions is possible.

8.4 Better ways to leverage secure hardware

Motivated by the problems of simple use of secure hardware, in this section we discuss better ways to leverage secure hardware in digital currencies. In particular, we present examples where the security of the entire digital currency system does not rely on the use of secure hardware (graceful degradation) and platform owners do not want to attack their own hardware (economic incentives).

Infrastructure hardening: Our first example is using secure hardware to harden the backend infrastructure of a digital currency system as a complementary *defense-in-depth* security mechanism. Assume a digital currency where a bank maintains an account balance for each user. Such critical data repositories are typically replicated among multiple servers (consensus nodes) using a Byzantine-fault tolerant (BFT) protocol (recall Section 3). Each node could store its credentials and execute the consensus protocol within secure hardware. Such protection mechanism raises the bar for successful attacks, as now the adversary not only has to obtain software control of a large fraction of the consensus nodes, but he *additionally* has to break the secure hardware protections in them. The owners of the computing platforms do not have an incentive to attack their own secure hardware and secure hardware failure alone is insufficient to compromise the currency system.

Simplified and efficient privacy: Many digital currency systems use cryptography for user privacy protection, as discussed in Section 6. One of the first examples is Chaum’s *e-cash* [222] that is based on a bank that issues coins to user. In this system a cryptographic construct called *blind signatures* enables anonymity protection for the payer (but not payment recipient). Another, more recent example is Zcash [168], which is based on a distributed ledger where all transactions are stored in encrypted format that make use of zero-knowledge proofs to show the correctness of a transaction without revealing its details. The main drawback is that the required zero-knowledge proofs make such systems complicated to deploy and have high resource requirements which often makes their use on e.g. mobile devices infeasible. For example, clients in Zcash are required to download and process the whole chain to benefit from Zcash’s privacy guarantees and transaction creation is relatively slow (several seconds on recent desktop PCs).

Such cryptographic protections could be *replaced* with transaction processing that takes place inside secure hardware. In a simple solution, the secure hardware maintains a balance for each user and users send encrypted transactions to the secure hardware where they are processed. Compared to centralized schemes like Chaum’s e-cash, such a solution achieves better privacy (also recipient anonymity and value privacy). Compared to ledger-based anonymous payment systems like Zcash, such solution provide greatly simplified deployment and better performance.

Complementary privacy: Another option is to *complement* cryptographic privacy protections with the use of secure hardware for increased privacy protection. For example, transactions that use cryptographic commitments [223] offer payer and recipient privacy and value privacy, but no “transaction graph privacy” which prevents adversaries from linking transactions to each other, as explained in Section 6. The users could send commitment-based transactions to secure hardware that is operated by a bank and the secure hardware would process the transactions. Such a deployment would provide improved privacy (added transaction graph privacy protection) and graceful degradation: if secure hardware is compromised, only the additional gained privacy protection is lost and all the other privacy protections still apply due to the use of cryptography.

Compliance rules: CBDC deployments should, most likely, protect user privacy and at the same time enforce compliance policies and audit mechanisms, such as ones that are commonly used for anti money laundering and tax evasion detection purposes. As explained in Section 6, supporting both user privacy and compliance simultaneously is technically challenging. One possible way to address this challenge is to leverage sophisticated cryptographic constructs such as zero-knowledge proofs that allow users to show that their payments are compatible with compliance rules without revealing their identity or other transaction details. However, such schemes have drawbacks like complicated deployment and poor performance.

The use of secure hardware could allow greatly simplified systems where compliance policies could be enforced without violating the privacy of the users. The users could send their transactions in an encrypted format to secure hardware that would process them and at the same time enforce that each transaction complies with regulatory rules. Such policy enforcement would be easy to implement, because the necessary details like how much each user has spent within a given time period could be visible in plaintext inside the secure hardware.

Lightweight clients: Digital currency systems that store all transactions on a public ledger have benefits like *public verifiability*, which means that any third party can verify that all transactions are correctly formed. The downside of such a solution is heavy download requirements. Especially mobile clients, such as smartphones, would not want to download the entire ledger that can easily be multiple gigabytes in size. Selectively downloading only transactions that are relevant for the user, might reveal the identity of the user, even in systems with strong cryptographic transaction protections.

In such a setting, mobile clients could send encrypted queries to secure hardware on an infrastructure server that has access to the entire ledger. The secure hardware could then return the relevant transactions back to the client, without revealing the identity of the client to the operator of that infrastructure server. Such schemes have been developed for permissionless cryptocurrencies in recent research [224], [225] and the same principle could be applied to centralized CBDC deployment as well, if the CBDC system uses a public ledger.

Hardware wallets: Similar to infrastructure hardening, secure hardware could also be used to harden the client devices. Systems where client credentials are protected by some form of secure hardware are typically called "hardware wallets" and such hardware solutions are already widely used in permissionless cryptocurrencies, such as the hardware wallets produced by Ledger [226] or Trezor [227]. Hardware wallets protect the user's private keys from external adversaries that may be able to install malicious software on the computing platform of the user (PC or smartphone). To create a transaction, the user connects the hardware wallet to his PC or phone, where the transaction gets created and then sent to the hardware wallet. The user is expected to confirm the transaction amount and recipient from a small screen on the hardware wallet before the hardware wallet authorizes the payment by signing the transaction.

While hardware wallets can help to keep a user's credentials safe, they do not solve all problems of key management and payment safety. For example, users still need to be careful when confirming transactions details and they should ensure that they have a backup in case they lose their hardware wallet.

Smart contracts: Besides payments, CBDCs might support more complicated financial applications implemented as smart contracts, as discussed in Section 7. One challenge with the current smart contract solutions is that all contract data is typically recorded on a public ledger. This prevents deployment of a large class of financial applications that require confidential contract data. Recent research has explored techniques that could allow smart contracts to support confidential data on-chain [176], [181], [228]. However, such solutions require expensive and complicated cryptographic techniques like zero-knowledge proofs that can be difficult to deploy and suffer from poor performance. Secure hardware could be used to enable an easier way to execute smart contracts with confidential data, as demonstrated by recent research [180].

8.5 Summary and recommendations

Secure hardware is clearly not a panacea for any digital currency including CBDC. The currently available secure hardware technologies offer significant security benefits compared to standard program, but this technology also has its limitations. Thus, our recommendation is to be cautious of solutions where the integrity and security of the currency depends solely on secure hardware.

However, this does not mean that the use of secure hardware cannot offer benefits for CBDCs. When deployed in carefully chosen ways, secure hardware can either replace expensive cryptographic protections or function as a complementary security mechanism in addition to cryptographic protections. Therefore, our recommendation is that institutions currently investigating the possibility of CBDC deployments should understand the potential benefits of secure hardware technology.

Reading Materials

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

9 Opportunities for Novel Financial Technology

As discussed in the introduction to this paper, a retail CBDC offers several commonly identified benefits: (i) gains in transactional efficiency: higher speed, lower cost, and finality, (ii) broader tax base, reduced tax evasion, (iii) backstop to private sector managed payment systems, and (iv) enhanced financial inclusion.

In principle, however, even more important than these benefits are the implications of CBDC for monetary policy and financial stability. CBDC can enable mechanisms for implementing monetary policy that are analogous to those available today, but novel in terms of their practically achievable parameters. Additionally, CBDC offers opportunities to implement a range of innovative monetary policies that operate at finer granularity, with greater transparency, and with more sophisticated programmatic logic than is technically possible in existing financial systems. These opportunities have implications for both the implementation and transmission of monetary policies. There are also a few risks, which we discuss below.

9.1 Implementing monetary policy

The basic mechanics of monetary policy implementation will not be affected by a switch from physical currency to CBDCs. Given that a relatively modest share of the supply of broad money is in physical form, this should not be surprising. However, other technological changes that are likely to affect financial markets and institutions could have significant effects on monetary policy implementation and transmission.

Retail CBDC disseminated through electronic wallets would make it easier to implement monetary policy more effectively in two ways. First, the nominal zero lower bound, which became a binding constraint for traditional monetary policy in advanced economies during the worst of the global financial crisis, would no longer apply. The central bank could institute a negative nominal interest rate simply by reducing balances on these electronic wallets at a pre-announced rate.

In an economy with physical cash, this should in principle not be possible since consumers (and firms) have the alternative of holding physical currency banknotes, a zero nominal interest rate instrument. In a scenario where there was no zero-interest central bank-issued alternative such as cash, it would be easier to implement a negative nominal interest rate on CBDC. If a CDBC co-existed with cash, there would be a limit (determined by cash storage costs, frictions in the use of cash etc.) to how low the central bank could drive the interest rate on the CBDC. In principle, negative nominal interest rates that would become feasible with certain forms of CBDC should encourage consumption by making it expensive for households to maintain cash positions.

Monetary policy could also be implemented through "helicopter drops" of money, once seen as just a theoretical possibility of increasing cash holdings in an economy in a non-distortionary fashion by making lump sum transfers to all eligible individuals or households. This would be easy to implement, at least in principle, if all citizens in an economy had official electronic wallets and the government could transfer central bank money into (or out of) those wallets. Channels for injecting outside money into an economy quickly and efficiently become important in circumstances of weak economic activity or looming crises, when banks might slow down or even terminate the creation of outside money.[15]

One challenge, if a CBDC is issued through a two-layer approach in which the digital wallets are maintained by commercial banks, is the possibility that an individual or household might maintain multiple wallets at different institutions. Some coordination would be required to avoid double-dipping or multiple-dipping from helicopter drops of money. This concern would be obviated if the central bank directly managed identities and accounts. In both cases, however, there would be adverse implications for privacy.

Thus, a central bank could substantially reduce deflationary risks by resorting to such measures in order to escape the liquidity trap that results when it runs out of room to use traditional monetary policy tools in a physical cash-based economy.

There is an important asymmetry in this context that could become even more consequential if outside money were to have only a small role in the overall money supply. In that case, if banks were expanding outside money rapidly at a time of strong economic activity with rising inflationary risks, the central bank's ability to shrink electronic wallets holding CBDC might not do much to control the overall money supply. Although most advanced economy central banks now use price-based monetary policy measures (policy interest rates) rather than quantity-based monetary policy measures, this might be another reason for central banks to issue CBDCs rather than letting central bank money wither away if households were to use less and less cash.

There is a flip-side to the ease with which a central bank can increase or decrease the supply of outside money. The ability to impose a haircut on CBDC holdings, or to increase them rapidly in case the government were to apply pressure on a central bank to monetize its budget deficit, could lead to substitution away from the CBDC. The reduction in nominal balances and the erosion in the real purchasing power of nominal balances through monetary injections would have similar effects—decreasing confidence in the currency as a safe asset that can hold its value, at least in nominal terms. This could pose potential risks to monetary stability.

9.1.1 Transparency

With broad adoption, retail CBDC may capture a significant segment of economic activity at a national level and even, for CBDCs that serve as global reserves, at an international level. Data harvested from the resulting panoramic view of monetary flows on the underlying ledger can in principle provide policymakers with unprecedented data and insights. One consequence, as noted above, is an ability to limit tax

[15] There is a precedent for this rooted in Silvio Gesell's accelerated "free money" idea [229], physically implemented as stamp scrip, which showed promise to jump-start local economies in some historical experiments [230]. Also, there are a number of non-governmental cryptocurrency proposals and projects for permissionless cryptocurrencies with some form of "universal basic income" built-in: see, for example, [231]–[234]. A government implementing a CBDC is better-positioned to implement policies like this at large scale, of course.

evasion, but there are many others.

The ability to monitor monetary expenditures at the level of individual consumers is already available to credit-card issuers and provides predictive power at the level of the individual consumer, as well as offering microeconomic and macroeconomic insights. Goldman Sachs, for example, advertises a service called Quantinomics that leverages credit-card data to forecast corporate earnings growth, purportedly more accurately than with traditional methods [235]. Lenders have long exploited data on individuals' expenditures to make accurate predictions about their likelihood of divorce, patterns of travel, and creditworthiness [236], [237]. A CBDC that has disintermediated or overlaps with private payment systems can potentially relay the result of detailed analytics in real or near-real time to monetary policymakers.

Naturally, there is a tension here between transparency and privacy similar to those discussed in section 6. Given the potential scale and scope of CBDCs, however, an analytics system with global view of transaction data—or even metadata—could be repurposed as or support mass surveillance tools. Consequently, it is of vital importance that the transparency benefits of CBDCs be balanced against and leveraged with an eye to privacy requirements.

9.1.2 Non-fungible money

Certain forms of CBDC permit the implementation of monetary policy that affects accounts or units of money *selectively* and *conditionally*, that is, in a non-fungible manner.

Money transmitted in "helicopter drops," for instance, can carry spending conditions that permit only certain classes of expenditure. To amplify their effect in stimulating economic activity, lump sum transfers might for example carry the requirement that they be spent on, e.g., durable goods, as such spending has been shown to demonstrate limited responsiveness to economic stimulus during recessions [238]. As discussed in section 11, the People's Bank of China has filed a patent application—perhaps meant for use with the DCEP (Digital Yuan)—that suggests the idea of a central bank issuing currency for loans that carry central-bank-set interest rates and borrower qualifications.

Spending policies can alternatively be linked to aggregate data by analogy with inflation-adjusted financial instruments or even data about the holder of the funds (e.g., for the implementation of age limits on retirement-account withdrawals). As another example, the USDA's existing Supplemental Nutrition Assistance Program (SNAP) (formerly "food stamps") could be implemented in a CBDC through the distribution of dollars that are only eligible for transfer to accounts held by authorized food retailers. The policy attached to such dollars can be modified in real time, enabling immediate grants and revocation of food retailer authorization. With certain technical enhancements, such a policy could also stipulate the types of goods eligible for purchase using SNAP funds or make additional funds available in order to incentivize the purchase of particular types of food.

CBDC can in principle permit all money to take the form of such financial instruments, with individual policies that determine nominal value and spending conditions based on nearly any desired form of data. At the extreme limit, *it may ultimately be feasible for every penny to be its own smart contract.*

There are potential downsides to non-fungibility, and fungibility is in fact treated as a design goal in many cryptocurrencies. This is because non-fungibility can be at odds with privacy and choice for currency holders. The ability to differentiate among units of currency based on serial numbers or transaction histories facilitates tracing, and indeed the distinctive transaction histories of Bitcoin enable blacklisting of units tainted by criminal activity [239] and transaction tracing by companies specializing in that activity, e.g., Chainalysis [160]. Similarly, the SNAP program places limitations on currency holders' purchasing behavior. Non-fungible currency would offer new mechanisms for government control of citizens' spending behavior that could catalyze new classes of "nanny state" interventions that may be unduly heavy-handed or micromanaging, and/or infringe on consumers' civil liberties.

9.2 Monetary policy transmission

A central bank endeavors to use the policy tools at its disposal to deliver objectives such as low and stable inflation, low unemployment, and financial stability. The transmission of monetary policy to economic variables such as GDP growth, unemployment, and inflation occurs mainly through the banking system but also through other financial channels.

A number of banks and consortia of banks are exploring the use of distributed ledger technologies (DLT) for bilateral settlement of clearing balances without going through a trusted intermediary such as the central bank. DLTs, as discussed earlier, make it easier to track and verify transactions. If all participants in a closed pool can monitor such activities and if there is a permanent indelible transaction record that is tamper-proof, they may be able to use group monitoring as an alternative for a trusted central counterparty.

Will such developments dilute the ability of the central bank to affect interest rates in the economy through its control of very short-term policy interest rates (such as the discount rate and the Fed funds rate in the U.S.)? This gets to the crux of the question about whether central banks can maintain their influence over aggregate demand and inflation even if they are sidelined from some of their traditional roles—issuing (outside) money and providing payment and settlement services for major financial institutions.

If banks and other major financial institutions do create such payments and settlement mechanisms among themselves (both bilaterally and across members in the group), and are also able to manage their liquidity positions and overnight balances more effectively, then settlement and liquidity management through the central bank might play a less important role. Still, competitive forces might limit the use of DLTs as an alternative for a trusted third party such as a central bank to provide settlement services while maintaining the confidentiality of those transactions. If these challenges are overcome, one possibility is that the central bank eventually becomes a liquidity provider of last resort in times of crises but, otherwise, commercial banks route their settlement and liquidity management operations through direct channels among themselves.

A related issue is whether nonbank and informal financial institutions, such as Fintech lending platforms, are less sensitive to policy interest rate changes than traditional commercial banks. If these institutions do not rely on wholesale funding and have other ways of intermediating between savers and borrowers, then the central bank might face significant challenges to the effectiveness of monetary policy transmission. The relative sensitivity of the nonbank financial sector to changes in policy interest rates and other operational tools of monetary policy needs further study as the structures of financial systems undergo changes that could significantly affect the implementation and transmission of monetary policy.

9.3 Selective review of academic literature

The academic literature has only recently begun to grapple with the implications of CBDC as well as Fintech more broadly for monetary policy. Some authors argue that a CBDC will not in any material way affect the implementation of monetary policy, although there could be other macroeconomic effects. The conclusions, as indicated by the limited and selective survey below, depend to a great extent on the model structure and the manner in which the CBDC is introduced into the economy.

Barrdear and Kumhof [240] develop a DSGE model with multiple sectors and several nominal and real rigidities to understand the effect of introduction of CBDC. These authors suggest that infusing CBDC into an economy could result in substantial steady state output gains of nearly 30 percent. This effect persists if the central bank issues a large amount of CBDC against government bonds.

Andolfatto [241] studies the implications of CBDC in an overlapping generation model with a monopolistic banking sector. In this model, the introduction of interest-bearing CBDC increases the market deposit rate, leads to an expansion of the deposit base, and reduces bank profits. This is because competition from the CBDC causes banks to raise deposit rates. However, the CBDC has no effect in terms of bank lending activity and lending rates. Although the introduction of the interest-bearing CBDC increases financial inclusion, diminishing the demand for physical cash, it does not disintermediate banks.

Bordo and Levin [242] consider how digital cash could bolster the effectiveness of monetary policy. They lay out some steps for implementing digital cash via public-private partnerships between the central bank and supervised financial institutions. They conclude that digital cash could significantly enhance the stability of the financial system.

9.4 Smart contracts: realizing other novel capabilities

Beyond non-fungible units of currency, CBDC platforms that incorporate or serve as a substrate for smart-contract functionality can realize a range of monetary policy tools and novel financial instruments. Such instruments could serve as new conduits for monetary policy, but could also fundamentally impact monetary policy transmission. Experience with smart contract platforms such as Ethereum illuminates some of the possibilities for new financial instruments in CBDC platforms. It also highlights the fundamental questions and challenges these instruments could surface around platform control and governance.

We encourage readers to refer to also section 7 for a more in-depth treatment of smart contract mechanics.

Atomic and instantaneous execution: Most smart contract platform architectures today permit multi-step transactions to execute *atomically*, that is, in an all-or-nothing manner. In a serialized DLT, that is, one in which transactions are fully ordered, and not processed in parallel, it is additionally possible for transactions to be executed *instantaneously*, in the sense that no changes to platform state from other transactions can occur at the same time.

These properties enable new capabilities without parallel or precedent in existing financial systems. One example is known as a *flash loan*. A flash loan is a loan that is initiated and repaid *within a single transaction*. Between the steps of borrowing and repayment, the transaction can execute any desired logic supported by the underlying DLT—for example, arbitrage on DLT-resident currency exchanges. If at the end of the transaction the loan is not repaid (with the requisite interest), the transaction aborts and, thanks to atomicity, has no persistent effect on platform state. If the borrower defaults on the loan, in other words, the loan is retroactively unwound, and in effect never took place. Because the lender assumes no risk, flash loans require no identification of or collateral from borrowers. They also typically carry very low interest rates, e.g., 0.1% [260], as the duration of the loan is nearly instantaneous.

Similar properties could provide a central bank with new mechanisms for implementing monetary policy. For example, it would be possible to effect systemic changes across a platform instantaneously. This could prove useful in preventing financial intermediaries from exploiting arbitrage opportunities resulting from temporally inconsistent implementation of policy changes—even when a central bank publicizes these changes in advance.

Distributed Autonomous Organizations (DAOs) and Decentralized Finance (DeFi): In the predominant model of smart contract execution, smart contracts run autonomously. They take the form of unmodifiable code that may be called by any user.[16] As discussed in section 7, this execution model is critical if smart contracts are to realize their intended role as virtual trusted third parties, but also carries risks, as historical incidents discussed in section 7 have shown.

A side-effect of smart contracts' autonomy is their ability to realize financial instruments or markets that run programmatically outside the control of the contract creator or any other single entity, resulting in efficiencies in execution and enforcement of terms unavailable in conventional contracts.

One class of such smart contracts is known as a *Distributed Autonomous Organization* (DAO). The best known example, called *The DAO*, was launched early in the

[16] Smart contracts can be instrumented to permit code updates and enforce access controls, but such features are only available if they are hard-wired into a contract's original code.

history of the Ethereum blockchain. It implemented a form of crowdsourced venture fund, allowing users to invest money in the contract and vote on the allocation of the resulting pool of money. The DAO accumulated some 15% of all the cryptocurrency in the ecosystem. (See section 7 for a discussion of a vulnerability that caused the failure of The DAO.)

DAOs are one design pattern for *decentralized finance (DeFi)*, a broad label that applies to smart contracts that lend money, support stablecoins, i.e., tokens that aim to maintain parity with fiat currencies, or run marketplaces where trades execute on a blockchain. DeFi instruments at the time of writing make up a small but rapidly growing $1+ billion market [261]. Many DeFi instruments lack exact counterparts in traditional financial systems, making the DeFi ecosystem a crucible of financial innovation. (See also section 7 for discussion.)

Support for smart contracts within or on top of a CBDC could give rise to similar innovations in a setting that is more tightly aligned with existing regulatory and legal frameworks and financial controls than cryptocurrency ecosystems are today.

Challenges and questions: Such incidents as The DAO hack and the weaponization of flash loans, both discussed in section 7, raise a number of questions that will inevitable surface in a CBDC platform with smart-contract functionality. While a cryptocurrency-based smart-contract system Ethereum is decentralized in a degree that a CBDC platform is unlikely to be, smart contracts nonetheless make it easier to create financial instruments whose control is shared or ambiguous. The rules and regulations governing the platform as a whole then become critical in assuring its integrity.

These questions include the following:

- *Accountability:* Should all smart contracts be required to have owners who assume responsibility and liability for their effects in the system? How will these owners be identified? (See section 4.)
- *Oversight:* Should smart contracts be instrumented by design with reporting functionality for regulators? What privacy considerations then come into play? (See section 6.4.)
- *Functionality:* Should smart contracts have the richest possible functionality supported by the underlying DLT, or should their functionality be constrained, e.g., through imposition of a domain-specific programming language?
- *Intervention:* Under what circumstances would a central bank administering a CBDC intervene should code running on the underlying DLT prove to be buggy, fraudulent, criminal [262], or otherwise problematic? Techniques such as those in, e.g., [199], [200], [263] may be worth considering.

Such questions arise even in CBDC designs where smart-contract functionality is overlaid on a DLT by third parties, one option considered in, e.g., [10], as application-layer functionality can have a systemic impact on the underlying currency.

9.5 Summary

The opportunities CBDCs offer for financial innovation may be summarized as follows:

- *Implementing monetary policy:* CBDCs offer the possibility of creating currency with *nominal negative interest rates*, as a means of stimulating consumption. They also can in principle allow the creation of various types of *non-fungible currency* with particular constraints on or incentives for their expenditure. CBDCs potentially panoramic view of national economies could *yield deeper insight for regulators and policymakers* into historical and ongoing economic activity than today's monetary systems, thus enabling better informed implementation of monetary policies.
- *Monetary policy transmission:* Should banks and other major financial institutions be able to create payment and settlement mechanisms among themselves with suitably strong transaction confidentiality, they could assume many of the settlement and liquidity management operations that are traditionally the province of central banks. CBDCs could thereby potentially blunt central banks' ability to transmit monetary policy.
- *Smart contracts for other novel capabilities:* By acting as a substrate for smart contracts, CBDCs could provide a way to translate a variety of financial innovations arising in cryptocurrency-based platforms into a setting more closely aligned with existing regulatory and legal systems.

With such capabilities, of course, come risks. Chief among them are:

- *Privacy concerns:* In a richly featured platform—e.g., one with a global analytics capability—the ability of platform operators to gather information about end users could resemble or extend even beyond those discussed in section 6.
- *Micromanagement:* The rich range of policies realizable by highly targeted capabilities of non-fungible currency and smart contracts could tempt policymakers into interventions that are unduly complex and representative of special interests (like the U.S. tax code [264]) and/or influence consumer behaviors in ways that infringe on civil liberties or are otherwise harmful.

10 Legal Considerations

The specific legal requirements for a CBDC depend on the jurisdiction and often can be modified by the jurisdiction establishing the CBDC. Thus, rather than discussing specific doctrines, it is more helpful to consider a few high-level issues involved in the design of a CBDC and its governing legal framework. The specific examples in this section are primarily drawn from the United States, but the same general issues will arise in most legal systems.

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

10.1 Jurisdiction

A CBDC is a national institution by definition, and will need to interface with its nation's laws and legal system. There will usually be no question of which nation's laws and legal system take priority in case of international disagreement: its own. Other legal systems may resolve disputes about CBDC assets, sometimes under their own law, and they may enter orders binding CBDC users. But to the extent that parties to a foreign dispute want the CBDC's own institutions to take any action to enforce those orders, it is reasonable to expect that they must first domesticate that judgment in a court within the CBDC's own national legal system.

That said, in a *federal* system such as the United States or the European Union, the CBDC will still be exposed to many subnational jurisdictions with varying laws. Relatedly, it may need to deal with a diversity of national and local courts. Some thought should be given as to how to authenticate orders and verify the authority of the courts issuing them, given that forgery of court orders is not unknown. Two options to simplify this task are to centralize all orders affecting CBDC assets in a single national tribunal, or to require all such orders to proceed through a common set of procedures before CBDC administrators are expected to act on them.

10.2 Compliance

Money laundering is the use of financial transactions to conceal the source of funds. Governments prohibit money laundering not because they care about funds as such, but because money laundering makes it easier for criminals to conceal their crimes, evade taxes, and profit from their ill-gotten gains. Relatedly, governments increasingly prohibit the use of financial transactions to support terrorist organizations. Roughly speaking, anti-money-laundering and countering the funding of terrorism (AML/CFT) laws come in three layers:

1. General prohibitions, such as the Money Laundering Control Act, that directly target money laundering itself by prohibiting the use of financial transactions to conceal the source of proceeds of criminal activity. Examples include "spending" cash received from drug dealing at a front business, or making wire transfers to make kickbacks look like legitimate business receipts. Similarly, the Antiterrorism and Effective Death Penalty Act makes it illegal to "knowingly provide[] material support or resources to a foreign terrorist organization."

2. Reporting requirements, such as the Bank Secrecy Act (BSA), which requires that financial institutions report to the government all transactions in cash of 10,000 USD or more. Reporting requirements also include Know Your Customer (KYC) rules, which require institutions to verify the identities of their clients, as well as more open-ended standards requiring institutions to report suspicious transactions. These rules are designed to help regulators find money laundering by enlisting surveillance at the financial institution level.

3. Anti-evasion (or "structuring") rules that prohibit attempts to circumvent reporting requirements, e.g., by breaking a larger transaction down into smaller

ones under the reporting threshold.

Collectively, these are the specific enforcement rules that governments currently thinks they need to achieve the broad functional goals of preventing money laundering. With a CBDC, it is useful to ask (a) whether these existing rules are enforceable against a proposed CBDC, (b) whether they are sufficient for the functional goals, and (c) if the answer to either previous question is "no," what other rules might be enforceable and sufficient. In general, if a payment or deposit system has any significant potential to facilitate transactions not meeting these goals, the financial regulatory system will attempt to strictly regulate and monitor transfers in and out of it. Thus, for example, if a CBDC itself offers strong anonymity (thus making KYC impossible at this layer), regulators may demand that exchanges which convert between the CBDC and other currencies implement KYC rules for all customers.

A hybrid two-tier CBDC in which the core digital currency is traceable can meet the requirements of existing AML laws. The institutions which provide customer accounts would be required to implement all of the reporting requirements under BSA, KYC, etc. Regulators could then monitor transactions entered into the system to trace funds as needed. In fact, the centralization of a single transactional ledger might help with monitoring, making the CBDC comparatively unattractive for money laundering.

Other CBDC designs raise serious AML issues. Designs that allow for the mixing of transactional inputs or with weak identity verification make some aspects of AML enforcement much more difficult. Designs with strong untraceability are almost certainly incompatible with AML regulation. This may be considered a virtue from their designers' privacy-oriented perspective, but is a deficit from the perspective of a financial regulator considering introducing a CBDC.

10.3 Privacy

Privacy *law* (as contrasted with privacy norms and privacy goals) interacts with CBDC design in two ways. The first is that existing legal rules about financial privacy already reflect considered balances between customer privacy and law-enforcement needs. In the United States, these rules are primarily statutory, as the Fourth Amendment generally does not apply to financial transaction records. (Under the "third party doctrine," a financial services customer "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." United States v. Miller, 425 U.S. 435, 443 (1976)). Instead, statutes like the Right to Financial Privacy Act (RFPA) specify the procedures law enforcement must follow to obtain such records and the legal standards of relevance they must meet. These rules apply in money laundering investigations, so the AML rules described above are compromises that already try to preserve some measure of privacy. But these statutory privacy rules also apply more broadly in any investigations, for whatever type of crime. So, for example, the RFPA standards apply when law enforcement seeks to examine the transaction records of a business it suspects of credit-card fraud, bribery, tax evasion, or hiding money from creditors.

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

A CBDC design could depart from this baseline by being either more or less technically protective of privacy. A design that is *less* protective — e.g., a public blockchain with identities easily linked to specific users — effectively provides law enforcement with freer access to transaction information. (One federal appeals court has held that under the third-party doctrine, there is no privacy interest in transaction information on the public Bitcoin blockchain. United States v. Gratkowski, No. 19-50492 (5th Cir. June 30, 2020.)) A design that is *more* protective — e.g. a public blockchain with strong untraceability and strong anonymity — raises questions about whether law enforcement access is sufficient. A hybrid two-tier CBDC design comes close to the status quo: federal law enforcement would need to proceed under the RFPA standard to obtain account information from financial institutions about specific customers. It would be appropriate to make clear (which might require statutory amendments) that a similar standard should apply for obtaining transaction records from the transaction ledger itself.

The second way in which privacy law pushes on CBDC designs is that it also imposes requirements *for* privacy against other parties. That is, privacy law sets a floor which the existing banking system is legally required to meet. In the United States, the RFPA, the Financial Services Modernization Act (a/k/a Gramm-Leach-Bliley or GLB), the identity-theft rules of the Fair and Accurate Credit Transactions Act, and the Electronic Fund Transfer Act all place limits on whom a financial institution is allowed to disclose customer information to, and when. These rules reflect a broad consensus that some degree of financial privacy is appropriate, not just against governments but also against private parties. In the European Union, the General Data Protection Regulation (GDPR) establishes a broad and high privacy baseline.

Again, a CBDC could depart from this baseline by being either more or less private. A design that is *less* privacy protective is not necessarily legally problematic: for example, a blockchain that makes transaction details public often reflects a decision by users to make their transactions public, rather than a privacy violation by the blockchain or by any institutions dealing with it. That said, it might be a tough sell for a payment system to come with lower privacy safeguards than users expect from existing ones. (Imagine the reaction from businesses if a central bank decided to standardize on Venmo, in which transactions are visible to all users by default.) A design that is *more* privacy protective is not necessarily legally problematic either: these statutes generally set a floor and not a ceiling. Again, a hybrid two-tier design comes closest to the status quo. In general, a CBDC is unlikely to perfectly replicate the balance struck by existing privacy law. Some aspects will likely be either more private or more public.

Unless a CBDC's designers secure legislative changes, therefore, a CBDC must be capable of complying with these privacy mandates. A few such requirements of note include:

- **Purpose Limitation:** Under the GDPR, personal information may only be used for the purposes for which it was collected; new uses require fresh consent.
- **Disclosure Limitation:** Under GLB, consumers have a right to opt out of having their personal information disclosed to unaffiliated third parties. Under

the GDPR, such disclosures generally may not take place without affirmative opt-in consent.

- **Access and Portability:** The GDPR gives each data subject a right to obtain any information "concerning him or her" in a structured digital format so that they may give that data to other services.
- **Rectification:** The GDPR gives each data subject a right to correct any erroneous data "concerning him or her."
- **Security Breach Notices:** The GDPR and numerous American state laws give each data subject the right to be notified promptly if their data is the subject of a security breach.

Some of these privacy restrictions significantly constrain the design space for a CBDC. It is not clear, for example, that a CBDC built around a public blockchain can ever comply with the GDPR's rules on disclosure limitation and rectification. Others require particular features in a CBDC rollout: any system that handles accounts for individuals, for example, will need to be designed such that it is possible to generate and send breach notifications if needed.

10.4 Fraud and mistake

While a well-designed CBDC, like any well-designed banking or payment infrastructure, can potentially reduce the incidence of fraud and mistake (or exacerbate them if poorly designed and implemented), it is not feasible to eliminate them entirely. Thus, a CBDC and associated legal regime must consider and balance two related concerns: *preventing* and *correcting* incorrect transactions. These transactions fall into a few recurring patterns, including:

1. *Disloyal Agents*: People frequently authorize others to act on their behalf. Sometimes this is informal: spouses ask each other to do their online banking. Sometimes it is legally necessary: guardians must have this power to do their job of protecting incapacitated or underage principals. And sometimes it is unavoidable: entities like corporations only act by and through human agents. Whenever an agent is authorized to take some action affecting a CBDC, the agent may exceed its authority and engage in unauthorized transactions.
2. *Impersonation* of an authorized user by an unauthorized one. Any credentials associated with an authorized user are themselves attack targets. 2FA and other authentication protocols are designed to furnish additional evidence that a user is who they say they are, but are necessarily less than completely reliable. (The design trade-offs involved are discussed further in Section 4.2.)
3. *Mistakes*: Phishing and related attacks induce users to engage in intended transactions with unintended parties, and sometimes parties make incorrect transactions even when there is no malicious intent (e.g., using the wrong recipient

account number in an electronic transfer). Some of these issues can be mitigated with good UI designs and identity management (discussed in Section 4.2), but some mistakes, such as making an incorrectly large transfer by fat-fingering an extra zero, can never be entirely eliminated.

4. *Fraud in the Factum*: Parties can be presented with the authorization for a transaction and misled into believing they are taking some other action when they authorize it. Attacks of this sort range from swapping the pages of a paper contract to simulating UI elements.

5. *Fraud in the Inducement*: Parties are sometimes tricked into entering into transactions under false pretenses. For example, a fraudster might pass off a cheap fake as a $10,000 watch, or "sell" a watch stolen from another party. In both cases, the buyer's payment to the seller is intentional, but the overall deal is fraudulent.

Importantly, *none of these patterns* can be reliably detected by any mechanism internal to the CBDC, because the legal validity of the transaction is determined by external facts that are not directly observable by the CBDC's participants.

In all of these cases, existing law typically gives the victim a right to recover from a purposeful wrongdoer. But the law is more complicated on the questions of (a) whether the victim has a right to rescind a transaction not involving fraud, (b) whether this right extends to recover assets from third parties to whom they have been transferred in the interim. These issues often cannot be disentangled from the specifics of the payment system used. Thus, for example, in the United States cash is both fungible and negotiable: if B steals $10,000 from A, A is entitled to recover $10,000 but not the specific bills stolen, and if B then buys and destroys a watch from C with the $10,000, A cannot recover from C at all.

Any CBDC must consider, therefore, not just how it will be designed to limit the opportunities for these incorrect transactions, but how it will recover when such transactions take place. Many decentralized blockchains have taken an extreme "user beware" attitude: all transactions are effectively irrevocable once entered on the blockchain and assets cannot be recovered from an unwilling recipient. This option is not viable for a CBDC intended for mass adoption, and it is worth noting that no existing non-blockchain banking system or payment system receives such treatment under existing law. Nor is it feasible to plan for recovery with the legally compelled cooperation of the recipient: an identity thief could well be an unknown overseas hacker not subject to compulsion from the legal system of the CBDC's jurisdiction.

Instead, the CBDC's administrators must be capable of modifying its state in accordance with property, contract, payment, and banking law. This raises several important subsidiary design questions.

First, the CBDC needs an appropriate governing legal regime. Cash, checks, debit cards, credit cards, wire transfers, private systems such as PayPal and Venmo, and other payment systems all have their own governing laws (typically a mixture of public regulations and private contracts). The specifics of liability for unauthorized transfers and the circumstances under which transactions can be halted, modified, or reversed will need to be worked out by analogy and with careful attention to the technical details of the CBDC.

Second, the CBDC needs an appropriate management infrastructure. Someone will need to verify when a transaction should be modified in accordance with the jurisdiction's law and then make the appropriate changes. This requires a dispute resolution system within the CBDC's administration, an interface to the judicial system capable of authenticating legitimate orders, an interface to other agents capable of giving trusted instructions for transaction modification (such as banks), or some combination of all of the above. This infrastructure will require its own security, auditing, and compliance processes. In a hybrid two-tier design, some of these procedures can be handled by the institutions that layer customer services on top of the payment layer, but some of them will need to be implemented directly against the underlying ledger.

Third, the CBDC needs systems for reporting out its state to appropriate authorities. This may be more than just the state of the transactions that have been entered. The process of determining whether a transaction was properly authorized, for example, may depend on information such as the IP address from which it was requested and on the history of similar attempted transactions. Such information is relevant in litigation and dispute resolution for existing payment systems, and there is no reason to think that a CBDC will be any different. With a blockchain or other public ledger, the authorities can directly inspect its state (although this may fail to capture some details of how users interacted with it). In a hybrid two-tier system, existing reporting systems would largely suffice at the customer layer; the transaction layer would require one if the ledger is not already public.

10.5 Liens

Most kinds of property can be used as collateral for debts. Legally, the creditor is said to hold a *lien* in the property. The debtor remains the owner, but under appropriate circumstances (typically default), the creditor can seize the property and force a sale to help satisfy the debt. Some liens are *possessory*, e.g., a margin loan is collateralized by securities deposited with a broker. Other liens, such as mortgages, are *nonposessory*: the debtor retains possession and control of the property. Some liens are created explicitly by the parties as part of a loan transaction. But others arise by operation of law. For example, unpaid taxes on property may give the government a tax lien against the property, or a person who wins a lawsuit for damages can obtain a judgment lien over the defendant's assets.

Creditors collecting a debt or judgment can typically seize the defendant's property, subject to detailed and jurisdiction-specific rules on what property can be seized and how. Liens give secured creditors priority over other creditors, come with expedited procedures for a creditor to proceed quickly against the property subject to the security interest (e.g., repossessing and foreclosing on a car subject to an unpaid loan is faster and less regulated than seizing a car to pay off an unrelated debt), and are subject to fewer restrictions on what property can be seized (e.g. some states protect a debtor's primary residence from seizure for unsecured debt, but not from mortgage foreclosure) [265]. A closely related concept is *garnishment*, in which a creditor obtains payment of a debt by seizing the debtor's assets from a third party. Garnishment orders can be particularly effective because the third party can hold the property as soon as the debtor acquires it, e.g., when a bank garnishes a parent's wages for payment of a child support order.

The widespread use of liens impacts CBDC design in two important and related ways. First, it raises doctrinal questions of how CBDC accounts and related assets should be treated as collateral. How can liens in them be created, and how can they be repossessed and foreclosed on? (See [266]–[269].) Existing law on security interests varies greatly by type of property, even within a jurisdiction, which means that categorization questions matter greatly. If the default legal regime that would govern CBDC assets is unclear or undesirable, then legislation to establish more appropriate treatment will be necessary. Second, the CBDC's design should facilitate the use of security interests in a manner that integrates smoothly with the rest of the financial and legal system.

It is important to note that while excluding CBDC assets from the lien system is doctrinally possible (almost anything is with appropriate legislation), this likely would be a complete non-starter for many financial institutions. For one thing, CBDC assets which can never be pledged as collateral for loans are worth less to borrowers; businesses which would otherwise be willing to deal in CBDC accounts might avoid them for that reason. Second, the security of secured lending frequently depends on the ability to trace collateral through changes in form. A creditor who holds a lien in the inventory of a farm-equipment dealer would be shocked and outraged if its lien failed to attach to the money the dealer receives in exchange when it sells a tractor out of its inventory. Categorically excluding CBDC assets from being encumbered by liens would give debtors a loophole capable of destroying almost any lien.

Assuming, therefore, that CBDC assets will need to be part of a secured credit system, the following are a few of the regulatory and design considerations involved.

10.5.1 Collection

The CBDC design should provide a mechanism for the satisfaction of debts from CBDC assets. The most basic considerations here are similar to those above: the CBDC should have a management infrastructure that can accept and authenticate instructions from the legal system directing one user's assets to be paid over to another in satisfaction of a debt. In some cases, such as judgment debts, these orders could come directly from a government official: e.g., from a court or from a sheriff levying upon the debtor's property. In others, legal systems provide mechanisms for private repossession: e.g., brokers can unilaterally sell securities held on margin if the debtor fails a margin call. The CBDC should consider whether and how to support these private repossession mechanisms. Whatever mechanisms are in place, the CBDC must be capable of providing properly authenticated documentation that levy or repossession has been made. This is most straightforward in a hybrid two-tier system: the financial institutions that manage customer accounts can freeze and seize accounts as required. In a centralized one-tier ledger, the administrator can do so directly. The absence of an appropriate mechanism in a decentralized blockchain architecture is an argument against such architectures for a CBDC.

Once a creditor repossesses an asset subject to a lien, there are questions about what happens next. Some such assets, such as houses subject to mortgages, are required to be sold at a public auction; in other cases, as under the Uniform Commercial Code, the creditor may follow any "commercially reasonable" procedure to sell the assets. To the extent that a CBDC is fungible and has clearly-defined exchange rates, few such issues are likely to arise in CBDC design. The important part is that the legal system should be able to clearly determine how much of a debt has been satisfied by the sale of collateral.

10.5.2 Locking

One common use case for assets subject to a lien is to prevent the assets from being transferred without the consent of the creditor. The creditor's fear, of course, is that transfer will place the assets beyond its reach, either legally or practically. A CBDC's designers should consider whether this is a use case the CBDC should support. If so, then it requires an appropriate interface to receive and authenticate locking orders. Again, in a hybrid two-tier system, the financial institutions that manage customer accounts have experience dealing with such orders and infrastructure to handle them. A one-tier centralized ledger would require building an analogous infrastructure, while a decentralized ledger would require that creditors have an interface they can use to register their claims in a way that enables them to lock assets under appropriate circumstances.

Forward-looking remedies provide further challenges. Garnishment, for example, can attach to wages *as soon as the debtor becomes entitled to them.* This requires that the appropriate locking be attached to a user's CBDC account, not just to specific CBDC assets. As assets are deposited in the account, they are immediately garnished, before the creditor can deal in them. Note that since garnishment orders are typically not all-or-nothing (e.g. a fixed percentage of wages up to a set total), a CBDC design supporting this use case will need to implement the appropriate logic. In a hybrid two-tier system this logic could be added to existing processes in financial institutions; in a centralized design, it would need to be reimplemented; in a decentralized design, it might need to be hard-wired into the CBDC design in a deep (and technically challenging) way.

10.5.3 Notice

Liens are invisible and intangible. But people considering buying or lending against property want to make sure that there are no liens they don't know about. This raises the question of how to provide effective notice to third parties. (If a CBDC asset is locked, this issue does not arise: the locking itself is an effective form of notice.) Under United States law, the validity of security interests against third parties often depends on "perfection," which roughly requires giving specific statutorily required forms of notice.

A CBDC's designers should give thought to how liens in CBDC assets should be communicated to third parties. In the United States, there are, very roughly, three techniques in widespread use. The first is debtor-specific recording: the creditor files a form, indexed by the name of the debtor, with an appropriate office in the debtor's state. This, for example, is what the Uniform Commercial Code requires for the catch-all category of "general intangibles." The second is asset-specific recording: the creditor files a form with an appropriate office, indexed by a unique identifier for the asset subject to the lien. This, for example, is commonly used for cars (which have unique alphanumeric Vehicle Identification Numbers) and for registered copyrights (which have unique registration numbers). The third, and in some way the most complex, involves possession of the asset by the creditor or an appropriate custodian. For example, a lien on a bank account can be perfected by transferring the account into the name of the creditor. Debtor-specific recording requires the least investment to set up, as the infrastructure is already in place, but does not provide easily searchable information on whether a given CBDC asset is subject to a lien. Involvement of CBDC asset custodians, as in a two-layer or centralized design, requires the most supporting infrastructure, but it also allows these assets to be locked, preventing transactions without appropriate creditor consent [266].

10.6 Tracing

Some kinds of property, such as cash, are regarded as completely fungible. Other kinds, such as ancient art, are regarded as completely unique. (See Section 9.1.2). One important difference along this spectrum is the degree to which the legal system attempts to trace ownership of specific property through multiple hands. Tracing is a way of asserting that one particular aspect of an asset's identity – its transaction history – renders it less than completely fungible. Tracing may be necessary, for example, when the property has been stolen and the original owner claims it from a downstream transferee. It may also be necessary when the property was subject to a lien and the creditor seeks to obtain it from a downstream transferee.

Different CBDC technical designs can facilitate different degrees of traceability, with important implications for their legal treatment. If all assets in the system are globally unique, for example, then perfect tracing is possible and property can in theory be recovered from a remote transferee many steps down the line. In other systems, the interchangeability of assets prevents such perfect tracing. Bitcoin, for example, does not attempt to tag specific transaction outputs with specific transaction inputs. After a series of transactions, it is possible to say that that *some* of this BTC came from *some* of that BTC, but not that *these specific* Bitcoins are exactly the same as *those specific* Bitcoins. Some anonymity-preserving cryptocurrencies, such as Zcash and Monero, are designed to eliminate traceability entirely: assets cannot be identified across transactions. (See Section 6.1.)

Traceability has advantages and disadvantages. It provides simplicity and clarity when unwinding tainted transactions. It also obviates the need for the legal system to apply crude approximations, such as identifying stolen funds *deposited* in an account with the last funds *withdrawn* from that account following the deposit. On the other hand, the impossibility of tracing paradoxically provides clarity for transferees. It means they do not need to investigate the remote provenance of the assets they are receiving for fear that some transaction somewhere far back in the chain of title was tainted. This is one of the chief advantages of cash: except in the most blatant cases, cash is cash and it provides a reliable payment mechanism from the recipient's perspective. CBDC design should consider the advantages and disadvantages of traceability in light of their legal consequences.

10.7 Taxation

The general principles of taxation apply without great difficulty to CBDCs. For example, in computing a person's income from the sale of property, they are typically allowed to deduct the purchase price (or "basis") of an asset from the sale price in computing their gain or loss. Nothing in a CBDC design is likely to disrupt such bedrock principles. Two broad overarching themes, however, are worth consideration by a CBDC designers.

First, tax authorities have confronted the question of how to categorize various digital assets for tax purposes. In the United States, for example, cryptocurrencies like Bitcoin have been treated as "property" rather than as "foreign currency" for income tax purposes [270]. Given the importance of a CBDC, its tax categorization should be made as explicit as possible.

Second, income-based taxation does not attempt to continually mark to market the value of all assets, i.e., impose tax on them based on their current valuation, regardless of whether the owner has actually realized that value by selling them. This would be administratively difficult, could lead to significant errors for assets that do not trade in thick liquid markets, and would be unfair to taxpayers who hold illiquid appreciated assets. Instead, tax is assessed on gain or loss from the change in value of an asset only when it is sold or some other "realization event" occurs (such as the release of a debt). The design of a CBDC should be sensitive to which events and transactions will be regarded as realization events. To the extent that a CBDC is highly liquid and is denominated in, easily interchangeable with, identical to, or replaces a fiat currency, there is no great difficulty of or injustice in frequent realization events. Such events might include the payment of interest on CBDC accounts, the transfer of CBDC from one account to another, or the mining of CBDC by blockchain participants. To the extent that the CBDC is illiquid, only conversions between the CBDC and other property should be deemed realization events.

10.8 Conclusion

Existing legal requirements are easiest to meet in a hybrid two-tier CBDC design, in which banks manage digital wallets for individuals and entities. These financial institutions already have the infrastructure to support oversight and reporting, to freeze and transfer assets when required by law, and to perform extensive customer service. A design in which users directly interact with a CBDC managed by a central bank requires it to take on these functions and to interface extensively with the legal system. A decentralized design in which financial institutions or central bank administrators cannot directly modify the state of CBDC assets would likely require extensive and controversial legal changes.

11 Overview of Libra and Digital Yuan

Two projects have played a central role in catalyzing the global CBDC discussion: Libra and the digital yuan. By examining the designs of these two digital currencies, we see some ways in which the needs for a highly scalable digital currency can be met. With the scale and resources of a powerful group of participants, the Libra Association has set lofty goals for its influence. A stated goal of Libra's digital currency is to give access to the financial system to the world's 1.7 billion unbanked. It hopes to make financial transactions as easy as "sending a message." Although not backed by a central bank, the Libra Association has the resources to disseminate its technology across national borders and influence how digital money is spent globally. With the backing of the Chinese government, the People's Bank of China (PBoC) is poised to be the first large economy to issue a digital currency. It envisions its digital currency as a cash equivalent with the potential to be the first CBDC to gain global traction.

11.1 Libra

Financial model: In 2019, Facebook's announced its intention to issue a cryptocurrency called Libra. While Facebook created Libra, Facebook will not control it. Libra will instead be controlled by the Libra Association, a nonprofit entity based in Switzerland with a governing board of 27 leading corporations in tech, finance, and nonprofit. The Libra Association has identified banking the 1.7 billion globally unbanked, people without access to traditional bank accounts, as a fundamental goal. The Libra Association released its initial white paper in June 2019 and a second, updated white paper in May 2020 detailing their plans for the Libra cryptocurrencies [20].

Libra plans to produce single-currency stablecoins, meaning cryptocurrencies that will exactly track the value of existing fiat currencies. These stablecoins will be tied to reserves of major global currencies (e.g., LibraUSD or ≋USD, LibraEUR or ≋EUR, LibraGBP or ≋GBP, LibraSGD or ≋SGD). Each stablecoin will be fully backed 1:1 by reserves of cash, cash-equivalents, and short term government securities denominated in that currency. This means that to create a new stablecoin, for example 1 new LibraUSD, the association will acquire $1 for their reserve. In order to remove 1 LibraUSD from circulation, the reserve will release $1. With these guidelines for generation and removal, Libra stablecoins will not generate value, rather they will be digital representations of existing fiat currencies held in the Libra reserve.

As central banks begin to issue CBDCs, Libra hopes to integrate them directly into the Libra network. Libra will also maintain a capital buffer, in addition to the reserve of circulating Libra stablecoins, in order to ensure solvency. Libra stablecoins will be minted and burned by the reserve based on demand, with supply expanding and contracting based on the market for each Libra stablecoin.

The Libra Association will also create a platform-specific cryptocurrency called the ≋LBR. It will be a digital composite of the single-currency stablecoins offered, set at a fixed ratio. The ≋LBR will be administered by a smart contract. LBR is intended for use in efficient cross-border settlement and as a low-volatility option for those in nations that do not yet have a single currency Libra stablecoin available. Because it is made up of single-currency Libra stablecoins, each fully backed by reserves, ≋LBR will also be fully backed by reserves.

Conversation from ≋LBR and Libra stablecoins into fiat currency will be handled by third party financial institutions called VASPs (Virtual Asset Service Providers), who will interact with end users. Wallets belonging to users other than known financial institutions and VASPs are referred to as "unhosted wallets." Unhosted wallets are supported, but with tight controls (transaction limits, maximum balance enforced by the protocol). Their aim is to facilitate Libra participation for users who may be unable to interact with the system via a VASP.

Single currency stablecoins predate Libra. Tether (USDT), a stablecoin pegged to the US dollar, currently trades on over 100 cryptocurrency exchanges. Like Libra, it is controlled by a central party that pegs its value to USD and backs each USDT with $1 reserve. Tether's reserves are different from Libra's in that they (controversially) allow inclusion of short term loans from third-parties in addition to cash and cash equivalents. Tether has also expanded beyond US dollar stablecoins, now offering stablecoins for additional assets including gold, the Chinese Yuan, and the Euro [271].

Technical foundations: The Libra system will use a fully permissioned, Byzantine Fault Tolerant (BFT) ledger / blockchain that relies on open-source software. Libra does not plan to transition to a permissionless system. The stated design goal for the system is to "serve as a foundation for financial services, including a new global payment system that meets the daily financial needs of billions of people." To achieve this goal, Libra prioritizes flexibility, security, and scalability to billions of accounts in its design. Libra will support programs written in its bespoke Move programming language.

The Move programming language is designed to implement custom transaction logic and smart contracts on the Libra blockchain. Its goals are safety and security, its design explicitly informed by past security incidents involving smart contracts, including those discussed in section 7. Move includes first-class support for operations on currency and tokens and regulatory compliance features.

Initially, only the Libra Association will be able to publish smart contracts that interact directly with the payment system. Over time, third parties will be able publish smart contracts. Libra's (BFT) consensus protocol, called LibraBFT, a variant of Hotstuff [28], is designed to facilitate high transaction throughput and low latency. As a permissioned system, it will require relatively little energy—far less than Proof of Work. Its security relies on the standard BFT assumption that fewer than 1/3 of validator nodes, the machines that maintain the ledger, are compromised.

Validators will be approved / permissioned by the Libra Association. Transactions are finalized when approved by a quorum of validators, and confirmed transactions are final and visible on the ledger. Thanks to its use of a publicly verifiable ledger, Libra will be fully auditable by law enforcement, regulators, and users, meaning that anyone can view an authoritative sequence of all processed transactions. Rather than grouping transactions into blocks like previous blockchains (Bitcoin, Ethereum, etc.), the Libra blockchain will be structured as one continuous data structure.

11.2 The digital yuan

China's central bank, the People's Bank of China (PBoC) has pursued creation of a CBDC more actively than any other global economic power. They are the first major economy to pilot a sovereign digital currency. They have publicly released very little about their digital currency, and limited technical information is available since the PBoC has not publicly released a whitepaper. Therefore, the information below is based on a combination of news reports, official statements, and analysis of Chinese patents filed for technologies that we conjecture are related to CBDC planning and may yield insight into the design choices under consideration.

Background: The PBoC has named their CBDC the Digital Currency for Electronic Payments (DC/EP). As implied by the name, this digital currency will be used for some payments in lieu of traditional fiat. The PBoC formed a research team to explore how to issue a "legal digital tender" in 2014 [272]. One of the goals of this digital currency was to internationalize China's fiat currency, the RMB [273]. This research group was expanded and formalized into the Digital Currency Research Institute in 2017, with the objective of conducting research and technical trials for a digital currency. The Chinese Agricultural bank began testing a wallet application for the digital currency internally in April 2020 [2]. The mobile payment platform Alipay has also filed patents related to its role as a likely secondary issuer of DC/EP [274].

System overview: The DC/EP is expected to be centrally issued and widely available. The PBoC envisions the DC/EP as a replacement for cash and with equal status as a legal tender. The former head of the PBoC's Digital Currency Research Institute described that the DC/EP would be based on the model: "one coin, two repositories, three centers." "One coin" is the DC/EP, the "two repositories" lie in the central bank as well as the commercial banks who will distribute the digital currency and individual wallets; "three centers" refers to the data centers which will perform authentication, registration, and big data analysis [272].

According to Fan Yifei, the Deputy Governor of the PBoC, the system should operate in two tiers with two distinct layers of functionality: interaction with commercial banks and token-based interactions [275]. The PBoC is expected to issue and redeem DC/EP via large, commercial banks. The DC/EP would will be token based, with commercial banks and financial institutions circulating the tokens. This structure is similar to the way fiat is currently handled by central banks, with a two-tiered system in which central banks issue currency and distribute it to financial institutions who manage user interactions [276]. By leaving user-facing activities to banks, the DC/EP will avoid disintermediating the financial system and increasing the responsibilities and risk exposure of the central bank [275].

DC/EP will earn interest only if it is moved from the digital wallet into a deposit account, where it can be used for payment only through a bank card linked to that particular deposit account. Its two-tier structure will permit application of existing monetary policy tools [272]. DC/EP will make use of non-fungible tokens: Each coin will have an individual denomination and serial number [277].

To store DC/EP, users will hold digital wallets with digital ledgers, protected by cryptography and consensus protocols [278]. The DC/EP wallet currently undergoing trials is available as a smartphone application for individual users. It offers user-to-user payments by QR code; payments can also be initiated by tapping smartphones with another user [2].

11.3 What patent filings reveal about the digital yuan

As of early 2020, the PBoC has filed more than 80 patent applications related to digital currency. These patent applications may be viewed as falling into four categories: "digital currency management, circulation and interbank settlement; digital currency wallets; processing payments and deposits; and distributed ledger transactions and technology" [279]. On the whole, these patents suggest a system under very tight control by the central bank, more so than is consistent with the banking system in Western nations. They also place a strong emphasis on compatibility with existing banking infrastructure; for example, some PBoC patent applications describe technical mechanisms for users to make deposits with their existing banks and then exchange deposited money for DC/EP.

Alipay, a mobile payment platform established in China by Alibaba, has also filed several patent applications explicitly related to the DC/EP. These filings include interesting capabilities and architectural nuances relating to the financial institutions managing the second tier of the DC/EP system [274], and are not discussed in previous treatments of DC/EP of which we're aware, e.g., [279].

Initially, the PBoC was interested in embracing innovative financial tools, particularly smart contracts and a distributed ledger, as expressed by the former head of the Digital Currency Research Institute, Yao Qian [280]. However, according to Fan Yifei, the Deputy Governor of the PBoC, that interest is tempered by concerns about undermining its cash-like status by supporting smart contracts [281]. Given this tension, the portfolio of patent applications we review here should be viewed as a spectrum of technologies that the PBoC may someday choose to develop rather than as a preview of the DC/EP at its release.

Rather than providing a comprehensive survey, we highlight some of the most interesting and salient features of the relevant PBoC and Alipay patent filings.

Anonymity: PBoC patent applications support a system design in which person-to-person or person-to-business transfers can be anonymous at the user level. Commercial banks in the first layer, however, would collect identifying information about transacting parties that the central bank could also access. This tiered anonymity was referred to as "controllable anonymity," by Mu Changchun, the head of the PBoC Institute for Digital Currency. Users enjoy some degree of anonymity with respect to other users; banks, however, have a mechanism to deanonymize suspicious transactions, in order to combat money laundering and the financing of terrorism [282]. A patent application filed by Alipay, which uses the same phrase, "controllable anonymity," describes a mechanism for anonymity in user-to-user transactions, but does not provide any support for anonymity for the user from her financial institution. User-to-user anonymity could possibly extend to transactions between users in different banks [283].

Two other patent applications [284], [285] filed by PBoC in 2017 describe a cryptographic scheme—similar to Greg Maxwell's confidential transactions [223]—that hides the amount of currency in individual accounts as well as the amount of currency transferred in a given transaction from all parties but the participants in a transaction.

None of these patent applications, however, describes technology to hide transaction graphs, i.e., the pseudonyms of participants in transactions are recorded on the ledger. This means that the ledger *must be private to the authorities managing the system*. Otherwise users can deanonymize other users using the information revealed in the transaction graphs, as discussed in section 6.1.

Account control: A recent patent application filed by Alipay describes a command-and-control architecture in which regulators can directly, instantaneously, and unilaterally freeze users' funds. This account control could change the type of account belonging to a particular user, stop the flow of money in or out of a particular account, or freeze part or all of the DC/EP in the account [286]. As envisaged in this patent application, accounts are categorized in four levels, with the level of the account determined based on the amount and anticipated kinds of use, as well as the type of identifying information a user provides to open the account. Higher-level accounts offer more flexibility to their holders. For example, a user can apply for either an "anonymous" account or an account associated with his or her real name. "Anonymous" accounts (which in fact require some identifying information, like an email address or phone number, upon registration) are "low-level" in the sense that they provide only minimal functionality [277], such as strict balance limits.

Novel tools: PBoC patent propose technology to adjust the supply of DC/EP using an algorithm tracking certain triggers, like loan interest rates [287]. They also lay the groundwork for digital currency smartcards and digital wallets that a user can link directly to conventional bank accounts [288]. Additionally, the PBoC filed a patent application which specifies means for the central bank to activate tokens it distributes to banks with designated interest rates based on market conditions; these interest rates functionally tag coins with repayment conditions when they are used in loans [280].

Uses of secure hardware: As discussed in section 8, the role of secure hardware in digital currencies is a controversial and often misunderstood topic. However, recent patent applications filed by Alipay reveal a potential interest in embracing secure hardware, in particular Trusted Execution Environments (TEEs), in critical operations such as currency issuance. [289], [290] describes a TEE-based implementation of the two-layer issuance architecture. The central bank may deploy a “front-end encryption machine” (FEM), potentially realized by a TEE, at second-layer operators. The TEE functions in effect as a delegate of the central bank. The FEM stores the central bank’s secret keys and is invoked by operators to issue and exchange digital currencies. To provide more detail, the second-layer issuance works as follows. First, an operator deposits a 100% reserve at the central bank, in exchange for a receipt in the form of an “encrypted string.” The operator then feeds the FEM with the receipt and receives digital currency tokens of equivalent value. Another use of the FEM is to split a digital currency token of a large value into multiple ones with smaller denominations.

More commonplace applications of TEEs are also mentioned in these patent applications. One patent application [221] describes a digital wallet design that uses TEEs to protect users’ private keys and perform *offline transactions* when the sender and/or receiver is not connected to the ledger. The patent implicitly assumes a perfectly secure TEE, however, and does not address the possibility of TEE compromise or failure. For example, since private keys are only accessible to the TEE, availability failures (e.g., permanent malfunctions) could lead to loss of funds. TEE can support flexible access control policies (e.g., [155]) capable of remedying such problems, but the patent filing does not consider this important direction.

12 Summary Position

Our explorations in this paper suggest a number of topics and issues that deserve special consideration by CBDC designers.

Monetary policy considerations: The issuance of CBDC will not in any way mask underlying weaknesses in central bank credibility or other issues such as fiscal dominance that affect the value of cash. In other words, digital central bank money is only as strong and credible as the central bank that issues it. In considering a shift to digital forms of retail central bank money, it is important to keep in mind that the transitional risks could be higher in the absence of stable macroeconomic and structural policies, including sound regulatory frameworks that are agile enough to be able to recognize and deal with financial risks created by new types of financial intermediaries.

It should also be recognized, notwithstanding the potential benefits, there are many unanswered questions about how the new financial technologies could affect the structure of financial institutions and markets. Questions also abound about whether retail CBDC will in any significant way affect monetary policy implementation and transmission. These uncertainties suggest a cautious approach to embracing the concept of CBDC.

Ledger infrastructure: We discuss a range of architectural options for the digital ledger underpinning a CBDC. Our expectation is that central banks will wish to retain tight control over currency issuance and transaction processing, including the ability to alter or reverse transactions.

Such control is especially important given the historically demonstrated risks of catastrophic error in ledger-based systems, and existing legal requirements for handling error and fraud. In principle, tight ledger control is possible for any type of ledger, even public (“permissionless”) ones, as central bank privileges can be hardwired in, but in practice permissioned ledger systems, i.e., those limited to predesignated entities, or centralized systems are more suitable choices. As multi-entity permissioned systems have not seen extensive deployment yet—their planned use in Libra constituting a significant technical experiment—our expectation is that central banks will opt for centralized CBDCs, and indeed the digital yuan appears to be embracing such an approach.

Central banks may wish to consider use of *authenticated data structures* (ADSs) as an extension for centralized CBDC deployments. An ADS may be thought of as a highly compressed version (“digest”) R of the ledger at a given time. The central bank can distribute this digest R publicly without revealing ledger contents. It can prove the inclusion of particular transactions in the ledger with reference to R alone. It can also use R to demonstrate that it is not “forking,” that is, showing different ledger contents / balances to different entities. Forking could occur as a result of operator malfeasance or a breach, so the ability to prove that forking has not taken place can strengthen users’ confidence in the system.

Wallets and funds / key custody: One of the major challenges in successful democratization of cryptocurrency has arisen around the usability of wallets, and in particular the problem of *key management.* To authenticate users’ transactions, that is, create strong evidence that they are submitted legitimately by holders of the relevant funds, it is necessary to *digitally sign* them. Digital signatures are a powerful cryptographic tool used in all modern computing infrastructure, but require the use of a *secret key.* Cryptocurrency users have found protecting and backing up keys to be unduly burdensome, and the result has been a heavy reliance on service providers that hold users’ assets and act effectively like financial intermediaries. While CBDCs are likely to rely primarily on financial intermediaries[17], it is unclear how CBDCs can significantly advance the explicitly stated goal for CBDCs of financial inclusion should consumers need to engage with financial institutions.[18] Workable approaches to custody of funds and/or secret keys will be of pivotal importance in a CBDC.

[17] It appears that some designs, such as the digital yuan, may offer limited support for user-administered accounts.

[18] CBDCs would, however, make it easy to prepopulate individual accounts with funds, which would be an important first step in enrolling consumers in the financial system.

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

Privacy: Should a CBDC maintain the account balances of individuals on the ledger, which would seem to be a prerequisite for a retail CBDC, then *privacy* will become an issue of major importance. (The same is true for alternative representations of value, such as digital banknotes.) While there are cryptographic systems for maintaining transactional privacy in such settings, they are complex and costly, and unlikely to scale to meet the requirements of a CBDC in the short-to-medium term. One critical observation is that *pseudonymous* accounts, i.e., accounts in which account holders' names are kept secret, *offer only weak privacy.* Under many circumstances, as the history of cryptocurrencies shows, it would be possible to *deanonymize* accounts. In a practical sense, therefore, a CBDC will *reveal significantly more information about individuals' transactions to central banks than existing systems do.* This observation strongly motivates considered technical and legal confidentiality protections for ledger contents.

Opportunities for innovation: On the positive side, we believe there is a rich range of opportunities for innovation in a CBDC beyond mere reduction of frictions in transaction processing. Some derive from the unprecedented transparency a CBDC would afford regulators, including an ability to obtain a panoramic yet fine-grained view of global spending in an economy. These opportunities would also include new monetary policy levers, such as the ability of central banks to institute negative nominal interest rates, create currency with time-limits or other spending conditions (e.g., required spending on durable goods) in order to create highly targeted monetary interventions in a national economy.

Opportunities for novel financial technologies may be best captured with CBDC support for smart contracts, which would offer a flexible means of defining policies. Smart contracts would also offer opportunities for the creation of new types of financial instruments; in cryptocurrency systems, they have led to the creation of instruments so novel (e.g., "flash loans") that they have no direct analogs in the existing financial system. Given the historically demonstrated hazards of smart contract bugs (e.g., The DAO), however, software assurance and oversight will be of paramount importance.

Secure hardware: We also believe that central banks should explore the use of secure hardware to strengthen elements of a CBDC system. While vulnerabilities have surfaced in recently produced secure hardware, suggesting that it should not be used in mission-critical subsystems, there are a number of places in which it can serve as an adjunct to strengthen or harden systems in which it is deployed. We describe several such opportunities, such as improving privacy through defense-in-depth, i.e., as an added protective layer, improving compliance enforcement by constraining system use according to regulatory rules, and protecting the wallets of individual users.

Two-layer architectures: The publicly revealed plans or explorations of central banks to date focus on two-layer CBDC architectures. In such architectures, existing non-governmental financial institutions or payment application providers—dubbed

"Payment Interface Providers" (PIPs) in [10]—constitute a second layer on top of the CBDC, serving as the main interface between users and the CBDC. Two-layer architectures align closely with current customer service delivery models and compliance mechanisms for anti-money-laundering and countering the funding of terrorism (AML/CFT) laws, and would also appear to have the merit of avoiding disruptive disintermediation of the existing banking system.

It is important to note that a two-layer system would not remedy the privacy concerns associated with representation of individuals' accounts (or banknotes) in the CBDC. It could also introduce additional complications. For example, should smart contracts be deployed by by PIPs, rather than directly on the CBDC, systemic risks could escape the observation and control of regulators, and different PIPs' deployments could be mutually incompatible, creating patchwork interfaces to the CBDC. Conversely, tight control of smart contract environments by a central bank could stifle innovation. Establishment of basic technical and operating standards by the central bank could prove fruitful middle ground.

In summary, the benefits and risks of CBDC are complex, encompassing an interplay among financial, legal, and technical considerations. Each country will have to take into account its specific circumstances and initial conditions before deciding whether the potential benefits of introducing a CBDC outweigh the possible costs.

Acknowledgments

The authors wish to thank IC3's industry partners for their support of this work. Thanks also to Jim Ballingall for helpful comments. Ittay Eyal was partially funded by ISF (1641/18) and BSF grants. Giulia Fanti was partially funded by NSF grant CIF-1705007 and ARO grant W911NF17-S-0002. Bryan Ford was partially funded by ONR grant N00014-19-1-2361 and the AXA Research Fund. Ari Juels was partially funded by NSF grants CNS-1704615 and CNS-1933655. Sarah Meiklejohn was partially funded by EPSRC Grant EP/N028104/1. Andrew Miller was partially funded by NSF grant CNS-1943499.

References

[1] C. Boar, H. Holden, and A. Wadsworth, *Impending arrival – a sequel to the survey on central bank digital currency*, https://www.bis.org/publ/bppdf/bispap107.pdf, BIS Publication 107, 2020.

[2] W. Zhao, *Chinese state-owned bank offers test interface for pboc central bank digital currency*, Apr. 2020. [Online]. Available: https://www.coindesk.com/chinese-state-owned-bank-offers-test-interface-for-pboc-central-bank-digital-currency.

[3] V. Bharathan, "Digital dollar project in light of recent congressional hearings", *Forbes*, Jun 29, 2020.

[4] Y. Mersch, "An ECB digital currency – a flight of fancy?", Speech at Consensus 2020 virtual conference, 11 May 2020. [Online]. Available: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200511~01209cb324.en.html.

[5] Sveriges Riksbank, *The Riksbank to test technical solution for the e-krona*, Riksbank press release, 20 Feb. 2020.

[6] J. Light, B. Bain, and O. Kharif, "Facebook weighs Libra revamp to address regulatory concerns", *Bloomberg News*, 3 March 2020.

[7] V. Mislos, "CBDC 'not a reaction' to Libra despite study confirming consumer benefits of stablecoins", *International Business Times*, 26 June 2020.

[8] M. Ricks, J. Crawford, and L. Menand, "Central banking for all: A public option for bank accounts", *The Great Democracy Initiative Report*, June 2018.

[9] H. Jones, "Pandemic pushes central bank digital currencies into top gear", *Reuters Technology News*, 11 June 2020.

[10] "Central Bank Digital Currency: Opportunities, challenges and design", 12 March 2020. [Online]. Available: https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper.

[11] M. Kumhof and C. Noone, "Central bank digital currencies—design principles and balance sheet implications", Bank of England working paper No. 725, 2018.

[12] Q. Yao, "A systematic framework to understand central bank digital currency", *Science China Information Sciences*, vol. 61, no. 3. Article 033101, 2018.

[13] O. Bjerg, "Designing new money-the policy trilemma of central bank digital currency", CBS Working Paper, June 2017.

[14] M. D. Bordo and A. T. Levin, "Central bank digital currency and the future of monetary policy", National Bureau of Economic Research Working Paper No. 23711, 2017.

[15] K. S. Rogoff, *The curse of cash: How large-denomination bills aid crime and tax evasion and constrain monetary policy.* Princeton University Press, 2017.

[16] B. Mishra and E. Prasad, "A simple model of a central bank digital currency", Manuscript, Cornell University, 2019.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Tech. Rep., 2008.

[18] V. Buterin, *A next generation smart contract & decentralized application platform*, 2013. [Online]. Available: https://www.ethereum.org/%20pdfs/EthereumWhitePaper.pdf/.

[19] M. Lokhava, G. Losa, D. Mazières, G. Hoare, N. Barry, E. Gafni, J. Jove, R. Malinowsky, and J. McCaleb, "Fast and secure global payments with stellar", in *Proceedings of the 27th ACM Symposium on Operating Systems Principles*, 2019, pp. 80–96.

[20] *Libra white paper: Blockchain, association, reserve*, Apr. 2020. [Online]. Available: https://libra.org/en-US/white-paper/.

[21] Amazon AWS, *Amazon quantum ledger database*. [Online]. Available: https://aws.amazon.com/qldb/.

[22] L. Lamport, "Time, clocks, and the ordering of events in a distributed system", in *Concurrency: the Works of Leslie Lamport*, 2019, pp. 179–196.

[23] ——, "The part-time parliament", *ACM Transactions on Computer Systems*, vol. 16, no. 2, pp. 133–169, 1998.

[24] ——, "Fast Paxos", *Distributed Computing*, vol. 19, no. 2, pp. 79–103, 2006.

[25] M. Castro and B. Liskov, "Practical byzantine fault tolerance", in *OSDI*, vol. 99, 1999, pp. 173–186.

[26] I. Abraham, G. Chockler, I. Keidar, and D. Malkhi, "Byzantine disk Paxos: Optimal resilience with Byzantine shared memory", *Distributed Computing*, vol. 18, no. 5, pp. 387–408, 2006.

[27] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm", in *2014 USENIX Annual Technical Conference (USENIX ATC 14)*, 2014, pp. 305–319.

[28] M. Yin, D. Malkhi, M. K. Reiter, G. Golan-Gueta, and I. Abraham, "Hotstuff: BFT consensus with linearity and responsiveness", in *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC 2019*, P. Robinson and F. Ellen, Eds., ACM, 2019, pp. 347–356. [Online]. Available: https://doi.org/10.1145/3293611.3331591.

[29] M. Garcia, A. Bessani, I. Gashi, N. Neves, and R. Obelheiro, "Analysis of operating system diversity for intrusion tolerance", *Software: Practice and Experience*, vol. 44, no. 6, pp. 735–770, 2014.

[30] L. Breidenbach, P. Daian, F. Tramer, and A. Juels, "Enter the hydra: Towards principled bug bounties and exploit-resistant smart contracts", in *27th USENIX Security Symposium*, Aug. 2018.

[31] R. Tamassia, "Authenticated data structures", in *Proceedings of the 11th Annual European Symposium on Algorithms*, vol. 2832, Springer, 2003, pp. 2–5.

[32] S. Crosby and D. Wallach, "Efficient data structures for tamper-evident logging", in *Proceedings of the 18th USENIX Security Symposium*, 2009.

[33] A. Eijdenberg, B. Laurie, and A. Cutter, *Verifiable data structures*, github.com/google/trillian/blob/master/docs/VerifiableDataStructures.pdf, 2015.

[34] L. Reyzin, D. Meshkov, A. Chepurnoy, and S. Ivanov, "Improving authenticated dynamic dictionaries, with applications to cryptocurrencies", in *Proceedings of Financial Cryptography and Data Security*, 2017.

[35] L. Chuat, P. Szalachowski, A. Perrig, B. Laurie, and E. Messeri, "Efficient gossip protocols for verifying the consistency of certificate logs", in *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS)*, 2015.

[36] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman, "CONIKS: Bringing key transparency to end users", in *Proceedings of the 24th USENIX Security Symposium*, 2015.

[37] A. Tomescu and S. Devadas, "Catena: Efficient non-equivocation via Bitcoin", in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2017.

[38] M. Al-Bassam and S. Meiklejohn, "Contour: A practical system for binary transparency", in *Proceedings of the 2nd International Workshop on Cryptocurrencies and Blockchain Technology (CBT)*, 2018.

[39] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, P. Jovanovic, L. Gasser, N. Gailly, I. Khoffi, and B. Ford, "Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning", in *37th IEEE Symposium on Security and Privacy*, May 2016.

[40] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Large-scale Network Attacks on Cryptocurrencies", *38th IEEE Symposium on Security and Privacy*, May 2017.

[41] B. Ford, "Apple, FBI, and Software Transparency", *Freedom to Tinker*, Mar. 2016.

[42] P. Bright, *Independent Iranian hacker claims responsibility for Comodo hack*, Mar. 2011. [Online]. Available: www.wired.com/2011/03/comodo_hack/.

[43] J. Menn, *Key Internet operator VeriSign hit by hackers*, Feb. 2012. [Online]. Available: www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202.

[44] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies", in *Proceedings of NDSS*, 2016.

[45] J. Kwon, "Tendermint: Consensus without mining", *Draft v. 0.6, fall*, vol. 1, no. 11, 2014.

[46] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing", in *25th USENIX Security Symposium (USENIX Security 16)*, 2016.

[47] M. Baudet, A. Ching, A. Chursin, G. Danezis, F. Garillot, Z. Li, D. Malkhi, O. Naor, D. Perelman, and A. Sonnino, "State machine replication in the Libra blockchain", *The Libra Assn., Tech. Rep*, 2019.

[48] G. Andresen, *March 2013 chain fork post-mortem*. [Online]. Available: https://en.bitcoin.it/wiki/BIP_0050.

[49] B. Community, *2015 BIP66 blockchain fork*. [Online]. Available: https://en.bitcoin.it/wiki/Softfork#2015_BIP66_Blockchain_Fork.

[50] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability", pp. 566–583, 2020.

[51] Y. Doweck and I. Eyal, "Multi-party timed commitments", *arXiv preprint arXiv:2005.04883*, 2020. [Online]. Available: https://arxiv.org/abs/2005.04883v2.

[52] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail", in *Annual International Cryptology Conference*, Springer, 1992, pp. 139–147.

[53] M. Jakobsson and A. Juels, "Proofs of work and bread pudding protocols", in *Secure information networks*, Springer, 1999, pp. 258–272.

[54] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable", in *Financial Cryptography and Data Security*, 2014.

[55] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in Bitcoin", in *Financial Cryptography and Data Security*, 2016.

[56] R. Pass and E. Shi, "Fruitchains: A fair blockchain", in *Proceedings of the ACM Symposium on Principles of Distributed Computing*, 2017, pp. 315–324.

[57] C. Hou, M. Zhou, Y. Ji, P. Daian, F. Tramer, G. Fanti, and A. Juels, "Squirrl: Automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning", *arXiv preprint arXiv:1912.01798*, 2019.

[58] R. B. Zur, I. Eyal, and A. Tamar, "Efficient MDP analysis for selfish-mining in blockchains", *arXiv preprint arXiv:2007.05614*, 2020. [Online]. Available: https://arxiv.org/abs/2007.05614.

[59] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels, "BDoS: Blockchain denial of service", in *Proceedings of the 2020 ACM SIGSAC conference on Computer and Communications Security*, 2020.

[60] A. Miller, E. Shi, A. Juels, B. Parno, and J. Katz, "Permacoin: Repurposing Bitcoin work for data preservation", in *Proceedings of the IEEE Symposium on Security and Privacy*, San Jose, CA, USA: IEEE, 2014. [Online]. Available: http://research.microsoft.com/apps/pubs/default.aspx?id=217984.

[61] F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. Van Renesse, "REM: Resource-efficient mining for blockchains", in *26th USENIX Security Symposium (USENIX Security 17)*, 2017, pp. 1427–1444.

[62] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol", in *Annual International Cryptology Conference*, Springer, 2017, pp. 357–388.

[63] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies", in *Proceedings of the 26th Symposium on Operating Systems Principles*, 2017, pp. 51–68.

[64] I. Tsabary, A. Spiegelman, and I. Eyal, "Heb: Hybrid expenditure blockchain", *arXiv*, arXiv–1911, 2019.

[65] B. Ford and R. Böhme, *Rationality is Self-Defeating in Permissionless Systems*, Sep. 2019.

[66] J. Kroll, I. Davey, and E. Felten, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries", in *Workshop on Economics and Information Security (WEIS)*, Washington, DC, 2013.

[67] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency", in *The Economics of Information Security and Privacy*, R. Böhme, Ed., Springer, 2013, pp. 135–156.

[68] J. Bonneau, "Hostile blockchain takeovers (short paper)", in *Financial Cryptography and Data Security Workshops*, A. Zohar, I. Eyal, V. Teague, J. Clark, A. Bracciali, F. Pintore, and M. Sala, Eds., ser. Lecture Notes in Computer Science, vol. 10958, Springer, 2018, pp. 92–100.

[69] A. Judmayer, N. Stifter, A. Zamyatin, I. Tsabary, I. Eyal, P. Gazi, S. Meiklejohn, and E. Weippl, *Pay-to-win: Incentive attacks on proof-of-work cryptocurrencies*, Cryptology ePrint Archive, Report 2019/775, 2019.

[70] E. Attah, *Five most prolific 51.1667em% attacks in crypto: Verge, Ethereum Classic, Bitcoin Gold, Feathercoin, Vertcoin*, Cryptoslate.com, https://tinyurl.com/yyrvxyoh, Apr. 2019.

[71] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol.", in *NSDI*, 2016.

[72] R. Pass and E. Shi, "Thunderella: Blockchains with optimistic instant confirmation", in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2018, pp. 3–33.

[73] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, “Prism: Deconstructing the blockchain to approach physical limits”, in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 585–602.

[74] H. Yu, I. Nikolic, R. Hou, and P. Saxena, “Ohie: Blockchain scaling made simple”, in *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 112–127.

[75] Y. Sompolinsky and A. Zohar, “PHANTOM and GHOSTDAG: A scalable generalization of nakamoto consensus”, *IACR Cryptology ePrint Archive, Report 2018/104*, 2018. [Online]. Available: https://eprint.iacr.org/2018/104.

[76] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding”, in *IEEE Symposium on Security and Privacy (SP)*, IEEE, 2018, pp. 19–34.

[77] M. Zamani, M. Movahedi, and M. Raykova, “Rapidchain: A fast blockchain protocol via full sharding.”, *IACR Cryptology ePrint Archive*, vol. 2018, p. 460, 2018.

[78] A. Manuskin, M. Mirkin, and I. Eyal, “Ostraka: Secure blockchain scaling by node sharding”, in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&B)*, IEEE, 2020.

[79] P. Thompson, “Most significant hacks of 2019 — new record of twelve in one year”, Jan. 2020. [Online]. Available: https://cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year.

[80] SelfKey, *A comprehensive list of cryptocurrency exchange hacks*, Feb. 2020. [Online]. Available: https://selfkey.org/list-of-cryptocurrency-exchange-hacks/.

[81] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: A survey”, *Cryptography*, vol. 2, no. 1, Jan. 2018.

[82] S. Srinivas, D. Balfanz, E. Tiffany, A. Czeskis, and F. Alliance, “Universal 2nd factor (u2f) overview”, *FIDO Alliance Proposed Standard*, pp. 1–5, 2015.

[83] N. Poh, C. H. Chan, J. Kittler, S. Marcel, C. M. Cool, E. A. Rúa, J. L. A. Castro, M. Villegas, R. Paredes, V. Štruc, N. Pavešić, A. A. Salah, H. Fang, and N. Costen, “An evaluation of video-to-video face verification”, *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, Dec. 2010.

[84] R. Chesney and D. K. Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security”, *California Law Review*, Jul. 2018.

[85] D. Mack, “This PSA About Fake News From Barack Obama Is Not What It Appears”, *Buzzfeed News*, Apr. 2018.

[86] T. C. King, N. Aggarwal, M. Taddeo, and L. Floridi, "Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions", *Science and Engineering Ethics*, vol. 26, pp. 89–120, Feb. 2020.

[87] M. R. Anderson, "Twenty years on from Deep Blue vs Kasparov: How a chess match started the big data revolution", *The Conversation*, May 2017. [Online]. Available: https://theconversation.com/twenty-years-on-from-deep-blue-vs-kasparov-how-a-chess-match-started-the-big-data-revolution-76882.

[88] J. Markoff, "Computer wins on 'Jeopardy!': Trivial, it's not", *The New York Times*, Feb. 2011. [Online]. Available: https://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html.

[89] S. Borowiec, "Alphago seals 4-1 victory over Go grandmaster Lee Sedol", *The Guardian*, Mar. 2016. [Online]. Available: https://www.theguardian.com/technology/2016/mar/15/googles-alphago-seals-4-1-victory-over-grandmaster-lee-sedol.

[90] F.-Y. Wang, J. J. Zhang, X. Zheng, X. Wang, Y. Yuan, X. Dai, J. Zhang, and L. Yang, "Where does AlphaGo go: From Church-Turing thesis to AlphaGo thesis and beyond", *IEEE/CAA Journal of Automatica Sinica*, vol. 3, no. 2, Apr. 2016.

[91] G. Ye, Z. Tang, D. Fang, Z. Zhu, Y. Feng, P. Xu, X. Chen, and Z. Wang, "Yet another text Captcha solver: A generative adversarial network based approach", in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Jan. 2018, pp. 332–348.

[92] J. Dzieza, "Why CAPTCHAs have gotten so difficult", *The Verge*, Feb. 2019. [Online]. Available: https://www.theverge.com/2019/2/1/18205610/google-captcha-ai-robot-human-difficult-artificial-intelligence.

[93] M. Read, "How Much of the Internet Is Fake? Turns Out, a Lot of It, Actually.", *New York Magazine*, Dec. 2018.

[94] A. Berger, *Bot vs. Bot: Will the Internet Soon Be a Place Without Humans?*, Singularity Hub, Jul. 2018.

[95] M. Latah, *The art of social bots: A review and a refined taxonomy*, May 2019. [Online]. Available: https://arxiv.org/pdf/1905.03240.pdf.

[96] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: using hard AI problems for security", in *Eurocrypt*, 2003.

[97] C. Doctorow, "Solving and creating CAPTCHAs with free porn", *Boing Boing*, Jan. 2004. [Online]. Available: http://www.boingboing.net/2004/01/27/solving_and_creating.html.

[98] L. Kang and J. Xiang, "CAPTCHA phishing: A practical attack on human interaction proofing", in *Information Security and Cryptology (Inscrypt)*, Dec. 2009.

[99] B. Krebs, *Virtual sweatshops defeat bot-or-not tests*, Krebs on Security, Jan. 2012. [Online]. Available: `https://krebsonsecurity.com/2012/01/virtual-sweatshops-defeat-bot-or-not-tests/`.

[100] R. Brandom, "This is why you shouldn't use texts for two-factor authentication", *The Verge*, Sep. 2017. [Online]. Available: `https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin`.

[101] G. Tu, C. Li, C. Peng, Y. Li, and S. Lu, "New security threats caused by IMS-based SMS service in 4G LTE networks", in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, Oct. 2016, pp. 1118–1130.

[102] A. Bhatia and J. Bhabha, "India's Aadhaar scheme and the promise of inclusive social protection", *Oxford Development Studies*, vol. 45, no. 1, pp. 64–79, Jan. 2017.

[103] B. Chaudhuri and L. König, "The Aadhaar scheme: a cornerstone of a new citizenship regime in India?", *Contemporary South Asia*, vol. 26, no. 2, pp. 127–142, Sep. 2017.

[104] R. Abraham, E. S. Bennett, R. Bhusal, S. Dubey, Q. (Li, A. Pattanayak, and N. B. Shah, "State of Aadhaar Report 2017-18", IDinsight, Tech. Rep., May 2018.

[105] B. Schneier, "Tigers use scent, birds use calls – biometrics are just animal instinct", *The Guardian*, Jan. 2009.

[106] A. Chanthadavong, "Biometrics: The password you cannot change", *ZDNet*, Aug. 2015.

[107] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, Jun. 2011.

[108] Q. Zhao, A. K. Jain, N. G. Paulter, and M. Taylor, "Fingerprint image synthesis based on statistical feature models", in *IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, VA, USA, Sep. 2012.

[109] N. Brandenberg, S. Hoehnel, F. Kuttler, K. Homicsko, C. Ceroni, T. Ringel, N. Gjorevski, G. Schwank, G. Coukos, G. Turcatti, and M. P. Lutolf, "High-throughput automated organoid culture via stem-cell aggregation in microcavity arrays", *Nature Biomedical Engineering*, Jun. 2020.

[110] P. Dixon, "A Failure to "Do No Harm" – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.", *Health and Technology*, vol. 7, no. 4, pp. 539–567, Dec. 2017.

[111] J. Srinivasan, S. Bailur, E. Schoemaker, and S. Seshagiri, "The Poverty of Privacy: Understanding Privacy Trade-Offs From Identity Infrastructure Users in India", *International Journal of Communication*, vol. 12, pp. 1228–1247, Mar. 2018.

[112] M. Gomez-Barrero and J. Galbally, "Reversing the irreversible: A survey on inverse biometrics", *Computers & Security*, vol. 90, Mar. 2020.

[113] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", in *International conference on the theory and applications of cryptographic techniques*, Springer, 2004, pp. 523–540.

[114] R. Chatterjee, M. S. Riazi, T. Chowdhury, E. Marasco, F. Koushanfar, and A. Juels, "Multisketches: Practical secure sketches using off-the-shelf biometric matching algorithms", in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1171–1186.

[115] R. Aggarwal, J. W. Goodell, and L. J. Selleck, "Lending to women in microfinance: Role of social trust", *International Business Review*, vol. 24, no. 1, pp. 55–65, Feb. 2015.

[116] E. Hughes, *A cypherpunk's manifesto*, Mar. 1993. [Online]. Available: https://www.activism.net/cypherpunk/manifesto.html.

[117] J. Assange and J. Appelbaum, *Cypherpunks: Freedom and the Future of the Internet*. OR Books, Oct. 2016, ISBN: 978-1944869083.

[118] W. Stallings, "The PGP Web of Trust", *BYTE Magazine*, vol. 20, no. 2, pp. 161–164, Feb. 1995.

[119] P. R. Zimmermann, *The Official PGP User's Guide*. Cambridge, MA, USA: MIT Press, 1995, ISBN: 0-262-74017-6.

[120] R. Rivest and B. Lampson, *SDSI: A Simple Distributed Security Infrastructure*, Apr. 1996.

[121] C. Ellison *et al.*, *SPKI Certificate Theory*, RFC 2693, Sep. 1999.

[122] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0.", in *USENIX Security Symposium*, vol. 348, 1999, pp. 169–184.

[123] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: Somebody you know", in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 168–178.

[124] A. Mislove, A. Post, P. Druschel, and K. P. Gummadi, "Ostra: Leveraging trust to thwart unwanted communication", in *5th USENIX Symposium on Networked Systems Design and Implementation*, Apr. 2008, pp. 15–30.

[125] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks", in *29th IEEE Symposium on Security and Privacy*, Oakland, CA, May 2008. [Online]. Available: https://www.iscs.nus.edu.sg/~yuhf/sybillimit-tr.pdf.

[126] N. Tran, B. Min, J. Li, and L. Submaranian, "Sybil-resilient online content voting", in *6th Symposium on Networked System Design and Implementation (NSDI)*, Apr. 2009, pp. 15–28.

[127] B. Viswanath, M. Mondal, K. P. Gummadi, A. Mislove, and A. Post, "Canal: Scaling social network-based sybil tolerance schemes", in *EuroSys Workshop on Social Network Systems (SNS)*, Apr. 2012.

[128] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks", in *Internet Measurement Conference (IMC)*, San Diego, USA, Oct. 2007.

[129] B. Viswanath and A. Post, "An Analysis of Social Network-Based Sybil Defenses", in *ACM SIGCOMM*, New Delhi, India, Aug. 2010.

[130] S. Ghosh, B. Viswanath, F. Kooti, N. K. Sharma, G. Korlam, F. Benevenuto, N. Ganguly, and K. P. Gummadi, "Understanding and Combating Link Farming in the Twitter Social Network", in *21st International Conference on World Wide Web (WWW)*, Lyon, France, Apr. 2012.

[131] J. Messias, L. Schmidt, R. Oliveira, and F. Benevenuto, "You followed my bot! Transforming robots into influential users in Twitter", vol. 18, no. 7, Jul. 2013.

[132] C. A. Freitas, F. Benevenuto, S. Ghosh, and A. Veloso, "Reverse Engineering Socialbot Infiltration Strategies in Twitter", in *Advances in Social Networks Analysis and Mining (ASONAM)*, Paris, France, Aug. 2015, pp. 25–32.

[133] E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The Rise of Social Bots", *Communications of the ACM*, vol. 59, no. 7, Jul. 2016.

[134] A. Bessi and E. Ferrara, "Social bots distort the 2016 U.S. Presidential election online discussion", *First Monday*, vol. 21, no. 11, Nov. 2016.

[135] D. A. Broniatowski, A. M. Jamison, S. Qi, L. AlKulaib, T. Chen, A. Benton, and S. C. Q. M. Dredze, "Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate", *American Journal of Public Health*, Sep. 2018.

[136] C. Allen, *The path to self-sovereign identity*, Apr. 2016. [Online]. Available: `http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html`.

[137] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity", *Computer Science Review*, vol. 30, pp. 80–86, Nov. 2018.

[138] J. S. Martin Schanzenbach Georg Bramm, "reclaimID: Secure, Self-Sovereign Identities using Name Systems and Attribute-Based Encryption", in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, New York, NY, USA, Aug. 2018.

[139] Q. Stokkink and J. Pouwelse, *Deployment of a blockchain-based self-sovereign identity*, Aug. 2018.

[140] A. Abraham, *Self-sovereign identity*, Oct. 2017. [Online]. Available: `http://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf`.

[141] A. Satybaldy, M. Nowostawski, and J. Ellingsen, *Self-sovereign identity systems: Evaluation framework*, Apr. 2020. [Online]. Available: https://www.researchgate.net/publication/339836401_Self-Sovereign_Identity_Systems_Evaluation_Framework.

[142] Decentralized Identity Foundation, *DIF website*, https://identity.foundation/, 2020.

[143] W3C, *Peer DID method specification*, https://openssi.github.io/peer-did-method-spec/index.html#privacy-considerations, 2020.

[144] O. Kharif, "Cryptokitties mania overwhelms ethereum network's processing", *Bloomberg (4 Dec. 2017)*, 2017.

[145] G. Fenu, L. Marchesi, M. Marchesi, and R. Tonelli, "The ICO phenomenon and its relationships with Ethereum smart contract environment", in *2018 IEEE 1st International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Mar. 2018.

[146] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and L. Föhr, "The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators", *Harvard International Law Journal*, vol. 60, no. 2, 2019.

[147] Wikipedia contributors, *Multi-factor authentication — Wikipedia, the free encyclopedia*, [Online; accessed July 2020], 2020. [Online]. Available: https://en.wikipedia.org/wiki/Multi-factor_authentication.

[148] E. Cecchetti, F. Zhang, Y. Ji, A. Kosba, A. Juels, and E. Shi, "Solidus: Confidential distributed ledger transactions via PVORM", in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 701–717.

[149] J. J. J. Roberts and N. Rapp, "Nearly 4 million Bitcoins lost forever, new study says", *Fortune*, 25 Nov. 2017.

[150] B. Armstrong, *Coinbase is not a wallet*, 25 Feb. 2016.

[151] F. Wu, "No easy answers in the fight over iPhone decryption", *Communications of the ACM*, vol. 59, no. 9, pp. 20–22, 2016.

[152] R. Gennaro and S. Goldfeder, "Fast multiparty threshold ECDSA with fast trustless setup", in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1179–1194.

[153] V. Shoup, "Practical threshold signatures", in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2000, pp. 207–220.

[154] M. Möser, I. Eyal, and E. G. Sirer, "Bitcoin covenants", in *International Conference on Financial Cryptography and Data Security*, Springer, 2016, pp. 126–141.

[155] F. Zhang, P. Daian, I. Bentov, I. Miers, and A. Juels, “Paralysis proofs: Secure dynamic access structures for cryptocurrency custody and more”, in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, ser. AFT ’19, Zurich, Switzerland: Association for Computing Machinery, 2019, pp. 1–15. [Online]. Available: https://doi.org/10.1145/3318041.3355459.

[156] D. Akhawe and A. P. Felt, “Alice in Warningland: A large-scale field study of browser security warning effectiveness”, in *22nd {USENIX} Security Symposium ({USENIX} Security 13)*, 2013, pp. 257–272.

[157] E. Almutairi and S. Al-Megren, “Usability and security analysis of the KeepKey wallet”, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2019, pp. 149–153.

[158] I. Sakharova, “Payment card fraud: Challenges and solutions”, in *2012 IEEE international conference on intelligence and security informatics*, IEEE, 2012, pp. 227–234.

[159] Ulrich Bindseil, *Tiered CBDC and the financial system*, https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf, 2020.

[160] *Chainalysis*, Referenced July 2020. [Online]. Available: chainalysis.com.

[161] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, “Evaluating user privacy in Bitcoin”, in *International Conference on Financial Cryptography and Data Security*, Springer, 2013, pp. 34–51.

[162] D. Ron and A. Shamir, “Quantitative analysis of the full Bitcoin transaction graph”, in *Proceedings of the 17th International Conference on Financial Cryptography & Data Security*, 2013, pp. 6–24.

[163] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of Bitcoins: Characterizing payments among men with no names”, in *Proceedings of the 2013 conference on Internet measurement conference*, 2013, pp. 127–140.

[164] M. Spagnuolo, F. Maggi, and S. Zanero, “BitIodine: Extracting intelligence from the Bitcoin network”, in *Proceedings of the 18th International Conference on Financial Cryptography & Data Security*, 2014, pp. 457–468.

[165] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, “An empirical analysis of anonymity in Zcash”, in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 463–477.

[166] A. Kumar, C. Fischer, S. Tople, and P. Saxena, “A traceability analysis of Monero’s blockchain”, in *ESORICS 2017*, 2017, pp. 153–173.

[167] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin, “An empirical analysis of linkability in the Monero blockchain”, *Proceedings on Privacy Enhancing Technologies*, pp. 143–163, 3 2018.

[168] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from Bitcoin", in *Security and Privacy (SP), 2014 IEEE Symposium on*, IEEE, 2014, pp. 459–474.

[169] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: the second-generation onion router", in *12th USENIX Security Symposium*, Aug. 2004.

[170] K. Hill, "How did the FBI break Tor?", *Forbes*, Nov. 2014.

[171] C. Farivar, "Judge confirms what many suspected: Feds hired cmu to break tor", *Ars Technica*, Feb. 2016.

[172] F. Tramèr, D. Boneh, and K. G. Paterson, "Remote side-channel attacks on anonymous transactions.", *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 220, 2020.

[173] K. Nikitin, E. Kokoris-Kogias, P. Jovanovic, N. Gailly, L. Gasser, I. Khoffi, J. Cappos, and B. Ford, "CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds", in *26th USENIX Security Symposium*, 2017, pp. 1271–1287.

[174] E. Kokoris-Kogias, "Secure, Confidential Blockchains Providing High Throughput and Low Latency", PhD thesis, École Polytechnique Fédérale de Lausanne (EPFL), May 2019.

[175] Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, G. Cabrera, C. Catalini, K. Chalkias, E. Cheng, A. Ching, A. Chursin, G. Danezis, G. D. Giacomo, D. L. Dill, H. Ding, N. Doudchenko, V. Gao, Z. Gao, F. Garillot, M. Gorven, P. Hayes, J. M. Hou, Y. Hu, K. Hurley, K. Lewi, C. Li, Z. Li, D. Malkhi, S. Margulis, B. Maurer, P. Mohassel, L. de Naurois, V. Nikolaenko, T. Nowacki, O. Orlov, D. Perelman, A. Pott, B. Proctor, S. Qadeer, Rain, D. Russi, B. Schwab, S. Sezer, A. Sonnino, H. Venter, L. Wei, N. Wernerfelt, B. Williams, Q. Wu, X. Yan, T. Zakian, and R. Zhou, *The Libra blockchain*, May 2020. [Online]. Available: https://developers.libra.org/docs/assets/papers/the-libra-blockchain/2020-05-26.pdf.

[176] E. Kokoris-Kogias, E. C. Alp, S. D. Siby, N. Gailly, L. Gasser, P. Jovanovic, E. Syta, and B. Ford, *Verifiable Management of Private Data under Byzantine Failures*, Cryptology ePrint Archive, Report 2018/209, 2018.

[177] E. C. Alp, E. Kokoris-Kogias, G. Fragkouli, and B. Ford, "Rethinking General-Purpose Decentralized Computing", in *17th Workshop on Hot Topics in Operating Systems (HotOS XVII)*, Bertinoro, Italy, May 2019.

[178] F. Benhamouda, S. Halevi, and T. Halevi, "Supporting private data on Hyperledger Fabric with secure multiparty computation", *IBM Journal of Research and Development*, vol. 63, no. 2/3, pp. 3–1, 2019.

[179] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: Scalable, private smart contracts", in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1353–1370.

[180] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song, "Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts", in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019.

[181] S. Bowe, A. Chiesa, M. Green, I. Miers, P. Mishra, and H. Wu, "Zexe: Enabling decentralized private computation", in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020.

[182] H. Berghel, "Equifax and the Latest Round of Identity Theft Roulette", *IEEE Computer*, vol. 50, no. 12, Dec. 2017.

[183] J. Feigenbaum, J. A. Hendler, A. D. Jaggard, D. J. Weitzner, and R. N. Wright, "Accountability and deterrence in online life", in *International Conference on Web Science (ICWS)*, 2011.

[184] A. Shamir, "How to Share a Secret", *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[185] R. Geambasu, T. Kohno, A. A. Levy, and H. M. Levy, "Vanish: Increasing Data Privacy with Self-Destructing Data.", in *USENIX Security Symposium*, 2009, pp. 299–316.

[186] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Balancing accountability and privacy using e-cash", in *International Conference on Security and Cryptography for Networks*, Springer, 2006, pp. 141–155.

[187] C. Garman, M. Green, and I. Miers, "Accountable privacy for decentralized anonymous payments", in *International Conference on Financial Cryptography and Data Security*, Springer, 2016, pp. 81–98.

[188] K. Wüst, K. Kostiainen, V. Čapkun, and S. Čapkun, "Prcash: Fast, private and regulated transactions for digital currencies", in *International Conference on Financial Cryptography and Data Security*, Springer, 2019, pp. 158–178.

[189] J. A. Kroll, E. W. Felten, and D. Boneh, *Secure protocols for accountable warrant execution*, Apr. 2014.

[190] A. Segal, B. Ford, and J. Feigenbaum, "Catching bandits and only bandits: Privacy-preserving intersection warrants for lawful surveillance", in *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI'14)*, Aug. 2014.

[191] A. Segal, J. Feigenbaum, and B. Ford, "Privacy-Preserving Lawful Contact Chaining", in *Workshop on Privacy in the Electronic Society (WPES)*, Oct. 2016.

[192] J. Feigenbaum, "Multiple Objectives of Lawful-Surveillance Protocols (Transcript of Discussion)", in *Cambridge International Workshop on Security Protocols*, Springer, 2017, pp. 9–17.

[193] J. Frankle, S. Park, D. Shaar, S. Goldwasser, and D. J. Weitzner, "Practical Accountability of Secret Processes", in *27th USENIX Security Symposium*, Aug. 2018.

[194] G. Panwar, R. Vishwanathan, S. Misra, and A. Bos, "Sampl: Scalable auditability of monitoring processes using public ledgers", in *2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, Nov. 2019.

[195] A. Miller, Z. Cai, and S. Jha, "Smart contracts and opportunities for formal methods", in *International Symposium on Leveraging Applications of Formal Methods*, Springer, 2018, pp. 280–299.

[196] E. Hildenbrandt, M. Saxena, N. Rodrigues, X. Zhu, P. Daian, D. Guth, B. Moore, D. Park, Y. Zhang, A. Stefanescu, *et al.*, "KEVM: A complete formal semantics of the Ethereum virtual machine", in *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, IEEE, 2018, pp. 204–217.

[197] S. Blackshear, E. Cheng, D. L. Dill, V. Gao, B. Maurer, T. Nowacki, A. Pott, S. Qadeer, D. R. Rain, S. Sezer, *et al.*, *Move: A language with programmable resources*, 2019.

[198] K. Crary and M. J. Sullivan, "Peer-to-peer affine commitment using Bitcoin", in *Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation*, 2015, pp. 479–488.

[199] S. A. K. Thyagarajan, A. Bhat, B. Magri, D. Tschudi, and A. Kate, "Reparo: Publicly verifiable layer to repair blockchains", *arXiv preprint arXiv:2001.00486*, 2020.

[200] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain–or–rewriting history in bitcoin and friends", in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2017, pp. 111–126.

[201] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, "Hyperservice: Interoperability and programmability across heterogeneous blockchains", in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 549–566.

[202] A. E. Gencer, R. van Renesse, and E. G. Sirer, "Service-oriented sharding with Aspen", *arXiv preprint arXiv:1611.06816*, 2016.

[203] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, *Enabling blockchain innovations with pegged sidechains*, 2014. [Online]. Available: https://blockstream.com/sidechains.pdf.

[204] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake", *self-published paper, August*, vol. 19, p. 1, 2012.

[205] *Intel Software Guard Extensions, Reference Number: 332680-002*, 2015. [Online]. Available: https://software.intel.com/sites/default/files/332680-002.pdf.

[206] T. Alves and D. Felton, *TrustZone: Integrated Hardware and Software Security-Enabling Trusted Computing in Embedded Systems*, 2004. [Online]. Available: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf.

Source: **Brookings Institution. 2020. "Design Choices for Central Bank Digital Currency: Policy and Technical Considerations," Global Economy & Development Working Paper 140, July.**

[207] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic processors-a survey", *Proceedings of the IEEE*, vol. 94, no. 2, pp. 357–369, 2006.

[208] Bitcoin Wiki, *Hardware wallet*, 2020. [Online]. Available: https://en.Bitcoin.it/wiki/Hardware_wallet.

[209] I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative technology for cpu based attestation and sealing", in *Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy*, ACM New York, NY, USA, vol. 13, 2013, p. 7.

[210] F. Brasser, U. Müller, A. Dmitrienko, K. Kostiainen, S. Capkun, and A.-R. Sadeghi, "Software grand exposure: SGX cache attacks are practical", in *11th USENIX Workshop on Offensive Technologies,WOOT 2017*, USENIX, 2017.

[211] J. Götzfried, M. Eckert, S. Schinzel, and T. Müller, "Cache attacks on Intel SGX", in *Proceedings of the 10th European Workshop on Systems Security*, ACM, 2017, p. 2.

[212] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, "Meltdown: Reading kernel memory from user space", in *27th USENIX Security Symposium (USENIX Security 18)*, 2018.

[213] J. Van Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx, "FORESHADOW: Extracting the keys to the Intel SGX kingdom with transient out-of-order execution", in *Proceedings of the 27th USENIX Security Symposium. USENIX Association*, 2018.

[214] A. Rane, C. Lin, and M. Tiwari, "Raccoon: Closing digital side-channels through obfuscated execution", in *USENIX Security Symposium*, 2015.

[215] F. Brasser, S. Capkun, A. Dmitrienko, T. Frassetto, K. Kostiainen, and A.-R. Sadeghi, "DR.SGX: Automated and adjustable side-channel protection for SGX using data location randomization", in *Proceedings of the 35th Annual Computer Security Applications Conference*, ser. ACSAC '19, New York, NY, USA: Association for Computing Machinery, 2019, pp. 788–800, ISBN: 9781450376280. [Online]. Available: https://doi.org/10.1145/3359789.3359809.

[216] D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer, "Physical key extraction attacks on pcs", *Communications of the ACM*, vol. 59, no. 6, 2016.

[217] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices", in *International Workshop on Security Protocols*, Springer, 1997, pp. 125–136.

[218] ——, "Tamper resistance-a cautionary note", in *Proceedings of the second Usenix workshop on electronic commerce*, vol. 2, 1996, pp. 1–11.

[219] O. Kömmerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors.", *Smartcard*, vol. 99, pp. 9–20, 1999.

[220] D. Lee, D. Kohlbrenner, S. Shinde, K. Asanović, and D. Song, "Keystone: An open framework for architecting trusted execution environments", in *Proceedings of the Fifteenth European Conference on Computer Systems*, ser. EuroSys '20, New York, NY, USA: Association for Computing Machinery, 2020, ISBN: 9781450368827. [Online]. Available: https://doi.org/10.1145/3342195.3387532.

[221] Q. Yao, Z. Xu, and Y. Zhang, *A kind of safety method, system and the terminal of digital cash of the use based on block chain*, Jan. 2017. [Online]. Available: https://patents.google.com/patent/CN106850200B/en.

[222] D. Chaum, "Blind signatures for untraceable payments", in *Advances in cryptology*, Springer, 1983, pp. 199–203.

[223] M. Greg, *Confidential transactions*, 2015. [Online]. Available: https://web.archive.org/web/20150630144253/https://people.xiph.org/~greg/confidential_values.txt.

[224] K. Wüst, S. Matetic, M. Schneider, I. Miers, K. Kostiainen, and S. Čapkun, "Zlite: Lightweight clients for shielded zcash transactions using trusted execution", in *International Conference on Financial Cryptography and Data Security*, Springer, 2019, pp. 179–198.

[225] S. Matetic, K. Wüst, M. Schneider, K. Kostiainen, G. Karame, and S. Capkun, "BITE: Bitcoin lightweight client privacy using trusted execution", in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 783–800.

[226] *Ledger hardware wallet*, https://www.ledger.com/, 2020.

[227] *Trezor hardware wallet*, https://trezor.io/, 2020.

[228] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", in *2016 IEEE symposium on security and privacy (SP)*, 2016.

[229] S. Gesell, *The Natural Economic Order*. London: Peter Owen Limited, 1958, Translated by Philip Pye M.A.

[230] B. Champ, "Stamp Scrip: Money People Paid to Use", Jan. 2008. [Online]. Available: https://www.clevelandfed.org/newsroom-and-events/publications/economic-commentary/economic-commentary-archives/2008-economic-commentaries/ec-20080401-stamp-scrip-money-people-paid-to-use.aspx.

[231] D. Grant, *An overview of blockchain-based universal basic income projects*, Jul. 2018. [Online]. Available: https://www.usv.com/writing/2018/07/an-overview-of-blockchain-based-universal-basic-income-projects/.

[232] A. Brenzikofer, *Encointer – an ecological, egalitarian and private cryptocurrency and self-sovereign identity system*, Dec. 2019. [Online]. Available: https://arxiv.org/abs/1912.12141.

[233] A. Howitt, *Roadmap to a government-independent basic income (UBI) digital currency*, Feb. 2019. [Online]. Available: https://basicincome.org/wp-content/uploads/2020/03/UBI-ROADMAP-v1.2.1.pdf.

[234] B. Ford, *Democratic Value and Money for Decentralized Digital Society*, Mar. 2020. [Online]. Available: https://arxiv.org/abs/2003.12375.

[235] Goldman Sachs Group, Inc., *Quantinomics*, Referenced June 2020. [Online]. Available: https://www.gsam.com/content/gsam/global/en/market-insights/gsam-insights/quantinomics.html.

[236] I. Ayres, *Super crunchers: Why thinking-by-numbers is the new way to be smart*. Bantam Books, 2007.

[237] J. Dew, "The association between consumer debt and the likelihood of divorce", *Journal of Family and Economic Issues*, vol. 32, no. 4, pp. 554–565, 2011.

[238] D. Berger and J. Vavra, "Consumption dynamics during recessions", *Econometrica*, vol. 83, no. 1, pp. 101–154, 2015.

[239] N. De, "Story from news US Treasury Department blacklists 20 Bitcoin Addresses tied to alleged North Korean hackers", *Coindesk*, 2 March 2020.

[240] J. Barrdear and M. Kumhof, "The macroeconomics of central bank issued digital currencies", Bank of England working paper No. 605, 2016.

[241] D. Andolfatto, "Assessing the impact of central bank digital currency on private banks", FRB St. Louis Working Paper No. 2018-25, 2018.

[242] M. D. Bordo and A. T. Levin, "Digital cash: Principles & practical steps", National Bureau of Economic Research Working Paper No. 25455, 2019.

[243] D. Andolfatto, "Bitcoin and central banking", *MacroMania (blog)*, 2015. [Online]. Available: http://www.andolfatto.blogspot.com/2015/11/bitcoin-and-central-banking.html.

[244] K. Assenmacher and S. Krogstrup, *Monetary policy with negative interest rates: Decoupling cash from electronic money*. International Monetary Fund Working Paper No. 18/191, 2018.

[245] M. L. Bech and R. Garratt, "Central bank cryptocurrencies", *BIS Quarterly Review September*, pp. 55–70, 2017.

[246] C. on Payments and M. Infrastructures, *Digital currencies*, 2015.

[247] ——, *Central bank digital currencies*, 2018.

[248] B. Broadbent, "Central banks and digital currencies", Speech at Centre for Macroeconomics, London School of Economics, 2016. [Online]. Available: https://www.bis.org/review/r160303e.pdf.

[249] A. Carstens, "Money in the digital age: What role for central banks?", Lecture at the House of Finance, Goethe University, Frankfurt, 2018.

[250] W. Engert and B. S.-C. Fung, “Central bank digital currency: Motivations and implications”, Bank of Canada Staff Discussion Paper No. 2017-16, 2017.

[251] B. S. Fung and H. Halaburda, “Central bank digital currencies: A framework for assessing why and how”, Bank of Canada Staff Discussion Paper No. 2016-22, 2016.

[252] T. M. Griffoli, M. M. S. M. Peria, M. I. Agur, M. A. Ari, M. J. Kiff, M. A. Popescu, and M. C. Rochon, *Casting Light on Central Bank Digital Currencies.* International Monetary Fund Staff Discussion Note, 2018.

[253] A. Grym, P. Heikkinen, K. Kauko, K. Takala, *et al.*, “Central bank digital currency”, *Bank of Finland Economics Review No. 5/2017*, 2017.

[254] S. Ingves, “Do we need an e-krona?”, Speech at Swedish House of Finance, Stockholm, 2017. [Online]. Available: https://www.riksbank.se/en-gb/financial-stability/the-financial-system/payments/does-sweden-need-an-e-krona/.

[255] E. Prasad, “Central banking in a digital age: Stock-taking and preliminary thoughts”, Brookings Institution Report, 2018.

[256] M. Raskin and D. Yermack, “Digital currencies, decentralized ledgers and the future of central banking”, National Bureau of Economic Research Working Paper No. 22238, 2018.

[257] H. Rey, “Dilemma not trilemma: The global financial cycle and monetary policy independence”, Proceedings of the Jackson Hole Symposium, Federal Reserve Bank of Kansas City, 2015.

[258] M. Tolle, “Central bank digital currency: The end of monetary policy as we know it?”, *Bank Underground (blog), Bank of England*, 2016. [Online]. Available: https://bankunderground.co.uk/2016/07/25/central-bank-digital-currency-the-end-of-monetary-policy-as-we-know-it/.

[259] Q. Yao, “The application of digital currency in interbank cash transfer scenario”, *Finance Comput.*, vol. 5, pp. 16–19, 2017.

[260] K. Qin, L. Zhou, B. Livshits, and A. Gervais, “Attacking the DeFi ecosystem with flash loans for fun and profit”, *arXiv preprint arXiv:2003.03810*, 2020. [Online]. Available: https://arxiv.org/abs/2003.03810.

[261] *DeFi Pulse*, Referenced July 2020. [Online]. Available: defipulse.com.

[262] A. Juels, A. Kosba, and E. Shi, “The Ring of Gyges: Investigating the future of criminal smart contracts”, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 283–295.

[263] B. Marino and A. Juels, “Setting standards for altering and undoing smart contracts”, in *International Symposium on Rules and Rule Markup Languages for the Semantic Web*, Springer, 2016, pp. 151–166.

[264] A. B. Laffer, W. H. Winegarden, and J. Childs, “The economic burden caused by tax code complexity”, *The Laffer Center for Supply-Side Economics*, 2011.

[265] L. M. LoPucki and E. Warren, *Secured Transactions: A Systems Approach.* Wolters Kluwer, 2019.

[266] R. J. Mann, "Reliable perfection of security interests in crypto-currency", *SMU Sci. & Tech. L. Rev.*, vol. 21, p. 159, 2018.

[267] K. V. Tu, "Crypto-collateral", *SMU Sci. & Tech. L. Rev.*, vol. 21, p. 205, 2018.

[268] J. L. Schroeder, "Bitcoin and the uniform commercial code", *U. Miami Bus. L. Rev.*, vol. 24, p. 1, 2015.

[269] X.-T. Nguyen, "Lessons from case study of secured transactions with bitcoin", *SMU Sci. & Tech. L. Rev.*, vol. 21, p. 181, 2018.

[270] Internal Revenue Service (IRS), *Notice 2014-21*, 2014.

[271] Tether, *Tether: Digital money for a digital age.* [Online]. Available: tether.to, (accessed: 07.03.2020).

[272] Jinze and Etiene, *First look: China's central bank digital currency*, Aug. 2019. [Online]. Available: https://research.binance.com/analysis/china-cbdc.

[273] L. Baitao, *Central bank digital currency will become the biggest magic weapon for RMB internationalization*, Aug. 2019. [Online]. Available: https://finance.sina.com.cn/blockchain/coin/2019-08-12/doc-ihytcitm8648461.shtml.

[274] J. Martin, *Alipay patents reveal more details about China's forthcoming CBDC*, Mar. 2020. [Online]. Available: https://cointelegraph.com/news/alipay-patents-reveal-more-details-about-chinas-forthcoming-cbdc.

[275] H. Murphy and Y. Yang, *Patents reveal extent of China's digital currency plans*, Feb. 2020. [Online]. Available: https://www.ft.com/content/f10e94cc-4d74-11ea-95a0-43d18ec715f5.

[276] M. del Castillo, *Alibaba, Tencent, five others to receive first Chinese government cryptocurrency*, Aug. 2019. [Online]. Available: https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/#4202c28b1a51.

[277] X. Jing, *Method and device for opening digital currency wallet and electronic equipment*, Feb. 2020. [Online]. Available: https://patents.google.com/patent/CN110852729A/en.

[278] Y. Qian, *Blockchain and central bank digital currency*, Mar. 2020. [Online]. Available: https://www.ccvalue.cn/article/216773.html.

[279] P. Boring and M. Kaufman, *Blockchain: The breakthrough technology of the decade and how China is leading the way – an industry white paper*, Feb. 2020. [Online]. Available: https://digitalchamber.org/wp-content/uploads/dlm_uploads/2020/02/Blockchain-The-Breakthrough-Technology-of-the-Decade-and-How-china-is-Leading-the-Way.pdf.

[280] Y. Qian, "Experimental research on central bank digital currency prototype system", *Journal of Software*, vol. 29, no. 09, pp. 2716–2712, 2018.

[281] F. Yifei and L. Jiechen, *Several considerations about central bank digital currency*, Jan. 2018. [Online]. Available: https://www.yicai.com/news/5395409.html.

[282] J. Ossinger, *Pboc wants 'controllable anonymity' in China's digital currency*, Nov. 2019. [Online]. Available: https://www.bloomberg.com/news/articles/2019-11-13/pboc-wants-controllable-anonymity-in-china-s-digital-currency.

[283] Y. Wei, *Anonymous transaction method and system based on digital currency*, Mar. 2020. [Online]. Available: https://patents.google.com/patent/CN110889681A/en.

[284] Y. Qian, D. Gang, Q. Youcai, H. Lieming, C. Haibo, Z. Xinyu, W. Jiwei, and Z. Dawei, *A kind of method of commerce and device based on digital cash*, Oct. 2017. [Online]. Available: https://patents.google.com/patent/CN107358424A/en.

[285] ——, *Use the method for commerce and device of digital cash*, Nov. 2017. [Online]. Available: https://patents.google.com/patent/CN107392603A/en.

[286] Y. Wei, *Digital currency account control method and device*, Feb. 2020. [Online]. Available: https://patents.google.com/patent/CN110838061A/en.

[287] Q. Yao, *Digital cash management method and system based on the triggering of loan interest rate condition*, Aug. 2018. [Online]. Available: https://patents.google.com/patent/CN108416671A/en?oq=+CN108416671A.

[288] X. Jing, *Method and device for opening digital currency wallet and electronic equipment*, Feb. 2019. [Online]. Available: https://patents.google.com/patent/CN110852729A/en.

[289] Z. Meng, S. Xu, and H. Zhou, *Method and device for executing digital currency transaction and electronic equipment*, Oct. 2019. [Online]. Available: https://patents.google.com/patent/CN110827146A/en.

[290] Z. Meng, H. Yang, and H. Zhou, *Transaction processing method and device based on digital currency and electronic equipment*, Oct. 2019. [Online]. Available: https://patents.google.com/patent/CN110852730A/en.

The Technology of Retail Central Bank Digital Currency

Raphael Auer
raphael.auer@bis.org

Rainer Böhme
rainer.boehme@uibk.ac.at

The technology of retail central bank digital currency[1]

Central bank digital currencies (CBDCs) promise to provide cash-like safety and convenience for peer-to-peer payments. To do so, they must be resilient and accessible. They should also safeguard the user's privacy, while allowing for effective law enforcement. Different technical designs satisfy these attributes to varying degrees, depending on whether they feature intermediaries, a conventional or distributed infrastructure, account- or token-based access, and retail interlinkages across borders. We set out the underlying trade-offs and the related hierarchy of design choices.

JEL classification: E42, E44, E51, E58, G21, G28.

The question of whether central banks should issue digital currency to the general public has attracted increasing attention. This special feature sketches out some key technological design considerations for a retail CBDC, in the event that a central bank decided to issue one. We do not investigate the case for or against issuance, the systemic implications, or how these might be managed.[2]

We structure our approach around consumer needs and the associated technical design choices. Current electronic retail money represents a claim on an intermediary, rather than functioning as the digital equivalent of cash. CBDCs could potentially provide a cash-like certainty for peer-to-peer payments. At the same time, they should offer convenience, resilience, accessibility, privacy and ease of use in cross-border payments. Different technical designs meet these criteria to varying degrees, with attendant technical trade-offs. We explore these issues. The aim is not to promote or highlight any particular approach, but to lay some groundwork for more systematic discussions.

[1] We thank Morten Bech, Codruta Boar, Claudio Borio, Stijn Claessens, Benoît Cœuré, Jon Frost, Leonardo Gambacorta, Marc Hollanders, Henry Holden, Ross Leckow, Cyril Monet, Hyun Song Shin, Rastko Vrbaski, Amber Wadsworth and Philip Wooldridge for comments, and Haiwei Cao, Giulio Cornelli and Alan Villegas for exceptional research assistance. The views expressed in this article are those of the authors and do not necessarily reflect those of the Bank for International Settlements.

[2] For the systemic implications, see the survey in CPMI-MC (2018). Andolfatto (2018), Kumhof and Noone (2018), and Bindseil (2020) examine how the impact on the central bank's balance sheet can be managed, while Brunnermeier and Niepelt (2019) investigate how financial instability risks can be mitigated.

Source: **Auer, R. and R. Boehme. 2020. "The Technology of Retail Central Bank Digital Currency," Bank for International Settlements Quarterly Review, March.**

Key takeaways

- A trusted and widely usable retail CBDC must be secure and accessible, offer cash-like convenience and safeguard privacy.
- Various technical designs satisfy these criteria to different degrees, and the associated trade-offs need to be identified.
- The design of a retail CBDC needs to balance the credibility of direct claims on the central bank with the benefits of using payment intermediaries.

Our approach is graphically represented in the "CBDC pyramid", which maps consumer needs onto the associated design choices for the central bank. This scheme forms a hierarchy in which the lower layers represent design decisions that feed into subsequent, higher-level decisions.

We start by introducing the four main design choices, as represented in the four layers of the CBDC pyramid. We assess the legal structure of claims and the operational roles of the central bank and private institutions in different CBDC architectures. We discuss the choice between distributed ledger technology (DLT) and a centrally controlled infrastructure. We compare token-based systems and account-based systems. Before concluding, we assess how the development of CBDCs might reinforce current efforts to overhaul cross-border payments.

From consumer needs to design choices: the CBDC pyramid

The focus of our approach is the "retail" aspect of CBDC; we ask what consumer needs a CBDC could address.[3] We thus sketch the development of a CBDC through an approach that proceeds from consumer needs to design choices.[4] The left-hand side of the CBDC pyramid (Graph 1) sets out such consumer needs and six associated features that would make a CBDC useful. Starting with cash-like peer-to-peer usability, these features also comprise convenient real-time payments, payments security, privacy, wide accessibility and ease of use in cross-border payments. The pyramid's right-hand side lays out the associated design choices.

The consumer's prime need is that the CBDC embodies a cash-like claim on the central bank, ideally transferable in peer-to-peer settings. Today, even consumers who normally prefer to pay electronically are confident that, if an episode of financial turmoil were to threaten, they could shift their electronic money holdings into cash. This flight to cash has been seen in many crisis episodes, including recent ones. The main concern is that if, in the future, cash were no longer generally

[3] All private sector non-financial users are referred to as "consumers" in what follows. For a discussion of "wholesale" CBDC for use in the financial industry, see CPMI-MC (2018).

[4] The survey in Boar et al (2020) highlights that central banks have advanced other motivations for issuance, including monetary policy implementation and financial stability considerations. These aspects are considered in the CBDC design frameworks of Fung and Halaburda (2016), Bjerg (2017), CPMI-MC (2018), Mancini-Griffoli et al (2018), Wadsworth (2018), Kahn et al (2019) and Adrian (2019). Although it takes a more positive stance towards CBDC, our focus on technical design elements is related to Pichler et al's (2020) analysis of the limits of CBDC when compared with cash.

accepted, a severe financial crisis might create further havoc by disrupting day-to-day business and retail transactions.[5]

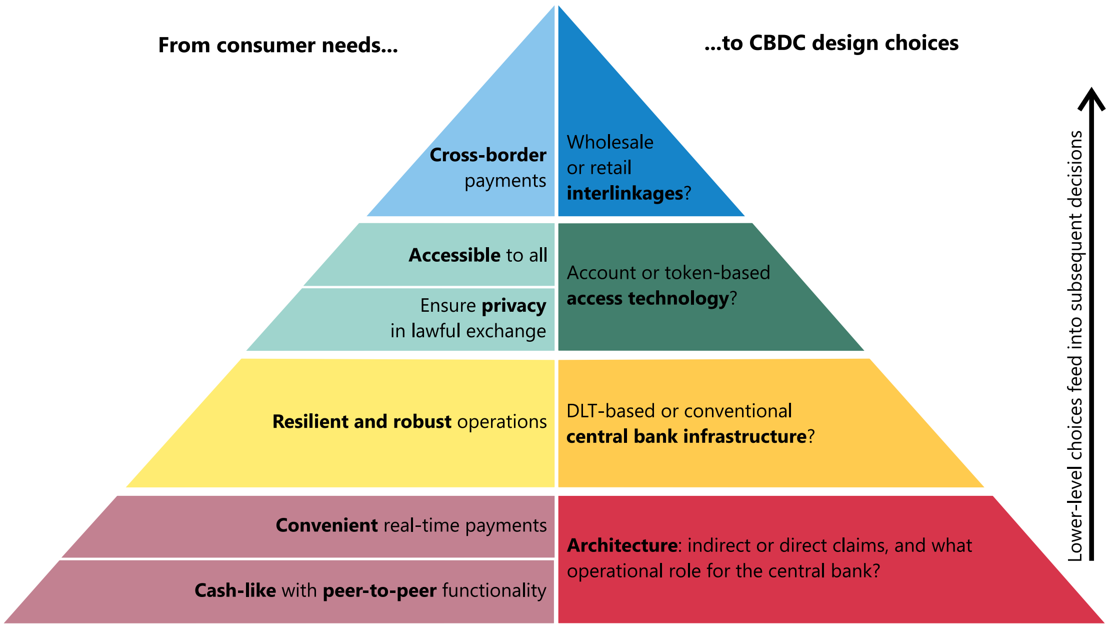
At the same time, consumers are unlikely to adopt a CBDC if it is less convenient to use than today's electronic payments. Banks and payment service providers run sophisticated infrastructures that can handle peak demand, such as on Singles Day in China or Black Friday in the United States. And intermediaries help to smooth the flow of payments by taking on risk, for example during connectivity breaks or offline payments.

These two needs – cash-like safety and convenience of use – lead to the foundational design consideration for a CBDC (see lowest layer of pyramid in Graph 1): the choice of the operational architecture, and how it will balance the consumer's demand for a cash-like claim on the central bank with the convenience that intermediaries confer on the payment system. The choice is shaped by two questions. Is the CBDC a direct claim on the central bank or is the claim indirect, via payment intermediaries? What is the operational role of the central bank and of private sector intermediaries in day-to-day payments?

Further, the consumer's need for cash-like payment safety means that a CBDC must be secure not only from the insolvency or technical glitches of intermediaries, but also from outages at the central bank. The choice is whether to base this infrastructure on a conventional centrally controlled database or instead on DLT – technologies that differ in their efficiency and degree of protection from single

The CBDC pyramid

Graph 1


From consumer needs...
...to CBDC design choices
Cross-border payments
Wholesale or retail **interlinkages**?
Accessible to all
Ensure **privacy** in lawful exchange
Account or token-based **access technology**?
Resilient and robust operations
DLT-based or conventional **central bank infrastructure**?
Convenient real-time payments
Cash-like with **peer-to-peer** functionality
Architecture: indirect or direct claims, and what operational role for the central bank?
Lower-level choices feed into subsequent decisions

The CBDC pyramid maps consumer needs (left-hand side) onto the associated design choices for the central bank (right-hand side). The four layers of the right-hand side form a hierarchy in which the lower layers represent design choices that feed into subsequent, higher-level decisions.

Source: Authors' elaboration.

[5] In Sweden, where cash use has already declined substantially, considerations along these lines have led the central bank to propose a review of the concept of legal tender (Sveriges Riksbank (2019)).

points of failure. Importantly, this decision can only be made once the architecture has been decided upon, as DLT is only feasible for some operational setups. This is why the choice of infrastructure lies in the pyramid's second layer.

Two further consumer needs are easy, universal access and privacy by default.[6] From a technical perspective, there is an underlying trade-off between privacy and ease of access on the one hand and ease of law enforcement on the other. The associated design choice – the pyramid's third layer – is whether access to the CBDC is tied to an identity system (ie an account-based technology) or instead via cryptographic schemes that do not require identification (ie an access technology based on so-called digital tokens).

The final consumer need we consider is that CBDCs should also enable cross-border payments. At a design level, this could be arranged via technical connections at the wholesale level that are built on today's systems. Alternatively, novel interlinkages could be envisaged at the retail level, ie allowing consumers to hold foreign digital currencies directly. Importantly, the means of implementing the latter option would depend on whether the CBDC was account- or token-based. This is why this design choice belongs in the top layer of the pyramid.

Architecture: indirect or direct claims, and the operational role for the central bank

The CBDC pyramid's bottom layer is the legal structure of claims and the respective operational roles of the central bank and private institutions in payments. Our analysis starts with an overview of possible technical architectures for CBDCs. In all three architectures shown in Graph 2, the central bank is, by definition, the only party issuing and redeeming CBDC. We note that all three architectures could be either account- or token-based, and might run on various infrastructures. These choices are discussed below.

The key differences here are in the structure of legal claims and the record kept by the central bank. In the "indirect CBDC" model (Graph 2, top panel), the consumer has a claim on an intermediary, with the central bank keeping track only of wholesale accounts. In the "direct CBDC" model (centre panel), the CBDC represents a direct claim on the central bank, which keeps a record of all balances and updates it with every transaction. The "hybrid CBDC" model (bottom panel), is an intermediate solution providing for direct claims on the central bank while allowing intermediaries to handle payments.

Consider first the indirect CBDC model (top panel). This term is used by Kumhof and Noone (2018), and is equivalent to the "synthetic CBDC" in Adrian and Mancini-Griffoli (2019). This model is also known as the "two-tier CBDC" for its resemblance to the existing two-tier financial system; a token-based variant is proposed as a "multi-cell CBDC" in Ali (2018). For consumers, this type of CBDC is not a direct claim on the central bank. Instead, the intermediary (labelled "CBDC bank" in Graph 2 for its close resemblance to a narrow payment bank) is mandated to fully back each outstanding indirect CBDC-like liability to the consumer (labelled "ICBDC"

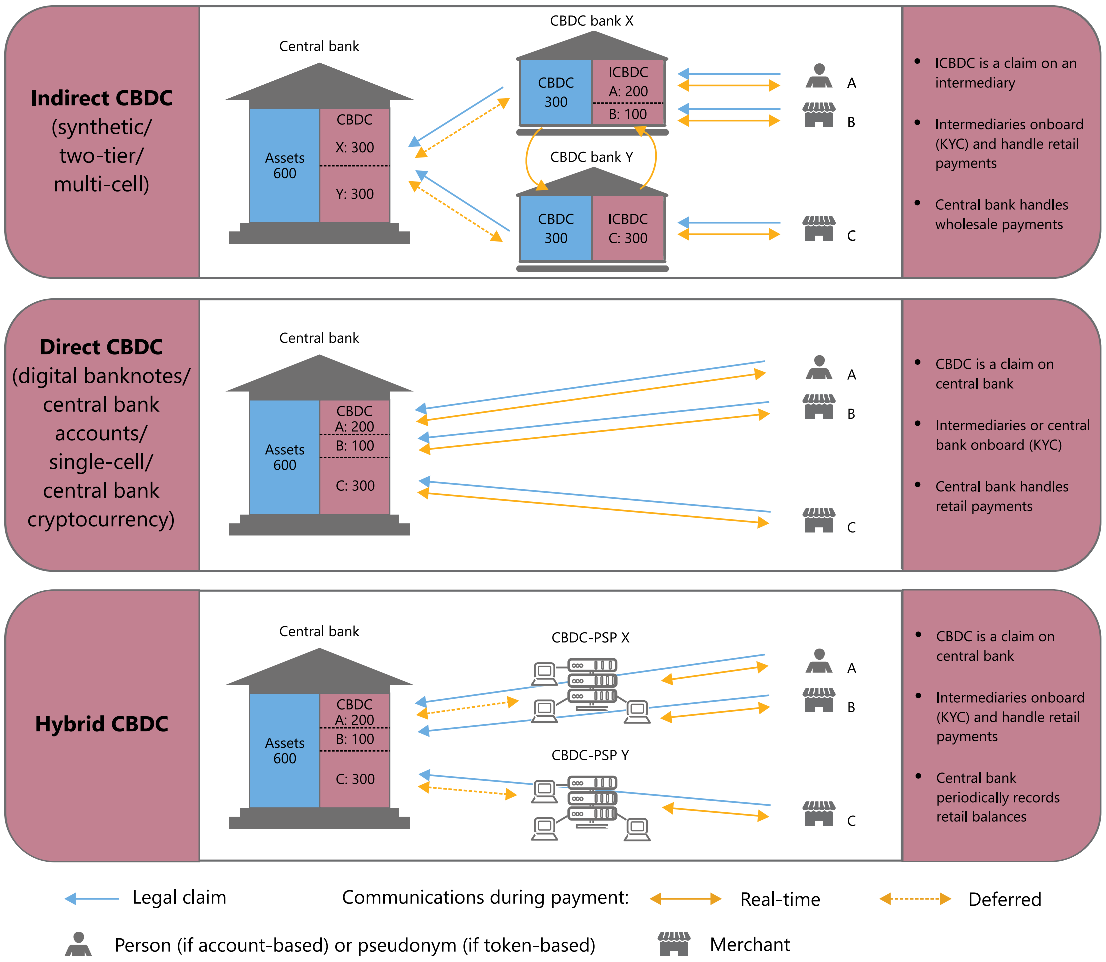
[6] Privacy here means that the consumer's data are used only in steps strictly necessary for the specific purpose of determining whether a transaction is lawful and, if this the case, executing it. "By default" implies that privacy is ensured without requiring any intervention by the user.

in Graph 2) to retail consumers via its holding of actual CBDCs (or other central bank money) deposited at the central bank.[7] Just as in today's system, intermediaries handle all communication with retail clients, net payments and send payment messages to other intermediaries and wholesale payment instructions to the central bank. The latter settles wholesale CBDC accounts with finality.

Besides offering the convenience of today's systems based on intermediaries, the indirect CBDC also relieves the central bank of the responsibility for dispute

An overview of potential retail CBDC architectures

Graph 2


Indirect CBDC
(synthetic/
two-tier/
multi-cell)
Central bank
Assets
600
CBDC
X: 300
Y: 300
CBDC bank X
CBDC
300
ICBDC
A: 200
B: 100
CBDC bank Y
CBDC
300
ICBDC
C: 300
A
B
C
ICBDC is a claim on an intermediary
Intermediaries onboard (KYC) and handle retail payments
Central bank handles wholesale payments
Direct CBDC
(digital banknotes/
central bank
accounts/
single-cell/
central bank
cryptocurrency)
Central bank
Assets
600
CBDC
A: 200
B: 100
C: 300
A
B
C
CBDC is a claim on central bank
Intermediaries or central bank onboard (KYC)
Central bank handles retail payments
Hybrid CBDC
Central bank
Assets
600
CBDC
A: 200
B: 100
C: 300
CBDC-PSP X
CBDC-PSP Y
A
B
C
CBDC is a claim on central bank
Intermediaries onboard (KYC) and handle retail payments
Central bank periodically records retail balances
Legal claim
Communications during payment:
Real-time
Deferred
Person (if account-based) or pseudonym (if token-based)
Merchant

In all three architectures, the CBDC is issued only by the central bank. In the indirect CBDC architecture (top panel), this is done indirectly, and an ICBDC in the hands of consumers represents a claim on an intermediary. In the other two architectures, consumers have a direct claim on the central bank. In the direct CBDC model (centre panel), the central bank handles all payments in real time and thus keeps a record of all retail holdings. The hybrid CBDC model (bottom panel) is an intermediate solution providing for direct claims on the central bank while real-time payments are handled by intermediaries. In this architecture, the central bank retains a copy of all retail CBDC holdings, allowing it to transfer holdings from one payment service provider to another in the event of a technical failure. All three architectures allow for either account- or token-based access.

Source: Authors' elaboration.

[7] Some have argued that this architecture does not warrant the CBDC label. However, the label does apply if one follows CPMI-MC (2018) in defining a retail CBDC as any claim on the central bank that is different from today's wholesale accounts (see also Bech and Garratt (2017)).

resolution, know-your-customer (KYC) and related services. But the downside is that the central bank keeps no record of individual claims (only the intermediaries do, whereas the central bank records only wholesale holdings) nor is there any cash-like direct proof of the claim. Thus, the central bank cannot honour claims from consumers without information from the intermediary.[8] If the intermediary is under stress, determining the legitimate owner might involve a potentially lengthy and costly legal process with an uncertain outcome. This model's regulatory and supervisory issues, as well as those pertaining to deposit insurance, are hence similar to those of today's system.

Consider next a CBDC directly operated by the central bank, the direct CBDC architecture (centre panel). One version would comprise accounts managed by the central bank. Several private sector companies are developing token-based variants, or "digital banknotes".[9] In this architecture, KYC and customer due diligence could be handled by the private sector or the central bank or another public sector institution. The central bank, however, would be the only institution handling payment services.

The direct CBDC is attractive for its simplicity, as it eliminates dependence on intermediaries by doing away with them. However, this entails compromises in terms of the payment system's reliability, speed and efficiency. One aspect is that building and operating technical capacity on this scale is often viewed as being better undertaken by the private sector, as seen in today's credit card networks. Second, even if a central bank were to build the necessary technological capability, the resulting CBDC might be less attractive to consumers than today's retail payment systems. Electronic payments must deal with connectivity outages or offline payments, which involves risk-taking by intermediaries. Importantly, it is the customer relationship – based on KYC – that allows the intermediary to accept such risks. Unless a central bank were to take on responsibility for KYC and customer due diligence – which would require a massive expansion of operations, well beyond existing mandates – it would find it difficult to provide this service.[10]

In addition to these two pure options, one can also envisage novel future solutions that merge elements of both the indirect and the direct CBDC.[11] We label this third type of architecture the hybrid CBDC (bottom panel). In this model, a direct claim on the central bank is combined with a private sector messaging layer. Again, variations on this theme might include both token- and account-based ones.

One key element of the hybrid CBDC architecture is the legal framework that underpins claims, keeps them segregated from the balance sheets of the payments service providers (PSPs), and allows for portability. If a PSP fails, holdings of the

[8] A further difficulty is that it is unclear what the holder of an ICBDC would actually be entitled to, as, by definition, retail investors are prohibited from holding the actual CBDCs issued by the central bank.

[9] These token-based versions are termed "single-cell" CBDC structures in Ali (2018) and "central bank cryptocurrencies" in Berentsen and Schär (2018).

[10] The respective advantages and disadvantages of direct and indirect CBDC architectures mirror those of the direct and indirect security holding systems that are discussed in the context of the future of settlement in Bech, Hancock, Rice and Wadsworth (2020, in this issue).

[11] Although these authors do not spell out the underlying structure of legal claims, several ways to distribute payment functions and communications over multiple parties have been studied in the field of computer science. One example is the proposal of Danezis and Meiklejohn (2016), which shifts real-time communications from the central bank to dynamically appointed intermediaries.

CBDC are not considered part of the PSP's estate available to creditors. The legal framework should also allow for portability in bulk, ie give the central bank the power to switch retail customer relationships from a failing PSP to a fully functional one.[12] The second key element is the technical capability to enable the portability of holdings. Since the requirement is to sustain payments when one intermediary is under technical stress, the central bank must have the technical capability to restore retail balances. It thus retains a copy of all retail CBDC holdings, allowing it to transfer retail CBDC holdings from one PSP to another in the event of a technical failure.[13]

The hybrid CBDC would have both advantages and disadvantages vis-à-vis the indirect or direct CBDC architectures. As an intermediate solution, it might offer better resilience than the indirect CBDC, but at the cost of a more complex to operate infrastructure for the central bank. On the other hand, the hybrid CBDC is still simpler to operate than a direct CBDC. As the central bank does not directly interact with retail users, it can concentrate on a limited number of core processes, while intermediaries handle other services including instant payment confirmation.

Conventional or DLT-based central bank infrastructure?

What infrastructure might the different CBDC architectures require for the central bank, and how could they be implemented in the most resilient way? This choice, represented as the second tier of the CBDC pyramid, follows immediately after the decision on architecture because the infrastructure requirements for the central bank differ substantially across the three architectures shown in Graph 2.

For the central bank, the indirect CBDC implies loads similar to those of today's system. By contrast, the direct CBDC would require massive technological capabilities, as the central bank processes all transactions by itself, handling a volume of payments traffic comparable with that of today's credit or debit card operators. The hybrid CBDC architecture is more complex to operate than the indirect model, as the central bank does maintain retail balances. Nevertheless, it could be implemented at scale using today's technology and with a relatively modest infrastructure even in the world's largest currency areas.[14]

The infrastructure could be based on a conventional centrally controlled database, or on a novel distributed ledger. Graph 3 shows how elements of DLT could play a role in CBDC. The first DLT-related design choice hinges on whether

[12] While functionally similar, such segregation differs from deposit insurance in terms of legal procedures and associated delays. Today's deposits are often insured but, in the case of a bank failure, the funds can only be retrieved through a reimbursement process. Further, deposit insurance may be limited in amount and ultimately depends on the strength of the deposit insurer (see Baudino et al (2019) for an overview).

[13] Note that a variant of this CBDC architecture could allow users to retain cryptographic proofs of their CBDC balances, rather than oblige the central bank to hold them. These proofs could be used to retrieve balances in case of a technical failure. The advantage would be to circumvent potential privacy and legal issues connected with the central bank storing retail account balances. The disadvantage would be that entrusting users with cryptographic proofs may open the door to loss and theft of funds.

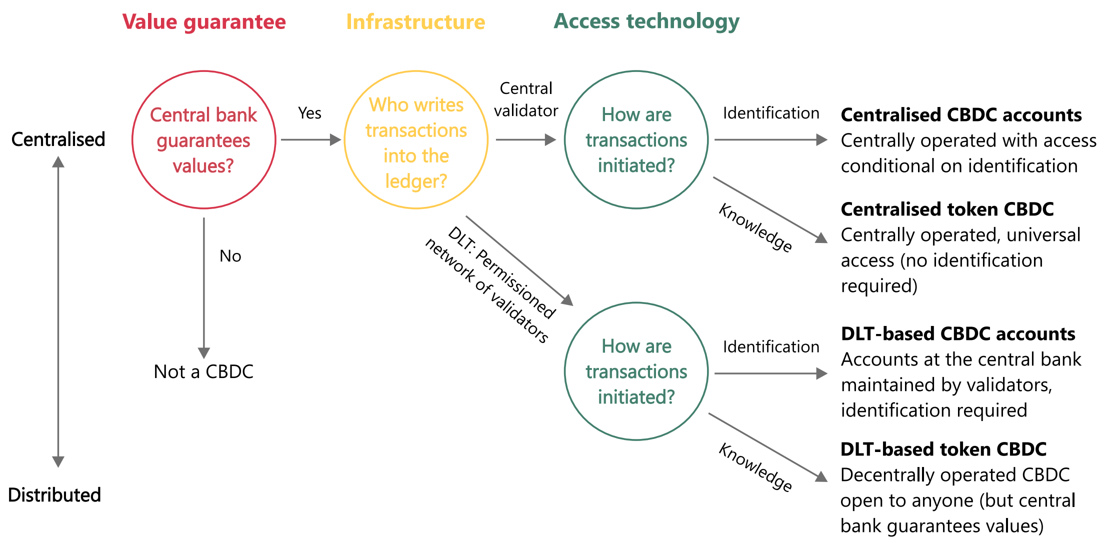
[14] For example, even for a payment area with a billion users, it would be feasible to verify each digital signature (computationally, the most costly operation of a transaction) for all accounts on an hourly basis with a two-digit number of standard servers.

the authority to update the database is centralised or delegated to a network of identified and vetted validators.[15]

Conventional and DLT-based infrastructures often store data multiple times and in physically separate locations. The main difference between them lies in how data are updated. In conventional databases, resilience is typically achieved by storing data over multiple physical nodes, which are controlled by one authoritative entity – the top node of a hierarchy. By contrast, in many DLT-based systems, the ledger is jointly managed by different entities in a decentralised manner and without such a top node. Consequently, each update of the ledger has to be harmonised between the nodes of all entities (often using algorithms known as "consensus mechanisms"). This typically involves broadcasting and awaiting replies on multiple messages before a transaction can be added to the ledger with finality.

The overhead needed to operate a consensus mechanism is the main reason why DLTs have lower transaction throughput than conventional architectures. Specifically, these limits imply that current DLT could not be used for the direct CBDC except in very small jurisdictions, given the probable volume of data throughput. However, DLT could be used for the indirect CBDC architecture, as the number of transactions in many wholesale payment systems is comparable with that handled by existing blockchain platforms, as also demonstrated in several wholesale

Elements of decentralisation: DLT and token-based access Graph 3


Value guarantee
Infrastructure
Access technology
Centralised
Distributed
Central bank guarantees values?
Yes
No
Not a CBDC
Who writes transactions into the ledger?
Central validator
DLT: Permissioned network of validators
How are transactions initiated?
Identification
Knowledge
How are transactions initiated?
Identification
Knowledge
Centralised CBDC accounts
Centrally operated with access conditional on identification
Centralised token CBDC
Centrally operated, universal access (no identification required)
DLT-based CBDC accounts
Accounts at the central bank maintained by validators, identification required
DLT-based token CBDC
Decentrally operated CBDC open to anyone (but central bank guarantees values)

This graph maps out the four possible combinations of whether a CBDC infrastructure is distributed or centralised and whether access is based on identification (accounts) or cryptographic knowledge (digital tokens). All four combinations are possible for any CBDC architecture (indirect, direct or hybrid), but in the different architectures, the central bank and the private sector operate different parts of the respective infrastructure.

Source: Authors' elaboration.

[15] Most likely, central banks would consider only "permissioned" DLT, in which a network of pre-selected entities performs the updating. While it is technically possible to use "permissionless" technology, in which unknown validators perform the updating, the economic cost of this process is very high (see Böhme et al (2015) for an introduction for the case of Bitcoin, Auer (2019a) for a discussion of the underlying economics and Ali and Narula (2020) for a specific analysis in the context of CBDCs).

CBDC experiments conducted by central banks (Bech, Hancock, Rice and Wadsworth (2020, in this issue)). Enterprise versions of DLT might also be feasible for the hybrid CBDC architecture.

When it comes to achieving resilience, neither a DLT-based system nor a conventional one has a clear-cut advantage. The vulnerabilities are simply different. The key vulnerability of a conventional architecture is the failure of the top node, for example via a targeted hacking attack. The key vulnerability of DLT is the consensus mechanism, which may be put under pressure, for example, by a denial-of-service type of attack.

Overall, one needs to weigh carefully 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,[16] which is advantageous only if one trusts this network to operate more reliably than the central bank. Ongoing assessments of DLT-based proofs-of-concept tend to be negative (see box for a brief overview). Among the DLT-based projects that are still ongoing, it remains to be seen whether scalable implementations will actually rely on the technology.[17]

That said, even if one decides against using DLT as the backbone infrastructure of a CBDC, one closely related technology might still be useful. Whether or not the infrastructure is based on DLT, access can still be based on cryptography rather than identification – Graph 3 outlines the possible combinations, and the box shows which combinations are being investigated by central banks.

Token- or account-based access, and how to safeguard privacy?

Once the CBDC's architecture and infrastructure have been chosen, the question arises of how and to whom one should give access. This is the third layer of the CBDC pyramid.

A first option is to follow the conventional account model and tie ownership to an identity (Graph 4, left-hand side). Claims are represented in a database that records the value along with a reference to the identity, just as in a bank account. This has drawbacks in the case of CBDCs. In particular, it depends on "strong" identities for all account holders – schemes that map each individual to one and only one identifier across the entire payment system. Such schemes can present a challenge in some jurisdictions, thus impairing universal access.[18]

The second option is for the central bank to honour claims solely when the CBDC user demonstrates knowledge of an encrypted value – an option sometimes

[16] In the indirect CBDC architecture, validators of the central bank ledger update the wholesale accounts, while in the hybrid and direct architectures they update the retail accounts.

[17] Experiments are based on enterprise versions of distributed ledgers, which allow for decentralisation but, in practice, are often run under centralised control. Ali and Narula (2020, p 6) note that the platforms typically used "are useful for experimentation and prototyping because of their flexibility and features […]. However, what is helpful for prototyping might not be good for practice; these complex platforms make trade-offs when it comes to security, stability, and scale."

[18] There are broader benefits to universal digital identity frameworks, such as the scope for supporting open banking and enabling the distribution of other financial services. D'Silva et al (2019) discuss the Indian experience.

referred to as digital tokens (Graph 4, right-hand side). One example is when the secret part of a public-private key pair is used to sign a message, a technology outlined by Auer, Böhme and Wadsworth (2020, in this issue).

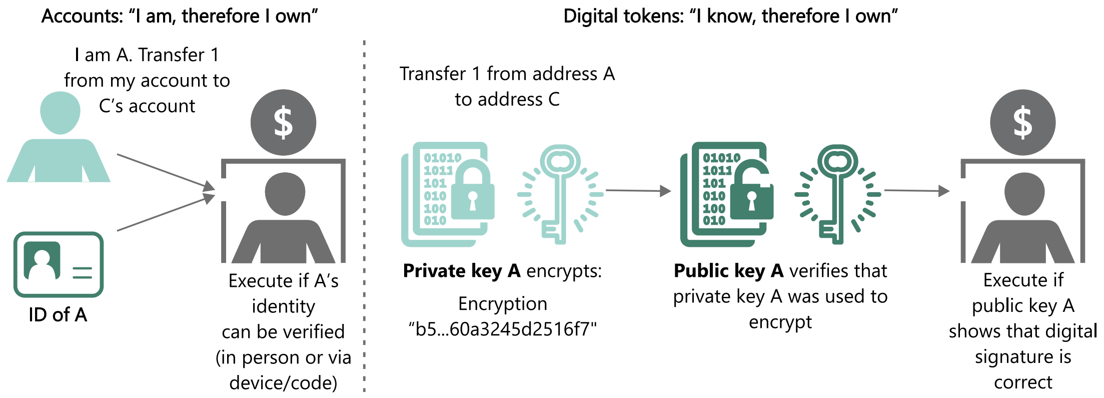
A token-based system would ensure universal access – as anybody can obtain a digital signature – and it would offer good privacy by default. It would also allow the CBDC to interface with communication protocols, ie be the basis for micropayments in the internet of things. But the downsides are severe. One is the high risk of losing funds if end users fail to keep their private key secret. Moreover, challenges would arise in designing an effective AML/CFT framework for such a system. Law enforcement authorities would run into difficulties when seeking to identify claim owners or follow money flows, just as with cash or bearer securities. Retail CBDCs would thus need additional safeguards if they followed this route.[19]

We emphasise that the privacy dimension goes far beyond the question of whether the system is based on accounts or digital tokens. Transaction-level financial data reveal sensitive personal data. Hence, two aspects of privacy by default are crucial for the design of a CBDC. First is the amount of personal information transaction partners learn about each other when the system is operating normally.[20] Second is the risk of large-scale breaches of data held by the system operator or intermediaries.

Crucially, a CBDC that lets merchants collect and link payment data to customer profiles transforms the very nature of payments, from a simple exchange of value to the exchange of value for a bundle of data. Hence, a CBDC should preserve its users' privacy vis-à-vis their transaction partners, ie by default, transaction partners

Account-based access compared with token-based access

Graph 4


Accounts: "I am, therefore I own"
I am A. Transfer 1 from my account to C's account
$
ID of A
Execute if A's identity can be verified (in person or via device/code)
Digital tokens: "I know, therefore I own"
Transfer 1 from address A to address C
01010 1011 101 010 100 010
Private key A encrypts:
Encryption "b5...60a3245d2516f7"
Public key A verifies that private key A was used to encrypt
$
Execute if public key A shows that digital signature is correct

In an account-based CBDC (left-hand side), ownership is tied to an identity, and transactions are authorised via identification. In a CBDC based on digital tokens (right-hand side), claims are honoured based solely on demonstrated knowledge, such as a digital signature.

Source: Authors' elaboration.

[19] The legal framework would need to allow claims to be put "on hold" until the legitimacy of a transaction history has been demonstrated (Böhme et al (2015)). This could be part of a broader regulatory framework allowing for "embedded supervision", ie an approach in which supervisory and other public authorities automatically monitor market ledgers to check for compliance with regulatory goals (Auer (2019b)).

[20] See ECB (2019) for a practical proposal and Frost et al (2019) for a broader discussion of the use of data in finance.

would interact via "unlikable pseudonyms", as envisaged in Chaum's (1985) pioneering work on electronic money. In such a system, a merchant is presented with a proof that the payment for a specific invoice has been made, but no information about the payee is revealed.

Depending on the involvement of intermediaries and the information they receive, technical safeguards for data protection need to be complemented by a legal framework restricting data collection by front-end applications, for example the smartphone payment app. Data loss is a further threat, given that payment systems are a prime target for cyber attacks. In this context, it must be noted that not all privacy-enhancing technologies are mature. For example, some so-called zero-knowledge proofs have already been shown to be vulnerable (Ruffing et al (2018)). The only sure-fire way to avoid losing much data is not to store it or to irrevocably delete old transactions as soon as possible. This principle of data minimisation is embodied in many data protection laws. Where this is not an option, aggregation and anonymisation must be relied on. A last resort is storage in physically separated (and offline) places guarded by legal access procedures.

Cross-border payments: wholesale or retail linkages?

Once a CBDC's configuration is clear, as well as how resident consumers can access it, the question arises whether it can be used only domestically or also elsewhere. This is the topmost layer of the CBDC pyramid.

The demand for seamless and inexpensive cross-border payments has grown in parallel with growth in international e-commerce, remittances and tourism. A CBDC might come with the same wholesale interlinkage options explored in the current system (Bech, Faruqui and Shirakami (2020, in this issue)).

Here, one noteworthy aspect is that a coordinated CBDC design effort could take a clean-slate perspective and incorporate these interlinkage options right from the start. This would represent a unique opportunity to facilitate easier cross-border payments (eg Carney (2019) and Cœuré (2019)), reducing inefficiencies and rents by shortening the payment value chain.

CBDCs would also permit novel retail interlinkages if they were to allow consumers to hold multiple currencies. In today's account-based system, a cross-border transaction is inseparably linked to a foreign exchange transaction. The intermediary processing the transaction can apply extra fees and unfavourable exchange rates. In contrast, if consumers were given the option of buying foreign currency in advance, before spending it abroad, just as they can with cash, this would separate the payment from the foreign exchange transaction. In turn, this would open up the possibility of interfacing retail wallets directly with competitive foreign exchange markets.

Importantly, the scope for such retail interlinkages and their design would depend on the national access framework. If a national system is based on digital tokens, it will by default be accessible to foreign residents. If it is account-based, interoperability would be a design choice, one that could also be coordinated internationally.

Reading Materials

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

Conclusion

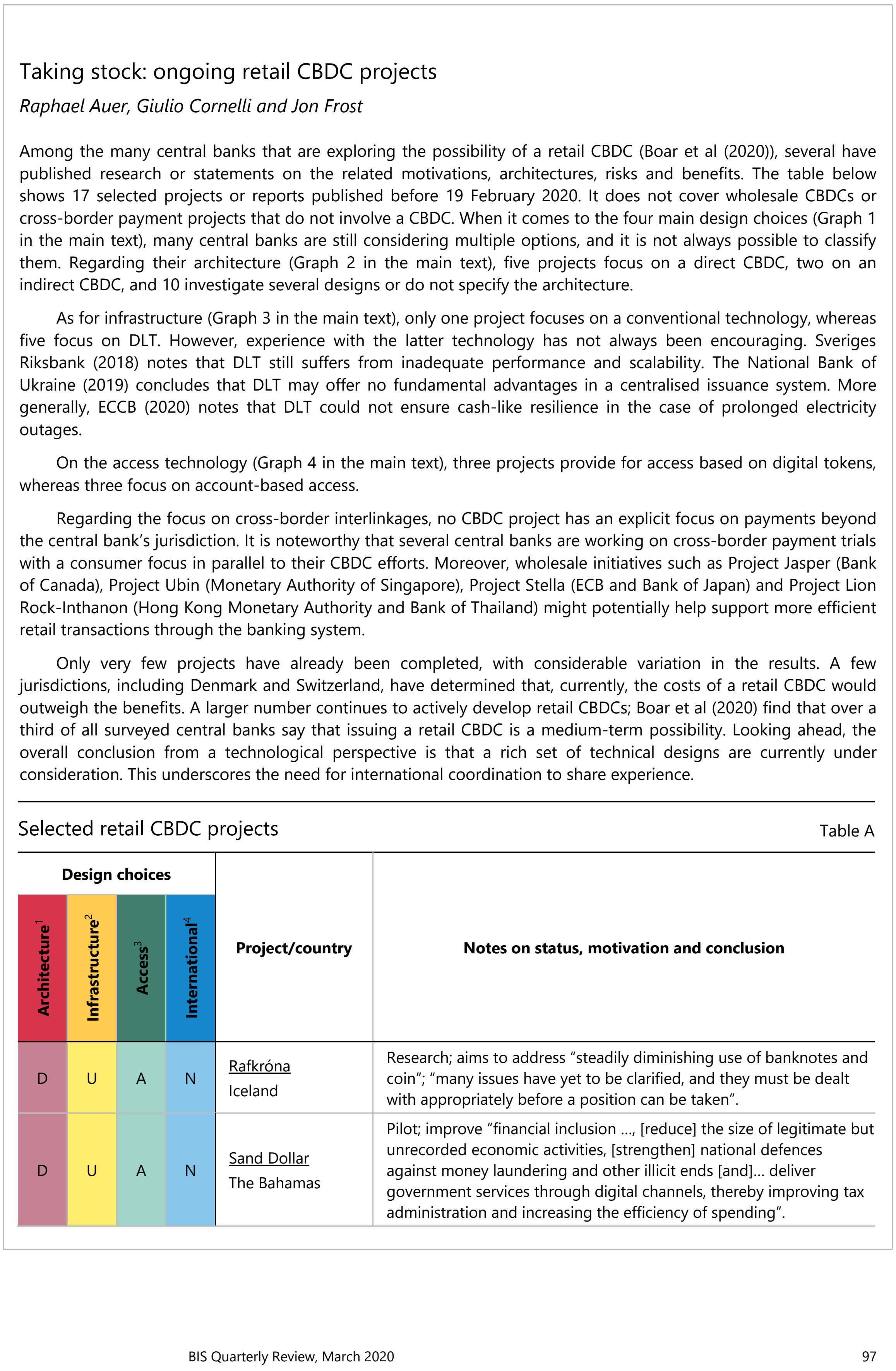
As central banks play a key role in payment systems, both the declining use of cash and related developments in the private sector may require them to “step up” and take a more active role (Carstens (2019 and 2020, in this issue)). Should they wish to do so, many ways are open to them.

This feature has gone down a hypothetical road by investigating the choices that might be encountered during the design stage of a CBDC, and how the related decision-making process could be structured. On the way, we have highlighted how consumer needs might translate into technical trade-offs. Some design-related considerations emerge from our analysis, for example, regarding the feasibility of DLT-based vis-à-vis that of more conventional technical infrastructures, but other choices remain less clear-cut.

With a framework for decision-making in mind, more hands-on experience with specific design choices could be helpful. The box surveys ongoing technical design efforts by central banks along the technical dimensions identified in this feature. As most projects are still in their early stages, the most important takeaway is that central banks around the world are investigating a rich set of prototypes, spanning almost the full range of potential designs encompassed in the CBDC pyramid. If the results of these experiments are shared internationally, a clearer picture will emerge of which technological choices are generally suited for CBDCs, and how the optimal design might depend on the specific circumstances of each jurisdiction. This, in turn, could help to inform the debate on whether and how CBDCs should actually be issued.

Reading Materials

Source: **Auer, R. and R. Boehme. 2020. "The Technology of Retail Central Bank Digital Currency," Bank for International Settlements Quarterly Review, March.**



Taking stock: ongoing retail CBDC projects

Raphael Auer, Giulio Cornelli and Jon Frost

Among the many central banks that are exploring the possibility of a retail CBDC (Boar et al (2020)), several have published research or statements on the related motivations, architectures, risks and benefits. The table below shows 17 selected projects or reports published before 19 February 2020. It does not cover wholesale CBDCs or cross-border payment projects that do not involve a CBDC. When it comes to the four main design choices (Graph 1 in the main text), many central banks are still considering multiple options, and it is not always possible to classify them. Regarding their architecture (Graph 2 in the main text), five projects focus on a direct CBDC, two on an indirect CBDC, and 10 investigate several designs or do not specify the architecture.

As for infrastructure (Graph 3 in the main text), only one project focuses on a conventional technology, whereas five focus on DLT. However, experience with the latter technology has not always been encouraging. Sveriges Riksbank (2018) notes that DLT still suffers from inadequate performance and scalability. The National Bank of Ukraine (2019) concludes that DLT may offer no fundamental advantages in a centralised issuance system. More generally, ECCB (2020) notes that DLT could not ensure cash-like resilience in the case of prolonged electricity outages.

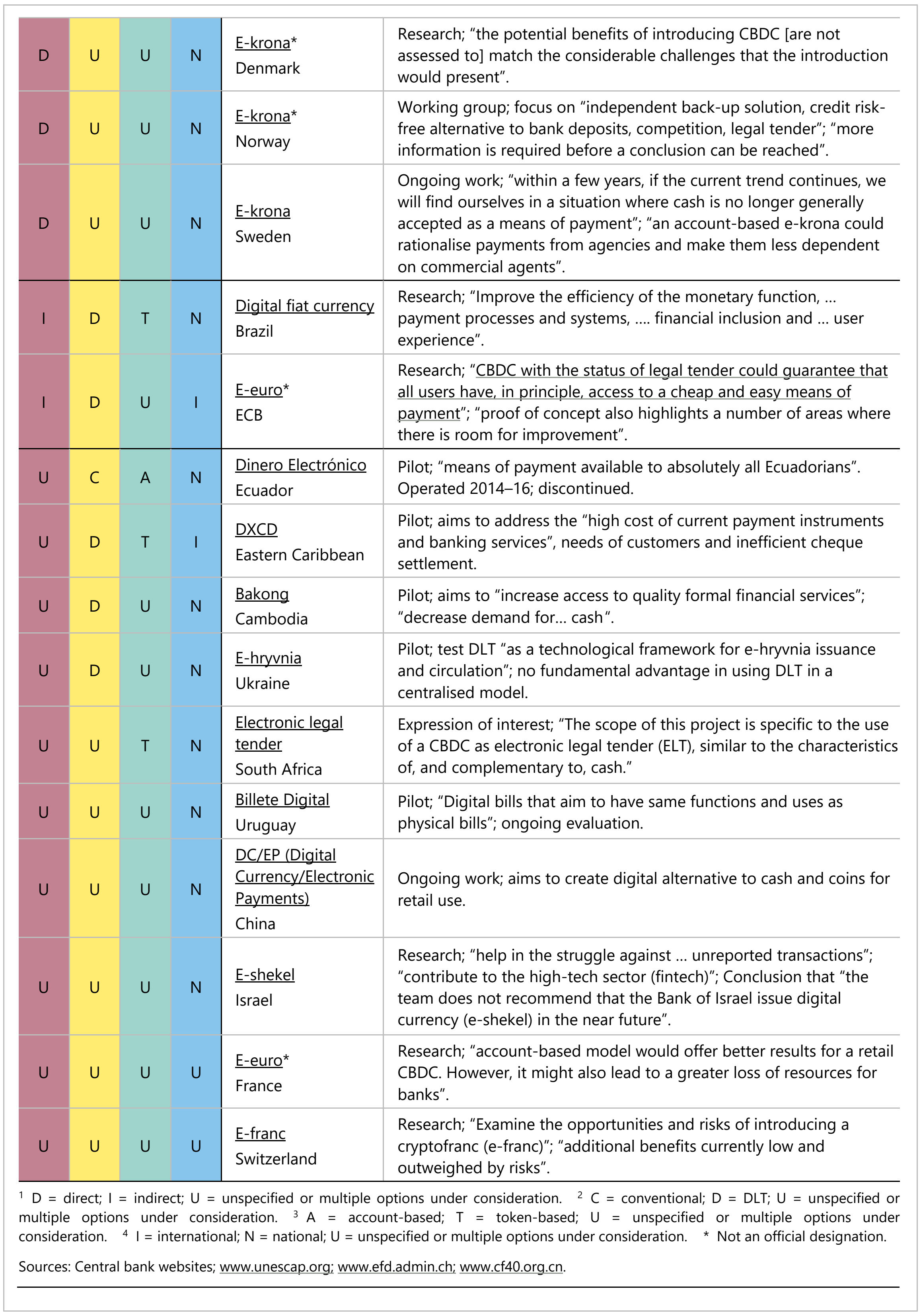
On the access technology (Graph 4 in the main text), three projects provide for access based on digital tokens, whereas three focus on account-based access.

Regarding the focus on cross-border interlinkages, no CBDC project has an explicit focus on payments beyond the central bank's jurisdiction. It is noteworthy that several central banks are working on cross-border payment trials with a consumer focus in parallel to their CBDC efforts. Moreover, wholesale initiatives such as Project Jasper (Bank of Canada), Project Ubin (Monetary Authority of Singapore), Project Stella (ECB and Bank of Japan) and Project Lion Rock-Inthanon (Hong Kong Monetary Authority and Bank of Thailand) might potentially help support more efficient retail transactions through the banking system.

Only very few projects have already been completed, with considerable variation in the results. A few jurisdictions, including Denmark and Switzerland, have determined that, currently, the costs of a retail CBDC would outweigh the benefits. A larger number continues to actively develop retail CBDCs; Boar et al (2020) find that over a third of all surveyed central banks say that issuing a retail CBDC is a medium-term possibility. Looking ahead, the overall conclusion from a technological perspective is that a rich set of technical designs are currently under consideration. This underscores the need for international coordination to share experience.

Selected retail CBDC projects — Table A

Design choices				**Project/country**	**Notes on status, motivation and conclusion**
Architecture[1]	**Infrastructure**[2]	**Access**[3]	**International**[4]		
D	U	A	N	Rafkróna Iceland	Research; aims to address "steadily diminishing use of banknotes and coin"; "many issues have yet to be clarified, and they must be dealt with appropriately before a position can be taken".
D	U	A	N	Sand Dollar The Bahamas	Pilot; improve "financial inclusion ..., [reduce] the size of legitimate but unrecorded economic activities, [strengthen] national defences against money laundering and other illicit ends [and]... deliver government services through digital channels, thereby improving tax administration and increasing the efficiency of spending".



D	U	U	N	E-krona* Denmark	Research; “the potential benefits of introducing CBDC [are not assessed to] match the considerable challenges that the introduction would present”.
D	U	U	N	E-krona* Norway	Working group; focus on “independent back-up solution, credit risk-free alternative to bank deposits, competition, legal tender”; “more information is required before a conclusion can be reached”.
D	U	U	N	E-krona Sweden	Ongoing work; “within a few years, if the current trend continues, we will find ourselves in a situation where cash is no longer generally accepted as a means of payment”; “an account-based e-krona could rationalise payments from agencies and make them less dependent on commercial agents”.
I	D	T	N	Digital fiat currency Brazil	Research; “Improve the efficiency of the monetary function, … payment processes and systems, …. financial inclusion and … user experience”.
I	D	U	I	E-euro* ECB	Research; “CBDC with the status of legal tender could guarantee that all users have, in principle, access to a cheap and easy means of payment”; “proof of concept also highlights a number of areas where there is room for improvement”.
U	C	A	N	Dinero Electrónico Ecuador	Pilot; “means of payment available to absolutely all Ecuadorians”. Operated 2014–16; discontinued.
U	D	T	I	DXCD Eastern Caribbean	Pilot; aims to address the “high cost of current payment instruments and banking services”, needs of customers and inefficient cheque settlement.
U	D	U	N	Bakong Cambodia	Pilot; aims to “increase access to quality formal financial services”; “decrease demand for… cash“.
U	D	U	N	E-hryvnia Ukraine	Pilot; test DLT “as a technological framework for e-hryvnia issuance and circulation”; no fundamental advantage in using DLT in a centralised model.
U	U	T	N	Electronic legal tender South Africa	Expression of interest; “The scope of this project is specific to the use of a CBDC as electronic legal tender (ELT), similar to the characteristics of, and complementary to, cash.”
U	U	U	N	Billete Digital Uruguay	Pilot; “Digital bills that aim to have same functions and uses as physical bills”; ongoing evaluation.
U	U	U	N	DC/EP (Digital Currency/Electronic Payments) China	Ongoing work; aims to create digital alternative to cash and coins for retail use.
U	U	U	N	E-shekel Israel	Research; “help in the struggle against … unreported transactions”; “contribute to the high-tech sector (fintech)”; Conclusion that “the team does not recommend that the Bank of Israel issue digital currency (e-shekel) in the near future”.
U	U	U	U	E-euro* France	Research; “account-based model would offer better results for a retail CBDC. However, it might also lead to a greater loss of resources for banks”.
U	U	U	U	E-franc Switzerland	Research; “Examine the opportunities and risks of introducing a cryptofranc (e-franc)”; “additional benefits currently low and outweighed by risks”.

[1] D = direct; I = indirect; U = unspecified or multiple options under consideration. [2] C = conventional; D = DLT; U = unspecified or multiple options under consideration. [3] A = account-based; T = token-based; U = unspecified or multiple options under consideration. [4] I = international; N = national; U = unspecified or multiple options under consideration. * Not an official designation.

Sources: Central bank websites; www.unescap.org; www.efd.admin.ch; www.cf40.org.cn.

References

Adrian, T (2019): "Stablecoins, central bank digital currencies, and cross-border payments", lecture at International Monetary Fund-Swiss National Bank Conference, Zurich, 14 May.

Adrian, T and T Mancini-Griffoli (2019): "The rise of digital money", *IMF Note*, no 19/001, July.

Ali, R (2018): "Cellular structure for a digital fiat currency", paper presented at the P2P financial system international workshop, Federal Reserve Bank of Cleveland, 27 July.

Ali, R and N Narula (2020): "Redesigning digital money: what can we learn from a decade of cryptocurrencies?", *MIT DCI Working Papers*, January.

Andolfatto, D (2018): "Assessing the impact of central bank digital currency on private banks", Federal Reserve Bank of St Louis, *Working Papers*, no 2018-25.

Auer, R (2019a): "Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies", *BIS Working Papers*, no 765.

——— (2019b): "Embedded supervision: how to build regulation into blockchain finance", *BIS Working Papers*, no 811.

Auer, R, R Böhme and A Wadsworth (2020): "An introduction to public-private key cryptography in digital tokens", *BIS Quarterly Review*, March, p 73.

Baudino, P, R Defina, J Fernández Real, K Hajra and R Walters (2019): "Bank failure management – the role of deposit insurance", *FSI Insights on policy implementation*, no 17, August.

Bech, M and R Garratt (2017): "Central bank cryptocurrencies", *BIS Quarterly Review*, September, pp 55–70.

Bech, M, U Faruqui and T Shirakami (2020): "Payments without borders", *BIS Quarterly Review*, March, pp 53–65.

Bech, M, J Hancock, T Rice and A Wadsworth (2020): "On the future of securities settlement", *BIS Quarterly Review*, March, pp 67–83.

Berentsen, A and F Schär (2018): "The case for central bank electronic money and the non-case for central bank cryptocurrencies", *Federal Reserve Bank of St Louis Review*, vol 100, no 2, pp 97–106.

Bindseil, U (2020): "Tiered CBDC and the financial system", *ECB Working Paper Series*, no 2351.

Bjerg, O (2017): "Designing new money – The policy trilemma of central bank digital currency", *Copenhagen Business School Working Papers*.

Boar, C, H Holden and A Wadsworth (2020): "Impending arrival – a sequel to the survey on central bank digital currency", *BIS Papers*, no 107, January.

Böhme, R, N Christin, B Edelman and T Moore (2015): "Bitcoin: economics, technology, and governance", *Journal of Economic Perspectives*, vol 29, no 2, pp 213–38.

Brunnermeier, M and D Niepelt (2019): "On the equivalence of private and public money", *Journal of Monetary Economics*, vol 106, pp 27–41.

Carstens, A (2019): ”The future of money and the payment system: what role for central banks?”, lecture at Princeton University, 5 December.

——— (2020): “Shaping the future of payments”, *BIS Quarterly Review*, March, pp 17–20.

Chaum, D (1985): “Security without identification: transaction systems to make big brother obsolete”, *Communications of the ACM*, vol 28, no 10, pp 1030–44.

Cœuré, B (2019): “Digital challenges to the international monetary and financial system”, conference on “The future of the international monetary system”, Luxembourg, 17 September.

Committee on Payments and Market Infrastructures and Markets Committee (2018): *Central bank digital currencies*, March.

Danezis, G and S Meiklejohn (2016): “Centrally banked cryptocurrencies”, proceedings of the 23rd Annual Network and Distributed System Security Symposium, The Internet Society.

D’Silva, D, Z Filková, F Packer and S Tiwari (2019): “The design of digital financial infrastructure: lessons from India”, *BIS Papers*, no 106, December.

Eastern Caribbean Central Bank (2020): “ECCB digital EC currency pilot: what you should know”, accessed 27 January.

European Central Bank (2019): “Exploring anonymity in central bank digital currencies”, *In Focus*, no 4, December.

Frost, J, L Gambacorta, Y Huang, H S Shin and P Zbinden (2019): “BigTech and the changing structure of financial intermediation”, *BIS Working Papers*, no 779, April.

Fung, B and H Halaburda (2016): “Central bank digital currencies: a framework for assessing why and how”, Bank of Canada, *Staff Discussion Papers*, no 22.

Kahn, C, F Rivadeneyra and T-N Wong (2019): “Should the central bank issue e-money?”, *Federal Reserve Bank of St Louis Working Papers*, no 3.

Kumhof, M and C Noone (2018): “Central bank digital currencies – design principles and balance sheet implications”, *Bank of England Working Papers*, no 725.

Mancini-Griffoli, T, M Peria, I Agur, A Ari, J Kiff, A Popescu and C Rochon (2018): *Casting light on central bank digital currencies*, International Monetary Fund, November.

National Bank of Ukraine (2019): *Analytical Report on the E-hryvnia Pilot Project*, February.

Pichler, P, M Summer and B Weber (2020): “Does digitalization require central bank digital currencies for public use?”, *Monetary Policy and the Economy*, forthcoming.

Ruffing, T, S Thyagarajan, V Ronge and D Schroder (2018): “Burning Zerocoins for fun and for profit – a cryptographic denial-of-spending attack on the Zerocoin protocol”, proceedings of the Crypto Valley conference on Blockchain Technology, Institute of Electrical and Electronics Engineers, pp 116–9.

Sveriges Riksbank (2018): “The Riksbank’s e-krona project: Report 2”, October.

——— (2019): “The Riksbank proposes a review of the concept of legal tender”, press announcement.

Wadsworth, A (2018): “The pros and cons of issuing a central bank digital currency”, *Reserve Bank of New Zealand Bulletin*, vol 81, no 7, June.

Reading Materials

Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations

WP/20/254

IMF Working Paper

Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations

by Wouter Bossu, Masaru Itatani, Catalina Margulis,
Arthur Rossi, Hans Weenink and Akihiro Yoshinaga

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

INTERNATIONAL MONETARY FUND

Reading Materials

Source: **Bossu, W., M. Itatani, C. Margulis, A. Rossi, H. Weenink and A. Yoshinaga. 2020. "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations," IMF Working Paper No. 20/254.**

WP/20/254

IMF Working Paper

Legal Department

Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations

Prepared by Wouter Bossu, Masaru Itatani, Catalina Margulis, Arthur Rossi, Hans Weenink and Akihiro Yoshinaga

Authorized for distribution by Yan Liu

November 2020

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

Abstract

This paper analyzes the legal foundations of central bank digital currency (CBDC) under central bank and monetary law. Absent strong legal foundations, the issuance of CBDC poses legal, financial and reputational risks for central banks. While the appropriate design of the legal framework will up to a degree depend on the design features of the CBDC, some general conclusions can be made. First, most central bank laws do not currently authorize the issuance of CBDC to the general public. Second, from a monetary law perspective, it is not evident that "currency" status can be attributed to CBDC. While the central bank law issue can be solved through rather straithforward law reform, the monetary law issue poses fundmental legal policy challenges.

JEL Classification Numbers: E42, E52, E58, F24, F33, O33

Keywords: Central Bank Digital Currency; CBDC; Blockchain; Cryptocurrency; Crypto assets

Author's E-Mail Address: Wbossu@imf.org; masaru.itatani@boj.or.jp; Cmargulis@imf.org; Arossi@imf.org;Hweenink@imf.org; Ayoshinaga@imf.org

Reading Materials

Source: **Bossu, W., M. Itatani, C. Margulis, A. Rossi, H. Weenink and A. Yoshinaga. 2020. "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations," IMF Working Paper No. 20/254.**

Contents

Page

Boxes

Figures

Annexes

Reading Materials

Source: **Bossu, W., M. Itatani, C. Margulis, A. Rossi, H. Weenink and A. Yoshinaga. 2020. "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations," IMF Working Paper No. 20/254.**

"*The study of money, above all other fields in economics, is the one in which complexity is used to disguise truth or to evade truth, not to reveal it*."

J.K. Galbraith
Money: Whence it came, where it went

I. Introduction[1]

1. In reaction to digital ledger, blockchain and other technological developments, as well as the possible issuance of private virtual currencies ("stablecoins"), the central banking community is actively considering the merits of issuing so-called "central bank digital currency" ("CBDC"). Many central banks have started in-depth discussions on the appropriateness and feasibility of issuing such currency.[2] A survey concludes that "at this stage, most central banks appear to have clarified the challenges of launching a CBDC, but they are not yet convinced that the benefits will outweigh the costs."[3]

2. International financial institutions are also contributing to this debate.[4] In a Staff Discussion Note ("SDN"), IMF staff concluded that "CBDC could be the next milestone in the evolution of money," while at the same time cautioning that staff finds "no universal case for CBDC adoption yet."[5] The leadership and staff of the Bank for International Settlements (BIS) have also issued thoughtful analysis and views.[6] The Committee on Payment and

[1] This paper was written while Masaru Itatani was on secondment with the IMF. While the views expressed in this paper are to some extent based upon the authors' experience as Fund counsels, the views expressed herein are their own and should not necessarily be attributed to the Fund or the institution an author belongs to. The authors are grateful to Jason Allen, Niels Andersen, Phoebus Athanassiou, Susanne Bohman, Ludovico Cardone, Cristiano Crozer, Jose Garrido, Lorenzo Gatti, Christopher Hunt, Barend Jansen, Monika Johansson, Naoto Katagiri, Christoph Keller, Benedicte Nolens, Rosa Lastra, Yan Liu, Manuel Monteagudo, Panagiotis Papapaschalis, Charles Proctor, Mario Tamez, Kristof Van Nuffel, and staff from the Peoples Bank of China, Central Bank of Ghana, Bank of Israel, Banco de Mexico, Central Bank of the Philippines, the Monetary Authority of Singapore and the Bank of Thailand, for their review and comments. This paper also benefitted greatly from comments of other IMF departments. Obviously, all errors and omissions are the authors' alone.

[2] See *Central Bank Digital Currencies: Foundational Principles and Core Features*: *Report No. 1 in a series of collaborations from a group of central banks*, BIS, 2020.

[3] Barontini, C., and Holden, H., *Proceeding with Caution-a Survey on Central Bank Digital Currency*, BIS Papers No. 101, January 2019, p. 12.

[4] Think tanks are also formulating views: see Gnan, E., and Masciandaro, D., *Do We Need Central Bank Digital Currency? Economics, Technology and Institutions*, SUERF, 2018/2; Shirai, S., *Central Bank Digital Currency: Concepts and Trends*, VOX CEPR Policy Portal, 6 March 2019.

[5] IMF Staff, *Digital Money Across Borders: Macro-Financial Implications,* IMF, 2020; IMF Staff, *Casting Light on Central Bank Digital Currency*, IMF, SDN/18/08; IMF Staff, *A Survey of Research on Retail Central Bank Digital Currency*, WP/20/104.

[6] Carstens, A., *The Future of Money and Payments*, Central Bank of Ireland 2019 Whitaker Lecture, 2019; Barontini, C., and Holden, H., *o.c.*; Auer, R., Cornelli, G, and Frost, J., *Rise of the Central Bank Digital*

(continued…)

Market Infrastructures (CPMI), hosted by the BIS and composed of representatives of central banks, noted that "CBDC raises old questions about the role of central bank money."[7] A similar view was taken by staff of the Asian Development Bank Institute.[8]

3. As often highlighted by central banks and other policymakers, the introduction of CBDC would raise important legal questions. Some of these touch upon the very fundamental relationship between money, the State, and the law.[9] Do central banks have the authority to issue digital "currency"? Can CBDC be real "currency"? Should digital currency be legal tender? These questions are highly relevant and practical: in the absence of a clear response, the monetary system will struggle to adopt CBDC widely and the digital space might become 'populated' by private alternatives.

4. This paper seeks answers to those legal questions, by analyzing the two most important public law aspects of CBDC, namely the legal foundations of CBDC under central bank law and its treatment under monetary law. The issuance of CBDC will naturally also raise questions under tax law, private law (including property law), contract law, payment systems and settlement finality law, insolvency law, privacy and data protection law, and private international law. Moreover, CBDC needs to be carefully designed to ensure the effective implementation of the AML/CFT framework. While acknowledging their importance, this paper will not address those other issues, except where directly relevant under monetary law.[10] Finally, the purpose of this paper is not to advocate for the issuance of CBDC—this is a policy and political matter—but merely to ensure that, when and if CBDC is issued, it enjoys a robust legal basis.

Currencies: Drivers, Approaches and Technologies, BIS, WP No. 880, August 2020; and Bech, M., and Garratt, R, *Central Bank Cryptocurrencies*, in BIS, Quarterly Review, 2017, p. 55-70.

[7] CPMI, *Central Bank Digital Currencies*, BIS, March 2018*,* p. 1.

[8] See ADB Institute, *Central Bank Digital Currency and Fintech in Asia*, 2019, and Section 3.3.1. on "legal certainty" in particular.

[9] For a public law perspective on the relations between money, central banks, the State and the law: see Lastra, R., *Legal Foundations of International Monetary Stability*, Oxford University Press, 2006, chs. 1 and 2 and Lastra, R., *International Financial and Monetary Law*, Oxford University Press, 2015, chs. 1 and 2.

[10] While monetary and central bank law are reasonably harmonized among jurisdictions, legal frameworks and traditions vary considerably in their likely treatment of CBDC under private law and tax law. The complexities raised by the various private and tax law issues deserve a separate space and attention. See Perkins, J., and Enwezor, J., *The legal aspect of virtual currencies*, Butterworths Journal of International Banking and Financial Law, November 2016, p. 569; Zilioli, C., *Crypto-assets: Legal Characterization and Challenges under Private Law*, EL Review, April 2020; Allen, J.G., *Property in Digital Coins*, (2019) 8(1) *European Property Law Journal* 64; Fox, D., and Green, S., (eds.), *Cryptocurrencies in Public and Private Law,* Oxford University Press, 2019; and Waerzeggers, C., and Aw, I., *Difficulties in Achieving Neutrality and other Challenges in Taxing Crypto Assets,* in Chris Brummer, ed, Cryptoassets: Legal, Regulatory and Monetary Perspectives (New York: Oxford University Press, 2019) 219.

5. This paper is structured as follows. The first section will briefly present definitions, the concept and design features of CBDC, and lay down the key legal implications. The next two sections will discuss in detail the central bank and monetary law aspects of CBDCs respectively. A final section will conclude. Draft sample legislation aimed at providing a sound legal basis to CBDC under central bank and monetary law is included in the annex.

II. CBDC: The Concept, Design Features and Legal Implications

CBDC: What's in a Name? CBDC is certainly *Digital*…

6. Despite the lively debate on the merits of CBDC, no widely accepted definition of CBDC has yet emerged.[11] Over the past few years, the CPMI and IMF staff have provided some guidance on key features and a definition of CBDC.

- The CPMI highlighted that *"CBDC is not a well-defined term. It is used to refer to a number of concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serve both as a medium of exchange and a store of value."*[12]

- In the above-referenced SDN, IMF staff defined CBDC as *"a new form of money, issued digitally by the central bank and intended to serve as legal tender."*[13]

Even though the definition of CBDC is not yet settled, a key distinctive feature of CBDC is that it is *digital*.

7. If CBDC is digital, could it qualify as "electronic money?" The answer will depend on jurisdiction-specific circumstances. This said, electronic money is commonly defined as electronically stored monetary value represented by a claim on the issuer that is issued on receipt of funds for the purpose of making payment transactions and is accepted by natural or legal persons other than the issuer. In most jurisdictions, electronic money does not enjoy legal tender status. It is issued at par on receipt of funds (and the monetary value can be redeemed at par) by electronic money institutions that are licensed to provide specific payments services. Its regulatory framework generally consists of rules on the licensing of electronic money institutions, their required initial capital and own funds, general prudential rules, oversight, as well as rules safeguarding funds received in exchange for electronic

[11] On definitional issues, see Allen, J., and Lastra, R., "Virtual Currencies in the Eurosystem: Challenges Ahead", *The International Lawyer,* Vol. 53, No. 2, 2019, pp. 177-232. They further consider these as well as border issues in "Border Problems: Mapping the Third Border", *Modern Law Review,* 2020, DOI:10.1111/1468-2230.12506, https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2230.12506?af=R

[12] CPMI, *o.c., p. 3.*

[13] IMF Staff (2018), *o.c.*, p. 7.

money.[14] In most countries, the legal framework contemplates the issuance of electronic money by private institutions, and not by the central bank—in the EU, issuance by central banks is actually excluded from the scope of the directive.

…but can it legally also be *Central Bank Currency*?

8. While the digital nature (the "D") of CBDC is relatively easy to grasp, its two other key features (the "CB" and the "C") raise fundamental legal issues.

- ***Issuance by the Central Bank***—As correctly highlighted in the definition used by the CPMI quoted above, to qualify as real (as opposed to "synthetic" CBDC discussed below) CBDC, this type of money should be issued in the form of a liability of the central bank. This is what differentiates central bank money from private money, such as credit balances on accounts in commercial banks (i.e. liabilities of the latter) or cryptocurrencies (which are potentially no liability at all, such as Bitcoin). However, as any other activity of the central bank, the creation of central bank liabilities is regulated in detail by so-called "central bank laws" (as defined below). Do ***central bank laws*** authorize the creation of central bank liabilities, and the issuance of "currency" in particular, in digital form? In the absence of a clear answer, CBDC would not have a robust legal basis, and its issuance should be reconsidered.

- ***Currency***—The "C" suggests that this "new form of money" is "currency." (For the difference between "currency" and "money," see Box 1 below) But is that so? To qualify as currency, a means of payment must be considered as such by ***monetary law*** (as defined below). Can monetary laws consider CBDC to be currency? If so, what are the legal consequences of CBDC issuance? If not, what does this entail for CBDC? The answers to those questions are equally critical, in particular to discern the role which CBDC could play under the legal framework as a means of payment, i.e. to extinguish monetary obligations.

These two legal issues are the subject of the analysis in the remainder of this paper.

[14] Examples of such regulations are the Central Bank of Kenya's 2013 E-money Regulation, the EU's Directive on electronic money institutions (2009/110/EC), and the State Bank of Pakistan's 2019 Regulations for electronic money institutions.

Box 1. Currency, Money and Payment Instruments: What Is in a Legal Name?

Over the past centuries, the law and banking practice have developed three, legally very different "tools" for making payments. Importantly, the legal nature of those tools does not exactly overlap with the economic conception of money (unit of account, means of payment and store of value): in answering legal questions about money, "economic theory is unlikely to assist the lawyer to any appreciable extent."[1] This said, there are some links, such as the "unit of account" being the "official monetary unit" under monetary law (see below).

The delineation between these three legal concepts can be summarized as follows:

"**Currency**" can be defined as the official means of payment of a State/monetary union, recognized as such by "monetary" law. Most monetary laws reserve currency status to banknotes and coins, issued by the central bank (or coins issued by the State). Currency is always denominated in the official monetary unit. "Legal tender" status is a key attribute of currency: it entitles a debtor to discharge monetary obligations by tendering currency to the creditor.

While there is no universally accepted legal definition of money, it is widely accepted that the legal concept of "**money"** is broader. In addition to currency (banknotes, coins), in many (but not all) jurisdictions, it also includes certain types of assets or instruments that are readily convertible or redeemable into currency. This include first and foremost central bank and commercial bank "book money" (credit balances on accounts). Such book money can be converted into currency (subject to contractual stipulations) or transferred through payment systems or payment instruments (see below). At any rate, book money is not currency and enjoys legal tender status only in a few jurisdictions. This said, increasingly jurisdictions have given some form of legal recognition to this type of money, for instance as an authorized form of paying taxes or other legal obligations. In some jurisdictions,[2] "electronic money" is also classified as a type of money. Some assets (e.g., Bitcoins) may be considered as money under one body of law (e.g., VAT law), but not under another (e.g., financial law).

"**Payment instruments**" are a third means of payment: they are neither currency nor money but are legally used to effect payment in commercial bank book money or in currency. Cheques, bills of exchange and promissory notes are payment instruments.

1/ Mann, F., *The Legal Aspect of Money,* 4th Ed., p. 5.
2/ See e.g. the EU's E-Money Directive.

CBDC: Design Features and Legal Implications

9. The legal treatment of CBDC under central bank and monetary law will very much depend on its operational and technical design features. As of the publication date of this

paper, very few central banks have officially and formally issued CBDC.[15] At this stage, many central banks are transitioning from general research to more concrete proof-of-concepts and next to hands-on pilot phases. In that context, they are often still debating some key design features, which are also more widely discussed in the central banking and academic communities.

10. At any rate, the design features contemplated by central banks can be plotted on four axes: (i) account-based v. token-based, (ii) wholesale v. retail, (iii) direct v. indirect, and (iv) centralized v. decentralized. Most of these dichotomies raise important legal issues, which will be briefly mentioned in preparation for the more detailed discussion below.

Account-based vs. Token-based CBDC

11. Some central banks intend to structure the CBDC in a manner that digitalizes balances in cash current accounts in the books of the central bank. Other central banks are exploring the design of CBDC in the form of a digital token, not connected to an account-relationship between the central bank and the holder.

12. From a legal perspective, this distinction is fundamental. Balances in current accounts in the books of central banks are as old as central banking—they were developed by the Amsterdamse Wisselbank, arguably the first central bank. Their legal status under private and public law is well developed and understood. For instance, book money is transferred between account holders by debits and credits of their current accounts. Digital tokens, in contrast, do not benefit from a long history and their legal status under public and private law is currently unclear.

Wholesale v. Retail/General Purpose CBDC

13. Some central banks contemplate to issue CBDC only to their existing account holders and participants in their RTGS payment systems. These are mainly (big "clearing") banks and public bodies ("wholesale"). Other central banks cast the web much wider and are looking to offer CBDC to the general public ("retail"), without offering it to their wholesale clients. Finally, some central banks consider that their CBDC should be "general purpose" and be available to both wholesale and retail counterparties.

14. From a legal perspective, this distinction would be very relevant where the CBDC is designed as account balances in current account. As will be discussed in detail below, many central bank laws limit the categories of entities and persons that can open such accounts.

[15] To date, the Central Bank of The Bahamas has issued a digital "Sand Dollar" and the Central Bank of Lithuania launched a commemorative digital currency (LBCOIN). Pilot projects cannot be considered as official launches, including because often there is no sufficient legal basis for the issuance. However, some countries, such as China, have been developing the legal basis in preparation for issuing CBDC.

Other critical legal issues are the Anti-Money Laundering rules and competition law, but these issues will not be discussed in this paper.[16]

Direct/1-tier v. Indirect/2-tier CBDC

15. Some central banks contemplate to issue CBDC in direct or a 1-tier form: they would issue the CBDC and administer its circulation themselves. Other central banks contemplate issuance in indirect, 2-tier form (also called "synthetic"), whereby the liability is issued by a commercial bank but is fully backed with central bank liabilities. A hybrid form would consist of direct claims on the central bank, with intermediaries handling payments.

16. From a legal perspective, two important issues arise. First, to qualify as a real CBDC, the "currency" needs to be a direct liability of the central bank; this is what makes them risk free.[17] Liabilities of commercial banks, even if backed by a 100% cash deposit in the books of the central bank, are not a central bank liability.[18] Second, in case of token-based CBDC, the question arises as to whether, and under which conditions, the legal framework allows to "deposit" the CBDC in the books of commercial banks (discussed in detail below).

Centralized v. Decentralized CBDC

17. Central banks are discussing whether CBDC transfers will be settled in a centralized fashion—as in their current RTGS—or in decentralized fashion, especially by way of distributed ledger technology (DLT). As to the latter, an additional variable is whether the DLT will operate on a permissioned or permission-less basis. Given the impact that a permission-less DLT may have on the functioning of the CBDC, including potentially complicating the central bank's ability to manage the money supply, [19] it is highly probable that central banks will opt for a permissioned DLT. The legal ramifications of this choice still have to fully crystallize. This paper will focus below on one specific legal aspect of DLT.

18. While all these design features have some legal relevance, the distinction between account-based and token-based CBDC has the most significant legal implications. (This is the case even if in practice some forms of CBDC may be hard to distinguish, especially for the general public.) Therefore, this paper will structure its analysis around this distinction,

[16] In the case of a retail CBDC directly operated by the central bank, the central bank itself may need to implement AML/CFT measures, including those on customer due diligence. This may require additional resources and expertise for the central bank.

[17] See *Central Bank Digital Currencies: Foundational Principles and Core Features*: *Report No. 1 in a series of collaborations from a group of central banks*, Box 1 ("Synthetic CBDC is not a CBDC").

[18] In case of insolvency of the issuing commercial bank, holders will only have a claim on the latter, and not the central bank. This is so even if the credit balance in the books of the central bank is reserved for the holders. In case the 100% reserve requirement was not met, this could lead to losses. This is not the case of real CBDC.

[19] AML/CFT and privacy/anonomity concerns will also be relevant in this regard.

while referring to other design features where legally relevant. In any event, to facilitate a focused legal analysis, the analytical approach of this paper must be stylized and may not completely map with the actual manifestations of CBDC.

Does the technology used for token-based CBDC shape its legal nature as currency?

19. As discussed above, the legal status of token-based CBDC is not clear. Various approaches for its conceptualization have been proposed. One very compelling approach is to distinguish the forms of CBDCs and traditional central bank money along the lines of the *identification* requirement for using the money:[20]

- For book money in general, including account-based CBDC, the identity of the account holder allows the holder to access the funds: "I am therefore I own";
- For money in the form of physical tokens, the physical possession of the banknotes and coins allows the holder to dispose of the funds "I possess therefore I own";
- For digital tokens, the knowledge of a password (often referred to as "private key") allows the holder to transfer the funds "I know therefore I own."

20. In turn, this allows this paper to analytically approximate token-based CBDC with banknotes and coins, i.e. "currency" (see below) for the following three, related reasons.

- First, token-based CBDC amounts to a (*sui generis*) claim on the central bank incorporated in an, albeit immaterial, token, and will circulate in the economy by transfer of the token. What it has in common with banknotes and coins is that the transfer of the token equals transfer of the claim. This is what distinguishes banknotes, coins and token-based CBDC from book money and bills (debt securities), which are transferred by debit and credits between cash current accounts and securities accounts respectively.
- Second, for both the physical and digital token forms of currencies, the holder seeking to make a payment must either be in the possession of the banknotes/coins or know the password allowing to dispose of the currency. If the holder loses either the banknotes/coins or the password, he/she cannot use the currency anymore. In contrast, for book money, even if the holder loses the password, he or she will still be able to dispose of the funds as long as that person can prove his or her identity to the entity maintaining the account.
- Third, in the taxonomy of central bank liabilities, token-based CBDC is neither book money nor a bill. Especially in case the CBDC would be issued to the general public,

[20] The identification criteria to distinguish between account and token-based CBDC was articulated in a number of publications, including: Auer, R., and Bohme, R., *The Technology of retail central bank digital currency*, BIS, 2020; and Kahn C, *How are payments accounts special*?, Federal Reserve Bank of Chicago, 2016.

it would have this feature in common with banknotes and coins which are also issued to circulate widely. (At least from a legal perspective, it would make a lot of sense to issue wholesale CBDC in the account-based form.)

21. Do technological methods used to transfer token-based CBDC challenge this approach? Many central banks are considering the issuance of token-based CBDC on DLT, which would entail that the currency is booked in some form of ledger. What are the legal consequences of this approach? This issue certainly requires further attention, as token-based CBDC is being developed. At this stage, the use of DLT does not alter this paper's assumption that token-based and account-based CBDC are different forms of money. This is mainly because the booking of token-based CBDC in a register or ledger operated by the central bank is legally not the same as the booking of a credit balance in a cash current account. This is explained in more detail in Box 2. This entails in turn that the legally robust issuance of token-based CBDC requires special provisions in central bank and monetary law that are different from the ones needed for the issuance of account-based CBDC.

Box 2. Cash Accounts v. Ledger Accounts: The Legal Distinction

To adequately assess the legal distinctions between account-based CBDC and token-based CBDC processed in a centralized manner or through permissioned DLT, the legal distinction between cash current accounts and (general) ledger accounts must be highlighted.

- ***Cash current accounts***—These accounts are a banking technique and represent a *sui generis* contractual legal relationship between a financial institution and an account holder. By consequence, the rights and obligations of the parties are mainly provided by the contractual terms and conditions governing the account. Legislative provisions and general legal principles may also be applicable. In most jurisdictions, cash current accounts operate on the basis of the Roman law *mutuum* contract: even though the moneys credited to the account are called "deposits," the financial institution is not required to safekeep those monies, but is authorized to use them by lending them onwards. Credit balances in cash current accounts are called "book money" (see above) and are transferred by debits and credits between such accounts.
- ***Ledger accounts***—These accounts are an accounting technique and not a contractual concept: they represent a financial situation of a reporting entity based on sub-accounts established by the entity's chart of accounts. Ledger accounts can represent an asset, a liability, an income or an expense. Ledger accounts do not establish or represent per se a legal relationship between the reporting entity and a third party and do not create rights and obligations between the reporting entity and other parties. (But nothing prevents the reporting entity and third parties to enter into a contractual relationship.)

Importantly, these two distinct concepts are not completely disconnected. For instance, the total amount of credit balances held by counterparties in cash current accounts in the books of the central bank should be represented in the appropriate general ledger account. Also, this general ledger account can technically be subdivided in sub-accounts per account holder, representing for each of the latter the credit or debit balance that is the balance of the cash current account. These connections do not, however, change the fundamental distinction between the two concepts.

Box 2. Cash Accounts v. Ledger Accounts: The Legal Distinction (cont'd)

The ultimate legal consequence of the distinction is that, while token-based CBDC can be represented in centrally managed ledger accounts by the central bank, it is not a credit balance in current account. This entails that no contractual relationship exists between the central bank and the holder of token-based CBDC, except for the (admittedly very *sui generis*) claim incorporated in the token, very similar to the legal status of banknotes.

III. Central Bank Law

A. What is "Central Bank Law" and why is it relevant for CBDC?

22. The activities of all central banks are governed by so-called "central bank laws" (which in the case of monetary unions can take the form of a treaty). These laws—often called "organic"—establish (or authorize to establish) central banks, provide for their decision-making bodies, lay the foundations for their autonomy, and prescribe their mandate. The key concept here is the *mandate*. Actions of a central bank beyond its mandate are vulnerable to political and legal challenges, in particular on grounds of general principles of administrative law (such as the "attributed powers" or "specialty" principles). Box 3 explores these concepts in some more detail.

Box 3. Central Banks and the Principle of Attribution of Powers

The principle of the attribution of powers means that a public entity—such as a central bank—may only conduct, or participate in, those operations for which it has received a mandate, either explicitly or, in some legal orders, implicitly ("implied powers"). The legitimacy of the delegation of powers to an autonomous central bank is enhanced by requiring the autonomous central bank to be accountable and transparent about the way it exercises its clearly defined mandate. Clearly defined mandates enhance legal certainty and are a precondition for entrusting sensitive technical policy decisions to an autonomous central bank.

A central bank's objective(s), functions and powers constitute its mandate. The requirement of a clear mandate means that a central bank should have clearly defined functions and the associated powers to achieve its objective(s).

The concept of attribution of powers is found in federal states, supranational organizations like the European Union,[1] but also in central bank laws. For example, Chapter 1, Section 1 of the Swedish

Central Bank Act, provides that the Riksbank "*may only conduct or participate in such activities for which it has been authorized by Swedish law.*"

[1] Article 5 of the Treaty of the European Union provides that "the limits of Union competences are governed by conferral". See also Jacqué, J.P., *Droit Institutionel de l'Union Européenne*, 2010, par. 215.

23. In light of the principle of *attribution of powers*, the issuance of CBDC will require a firm anchor in the mandate established by the central bank law. This is especially important because the issuance of CBDC is a novel and potentially contentious activity. Without a clear and explicit mandate to issue CBDC, questions can arise as to whether a central bank is legally authorized to issue such currency, which is ultimately a liability, i.e., a debt, of the central bank. The issuance of non-authorized debt by a central bank would in turn give rise to serious legal, financial and reputational risks for the central bank and (the members of) its decision-making bodies. The importance of this principle is illustrated by the fact that today most central bank laws are explicit on the powers of central banks to issue their three standard liabilities, to wit (i) banknotes and coins, (ii) book money (i.e. credit balances on current and other (e.g. minimum reserves) accounts, and usually also (iii) bills.

24. Whether the issuance of CBDC falls under the mandate of a central bank requires an analysis of the central bank law's provisions concerning two aspects of its mandate,[21] namely its *functions (*sometimes also called *"tasks"* or *"duties")*—"what" a central bank must do to achieve its objectives—and its *powers*—"how" a central bank can act to implement its functions.[22] The link between those two legal concepts is important. On the one hand, statutory functions can in many instances only be executed through the exercise of legal powers. On the other hand, a central bank can only exercise its legal powers in the context of the exercise of its statutory functions. As will be seen, the relevance of a particular function or power varies depending on the design features of the CBDC that would be issued.

Central Bank Functions

25. Noting that most central bank laws include a single provision stating the functions of the central bank—this is indeed a good practice—there are two typical central bank functions that are particularly relevant for the issuance of CBDC.

- *Currency Issuance Function*: This is the traditional function of central banks to issue currency to the national economy. This function is relevant for token-based CBDC.

[21] On the legal concept of "central bank mandate," see Bossu, W., and Rossi, A., *The Role of Board Oversight in Central bank Governance: Key Legal Design Issues*, WP/19/293, p. 10-11. It is noted that not all central bank laws make a sufficiently clear distinction between objectives, functions and powers. On the evolution of the functions and objectives of central banks as well as on the need for central bank accountability, see Lastra, R., *International Financial and Monetary Law* (Oxford University Press, 2015), chapter 2 and Goodhart, C., *The Evolution of Central Banks,* MIT Press, 1985.

[22] Consideration should also be given to the third legal component of the central bank mandate: the objectives. Today, this aspect may appear less relevant, as the issuance of currency constitutes only a minor element of pursuing price stability. Going forward, central banks contemplating the issuance of CBDC will need to justify how such issuance contributes to the pursuit of their objectives, which may in some jurisdictions require compliance with a "proportionality test." In that regard, the impact of the issuance of CBDC on the stability of the banking sector and the possibility to charge (including negative) interest on CBDC may influence this assessment. For instance, the latter may establish a very direct link between the central bank's objectives and the functions of the issuance of currency and the formulation and implementation of monetary policy.

Whether the issuance of token-based CBDC is authorized depends on the issuance function of the central bank: does this function authorize to issue *all types* of currency or only banknotes and coins?

- *Payment Systems Function*: This is another traditional function of central banks to operate and oversee payment systems. What does this function entail for the issuance of CBDC? Naturally, any design of a form of money must inherently include a manner to transfer that money between economic agents. For money that is not a physical token, such transfer must almost by definition occur through some form of a "system." For token-based CBDC, an argument could hence be made that the technology and procedures to be used to transfer the CBDC, say on a permissioned distributed ledger, could amount to a payment system. For retail account-based CBDC, it could similarly be argued that the issuance of this type of CBDC results in the establishment of a payment system open to the general public. If that would be case, the question arises whether the central bank has the legal authorization to open access to its payment systems to the general public.

Central Bank Powers

26. Similarly, two typical central bank powers are relevant for token- and account-based models of CBDC respectively:

- *Power to issue certain types of currency*: Many central bank laws include a specific power to issue currency. Moreover, to enable such issuance, several central bank laws include specific powers pertaining to the production, circulation and withdrawal of banknotes and coins. Do these powers extend, or should they be extended, to token-based CBDC?
- *Power to open accounts in the central bank's books*: Many central bank laws include a specific power to open and hold for clients cash current accounts in their books. Such a power has many purposes: allow the central bank to act as banker to banks and to State, support the payment system function, and serve the implementation of monetary policy. Because account-based CBDC is essentially book money, its issuance will only be authorized for those entities for whom the central bank has the legal power to open cash current accounts.

27. By reviewing current practice, this paper will seek to answer the questions noted above, by applying the widely accepted textual, historical, teleological and contextual legal interpretation methods. However, it does not attempt to answer what is allowed and prohibited under any specific central bank law.

B. Central Bank Law and Token-based CBDC

Most Central Bank Laws only authorize the issuance of cash currency, i.e., banknotes and coins.

28. To ascertain whether a central bank law authorizes token-based currency, a two-step approach must be taken.

- First, it is necessary to analyze whether the central bank law explicitly and directly authorizes the issuance of currency, through an issuance function or power. This will allow to apply a textual interpretation to determine what is allowed or not.

- When that is not the case, other, more indirect legislative provisions pertaining to the issuance of currency will need to be considered with a view to establish contextual, teleological, and historical interpretations of the central bank law.

Direct Issuance Function or Power

29. Central bank laws display two variants in respect of the wording of the ***function*** **of the issuance of currency**.

- The first variant consists of central bank laws that explicitly limit the function of issuance of currency to banknotes and coins only.[23] There are cases where the wording of the function has recourse to broad language ("currency"), but where the central bank law includes separately a ***definition*** limiting "currency" to "banknotes and coins."[24] At any rate, it is uncommon to define "banknotes and coins." Thus, those concepts must be given their plain reading. In many, if not most, legal orders this will be limited to paper (or plastic) banknotes and metallic coins.[25]

- The wording of the second variant is broader and authorizes the central bank to issue "currency," without limiting it to banknotes and coins.[26]

[23] Article 4 (B). 7 of the Central Bank of Jordan Law provides the central bank with the function "to issue banknotes and coins in the Kingdom." Article 3 of the Dutch Central Bank Law mentions that DNB's functions include "to provide for the circulation of money as far as it consists of banknotes."

[24] Such a definition could also be included in a "monetary" or "currency act."

[25] In some countries, the argument is actually more straightforward: banknotes are legally equated with promissory notes and these notes must always be "in writing" (see, e.g., Section 83(1) of the UK's Bills of Exchange Act 1882).

[26] Article 7 of the National Bank of Ukraine Law provides the central bank with the function of "solely issuing the domestic currency of Ukraine and to organize its circulation." Section 2(b) of the Central Bank of Nigeria Act 2007 prescribes a "principal object" of the central bank to "issue legal tender currency in Nigeria."

30. The ***power* to issue currency** can also vary in central bank laws.

- On one side of the spectrum, there are some central bank laws with *no power*, given that the currency issuance *function* is clear enough and offers a sufficient legal basis to issue currency.[27]
- At the other side of the spectrum, there are central bank laws that include *only a power*, but *no function*, related to the issuance of currency. This can be because the central bank law does not include a list of functions.
- In between, there are central bank laws with *both a function and power* related to the issuance of currency. Under this approach, the legal interaction between the power and the function must be interpreted following the principle that "*lex specialis derogat legi generali*," namely the more specific of the two concepts prevails.

31. As with the function, the central bank's currency issuance powers will sometimes be general—authorizing the issuance of "currency" or "other forms of currency"[28]—and in other cases specific—authorizing only the issuance of banknotes and coins.[29]

Indirect Provisions pertaining to the Issuance of Currency

32. Many central bank laws include **specific ancillary *powers*** to the issuance of currency, and more specifically, banknotes and coins. These powers are ancillary in that they do not authorize the issuance as such, but rather authorize a number of activities that are conducive to, or necessary for, the issuance of currency. Typically, these specific powers pertain to the printing and minting of respectively banknotes and coins, the planning of their circulation, and the withdrawal, demonetization and destruction of banknotes.

33. Some central bank laws require an ***"asset cover"*** for the currency put into circulation. This requirement is a remnant of the gold standard, when central banks were required to maintain a sufficient amount of gold coin or bullion to satisfy demands for conversion *in*

[27] In line with the principle of implied powers (see Box 3), the function of issuance of currency may be taken to include all the powers – such as the printing and minting of banknotes and coins, bringing them into circulation, or withdrawing them from circulation, and defining rules on their reproduction—that are necessary to enable the issuance of banknotes and coins. To hold otherwise would undermine the function of issuing banknotes and coins. See Smits, R., *The European Central Bank Institutional Aspects*, 1995, p. 206.

[28] As an example of a general power, Article 37 of the National Bank of Rwanda Act states that "Banknotes and coins issued by NBR are sole legal tender on the territory of the Republic of Rwanda. However, NBR may issue other forms of currency being legal tender."

[29] Article 17 of the Organic Law of the Central Bank of Argentina states that "The Bank shall be empowered to conduct the following operations – a) Issue bills and coins pursuant to the powers delegated by the National Congress." In Brazil, Article 10 of Law 4595/1964 states that the Central Bank of Brazil has the exclusive power to "I - issue paper money (*moeda-papel*) and metal money (*moeda metálica*)". Similarly, Article 28 of the Organic Constitutional Law of the Central Bank of Chile establishes that "the Bank has the exclusive power to issue banknotes and to mint coins in accordance with the provisions of this section."

specie from holders of banknotes. Today, those provisions typically require a central bank to maintain a combination of official foreign reserve assets and local government bonds in an amount equal to the currency in circulation. Those provisions are relevant for this paper in that their wording will give an indication of which type of currency is contemplated by the law (to the exclusion of other types).[30] A variant of those provisions are rules on the ***definition of monetary liabilities***, especially under currency board arrangements.[31] This definition is important because under such arrangement the central bank will be obligated to ensure a 100% backing of the defined monetary liabilities in a specific foreign currency.[32]

34. A third type of indirectly relevant provision is one that seeks to grant the central bank the so-called "**monopoly of issuance**." This is a typical monetary law provision (to be discussed in detail below) which grants the central bank the exclusive right to issue currency within its jurisdiction or currency area. Often, this provision is combined with another provision prohibiting other private or public institutions or persons to issue currency or notes or tokens that by general public could be mistaken for currency due to a resemblance to the latter.[33] In some countries, this prohibition is enforced by criminal sanctions on the issuance of banknotes by other entities.[34] Importantly, the purpose of "monopoly of issuance" provisions is to limit the issuance of currency to the central bank only, and not to limit the types of currency that the central bank may issue. In other words, if the central bank law states that the central bank has the exclusive right to issue banknotes and coins, this does not automatically entail that the central bank can only issue banknotes and coins.

35. Finally, some central banks enjoy ***broad*** so-called ***incidental or ancillary functions and powers***. Their central bank laws contain explicit provisions mandating the central bank

[30] Section 19 (1) of the Bermuda Monetary Authority Act illustrates this point: "The Authority shall at all times maintain a reserve of external assets which—shall be in value not less than an amount equivalent to 50% of the total liabilities of the Authority in relation to the face value of currency notes in circulation; and shall consist of all or any of the following—"

[31] On the matter of currency boards, see of Lastra, R., *International Financial and Monetary Law*, Chapter 2.

[32] This is illustrated by Article 31 of the Law of the Central Bank of Bosnia Herzegovina, which states that "For the purposes of this Law: a. The aggregate amount of the monetary liabilities of the Central Bank shall be at any time the sum of: (A) all outstanding banknotes, coins put in circulation by the head office, main units, and other branches of the Central Bank."

[33] See Section 17 of the Central Bank of Nigeria Act: "The Bank shall have the sole right of issuing currency notes and coins throughout Nigeria and neither the Federal Government nor any State Government, Local Government, other person or authority shall issue currency notes, bank notes or coins or any documents or tokens payable to bearer on demand being document or token which are likely to pass as legal tender."

[34] See Art. 4.3 of the Law concerning Currency, the Central Bank of Kuwait and the Organization of Banking Business.

to exercise those functions or powers that are normally accorded to central banks,[35] or even commercial banks. This is different from the concept of implied powers mentioned in Box 3, in that these central bank laws contain explicit, broad wording that provides a legal basis allowing a central bank to undertake central bank activities, without having to list them specifically in the central bank law. This allocation of *incidental* functions or powers to a central bank is not unlimited, in that such functions or powers are those that are commonly undertaken by central banks. Also, these incidental functions or powers do not allow to undertake what is otherwise prohibited by the central bank law, or to undertake activities in a different fashion than as prescribed in detail by the central bank law. Other central bank laws include an explicit provision on broad *ancillary* powers (which must be distinguished from the specific currency-related ancillary powers discussed above).[36]

What does this mean with regard to the issuance of token-based CBDC?

36. ***Issuance of Token-based CBDC is authorized***: On the basis of the types of legal provisions discussed above, the issuance of token-based CBDC could be considered as legally authorized in the following two cases (that is of course in addition to cases where the issuance of token-based CBDC would be explicitly authorized: see below):

(a) The central bank law includes a broadly worded currency issuance *power* (a) enabling the central bank to issue domestic "currency," without limiting this to banknotes and coins, and the currency issuance function is equally open or absent,[37] or (b) referring explicitly to other means of payment than banknotes and coins.

(b) The central bank law does not include a currency issuance power, but a broad *function* to issue "currency," without limiting this to banknotes and coins, and the law does not include specific ancillary powers or other indirect provisions that (seem to) restrict the currency issuance to banknotes and coins.

[35] Article 4(B)15 of the Central Bank of Jordan Law enables the central bank to "carry out any other functions and transactions normally performed by central banks as well as any duties entrusted to it under this law". Section 26 of the Reserve Bank of Australia Act states that "The Reserve Bank: (a) is the central bank of Australia; (b) shall carry on business as a central bank; and (c) subject to this Act and to the Banking Act 1959 shall not carry on business otherwise than as a central bank."

[36] Article 8 (1.11) on the Law on the Central Bank of the Republic of Kosovo clarifies that the central bank may "carry out any ancillary activities incidental to the exercise of its tasks under this Law or under any other Law."

[37] A possible counter argument could be that token-based CBDC may have different design features from the traditional characteristics of paper money (e.g., as regards interest accrual, the degree of availability to users, or limits to anonymity). The consequence would be that, however broad the language used by the law, it would not necessarily warrant that all conceivable designs of CBDC would be encompassed by the broad legal authorization to issue currency.

These conclusions hold, even if the central bank law includes specific ancillary powers that only refer to the printing, circulation, and withdrawal of banknotes and coins.[38]

37. ***Issuance of Token-based CBDC is not authorized***: In the following cases, the central bank would not be authorized to issue token-based CBDC:

(a) The central bank law includes a narrow *function* to issue "banknotes and coins" and no power to issue "currency."

(b) The central bank law includes a broad power to issue "currency" but a narrow *function* to issue "banknotes and coins" (in such case the power must be read in light of the function).

(c) The central bank law includes a narrow *power* to issue currency only in the form of "banknotes and coins." As discussed above, those terms must be given their plain meaning: banknotes refer to paper or plastic notes and coins to metallic coins. Admittedly, in some jurisdictions, it could be argued that the existing legal concept of "banknotes" includes *digital* banknotes[39]—these would be "banknotes" in digital, not material form—but in many countries, this might be a stretched legal interpretation.[40] A narrow issuance power would be an obstacle to issuance of token-based CBDC when there is (i) no issuance function, (ii) a broadly worded issuance function, (iii) a narrowly worded issuance function or (iv) no issuance function but incidental powers.

(d) The central bank law includes no, or broadly worded, issuance function or power, but includes an *"asset cover" rule* that directly, or indirectly through the *definition* of "monetary liabilities," restricts the currency to be issued to "banknotes and coins."

(e) The central bank law includes no issuance function or power, and only provides for the *monopoly of issuance* and *specific ancillary powers*, and those provisions are limited to banknotes and coins. A contextual and historical interpretation of those

[38] The role of specific ancillary powers deserves consideration. The legal question is whether the drafting of these specific powers could be extended to token-based CBDC? Of course, similar to banknotes and coins, token-based CBDC is also produced, put into circulation and can be withdrawn; after all the central bank will determine the total amount of pre-paid values to be transferred, and stored on a device, card, or an app. Therefore, these specific ancillary powers can also be relevant for token-based CBDC. The only difference would be the specific powers for printing and dealing with counterfeit banknotes and coins, which are not needed as token-based CBDC cannot be printed or counterfeited (at least not in the traditional sense of the word). Nevertheless, a central bank would have to determine how it would legally deal with faulty devices, cards and apps and falsified token-based CBDC.

[39] The Central Bank of Uruguay is justifying the issuance of token-based CBDC on the basis of this argument.

[40] This option is discussed in Banque de France, *Central Bank Digital Currency*, 2020, p. 31.

provisions allows to conclude that the central bank is only authorized to issue those specifically mentioned forms of currency.

38. ***Issuance of Token-based CBDC is unclear:***

It is unclear whether the central bank is allowed to issue token-based CBDC when:

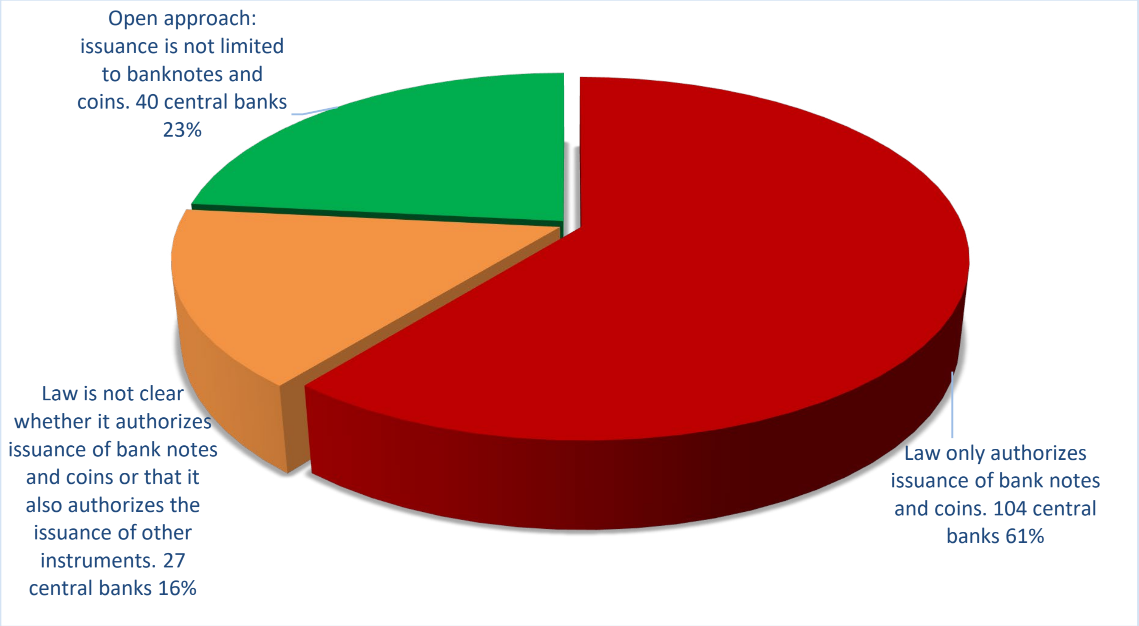
- the central bank law does not provide for an issuance function or power, or specific ancillary powers, but includes broad *incidental functions or powers*;

- the central bank law includes a broad *function* to issue "currency," without limiting this to banknotes and coins, albeit with specific ancillary powers or other indirect provisions that (seem to) restrict the currency issuance to banknotes and coins.

Country Practice

39. Among the 171 central banks of the IMF membership, 61% of central bank laws limit the authority of issuance of currency to banknotes and coins. 23% of central bank laws allow directly for the issuance of currency in a digital format. 16% of central bank laws are unclear as to whether they authorize the issuance of a digital version of central bank currencies.

Chart 1. Authorization to Issue Currency



Source: IMF Staff

C. Central Bank Law and Account-based CBDC

Many central bank laws will support the issuance of account-based CBDC to financial institutions, but its issuance to the general public will often lack a sufficient legal basis.

40. Many central bank laws include legislative provisions on the ***power*** of the central bank ***to open cash current accounts*** in its books. As with the issuance of currency, practices among the IMF membership differ.

- One group of central bank laws restricts the power of the central bank to open cash current accounts to a closed group of institutions, which typically are limited to the State, public institutions and financial institutions, or even narrower to banks.[41]

- Another group of central bank laws does not restrict the opening of cash current accounts to a closed group of institutions. In some cases, the law will simply not impose any restrictions.[42] In other cases, offering cash current accounts to natural persons is explicitly allowed.[43] In rare cases, opening cash current accounts to the general public is allowed, but only under certain circumstances.[44]

- In a third category of laws, restrictions on the type of account holders can be lifted by decision of the central bank's board of directors or the minister of finance.[45]

41. In the absence of an explicit authorization to open cash current accounts, the central bank might be deemed to have such a power as a result of the implied powers doctrine in jurisdictions where this doctrine is accepted. In the same situation, wording allowing a

[41] Section 28 (c) of the Reserve Bank of Malawi Act lists the powers of the RBM, which include to "open accounts for, and accept deposits from the Government, funds, corporations and institutions controlled by the Government, banks and other financial institutions in Malawi." Article 55 of the Organic Constitutional Law of the Central Bank of Chile allows the Bank to "open current accounts for banking and financial entities, the General Treasury of the Republic, and to other public institutions, organisms or State companies when necessary to conduct operations with the Bank, according to the qualification of the majority of the Board."

[42] Article 60 of the Law of the Central Bank of Costa Rica states that "the Central Bank is authorized to receive deposits in current account or at term, in national or foreign currency." Article 10 of the Law of the Central Bank of Curacao and Sint Maarten states that "the Bank is also authorized to perform the following activities: 2. to receive funds in trust, on deposit or in a current account;"

[43] Article 55 (4) in the Statute of the Bank of Greece gives the BoG the power to "keep an account for the State, as well as for public entities, credit institutions, legal entities, natural persons, and other market participants".

[44] Article 48, 2nd para, of the Central Bank of the Russian Federation Act stipulates that "the Bank of Russia shall be entitled to provide services to clients other than credit institutions in regions where there are no credit institutions."

[45] Section 75 of the Central Bank of Malaysia Act lists Bank Negara Malaysia's general powers which include the power to "open accounts for (…) (i) the Government, any State Government, public authority or financial institution; or (ii) any other person in Malaysia with the prior approval of the Minister".

central bank to undertake central bank activities incidental to the performance of its functions could be helpful in this regard. The same applies to ancillary powers.

What does this mean with regard to the issuance of account-based CBDC?

42. ***Issuance of Account-based CBDC is authorized***: Those central bank laws which include an explicit power to open cash current accounts for the State and banks, can be considered to be authorized to offer account-based CBDC to the State and banks. Where the central bank is also allowed to open cash current accounts to physical persons—as the case may be, by special decision—the central bank is, or can be, authorized to issue account-based CBDC also to the general public. Where the central bank law is silent on the opening of current accounts, the same conclusion may apply to central banks with implied or incidental functions and powers (for the latter, at least once a critical mass of central banks will have issued account-based CBDC to the general public).

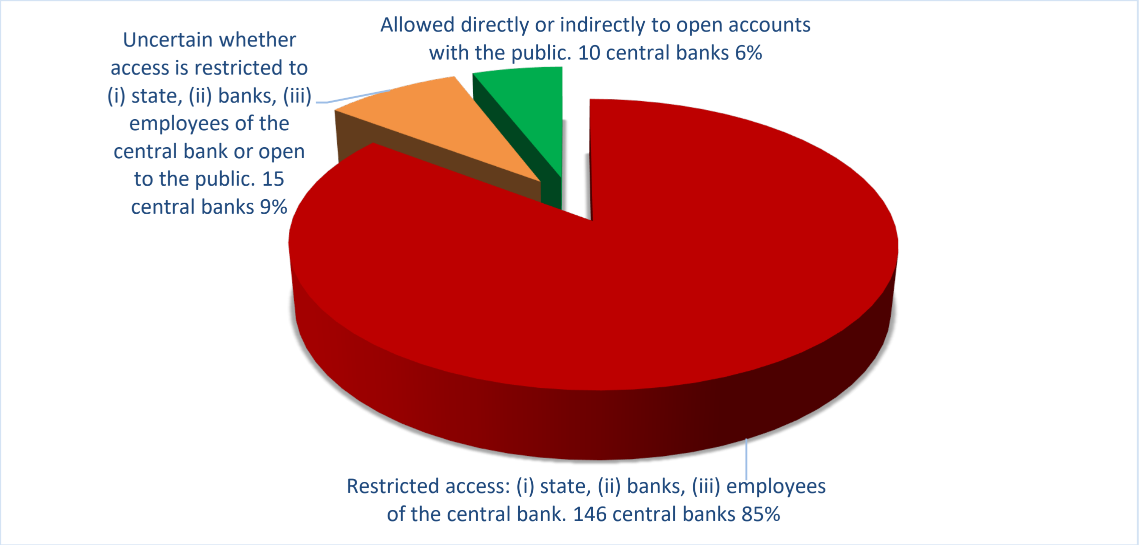
43. ***Issuance of Account-based CBDC is not authorized***: Central bank laws that only grant the power to open cash current accounts to the State, public bodies and banks, but not to physical persons, do not authorize to issue account-based CBDC to the general public.

44. ***Issuance of Account-based CBDC is uncertain:*** In case the law is silent on opening current accounts, and the central bank does not enjoy implied or incidental powers, there is substantial uncertainty as to whether the central bank is authorized to issue account-based CBDC to the general public. In such case, it could however be argued that the central bank is authorized to issue this form of CBDC to its existing accountholders.

Country Practice

45. Among the IMF membership, 85% of central bank laws limit the power to open cash current accounts to a limited category of institutions, while a minority of central bank laws (10 central banks corresponding to 6% of the total) allow for the opening of current accounts to a broader public. 9% of central bank laws include some form of provision on the opening of current accounts, but it is not clear whether accounts can be opened to the general public.

Chart 2. Power to Open Current Accounts



Source: IMF Staff

D. Central Bank Law Issues Common to Both Types of CBDC

46. What is the legal impact of ***the payment system function***?[46] Central bank laws differ in the manner in which they establish this function.[47]

- Many central bank laws limit this function to payment systems in the strict sense of the word, i.e., a specific payment infrastructure.[48] Among those central bank laws, there are a few which limit the payment system even further to "interbank" payment systems only.[49]

- Other central bank laws are more general and charge the central bank with overseeing and promoting the soundness of "the (national) payment system."[50] This is a much

[46] In some central bank laws (e.g., Mexico), this is actually an objective of the central bank.

[47] National payment system acts can also be relevant in this regard.

[48] Article 5 of the Federal Act on the Swiss National Bank mentions the SNB's function of "facilitating the operation of cashless payments systems." Section 4A (1) of the Central Bank of Kenya Act states that "the Bank shall: (d) formulate and implement such policies as best promote the establishment, regulation and supervision of efficient and effective payment, clearing and settlement systems."

[49] An example can be found in Article 7 of the Law on the National Bank of Cambodia, which counts among the functions of the central bank: "to oversee payment systems in the Kingdom and to enhance interbank payments." Article 18 of the Bank Indonesia Law states that "Bank Indonesia shall arrange the final settlement of interbank payment transaction both in rupiah and or foreign currencies."

[50] Chapter 1, Section 2 of the Swedish Riksbank Act states that "The Riksbank shall also promote a safe and efficient payments system." Article 3.3 of the Law on the National Bank of Georgia similarly declares that:

(continued…)

broader concept than the “payment systems” discussed above and refers to the ensemble of institutions (banks, payment institutions) and infrastructures (payment and securities settlement systems, central securities depositories, central counterparties, clearing houses) that, taken together, are used to transfer monetary value within an economy.

47. What is the relevance of those provisions for CBDC? Irrespective of the exact circumscription of the payment system function, the payment systems which central banks operate today are almost all *interbank* payment systems, in that the participation in those systems is limited to banks—and often only sizeable banks.[51] The establishment of token-based or account-based CBDC will inevitably entail the creation of a technical, operational and legal infrastructure that will transfer monetary value between users. This infrastructure can arguably be considered as a “payment system.” As long as only banks (and similar financial institutions) participate in such a system, there is no problem. But if CBDC would be made available to the general public, the central bank could be considered to operate a payment system with almost the entire population as participants. For those central banks with a payment system function formulated in a general wording, this should not raise major legal issues. But for those central banks that are only mandated to operate *interbank* payment systems, that mandate may be too narrow. This is because the adjective *interbank* denotes that the payment systems operated by the central bank only should serve to execute payment between banks, and not between broader categories of users, let alone the general public.[52]

48. Also, a few central bank laws include specific wording that the central bank has the ***function to promote technological innovation*** in the banking system.[53] Sometimes, the relevant provisions include an explicit link with the payment system function.[54] Such a type of provision can be relevant for CBDC. Specifically, when the legal basis is otherwise relatively weak, such a provision can be an additional argument to support the legal basis for the issuance of CBDC. At the same time, its usefulness should not be exaggerated, as such a

“The functions of the National Bank shall be to: f) facilitate secure, sustainable and effective functioning of the payment system.”

[51] The participation of FMIs is the exception that confirms the rule, as FMIs do not make payments on their own behalf but on behalf of their clients, which are also mostly banks.

[52] A similar conclusion can be reached for the oversight powers of central banks, which can also entail the establishment of a legal infrastructure for payment transfers via such “interbank” payment systems.

[53] In Mexico, this requirement is actually enshrined in the “fintech law.”

[54] Article 7(7) of the Law on the National Bank of Ukraine provides a function to: “shap(e) the development of modern electronic banking technologies, establishing payment and accounting systems, promoting their smooth and efficient operation, and ensuring development of payment and record-keeping systems created by the NBU; controlling the creation of payment instruments, banking automation systems and banking data protection systems”.

provision cannot overrule specific limitations in the powers to issue currency or offer current accounts to the general public.

E. The Need for Central Bank Law Reform

49. The absence of an explicit and robust legal basis for the issuance of token-and/or account-based CBDC can be relatively easily remedied through targeted central bank law reform. ANNEX I contains draft provisions to this effect. (Of course, it is accepted that other legal issues, such as for instance private law, may need to be addressed as well in the same context, which may in some cases complicate this exercise.)

50. ***Token-based CBDC***: To provide a firm legal basis for the issuance of this type of CBDC, the following amendments might need to be made to central bank laws.

i. The central bank law should include an explicit *function* "to issue currency" generally, without limiting the issuance of currency to banknotes and coins only.

ii. The associated *powers* to implement this function should be drafted, where appropriate,[55] with an explicit reference to the issuance of currency in the form of banknotes (and possibly coins) as well as in the form of a digital token.

The main argument for introducing such an explicit legal basis is that, depending on the intended design, such an amendment would support the more innovative CBDC features (e.g., limited privacy and general availability).

51. ***Account-based CBDC:*** To provide a firm legal basis for the issuance of this type of CBDC to the general public in particular, an amendment should be made to central bank laws to add a specific *power* to open current accounts for the general public. This can be done directly—by mentioning the general public in the central bank law—or indirectly by allowing the competent decision-making body of the central bank to decide on the categories of persons and entities that have access to current accounts in the books of the central bank.

52. ***Both Types of CBDC:*** If the wording of the payment system function were to be restricted to *interbank* payment systems, this restriction would best be removed.

[55] For instance, there is no need to extend the provisions on the printing of banknotes to token-based CBDC.

IV. Monetary law

A. What is Monetary Law and why is it relevant for CBDC?

53. Monetary law is the legislative and regulatory framework that provides the legal foundations for the use of monetary value in society, the economy and the legal system.[56] The basic principle of monetary law provides that it is for a sovereign State to determine and establish its own currency system.[57] (The sovereign power may of course be ceded to a monetary union, in which case this power is exercised collectively by the monetary union on behalf of the member states.) Central bank laws often include key provisions of monetary law: the distinction in this paper between central bank and monetary law is *substantive* (i.e. focuses on the issues the respective bodies of law seek to regulate), not *formal*. This being said, many countries also have a formal "monetary" or "currency act."

54. In many countries, the Constitution lays down the basic rules governing the interaction between the State and the monetary system. As can be seen from Box 4, the main purposes of those constitutional provisions are (i) to allocate the competency to adopt monetary law in federal states to the federal level and (ii) to confirm that the issuance of currency is a State matter.

Box 4. Constitutional Provisions on Currency

The issuance and circulation of currency is a core element of sovereign power. Therefore, many Constitutions contain general provisions on this power, which is subsequently detailed in primary legislation, such as central bank laws.

Section 51 of the Australian Constitution provides that *"Parliament shall have the power to make laws for the peace, order and good government of the Commonwealth with respect to", inter alia, "xii. Currency, coinage and legal tender."* Article 99.1 of the Swiss Constitution clarifies that *"the Confederation is responsible for money and currency".* A third example is provided by Article 227.1 of the Polish Constitution which says that *"the National Bank of Poland shall have the exclusive right to issue currency".*

It is instructive to note that the language used in various Constitutions is such that it might raise questions about the power to issue CBDC.

[56] Hahn, H., Häde, U., *Währungsrecht*, 2010, §2. The concept of another country's "monetary law" is often referred to by legislation. For example, 31 USC § 5151 provides rules on "conversion of currency of foreign countries". Also, private international law rules usually refer to the country of issuance as *locus* of monetary law issues: see e.g. Swiss Federal Code on Private International Law, Section 147(3).

[57] The Permanent Court of International Justice recognized that the *lex monetae* determines the value of the currency, albeit that it is for the *lex contractus* to determine the effect of a devaluation on contractual obligations; Judgments in the Serbian and Brazilian Loan Cases, July 12, 1929, Series A No. 20 and 21.

Box 4. Constitutional Provisions on Currency (Cont’d)

For example, Section 91 of the Canadian Constitution declares that *“the exclusive legislative authority of the Parliament of Canada extends to all Matters coming within the Classes of Subjects next hereinafter enumerated (...) 15. Banking, Incorporation of Banks and the Issue of Paper Money.”* Similarly, Article 4 of the Israel Basic law on the State Economy specifies that the *“printing of legal tender currency notes and the minting of legal tender coins, and the issue thereof, shall be done under Law.”* A third example is Article 83 of the Peruvian Constitution according to which *“the Law determines the monetary system of the Republic. Issuance of bills and coins is under the exclusive power of the State.”*

As these and other Constitutional provisions explicitly refer to only banknotes and coins, constitutional scholars would have to assess whether the existing provisions could be interpreted to cover the issuance of digital currency as well.

55. Building upon those international and constitutional law principles, monetary law basically seeks to regulate two issues:

a) What is the **official monetary unit** (*unité monétaire*) of the country/monetary union and how is its value determined or defined?

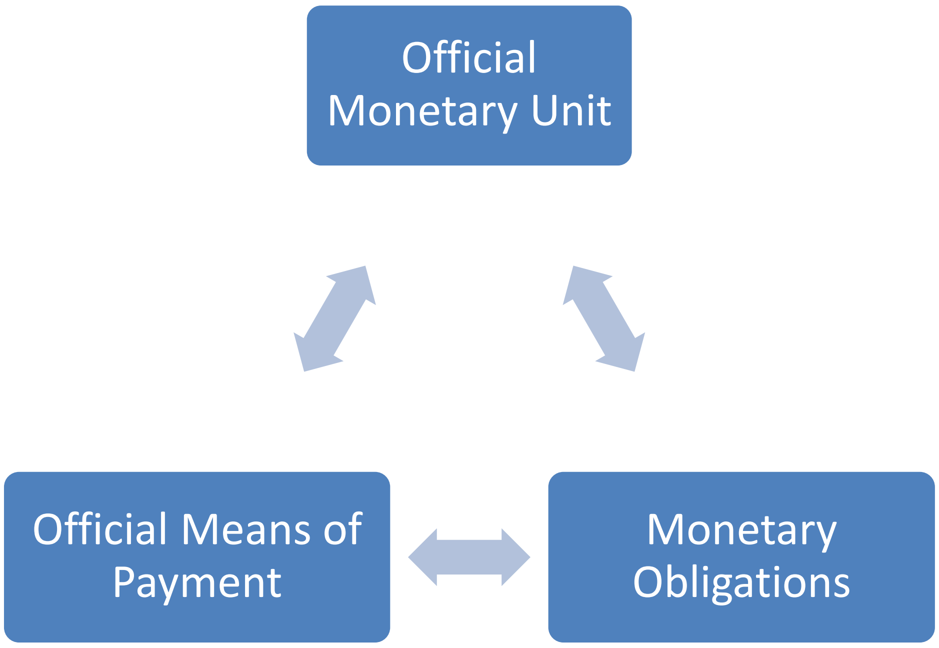
b) What are the **official means of payment** (*signes monétaires*) of the country/monetary union?[58]

All States/monetary unions define in legislation both the official monetary unit and official means of payment valid on their territory.

56. There is a very strong legal link between the two legal concepts. In one direction, the official means of payment must, by law, be expressed in the official monetary unit. In the other direction, monetary obligations expressed in the official monetary unit can, in principle, always be paid by tendering official means of payment. Monetary obligations are obligations to pay an amount of “money” and must in principle be expressed in an official monetary unit.[59] Monetary obligations can arise out of contracts, torts and public law obligations (e.g., taxes, fines). The obligor of a monetary obligation must, by law, satisfy his/her obligation by a transfer of money.

[58] We cite the French terms here because the English language is particularly confusing in the loose use of the term “currency,” which in common language is often used to denote both aspects, although strictly speaking the synonym for the official monetary unit should be “currency unit.”

[59] Mann, F., *The Legal Aspect of Money*, 4th Ed., p. 80.



57. The ultimate unifying principle between those concepts is the one of "nominalism." This principle means that any monetary obligation must be satisfied by paying the exact amount stipulated in the contract or law.[60] In other words, absent contractual provisions to the contrary, the loss of value of the official monetary unit, either domestically through inflation or externally through depreciation of the exchange rate, is at the risk of the creditor.

58. With respect to CBDC, the fundamental questions that arise under monetary law are:

i. Is CBDC a new official monetary unit and/or a new official means of payment? and

ii. In function of the response to (i), what are CBDC's essential monetary law attributes?

To respond to those questions, we need first to analyze in some degree of detail what those two legal concepts entail.

Official Monetary Unit

59. Monetary law establishes the official monetary unit of a State/monetary union.[61] It is this aspect that economists refer to when they mention the "unit of account" role of money.

[60] Mann, F., *o.c.*, p. 84.

[61] Monetary law will also define the subdivision of the official monetary unit, for instance that 100 cents equal a Dollar or a Euro.

Examples of official monetary units are the Dollar in the USA, the Euro in the Euro Area, and the Yen in Japan. These monetary units are clearly established by relevant legislation and must be distinguished from non-official quasi-monetary units (such as BTC (Bitcoin), ETH (Ethereum) and XRP (Ripple)) which are not established by law.

60. Moreover, monetary law often prescribes how the value of the official monetary unit is established.[62] Historically, many monetary units were defined by reference to either another monetary unit or, more commonly, a quantity of gold. Since the end of the Bretton Woods system, the external value of many official monetary units is determined by the foreign exchange market—naturally, domestic economic policies (monetary, fiscal) will shape the internal value (price level) of the monetary units.

Official Means of Payment: “Currency”

61. Monetary law also establishes which means of payment are officially sanctioned as such by the State/monetary union. Almost all States/monetary unions legally and officially sanction one or more types of means of payment.[63] The reason for this is that the use of means of payment and sovereignty are historically two closely connected concepts, as illustrated for example by the presence of the emperor’s or king’s face on coins and banknotes. The main types of official means of payment are banknotes and coins. These are in the English language commonly called “currency.”

62. The State has sanctioned the use of currency essentially through five important legal mechanisms: (i) the monopoly of issuance by the State or its agent, (ii) *cours forcé*, (iii) legal tender status, (iv) privileges under private law, and (v) protection under criminal law.

Issuance Monopoly of the State

63. Nowadays, in almost all countries, the official means of payment are issued by the State, and in particular its agent—the central bank.[64] (For the few jurisdictions where that is

[62] Kenyan law provides a good example of how those two principles of monetary law are actually enshrined in legislation. Section 19 of the Central Bank of Kenya Act provides that “the unit of currency of Kenya shall be the Kenya shilling, which shall be divided into one hundred cents.” In turn, Section 20 of the same Act states that: “The external value of the Kenya shilling shall be determined by the market.”

[63] This does not preclude the existence and use of non-official means of payment. Specifically, the use of commercial bank book money as a means of payment is in many countries more widespread than that of the official means of payment. But ultimately commercial bank book money is (unless contractually otherwise stipulated or limited) a claim to receive officially issued banknotes and coins.

[64] This point is nicely illustrated by Article 42 of the Law of the Central Bank of Peru: “the issuance of banknotes and coins is the exclusive capacity of the State, which exercises it through the central bank.” In most cases, these means of payment are issued by a country’s central bank, and coins in some countries by the Treasury. An important quid pro quo for this official sanction is that the issuer pays (part of) the income generated by the issuance of the monetary instruments to the State: this is the so-called seignorage.

not the case, the issuance of "currency" must at least be sanctioned by the State.[65]) This is the monopoly of issuance, discussed above, which was established in reaction to the distress caused in the 19th century to monetary systems around the world by commercial banks issuing their own banknotes representing gold deposits and insufficient gold cover, which often caused bank runs and financial instability. However, not all claims on the central bank are "currency:" central bank book money and central bank bills do not qualify as currency under law, because they lack the other features discussed below.

Cours Forcé

64. The second mechanism through which States sanction a means of payment is through *cours forcé*. The contemporary meaning of this concept is that the value of a banknote is the amount of official monetary unit printed upon it by the issuer. Banknotes are to be accepted in payment for that value, without convertibility into gold coins.[66] It is this feature that leads economists to call banknotes "fiat money."

65. *Cours forcé* must be distinguished from convertibility in other monetary liabilities of the central bank. The general public can in principle only convert banknotes into banknotes. However, current account holders of the central bank can convert banknotes into central bank book money, in principle without limitation. Conversely, current account holders of the central bank can also in principle convert without limitation central bank book money into banknotes.[67] These two features flow from a combination of the central bank law, central bank policies on current account holders, and the central bank's current account rules.

Legal Tender Status

66. The third legal mechanism is by granting by law to currency the power to validly and definitively extinguish monetary obligations: this power is called "legal tender status." By tendering a means of payment with legal tender status to the creditor, the debtor of a monetary obligation validly discharges his/her obligation. Jurisdictions, however, differ in

[65] This is the case of banknotes issued by private banks in Scotland and Northern Ireland.

[66] This term referred originally to the suspension and eventually the abolition of the convertibility in specie of banknotes issued by the central bank—the concept is not relevant for coins. Banknotes used to incorporate a claim for restitution of an amount of deposited gold (or silver) coin (or bullion). In the first half of the 20th century (often in response to the first World War), most countries suspended the convertibility of their banknotes, to avoid a panic run on the gold reserves and thus the bankruptcy of the central bank. This is a benefit of which ordinary claims on deposited gold (e.g. with goldsmiths) did not enjoy. This suspension was eventually made permanent and today all countries have no longer convertibility of banknotes in gold. As discussed above, there are still some central bank laws that require the central bank to back issued banknotes with foreign currencies, gold, government securities: see e.g. Art 109 Central Bank of Egypt Law. While this is a legacy from the convertibility under the gold standard, such provisions are no longer necessary (absent a currency board) nor good practice.

[67] Under negative interest rates, some central banks try to limit this convertibility, but this is done more through the cost structure of conversion than by restricting the principle itself.

how this is legally achieved. In some, this may entail that the creditor's claim deriving from that obligation is extinguished by his/her failure to accept a means of payment with legal tender status. In such a case, when the creditor refuses the payment in legal tender and brings a suit to the court, the court will consider that the debtor has validly paid.[68] In some other jurisdictions, this may merely grant certain privileges to the debtor. Under either approach, the creditor is indirectly forced to accept legal tender. Some countries even impose administrative- or criminal sanctions on creditors when they refuse to accept legal tender currency in payment.[69] Legal tender rules will apply unless, where this is permitted by law, there is a special contractual provision stipulating otherwise between the parties to the transaction. If parties to a contract establishing a monetary obligation do not make a special agreement regarding a different payment currency where that is allowed by law,[70] the debtor always has the option to pay in legal tender means of payment.

67. It is prevailing practice that a State/monetary union designates by legislation the means of payment it has issued—its banknotes and coins—as legal tender.[71] Some countries with an official dollarization or euroization policy designate foreign means of payment as legal tender either unilaterally or bilaterally and with or without parallel issuance of their own currency.[72] This illustrates that legal tender designation is a matter of State policy.

68. Legal tender status is merely one of the means of sanctioning, but not an essential feature, of official means of payment. Hence, the link between the official status of a means of payment and legal tender status is not absolute.[73] This has two consequences. First, not all means of payment with legal tender status are "currency": there are countries that have attributed legal tender status, albeit under certain restrictive conditions, to commercial bank

[68] This type of dispute has been observed in many countries when the creditor faced significant depreciation of local currency after the contract was entered into.

[69] Section 19 (5) of the Central Bank of Nigeria Act punishes criminally a "person who refuses to accept the Naira as a means of payment." In the past, Article 8, Paragraph 6 of the Japan's National Bank Ordnance (1872) stipulated also a criminal violation. Very recently, China's central bank issued a circular stating that cash payments must not be refused in regular transactions (Circular 10, 2018).

[70] Most jurisdictions allow up to a degree to choose the monetary unit of the contractual monetary obligation and the corresponding means of payment. There are, however, jurisdictions with more restrictive rules that authorize exclusively the use of the national monetary unit and means of payment.

[71] A State can also restrict the scope of legal tender status. For example, several laws limit the amount of banknotes and coins to be used in one transaction for the convenience of recipient parties or for AML purposes.

[72] For example, Section 19 of the Central Bank of Liberia Act provides that: (1) "The Liberian Dollar shall be the currency of Liberia and legal tender" (2nd sentence); and (2) "Currency of the United States of America shall be legal tender in Liberia" (1st sentence).

[73] Over time, other legal rules have been added to legal tender rules, which make the legal status of legal tender status quite complex. For instance, many countries actually forbid cash payments over a certain amount (for tax and AML concerns). In some cases, payment of a large sum by coins is also forbidden.

book money and cheques.[74] Second, some banknotes do not enjoy legal tender status, but can still be considered as "currency."[75]

69. In respect of the possible legal tender status of CBDC, the following ("natural law") question arises: is the sovereign's power to attribute by legislation ("positive law") legal tender status to a means of payment unlimited? The answer is open to discussion, but it is fair to say that the State can only meaningfully attribute legal tender status to a means of payment when that instrument is easily receivable by the vast majority of the population. (This explains why the legal tender status of banknotes and coins is so self-evident: basically, the entire population can accept these forms of payment, including the visually impaired through special braille features.) In other words, attributing legal tender status to a means of payment that cannot be received by the majority of the population might be legally possible but is raises fundamental questions, including from a fairness perspective.[76] This is recognized by countries that have attributed legal tender status to means of payment that are not currency: the designated group of creditors that are obligated to accept payment in the said means of payment must also take steps to ensure that payment can effectively be received.[77]

70. This perspective of protecting disadvantaged social groups in the use of currency has also inspired countries and subnational entities to adopt consumer protection rules that restrict the freedom of merchants to contract away the right to pay in currency.[78] While this type of rules must be distinguished from legal tender proper, it has a similar—if not stronger—effect in that it grants the general public an almost absolute right to make payments in legal tender currency.

[74] This is, for instance, the case of the Belgian Royal Decree Nr. 56 of 10 November 1967 "to promote the use of book money." Between merchants, payments in book money or cheque cannot be refused for amounts above 250 EUR (Art. 3).

[75] This is the case today of Scottish and Northern Irish banknotes issued by private banks.

[76] The Riksbank recently raised this issue clearly in the context of a discussion on declining usage of cash within the country. The Riksbank considers that there may be a need to make legal tender status technology-neutral, so that electronic means of payment issued by itself could also become legal tender. However, it also stressed the need to assess possible consequences of such legislation for the general public, including older people, disabled people and people who are financially or digitally excluded. See Riksbank, "The state's role on the payment market" 2019) https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/press-releases/2019/the-riksbank-proposes-a-review-of-the-concept-of-legal-tender/

[77] Art. 1 of the Belgian Royal Decree mentioned in footnote 60 requires all merchants to open a current account in the books of a bank and the account number must be mentioned on all invoices.

[78] Recently in the US, some municipalities (New Jersey, Philadelphia, New York City, and San Francisco) have introduced ordnances which prohibit certain retail businesses from declining acceptance of cash tendered by consumers.

Privileges under Private Law

71. The fourth legal mechanism through which States have officially sanctioned payment instruments is by granting them privileges under private law with a view to favor the circulation of "currency" relative to other possible means of payment. [79] However, currency is not the only means of payment that benefits from private law privileges: the check and bill of exchange, the original payment instruments, also enjoy certain privileges as "negotiable instruments."[80] As mentioned in the introduction, a full discussion of these private law aspects goes beyond the scope of this paper, but it is important to bear this aspect in mind.

Criminal Law Protection

72. The State has protected officially sanctioned means of payment by imposing criminal law sanctions on those who counterfeit, damage, or destroy those instruments. So far, national as well as public international law focus on the suppression of counterfeit or altered banknotes and coins.

B. CBDC under Monetary Law

CBDC and Official Monetary Unit

73. In principle, the introduction of CBDC would change nothing in regard of a State/monetary union's establishment of its official monetary unit. In other words, CBDC is not expected to be a new "currency unit." When the definitions above refer to CBDC being a "new form of money," they do not refer to this aspect of monetary law, irrespective of design features of CBDC. Rather, if the central bank is authorized to issue CBDC, the central bank will simply digitally issue a liability denominated in the official monetary unit, as are (almost) all its other monetary liabilities (banknotes and coins, book money and bills). This feature will also, in principle, guarantee constant convertibility at par of CBDC in other central bank monetary liabilities, in particular banknotes and book money (see below).

74. In theory, a country's monetary law could establish a new, second monetary unit in which CBDC would be expressed. However, such legislation would also have to establish the mechanism for determining the exchange rate with the country's existing monetary unit.

[79] As one example, Art. 2279, second para., of the Belgian civil code extends the good faith protection to the acquirer of banknotes issued by the central bank: the rule that allows a victim of loss or theft of a movable to revendicate during a 3 years period does not apply. As another example, Art. 14 of the Law on the Statute of the National Bank of Romania provides that "legal provisions regarding lost or stolen bearer certificates do not apply to banknotes and coins issued by the National Bank of Romania." Art. 64 of the Law on the Central Bank of Mauritania has a similar provision.

[80] The Doctrine of Negotiable Instruments or similar doctrines (*valeurs mobilières, Wertpapiere*) basically enshrine the once revolutionary idea that contractual claims can be incorporated in a piece of paper and be transferred by, i.a., the mere physical transfer of that piece of paper—and thus depart from the fundamental rules and procedural requirements of the Roman law *cessio* (assignment).

Historical experience shows that the population is likely to consider and use the original monetary unit as the one monetary unit for their activities,[81] which obviates the need for a second monetary unit. More generally, what would be the added value of establishing such a parallel domestic monetary unit? The formulation and execution of monetary policy would also unnecessarily be complicated by a purely domestic dual-currency system.

CBDC as Official Means of Payment

75. The fundamental question under monetary law is thus whether CBDC could be considered and established as an officially sanctioned means of payment, i.e. "currency". The answer to that question will depend on the design features of CBDC.

Token-Based CBDC

76. *Issuance by the State* – Provided that the central bank law adequately authorizes its issuance, token-based CBDC is to be considered as a valid central bank liability. In such a case, token-based CBDC can unqualifiedly be considered as issued "on behalf of the State."

77. The issue of whether the central bank is allowed to issue digital token-based currency immediately also raises the question whether the central bank should be the only entity authorized to issue such currency. This is discussed in more detail in Box 5.

[81] This was the experience of Belgium, where from 1926 to 1946 the traditional *franc* and the newly introduced *belga* coexisted legally at a rate of 5 *francs* for 1 *belga*. In fact, the *belga* was never widely accepted, not even on the exchange markets. By habit and for convenience's sake the Belgians continued to calculate in *francs* and never wanted to use the new name. See: https://www.nbbmuseum.be/en/2007/03/belga.htm Also in Brazil, during four months in 1994, two different monetary units coexisted as a step in the Real stabilization plan. At that time, the central bank published daily the conversion rates of the old monetary unit (Cruzeiro) to the new monetary unit (URV, acronym for "real unit of value" in Portuguese), up to the moment of the Cruzeiro's extinction.

Box 5. Should Central Banks be Granted a Monopoly for the Issuance of Digital Currency?

As discussed above, many central bank laws grant to the central bank a legal monopoly for the issuance of banknotes. This monopoly entails a prohibition for anybody else (including commercial banks) to issue "bearer on demand" notes and coins that are akin to, and could be confused with, banknotes and coins issued by the central bank. Often, the law protects the central bank's monopoly by imposing criminal law sanctions on the non-authorized issuance of notes or coins that resemble currency. For those rare cases where issuance of banknotes by private banks is still allowed, the central bank exercises firm oversight over such issuance.

Thus, if CBDC is to be equated with "currency," the fundamental question arises as to whether central banks should similarly be granted the monopoly for the issuance of digital currency? This would mean that private issuers, and commercial banks in particular, would not be authorized to issue digital tokens that incorporate "bearer on demand" claims on currency. (Those tokens would be different from crypto-currencies such as Bitcoin, which do not incorporate such claims, and are legally more akin to a commodity.)

Whether a central bank monopoly for digital currency is desirable or appropriate, is ultimately a question of political and policy choice. This being said, the issuance of private digital tokens that resemble CBDC could give rise to very much the same problems, including a severely disrupted monetary system, caused in the 19th century by the issuance of banknotes by private banks that subsequently could not honor their obligations to convert those notes in real currency.

As a legal matter, extending the current issuance monopoly to digital currency is not complicated. The existing monopoly provisions need only be expanded to cover: "bearer on demand notes, in paper and any other material *or immaterial (including digital) form*." Related criminal provisions will also need to be reviewed, as such provisions should be narrowly interpreted, under general principles of criminal law.

78. *Cours Forcé and Convertibility*—It will be very important to define legally what token-based CBDC exactly is. In contrast to central bank book money and bills, which are typically issued pursuant to a detailed contractual framework, the legal status of token-based CBDC will need to be established mainly by legislation. Legislation can grant token-based CBDC *cours forcé* status, similar to banknotes: the value of CBDC will be the amount that is digitally—how this can technically be achieved is another matter–attributed to the token.

79. Into which other central bank liabilities is token-based CBDC convertible? One would expect banknotes and token-based CBDC to be mutually fully convertible as "bearer on demand" claims on the central bank.[82] Under most legal systems, this would be the case, absent specific rules to the contrary. This would of course pre-suppose that banknotes and token-based CBDC have the same value. In principle, this should be the case, unless token-based CBDC would carry interest. Whether that is legally possible is discussed in Box 6.

[82] See *Central Bank Digital Currencies: Foundational Principles and Core Features,* p. 11.

Box 6. Can Token-based CBDC Carry Interest?

Economists have for long discussed the possibility of charging interest on banknotes. With CBDC, this question has regained interest. However, what is economically desirable is not necessarily legally feasible. From a central bank and monetary law perspective, the answer is not straightforward.

As long as central bank banknotes were (and in some legal systems still are) promissory notes, they could not carry a coupon and any interest would need to come from the price differential between face value and issue price (above or below par) at the time of issuance. Even though this is technically possible, it has never been put in practice: banknotes are always issued at par.

Since *cours forcé*, the value of banknotes and coins lays in the face value printed/minted upon the means of payment. As a legal matter, they do not any longer represent a loan of metallic coins camouflaged as a (irregular) deposit, but instead a *sui generis* legal relationship between holder and the issuing central bank. As contractual interest is legally the remuneration for a loan, without a loan there is no contractual interest. This makes it legally very questionable that banknotes can carry interest.

With respect to token-based CBDC, the question arises whether the digital nature of the "currency" changes anything to that conclusion? The answer lies in "first principles."

In respect of the legal relationship that is embedded in the "currency," token-based CBDC follows the same logic as banknotes with *cours forcé*: it is a means of payment for the amount of its face value. Making this form of "currency" subject to interest would break the link between face value and the actual value of the "currency." This would make its use as a means of payment extremely difficult: how can token-based CBDC extinguish monetary obligations at face value if the real value is different in function of interest? The same problem would complicate convertibility of token-based CBDC in banknotes and central bank book money, and thus hinder its circulation. Similarly, to banknotes, charging interest on token-based CBDC does not appear to be a legally robust course of action.

This conclusion is different for account-based CBDC, where the charging of interest, including negative interest, would be legally possible if policymakers would wish to do so. The interest rate for account-based CBDC would be the same as for similar credit balances held on current account in the books of the central bank.

80. This conclusion is different for convertibility into central bank book money. For those central banks that are allowed to open current accounts in their books only for the State, public bodies and banks, the general public will not be authorized to convert token-based CBDC in central bank book money, but the authorized account holders will be.

81. *Legal Tender Status*—Legislation could in principle grant legal tender status to any means of payment, including token-based CBDC. However, does this make sense if large

parts of the population are not technically in a position to receive token-based CBDC as payment?[83] Moreover, to operationalize legal tender status would require the State imposing on its population the acquisition of the technical infrastructure to hold and transfer this form of "currency." Such an approach might raise political as well as legal challenges, such as proportionality, fairness and other legal concerns (e.g., financial inclusion). An intermediate solution may be to grant legal tender status to token-based CBDC only for certain types of recipients, such as the State, public bodies and merchants beyond a certain size (in terms of balance sheet total or number of employees) or for certain private entities that are authorized to perform specific activities (e.g., banks).

82. *Private Law Privileges*—Since in most countries the private law legal status of token-based CBDC is unclear, this issue merits deeper analysis and discussion beyond this paper. As with banknotes, consideration could be given to granting to token-based CBDC a hybrid property law status, whereby this means of payment is considered as an intangible for some issues, and a tangible for others (e.g., *nemo plus* and conflict of laws rules).[84] However, the question also arises whether, if the technological infrastructure always allows for tracing (e.g. in a distributed ledger), token-based CBDC should not be considered as a full-fledged intangible, in which many of the private law privileges of banknotes make little sense.[85]

83. The private law status of token-based CBDC is extremely important to determine whether such CBDC can be lent by its owner to a commercial bank. Such lending[86] is the legal basis for what in common language is mis-labelled a "bank deposit." If that would be the case, token-based CBDC could be "deposited" on a bank account with a commercial bank and be deposited by the latter on its current account in the books of the central bank, so that the CBDC is fully integrated in the fractional reserve banking system. (For the account holder, this would of course transform his claim on the central bank into a claim on the commercial bank, as is the case with the "deposit" of banknotes today.) If this would not be the case, token-based CBDC would basically exist outside the banking system, which would have major monetary and financial implications. The problem is that legal traditions may struggle with countenancing a *mutuum*-type of lending for intangible goods. This issue will need to be thoroughly analyzed by monetary and private law specialists.

84. *Criminal Law Protection*—Most jurisdictions will not be able to apply their counterfeiting rules to token-based CBDC: current law focuses on material forms of currency (banknotes and coins) and criminal law incriminations must be interpreted narrowly,

[83] See also Banque de France, *o.c.*, p. 32.

[84] See Perkins, J., and Enwezor, J., *o.c.,* p. 570, who refer to "virtual choses in possession."

[85] At the same time, it must be acknowledged that even banknotes can, up to a degree, be traced by a serial number, but this does not prevent the legal system from applying absolute protection to the *bona fide* acquirer.

[86] Lending in the Roman law sense of *mutuum*, not *commodatum*: the bank can use the currency lent and only needs to restitute a same amount of similar currency.

following the foundational criminal law principle that no crime exists and can be punished without a law (*nullum crimen, nulla poena sine lege)*. The use of distributed ledger technology may ease this concern. This being said, cyber security law is an existing body of national and public international law, which could be used to regulate the digital counterfeiting of CBDC. This issue goes beyond the scope of this paper and needs to be further investigated by specialists. Annex III includes more details on this issue.

85. *Conclusion*—Under current law, it will be difficult to fully recognize token-based CBDC as an official means of payment, i.e., as "currency." In that sense, it will be legally situated in the taxonomy of central bank monetary liabilities between, on the one hand, banknotes and coins (i.e. currency) and, on the other hand, bills. Well-designed token-based CBDC (including with the appropriate legal authorization for issuance) will certainly be able to circulate more widely and be used as a means of payment than central bank bills, but it is unlikely to attain, absent law reform, the same status as banknotes.

Account-Based CBDC

86. *Issuance by the State*—The issuance of account-based CBDC to banks raises few central bank law issues, and thus issued CBDC will be considered as a valid central bank liability. In the absence of a robust legal basis, the opposite would be true for account-based CBDC issued to the general public. This can, however, be remedied through targeted reform of the central bank law (see above).

87. *Cours Forcé and Convertibility*—As book money, account-based CBDC needs not be granted *cours forcé* status. In contrast to banknotes, the current accounts in the books of central banks are typically governed by detailed contractual rules (often called "current account rules"). By consequence, the central bank can stipulate in those contractual rules the convertibility of account-based CBDC to the extent special rules are needed. In general, there appears no argument why full convertibility into banknotes should not be allowed. The current account rules will also need to stipulate how account-based CBDC can be transferred to other account holders in the books of the central bank and, through the use of payments systems, to accounts in the books of commercial banks (thus transforming it into commercial bank book money), to effect payments.

88. *Legal Tender Status*—Central bank book money does not usually have legal tender status.[87] Thus, account-based CBDC need not be granted legal tender status, at least not as long as this means of payment is only used between financial institutions. This conclusion might be different for account-based CBDC issued to the general public, but the same principles apply as for token-based CBDC: while it is in theory legislatively possible to grant legal tender status to account-based CBDC, this raises fundamental fairness and public policy concerns if large parts of the population are technically not in a position (e.g., not in the

[87] An exception is Article 2 c) of the Swiss Federal Act on Currency and Payment Instruments.

possession of a computer or smartphone) to receive this type of CBDC as payment.[88] Legally, it may not be possible either, because the creditor without access to the technology cannot accept the payment even if he wants to.

89. *Private Law Privileges*—To grant privileges under private law to account-based CBDC would make little sense. The legal nature of book money is clear under private law: it is an intangible that is transferable through the banking technique of debits and credits of the accounts on which it is held. For intangibles, because of perfect traceability, there is no such thing as protection of the good faith acquirer and the *nemo dat* rule will apply. The conflict of laws treatment is similarly the same as for other intangibles (*lex contractus*).

90. There is, however, one element of private law that calls for attention. A creditor's action against a debtor's CBDC account may create a conflict with an existing protection for the central bank. The creditor may seek to attach a debtor's CBDC account balance, but the debtor's access device does not contain monetary value in itself. Rather, an attachment order issued by the court should thus be directed to the central bank to apply to the specific current account linked to the CBDC. However, central banks are often protected from such judicial actions, which are likely to interfere with central banks' mandate to facilitate smooth payments and settlements. Many central bank laws articulate this type of legal protection.[89] Should this protection from attachment also apply to accounts held by the general public and non-financial firms in the books of the central bank? While this question merits further consideration, at first sight the argument of financial stability does not apply.[90]

91. *Criminal Law Protection*—As with token-based CBDC, the criminal law rules on counterfeiting will not apply: book money cannot be counterfeited—of course this does not prevent the application of criminal law on fraud. Yet another question is whether cyber security law would provide special protection to the integrity of the central banks' IT systems that are being used to issue this type of CBDC, for instance by criminalizing hacking.

92. *Conclusion*—Under current law, it will be difficult, but not impossible, to consider account-based CBDC as an official means of payment. Furthermore, it is hard to imagine how law reform can turn this digital claim on the central bank into "currency." This is not a

[88] In Switzerland, this is solved by limiting the obligation to accept Swiss franc sight deposits at the Swiss National Bank in payment without restriction to "any person holding an account there" (Article 3.3). Moreover, "the National Bank shall specify the conditions under which institutions offering payment transaction services may maintain Swiss franc sight deposits" (Article 10).

[89] See for instance Article 9 of the Belgian "Settlement Finality Law" (of 28 April 1999), which prohibits attachment of a "settlement account of a designated (payment or settlement) system." It is unlikely that current accounts held by the general public for account-based CBDC would qualify as such.

[90] If the central bank decides to give access to individuals and firms and attachment and garnishment of accounts in its books is prohibited, there is a real risk that recalcitrant debtors will open these accounts, which would be impossible to seize by creditors.

problem. In most countries, central bank book money plays today a central role in the monetary system without having currency status.

C. The Need for Monetary Law Reform

93. In contrast to central bank law, it will be much more challenging to remedy monetary law obstacles to CBDC. In particular, and in contrast to the need for central bank law reform, some of the issues mentioned below raise very fundamental and conceptual legal policy questions that will require careful analysis and discussion in policy preparation circles and within the competent political bodies. Moreover, as discussed above, the capabilities of a State to engage in monetary law reform to accommodate the issuance of CBDC may be constrained by provisions in the Constitution.

- ***Token-based CBDC***—To legally equate token-based CBDC with banknotes—to the extent this is even possible—will require significant monetary law reform. Countries will first need to consider whether this type of CBDC should and could be granted legal tender status. One option in this respect is to limit the legal tender status to a closed category of sophisticated entities (the State, public bodies and merchants beyond a certain size and/or firms with authorized activities, such as banks). ANNEX II contains draft provisions to this effect. As a next step, countries will need to analyze the private law classification of token-based CBDC and whether this new form of money should be given privileges under private law, in particular with a view to promote its circulation. As a third step the authorities would have to review the definitions of cybercrime offences so as to ensure that they clearly cover cybercrime offences against CBDC.

- ***Account-based CBDC***—At this stage, no monetary law reform is recommended for account-based CBDC.

V. CONCLUSIONS

94. CBDC raises important questions under central bank and monetary law. The legal treatment under those bodies of law will considerably depend on the design features of CBDC. At any rate, token-based and account-based CBDC are legally very different concepts and forms of money. Legally speaking, token-based CBDC would truly be a new form of money: a central bank liability incorporated in a digital token and transferred by transfer of that token. In contrast, account-based CBDC is not a new form of money, but merely book money expressed in digital form.

95. The issuance of CBDC should be founded on a robust, ideally explicit, legal basis in the central bank law. Absent such a basis, the issuance of CBDC may expose central banks to legal and political challenges. Applying textual, contextual, historical and purpose-based interpretation methods, the paper concludes that few central bank laws today offer a sufficiently strong legal basis.

- In respect of token-based CBDC, the question is whether central banks are legally authorized to issue this new type of liability incorporated in a digital token. Most central bank laws currently only authorize the issuance of currency in the form of (paper or plastic) banknotes and metallic coins, and not in the form of a digital token.

- As account-based CBDC is "book money," it can only be offered to entities for whom the central bank is authorized to offer cash current accounts. Many central bank laws currently do not authorize the central bank to offer accounts to the general public.

In either case, this lack of legal basis can be remedied through rather straightforward amendments to the central bank law.

96. Even if the issuance of CBDC enjoys a sound legal basis under central bank law, its status under monetary law raises many complex issues. Importantly, neither form of CBDC would constitute a "new monetary unit." Rather, CBDC would be a form of a means of payment expressed in the official monetary unit. Hence, this paper focuses on the inherent capability of CBDC to acquire the status of *official* means of payment, i.e. currency.

97. In that regard, token-based CBDC raises many questions. Under current law, it would in most countries not qualify as currency, as this legal category is hitherto typically reserved to physical banknotes and metallic coins. In theory, monetary law could through law reform establish token-based CBDC as currency, but this will be subject to a number of challenges and complexities.[91]

- First, allocating to it legal tender status—which admittedly is not a *sine qua non*—is not obvious as long as broad layers in the population are not in a position to technically receive such a means of payment.

- Second, because token-based CBDC has no clear status under private law, it will be difficult to extend to it the private law privileges that legal systems attribute to currency with the aim to promote its circulation.

- Third, providing criminal law protection against electronic counterfeiting will raise fundamental questions, including whether electronic counterfeiting is a legal concept that fits into the broader criminal law system.

By consequence, even if token-based CBDC were to be legislatively labelled "currency," it is doubtful that it will be able to fully enjoy the same privileged legal status as traditional currency in the broader legal system. This is not *per se* problematic, as in many countries,

[91] Rogoff, K., *The Curse of Cash*, 2016, p.213.

commercial bank book money is the most widely used means of payment, despite the fact that legally it does not qualify as currency.

98. In turn, account-based CBDC is actually not currency at all. There is nothing wrong with that—it would have the same legal status as other central bank book money, which as risk free asset plays an important role in the financial system. Therefore, no reforms to monetary law legislation are necessary to make this form of book money legally operational.

99. Finally, the "meta-message" of the paper is that countries should carefully consider the legal foundations of CBDC when and if they decide to introduce this digital means of payment. In some jurisdictions, there will be an ostensibly easier route of simply providing broad interpretations to existing legal provisions. However, a comprehensive review of the central bank and monetary law framework will ensure that the legal aspects of the intended public policy choices are well understood and codified in law. Ideally, this exercise takes place within a broader endeavor to also review other legal issues, including (but not limited to) private law and tax law.

ANNEX I: DRAFT CENTRAL BANK LAW PROVISIONS RELATED TO CBDC

Central Bank Functions

Art. Xx. *Functions*

With a view to achieving its objectives, the Central Bank has the following functions:

i. to define and implement monetary policy;

ii. …

iii. to issue currency;

iv. to promote a sound and efficient payment system;

v. ….

Central Bank Powers

Art. Xx. *Currency*

The Central Bank is authorized to issue banknotes, coins and currency in digital form.

[Art. Xx. *Powers Ancillary to the Issuance of Currency*

The Central Bank is authorized to produce, acquire, distribute, withdraw and destroy banknotes, coins and currency in digital form and to adopt measures to ensure the storage of value and transaction processing of currency in digital form.]

Art. Xx. *Current Accounts*

The Central Bank is authorized to open current and other accounts in its books for the State, public bodies, banks, and other categories of accountholders established by the [Executive Board/Board of Directors].

The credit balances on those accounts may be remunerated.

ANNEX II: Draft Monetary Law Provisions related to CBDC

Art. Xx. *Legal Tender of Currency*

The banknotes and coins issued by the Central Bank are legal tender in [name country].

The currency issued by the Central Bank in digital form is legal tender for payment of monetary obligations to the State, municipalities, banks and [to be determined]. The Government is authorized to expand these entities by Decree.

Art. Xx. *Monopoly of Issuance of Currency*

The Central Bank has the sole right of issuing metallic coins and bearer on demand notes, in paper and any other material *or* immaterial (including digital) form.

Any person or entity who issues coins, bearer on demand notes, in paper and any other material or immaterial (including digital) form, or any other document or token which is likely to pass as currency or means of payment will be punishable by [TBC].

[This provision applies without prejudice to the issuance of electronic money pursuant to {legislation}.]

ANNEX III. CRIMINAL LAW AND CBDC

So far national laws only focus on the suppression of counterfeit banknotes and coins; i.e. not explicitly on the counterfeiting of CBDC.

Box 1. National Law on Counterfeiting and Mutilating Legal Tender

Whereas the definition of counterfeiting and the appropriate sanctions are commonly set out in criminal codes, various central bank laws do contain relevant provisions, as the following example of Article 64 of the Organic Constitutional Law of the Central Bank of Chile (as amended) demonstrates: "Whoever manufactures or sets in circulation objects whose shape resembles banknotes of legal tender in a manner that such forged banknotes are easily accepted in place of the real ones, shall be penalized with 541 days to 5 years of imprisonment."

Various countries also have criminal law provisions prohibiting the mutilation of banknotes and coins. This is to protect issued legal currency. For example, in the USA 18 USC 333 prescribes criminal penalties against anyone who "mutilates, cuts, defaces, disfigures or perforates, or unites or cements together, or does any other thing to any bank bill, draft, note…". Similarly, Section 28(1) of the Reserve Bank of New Zealand Act provides that "no person shall, without the prior consent of the Bank, willfully deface, disfigure or mutilate any banknote". A contravention of this probation qualifies as an offence and makes the perpetrator liable on conviction to a fine not exceeding $ 1000.

The same focus on the suppression of counterfeit banknotes and coins is found in public international law.

Box 2. Geneva Convention for the Suppression of Counterfeiting

The Geneva Convention for the Suppression of Counterfeiting of April 20, 1929 aims to harmonize the national criminal substantive law elements of offences in counterfeiting. This Convention is still in force.

Article 2 of the Convention defines currency to mean "paper money (including banknotes) and metallic money, the circulation of which is legally authorized".

Article 3 provides that member countries should ensure that the following acts are punishable as ordinary crimes:

(i) the fraudulent making or altering of currency, whatever means are employed, (ii) the fraudulent uttering of counterfeit currency,

(iii) introducing, receiving, or obtaining currency with a view to uttering the same and with knowledge that it is counterfeit,

(iv) attempts to commit, and intentional participation in the foregoing and

(v) the fraudulent making, receiving or obtaining of instruments or other article peculiarly adapted for counterfeiting or altering currency.

Each of the aforementioned acts should be considered as a distinct offence if they are committed in different countries.

The Convention also establishes a mechanism for international cooperation against counterfeiting. Article 12 requires the member countries to centralize, within the framework of their domestic laws, investigations about counterfeiting in a Central Office. Such central office must be in close contact with the central bank issuing currency, the national police and the Central Offices in other countries. ICPO-Interpol acts as the International Central Office for the Suppression of Currency Counterfeiting (Article 15).

An important point is that the counterfeiting provisions in central bank laws (or criminal laws) do not explicitly address cybercrimes affecting digital currencies. Nevertheless, cyber security law is an existing body of law which could—with due observance of the principle of *nullum crimen sine lege, nulla poena sine lege*—be used to regulate digital counterfeiting of CBDC. Indeed, on November 23, 2001 the Council of Europe adopted the first international treaty on cybercrime: the Budapest Convention on Cybercrime.[92]

[92] European Treaty series No. 185. The Convention has been signed and ratified primarily by member countries of the Council of Europe, but it is open for accession by non-member countries. As a result, a number of important non-members such as Australia, Canada, Israel, Japan and the USA have also signed and ratified this Convention.

Box 3. Budapest Convention on Cybercrime

Like the Geneva Convention, the Budapest Convention aims to harmonize the national criminal substantive law elements of offences in cybercrime and it also establishes a mechanism for international cooperation against cybercrime.[93]The Budapest Convention does not explicitly mention offences against central bank digital currencies.

However, it lists several offences which consist in interfering with, the misuse of, forgery, or fraud related to computer data. Article 1 of the Budapest Convention defines computer data to mean "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function". This definition could reasonably be taken to include data incorporated in a central bank digital currency. Therefore, the following substantive criminal law offences, which are harmonized by the Budapest Convention, are drafted in a broad manner and are therefore particularly relevant to the forgery, fraud and interference with central bank digital currencies:

(i) intentionally damaging, deleting, deteriorating, altering or suppressing computer data without right (Article 4),

(ii) Intentionally (seriously) hindering without right the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (Article 5),

(iii) intentionally producing, selling, procuring for use, import, distribution or otherwise making available devices, including computer programs, designed or primarily adapted for the purpose of cybercrime (Article 6),

(iv) committing intentionally and without right, the input, altering, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible (computer-related forgery) (Article 7),

(v) causing the loss of property to another person by any input, alteration, deletion or suppression of computer data (computer-related fraud) (Article 8), and

(vi) the infringement of copyright and related IP rights (Article 10).

Note that the wording of the cybercrime offences is broad enough so that it does not seem necessary to define mutilation as a criminal offence (as is the case for legal tender banknotes and coins). Indeed, the wording of "intentionally damaging, deleting, deteriorating, altering or suppressing computer data without right" in Article 4 would cover intentional mutilation of central bank digital currency.

[93] ICO-Interpol's Global Cybercrime Strategy for 2016 to 2020 outlines the organization's support to member countries to combat cybercrime by coordinating and delivering specialized police capabilities in this regard.

While the wording of the Budapest Convention’s cybercrimes is in principle broad enough to cover offences to CBDC, the principle of *nullum crimen sine lege, nulla poena sine lege* would require the authorities to precisely define the cybercrime offences against CBDC. Therefore, most jurisdictions will not be able to apply their counterfeiting rules to token-based CBDC. Also, as already noted, the criminal law rules on counterfeiting will not apply to account-based CBDC as book money cannot be counterfeited. Of course, cyber security law could provide special protection to the integrity of the central banks’ IT systems that are used to issue this type of CBDC.

REFERENCES

ADB Institute, 2019, *Central Bank Digital Currency and Fintech in Asia*.

Allen, J., 2019, Property in Digital Coins, 8(1) *European Property Law Journal,* 64.

Allen, J., and Lastra, R., 2019, Virtual Currencies in the Eurosystem: Challenges Ahead, *The International Lawyer,* Vol. 53, No. 2.

Allen, J., and Lastra, R., 2020, Border Problems: Mapping the Third Border, *Modern Law Review*, 83(3).

Auer, R., and Bohme, R., 2020, *The Technology of retail central bank digital currency*, BIS.

Auer, R., Cornelli, G, and Frost, J., 2020, *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies,* BIS, WP No. 880.

Bank of Canada, ECB, Bank of Japan, Sverigse Riksbank, Swiss national bank, Bank of England, Board of Governors of the Federal Reserve System and BIS, 2020, *Central Bank Digital Currencies: Foundational Principles and Core Features*: *Report No. 1 in a series of collaborations from a group of central banks*.

Banque de France, 2020, *Central Bank Digital Currency*.

Barontini, C., and Holden, H., 2019, *Proceeding with Caution-a Survey on Central Bank Digital Currency*, BIS Papers No. 101.

Bech, M., and Garratt, R, 2017, *Central Bank Cryptocurrencies*, BIS Quarterly Review.

Bossu, W., and Rossi, A., 2019, *The Role of Board Oversight in Central bank Governance: Key Legal Design Issues*, WP/19/293.

Carstens, A., 2019, *The Future of Money and Payments*, Central Bank of Ireland 2019 Whitaker Lecture.

CPMI, 2018, *Central Bank Digital Currencies*, BIS.

Fox, D., and Green, S., (eds.), 2019, *Cryptocurrencies in Public and Private Law,* Oxford University Press.

Gnan, E., and Masciandaro, D., 2018, *Do We Need Central Bank Digital Currency? Economics, Technology and Institutions*, SUERF.

Goodhart, C., 1985, *The Evolution of Central Banks,* MIT Press.

Hahn, H. and Häde, U., 2010, *Währungsrecht*.

IMF Staff, 2018, *Casting Light on Central Bank Digital Currency*, IMF, SDN/18/08.

IMF Staff, 2020, *A Survey of Research on Retail Central Bank Digital Currency*, WP/20/104.

IMF Staff, *Digital Money Across Borders: Macro-Financial Implications,* IMF, 2020.

Jacqué, J.P., 2010, *Droit Institutionel de l'Union Européenne*.

Kahn C, 2016, *How are payments accounts special*?, Federal Reserve Bank of Chicago.

Lastra, R., 2006, *Legal Foundations of International Monetary Stability*, Oxford University Press.

Lastra, R., 2015, *International Financial and Monetary Law*, Oxford University Press.

Mann, F., *The Legal Aspect of Money,* 4th Ed.

Perkins, J., and Enwezor, J., 2016, The legal aspect of virtual currencies, *Butterworths Journal of International Banking and Financial Law,* November 2016.

Riksbank, 2019, *The state's role on the payment market*.

Rogoff, K., 2016, *The Curse of Cash*.

Shirai, S., 2019, *Central Bank Digital Currency: Concepts and Trends*, VOX CEPR Policy Portal, 6 March 2019.

Smits, R., 1995, *The European Central Bank Institutional Aspects*.

Waerzeggers, C., and Aw, I., 2019, Difficulties in Achieving Neutrality and other Challenges in Taxing Crypto Assets, in Chris Brummer, ed, *Cryptoassets: Legal, Regulatory and Monetary Perspectives*, New York: Oxford University Press.

Zilioli, C., 2020, Crypto-assets: Legal Characterization and Challenges under Private Law, 46 *EL Review*.

Slide Decks