WORLD ECONOMIC FORUM

Digital Currency Governance Consortium White Paper Series

COMPENDIUM REPORT

NOVEMBER 2021

Images: Getty Images

Contents

Preface 3

Introduction to the DCGC white paper series 4

Reading guide 5

Digital Currency Governance Consortium Steering Committee 6

Contributors 7

Glossary 11

Endnotes 14

Paper 1 The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth 15

Paper 2 Regulatory and Policy Gaps and Inconsistencies of Digital Currencies 43

Paper 3 Digital Currency Consumer Protection Risk Mapping 64

Paper 4 What is the Value Proposition of Stablecoins for Financial Inclusion? 85

Paper 5 Blockchain-Based Digital Currency and Tools for Cross-Border Aid Disbursement 128

Paper 6 Privacy and Confidentiality Options for Central Bank Digital Currency 155

Paper 7 Defining Interoperability 175

Paper 8 CBDC Technology Considerations 197

Preface

Sheila Warren
Deputy Head of the C4IR Global Network, Head of Data, Blockchain and Digital Assets, World Economic Forum

Ziyang Fan
Head of Digital Trade, World Economic Forum

Matthew Blake
Head of Platform of Shaping the Future of Financial and Monetary Systems, World Economic Forum

As digital currencies begin to play a critical role in the global economy, their responsible design and deployment must be a focus for decision-makers around the world.

Globally, there is an accelerating shift towards digital payments and the ownership and use of digital currency. Innovations in technology are driving discussions and development of new forms of money with which the public can interact. The way global leaders – from public and private sectors – develop, coordinate and regulate such digital currencies will have profound implications on society's capacity to harness their compelling benefits and avoid the potentially significant risks they introduce.

Two distinct forms of digital currency – central bank digital currency (CBDC) and "stablecoins" – have caught the attention of policy-makers and the private sector in recent years. CBDC and stablecoins are the focus of this series of white papers. More than 70% of central banks are currently exploring the design and issuance of CBDC for their economies, attracted by opportunities to improve – among other things – financial inclusion, digital trade, payment efficiency and access to safe central bank money in an era of dwindling cash usage.[1]

China has launched large-scale pilots of its Digital Currency Electronic Payment (DC/EP), while smaller nations such as the Bahamas have started to launch their CBDC. Yet, successful CBDC deployment is easier said than done. CBDC can introduce considerable risks to its native economy and citizens, as well as to foreign jurisdictions to which it grants access.

Stablecoins – issued by private entities rather than monetary authorities – are a form of cryptocurrency operating on blockchain technology, with price-stabilization mechanisms that aim to keep their prices stable relative to a fiat currency or other assets.[2] Stablecoins can offer the capabilities of cryptocurrency without the price volatility. However, some stablecoins have been rapidly issued and adopted, without always adhering to sufficient regulatory oversight or consumer protection practices.

The World Economic Forum's Digital Currency Governance Consortium (DCGC) – comprising a global, multi-sector set of more than 85 leading organizations – has gathered since early 2020 to co-design research and policy frameworks to guide the private sector and policy-makers through some of the most pressing challenges, opportunities and decisions related to CBDC and stablecoins. It plays a critical role in leading multi-stakeholder discussions on these subjects in a neutral and objective manner, catalysing the cross-sector global cooperation that is essential to successfully address the opportunities and risks introduced by CBDC and stablecoins in the age of new digital money.

Introduction to the DCGC white paper series

> The DCGC attempts to provide a neutral, objective and analytical perspective on the pertinent issues surrounding the governance of new digital currencies

The Digital Currency Governance Consortium (DCGC) convenes more than 85 organizations from the public sector, private sector, civil society and academia to provide a global perspective towards addressing high-priority policy and governance issues surrounding new forms of digital currency. DCGC has focused its initial phase of work on CBDC and price-stabilized cryptocurrencies, referred to as "stablecoins". This series of eight white papers delivers on the scope of work outlined in the Forum's January 2021 publication, *Digital Currency Governance Consortium: Vision for 2021 Deliverables*.[3]

Non-stabilized cryptocurrencies (such as bitcoin or ether) and decentralized finance ("DeFi") applications, while important, are not the focus of this white paper series. However, the white papers under the theme "Value Proposition for the Under-served" explore the use of cryptocurrencies in cross-border humanitarian aid, as well as the potential value of cryptocurrencies and DeFi for financial inclusion. A deeper focus on cryptocurrencies is likely to be contemplated in the second phase of DCGC's work, which launches in January 2022.

This white paper series considers both generally available "retail CBDC", which would enable all households to transact in electronic central bank money, and "wholesale CBDC", which would be limited to licensed financial institutions. Moreover, it attempts where possible to generalize about stablecoins as a broad class of digital currency. That said, this goal is challenging given extensive differences among stablecoins in terms of economic and technical design, quality of reserves and collateral, legal protections and regulatory oversight.

The scope of this white paper series was carefully selected through a range of multi-stakeholder workshops. The criteria set forth for the content include the following:

- Would the issue benefit from multi-stakeholder engagement?
- Is this issue already being addressed by other entities?
- Is this issue amenable to contributions from research or governance frameworks?
- Could work on this issue have a positive impact for the world?

As per the criteria above, the questions and issues explored in this series include:

- What are the various roles and opportunities for the public sector, public-private cooperation and intergovernmental cooperation in an era of rapid and expansive digital currency growth?
- Which regulatory gaps and inconsistencies should policy-makers be aware of as they consider oversight and regulation of new forms of digital currency? How can these gaps be closed?
- What are the key risks to consumers of various forms of digital currencies? How should these risks be addressed for consumer protection?
- Can stablecoins and blockchain-based payments deliver the claimed benefits of promoting financial inclusion and improving the efficiency of cross-border retail payments?
- What efforts are currently underway employing blockchain technology for cross-border aid disbursement?
- Which privacy and confidentiality approaches are technically feasible and available for CBDC?
- What does "interoperability" mean for digital currencies issued on distributed ledger platforms? What are the high-level design principles for interoperability and how can they be operationalized?
- What are the key technical design choices and issues at play for policy-makers who are seeking to deploy a CBDC?

Building on the World Economic Forum's 2020 publication, *Central Bank Digital Currency Policy-Maker Toolkit*, DCGC participants have reviewed a wide range of published material, including those from international and intergovernmental organizations. The DCGC carried out its investigations alongside existing and new efforts in this space, such as those by the Financial Stability Board (FSB), the Financial Action Task Force (FATF) and the Bank for International Settlements (BIS), many of which involve DCGC-member organizations. Our hope is that this white paper series will augment the work of these organizations and other initiatives.

Lastly, this report series is informed by numerous dialogues, workshops, interviews and panels including World Economic Forum meetings at The Davos Agenda 2021 and the Global Technology Governance Summit.[5] Above all, the DCGC attempts to provide a neutral, objective and analytical perspective on the pertinent issues surrounding the governance of digital currencies.

Reading guide

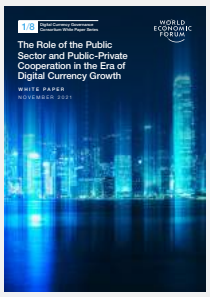
This report series is composed of eight distinct white papers that have been grouped into three high-level thematic categories as follows:

1. Regulatory Choices
2. Value Proposition for the Underserved
3. Technology Choices

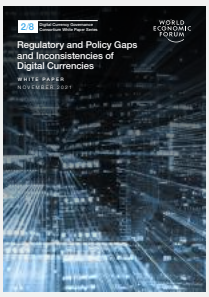
All eight white papers focus on CBDC and stablecoins only, although this work relates to and speaks to other forms of digital currency such as cryptocurrency in several areas.

The series can be read in either a linear fashion from beginning to end, or in a modular fashion by paper. The eight white papers stand independently from one another, although they cross-reference content where relevant and to avoid duplication. The prevalence of cross-referencing between white papers highlights the extensive connections and inter-dependencies of their subject matter.

Theme 1 Regulatory Choices



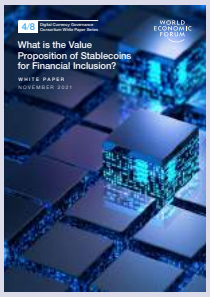
White Paper #1:
The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth



White Paper #2:
Regulatory and Policy Gaps and Inconsistencies of Digital Currencies

White Paper #3:
Digital Currency Consumer Protection Risk Mapping

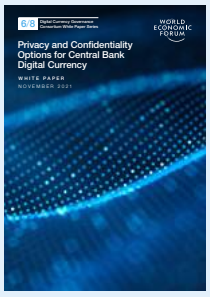
Theme 2 Value Proposition for the Underserved



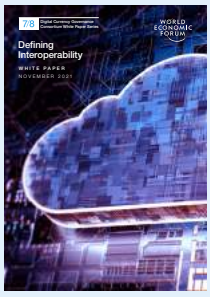
White Paper #4:
What is the Value Proposition of Stablecoins for Financial Inclusion?

White Paper #5:
Blockchain-Based Digital Currency and Tools for Cross-Border Aid Disbursement

Theme 3 Technology Choices



White Paper #6:
Privacy and Confidentiality Options for CBDC



White Paper #7:
Defining Interoperability

White Paper #8:
CBDC Technology Considerations

Digital Currency Governance Consortium Steering Committee

Mark Carney
COP26 Finance Adviser to the Prime Minister of the United Kingdom and United Nations Special Envoy for Climate and Finance

Benoit Cœuré
Head of the BIS Innovation Hub, Bank for International Settlements

Meltem Demirors
Chief Strategy Officer, CoinShares

Hikmet Ersek
President and Chief Executive Officer, The Western Union Company

Jacob A. Frenkel
Chairman of the Board of Trustees, The Group of Thirty (G30)

Glenn H. Hutchins
Chairman, North Island

Paula Ingabire
Minister of Information Communication Technology and Innovation, Rwanda

Eric Jing
Chairman and Chief Executive Officer, Ant Group

Eva Kaili
Member of the European Parliament

Charlotte Hogg
Chief Executive Officer, Europe, Visa Inc.

Alfred F. Kelly
Chairman and Chief Executive Officer, Visa Inc.

H.M. Queen Máxima of the Netherlands
United Nations Secretary-General's Special Advocate for Inclusive Finance for Development

Michael Miebach
President, Mastercard

Zhu Min
Chairman, National Institute of Financial Research

Sara Pantuliano
Chief Executive, Overseas Development Institute

Marcus Pleyer
President, Financial Action Task Force (FATF)

Anne Richards
Chief Executive Officer, Fidelity International

Dan Schulman
President and Chief Executive Officer, PayPal

Tharman Shanmugaratnam
Senior Minister, Singapore and Chairman, Monetary Authority of Singapore

Contributors

This series is based on the consolidated views of the World Economic Forum Digital Currency Governance Consortium (DCGC) community. It is a combined effort based on numerous interviews, discussions, workshops and research conducted over an 18-month period. The opinions expressed herein do not necessarily reflect the views of the individuals or organizations involved in the project or listed below. Sincere thanks are extended to those who contributed their insights, including those not captured below. Appreciation is further extended to those who contributed to the DCGC's workshops held in 2020 and to the 2021 World Economic Forum Davos Agenda and Global Technology Governance Summit.

World Economic Forum

Ashley Lannquist
Project Lead, Blockchain and Digital Currency, World Economic Forum LLC

Kathryn White
Project Fellow, Blockchain and Digital Currency, World Economic Forum LLC

Sheila Warren
Deputy Head of the C4IR Global Network, Head of Data, Blockchain and Digital Assets, and Executive Committee Member, World Economic Forum LLC

Yan Xiao
Project Lead, Digital Trade, World Economic Forum LLC

Ashlin Perumall
Project Fellow, Blockchain and Digital Currency, World Economic Forum LLC

Clarisse Awamengwi
Project Specialist, Blockchain and Digital Currency, World Economic Forum LLC

Co-authors

Sebastian Banescu
Senior Research Engineer & Country Manager, Quantstamp Inc, Germany

Brian Behlendorf
Executive Director, Hyperledger, Linux Foundation, USA

Daniel Benarroch
Director of Research, QEDIT, Israel

Ben Borodach
Vice President of Strategy and Operations, Team8, USA

Shearin Cao
Executive Director, Group Public and Regulatory Affairs, Standard Chartered Bank, United Kingdom

Riyad Carey
Senior Policy Analyst, Global Blockchain Business Council, Switzerland

Simon Chantry
Co-Founder and Chief Information Officer, Bitt, Barbados

Ezechiel Copic
Partner, Head of Official Sector Engagement, cLabs, USA

Nilixa Devlukia
Regulatory Consultant, Mastercard, USA

Erin English
Technology Policy Fellow, Visa Economic Empowerment Institute, Visa, USA

Susan Friedman
Head, Public Policy, Ripple, USA

Luc Froehlich
Global Head of Investment Directing, Fixed Income, Fidelity International, Hong Kong SAR, China

Vanessa Grellet
Global Head of Partnerships, Alliances and Channels, Consensys, USA

Seth Hertlein
Head, Policy and Government Relations, Stellar Development Foundation, USA

John Ho
Head, Legal, Financial Markets, Standard Chartered Bank, Singapore

Sasha Kapadia
Director, Government and Development, Mastercard, USA

Ala'a M. Kolkaila
Advisor, Ministry of International Cooperation of Egypt, Egypt

Ivy K. Lau
Lead Manager, Global Public Policy and Research, PayPal, USA

John S. Lee
Lead, Blockchain Product and Strategy, Shopify, Canada

Alfonso Pidal Ligués
Blockchain & Digital Assets Strategy, BBVA, Spain

Francisco Maroto
Blockchain & Digital Assets Discipline Head, BBVA, Spain

Vijay Mauree
Programme Coordinator, Study Groups Department, Standardization Bureau, International Telecommunication Union, Switzerland

Jesse McWaters
Global Head, Digital Policy, Mastercard, USA

Karen L. Ottoni
Director of Ecosystem, Hyperledger, Linux Foundation, USA

Dominic Paolino
Blockchain and Multiparty Systems, Accenture USA

Sandra Ro
Chief Executive Officer, Global Blockchain Business Council, Switzerland

Alejandro Rothamel
Chief Legal and Compliance Officer, Ripio, Argentina

Jonathan Rouach
Co-Founder and Chief Executive Officer, QEDIT, Israel

Matthieu Saint Olive
CBDC Advisor, ConsenSys, France

Erica M. Salinas
Independent Researcher, USA

Mai Santamaria
Head, Financial Advisory Team, Department of Finance of Ireland, Ireland

Geoffrey See
Co-Founder, Shoppalive, Vietnam

Alpen Sheth
Senior Technologist, Financial Innovation, Mercy Corps Ventures, USA

David Treat
Senior Managing Director, Accenture, USA

Tongyi Wang
Senior Expert, Ant Group Research Institute, Ant Group, China

Leila Yosef
Research Manager, Accenture, USA

Pēteris Zilgalvis
Head of Unit, Digital Innovation and Blockchain, European Commission, Brussels

Reviewer acknowledgements

Sincere appreciation is extended to the individuals below, who in many cases spent numerous hours providing critical input and feedback to the drafts. These individuals represent the majority of DCGC contributors and their diverse insights are fundamental to the success of this work.

Usman Ahmed
Head, Global Public Policy and Research, PayPal, USA

Jeremy Allaire
Co-Founder, Chairman, Chief Executive Officer, Circle Internet Financial, USA

Rania Al-Mashat
Minister of International Cooperation, Ministry of International Cooperation of Egypt, Egypt

Yasmeen Al-Sharaf
Head, FinTech and Innovation Unit, Central Bank of Bahrain, Bahrain

Ana Alvarez
MPA Candidate, Harvard Kennedy School, Harvard University, USA

Antonio Leal Batista
Software Engineer, Head of Project Pipeline, LACChain Ecosystem, Peru

Gabriel Bizama
International Policy Lead, Stellar Development Foundation, Switzerland

Adam Bornstein
Team Lead, Innovative Finance and System Change, Danish Red Cross, Vermont

Carolina Caballero
Vice President, Product Development, Mastercard, USA

David Carlisle
Director, Policy and Regulatory Affairs, Elliptic, United Kingdom

Sam Chadwick
Executive Director, Emerging Tech, UBS, Switzerland

Sean Colenso-Semple
Independent Researcher, Australia

Matthew Davie
Chief Strategy Officer, Kiva, USA

Sumedha Deshmukh
Platform Curator, Blockchain and Digital Assets, World Economic Forum LLC

Dante Disparte
Chief Strategy Officer, Head of Global Policy, Circle Internet Financial, USA

Denelle Dixon
Chief Executive Officer, Stellar Development Foundation, USA

James Edwards
Researcher and Consultant, Soramitsu, Germany

Douglas Elliott
Partner, Oliver Wyman, USA

Christopher Fabian
Giga Lead and Co-Founder, UNICEF, New York

Ziyang Fan
Head, Digital Trade, World Economic Forum

Mora Farhad
Information Technology Officer, Technology and Innovation Lab, The World Bank Group, Washington DC

Erik Feyen
Lead Financial Economist, Head Global Financial Systems, World Bank Group, Washington DC

Daniel Gabriel
Legal Director, Financial Services; BPO Global Regulatory Lead, Accenture, United Kingdom

Lucia Gallardo
Founder, Chief Executive Officer, Emerge, Canada

Nitin Gaur
Director, IBM Financial Sciences and Digital Assets, IBM, USA

Giuseppe Giordano
Senior Manager, Research and Development, Accenture Labs, Accenture, France

Arushi Goel
Project Specialist, Data Policy and Blockchain, World Economic Forum LLC

Robert Greenfield IV
President and Chief Executive Officer, Emerging Impact, USA

Jonas Gross
Research Assistant and Project Manager, Frankfurt School Blockchain Center, Frankfurt School of Finance and Management, Germany

Houman Haddad
Head, Emerging Technologies, United Nations World Food Programme, Italy

Sandra Hart
Chief Executive Officer, Advisory Services, Emerging Impact, USA

Lasse Herskind
Software Developer, Aave, Denmark

Justin Herzig
Senior Principal, Global Blockchain Research Lead, Accenture, USA

Nadia Hewett
Project Lead, Data for Common Purpose Initiative, World Economic Forum LLC

Satoru Hori
Project Fellow, Centre for the Fourth Industrial Revolution, World Economic Forum LLC

Kibae Kim
Project Fellow, Centre for the Fourth Industrial Revolution, World Economic Forum LLC

Patrick Killian
Senior Advisor, Humanitarian and Development, Mastercard, USA

Michael Klein
Managing Director, Blockchain and Multiparty Systems Architecture, Accenture, USA

Tayo Tunyathon Koonprasert
Senior Specialist, Digital Currency Team, Bank of Thailand, Thailand

Piotr Koszek
Consultant, Cloud, DevOps and Automation, Accenture, Poland

Bernhard Kowatsch
Head, Innovation Accelerator, United Nations World Food Programme, Germany

Stani Kulechov
Chief Executive Officer, Aave, United Kingdom

Andrey Kurennykh
Co-Founder and Chief Executive Officer, Tangem, Switzerland

Xavier Lavayssière
Digital Finance Expert, International Monetary Fund, Washington DC

Nikolai Layne
Financial Examiner, Financial Services Commission, Barbados

Will Le
Partner, Innovation, cLabs, USA

Larissa De Lima
Fellow, Oliver Wyman Forum, USA

Brynly Llyr
General Counsel, cLabs Inc, USA

Christina Lomazzo
Innovation Fund Lead, UNICEF, New York

Marcos Allende Lopez
IT Specialist, Blockchain, Quantum Technologies and SSI, Inter-American Development Bank, Washington DC

Vera Lubbersen
Policy Advisor, Central Bank of the Netherlands, Netherlands

Tim Marple
PhD Candidate, University of California Berkeley, USA

Ruth McCormack
Technical Advisor, CaLP, Canada

Raunak Mittal
Technology and Innovation Officer,
The World Bank Group, Washington DC

Matu Mugo
Assistant Director, Bank Supervision,
Central Bank of Kenya, Kenya

Aristides Andrade Cavalcante Neto
Chief of Cyber Security and Technological Innovation Office, Central Bank of Brazil, Brazil

Marek Olszewski
Partner, Engineering, cLabs, Germany

Karen Peachey
Director, CaLP, Kenya

Drew Propson
Head, Technology and Innovation in Financial Services,
World Economic Forum LLC

Jaikumar Ramaswamy
Chief Risk and Compliance Officer, cLabs, USA

Francisco Rivadeneyra
Director, CBDC and FinTech Policy,
Bank of Canada, Canada

Sebastian Rodriguez
Senior Manager, Development Partnerships,
Accenture, USA

Richard Rosenthal
Principal, Deloitte, USA

Rafael Sarres de Almeida
Senior Advisor, Cybersecurity and Financial Technology, Central Bank of Brazil, Brazil

Saundra Severtson
Partner, People, cLabs, USA

Dinesh Shah
Director, Fintech Research, Bank of Canada, Canada

Luca Schiatti
Manager, Research and Development,
Accenture, France

Ric Shreves
Director, Emerging Technology,
Mercy Corps, USA

Nicolo Stewen
Product and Strategy, Aave, United Kingdom

Anna Stone
Head of Strategy and Advocacy,
GoodDollar, USA

Florian Studer
Manager, Deloitte, USA

David Symington
Policy Advisor, Fintech and Digital Payments,
Office of the UNSGSA, United Nations, New York

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

Tamerlan Taghiyev
Executive Director, Islamic Development Bank, Azerbaijan

David Tercero-Lucas
Researcher and Economic Analyst,
Autonomous University of Barcelona, Spain

Joseph Thompson
Chief Executive Officer and Co-Founder,
AID:Tech, Singapore

Hervé Tourpe
Head of Digital Advisory, International Monetary Fund,
Washington DC

John Velissarios
Global Managing Director, Blockchain and Multiparty Systems; Digital Assets, Custody and CBDC Lead, Accenture, United Kingdom

Toh Wee Kee
Specialist Leader, Distributed Ledger Technology,
Monetary Authority of Singapore, Singapore

Ben Weisman
Project Lead, Financial Innovation,
World Economic Forum LLC

Sybil Welsh
Senior Project Specialist, Eastern Caribbean Central Bank, St. Kitts and Nevis

Editing and design

Jonathan Walter
Editor

Laurence Denmark
Studio Miko

Glossary

Anti-money laundering (AML)/Combating the financing of terrorism (CFT):
AML includes any policies, laws, regulations and protocols designed to combat the introduction of funds obtained from illicit activities (such as racketeering, corruption, drug trafficking and fraud) into legitimate money systems and exchanges. CFT consists of similar measures designed to prevent and combat the financing of terrorist activities. Both money laundering and terrorist financing activities generate financial flows that divert resources away from economically and socially productive uses, often with negative impacts on the financial sector, national fiscal stability and society.

Atomic swaps:
A situation in which two parties fully exchange assets without having to trust a centralized exchange or third party. In an "atomic" transaction in digital currency, if one leg of a transaction that involves payment for an asset fails, the whole transaction fails.

Anonymous:
According to the definition in the European Union's General Data Protection Regulation (GDPR), anonymity refers to "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".

Blockchain:
A form of distributed ledger technology (DLT) in which transactions are conducted in a peer-to-peer fashion and then broadcasted to the entire set of system participants, all or some of whom work to validate them in batches known as blocks. Such validation is executed using the system's consensus protocol (such as proof-of-work or proof-of-stake). Validated blocks are then cryptographically linked to a primary sequence of blocks, referred to as a blockchain.

Central bank digital currency (CBDC):
A digital form of central bank money that may be accessible to the public (general-purpose or retail CBDC), or to a select set of licensed participants such as financial organizations (wholesale CBDC). CBDC is denominated in the national unit of account. It is issued by and is a direct liability of the central bank.

Confidentiality:
Relates to the ability to keep certain information private from non-permitted parties. Confidentiality in some legal systems is protected by a duty on the recipient not to divulge to third parties without the discloser's consent. It is also sometimes protected by agreement between the discloser and recipient.

Centralized exchange:
A business service that acts as an intermediary in an exchange transaction to enable the conversion to and from certain assets or currencies.

Crypto-assets:
Crypto-assets typically refer to an asset that heavily involves the use of cryptography and that operates on a distributed ledger. Cryptocurrencies such as bitcoin and ether are examples. However, "crypto-assets" is a broad term that can also include other assets that exist and can exchange hands on a distributed ledger.

Decentralized atomic cross-chain swap:
A financial arrangement that enables trading digital assets across different blockchains without using an intermediary party, such as an exchange service.

Digital currency:
Typically used to refer to currency that exists in electronic form and that may or may not be available in physical form. Digital currencies often have some characteristics of a currency, namely serving as a store of value, unit of account or medium of exchange, although the term may also be used more liberally. They may also have characteristics of a commodity or other asset.

Digital identity (ID):
A set of digital credentials used to represent and prove the identity of a real-world individual, organization or electronic device on electronic or online systems, and their right to access, for example, certain information and services. Today, these typically take the form of digital certificates created using public-key cryptography to bind together a public-key with identity details and other details, such as a private key and the owner's digital ID.

Digital token:
A unit on a digital and typically decentralized ledger that is used to represent value, such as an asset or a basket of assets, including real-world assets such as commodities, stock or real-estate property. The token can be used to facilitate transactions and transfers of title to such underlying value or asset.

Digital wallet:
A digital device, software-based system or online application for storing payment information such passwords and private keys, which when used in conjunction with a payment system can enable online payments. When they involve cryptocurrency, digital wallets are also used as a mechanism to store private key information for users to access their cryptocurrencies.

Distributed ledger technology (DLT):
An overarching term that includes blockchain technologies and refers to the protocols and supporting infrastructure that allow computers in different locations to propose and validate transactions on a ledger and update ledger records in a synchronized way across a network. Many DLTs are designed to function without a centralized trusted authority, relying instead on distributed consensus-based validation procedures combined with cryptographic signatures.

Delivery versus payment (DvP):
A settlement mechanism that ensures that the final transfer of an asset, namely an investment security, occurs only if the final transfer of payment for the asset takes place. DvP transfers can occur within a jurisdiction or across borders.

E-money:
Short for "electronic money", e-money is stored value held in digital accounts or physical devices (e.g. a chip card or a hard drive in a personal computer) that is used as a means of payment and a store of value. E-money systems vary across different jurisdictions, but they are often fully backed by fiat currency, denominated in the same currency as central bank or commercial bank money and exchangeable at par value for such money or redeemable in cash.

Fiat currency:
A form of currency established by government decree and generally issued by a monetary authority such as a central bank. Fiat currencies can be distinguished from other historic forms of government-issued money by typically not being backed by a commodity such as gold or silver. Fiat currency can take the form of physically issued bank notes and cash or it can be represented electronically, such as with bank credit, central bank reserves or central bank digital currency (CBDC).

Financial inclusion:
The ability of individuals and businesses to access useful and affordable financial products and services that meet their needs, such as payment, savings, credit and insurance services, considering a variety of factors impacting that access, such as affordability, access to appropriate technology, education and literacy, geographic accessibility and financial infrastructure.

Know Your Customer (KYC):
Processes and protocols, usually prescribed by law, that apply to certain accountable institutions, such as banks, obliging them to verify and keep records of the identities of their customers in line with strict global or national anti-money laundering, anti-terrorism and other laws and regulations.

Mobile money:
A broad category defined as a service in which the mobile phone is used to perform financial services.

Peer-to-peer (P2P):
Refers to interactions between peers in a system, such as transactions or information exchange, which occur without the need of an intermediary. In the blockchain industry, this has come to refer to systems that enable transfers of value without an intermediary bank, utilizing, for example, distributed ledger technology.

Privacy-enhancing technology (PET):
Technologies or systems that incorporate technical processes, methods or knowledge to achieve specific privacy or data protection functionality, or that implement specific requirements of data protection laws and reduce the risks associated with processing personally identifiable information, such as the risk of data breaches.

Privacy:
Within this series, privacy can be defined as the right of an individual to keep their information secret to themselves and to self-designated others, and free from access, intervention and interference. Such a right includes control over how one's personal information is collected and used.

Pseudonymous:
According to the definition in the GDPR, pseudonymity refers to personal data that can no longer be attributed to a specific data subject without the use of additional information.

Public Key Infrastructure (PKI):
The policies, procedures, software and hardware required to create, manage, distribute, use, store and revoke public and private key pairs and digital certificates that are used for encryption and other purposes. The public key can be openly shared to relevant parties without compromising security, while the private key must be kept confidential. Private keys are typically required to decrypt confidential information and messages. They can also be used to create a digital signature on a message or document. A digital signature is a mathematical scheme that demonstrates to the recipients that the message or document in question originated with the private key's owner and that there has not been forgery or tampering.

Payment versus payment (PvP):
A settlement mechanism that ensures that the final transfer of a payment in one currency occurs only if the final transfer of a payment in another currency or currencies takes place. PvP transfers can occur within a jurisdiction or across borders.

Retail CBDC:
A form of central bank digital currency (CBDC) that is accessible to the general public. Retail CBDCs may take a two-tiered structure, where citizens would hold CBDC balances with commercial banks or other customer-facing financial entities, such as private payment service providers, rather than directly with the central bank. A retail CBDC could be used both domestically and cross-border (i.e. accessible and usable by foreign entities). Retail CBDCs are sometimes also referred to as general purpose or universally available CBDCs.

RTGS:
Real-time gross settlement, which in the context of interbank settlement refers to systems for the continuous and real-time transmission of funds or securities individually on an order-by-order basis, without netting.

Smart contract:
Self-executing agreements that are triggered based on pre-defined and agreed conditions without manual intervention. A smart contract may or may not be related to or constitute a legal contract. The term is often used to refer to smart contracts deployed in decentralized, distributed blockchain networks.

Special drawing right (SDR):
A supplementary foreign exchange reserve asset created and maintained by the International Monetary Fund (IMF) to supplement its member countries' official reserves. An SDR is neither a currency nor a claim on the IMF, but rather a potential claim on the freely usable currencies of IMF members and exchangeable for those currencies.

Stablecoin:
A broad term used to refer to digital currencies, most often DLT-based cryptocurrencies, that are designed to maintain a stable value relative to another asset (typically a unit of sovereign currency or commodity) or a basket of assets. To achieve this, a stablecoin's value may, for example, be pegged to the value of a sovereign currency such as the US dollar, other crypto-assets or commodities, or supported by algorithms. Depending on the effectiveness of the stabilization mechanism and backing, the digital currency may or may not hold a stable value relative to its reference asset.

Synthetic CBDC:
Refers to an alternative framework to central bank digital currency (CBDC), under which private payment service providers hold reserves at the central bank that fully back the digital currency they issue to customers. The regulatory framework would intend to guarantee that these providers' liabilities will always be fully matched by funds at the central bank, creating protection for users against issuer default. Such liabilities could share some of the characteristics of a CBDC issued by the central bank, but they could not constitute CBDC, as the end-user would not hold a direct claim on the central bank. Synthetic CBDC is neither issued by nor a direct liability of the central bank. Synthetic CBDCs have been referred to as a form of "narrow-bank" money.

Unbanked:
Refers to adults or households who do not utilize the services of a bank or similar financial organization for transactions or in any other capacity. Often such persons or households would make use of alternatives, such as cash or pre-paid vouchers to pay for goods or services.

Underbanked:
Refers to persons or households that utilize the services of a bank or similar financial institution but rely to a larger extent on alternative financial services. Examples of such alternative financial services used by underbanked households include non-bank money orders, non-bank cheque-cashing services, non-bank remittances, payday loans, rent-to-own services, pawn shop loans, refund anticipation loans, or auto-title loans.

Wholesale CBDC:
A form of central bank digital currency (CBDC) that would be used among licensed banks and other financial institutions that typically hold reserve deposits with a central bank for interbank payments and securities transactions. Wholesale CBDC could be used both domestically and cross-border. Domestic wholesale CBDC is akin or equivalent to the reserve accounts commercial banks often hold with central banks today.

Endnotes

1. See:

   1) International Monetary Fund, *The Rise of Digital Money – A Strategic Plan To Continue Delivering On The IMF's Mandate*, July 2021, p. 4, https://www.imf.org/-/media/Files/Publications/PP/2021/English/PPEA2021054.ashx.

   2) Boar, Codruta and Wehrli, Andreas, *Ready, steady, go? - Results of the third BIS survey on central bank digital currency*, Bank for International Settlements, January 2021, https://www.bis.org/publ/bppdf/bispap114.htm.

2. In this white paper series, the term "blockchain technology" is used generally to refer to blockchain and distributed-ledger technology. See the Glossary for a more precise definition of each. Additionally, from a technical perspective, stablecoins may operate on technology that ranges in its degree of decentralization. The major stablecoins today operate on public, permissionless blockchains, such as the Ethereum network with thousands of nodes validating transactions. However, stablecoins can also operate with ledgers that are more centralized. The most famous example is the Diem (formerly Libra) stablecoin conception, which plans to operate on private, permissioned blockchains with fewer nodes. See: "White Paper v2.0", *Diem*, 2020, https://www.diem.com/en-us/white-paper/.

3. World Economic Forum, *Digital Currency Governance Consortium: Vision for 2021 Deliverables*, 2021, http://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_2021.pdf.

4. World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, 2020, http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf.

5. See:

   1) White, Kathryn, et al., "Key takeaways on digital currency from The Davos Agenda", *World Economic Forum*, 5 February 2021, https://www.weforum.org/agenda/2021/02/key-takeaways-on-digital-currency-from-the-davos-agenda/.

   2) World Economic Forum, *Global Technology Governance Summit*, Virtual, 2021. https://www.weforum.org/events/global-technology-governance-summit-2021.

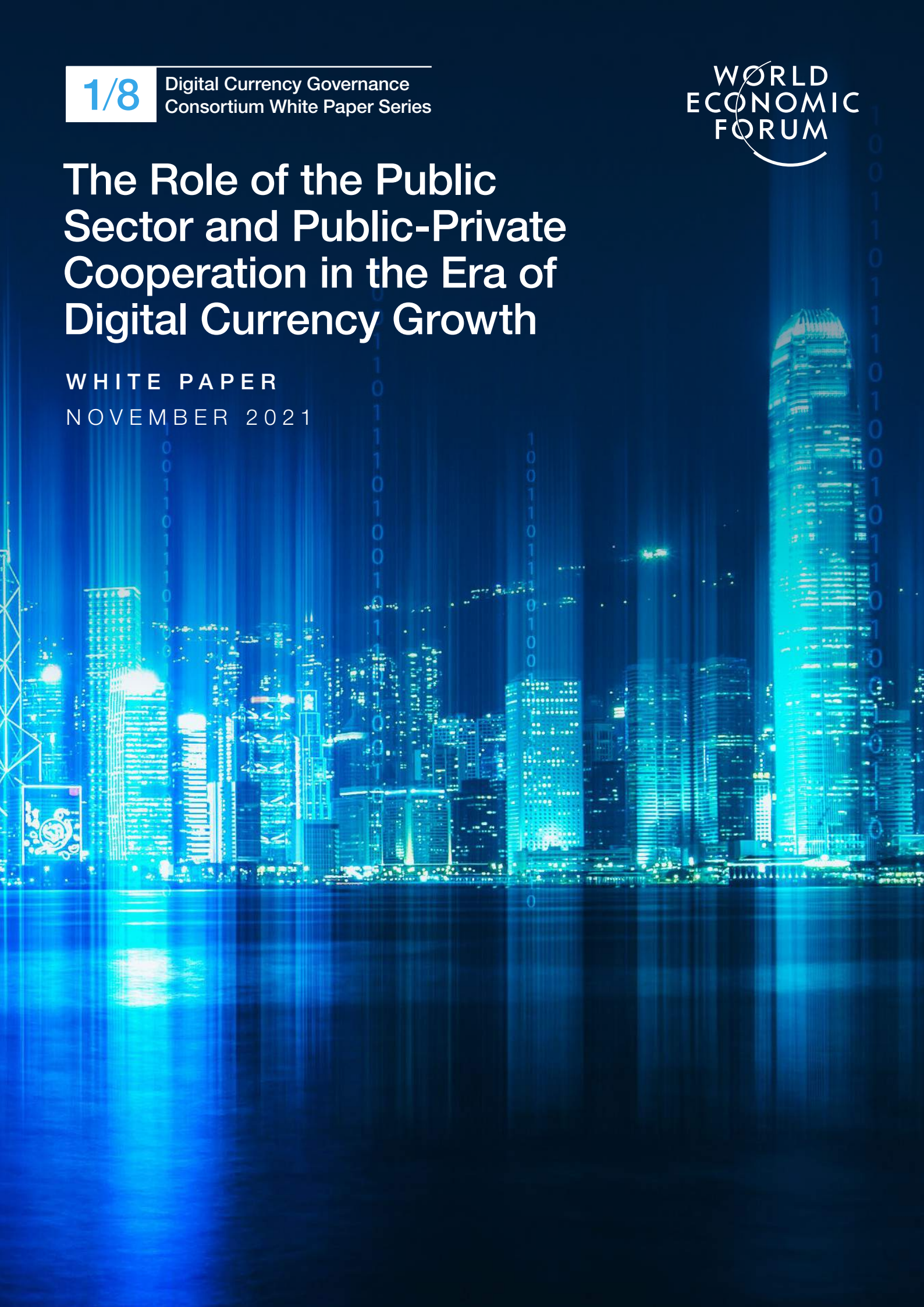
1/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

Preface 17

1 Public sector mandates for CBDC and stablecoin governance 18

2 Public sector roles 20

- 2.1 Public sector and stablecoins 21
- 2.2 Public sector and CBDC 23

3 Areas for public-private cooperation 26

- 3.1 Public-private cooperation on stablecoins 27
- 3.2 Public-private cooperation on CBDC 28

4 Areas for intergovernmental collaboration 32

- 4.1 Prevention of illicit activity 33
- 4.2 Consumer protection, data privacy and data management 33
- 4.3 Technical interoperability and coordination over cross-border and multilateral CBDC arrangements 34
- 4.4 Cross-border CBDC macroeconomic spillover effects and risks 35

Conclusion 37

Endnotes 38

Preface

This paper explores potential roles that central banks and public institutions could take with respect to stablecoins and CBDCs. It also highlights key opportunities for public-private and intergovernmental cooperation.

Public sector institutions globally have been increasingly called upon to take actions, develop perspectives and maintain oversight of emerging forms of digital currency. This paper highlights the most important roles and actions that the public sector can engage in with respect to two forms of digital currency: central bank digital currency (CBDC) and stablecoins. It aims to serve as a starting point, highlighting sets of actions available to policy-makers.

While CBDC and stablecoins should be considered distinctly, as they are very different forms of digital currency, their respective treatment by the public sector can be interconnected. For instance, CBDC may be issued to stimulate competition in the payment markets (including among stablecoin providers) or mitigate currency substitution risk from a widely adopted global stablecoin (or foreign CBDC). Or a government may mandate that dominant stablecoin-providers or private payment service-providers (PSP) should fully back customer holdings with reserves held at the central bank (a concept referred to as "synthetic CBDC" in this paper) – in which case, policy-makers may find less need to issue CBDC for payment stability purposes.[1]

This report seeks to help public sector institutions identify the roles they should play to support the kind of responsible innovation in stablecoins or CBDC that protects citizens and the financial system from risks, while allowing for beneficial technological advances. It is rooted in the mandates the public sector bears. Notably, it highlights the most important areas of public-private cooperation, based on the assumption that the private sector is well-placed to offer innovative technical solutions. It also highlights key areas for intergovernmental cooperation. It assumes that each country has distinct policy goals and political-economy constraints that inform their actions (or inactions) towards CBDC or stablecoins.

The paper identifies a range of roles, activities and opportunities which are not necessarily either independent or mutually exclusive. Policy-makers and the private sector can engage in multiple actions related to stablecoins or CBDC at the same time, and these efforts can be symbiotic depending on priorities and goals. In some cases, they may find these actions to be unnecessary, given a jurisdiction's particular interests and conditions.

1 Public sector mandates for CBDC and stablecoin governance

Central banks, finance ministries and regulatory or oversight bodies have multiple mandates that relate to stablecoins and CBDC, both directly and indirectly. Generally, central banks are tasked to maintain certain levels of employment and price stability using monetary policy. Their purview often extends to areas related to the oversight and management of monetary, financial and payment systems. In the words of the European Central Bank (ECB): "By pursuing its tasks of maintaining monetary and financial stability and the smooth operation of payment systems, [the ECB] ensures that money and payments serve European society. We have always been committed to maintaining confidence in our currency, which has meant adapting the form of money and payment services we provide to the changing ways in which people spend, save and invest."[2]

In a speech in August 2020, US Federal Reserve Governor Lael Brainard expanded on this concept: "The introduction of Bitcoin and the subsequent emergence of stablecoins with potentially global reach, such as Facebook's Libra [now Diem], have raised fundamental questions about legal and regulatory safeguards, financial stability, and the role of currency in society. This prospect has intensified calls for CBDCs to maintain the sovereign currency as the anchor of the nation's payment systems."[3]

Regulatory and oversight bodies, meanwhile, have mandates that apply more directly to private stablecoin initiatives. For example, the US Securities and Exchange Commission (SEC) is charged with protecting investors, maintaining fair, orderly and efficient markets, and facilitating market integrity and capital formation. Looking at Europe, the European Securities and Markets Authority (ESMA) is responsible for "enhancing the protection of investors and promoting stable and orderly financial markets."[4]

Table 1 presents a summary of common mandates for public sector financial institutions and oversight bodies. These mandates inform the potential appropriate roles of various institutions with respect to CBDC and stablecoin governance.

> **"The emergence of stablecoins with potentially global reach has raised fundamental questions about legal and regulatory safeguards, financial stability, and the role of currency in society.**
>
> US Federal Reserve Governor Lael Brainard

TABLE 1 | **Mandates for public sector financial institutions**

Consumer protection	Consumer protection in the financial space generally falls to a country's financial regulator. For example, in Australia, the Australian Securities and Investments Commission (ASIC) regulates "corporate, markets, financial services and consumer credit…It also licenses and regulates individuals and businesses that engage in consumer credit activities. In addition, ASIC's market regulation role makes it responsible for supervising financial market operators and participants, including real-time trading on Australia's domestic licensed markets."[5]
Financial stability	Financial stability is a goal shared across many government bodies. Those institutions that touch the financial sector often have a mandate to maintain financial stability. For example, the Financial Stability Oversight Council (FSOC) is a collaborative body chaired by the US Treasury Secretary that creates "collective accountability for identifying risks and responding to emerging threats to financial stability."[6] It is made up of representatives from the Federal Reserve, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, Securities and Exchange Commission, Federal Deposit Insurance Corporation, Commodity Futures Trading Commission, Federal Housing Finance Agency and National Credit Union Administration.
Monetary stability	Central banks commonly adhere to core mandates centred on price stability, often in tandem with mandates related to high employment. As expressed by the Swiss National Bank (SNB), "Article 99 of the Federal Constitution entrusts the SNB, as an independent central bank, with the conduct of monetary policy in the interests of the country as a whole. The mandate is explained in detail in the National Bank Act (art. 5 para. 1), which requires the SNB to ensure price stability and, in so doing, to take due account of economic developments."[7]
Competitive markets	Most countries have opted to create governmental bodies solely responsible for maintaining competition. For example, Canada has its Competition Bureau, "an independent law enforcement agency, [which] ensures that Canadian businesses and consumers prosper in a competitive and innovative marketplace."[8] Finland has its competition and consumer protection authority in one body: the Finnish Competition and Consumer Authority. The US relies on the Federal Trade Commission and the US Department of Justice's Antitrust Division.
Market integrity	Market integrity is a broad mandate that falls under the remit of numerous regulators. In the context of regulation, it is generally understood to mean the elimination of market abuse activities, creation of non-discriminatory access to the market, transparent and accurate information about the prices of securities and accurate information about issuers of securities.[9]
Prevention of illicit activity	Countries regulate their financial and professional sectors for anti-money laundering and combating the financing of terrorism (AML/CFT) based on the Financial Action Task Force (FATF) Recommendations. These include requirements for financial institutions to apply risk-based preventive measures against money laundering and terrorist financing (e.g. customer due diligence/KYC, sanctions screening and reporting suspicious transactions to authorities). These actions need to be supported by supervising compliance with these obligations and building law enforcement capacity to investigate suspected illicit activity. The FATF Recommendations were amended in 2019 to explicitly require regulation of digital currencies and those providing digital currency services; the guidance was updated in October 2021, specifying how FATF standards apply to stablecoins and definitions for virtual assets, among other issues.[10]

2 Public sector roles

As a first step, the public sector has a responsibility to develop an understanding and awareness of relevant global trends and issues with respect to stablecoins and CBDC. Beyond this, some major roles that public sector institutions such as central banks, finance ministries and regulatory bodies could take with respect to stablecoins and CBDC are explored in this section. Actions under the stablecoins column are not mutually exclusive.

TABLE 2 **Major public sector roles and activities on stablecoins and CBDC**

Stablecoins	CBDC
Monitoring and regulation	Creation of CBDC
Actions that support innovation	Monitoring, research or experimentation
Granting central bank reserve access	Alternatives to CBDC issuance

2.1 Public sector and stablecoins

Monitoring and regulation

Regulatory bodies should carefully consider regulating stablecoins to preserve financial stability, support consumer protection and provide other safeguards to the public and to financial and monetary systems. Regulators should conduct a thorough review of the risks presented by stablecoins to their jurisdictions, alongside a review of existing laws and regulations. Special attention should be paid to the quality, liquidity and transparency of reserve assets backing stablecoins (see further discussion on digital "run risk" under the section Granting central bank reserve access below).[11] Critical attention should also be paid to the risk and prevention of illicit activity, such as money laundering, tax evasion and terrorist financing.

Regulators could identify policy and oversight gaps and inconsistencies with respect to stablecoins and seek to fill those. They could look to examples from other regions and consider the present and future risks stablecoins may present.[12] For instance, transparency, frequent disclosure and independent auditing requirements for stablecoin reserves and financial management could enhance the financial integrity of stablecoins and protect users. Left unchecked, widely held stablecoins with poor financial management could present significant risks to users as well as to financial systems. In extreme cases, policy-makers could even ban the use of stablecoins for certain activities, given the risks they may pose.

Regulators should, as far as possible, aim to develop policies that are "future-proof" and remain relevant as the technology and industry evolve. Policy flexibility and agility in the face of market developments would also be beneficial. Monitoring of stablecoin trends, risk areas and developments, as well as international regulatory developments involving stablecoins, are essential to inform policy-making and regulation.

When it comes to stablecoins and the use of blockchain, it is essential that regulatory frameworks are consistent across geographies to the greatest extent possible, as consistency can prevent mismatching regulatory frameworks that enable regulatory arbitrage and gaps. Consistency with existing regulation is also important and can be aligned with the principle – "same business, same risks, same rules".

For a detailed framework to identify regulatory and policy gaps and inconsistencies, please refer to the white paper in this report series entitled *Regulatory and Policy Gaps and Inconsistencies of Digital Currencies*. For recommendations with respect to consumer protection, please refer to the white paper entitled *Digital Currency Consumer Protection Risk Mapping*.

Actions that support innovation

Given the nascent nature of stablecoins and blockchain technology, many jurisdictions have opted to create regulatory "sandboxes" that allow companies to test offerings and innovate in a controlled environment with few regulatory requirements. Sandboxes have dual benefits. They allow companies to better understand how their services will work; and they allow regulators to better identify any gaps and problems in existing regulations and any new regulatory concerns that may arise. Examples of regulatory sandboxes with stablecoin or blockchain-related participants are widespread and include: the UK Financial Conduct Authority's (FCA) sandbox with several projects, such as a blockchain- based e-money platform;[13] the European Commission's pan-European blockchain regulatory sandbox;[14] a blockchain-based delivery-versus-payment (DvP) settlement system between the Japanese yen and crypto assets in Japan;[15] and tests in the Bank of Russia's regulatory sandbox.[16]

In another approach, the New York Department of Financial Services (NYDFS) hosted a regulatory TechSprint – essentially a government-sponsored "hackathon", where teams developed solutions to improve regulatory reporting for virtual currency companies.[17] These events allow regulators and innovators to interface and develop solutions to novel problems facing regulators.

Lastly, policy-makers might consider roles they can play in mandating or facilitating interoperability among stablecoins, to the extent it can support competitiveness and avoid network effects or closed-loop stablecoin systems that could lead to higher prices and lower convenience to users.

Granting central bank reserve access

A third, important type of public sector action relates to granting (or potentially requiring) stablecoin providers direct reserve access at the central bank. A synthetic CBDC constitutes a public-private partnership scheme where the stablecoin issuer (or other private issuer of digital money) fully backs reserves directly at the monetary authority or similar institution. The public sector can decide whether to allow or require this arrangement. A similar arrangement with less public sector involvement could require the stablecoin issuer to hold reserves with a commercial bank in a manner that is remote from bankruptcy of the bank and fully backed by reserves with the central bank (rather than partially backed as would be standard deposits).

These approaches involve multiple complexities that should be carefully considered. That said, they can be an important step in reducing the risk of a run on stablecoin reserves – where users lose confidence in the ability to redeem their stablecoins for physical cash or bank deposits, given problems at the stablecoin issuer or general market volatility, and redeem their stablecoins *en masse*. The risk of a run on some stablecoins remains a concern today, where a few have rapidly amassed billions of dollars of customer deposits without necessarily adhering to comprehensive regulatory requirements and oversight of typical deposit-taking institutions, or providing adequate transparency or guarantees as to the quality, liquidity and redeemability of reserve assets.[18]

These schemes could serve as complements to regulation in managing risks associated with stablecoins. Full-reserve backing with a central bank (either directly at the central bank as with synthetic CBDC or in bankruptcy-remote accounts with a commercial bank as intermediary) would improve consumer protection and the stablecoin's financial integrity. Users could have a first claim on the provider's reserves or other assets in the event of its insolvency. It is important to note that the stablecoin digital currency would remain an ultimate liability of the issuer and not the central bank; it would therefore not be considered a CBDC by definition. Researchers at the International Monetary Fund (IMF), European Central Bank and World Economic Forum have written further on this subject of synthetic CBDC.[19]

TABLE 3 **Key considerations for "synthetic CBDC" and stablecoin direct reserve access[20]**

Identification of programme goals and motivations	– Clear identification of goals, concerns or risks related to stablecoins present in the economy that could be meaningfully addressed through allowing or requiring fully backed reserves directly at the central bank. – Clear identification of the types of issuers who would or would not qualify for reserve access.
Consumer protection and risk management considerations	– Specification of reserve policies, legal structures and protections for user funds in case of issuer insolvency. – Oversight regimes, auditing, cybersecurity protections and other requirements for stablecoin issuers to ensure stability and meet the goals and objectives of the programme.
Legal considerations	– Pre-existing statutory or policy constraints that might prevent the central bank from allowing reserve access to non-bank institutions. – Appropriate regulatory and compliance policies, including KYC/AML/CFT capabilities.
Issues related to monetary policy	– Examination of monetary impacts, including with respect to effects on the central bank balance sheet, seigniorage[21] and commercial banks (who could compete for deposits and become disintermediated). – Consideration of how the central bank reserve rate will affect the digital currency issuer (a negative reserve rate could be passed on to the issuer or users).

"The risk of a run on some stablecoins remains a concern today, where a few have rapidly amassed billions of dollars of customer deposits without necessarily adhering to comprehensive regulatory requirements

2.2 Public sector and CBDC

Creation of CBDC

Central banks and national policy-makers can decide whether to create a CBDC and, if so, in what form and with what private sector role. For example, should PSPs or commercial banks play an intermediary role providing custody and other services related to CBDC assets (referred to in this paper as a "two-tiered CBDC")? Or should end-users hold accounts with the central bank directly?

CBDC issuance should stem from a rigorous evaluation of the policy objectives or goals that the CBDC could support, and the capabilities and opportunities that it could enable. These should be closely weighed alongside alternative methods of achieving those goals or opportunities, and the downsides and risks arising from the CBDC. Multi-stakeholder input and public consultations on potential CBDC issuance are very important and are likely to critically inform CBDC design and eventual adoption.[22] If the benefits from the envisaged CBDC do not outweigh the risks and downsides, then the CBDC should not be created, although policy-makers may wish to continue research and observation of related work around the world in case their position changes.

The policy goals that CBDC can support include the following:

- Mitigating currency substitution risk
- Payment system safety and resilience
- Financial inclusion
- Domestic or cross-border payment efficiency
- Monetary policy implementation
- Payment and banking system competitiveness
- Continued access to central bank money for the general public
- Household fiscal transfers

For further discussion, see the whitepaper in this report series entitled *CBDC Technology Considerations*.

Different forms of CBDC are outlined in Figure 1.

FIGURE 1 | **Different forms of CBDC[23]**

	Domestic	Cross-border
Retail	Financial and non-financial users could hold accounts of digitized central bank money	Foreign financial and 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

Several technical design choices are available for CBDC. Policy-makers must consider these, along with foreign access. For example, would CBDC be available to foreign entities and, if so, which types (e.g. tourists and foreign visitors, or overseas firms)?[24] As part of this decision, policy-makers should evaluate whether providing foreign access contributes to any policy goals or institutional mandates. They should robustly analyse the risks and complexities related to cross-border access, including exchange rate volatility, implications for domestic monetary policy, financial stability, the central bank balance sheet, or risks related to illicit fund flows. Negative consequences to overseas economies, such as those stemming from capital flight or loss of monetary control should also be considered and are discussed later in this paper (see Table 7).

Additional questions to address before creating a CBDC include: will there be any restrictions or additional requirements for certain types of domestic or overseas entities? For example, higher identification requirements, or varying levels of access to certain types of international financial or non-financial entities.

If policy-makers decide to issue a CBDC, next steps include important choices for design, technology infrastructure, governance and implementation strategy. The World Economic Forum's *Central Bank Digital Currency Policy-Maker Toolkit* provides a framework to guide policy-makers in the CBDC decision-making process.[25] *The CBDC Pyramid* presented by researchers from the Bank for International Settlements (BIS) provides a valuable model for identifying a CBDC's technical design and architecture, including the role of the private sector.[26] Initiatives and research such as the UK's CBDC Taskforce, the Riksbank's e-krona efforts or the BIS report *Central bank digital currencies: Foundational principles and core features* can also inform approaches and design for CBDC creation.[27]

Monitoring, research or experimentation

The central bank may decide not to move directly towards CBDC development, instead monitoring CBDC developments around the world while staying abreast of and potentially contributing to research and technical experimentation. This allows it to stay up to date with the latest research, trends and findings related to CBDC, including those that can affect its economy. A flexible wait-and-see approach could be appropriate given the extensive impact (and reputational risk) that a new CBDC system could have on an economy, particularly a new, widely available retail CBDC. The central bank could also learn from work conducted in other countries without expending significant resources. If the value proposition of a CBDC in a given country becomes stronger over time, its policy-makers could change their stance towards use-cases and development.

Policy-makers can follow ongoing CBDC research through:

- Accessing online resources that compile and share research publicly[28]
- Attending international meetings, discussions and working groups related to CBDC
- Engaging with international organizations such as the IMF, BIS or World Economic Forum
- Developing bilateral relationships with CBDC research teams around the world

Before taking a wait-and-see approach, any first-mover advantages pertaining to CBDC issuance could be evaluated. One example of a potential first-mover advantage could be the setting of data or software standards for use in cross-border CBDC arrangements in the future. That said, such activity may not be that valuable for central banks. On balance, it is likely to prove more harmful than beneficial to create CBDC too quickly. Policy-makers should also monitor for risks to their jurisdictions posed by foreign CBDC, discussed in more detail in section 4.4 below.

“ It is likely to prove more harmful than beneficial to create CBDC too quickly

Alternatives to CBDC issuance

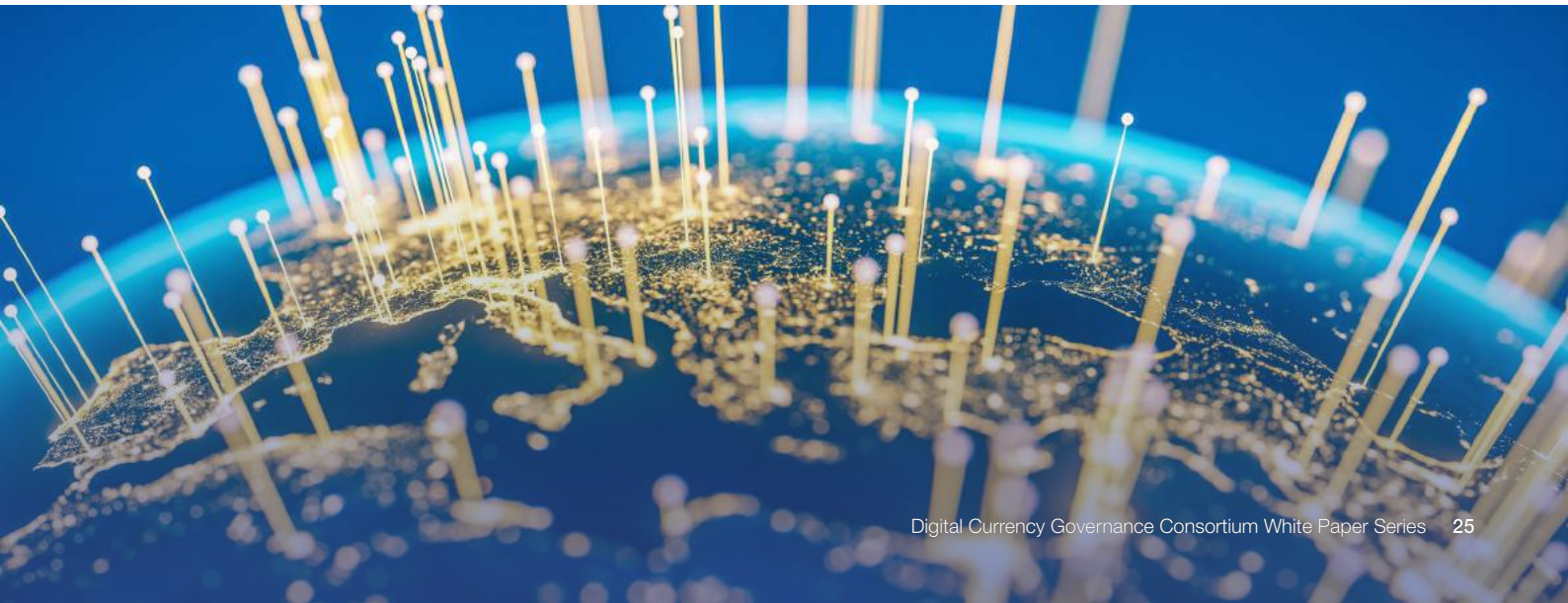
If relevant public sector institutions have reviewed the CBDC concept and determined that issuing a CBDC would not provide value to their citizens or the economy, or that resourcing is too constrained to design and develop a CBDC in the near or intermediate term, they may choose inaction towards CBDC. As with the approach of monitoring and researching CBDC projects described below, they may re-engage with the CBDC concept at any point in the future, learning from the work conducted until that point.

Although around 85% of central banks are engaging in CBDC research and development in some manner according to the BIS, very few economies (and no major developed economies as of the time of writing) have definitively concluded to develop or issue a CBDC.[29] Considering the risks of CBDC and the few cogent arguments for a first-mover advantage, central banks should not feel pressured to develop or experiment with CBDC if the case for their presence in the economy is not yet compelling.

There are numerous potential alternative solutions to meet the same policy goals that CBDC can provide and it may be the case that CBDC does not have a strong value proposition for various economies. Table 4 presents a non-exhaustive set of alternative solutions to various common CBDC policy goals.

TABLE 4 **Alternative public sector-led solutions to meet CBDC policy goals**

To address financial inclusion	– Financial and digital literacy and education programmes.[30] – Providing a monetary incentive for citizens to open and use a private financial account.
To stimulate competition in payment or deposit markets	– Regulation of PSPs, stablecoin issuers, cryptocurrency issuers, foreign CBDC, the banking sector, other financial organizations or digital currencies in question. For instance, dominant payment platforms or stablecoin providers may follow heightened regulations or hold reserves in the central bank in a partial or fully backed manner. Similarly, a country may decide to ban the use of a certain digital currency. – Additional antitrust and pro-competition policies.
To improve efficiency and reduce cost of payment services	– Legislation such as caps on retail transaction or credit card fees, limits to minimum account balances, or the establishment of open-banking and data-sharing requirements. – The development of a domestic “fast payments” retail system. – For international payments – bilateral or multi-lateral efforts, such as those connecting the fast payment systems of multiple countries.[31] – Creation of technical standards that can enhance interoperability for payment providers at both the application and the transaction-settlement layers.
For payment stability and resilience	– Investment in technical resilience of new or pre-existing domestic payment and settlement systems.



3 Areas for public-private cooperation

> **The question is where do you draw the line of what the public sector does and what the private sector does. The fundamental question is about issuing. Does the public sector issue and the private distribute or do we also allow the private sector to issue?**
>
> Tommaso Mancini-Griffoli, International Monetary Fund[32]

Public-private partnerships and cooperation in finance and industry are not new. Respecting local governments and laws, each jurisdiction must make its own decisions about how the public sector should cooperate with the private sector with respect to digital currency innovation and growth. Moreover, responses and approaches to public-private innovation may differ between developed economies, where banks and traditional financial institutions are well established, and emerging economies, where banking systems may be less established yet fintech ecosystems are strong.

Notwithstanding this, the expertise and core competencies of the private sector in technology innovation, user growth and adoption, customer service and other areas should be considered and valued. Often, the public sector cannot match the scale and pace of private industry research and development. Cooperation can enable government and public sector bodies to keep up with and benefit from private sector innovation.

Failure by the public sector to cooperate with the private sector and leverage its expertise where relevant can lead to deficiencies in some areas of technical expertise, unnecessary effort or reinventing the wheel, an inability for a public sector solution such as CBDC to connect with private sector financial services and tools, regulatory and policy gaps, and broader unintended negative consequences to the payments industry and financial services.

TABLE 5 **Areas for public-private cooperation**

Stablecoins	CBDC
Regulatory consultation	Consultations on CBDC
Innovation hubs, regulatory sandboxes and joint efforts	Sharing of knowledge and expertise from the private sector
	Joint piloting and experimentation
Synthetic CBDC development (central bank reserve access)	Two-tiered retail CBDC development
Prevention of illicit activity	Efforts supporting merchant acceptance and interoperability with private payment systems

3.1 Public-private cooperation on stablecoins

Regulatory consultation

The public sector can solicit feedback on the regulatory treatment of stablecoins from the private sector (as well as from civil society organizations, public citizens and other stakeholders). Consultations allow the public sector to gain perspectives and ideas on innovations and tactics, and to learn about any unintended consequences or externalities about a regulatory proposal. Recent examples include the crypto-assets consultation by the UK Treasury,[33] the consultations conducted by the European Commission regarding the Markets in Crypto-Assets Regulation (MiCA) effort,[34] and the recent Financial Action Task Force (FATF) consultation on stablecoin guidance.[35]

Given the complexity and novelty of stablecoins, the private sector and other relevant organizations can help regulators understand the nature of business activities more quickly and clearly, clarify relevant risks, and provide suggestions in the process of formulating and revising rules. Stablecoin issuers should strive to be as transparent and cooperative as possible in their financial and technical operations.

Innovation hubs, regulatory sandboxes and joint efforts

As discussed earlier, the public sector can cooperate with the private sector to design and implement appropriate and valuable regulatory sandboxes, innovation hubs, hackathons or other efforts that can support innovation and small-scale testing. It may also identify other formats in which to work with the private sector in supporting innovation and experimentation. The public sector may participate in initiatives started or led by the private sector. For instance, Temasek, Singapore's state-owned investment company, joined the Libra Association (now the Diem Association) in May 2020.[36]

Synthetic CBDC development (central bank reserve access)

As discussed, if a stablecoin has gained significant adoption, then that jurisdiction may want to take steps to counter the risks posed by the dominant stablecoin system and require that it fully back its reserves directly with the central bank (synthetic CBDC).[37] Undoubtedly, the stablecoin issuer would play important roles in this scheme, including but not limited to its pre-existing functions of customer screening and due diligence, user data management, user interface and experience, software development and integration, customer service, wallet development and cybersecurity.[38] Meanwhile, the central bank would perform transaction settlements along with creating the necessary compliance and regulatory guidelines.

Prevention of illicit activity

Public-private fora for sharing information on illicit finance risks and issues related to stablecoins could be constructive to address the risks identified by major regulatory and oversight bodies. As an example of such an effort related to cryptocurrency more broadly, the US Treasury Department's FinCEN has established a virtual currency information-sharing initiative with participation from the private sector including virtual currency money transmitters.[39]

3.2 Public-private cooperation on CBDC

Consultations on CBDC

CBDC can have substantial impacts on the economy and society, including on commercial banks, credit card networks and PSPs. The central bank should consult with these and other relevant parties (including civil society organizations, citizens and other stakeholders) to gather information on innovation strategies as well as risks and unintended consequences to these parties. Thorough and ongoing industry consultation should be a cornerstone of CBDC development.

Consultation and engagement can occur through documents published online, seminars, roundtable events, advisory groups and training sessions, among other avenues. The Bank of Thailand, the Bank of England and the ECB's consultations and external working groups on potential CBDC issuance serve as recent examples.[40] Moreover, the EU Outreach sessions are an example of open sessions where participants can discuss key issues with public sector officials in real time.[41]

Sharing of knowledge and expertise from the private sector

The public sector can benefit widely from the knowledge, experience and expertise of the private sector with respect to elements of digital currency that can help a CBDC achieve its intended goals, gain adoption, and operate safely and securely. Examples of expertise the private sector can share with the public sector include:

- Consumer education and adoption strategies
- End-user UI/UX for CBDC accessibility and usability
- Customer service and account management
- Customer data management and privacy
- Cybersecurity, technical resilience and risk management
- Fraud and illicit activity detection

Hackathons can be used to learn best practices and expertise from the private sector and other ecosystem participants. The BIS Innovation Hub and SWIFT's ISO 20022 and API hackathon is one example.[42] Another is the Global CBDC Challenge, led by the Monetary Authority of Singapore (MAS), where private-sector providers are invited to submit innovative solutions to specific technology challenges related to CBDC.[43]

Hackathons can be used to learn best practices and expertise from the private sector and other ecosystem participants

Joint piloting and experimentation

Central banks have been conducting joint CBDC experimentation with private sector entities, most commonly commercial banks or securities exchanges, for the past few years. Examples include the Bank of Canada's Project Jasper,[44] the National Bank of Cambodia's Project Bakong,[45] the Hong Kong Monetary Authority and Bank of Thailand's Project Inthanon-LionRock,[46] and the BIS and Swiss Digital Exchange's Project Helvetia.[47] In other examples, the central bank can be an observer to experimentation among private sector organizations, as seen with the Bank of Spain and five commercial banks experimenting with a blockchain-based platform for SEPA Instant Credit Transfer payments.[48]

Joint experimentation with relevant parties can enable CBDC testing in a manner that is more realistic and can more widely explore CBDC opportunities and functionalities that leverage the private sector. The central bank could lead working groups with retail banks and other businesses during project design, execution and testing.

Two-tiered retail CBDC development

In a two-tiered retail CBDC implementation, customers hold CBDC accounts with commercial banks or other private-sector financial organizations. The central bank issues CBDC to the financial intermediary who distributes it to citizens and other entities. The private sector organization serves as the user-facing intermediary, conducting and leveraging pre-existing expertise in customer due diligence and compliance processes, customer service and account management, IT security and other processes. The two-tiered model alleviates the burden on the central bank to perform these activities. CBDC remains a claim on the central bank. The exact structure of two-tiered CBDC can vary, but models could include the intermediary holding fully backed reserves at the central bank corresponding to customer CBDC deposits, or dedicated customer-specific balances within the intermediary's central bank reserve accounts.

Central banks who wish to implement two-tiered CBDC must decide the roles and responsibilities they and the private sector will conduct, to benefit from each other's core competencies and complementary capabilities. Adequate regulation and supervision are imperative for any intermediaries distributing CBDC. Intermediaries acting as PSPs may need to abide by existing payment services regulations related to security, transparency, data access, consumer protection and more.

Central bank and private sector participants can collaborate on the development and implementation of appropriate consumer protection standards, and where necessary identify clear allocations of liabilities between parties (for example in the event of fraudulent behaviour). A two-tiered CBDC should protect consumers' interests and give them the confidence necessary for in-person and online transactions. It should also ensure that consumers understand those protections and how they may differ from those offered by other payment methods.

The private sector may contribute more generally to public awareness-building and capacity development with the use of the CBDC. This might include informational and educational communications or campaigns. Such efforts can support the inclusion of the broader public in the CBDC programme, helping achieve financial inclusion goals and universal access.

The development and ongoing operation of a two-tier CBDC may require private sector participants to undertake a range of costly activities, including the development of intuitive user experiences, integration with new payment infrastructure and the enablement of various links in the payment value chain. Policy-makers may need to consider how best to balance costs and incentivization for the private sector. To ensure a vibrant and competitive ecosystem of payment innovators, the public and private sectors may need to establish a system of incentives that enables private sector participants to generate an appropriate return on their investments.

Efforts supporting merchant acceptance and interoperability with private payment systems

The public and private sectors should cooperate to ensure that a newly created CBDC can interact with private sector payment systems, so that its value to users is maximized and to avoid fragmented or closed-loop systems. Interoperability both among CBDC wallets provided by different financial organizations (e.g. two-tiered CBDC) and between CBDC and other payment and deposit facilities is likely to be necessary. While the central bank may establish and enforce technology and data standards supporting such interoperability, consultation with the private sector can inform standards and other requirements and help ensure fairness for private sector players engaging with CBDC.

Moreover, enabling integration with pre-existing payment messaging systems would allow consumers and businesses the freedom to choose whether to settle a given obligation using funds from their CBDC account or commercial bank account. Ensuring interoperability across different value storage accounts and payment systems will facilitate user satisfaction and economic efficiency and is likely to reinforce the role of central bank money at the heart of the economy. Achieving maximum interoperability is a challenging task, particularly in advanced economies where the banking and payment ecosystems are highly complex and developed. Active public-private collaboration will be critical to achieving this goal.

Merchant CBDC acceptance is another important issue. How will the infrastructure around the CBDC ensure that consumers can safely and conveniently use their holdings of CBDC funds to pay, in person or online, at a wide variety of merchants? Enabling acceptance points is one of the greatest challenges to driving mass adoption of any new payment solution. One approach to accelerating the acceptance of a CBDC could be to collaborate with existing acceptance networks, such as those provided by global card networks, domestic debit schemes, and a growing range of QR and “pay by account” solutions.

Interoperability with existing payment solutions would help ensure wide acceptance at the point of sale. This suggests that the public and private sectors should also work together to understand where existing payments infrastructure, such as real-time payment and automated clearing house (ACH) systems, might be leveraged to support the deployment of a CBDC, or where the policy objectives of the CBDC demand the development of new infrastructure. If a CBDC network is designed with the principles of open architecture, open connectivity and interoperability, it would support ease of integration across payment networks towards more seamless and end-to-end transaction processing. In this process, the participation and contribution of private institutions is likely to be essential. For in-depth discussions of interoperability, refer to the white paper in this report series entitled *Defining Interoperability*.

> Enabling acceptance points is one of the greatest challenges to driving mass adoption of any new payment solution

Additional recommendations

The following is a set of additional considerations and recommendations for public-private engagement with respect to CBDC and stablecoins.

Best practices and key considerations for public-private collaboration

As the public and private sectors collaborate to build and deploy CBDCs, developing and following best practice guidelines will help enable secure, robust and scalable solutions. Key considerations to consider include the following:

- A clear list of priorities and problems to cooperate on and solve
- Consideration of learnings, frameworks or best practices from historic cooperation in the financial sector and other industries
- Avoiding vendor lock-in or entrenchment in early technology developments
- Developing a private sector partner list that is diverse and extends beyond usual partners, and implementation of public, transparent, competitive and fair RFP processes
- Implementation of a thorough due diligence process to assess the quality and qualifications of private-sector providers or other options
- Advisory committee including private-sector representatives
- Periodic and potentially independent review and audit of private sector systems that closely relate to the CBDC
- Development of governance processes for system changes, upgrades and modifications as they relate to private sector involvement

Potential for privately created payment rails for CBDC

It is possible for the public sector to implement CBDC using payment infrastructure or databases and ledgers developed within the private sector. Several blockchain technology providers have developed permissioned or private blockchain ledgers or software frameworks that have been used extensively in experimentation. These include R3 Corda, Hyperledger Fabric and Quorum (originally developed within JP Morgan). Mostly found in wholesale CBDC experiments, these three platforms have demonstrated their ability to meet the requirements of financial infrastructure in terms of performance and reliability, although their performance in substantial full-scale deployments is not yet tested.

Performance relative to other pre-existing technology options must also be more fully investigated. Given the need for prudence with CBDC deployment and the complexity and newness of blockchain technology, the full set of risks and limitations of blockchain-based infrastructure must be strongly considered before it is employed in CBDC. For additional discussion on this topic, refer to the white paper in this report series entitled *CBDC Technology Considerations*.

Potential for privately created digital assets to facilitate CBDC

Existing private sector blockchain-based digital assets could potentially assist in the facilitation of cross-border wholesale interbank CBDC payments and transactions. Examples include the utility settlement coin (USC) and XRP digital assets. Such assets may serve as a "bridge currency" in cross-border interbank payments.[49] Before experimenting with such digital assets, policy-makers should have a clear understanding of the value-add they could provide from economic and technical perspectives, considering both pre-existing or alternative solutions and limitations or downsides.

4 Areas for intergovernmental collaboration

Among the most pressing issues regarding CBDC and stablecoins are how best to prevent illicit activity and establish consumer protection and privacy measures

This section discusses the critical opportunities and areas for intergovernmental collaboration with respect to CBDC and stablecoins. Policy-makers should consider participation in global efforts such as the IMF and World Bank Group's 2018 Bali Fintech Agenda that highlights the value of international cooperation and information-sharing for fintech developments.[50] The work on cross-border payment efficiency by the G20 and BIS Committee on Payments and Market Infrastructure (CPMI) is also pertinent. In their publication *Enhancing cross-border payments: building blocks of a global roadmap*, the G20 and CPMI identify 19 building blocks for enhancing cross-border payments, premised on international cooperation. These include building block 18, which focuses on "fostering the soundness of global stablecoin arrangements" and building block 19, which addresses "factoring an international dimension into CBDC designs".[51]

The BIS has launched an innovation hub that provides extensive collaboration opportunities among global policy-makers, central banks and other public institutions. Some of its work involves private sector firms and technology start-ups. The 2021-2022 work programme, which includes multiple projects related to CBDC, can be found at the innovation hub's website.[52] Policy-makers should consider participating in these and other relevant efforts. The remainder of this paper expands on additional areas for intergovernmental collaboration that are critical with respect to CBDC and stablecoins.

TABLE 6 **Areas for intergovernmental collaboration on CBDC and stablecoins**

Prevention of illicit activity
Consumer protection, data privacy and data management
Technical interoperability and coordination over cross-border and multilateral CBDC arrangements
Cross-border CBDC macroeconomic spillover effects and risks

4.1 Prevention of illicit activity

One of the most pressing issues regarding CBDC and stablecoins is how best to apply, establish or enforce compliance measures to prevent money laundering, terrorist financing, tax evasion and other illicit activity. With respect to stablecoins, the Financial Action Task Force (FATF), Financial Stability Board (FSB), European Central Bank (ECB) and G7 have identified several risks and vulnerabilities to be considered.[53]

While CBDC is treated separately from stablecoins by some regulatory and oversight bodies, it can entail similar risks of illicit activity. The FATF treats stablecoins and CBDC separately (the former as a type of virtual asset and the latter as a type of digital fiat currency), but both are subject to AML/CFT standards.[54] Mandating specific identity requirements would support compliance goals, but would come at the cost of privacy and accessibility for CBDC users.[55] The ECB and other organizations have explored methods to compromise between compliance, privacy and access in a safe manner.[56] For a more in-depth discussion of privacy for CBDC, refer to the white paper in this report series entitled *Privacy and Confidentiality Options for Central Bank Digital Currency*.

Ultimately, continued collaboration by jurisdictions through bodies such as the BIS and the FSB on CBDC design and the development of consistent and comprehensive AML/CFT rules is essential to prevent harmful activity with stablecoins and CBDC issued in the future. Information and knowledge-sharing, from low-level transaction data that can highlight potentially illicit activity to information about forthcoming policy changes, can be hugely constructive.

The avoidance of "regulatory arbitrage" opportunities through the adequate coverage and compatibility of regulatory requirements is critical to limiting the possibilities for illicit activity. The FSB, the International Organization of Securities Commissions (IOSCO) and the Basel Committee of Banking Supervision are, among others, actively considering such risks and advising on possible responses. Multilateral adherence to the recommendations articulated by such bodies can help reduce the likelihood of regulatory gaps.

To ensure that standard-setting and oversight bodies are promoting measures that effectively protect against the stablecoin risks they seek to prevent, they should engage in robust public consultations that generate understanding of these assets. Close coordination among all jurisdictions – both within oversight organizations and in bilateral communications – is vital to protect against regulatory arbitrage. This is in the context not only of recommendations related to financial stability but also of proposals that address AML/CFT, data privacy, cyber security, and consumer and investor protection. These latter concerns, if left unchecked, could all have consequences for financial stability, as recognized in the FSB's October 2020 report, *Regulation, Supervision and Oversight of Global Stablecoin Arrangements – Final Report and High-Level Recommendations*.[57]

Additional information on intergovernmental coordination in the prevention of illicit activity with globally available digital currencies can also be found in focus area B ("Coordinate regulatory, supervisory and oversight frameworks") of the G20 and CPMI report, *Enhancing cross-border payments: building blocks of a global roadmap*.[58]

4.2 Consumer protection, data privacy and data management

There is always considerable debate around the privacy regime that should apply to cross-border transfers of data. Many of the same considerations apply to cross-border payments in CBDC, and the issue of consumer data privacy could prove a major area for future conflict in cross-border CBDC arrangements. Moreover, where CBDC or stablecoin transactions occur across borders, governments must establish appropriate practices for the sharing, owning or acquiring of end-user account data in order to ensure its security and privacy. While some data will need to be shared for the purposes of tax collection, regulation enforcement and curbing illicit transactions, policy-makers should coordinate globally to develop responsible data-sharing protocols that meet these needs, while respecting user data privacy, especially as data leaves a citizen's home country.

Additional information on this topic can be found in "Building Block 6: Reviewing the interaction between data frameworks and cross-border payments" in the aforementioned G20 and CPMI report, *Enhancing cross-border payments: building blocks of a global roadmap*.[59] The *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the Group of Thirty (G30) report, *Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead* can also be referenced.[60]

4.3 Technical interoperability and coordination over cross-border and multilateral CBDC arrangements

Many central banks and international bodies have emphasized the importance of CBDC interoperability in cross-border areas, should they decide to issue CBDC that is accessible to entities abroad. Advocates for this approach argue that it could significantly reduce the time, risks and costs associated with cross-border payments for business and individuals alike. Multilateral policy and technical coordination will be critical to ensuring cross-border CBDC interoperability, including as it relates to regulatory requirements, risk control measures, and data and other standards (existing standards such as ISO 20022 can be leveraged).[61]

Cross-border CBDC interoperability features in the joint work of the BIS with several central banks in their 2020 report *Central bank digital currencies: foundational principles and core features*. It is worth quoting part of this report in full below:

"...for CBDC systems, their additional functionalities and future designs may require these [payment messaging] standards to be enhanced and for central banks to work collaboratively in their development. Similarly, if CBDC systems are linked with supplementary systems and data services (e.g. digital identity repositories), then commensurate international standards may be required for seamless cross-border payments. New systems based on different technologies (e.g. token-based) may also present challenges." [62]

"Multi-CBDC" (mCBDC) arrangements are being considered and evoke renewed questions about the value of a multilateral currency instrument.[63] In February, the Hong Kong Monetary Authority (HKMA), the Bank of Thailand (BOT), the Central Bank of the United Arab Emirates (CBUAE) and the Digital Currency Institute of the People's Bank of China (PBC DCI) announced they would collaborate on a cross-border CBDC project, moving from Project Inthanon-LionRock to the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project.[64] Furthermore, in the March 2021 BIS report *Multi-CBDC arrangements and the future of cross-border payments*, the authors point out three conceptual approaches to cross-border CBDC interoperability, emphasizing the importance of international coordination for achieving each:

1. Enhancing compatibility of CBDCs
2. Linking multiple CBDC systems
3. Integrating multiple CBDCs in a single mCBDC system[65]

These multilateral CBDC arrangements demand significant cooperation and trust between central banks and the challenges in their implementation should not be underestimated. Issues that may need to be considered include:

- Status of CBDC as legal tender
- Provision of services in CBDC
- Custody, security and regulation of CBDC issued in one country and used in another
- Privacy regimes applied to cross-border CBDC
- Regulatory clarity related to the potential use of distributed ledger technology in CBDC infrastructure or user-facing applications

Nevertheless, other approaches to improve cross-border payments are also possible. In the World Economic Forum's January 2021 virtual Davos Agenda summit, Tharman Shanmugaratnam, Senior Minister of Singapore and chairman of its monetary authority, argued that CBDC might not be necessary if international interoperability and identity were solved, suggesting that private money could be used over new structures.[66]

Policy-makers and the private sector should collaborate to closely analyse the relative merits of developing cross-border CBDC arrangements as compared to the costs and benefits of other approaches outlined in the G20's cross-border payment roadmap, including but not limited to interlinking domestic payment systems, extending RTGS operating hours and other new multilateral platforms. If CBDCs are identified as a desirable tool for cross-border payments, careful consideration will need to be given to their architecture, including whether cross-border interoperability of the CBDC would be restricted to wholesale institutions or directly accessible to retail users.

4.4 Cross-border CBDC macroeconomic spillover effects and risks

Designing a CBDC that is convenient for cross-border payments might lower the cost of international transactions. Enabling easy access for tourists and foreign visitors could help those individuals, while incentivizing merchant acceptance. Yet significant foreign access to a country's CBDC could result in serious unintended consequences to both the home country and foreign countries. Table 7 lists some potential negative consequences or international spillover effects from a cross-border CBDC with significant accessibility to foreign entities. Many of these consequences could also occur through the widespread adoption of stablecoins denominated in a foreign currency.

TABLE 7 | **Potential negative consequences of cross-border CBDC to issuing and foreign countries**

Country A (home country): Potential unintended consequences from issuance of cross-border CBDC	Country B (foreign country): Potential unintended consequences from usage of cross-border CBDC issued by country A
Currency appreciation and exchange rate volatility	Currency depreciation and exchange rate volatility
	Capital flight and loss of deposits in domestic banks and investments
Heightened risks related to cybersecurity of the CBDC or illicit activity involving the CBDC, depending on foreign accessibility (e.g. KYC requirements and other controls)	Currency substitution or "dollarization" and loss of monetary sovereignty
	Tax avoidance, money laundering or other illicit activity and general loss of oversight by domestic authorities, arising from citizen use of foreign CBDC[67]
Unexpectedly high operational or other costs if foreign adoption is higher than anticipated	Redundancy of payment systems
	Potentially heightened data privacy or cybersecurity risks from foreign CBDC versus domestic options

To the degree to which they are adopted, stablecoins can also substantially impact macroeconomic stability, particularly in emerging economies. However, jurisdictions can use regulation to block the adoption of foreign CBDC or stablecoins. It may also be the case that jurisdictions do not extensively issue cross-border CBDCs (either because they do not clearly support domestic policy goals or because they introduce significant risks, or both), and that stablecoins are not widely adopted.

Governments and the private sector should collaborate on investigating the potential for unintended international spillover impacts of CBDCs and stablecoins, particularly where they have the potential to negatively impact developing economies. The ECB's *Report on a digital euro*, published in October 2020, expresses concerns that a CBDC could have serious unintended consequences on foreign economies, potentially driving the substitution of domestic money and amplifying "the real and financial cross-border spillovers of domestic monetary policy shocks by creating a new channel for their propagation."[68] The IMF deepens this analysis in their recent policy paper, *Digital Money Across Borders: Macro-Financial Implications*, which expresses concerns that foreign-denominated CBDCs and stablecoins could "reduce the ability of local authorities to run monetary policy" and could "raise pressures for currency substitution and worsen vulnerabilities from currency mismatches."[69]

The cross-border circulation of a CBDC that does not include the necessary control mechanisms could be used to circumvent the law outside its jurisdiction. On this subject, the BIS and select central banks write: "Transparency and coordination between central banks and other public authorities will be needed to understand and manage any unintended consequences."[70]

Further study is required to identify and develop the correct policy tools to mitigate these spillover impacts and to effectively balance the risks and benefits that CBDCs and stablecoins pose to cross-border flows. As with other areas, this analysis will benefit from close public-private collaboration that brings to bear the complementary perspectives and capabilities of multiple parties.

The following resources provide additional information about the negative macroeconomic consequences of stablecoins and cross-border CBDCs:

- Bank for International Settlements, *BIS Annual Economic Report 2021 - III. CBDCs: an opportunity for the monetary system*, 2021.[71]
- European Central Bank, *Central bank digital currency in an open economy*, 2020.[72]
- Feyen, Erik et al., "Digital money: Implications for emerging market and developing economies", *VoxEU*, 16 January 2020.
- Ferrari, Massimo Minesso et al., "The international dimension of a central bank digital currency", *VoxEU,* 12 October 2020.[73]

"Governments and the private sector should collaborate on investigating the potential for unintended international spillover impacts of CBDCs and stablecoins, particularly where they have the potential to negatively impact developing economies

Conclusion

This paper identifies a range of different activities, roles and opportunities for the public sector, public-private cooperation and intergovernmental collaboration in the development and growth of central bank digital currency (CBDC) and stablecoins. While they are distinct and very different forms of digital currency, CBDC and stablecoins both present unique risks and opportunities. Policy-makers should carefully consider their approach to each. Their considerations will inevitably be based on domestic country conditions, policy goals and political-economy constraints. But policy-makers could apply the options presented in this paper as a starting point in determining their approach to CBDC and stablecoins.

Two themes are clear:

– Global coordination, including with the private sector, is essential

– Policy-makers have a responsibility to constituents to study, monitor and in many cases take action with respect to stablecoins and CBDC

Stablecoins present more immediate risks, as their issuance grows rapidly while regulatory coverage is currently limited. With CBDC, policy-makers have more time to wait and see. They can monitor and learn from CBDC arrangements, given their limited issuance and the low likelihood for foreign access with initial deployment.[74] That said, they should consider the opportunities that CBDC could provide their economies and potentially stand ready to participate in multilateral CBDC arrangements in the future, bearing in mind they may need to enact policies protecting their economies from any negative consequences of foreign cross-border CBDC.

Endnotes

1. See:

   1) Researchers at the International Monetary Fund (IMF) coined this term. See Adrian, Tobias and Mancini-Griffoli, Tommaso, "Public and Private Money Can Coexist in the Digital Age", *IMF Blog*, 18 February 2021, https://blogs.imf.org/2021/02/18/public-and-private-money-can-coexist-in-the-digital-age/.

   2) Researchers at the Bank for International Settlements (BIS) call this concept "indirect infrastructure" for CBDC, or "indirect CBDC". See Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, BIS Quarterly Review March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

   3) Additional insights are available at Auer, Raphael and Böhme, Rainer, "CBDC architectures, the financial system, and the central bank of the future", *VoxEU*, 29 October 2020, https://voxeu.org/article/cbdc-architectures-financial-system-and-central-bank-future.

2. European Central Bank (ECB), *Report on a digital euro*, 2020, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

3. Brainard, L., *An Update on Digital Currencies*, 18 August 2020, speech presented at the Federal Reserve Board and Federal Reserve Bank of San Francisco's Innovation Office Hours, San Francisco, https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm.

4. "ESMA in Brief", *European Securities and Markets Authority*, https://www.esma.europa.eu/about-esma/esma-in-brief.

5. "Chapter 3: Overview of ASIC", *Parliament of Australia*, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/ASIC/Final_Report/c03.

6. "About FSOC", *US Department of the Treasury*, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/about-fsoc.

7. "Monetary Policy Strategy", *Swiss National Bank (SNB)*, https://www.snb.ch/en/iabout/monpol/id/monpol_strat#t2.

8. "What is the Competition Bureau?", *Government of Canada*, 25 September 2019, https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04296.html.

9. Austin, Janet, *What Exactly is Market Integrity? An Analysis of One of the Core Objectives of Securities Regulation*, 8 Wm. & Mary Bus. L. Rev. 215 (2017), https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1126&context=wmblr.

10. See:

    1)Financial Action Task Force (FATF), *Virtual Assets and Virtual Asset Service Providers*, 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

    2) Financial Action Task Force (FATF), *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*, 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

11. For additional information and recommendations on risks and challenges with stablecoins, see:

    1) Gorton, Gary B. and Zhang, Jeffery, *Taming Wildcat Stablecoins*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888752.

    2) Catalini, Christian and de Gortari, Alonso, *On the Economic Design of Stablecoins*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499.

    3) BIS, G7 and IMF, *Investigating the impact of global stablecoins*, 2019, https://www.bis.org/cpmi/publ/d187.pdf.

12. A mapping of regulatory approaches by countries around the world with respect to blockchain-based digital currency in general can be found at the Global Blockchain Business Council's "Global Standards Mapping Initiative (GSMI)" website, https://gbbcouncil.org/gsmi/.

13. See:

    1) "Regulatory Sandbox", *FCA*, 2016, https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

    2) "Summary Terms – Moneyfold", *Moneyfold*, 2021, https://moneyfold.co.uk/terms/.

14. "Legal and regulatory framework for blockchain", *European Commission*, 2020, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain.

15. Raftery, Gavin et al. "Crypto Garage Becomes First Fintech Participant in Japan's Regulatory Sandbox", *Baker McKenzie*, 2019, https://blockchain.bakermckenzie.com/2019/02/08/crypto-garage-becomes-first-fintech-participant-in-japans-regulatory-sandbox/.

16. "Nabiullina spoke about the testing by the Central Bank of the cryptocurrency 'stablecoins'", *Interfax*, 25 December 2019, https://www.interfax.ru/russia/689362 (in Russian).

17. "Techsprint", *Department of Financial Services*, 2021, https://www.dfs.ny.gov/techsprint.

18. For additional information on digital run risk in stablecoins, see:

1) Gorton, Gary B. and Zhang, Jeffery, *Taming Wildcat Stablecoins*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888752.

2) Catalini, Christian and de Gortari, Alonso, *On the Economic Design of Stablecoins*, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499.

3) For information on historic mismanagement of reserve assets with the largest stablecoin, Tether, see "Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities In New York", *Letitia James NY Attorney General*, 2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.

19. See:

1) ECB Crypto-Assets Task Force, *Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area*, European Central Bank, 2020, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf.

2) Adrian, T., *Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System*, 14 May 2019, speech presented to IMF-Swiss National Bank Conference, Zurich, https://www.imf.org/en/News/Articles/2019/05/13/sp051419-stablecoins-central-bank-digital-currencies-and-cross-border-payments.

3) Adrian, Tobias and Mancini-Griffoli, Tommaso, "Public and Private Money Can Coexist in the Digital Age", *IMF Blog*, 18 February 2021, https://blogs.imf.org/2021/02/18/public-and-private-money-can-coexist-in-the-digital-age/.

4) World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit - Appendices*, 2020, p. 11. http://www3.weforum.org/docs/WEF_CBDC_Policy-maker_Toolkit_Appendices.pdf.

20. See:

1) World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, 2020, http://www3.weforum.org/docs/WEF_CBDC_Policy-maker_Toolkit.pdf.

2) Feyen, Eric, et al., "Digital Money: Implications for Emerging Market and Developing Economies", *VoxEU*, 16 January 2020, https://voxeu.org/article/digital-money-implications-emerging-market-and-developing-economies.

21. "Seigniorage" means "profit made by a government by issuing currency, especially the difference between the face value of coins and their production costs". Source: Oxford Languages.

22. As examples, see the ECB and Bank of Thailand's CBDC consultations:

1) European Central Bank, *Report on the public consultation of a digital euro,* 2021, https://www.ecb.europa.eu/paym/digital_euro/html/pubcon.en.html.

2) Bank of Thailand, *The Way Forward for Retail Central Bank Digital Currency in Thailand*, 2021, https://www.bot.or.th/English/PressandSpeeches/Press/2021/Pages/n2164.aspx.

23. World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, 2020, p. 10 http://www3.weforum.org/docs/WEF_CBDC_Policy-maker_Toolkit.pdf.

24. For discussion of foreign or cross-border CBDC access, including to tourists or domestic visitors, see Auer, Raphael et al., *CBDCs beyond borders: results from a survey of central banks*, BIS Papers No. 116, 2021, https://www.bis.org/publ/bppdf/bispap116.pdf.

25. World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, 2020, http://www3.weforum.org/docs/WEF_CBDC_Policy-maker_Toolkit.pdf.

26. See:

1) Auer, Raphael et al., *Rise of the central bank digital currencies: drivers, approaches and technologies*, BIS Working Papers No. 880, 2020, p. 17, https://www.bis.org/publ/work880.pdf.

2) Auer, Raphael et al., "Central bank digital currencies: Drivers, approaches, and technologies", *VoxEU*, 28 October 2020, https://voxeu.org/article/central-bank-digital-currencies-drivers-approaches-and-technologies. The authors describe a model for determining CBDC design that begins with the CBDC architecture and continues with technical infrastructure, access levels and interlinkages with retail, wholesale and cross-border individuals and firms.

27. See:

1) Bank of England, *Bank of England statement on Central Bank Digital Currency* [Press release], 19 April 2021, https://www.bankofengland.co.uk/news/2021/april/bank-of-england-statement-on-central-bank-digital-currency.

2) Riksbank, *E-krona,* https://www.riksbank.se/en-gb/payments--cash/e-krona/.

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

28. The World Economic Forum's public list of research papers related to CBDC is accessible here: https://docs.google.com/document/d/1c8iGtoG7BkPr-iufnIPELEWvtZiNtouOyJp2IYjhAEY/edit?usp=sharing.

29. Boar, Codruta and Wehrli Andreas, *Ready, set go? - Results of the third BIS survey on central bank digital currency*, BIS, 2021, https://www.bis.org/publ/bppdf/bispap114.htm.

30. The impact of financial education programmes may not be well established, as biases, heuristics and emotional influences can significantly affect individuals' financial decisions regardless of educational programmes and efforts. For further discussion, see Willis (2011): *The financial education fallacy*, AER, 101(3), https://www.aeaweb.org/articles?id=10.1257/aer.101.3.429.

31. See The BIS Innovation Hub and MAS's Project Nexus: https://www.bis.org/about/bisih/topics/fmis/nexus.htm.

32. The Money Movement, "Episode 4: Full Reserve Banking, Narrow Banks for Digital Currency and the China Model", *YouTube*, 26 May 2020. https://www.youtube.com/watch?v=7RhftMt4qtI.

33. Her Majesty's Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence,* 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf.

34. "Legal and regulatory framework for blockchain", *European Commission*, 2020, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain.

35. Financial Action Task Force, *Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers*, 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html.

36. "The Libra Association announces new members", *Libra Association*, 14 May 2020, https://www.diem.com/en-us/updates/new-members/.

37. As a reminder, PSPs and payment platforms beyond stablecoins may also be considered for central bank reserve access.

38. World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit - Appendices*, 2020, http://www3.weforum.org/docs/WEF_CBDC_Policy-maker_Toolkit_Appendices.pdf.

39. "Financial Crime Enforcement Network Exchange", *US Government*, 2021, https://www.fincen.gov/resources/financial-crime-enforcement-network-exchange.

40. See:

    1) Bank of Thailand, *The Way Forward for Retail Central Bank Digital Currency in Thailand*, 2021, https://www.bot.or.th/Thai/DigitalCurrency/Documents/BOT_RetailCBDCPaper.pdf.

    2) Bank of England, *Responses to the Bank of England's March 2020 Discussion Paper on CBDC*, 2021, https://www.bankofengland.co.uk/paper/2021/responses-to-the-bank-of-englands-march-2020-discussion-paper-on-cbdc.

    3) ECB, *Report on the public consultation of a digital euro*, 2021, https://www.ecb.europa.eu/paym/digital_euro/html/pubcon.en.html.

41. "Digital Finance Outreach", *European Commission*, 2021, https://ec.europa.eu/info/publications/digital-finance-outreach_en.

42. "BIS Innovation Hub and SWIFT launch ISO 20022 and API hackathon" [Press release], BIS, 23 February 2021, https://www.bis.org/press/p210223a.htm.

43. "MAS Partners with IMF, World Bank and others to launch Global Challenge for Retail CBDC Solutions" [Press release], *Monetary Authority of Singapore*, 28 June 2021, https://www.mas.gov.sg/news/media-releases/2021/mas-partners-imf-world-bank-and-others-to-launch-global-challenge-for-retail-cbdc-solutions.

44. "Digital Currencies And Fintech: Projects", *Bank of Canada*, 2021, https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/#project-jasper.

45. "Project Bakong – The Next-Generation Mobile Payments", *National Bank of Cambodia*, 2021, https://bakong.nbc.org.kh/en/.

46. Bank of Thailand and Hong Kong Monetary Authority, *Inthanon-LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments*, 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf.

47. BIS, SIX Group AG and Swiss National Bank, *Project Helvetia: Settling tokenized assets in central bank money*, 2020, https://www.bis.org/publ/othp35.htm.

48. "Programmable instant payments in DLT networks and distribution of digital money: An interview with Juan Luis Encinas, Managing Director at Iberpay", *European Payments Council*, 7 January 2021, https://www.europeanpaymentscouncil.eu/news-insights/insight/programmable-instant-payments-dlt-networks-and-distribution-digital-money.

49. World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit - Appendices*, 2020, pp. 9-10. http://www3.weforum.org/docs/WEF_CBDC_Policy-maker_Toolkit_Appendices.pdf.

50. IMF, *The Bali Fintech Agenda: A blueprint for Successfully Harnessing Fintech's Opportunities* [Press release], 11 October 2018, https://www.imf.org/en/News/Articles/2018/10/11/pr18388-the-bali-fintech-agenda.

51. BIS, Committee on Payments and Market Infrastructures, *Enhancing cross-border payments: building blocks of a global roadmap – Stage 2 report to the G20 – technical background report,* 2020, https://www.bis.org/cpmi/publ/d194.pdf.

52. "BIS Innovation Hub Work Programme", *Bank for International Settlements*, 2021, https://www.bis.org/topic/fintech/hub/programme.htm.

53. See:

1) Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins,* 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.

2) Financial Stability Board (FSB), *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Final Report and High-Level Recommendations*, 2020, https://www.fsb.org/wp-content/uploads/P131020-3.pdf.

3) ECB, ECB Crypto-Assets Task Force, *Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area*, 2020, https://www.ecb.europa.eu//pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf.

4) BIS, G7 Working Group of Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.

54. Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins,* 2020, p. 26, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.

55. For further discussion, see BIS, *BIS Annual Economic Report 2021*, 2021, p. 72 https://www.bis.org/publ/arpdf/ar2021e3.pdf.

56. For example, see ECB*, Exploring anonymity in central bank digital currencies*, 2019, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf?3824c3f26ad2f928ceea370393cce785.

57. FSB, *Regulation, Supervision and Oversight of Global Stablecoin Arrangements - Final Report and High-Level Recommendations*, 2020, https://www.fsb.org/wp-content/uploads/P131020-3.pdf.

58. BIS, Committee on Payments and Market Infrastructures, *Enhancing cross-border payments: building blocks of a global roadmap – Stage 2 report to the G20 – technical background report,* 2020, https://www.bis.org/cpmi/publ/d194.pdf.

59. BIS, Committee on Payments and Market Infrastructures, *Enhancing cross-border payments: building blocks of a global roadmap – Stage 2 report to the G20 – technical background report,* 2020, https://www.bis.org/cpmi/publ/d194.pdf.

60. See:

1) OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

2) Group of Thirty, *Digital Currencies and Stablecoins: Risks, Opportunities, and Challenges Ahead*, 2020, https://scholar.harvard.edu/files/rogoff/files/g30_digital_currencies_and_stablecoins.pdf.

61. See:

1) Auer, Raphael et al., *CBDCs beyond borders: results from a survey of central banks*, BIS Papers No. 116, 2021, https://www.bis.org/publ/bppdf/bispap116.pdf.

2) The Bank of Canada, the Bank of England and the MAS explored in a 2018 paper the interoperability of blockchains between different CBDC systems, data standards, and legal and regulatory considerations: Bank of Canada, Bank of England, Monetary Authority of Singapore, *Cross-Border Interbank Payments and Settlements: Emerging opportunities for digital transformation*, 2018, https://www.bankofengland.co.uk/-/media/boe/files/report/2018/cross-border-interbank-payments-and-settlements.pdf?la=en&hash=48AADDE3973FCB451E725CB70634A3AAFE7A45A3.

3) The Bank of Thailand and Hong Kong Monetary Authority also discussed cross-system interoperability in the Project Inthanon-LionRock: Bank of Thailand and Hong Kong Monetary Authority, *Inthanon-LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments,* 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf.

4) Lastly, in Project Jasper in 2017, the Bank of Canada proposed that the interoperability of domestic and global financial markets and infrastructure is not only very important for payment and settlement, but also necessary for effective support of global business activities: Chapman, James et al., *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?*, Bank of Canada, 2017, https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.

62. Group of Central Banks, *Central bank digital currencies: foundational principles and core features*, BIS, 2020, p. 7 https://www.bis.org/publ/othp33.pdf.

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

64. Hong Kong Monetary Authority, *Joint statement on Multiple Central Bank Digital Currency (m-CBDC) Bridge Project* [Press release], 23 February 2021, https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/02/20210223-3/.

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

66. World Economic Forum, "Resetting Digital Currencies (Option 2)", *The Davos Agenda*, Virtual, 2021, https://www.weforum.org/events/the-davos-agenda-2021/sessions/resetting-digital-currencies-2.

67. Auer, Raphael et al., *CBDCs beyond borders: results from a survey of central banks*, BIS Papers No. 116, 2021, https://www.bis.org/publ/bppdf/bispap116.pdf.

68. ECB, *Report on the public consultation of a digital euro,* 2021, https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

69. IMF, *Digital Money Across Borders: Macro-Financial Implications*, 2020, https://www.imf.org/en/Publications/Policy-Papers/Issues/2020/10/17/Digital-Money-Across-Borders-Macro-Financial-Implications-49823.

70. See:

    1) Auer, Raphael et al., *CBDCs beyond borders: results from a survey of central banks*, BIS Papers No. 116, 2021, https://www.bis.org/publ/bppdf/bispap116.pdf.

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

71. For further discussion, see BIS, *BIS Annual Economic Report 2021 - III. CBDCs: an opportunity for the monetary system*, 2021, https://www.bis.org/publ/arpdf/ar2021e3.pdf.

72. Ferrari, Massimo Minesso et al., *Central bank digital currency in an open economy*, European Central Bank, 2020, https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2488~fede33ca65.en.pdf?ac12ca088c73513aca6012ea1e3671d2.

73. 1) Feyen, Eric, et al., "Digital Money: Implications for Emerging Market and Developing Economies", *VoxEU*, 16 January 2020, https://voxeu.org/article/digital-money-implications-emerging-market-and-developing-economies.

    2) Ferrari, Massimo Minesso et al., "The international dimension of a central bank digital currency", *VoxEU,* 12 October 2020, https://voxeu.org/article/international-dimension-central-bank-digital-currency.

74. Owing to the greater complexity of enabling CBDC access to foreign entities, it is unlikely that most central banks will implement CBDC with immediate foreign/cross-border access. Many central banks are still unsure of the foreign access they will enable. For further information, see Bank for International Settlements, Auer, Raphael et al., *CBDCs beyond borders: results from a survey of central banks*, BIS Papers No. 116, 2021, https://www.bis.org/publ/bppdf/bispap116.pdf.

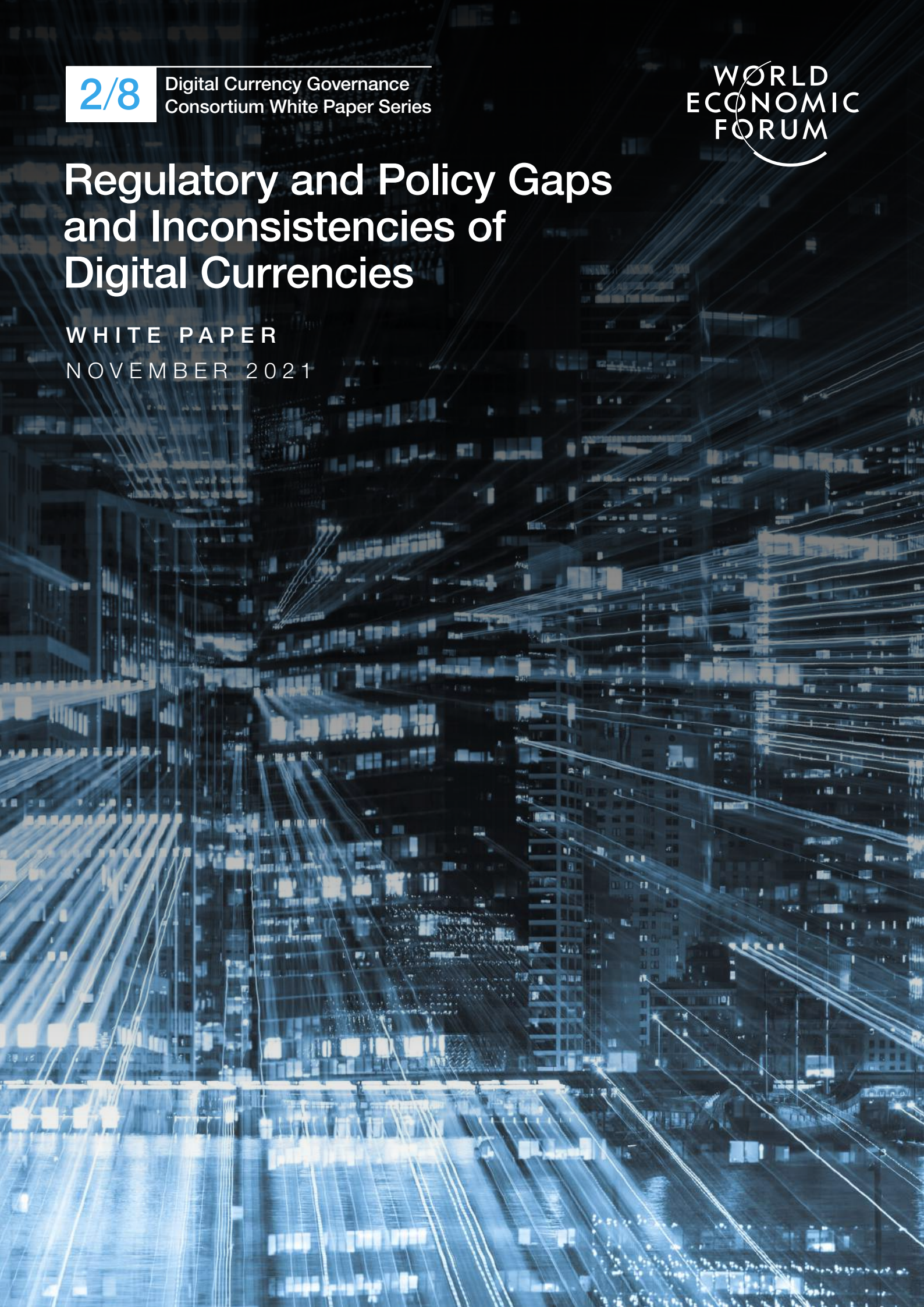
2/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Regulatory and Policy Gaps and Inconsistencies of Digital Currencies

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

Preface 45

1 Potential regulatory and policy gaps and inconsistencies 46

1.1 Gaps between innovations and existing laws and regulations 46

1.2 Gaps and inconsistencies created by the overlapping jurisdictions of different regulatory agencies 47

1.3 Gaps and inconsistencies created by lack of global coordination 49

1.4 Gaps and inconsistencies due to the similarities between retail CBDCs and stablecoins 50

2 Principles for regulation 51

2.1 Inter-agency and international coordination 51

2.2 Risk-based approach to regulate digital currencies 53

3 An initial framework to identify, prevent and address gaps and inconsistencies 54

Step 1 Risk mapping exercise 55

Step 2 Agency mapping 56

Step 3 Organize taskforce 57

Step 4 Set priorities 57

Step 5 Identify gaps and inconsistencies 58

Conclusion 61

Endnotes 62

Preface

This white paper explores potential regulatory and policy gaps and inconsistencies that stem from existing approaches towards retail CBDCs and stablecoins. It provides an initial framework for policy-makers to address these gaps and inconsistencies.

Designing a coherent, global and innovation-friendly regulatory and policy framework for digital currencies is a challenging task. Three key challenges face policy-makers:

- Conflict between rapidly changing technology and a reactive rule-making process
- Lack of coordination among rule-making bodies in financial services
- Lack of consensus on what digital currencies are designed to accomplish, especially relative to pre-existing alternatives

Many digital currencies claim to be created for the purpose of improving existing payments systems and promoting financial inclusion, by reducing transactional friction through improving settlement processes or bypassing intermediaries altogether. A fragmented regulatory environment with gaps, inconsistencies and redundancies at domestic or international levels could easily frustrate such purposes and stagnate innovation.

The term "digital currencies" used throughout this white paper refers mainly to retail CBDCs[1] and stablecoins. This paper chooses to focus on retail CBDCs and stablecoins, as their potential to gain wide-scale adoption may create significant risks for individuals as well as to financial and monetary systems. The aim of this white paper is to help foster a regulatory and policy environment conducive to the development and adoption of digital currencies, while the laws and regulations on digital currencies are still being shaped. The ecosystem will continue to see the emergence of new CBDCs, stablecoins and cryptocurrencies, so regulators should anticipate a complex and diverse landscape.

This white paper reflects insights generated through discussions and collaborations with senior public and private sector leaders. It builds on the work of various international standard-setting organizations. It identifies current trends of regulatory and policy developments shown by selected countries and key standard-setters. And it highlights how existing approaches to innovation may create regulatory and policy gaps and inconsistencies for digital currencies at both domestic and global levels.

In addition, this paper explores the interplay between retail CBDCs and stablecoins and probes how laws and regulations should approach these digital currencies, if policy-makers decide to make stablecoins available to consumers alongside retail CBDCs. It examines the pros and cons of some existing rule-making approaches and proposes an initial framework for policy-makers and regulators to consider, with the aim of helping to drive global and domestic coordination and interoperability in an environment with fast-moving technological innovation.

1 Potential regulatory and policy gaps and inconsistencies

This chapter examines potential regulatory gaps and inconsistencies in the following four areas:

1. **Gaps between innovations and existing laws and regulations**
2. **Gaps and inconsistencies created by the overlapping jurisdictions of different regulatory agencies**
3. **Gaps and inconsistencies created by lack of global coordination**
4. **Gaps and inconsistencies due to the similarities between retail CBDCs and stablecoins**

1.1 Gaps between innovations and existing laws and regulations

> Existing laws and regulations may not be equipped to provide a legal basis for the existence of digital currencies or address their risks

As the technology underlying digital currency continues to evolve and becomes more sophisticated, regulators and policy-makers are facing three key challenges that result in potential gaps and inconsistencies.

First, existing laws and regulations may not be equipped to provide a legal basis for the existence of digital currencies. Gaps can occur when the conventional definitions of terms such as "property", "funds", "assets" or "money" do not include or cannot be interpreted to include digital currencies. There may be gaps in granting legal grounds to support the creation of digital currencies and the financial services built upon digital currencies. For example, while many central banks are conducting research on CBDCs, with a few already in pilot phases, 104 central banks do not have the authority to issue CBDCs under their central banking laws, according to a survey by the International Monetary Fund (IMF).[2] With respect to stablecoins, there is little or no guidance in most jurisdictions as to who has the authority to issue stablecoins or – if the issuance requires a special licence or authorization – what are the mechanisms for supervising stablecoins and the required regulatory oversights.

Second, there may be regulatory and policy gaps in addressing risks unique to digital currencies, particularly those risks associated with the decentralization characteristics of digital currencies. The mandate of various regulatory bodies may need to evolve as the emergence of digital currencies requires them to handle new responsibilities and play new roles. Consumer protection is an area where regulators face significant challenges – for a more detailed discussion, refer to the white paper in this series entitled *Digital Currency Consumer Protection Risk Mapping*.

Another area where regulators face significant challenges is financial crime. As digital currencies can enable users to conduct transactions at high speed without an intermediary, there is a risk that criminals can exchange funds across borders much faster and more easily than if they used cash. Furthermore, a payer and a payee in a permissionless environment can easily create numerous anonymous, unhosted (self-custody) wallets[3] and multiple small-amount transactions to circumvent regulations that focus on monitoring large transactions. The Financial Action Task Force (FATF) amended its standards in 2019 to require regulation of digital currencies and since then it has issued various guidelines about combatting financial crimes involving digital currencies.[4]

The FATF's anti-money laundering and combatting the financing of terrorism (AML/CFT) measures generally place obligations on intermediaries between individuals and the financial system, while transactions between unhosted wallets are not subject to AML/CFT measures. The FATF addresses this by recommending that countries adopt measures such as:

– Creating a broad definition of "Virtual Asset Service Providers" (VASPs) to

bring everyone who has some level of control over the ecosystem under the jurisdiction of AML/CFT measures

– Requiring VASPs to obtain or keep a record of transactions and verify the information of payers and payees

– Placing additional controls or supervision over VASPs that allow transactions to unhosted wallets, including not permitting VASPs to transact with unhosted wallets

Such compliance measures may reduce the efficiency of transactions as, from technical standpoint, it may not be easy to determine if a counterparty is a VASP or an unhosted wallet.[5] As most countries in the world have not yet adopted FATF recommendations, it remains to be seen whether these recommendations will be effective in combatting financial crimes.

Third, there may be gaps due to policy-makers' inability to keep pace with the technology and implement and enforce the required regulations quickly enough. Policy-makers often find themselves playing catch-up when it comes to regulating innovations under the existing legislative process. The inability of policy-makers to keep up with technology could prevent the benefits of innovation from materializing and expose users to risks. Meanwhile, the few jurisdictions that have drafted regulations for VASPs are struggling to enforce them. Some jurisdictions have not been able to complete the licensing process even within two or three years of VASPs submitting applications. Where the process of licensing VASPs has been completed within a reasonable time period, regulators may not have been able to effectively restrict unlicensed exchanges from operating, thus disincentivizing VASPs that spend time and effort complying with regulatory frameworks.

1.2 Gaps and inconsistencies created by the overlapping jurisdictions of different regulatory agencies

While stablecoins have, to date, mostly been used to facilitate the trading of cryptocurrencies with high volatilities, the industry expects stablecoins to be used as medium of exchange for general commerce. The ability to have a stable value is important for stablecoins to meet such industry expectation. However, the design required to stabilize the value of stablecoins is complex.

Stablecoins may be backed by fiat currencies, short-term bonds and other securities or assets (including cryptocurrency). Certain stablecoins share similar characteristics with other traditional financial instruments, such as certificates of deposit, money market funds, securities or derivatives. From the perspectives of securities and commodity commissions, stablecoins may be considered as securities, commodities or derivatives, depending not only on how a stablecoin is structured but also on the nature of the assets that underpin the reserve.[6] Stablecoins may also be classified based on their systemic importance.

A survey conducted by the Financial Stability Board (FSB) on regulatory and supervisory approaches to stablecoins shows that while the complex design of stablecoins invites attention from multiple regulatory agencies, few countries have issued guidance on the classification and application of existing regulations or supervision to stablecoins.[7] For an overview of different classification criteria for cryptoassets, see Figure 1.

FIGURE 1 **Selected examples of cryptoasset classification criteria**[8]

Functionality criteria			
Categories	**Payment/exchange**	**Investment**	**Utility**
Description	Intended to be used as means of payment or exchange	Provides rights and obligations similar to traditional financial instruments like shares, debt instruments or units in a collective investment scheme.	Grants holders access to a current or prospective service/product in one or multiple company's network or ecosystem
Subcategories or labels*	payment token, e-money token, exchange token	security token	utility token
	hybrid token		

Stabilization mechanism criteria		
Categories	**Asset-linked**	**Algorithm-based**
Description	Stablecoin that purports to maintain a stable value by referencing physical or financial assets or cryptoassets (FSB (2020)). Can be further differentiated into currency-based, financial instrument-based, commodity-based and cryptoasset-based stablecoins.	Stablecoin that purports to maintain a stable value via protocols that provide for the increase or decrease of the supply of the stablecoins in response to changes in demand (FSB (2020)).
Subcategories or labels**	asset-referenced token, stable token	algorithmic stablecoins

Systemic importance criteria		
Categories	**Global**	**Non-global**
Description	Stablecoins with a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume (FSB (2020))	Stablecoins without a potential reach and adoption across multiple jurisdictions and the potential to achieve substantial volume
Subcategories or labels**	significant asset-referenced token, significant e-money token, systemic stable token	asset-referenced token, e-money token, stable token

Notes: * Examples of subcategories or labels used by some surveyed authorities.
** Examples of subcategories or labels proposed in regulations currently in consultation processes in some surveyed jurisdictions.

Source: Bank of International Settlements

The overlapping jurisdictions of different regulatory agencies create difficulties in classifying and regulating stablecoins both at domestic and international levels. Conflicting views may create regulatory and policy loopholes that could be exploited by the very individuals that regulators intend to forestall. While there may be case law that provides guidance on how and when stablecoins should be treated as "securities" in some jurisdictions,[9] regulators often request that market participants consult with them on a case-by-case basis given the novelty of these technologies.[10] Such case-by-case consultations could potentially increase the compliance costs for companies that are willing to comply with rules for issuing stablecoins (or increase potential fines for those intending to avoid or ignore compliance). This approach could also create complexity that may lead to gaps and inconsistencies within the governing agency.

Furthermore, this lack of regulatory certainty may deter new participants from entering the space and thus stifle innovation in a specific jurisdiction. The challenge of how to classify various digital currencies is the first question posed in the UK government's public consultation paper of January 2021, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*. The paper's authors, HM Treasury, acknowledge the importance of clarifying the taxonomy of stablecoins and creating regulatory certainty for consumers and businesses. They also emphasize the importance of any classification to be "future-proof and sufficiently flexible".[11] A clear classification of stablecoins should be the first step in achieving regulatory clarity on the governance of stablecoins.

1.3 Gaps and inconsistencies created by lack of global coordination

> Without regulatory consistency, a multi-jurisdictional stablecoin might need to comply with securities regulations in country A, derivatives regulations in country B, banking regulations in country C and perhaps no regulations at all in country D

A diversity of ways to classify stablecoins in one country not only complicates the legal framework for stablecoins within that jurisdiction, it also creates an additional layer of translation and confusion between countries and regions. While many international standard-setting organizations have been updating their guidance regarding stablecoins, there remains a lack of global coordination on stablecoin classification. Without organizations driving regulatory consistency over classification at a global level, it is not hard to imagine that an issuer of a multi-jurisdictional stablecoin might need to comply with securities regulations in country A, derivatives regulations in country B, banking regulations in country C and perhaps no regulations at all in country D.

Without coordination among countries, such potential gaps could allow for regulatory arbitrage. Issuers may choose to issue coins in jurisdictions with favourable classifications or where stablecoins are not governed by any regulations. Well-established financial institutions with global footprints may strive for broader compliance, while delaying product offerings that could provide better services to their consumers. A stablecoin-issuer exploiting such gaps may reach systemic status before any legal protection can be put in place. They could then be used to conduct money laundering, cyber-crime and other illicit activity.

Standard-setting organizations, such as the FSB, and regulators are increasingly considering how to regulate stablecoins that may present a systemic risk to financial stability. Part of the challenge with such an endeavour is that there is no agreed definition among jurisdictions of what constitutes a “systemic risk”. This lack of a globally accepted definition or a means to measure such risk can lead to a substantial amount of regulatory discretion, which may result in gaps and inconsistencies.[12]

While retail CBDCs may face a clearer regulatory landscape domestically, the possibility of using retail CBDCs for cross-border payments raises many questions. How will a retail CBDC be treated beyond its border? Do the receiving country’s laws and regulations allow for retail CBDCs? Do the existing definitions of money or e-money capture retail CBDCs? How are the financial products that are built on retail CBDCs classified? Will existing foreign exchange control rules apply? These are just some of the possible questions. Regulatory gaps can easily widen when the answers to such questions are not carefully evaluated, and inconsistencies will emerge if those questions are not dealt with in a consistent manner across various agencies.[13]

1.4 Gaps and inconsistencies due to the similarities between retail CBDCs and stablecoins

In the past few years, several analyses have examined the policy and regulatory implications of CBDCs and stablecoins, many of which have narrowly focused on one or the other. While stablecoins do not have the same legal status as CBDCs and the value of a stablecoin depends on its underlying stabilization mechanism and governance, stablecoins are similar to retail CBDCs in many ways:

- Both retail CBDCs and stablecoins can act as a medium of exchange and store of value, notwithstanding potentially higher risks associated with stablecoins due to their backing and reserve management
- Both retail CBDCs and stablecoins can be based on distributed ledger infrastructure
- Both can pose systemic risks (such as cybersecurity and financial stability risks) if widely adopted

The similarities between retail CBDCs and stablecoins have been recognized by several policy-makers. For example in the UK, HM Treasury has pointed out in its discussion paper that the category of tokens with stable value would also include "tokenized forms of central bank money".[14] If regulators choose to treat retail CBDCs outside the existing legal framework for digital currencies or cryptoassets, it is important that they close any regulatory gaps to cover risks associated with using retail CBDCs that are similar to stablecoins. For this reason, the FATF has emphasized in its updated guidance that even though CBDCs are not considered a "virtual asset", the same FATF standards applicable to fiat currencies would also apply to CBDCs.[15]

If central banks and policy-makers choose a future where retail CBDCs and stablecoins co-exist, it will be important to ensure similar regulations apply to both types of digital currency in areas where they create similar risks, while ensuring stronger regulations and protections where the risks are higher. Unequal treatment for the same risk may drive individuals and corporations away from adopting the type of digital currency that comes with the least regulatory protection. It could also create confusion from a user's perspective, particularly in cases where stablecoins and retail CBDCs co-exist.

Furthermore, there may be regulatory or policy gaps with respect to digital currencies in areas not covered by central banks' ordinary functions. One notable example is that of cyber risks, such as the lack of cyber resilience of a significant digital currency or a weakness or "bug" common to a number of digital currencies. When a cyber incident progresses from the operational level of an institution to impacting the entire financial system, citizens' trust of the system is affected, which could then turn what is simply an operational incident into a full-blown systemic financial crisis.[16]

2 Principles for regulation

When it comes to solutions to fill gaps and address inconsistencies, the first question is: Should we create a new regulatory regime and agency to govern digital currencies, or should we build upon existing laws and regulations? However, given how diverse the legal systems are across different jurisdictions and given the varying sophistication of laws and regulations on financial products and services, there cannot be a one-size-fits-all approach.

In common law countries, where the law could be derived from custom and judicial precedent, we may rely on the evolution of case law to take care of gaps and inconsistencies as digital currencies evolve, although this could be a lengthy process. In civil law countries that rely more on statutes, a comprehensive guideline may be a better approach. At the same time, it is difficult, if not impossible, to fashion a comprehensive guideline that is future-proof. In markets with sophisticated financial services products and well-designed legislation, the solution may be to update existing laws and regulations to capture the complexity of digital currencies. In markets where the development of financial services and respective laws and regulations are still at an early stage, it may make more sense to build a completely new regulatory framework to address digital currencies.

While the regulatory approach to digital currencies is still being shaped, some principles in law-making may be helpful to regulators who are trying to bridge the gap between innovation and regulation. This chapter presents some principles for regulation in two broad areas:

- Inter-agency and international coordination
- Risk-based approach to regulate digital currencies

2.1 Inter-agency and international coordination

Today, it is not uncommon for crypto-exchanges and fintech firms to conduct duplicative compliance processes. While each agency's set of requirements may have its own merits, the layering of such processes adds complexity that can prove untenably burdensome. With stablecoins, local regulations can have global ramifications. It is well understood that the private sector, policy-makers and regulators share the same goal: empowering strong compliance programmes and supporting innovation, while ensuring consumer protections and financial inclusion. However, when it comes to CBDCs, even though there is some cross-border collaboration, most central banks are principally focused on the domestic use cases for CBDCs in their current phase of research. Due to the complex design and inherent cross-border uses for digital currencies, regulators must work together, both between different domestic agencies and across jurisdictions.

In many jurisdictions, there are already frameworks that allow inter-agency coordination and which could be used to identify potential regulatory and policy gaps and inconsistencies in taking a coordinated approach towards digital currencies. For example, among financial regulators in Kenya, there is a Joint Financial Services Forum to work on issues across different agencies.[17] As part of this forum, there is now a common sandbox approach led by the Capital Markets Authority with representation from all financial sector regulators. Applications to the sandbox are comprehensively assessed by all financial sector regulators together. The Hong Kong Special Administrative Region adopts a multi-agency approach under which all relevant financial services agencies would need to work with one another even when a fintech firm only contacts one of the agencies.[18] The Bank of England and HM Treasury have formed a joint CBDC Taskforce to coordinate the exploration of CBDC.[19]

In terms of international coordination, countries can look to major international standard-setting bodies for guidance in drafting their respective laws, regulations and guidelines for digital currencies. These bodies include, but are not limited to:

- **Bank for International Settlements (BIS)**: an international financial institution owned by 63 central banks, which aims to promote global monetary and financial stability through the coordination of global central banks and their monetary policy efforts. BIS has published leading papers on CBDCs and stablecoins.

> The private sector, policy-makers and regulators share the same goal: empowering strong compliance programmes and supporting innovation, while ensuring consumer protections and financial inclusion

- **Basel Committee on Banking Supervision (BCBS)**: the primary global standard-setter for the prudential regulation of banks, which provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions. It has published various papers on cryptoassets.

- **European Commission (EC)**: the EU's politically independent executive arm, the EC is responsible for drawing up proposals for new European legislation and implements the decisions of the European Parliament and the Council of the European Union. In September 2020, the EC published a proposal for an EU regulation on markets in cryptoassets (MiCA).[20]

- **Financial Action Task Force (FATF)**: an inter-governmental organization overseeing the combatting of money laundering and terrorist finance, whose recommendations and standards (particularly on VASPs) have been followed by various domestic AML/CFT regulators.

- **Financial Stability Board (FSB)**: an international body that monitors and makes policy recommendations about the global financial system and whose publications provide clarity on the issues around financial stability, CBDCs and stablecoins.

- **International Organization of Securities Commissions (IOSCO)**: an international body that brings together the world's securities regulators and sets global standards for the securities sector. IOSCO works extensively with the G20 and the FSB on the global regulatory reform agenda. It has issued detailed assessments on how IOSCO principles and standards could apply to global stablecoin initiatives.

Such organizations have been active in their publication of, for example, risk-based guidance reports, standards recommendations, regional reports and collaborative pilot reports. These publications have helped in the scoping of macro issues and in assisting domestic policy-makers prioritize regulatory efforts around cross-jurisdictional issues.

In addition to activities led by the international standard-setting organizations, below are some examples of other types of international coordination which could be leveraged to drive regulatory interoperability and standards for retail CBDCs and stablecoins:

- **Global Financial Innovation Network (GFIN)**: a network formed by over 60 financial regulatory organizations, with a goal of supporting financial innovation at a global scale.[21] In 2019 and 2020, GFIN piloted a single-entry, cross-border testing application for firms wishing to test their innovative financial services across more than one jurisdiction.

- **Bilateral fintech agreements**: some financial regulatory agencies, such as the Commodity Futures Trading Commission (CFTC) in the US,[22] have entered into fintech cooperation agreements with counterparties from other countries, to create a framework for coordination, referrals and information-sharing. The Monetary Authority of Singapore is a champion of this approach and had entered into fintech cooperation agreements with 35 counterparties, as of 31 March 2021.

- **Bilateral or multilateral trade agreements**: trade agreements also play an important role in shaping standards and promoting interoperability. In the Australia-Singapore Digital Economy Agreement, which was signed at the end of 2020, both governments have committed to promote the adoption of internationally accepted standards for online payment systems.[23]

– **United Nations Commission on International Trade Law (UNCITRAL) model law approach**: UNICTRAL is the core legal body of the UN system focusing on the modernization and harmonization of rules on international business. UNCITRAL has published the model laws and regulatory guidelines on international credit transfers, electronic commerce, electronic signatures and electronic transferable records, which allow more uniformity across different jurisdictions.

For a more detailed discussion on global coordination, including public-private collaboration, refer to the white paper in this series entitled *The Role of Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth*.

2.2 Risk-based approach to regulate digital currencies

Ex-ante and ex-post[24] are two approaches that regulators often take when it comes to regulating the latest technologies. The risk of the ex-ante approach is that it may create unnecessary compliance burdens during the infancy of an innovation, which stymie the innovation. Ex-ante can also lead to poorly designed regulations due to a lack of sufficient knowledge of the innovation. In addition, an ex-ante approach may create an unlevel playing field between new entrants and established players who are more knowledgeable or who have more resources to satisfy compliance requirements. Meanwhile, the risk of the ex-post approach is that it may tolerate risky behaviours that could create systemic risk, or harm people or society.

One potential solution to address the dilemma created by the choice between an ex-ante or ex-post approach is to adopt a risk-based approach to law-making. One type of risk-based approach is to have sandbox or innovation labs, which allow innovation to be tested in a limited and controlled environment. Based on a recent study by the World Bank, sandboxes allow for an open dialogue between innovators and regulators and give regulators opportunities to collect empirical data to support policy development, particularly in areas where regulatory requirements are missing or unclear.[25]

Depending on how sandbox and innovation lab-related regulations are drafted, they may also create an unlevel playing field, tilted in favour of providing more incentives for start-ups. It is important to offer the same opportunities to both start-ups and existing players when it comes to innovation. From the sandbox applicant's perspective, sandboxes may not provide sufficient protection for true innovators to base their entire business models on, given that the legal environment may still be unpredictable outside the sandbox. In addition, there are limitations to an innovation lab or sandbox, such as the following:

– Given that sandbox activities are conducted within a controlled environment, the potential systemic risk of digital currencies may not surface
– There is no cross-border sandbox to test the cross-border nature of stablecoins
– Regulators may still need to come up with a comprehensive legal framework when stablecoin ecosystem participants exit the sandbox or innovation lab

Another risk-based approach is to create different levels of regulation based on the potential risks to which a digital currency may expose consumers and society. This approach is exemplified in the EU's proposed MiCA regulation, which will apply to any cryptoasset that is not already subject to EU regulation. MiCA acknowledges that the cryptoasset market today is still small and does not present significant risks to financial stability. The proposed MiCA regulation separates stablecoins into two types:

– "asset-referenced tokens", which maintain a stable value by referring to the value of several fiat currencies, commodities or other cryptoassets or a combination of such assets
– "e-money tokens", which are used as a means of exchange and maintain stability by referring to the value of one fiat currency

Given that the issuance and circulation of "asset-referenced tokens" present potentially higher risks, such tokens are subject to more stringent approval processes and compliance requirements. Furthermore, MiCA proposes a bespoke framework to regulate "significant" stablecoin-issuers and it will force them to comply with stronger capital, investor and supervisory requirements laid down by the European Banking Authority (EBA). These include rules and further requirements on governance, conflicts of interest, reserve assets, custody, investment and the disclosure document. However, MiCA creates a more light-touch approach for small and medium-sized issuers and providers that do not present systemic risk.

> One risk-based approach is to create different levels of regulation based on the potential risks to which a digital currency may expose consumers and society – as exemplified in the EU's proposed MiCA regulation

3 An initial framework to identify, prevent and address gaps and inconsistencies

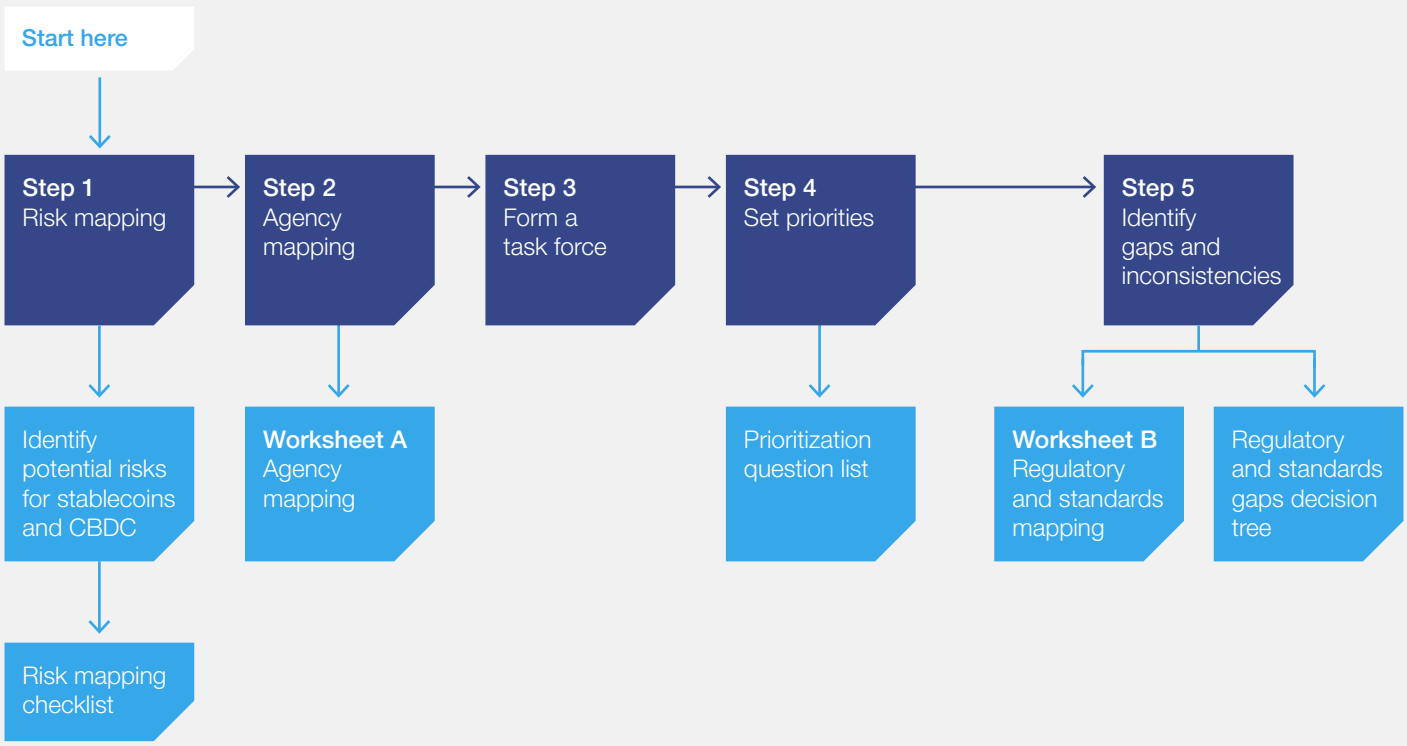
The policy development and regulation of digital currencies need a systemic approach to avoid creating confusion for the payments ecosystem. If policy-makers envisage a system where stablecoins and retail CBDCs co-exist with other payment methods, they will need to identify areas where existing regulations are sufficient and where new regulations are needed for these digital currencies.

As a starting point, this chapter proposes a five-step framework for identifying, preventing and addressing regulatory gaps and inconsistencies, which policy-makers and regulators could consider adopting. The five steps, presented in graphic form in Figure 2, are as follows:

1. Risk mapping
2. Agency mapping
3. Form a taskforce
4. Set priorities
5. Identify gaps and inconsistencies

While this framework may not be able to address all the issues we have identified in this white paper, and while we acknowledge that this framework offers an over-simplified view of a complex law-making process, we nonetheless hope it provides a way forward in addressing regulatory gaps and inconsistencies in relation to emerging digital currencies.

FIGURE 2 **Five-step framework for identifying, preventing and addressing regulatory gaps and inconsistencies**



Step 1 | Risk mapping exercise

Map out key risks to society posed by various users of the digital currency in question throughout its lifecycle, using the risk mapping checklist set out below (see Figure 3).

FIGURE 3 **Risk mapping checklist**

	Issuer	Exchange	Custody/wallet provider	Digital currency holder	Other relevant players?
Issuance	– Capitalization risk – Liquidity risk – Counterparty risk – Run risk – Customer fund risk – Cybersecurity risk – AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Technical risk (e.g. insufficient smart contract audits) – Data privacy	Not applicable	Not applicable	Not applicable	
Circulation (distribution/ exchange)	– AML/CFT – Cybersecurity risk – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Data privacy	– Liquidity risk – Cybersecurity risk – Customer fund risk – AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Technical risk (e.g. insufficient smart contract audits) – Data privacy	– Cybersecurity risk – Capitalization risk – Customer fund risk – Run risk – AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Concentration risk – Tax evasion risk – Data privacy	– AML/CFT – Fraud – Foreign exchange control – Monetary policy/ financial stability risk – Tax evasion risk – Cybersecurity risk – Data privacy	
Storage	Not applicable	Not applicable	– Cybersecurity risk – Capitalization – Counterparty – Customer fund risk – Fraud – Monetary policy/ financial stability risk – Concentration risk – Data privacy	– Non-custodial wallet: property risk (theft, damage etc.) – Cybersecurity risk – Monetary policy/ financial stability risk – Data privacy	
Governance	– Redemption risk – Market risk – Fraud – Monetary policy/ financial stability risk – Risk of minority holders' interests being infringed by majority holders	Not applicable	Not applicable	Not applicable	

Step 2 | Agency mapping

Identify all relevant agencies and standard-setting bodies that would impact the development of retail CBDCs and stablecoins, and address the risks identified in the risk mapping checklist, using Agency mapping: Worksheet A below (see Figure 4).

Worksheet A allows policy-makers and regulators to generate an overview of:

- The jurisdiction each government agency has over retail CBDCs and stablecoins and its respective subject matter expertise
- The jurisdiction each government agency has over the activities of different players in the ecosystem
- The coverage of the subject matter by various standard-setting organizations

Ask the following questions as you work through Worksheet A:

- What activities does this agency cover?
- What risks does this agency set out to prevent?
- What are the laws, regulations or standards published by this agency that would impact this type of digital currency or player?

FIGURE 4 **Agency mapping: Worksheet A (with examples)**

	Domestic retail CBDCs	Foreign retail CBDCs*	Domestic stablecoins	Foreign stablecoins**	Issuer	Exchange	Wallet	Users	Other relevant players?
Central bank	Issuance Circulation Financial stability AML/CFT	Foreign exchange AML/CFT	Issuance Circulation AML/CFT	Issuance Circulation AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	N/A
Finance ministry	Issuance	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Banking/financial services regulators	Circulation	Circulation	Issuance Circulation	Issuance Circulation	Licensing Auditing	Licensing Auditing	Licensing	N/A	N/A
Securities commission	N/A	N/A	Issuance Circulation	Issuance Circulation	Licensing Auditing	Licensing Auditing	N/A	Market stability Insider trading	N/A
Commodity/derivatives	N/A	N/A	Issuance Circulation	Issuance Circulation	Licensing Auditing	Licensing Auditing	N/A	N/A	N/A
Consumer protection bureau	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	Consumer education Fraud	N/A
Tax authorities	Income tax calculation and collection	Income tax calculation and collection	Income tax or capital gain tax calculation and collection	Income tax or capital gain tax calculation and collection	Tax reporting	Tax reporting	N/A	Tax reporting Income tax or capital gain tax calculation and collection	N/A
Other relevant agencies	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	Data privacy	N/A
Standards organizations (e.g. FATF)	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	AML/CFT	N/A

*Refers to retail CBDCs issued by foreign country
**Refers to stablecoins issued by entities incorporated outside of the jurisdiction

Step 3 | Organize taskforce

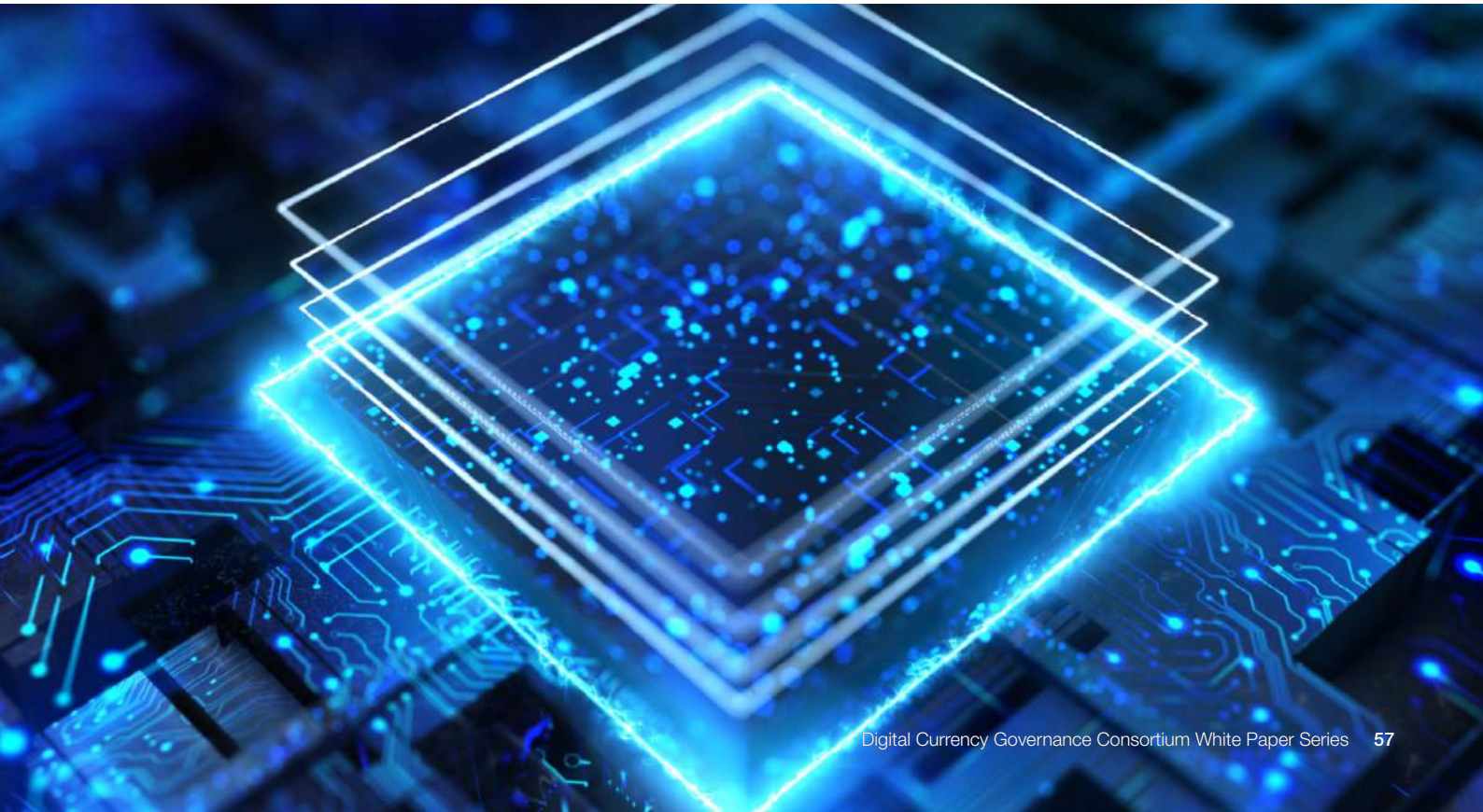
After completing Worksheet A, form a taskforce or similar body composed of the senior leaders of agencies and standard-setting bodies identified in Worksheet A for each subject matter or risk area, including representatives from international standard-setting organizations.

Step 4 | Set priorities

The taskforce can analyse the current state of development of retail CBDCs and stablecoins, and the digital currency regulatory environment, by asking the following questions:

- Where do we stand in terms of the development of our own CBDC?
- Where do our major trading partners stand in terms of the development of their CBDCs?
    - Is there a cross-border element in the design?
    - When will the cross-border function be in force?
    - How will this cross-border function impact our capital inflow and out-flow?
- Where do we stand in terms of the development of stablecoins?
    - What are the prevalent use-cases of stablecoins in our jurisdiction?
    - What is the critical mass of adoption that we are looking for before we put in place regulations or impose requirements, such as fully backing reserves at the central bank or in bankruptcy-remote accounts at regulated commercial banks?
    - What are the risks that we need to start regulating now?
    - Are there any stablecoins offered by corporations incorporated or located outside of our country that are gaining traction in our country?
- In respect of both CBDCs and stablecoins, what are the pros and cons of starting to regulate now, compared to a watch-and-wait approach?

Based on the answers to these questions, the taskforce can prioritize required actions. For example, the taskforce may decide simply to continue monitoring the development of CBDCs and stablecoins in their jurisdiction, or they might decide it is time to start drafting relevant laws and regulations.



Step 5 | Identify gaps and inconsistencies

For step five, the taskforce should aim to identify potential inconsistencies, overlaps and gaps in existing laws and regulations when they are applied to retail CBDCs and stablecoins. The taskforce can then make decisions on how to address these concerns using the tools below:

- Regulatory and standards mapping: Worksheet B (see Figure 5)
- Regulatory and standards mapping: Decision tree (see Figure 6)

While monitoring the development of digital currencies, the taskforce may leverage Worksheet B below to evaluate whether existing laws and regulations have covered all potential risks of retail CBDCs and stablecoins.

FIGURE 5 **Regulatory and standards mapping: Worksheet B (with examples)**

	Domestic retail CBDCs	Foreign retail CBDCs	Domestic stablecoins	Foreign stablecoins
Definition	Yes, defined in Article X, Section X, Clause X of central banking law	Not yet defined. Most appropriate agency to come up with the definition: central bank	Yes, defined in Article X, Section X, Clause X of banking law AND Article X, Section X, Clause X of securities law Definitions may create inconsistencies Action needed: banking regulatory body and securities commission to meet and reconcile the differences	
Authority to issue				
Licensing requirements for issuer				
Authority to circulate				
Licensing requirements for circulation				
Limitation to hold (quantity, qualification, if any)				

FIGURE 5 | **Regulatory and standards mapping: Worksheet B (continued)**

	Domestic retail CBDCs	Foreign retail CBDCs	Domestic stablecoins	Foreign stablecoins
Requirements on potential types of assets that could constitute reserve				
Reserve reporting requirements				
Reserve auditing requirements				
Authority to audit				
Licensing requirements for audit				
Reserve disclosure requirements				
Privacy requirements				
AML/CFT				
Consumer protection requirements				
Competition/Antitrust				
Taxation				
Others				

Regulatory and standards mapping: Decision tree

Policy-makers and regulators can ask themselves the following questions in the order below as they work through Worksheet B:

Q. Has this subject matter/issue/risk area been covered by any existing laws and regulations?

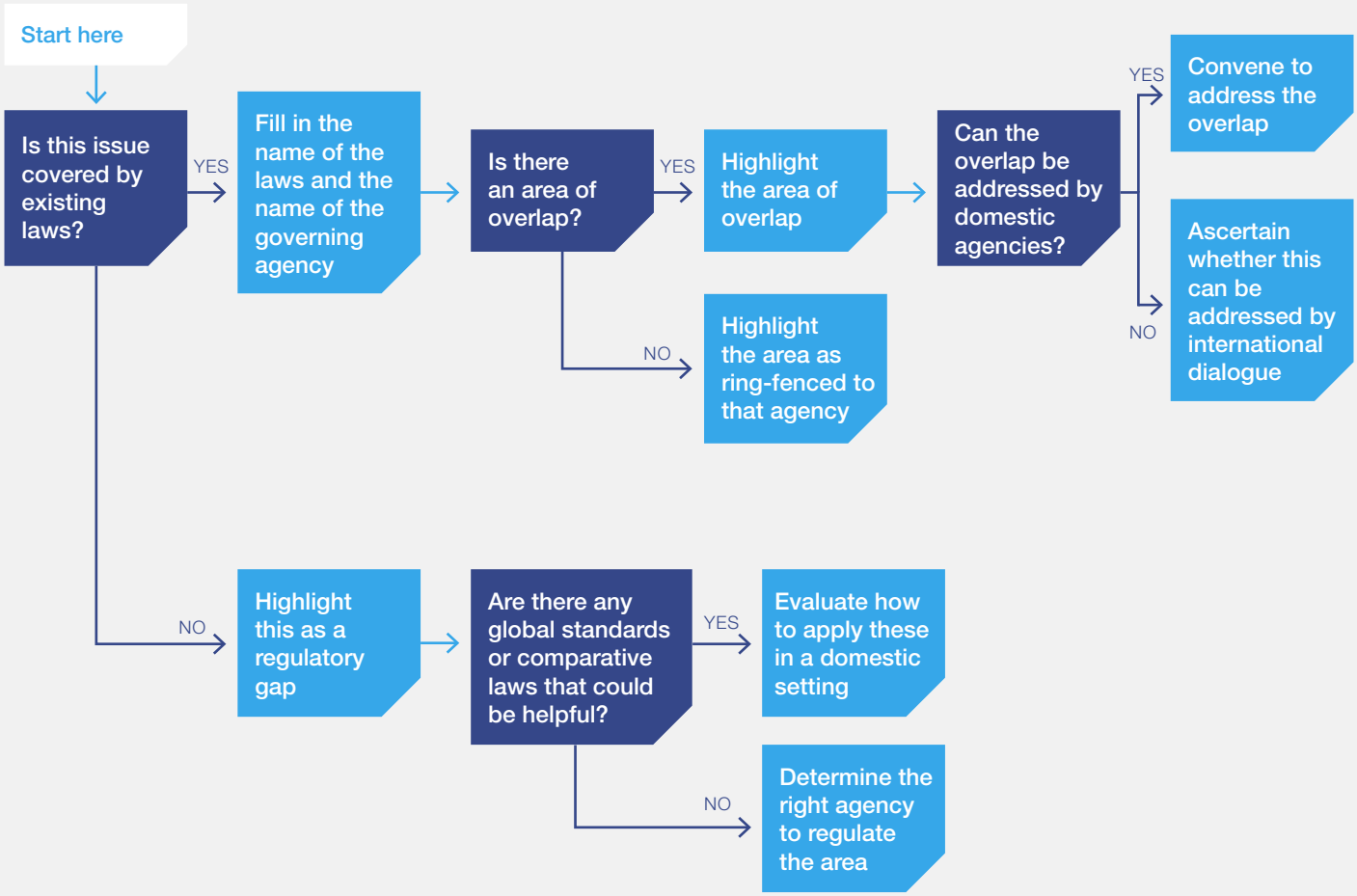
If yes – the risk is covered by existing regulations:

- Fill in the name of the laws and regulations, the relevant provision(s) and the name of the governing agency. Highlight the area as green.
- Is there an area of overlap? Highlight the area of overlap as yellow.
  - If yes, can this overlap be addressed by a domestic agency?
    - If yes, call for inter-agency discussions over the overlapping areas.
    - If no, engage relevant international agencies or those of other countries.
    - If no, mark as issue/risk ring-fenced by the relevant agency.

If no – the risk is not covered by existing regulations:

- Highlight the area of the gap as red.
- Are there any global standards or rules adopted by other countries that could be helpful?
  - If yes, evaluate to what extent the global standards/rules adopted by other countries could help.
  - If no, can this gap be addressed by a domestic agency? Should it be?
    - If yes, identify the relevant agency whose jurisdiction can cover such gap. If no existing agency covers the gap, then discuss if there is a need to create a new agency or assign it to an existing agency.
    - If no, mark as issue/risk ring-fenced by the relevant agency.
    - If no, engage relevant international agencies or those of other countries.

FIGURE 6 **Regulatory and standards mapping: Decision tree**



Conclusion

While both the private and public sectors are actively exploring the full potential of digital currencies, there are regulatory and policy gaps and inconsistencies. Most of these gaps and inconsistencies are a result of the mismatch between the speed of innovation and the pace of regulatory and policy development. To prepare for a future with digital currencies, policy-makers need to consider carefully how they should structure their laws and regulations, as well as how to create both domestic and cross-jurisdictional coordination structures.

A coordinated effort between various agencies within a country and among different countries and organizations could help bridge the gaps and address the inconsistencies, particularly in the areas of combatting financial crimes, privacy, consumer protection and dispute resolutions, where these are most critical. A risk-based regulatory approach can provide more flexibility to accommodate future innovation. While complete future-proofing is impossible in such an ever-evolving landscape for digital currency, premature regulations could stifle productive innovation and limit societal benefit. They could also promote regulatory havens and arbitrage for less-compliant participants, which would have an impact on the benefits these financial innovations may offer.

Given the impacts that regulatory gaps and inconsistencies could have on emerging digital currencies, this paper supports a measured, coordinated, multi-jurisdictional and inclusive approach to the creation and implementation of policy, laws and regulations, which is carefully calibrated to limit the creation of gaps and inconsistencies from the outset. Such an approach would lay the foundation for sustainable innovation, align regulatory frameworks and foster greater levels of international collaboration.

Endnotes

1. If central banks choose to issue retail CBDCs, it is most likely that they will follow a two-tier system to allow the private sector to participate in the distribution and maintenance of accounts for retail CBDCs, while allowing holders of such retail CBDCs to have direct claims against issuing central banks. See: World Economic Forum, *Central Bank Digital Currency Policy-Maker Toolkit*, January 2020, http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit.pdf.
2. Bossu, Wouter et el., *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*, International Monetary Fund, November 2020, https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827.
3. An unhosted wallet is a device to store, send and receive digital currencies, which is not hosted by a third-party financial system. Given an unhosted wallet is completely controlled by its owner, it can be very difficult or sometimes impossible to determine who is accessing or in control of the use of cryptocurrencies in an unhosted wallet. Unhosted wallets allow for anonymity and concealment of illicit financial activity.
4. Financial Action Task Force (FATF), *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*, 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.
5. In addition, if information exchange is not yet built into a network or is not automated, human interaction would be required to obtain the necessary information, which will slow down the speed of transactions using digital currencies and eventually increase costs.
6. The Board of the International Organization of Securities Commissions (IOSCO), *Global Stablecoin Initiatives: Public Report*, March 2020, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf.
7. Financial Stability Board, *Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document*, 14 April 2020, https://www.fsb.org/wp-content/uploads/P140420-1.pdf.
8. Coelho, Rodrigo et al., *FSI Insights on policy implementation No 31: Supervising Cryptoassets for anti-money laundering*, Financial Stability Institute of the Bank for International Settlements, April 2021, https://www.bis.org/fsi/publ/insights31.pdf.
9. Landy, Douglas, "Stabilized: OCC settles debate about regulatory characterization of bank-issued stablecoins", *White & Case LLP,* 21 January 2021, https://www.whitecase.com/publications/alert/stabilized-occ-settles-debate-about-regulatory-characterization-bank-issued.
10. "SEC FinHub Staff Statement on OCC Interpretation", *U.S. Securities and Exchange Commission*, 21 September 2020, https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation.
11. HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*, January 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf.
12. Hansen, Lars Peter, *Challenges in Identifying and Measuring Systemic Risk*, National Bureau of Economic Research, November 2012, https://www.nber.org/system/files/working_papers/w18505/w18505.pdf.
13. The Financial Action Task Force (FATF) has made it clear that CBDCs are not "virtual assets" for FATF purposes, and activities using CBDCs would be "covered as if they were using cash or electronic payments". See: The Financial Action Task Force, *FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, June 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.
14. HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence*, January 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf.
15. Financial Action Task Force (FATF), *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers*, 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.
16. European Systemic Risk Board, *Systemic cyber risk*, February 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.
17. Taylor, Charles et al., *Institutional Arrangements for Fintech Regulation and Supervision*, International Monetary Fund, December 2019, https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Institutional-Arrangements-for-Fintech-Regulation-and-Supervision-48809.
18. Taylor, Charles et al., *Institutional Arrangements for Fintech Regulation and Supervision*, International Monetary Fund, December 2019, https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Institutional-Arrangements-for-Fintech-Regulation-and-Supervision-48809.
19. "Bank of England statement on Central Bank Digital Currency", *Bank of England*, 19 April 2021, https://www.bankofengland.co.uk/news/2021/april/bank-of-england-statement-on-central-bank-digital-currency.

20. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

21. "About GFIN" [Homepage], *Global Financial Innovation Network*, 2021, https://www.thegfin.com/about.

22. "Fintech Cooperation Arrangements", *Commodity Futures Trading Commission*, 2021, https://www.cftc.gov/LabCFTC/FinTechCoopArrangements/index.htm.

23. "Australia-Singapore Digital Economy Agreement", *Australian Government, Department of Foreign Affairs and Trade*, 8 December 2020, https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement.

24. "Ex-ante" can be defined as "based on forecasts rather than actual results". "Ex-post" can be defined as "based on actual results rather than forecasts". Source: Oxford Languages, September 2021.

25. Appaya, Sharmista et al., *Global Experiences from Regulatory Sandboxes*, International Bank for Reconstruction and Development, The World Bank Group, 2020, http://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf.

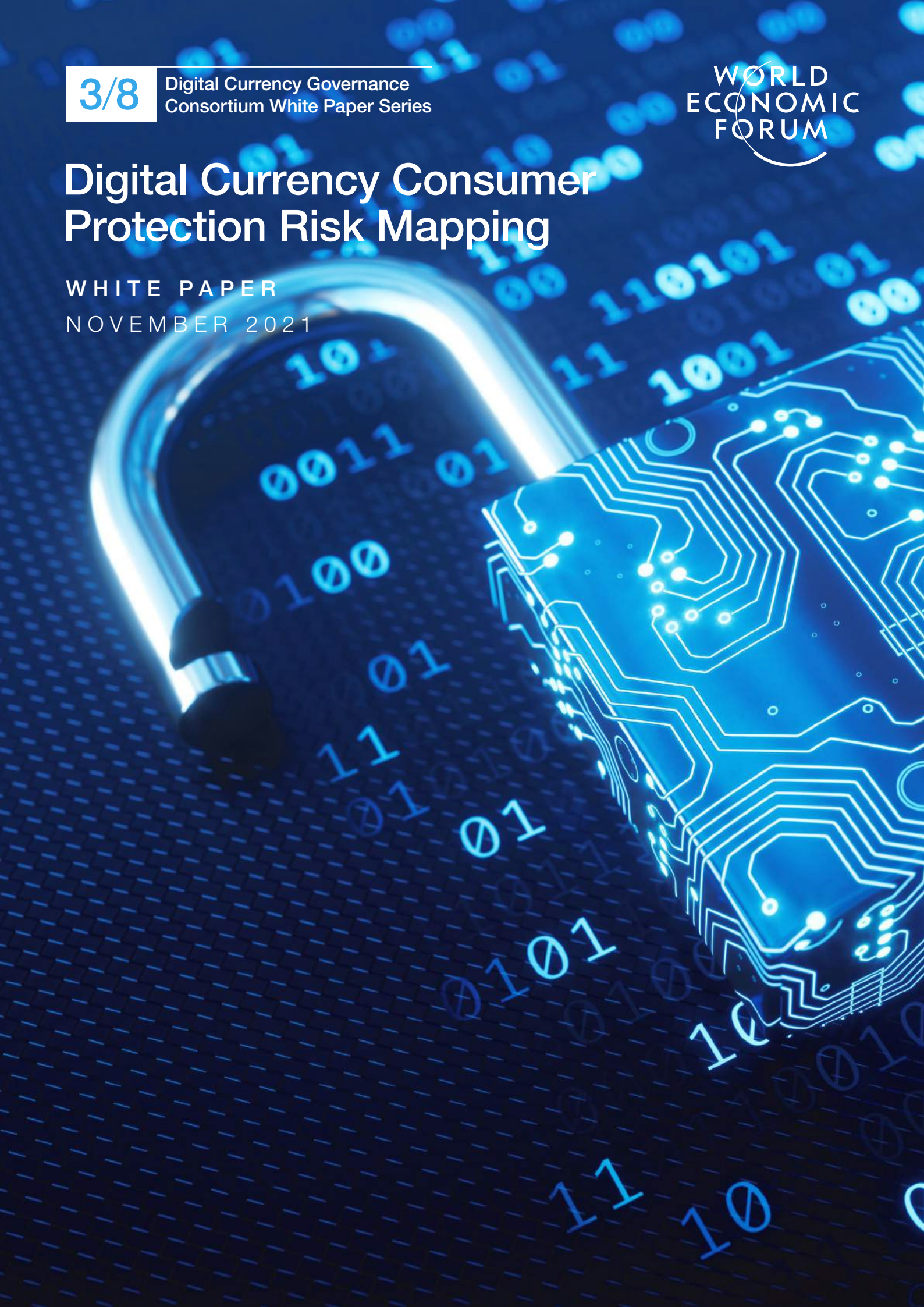
3/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Digital Currency Consumer Protection Risk Mapping

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

Preface 66

1 The risk landscape of digital currencies 67

1.1 Key issues to consider when mapping risks posed by digital currencies 67

1.2 Challenges around consumer protection in digital currency 72

1.3 The general risk to consumers of familiarity without a regulatory framework 73

2 Specific top-line consumer risks 74

2.1 Risks associated with value and backing 75

2.2 Risks associated with inadequate depositor protection 76

2.3 Payment risks 77

2.4 Privacy risks 78

2.5 Security & technology risks 78

2.6 Accountability risks 79

3 Recommendations 80

Conclusion 82

Endnotes 83

Preface

This white paper maps the risks of using various forms of digital currency, compared with existing forms of payment and currency. These insights could inform the drafting of principles for consumer protection for each type of digital currency.

With each advancement in payment technology, consumers face new opportunities, but also new challenges and risks, not all of which are easily perceptible. This was certainly the case with the introduction of e-money, which presented new concerns around information disclosure and variability in regulatory regimes, to name a few.[1] In the context of stablecoins, some of these challenges are already becoming clear, such as ambiguity in redemption rights and schemes backing the valuation. Assuming that consumer trust is critical for adoption, careful consideration of appropriate consumer protections is warranted before central bank digital currencies (CBDCs) or stablecoins are moved into widespread use.[2]

It is important to note that one of the reasons innovation occurs is in response to consumer demand; that is, new approaches are often (though not exclusively) developed to meet a need or provide a new benefit. It is essential to preserve these benefits while also ensuring protection and safety. This balance can be achieved by examining the totality of options available to consumers and assessing the relative risks and benefits that exist within the relevant context. Furthermore, it is important to note the potential for regulation to stifle both competition and innovation if it is not inclusively developed.

This paper sets out a typology of risks to consumers, associated with different digital currencies and different technology and governance options. Our analysis aims to help consumers, consumer-rights advocacy groups and policy-makers to better understand the risks. It also provides some high-level principles to guide policy-makers and regulators in designing an effective and coordinated consumer protection programme, as well as in identifying who owes duties to consumers in this context.

1 The risk landscape of digital currencies

This chapter addresses three broad areas of the risk landscape associated with the introduction of digital currencies:

- Key issues to consider when mapping risks posed by digital currencies
- The notion of consumer protection in digital currency
- The general risk to consumers where newer products mimic legacy products and appear familiar, without the technology underpinning them being subject to a similar regulatory framework

1.1 Key issues to consider when mapping risks posed by digital currencies

As discussed in more detail below, some of the key issues to consider when mapping the risks posed by digital currencies include the following:

- Stablecoins and CBDCs may carry different risks and benefits to consumers
- Risks may differ according to context, including across different types of users
- Not all risks are equal; some top-line consumer risks may warrant special attention
- Different ways of using digital currencies can attract different types of risk
- Accountability can be difficult to determine and enforce in stablecoin ecosystems

Our approach to mapping the risks posed by digital currencies is demonstrated in the graphic at Figure 1.

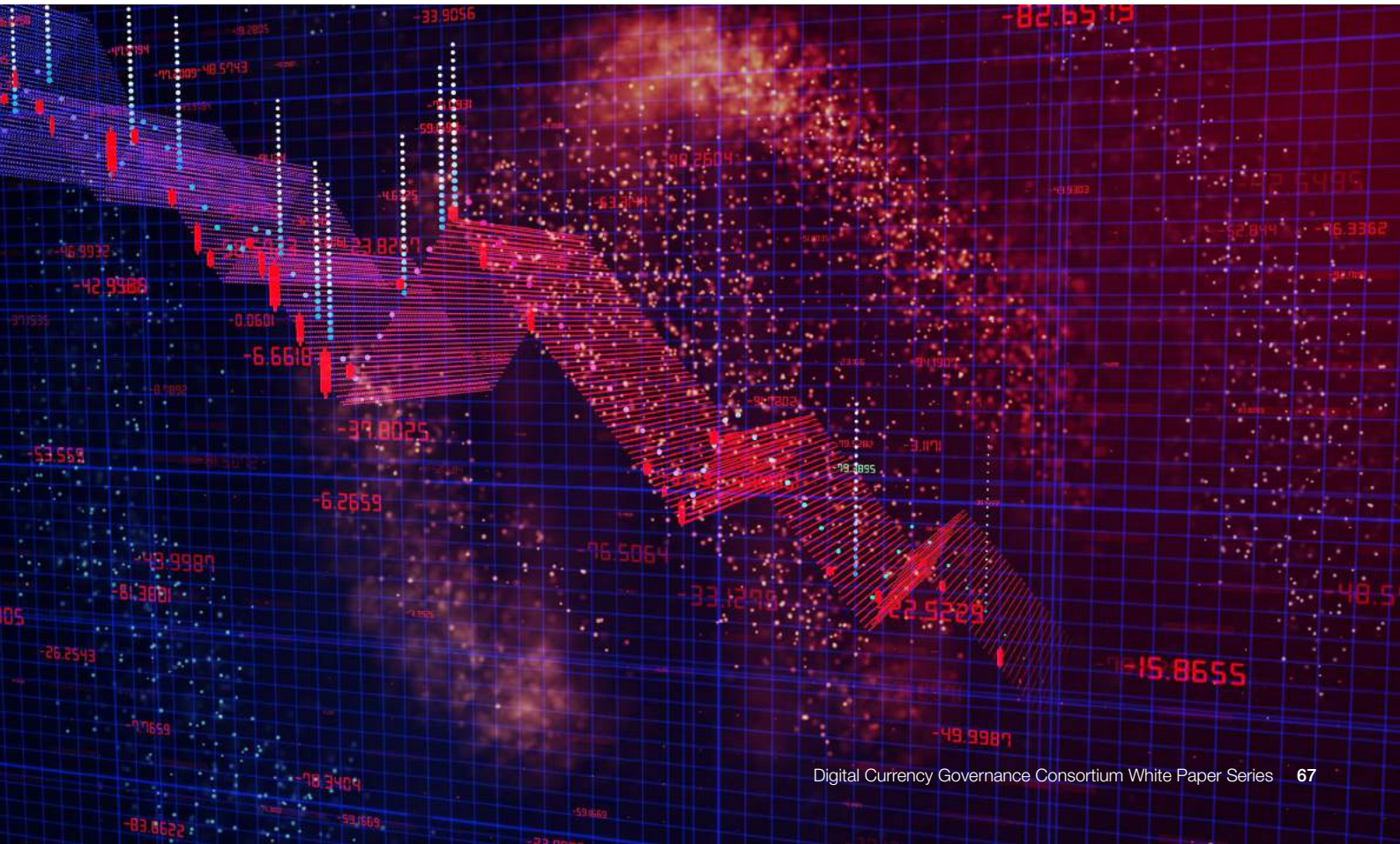
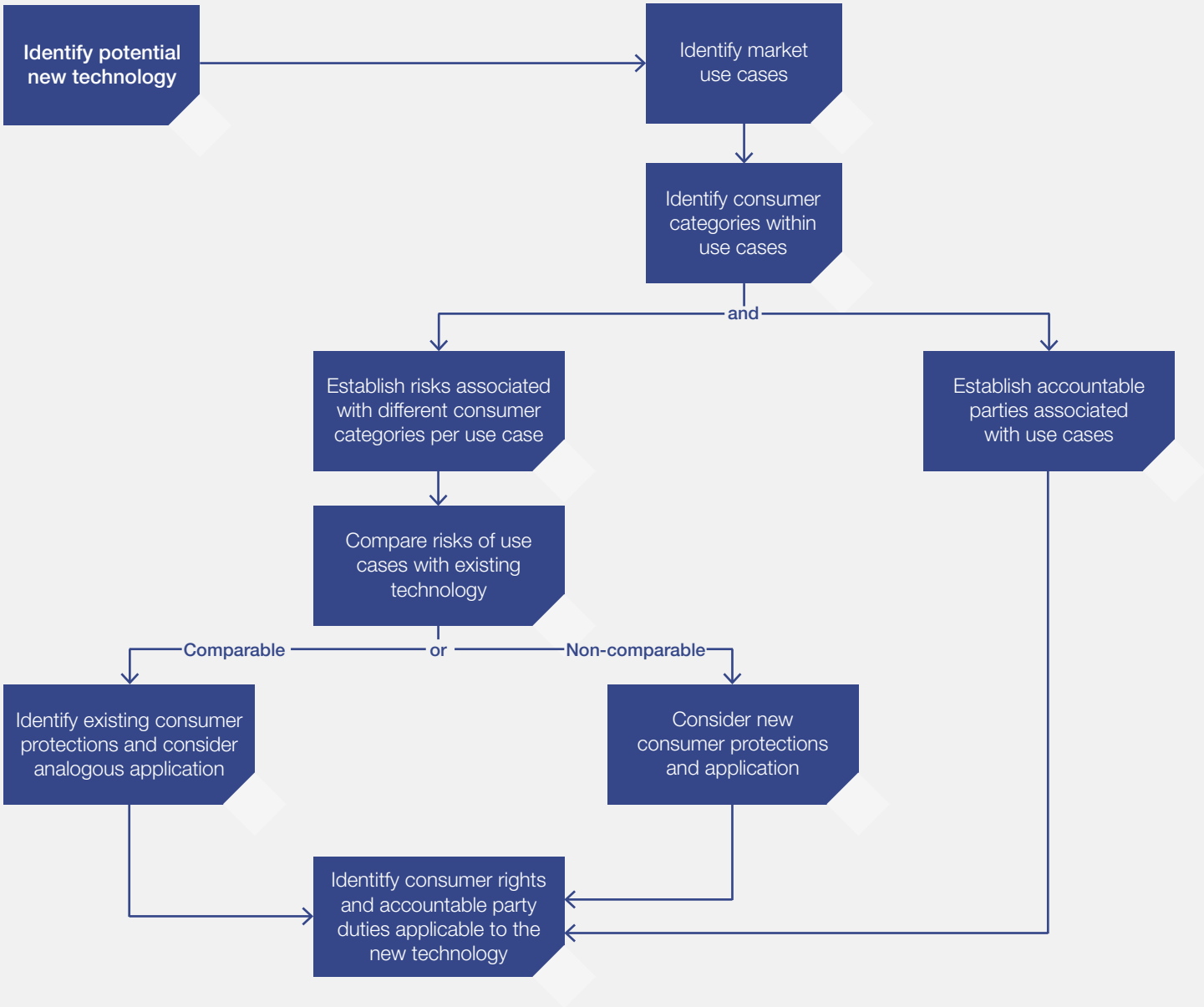


FIGURE 1 | **A suggested approach to mapping the risks posed by digital currencies**



Stablecoins and CBDCs may carry different risks and benefits to consumers

Generally, the risks that consumers face when using stablecoins may be of a different class from those posed by CBDCs. Whereas a CBDC carries the weight of the issuing central bank, a primary concern with stablecoins, in the context of consumer protection, is value and backing. Stabilization methodologies used to maintain the value of stablecoins are affected by a variety of concerns, such as the credibility and willingness of the issuer to maintain the stabilization and reserve backing, the choice of backing mechanism, the types of governance structures, the way the issuance is managed and the redemption and technical choices that are made.[3]

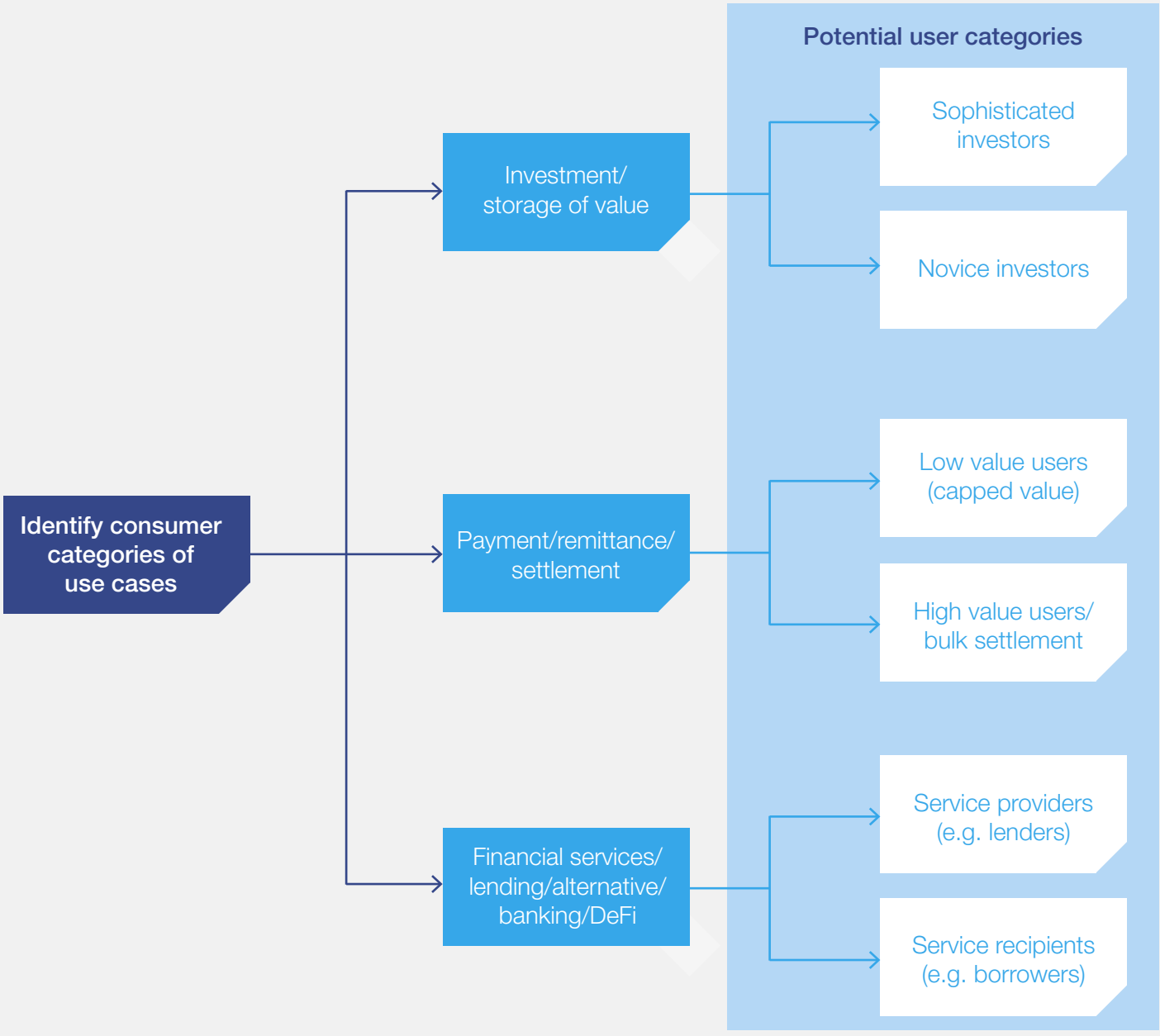
As a CBDC constitutes a direct central bank liability, CBDCs benefit from tested architecture to preserve value. On the other hand, CBDCs may present privacy issues, depending on their design.[4] For a more detailed discussion on potential privacy design choices for CBDCs, please refer to the white paper in this series entitled *Privacy and Confidentiality Options for Central Bank Digital Currency*.

This white paper focuses primarily on *stablecoin* consumer protection issues, while also mentioning where these may be relevant to CBDCs.

Risks may vary according to different types of users

In identifying risks, this paper acknowledges that risks may differ across different types of users. This is particularly true in the case of stablecoins, where some of the applications result in different potential users. In this paper, the term "users" refers to everyone who participates in distributing and holding digital currencies, while the term "consumers" refers to the end-users, whose interests would typically be subject to consumer protection policy and regulation in the face of new technology. Figure 2 shows examples of potential user categories, which may affect choices made in respect of consumer risk mitigation. The figure is not intended to be an exhaustive list, but rather a high-level example of use-case categorization.

FIGURE 2 **An example of potential user categories**



Some top-line consumer risks warrant special attention

In carrying out a mapping of consumer risk areas, an exhaustive approach creates the potential for blind spots and over-comparison, particularly in a new and fast-developing sector. Nonetheless, Figure 3 highlights some top-line consumer risks that warrant special attention, due to their widespread nature and the danger they pose to both the individual consumer and the wider public.

FIGURE 3 | **Top-line consumer risks**

Different ways of using stablecoins can attract different types of risk

Users may employ stablecoins for different purposes and have different levels of involvement in the governance of stablecoin protocols. Stablecoins were arguably invented to enable investors to trade cryptocurrencies and to hold blockchain-enabled assets without suffering from the volatility of cryptocurrency prices in their investments and other activities. Based on a report published by the Block Research in March 2021, the average transaction size for stablecoins was $9,000 in 2020.[5] The high average transaction value suggests that most users of stablecoins are engaged more with investment than retail buying or selling. Depending on their usage and roles, stablecoin users may be exposed to different types of risks.[6]

Figure 4 lays out different uses of stablecoins across different categories of users, along with the associated risks.

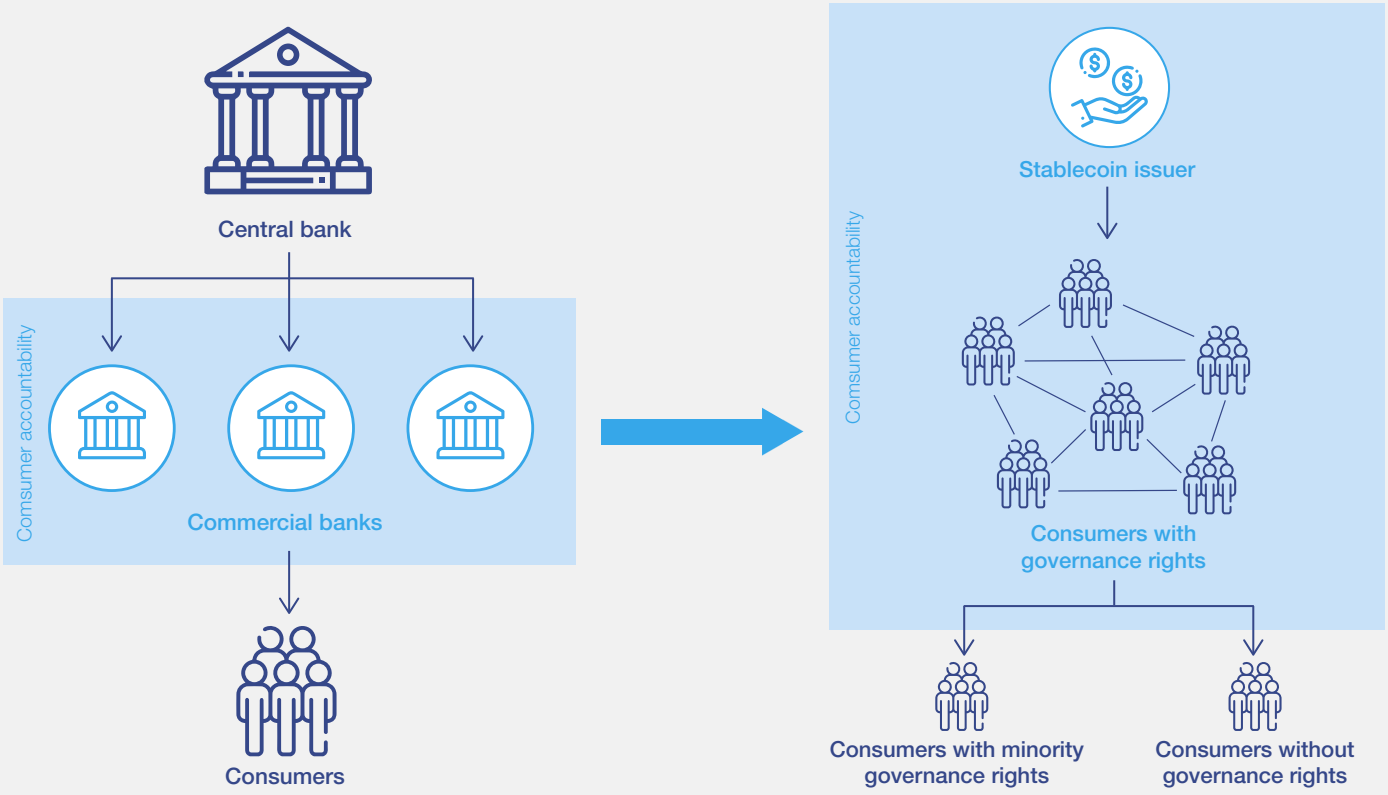
FIGURE 4 | **Risks associated with different uses of stablecoins**

	Investor	Retail buyer/seller	Participant of protocol governance[7]
Stablecoin usage	– Provide capital denominated in stablecoin to earn a return – Park money for future trading of cryptocurrencies	– Exchange for goods/services	– Can be either an investor or a retail buyer/seller
Risk	– Inability to redeem face value – Deposit liability claim – Price volatility	– Inability to redeem face value – Deposit liability claim – Price volatility	– Rights being infringed by majority holders

In stablecoin ecosystems, who should be accountable to consumers?

Owing to more decentralized management, accountability can be difficult to determine and enforce in the case of stablecoins[8]. With traditional central bank systems such as cash, commercial banks – as the distributors of money – provide consumer protections and guarantees,[9] and accountability tends to be easily determinable in bilateral engagements with consumers (see the left half of Figure 5). Policy-makers are now facing a new question: In stablecoin ecosystems, who should be accountable to consumers? (see the right half of Figure 5).

FIGURE 5 | **Who protects consumers in stablecoin ecosystems?**



1.2 Challenges around consumer protection in digital currency

Consumer protection and the challenges that arise when blockchain-based digital currencies are used for the purposes of payment have been addressed by regulators in a variety of ways. Often, initial consumer protection takes the form of restrictions or, in some instances, bans on the use of such digital assets. Several regulators have given warnings to consumers of their risks, as was seen in the growth of Bitcoin, for example.[10] Some jurisdictions, such as China, have gone as far as banning cryptocurrency trading altogether.[11]

In recent years, there have been attempts to draw cryptoassets into existing regulatory frameworks. In June 2019, for example, the Financial Action Task Force (FATF) revised its standards in respect of virtual asset service providers (VASPs), to apply anti-money laundering/combating the financing of terrorism (AML/CFT) requirements to virtual assets and their service providers (this was under review in 2021). The decentralized nature of cryptocurrencies and stablecoins, and how they are used, has often presented the biggest regulatory hurdle, as regulators struggle to determine which among them is responsible for regulation and how to enforce such regulation. These struggles have frustrated the creation of regulatory frameworks. As it is difficult to identify an individual or central organization which consumers can hold to account, protection and regulation have typically targeted the exchange of such assets in and out of fiat, for example crypto-exchanges and banks.

However, the evolution of digital assets and the emergence of privately issued stablecoins have moved the discussion beyond individual consumer risks. There has recently been a greater focus on the potential wider impacts to financial markets and to the public at large, with some pointing to dangers posed by the risk of large price movements or "runs", with rapid selling and withdrawals, particularly where stablecoins may not be fully backed by reserves[12]. The largest stablecoin, Tether – most often used as a medium of exchange in cryptocurrency trading – ties its value to the US dollar and has $62 billion of outstanding tokens at the time of writing. However, it does not fully back its tokens with US dollar reserves and has, at times, held significant shortfalls; it has also been found to repeatedly mislead clients about its reserves.[13]

Beyond the regulation of "on- and off-ramps" at national and supranational levels, proposed legislation is now emerging that seeks to regulate the use of digital assets in financial services.[14] Of course, this begs the question of how the assets are used and which regulator should do the regulating.

"When stablecoins are not fully backed by reserves, it may lead to significant dangers posed by the risk of large price movements or runs

1.3 The general risk to consumers of familiarity without a regulatory framework

Most ordinary consumers do not understand the difference between public money (fiat currencies issued and backed by central banks) and private money (money held in commercial bank deposits, which is a liability of private entities). In particular, the average consumer is often unaware that notes and coins issued by a central bank carry a claim against the central bank, which is passed on once those notes and coins are deposited into a bank account – that is to say, they become private money guaranteed to the extent of the local deposit guarantee scheme.

It is likely that firms in the blockchain industry will provide products and services that are similar in nature to those used by consumers today. This similarity, however, can be misleading as consumers may not understand the different protections (or lack thereof) that apply to different payment services – particularly given the rudimentary understanding of current systems by the average consumer – and may therefore not undertake fully informed risk assessments. For example, a purchase of groceries from a banking application, e-money wallet or stablecoin wallet may require consumers to undertake similar onboarding processes and payment flows. There are likely to be similar security requirements that consumers undertake to access their wallets. However, a payment that is inadvertently sent to the wrong merchant may result in different consequences depending on the payment type and local law.

This creates a risk of familiarity without protection, where equivalent regulatory frameworks have not yet been put in place for digital currency. When consumers perceive payment forms to be similar, they are more likely to behave in the same way as they would with legacy products or services, rather than watching out for new risks or taking care around similar risks in the digital space which lack the regulatory protection provided to legacy products.

2 Specific top-line consumer risks

This chapter addresses the following six top-line consumer risks, identified in Figure 3:

1. Risks associated with value and backing
2. Risks associated with inadequate depositor protection
3. Payment risks
4. Privacy risks
5. Security & technology risks
6. Accountability risks

These risks do not present the same degree of danger across all forms of currency. Before analysing these risks in the context of stablecoins and CBDCs, it is worth considering these same risks within existing systems (see Figure 6). It is important to note that stablecoins and CBDCs are far from monolithic, and design choices can significantly affect both the presence and magnitude of risks. In addition, the areas in red below are areas garnering significant attention from regulators and policy-makers, which could lead to changes that decrease the level of consumer risk.

FIGURE 6 **Comparison of current top-line consumer risks in existing systems and in digital currencies**

	Value & backing risks	Depositor protection risks	Payment risks	Privacy risks	Security & technology risks	Accountability risks
Cash	Backed by central bank	N/A	Fraud and theft	High level of privacy from all parties except direct recipient (payee)	At risk of counterfeiting	Depends on issue; payee responsible for accepting legitimate cash
E-money	Reliant on depositor protection	Two-layer risks (wallet-provider and deposit-taking institution where wallet-providers deposit customer funds)	Typically protected from user error and by debit guarantees	Account-based: dependent on privacy laws of country	Relatively secure and tested	Bank and wallet-providers accountable
Commercial bank money	Same as e-money	High degree of standardized protections and regulation	Same as e-money	Same as e-money	Same as e-money	Bank accountable
Stablecoins	Variety of backing mechanisms which carry different risks[15]	Varied: typically no or limited depositor protections	Limited examples of protections equivalent to bank money or e-money	Varied: governance systems differ on privacy. Many institutions push privacy obligations to VASPs	Varied: audit standards still to be fully developed Varied: Counter-feiting risk in the form of double spend	Unclear - See Fig. 5
CBDC	Same as cash	N/A	Some risk depending on architecture (e.g. in "push" vs "pull" transactions)	Dependent on design & architecture (see Privacy white paper)	Dependent on design & architecture. Early pilots reveal focus on security standards and the prevention of hacking or breach[16] Varied: Counter-feiting risk in the form of double spend or illegitimate copying of CBDC	Central bank accountable

High consumer risk Medium consumer risk Low consumer risk

2.1 Risks associated with value and backing

As discussed previously, stablecoins vary widely in their design, making it challenging to generalize about their risk profile. Detailed analysis of each offering is necessary to evaluate risk. Nevertheless, at present the lack of clear regulatory or other guidance means that it is likely that there will be ongoing challenges in maintaining the price stability of the reference assets of stablecoins. The term "stablecoin" itself can be misleading, as stablecoins may lose their ability to hold steady value relative to their reference asset (see Figure 7) and consumers are not universally guaranteed that stablecoins are free of underlying volatility.

Policy-makers will need to consider whether deposit insurance is appropriate in the same way as required for regulated financial institutions

With traditional currencies, consumers expect to be able to redeem the value of their deposits on a 1:1 basis, at any time. However, where proceeds from a stablecoin sale are held not in a depository account but in financial assets, such as securities or government bonds, with varying levels of risk exposure (which may not fully back outstanding stablecoins), the value of the stablecoin is also subject to such risk exposure. In addition, a lack of regulatory guidelines on the relevant governance and risk management policies of the issuer and its reserve management creates further risk exposure, which is not present with traditional bank deposits. This is further exacerbated by a lack of standardization of terms such as "stable", "backed by" or "backing" used in the marketing of many privately issued stablecoins. These terms often oversimplify the complex and varied forms of stablecoin collateralization, which include the following:

- **100% backed by funds**:[17] where stablecoins are backed by reserve funds that the stablecoin-issuer or custodian holds for safekeeping, implying a commitment to their full redeemability in fiat currency.
- **Off-chain collateralization**: where stablecoins are backed by assets held off the distributed ledger, often with a custodian for safekeeping.
- **On-chain collateralization/crypto-backed**: where stablecoins are backed by assets on the distributed ledger, which are capable of being recorded in a decentralized manner on the blockchain and may not require a custodian.
- **Algorithmic collateralization**: where stablecoins are backed using some form of price stabilization algorithm to track a particular unit price (usually linked to the US dollar) and where such backing is reliant on the expectations of users on the future purchasing power of their holdings. This form of backing does not need the custody of any underlying asset; it operates fully on-chain and in a decentralized manner.

These different forms of backing carry with them different consumer risks.[18] Figure 7 sets out these different types of stablecoin collateralization and their associated risks to the consumer.

FIGURE 7 **Different ways of backing stablecoins and their potential risks**

	100% backed by funds	Off-chain collateralization	On-chain collateralization	Algorithmic collateralization
Is there an accountable party if there is an issue with the backing mechanism?	Yes	Yes	No (replaced with smart contract)	No (replaced with smart contract)
Potential consumer risks	Fraud and operational risk (e.g. insufficient funds to quickly meet redemptions) High risk and susceptible to confidence crises or a run on the stablecoin if the funds are not legitimate or sufficiently liquid	Linked to underlying collateral and dependent on whether that value is fixed or fluctuates	High risk as collateral is volatile by nature	High risk and susceptible to confidence crises or a run on the stablecoin

For each type of stablecoin backing, it is important to be clear on whether and to what extent the consumer bears the risks associated with that collateralization. Where a redemption based on a fixed ratio is guaranteed, the issuer will typically bear liability for fluctuations from the fixed redemption price resulting from its reserve assets' risk exposure. Such an approach is more akin to traditional bank deposits and can inspire greater consumer confidence (even though most commercial bank deposits have deposit insurance protecting against risks such as theft or bank bankruptcy).

However, where the consumer bears the risk, the value of the stablecoin in the consumer's hands will fluctuate in line with the underlying reserve asset. Such exposure could dissuade widespread adoption, influence consumer confidence and result in mass withdrawals, destabilizing the value of the stablecoin further. This is amplified by the fact that, in such mass withdrawal events, consumers are unlikely to be protected by the traditional depositor scheme protections available for bank deposits or benefit from central bank protection as the lender of last resort. Other circumstances which could trigger mass withdrawals include the circumstances of the issuer, such as a change in governance or critical rules, or technological risks such as cyberattacks.

It is crucial for issuers to be transparent about forms of backing and their associated risks, and for consumers to be properly educated on the underlying value protections (or lack thereof) when compared to traditional bank deposits or e-money. Consumers will also need to be informed of new risks, such as those mentioned above, and how these may trigger a crisis of confidence among users that threatens the "at par" redeemability of stablecoins. Lastly, issuers should inform consumers of whether the redemption value is fixed at par and who bears the risk with respect to the volatility of the underlying assets. The practical feasibility of such education and transparency measures also needs to be assessed from jurisdiction to jurisdiction, as for some it may be more expedient and cost-effective to consider some form of "qualified investor" threshold instead.

2.2 Risks associated with inadequate depositor protection

> In the case of bankruptcy of the depository institution, e-money consumers may only get back a portion of their money unless the e-wallet or mobile wallet-providers are sufficiently capitalized

Deposit insurance is designed to protect consumers from the risk of bankruptcy of deposit-taking financial institutions. When it comes to e-money, there are two layers of consumer risks with respect to the money held by e-wallet service providers, which may also apply to digital currencies if they are held in a custodial account:[19]

- Risk of bankruptcy of the e-wallet service provider
- Risk of bankruptcy of the deposit-taking institution where the e-wallet service provider deposits its customers' funds

To address the first risk, countries often require e-wallet service providers to be sufficiently funded and to set aside a certain percentage of their fund liabilities in a custodian account with a deposit-taking financial institution. Since e-money providers do not typically leverage their balances, policy-makers will need to consider whether deposit insurance is appropriate in the same way as required for regulated financial institutions. A limited number of jurisdictions require e-wallet-providers to obtain a banking licence and subject all consumer accounts to deposit insurance, hence protecting e-wallet-providers from bankruptcy. China goes a step further by requiring e-wallet or mobile wallet-providers to deposit 100% of their customers' funds either with a commercial bank or with the central bank. In the European Union (EU), if e-wallet or mobile wallet providers purchase private insurance to cover any unfunded liabilities, they would not need to deposit customers' funds with an insured depository institution.[20]

In jurisdictions where banking licences are not required for e-money services, balances in e-wallets or mobile wallets are not considered as deposits and e-wallet-providers are usually not required to obtain deposit insurance to cover individual accounts they hold.[21] While e-wallet or mobile wallet-providers may deposit their customers' funds with an insured depository institution, the custodian account is protected up to the coverage limit of the deposit insurance. In the case of bankruptcy of the depository institution, e-money consumers may only get back a portion of their money unless the e-wallet or mobile wallet-providers are sufficiently capitalized.

Limited jurisdictions, such as the US, offer a "pass-through" approach, which allows each individual e-money account to be covered by the coverage limit of the deposit insurance.[22] The "pass-through" approach offers more protection to individual e-money consumers against the bankruptcy of depository institutions. In the case of emerging economies such as Kenya, the electronic value must be backed by a corresponding value in bank accounts. These bank accounts are essentially trust accounts that should ideally be independent and ring-fenced from any possible bankruptcy of the e-wallet provider. The challenge with this approach is that, for deposit protection purposes, the bank trust account is treated as one account and may not compensate the various underlying wallet holders. To mitigate this risk, regulators set stringent conditions for these funds to be held in various reputable and financially sound banks and invested in liquid assets, particularly government securities.

2.3 Payment risks

Different payment methods carry different consumer protections. For example, cash is 100% guaranteed by a central bank, and typically carries the status of legal tender. However, cash provides no inherent user protection in the case of loss or theft.

When placed into an account with a commercial bank, cash transforms into commercial bank money and is guaranteed, in the event of bank insolvency, to the extent of (for example) the applicable deposit guarantee schemes. Payments made using commercial bank money in many jurisdictions carry with them varying degrees of regulatory consumer protection for bank error, user error and debit guarantees, such as the Direct Debit Guarantee in the UK (a consumer reassurance system which provides protection for payment errors).[23] Although these protections are still to some degree reliant upon consumers identifying an error and making a claim, protections such as deposit insurance and the oversight of monitoring and regulatory authorities remain available.

When cash and commercial bank money is used to purchase electronic money, it becomes electronic money or "e-money". Within the EU and UK, for example, electronic money has the same regulatory protections as payments made with commercial bank money and benefits from the right of at-par redeemability.

Stablecoins that are not considered e-money at present carry no similar regulatory consumer protections for payments. For instance, under the proposed EU regulation on Markets in Crypto-assets (MiCA),[24] fewer consumer protections are available for payments made with tokens that are stabilized using assets (asset-referenced tokens or stablecoins) than for payments made with e-money tokens,[25] since asset-referenced stablecoins do not fall within the definition of funds under Payment Services Directive 2 (PSD2 – the European directive for electronic payment services).[26] This gap in protections for payments using stablecoins was identified an issue to be addressed in the recent UK consultation for a regulatory framework for cryptoassets and stablecoins.[27]

Even though both CBDCs and stablecoins are generally intended by their creators to serve as a payment medium similar to cash, bank money and e-money, some functionalities of CBDCs and stablecoins may differ from existing options and are worth highlighting to consumers. The "push" versus "pull" distinction in terms of payment mechanism is a good example. A push transaction refers to a transaction where it is initiated by the payer, who needs to know the name of the payee's financial institution and their account number. A pull transaction refers to a transaction where it is initiated by the payee and the payee needs to know the name of the payer's financial institution and their account information.

While both types of transactions are subject to cybersecurity risks,[28] a push transaction is fundamentally less risky than a pull transaction for both the payer and the payee, since only the account with sufficient funds could make the transaction happen. In contrast, a pull transaction could bounce because the payee has no visibility of the balance the payer has in his or her account. Currently, it is debatable whether transactions made in stablecoins will be push-only transactions, given the technology may enable automatic payment upon fulfilment of certain conditions. By contrast, transactions made through cards and bank accounts can be either push or pull transactions. Depending on their technical choice and how accounts are structured, CBDCs may facilitate either push or pull transactions.

2.4 Privacy risks

Given that stablecoins are typically privately operated, they are susceptible to business practices and models prevalent in the technology industry. For example, this may include business practices developed in unregulated environments or include models without robust privacy protection. Given the highly intimate nature of transactional data, transparency around the information-handling practices of stablecoin-issuers will be of paramount importance in supporting end-user protections and trust.

The Group of Seven (G7), the International Monetary Fund (IMF) and the Bank for International Settlements (BIS) have jointed called for regulators to subject stablecoin-issuers to applicable data protection and privacy laws and regulations.[29] This goes beyond the issuer itself, as mere internal policy may be insufficient in providing adequate protection, given that many wallet operators in stablecoin ecosystems are third parties to the issuer and may have local legal obligations for data retention. This creates an accountability dilemma in stablecoin ecosystems, as well as the potential for stablecoin-issuers to adhere to robust privacy standards as issuers, yet also operate parallel business operations as wallet-providers according to differing standards.

The choice of third-party wallet-providers and other application-level developers or operators may also have an impact on trust in stablecoin networks and create confusion among consumers regarding accountability for their data and the consequences of data breaches. This risk is heightened in the context of stablecoins. Both a loss of trust in the issuer and a significant data breach of its ecosystem have the potential to result in a crisis of confidence among users, which could have a knock-on effect on a stablecoin's value and deposit-protection mechanisms.

Outside stablecoin ecosystems, a further risk to privacy has emerged in respect of surveillance by blockchain analysis companies. These are organizations that analyse on-chain transactions and can match such data with other publicly available data. A variety of cryptoasset ledgers are already under significant surveillance by such organizations[30]. Given the permanent nature of on-ledger transaction history and behaviours, the robustness of a stablecoin infrastructure against such surveillance will play a significant role in its ability to protect consumer data and privacy.

> Stablecoin-issuers will need to demonstrate a high degree of transparency and clarity in their data-handling practices and de-identification techniques

Given the highly sensitive nature of transactional data and ease of re-identification and external surveillance – plus the risk of a compounded effect on value of a loss of confidence resulting from, for example, a data breach – stablecoin-issuers will need to demonstrate a high degree of transparency and clarity in their data-handling practices and de-identification techniques, not only internally but in their wider ecosystems. Safeguards will need to be put in place in respect of external service providers and their ability to influence consumer sentiment, to prevent external risks affecting value. Stablecoin-issuers may also need to consider protective measures against external surveillance of their ledgers. For more detailed discussions on privacy-preserving technology, refer to the white paper in this series entitled *Privacy and Confidentiality Options for Central Bank Digital Currency*.

2.5 Security & technology risks

Several issues must be addressed with regard to how security protocols are designed, as well as how they are technically implemented. Poor technical design, such as bugs in smart contract code or poor security design choices, may also have a serious impact on consumers and expose them to loss.

Given that a detailed technical understanding of the systems underlying digital currencies will be beyond the average consumer, appropriate technical and audit standards may be necessary to neutralize technical impediments which can indirectly cause consumer risk. Nevertheless, the value of greater digital literacy among consumers should not be understated: it could play a significant role in helping consumers themselves to reduce the impacts of technical errors or issues. Policy-makers should consider the following issues:

- Variations in the digital literacy of consumers and how this may reduce or catalyse consumer risks
- How to standardize ways of conducting technical audits
- How to increase consumer understanding and transparency so that an informed choice is possible

2.6 Accountability risks

The identification of who is accountable to consumers for consumer risks is crucial and a core issue in respect of the consumer protections associated with stablecoin-issuers. Unlike traditional currency options, the decentralized architecture and governance models of digital currencies can make it difficult to find the right party to be accountable. Three primary instances emerge that require special consideration:

- Where decentralized architecture is used
- Where other consumers can influence rule changes
- Where issuers delegate responsibility of consumer engagement to wallet-providers and other VASPs

Decentralized architecture

Where a decentralized architecture is used for a stablecoin's protocols, particularly where rules (such as those governing reserves) can be altered after being set up by an issuer, there is the potential risk of a lack of a legal causal link with the stablecoin-issuer. The question arises as to whether a consumer would be able to hold such an issuer accountable in respect of losses suffered by the consumer resulting from such rule changes. Policy-makers will need to consider whether the policy imperative in relation to such issuers requires a form of legislated strict liability to hold issuers accountable to consumers in such instances.

Consumer ability to alter rules

Similar to the scenario above, a further question arises when consumers themselves are able to alter rules associated with the relevant stablecoin. Unlike e-money or cash, consumers may play a more active role in the process of creating and maintaining some stablecoins, in that they can propose and approve new governance rules. In this capacity, consumers act in a similar manner to shareholders of a company. Some mechanisms of company laws and securities laws, especially those designed to protect minority shareholders from infringement of majority shareholders, could be considered to protect consumer rights with respect to their roles in governance rules-making. Existing tort laws could provide some form of protection for consumers if the code-writers or issuers fail to honour their governance rules changes.

Delegation to VASPs

Many stablecoin-issuers that are not consumer-facing may take the approach of delegating consumer protection responsibilities to wallet-providers and other VASPs, which interact more directly with consumers. Policy and regulatory considerations will need to address such practices to ensure they do not result in supply-chain gaps in accountability to consumers.

3 Recommendations

The recommendations below include approaches and measures to improve consumer protection for different types of digital currency; they are primarily for the attention of policy-makers and regulators.

Same activity, same risk, same regulation

The regulatory approach to addressing the risks of digital assets should balance the need for both competition and innovation, and ensure a level playing field for all participants in the broader payments ecosystem. This is best achieved with the principle of "same activity, same risk, same regulation". Applying this principle would provide a consistent approach to consumer protection across the regulated and currently unregulated sectors, and would increase opportunities for both new and existing actors to provide safer and better services across the financial ecosystem.

> Consumer education needs to be carried out by neutral and trusted parties to ensure a consistent and objective approach, free of marketing influence

Consumer education

To minimize potential negative impacts of stablecoins on consumers and to enhance their wider adoption beyond simply facilitating payments for cryptocurrency trading, it is important to carry out consumer education to ensure people understand risks as well as their legal rights. Effective consumer education would include highlighting the different risks that stablecoins present compared not only to other stablecoins and digital currencies but also to existing currency options. Consumer education needs to be carried out by neutral and trusted parties to ensure a consistent and objective approach, free of marketing influence.

New or developed regulation and audit

Different types of reserve assets expose consumers to different types of risks. For stablecoins with fiat currencies as a reserve asset, they are exposed to risks related to reserve management along with potential inflation of fiat currencies and bankruptcy of deposit-taking institutions. There is also a transparency-related risk that consumers may have difficulty in verifying the existence of adequate reserves.

For stablecoins that choose cryptocurrencies as reserve assets, the risk lies in the price and fundamentals of the reserve cryptocurrency. Such a structure is similar to loans secured by publicly traded securities, which are considered a type of derivative under US laws. To ensure sufficient protection, the US margin loan laws and regulations require the underlying securities to have twice the value of the loan amount to allow sufficient room to absorb market shocks. Many stablecoins with cryptocurrency backing are overcollateralized; even so, given the often violent price swings in cryptocurrency markets, this overcollateralization still may not provide adequate backing.[31]

Limiting stablecoins to high-asset or high-income constituents or institutions may hinder the financial inclusion value proposition of stablecoins. Nonetheless, underserved populations are potentially at greater risk of inadequate understanding and consequent losses. Policy-makers can consider certain types of protections, including:

- Setting limits to the sizes of transactions and wallet balances, to limit the risk exposure of consumers
- Framing auditing and disclosure requirements to ensure the value of stablecoins is indeed what the issuer claims them to be; this could incentivize stablecoin-issuers to provide robust disclosure as a way to gain trust with individual consumers

Policy-makers may also need to consider how stable the value needs to be for a digital currency to qualify as "stablecoin" and what kinds of assets can be used as underlying assets. Depending on the risk level of different types of underlying assets, further consideration should be given to whether a given product is fit for the general public and what the appropriate transaction or balance limits should be. This risk-based approach could provide sufficient protection while not crushing innovation. There is also the question of where the reserve should be kept in order to provide sufficient protection and transparency, for example with central banks, commercial banks or digital currency exchanges.

Authorization and supervision

Firms that offer financial services or cash are often authorized and supervised by a local regulator, a central bank or an independent body. Historically these entities have generally been banks, but more recently payment and e-money institutions have been able to provide consumer-facing payment services.

As new firms come to market with a stablecoin offering, consideration should be given to the regulatory umbrella under which these services will be provided, as well as which functionaries will be responsible within this framework for the procedural implementation of regulations, authorization for certain activities and supervision. Stablecoin and CBDC services are often seen through the lens of the two-tier model of issuance and distribution. This gives rise to a number of activities that need to be considered for the purposes of consumer protection, such as those set out below:

Payment services

Firms that wish to provide consumers with payment services in stablecoins or CBDC should be authorized and supervised for the provision of such services.

Distribution

The appropriate regulatory framework for distribution will be different for CBDCs and stablecoins as outlined below.

For CBDCs, the distribution of central bank money might follow the current two-tiered structure, whereby access to central bank money is provided and made available via private-sector institutions (such as commercial banks). Policy-makers will need to consider possible future frameworks for such distribution and for new types of participants (e.g. non-banks such as VASPs), and whether new rules would be required to address varying risk profiles. Either way, the applicable supervisory regimes would need to apply proportionately to bank and non-bank firms that have access to central bank money in the form of a CBDC or that play a role in its distribution or custody.

Stablecoins will be distributed through models similar to those seen in e-money ecosystems, so current e-money legislation may be a suitable framework for such distribution. Where services are related to stablecoins, it would be appropriate to consider the need for additional operational risk or security requirements for the distribution of such stablecoins.

Custody

Requirements around the custody of a CBDC or a stablecoin is one of the most critical areas of regulation that will need to be clarified for consumer protection. For example, existing regulatory frameworks, such as the EU's PSD2,[32] do not currently apply expressly to custodial wallet services. Furthermore, while the European Commission's recent proposal to regulate markets in cryptoassets (MiCA)[33] would introduce requirements for custodians of private cryptoassets, it does not apply to the custody of a CBDC.

Ultimately, for a CBDC or stablecoin held in a digital wallet, the key management practices, security standards and ability of the wallet to support mixed payment functionality may all raise issues around the applicability of an existing regulatory framework to the custody of digital assets. Policy-makers will need to decide on a regulatory framework for custodial wallets with the necessary consumer and insolvency protections for such custody.

Conclusion

Consumers of digital currencies are not homogenous and vary significantly in risk profiles and tolerances, across both products and jurisdictions. Similarly, digital currencies, including stablecoins and cryptocurrencies, vary meaningfully in their setup, design and risk exposure. Although risks can be broadly identified, it will be up to policy-makers to match these to local market use cases to design or develop appropriate regulatory protections. What is clear is that such protections are indeed necessary. Stablecoins, the focus of this paper, introduce new opportunities but also new consumer risks into environments that are historically heavily regulated and centrally controlled.

At the same time, there is currently a lack of clarity around accountability and available options for redress. Solving this challenge will be one for policy-makers and stablecoin-issuers alike, and should be a priority as wider consumer adoption occurs. Designing an approach that allows for both innovation and experimentation in this new and growing industry,[34] while ensuring that consumers do not suffer undue or even catastrophic loss during the course of that experimentation, is a challenge that will require innovative modes of policy-making and public-private cooperation. In addition, consumer education will be a critical component in ensuring that consumers can make informed decisions that match their needs without exposing them to undue risk.

Endnotes

1. OECD, *Report on Consumer Protection in Online and Mobile Payments*, *OECD Digital Economy Papers No. 204,* 2012, http://dx.doi.org/10.1787/5k9490gwp7f3-en.
2. However, consumer protection issues exist, particularly for stablecoins, regardless of scale. See: G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.
3. G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.
4. Allen, Sarah et al., *Design choices for Central Bank Digital Currency: Policy and technical considerations,* Brookings Institute, Global Economy & Development Working Paper 140, July 2020, https://www.brookings.edu/wp-content/uploads/2020/07/Design-Choices-for-CBDC_Final-for-web.pdf.
5. "Stablecoins: Bridging the Network Gap Between Traditional Money and Digital Value – Brought to you by GMO Trust", *The Block Crypto*, 10 March 2021, https://www.theblockcrypto.com/post/97769/stablecoins-bridging-the-network-gap-between-traditional-money-and-digital-value-brought-to-you-by-gmo-trust.
6. G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.
7. A "participant of protocol governance" is a holder of a stablecoin who has the ability to vote on the protocols governing the stablecoin.
8. World Economic Forum, *Bridging the Governance Gap: Dispute resolution for blockchain-based transactions*, December 2020, https://www.weforum.org/whitepapers/93bd1530-0ded-48fa-8dee-e9b2d109d84d.
9. In this generalized example, we ignore more complex financial services and financial market complexities, even though these also form part of the traditional systems and stablecoin ecosystem alike.
10. "Countries Where Bitcoin Is Banned or Legal In 2021", *Cryptonews,* August 2021, https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm. Note: the map in this article shows China as a country where bitcoin is legal – however on 24 September 2021, Reuters reported that China had banned all crypto transactions and mining, including bitcoin.
11. On 24 September 2021, Reuters reported that China had banned all crypto transactions and mining, including bitcoin. See: https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/.
12. Schonberger, Jennifer, "Treasury looks at run risks in stablecoins, pushes for new rule proposals", *yahoo!finance*, 15 September 2021, https://news.yahoo.com/treasury-looks-at-run-risks-in-stablecoin-pushes-for-new-rule-proposals-193053375.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKDA7qtrvFXvWYRrjcUwiDHw2igO3ugCjzN5vnjDli2_NOYQNFoPdvdl3TRC9DFZVkyT1ebHZf1GNixPt4HPkGE3DgpCHj6m78uCkrOm0iM85MYN0vrhXuFzLXXxYMv0lMMuV4d-ltUFx9XRmqFZl-rpmQ3ZOtkzuf9s0kF1KjMa.
13. For example, see:

    1) "Reserves Breakdown at March 31, 2021", *Tether,* https://tether.to/wp-content/uploads/2021/05/tether-march-31-2021-reserves-breakdown.pdf.

    2) "Independent Accountant's Report: To the Board of Directors and Management, Tether Holdings Limited", *Moore Cayman,* 6 August 2021, https://tether.to/wp-content/uploads/2021/08/tether_assuranceconsolidated_reserves_report_2021-06-30.pdf.

    3) "Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York", *Letitia James, NY Attorney General,* 23 February 2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.
14. For example, see:

    1) European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Cryptoassets, and amending Directive (EU) 2019/1937,* 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

    2) Singapore Government, *Payment Services Act,* 14 January 2019, https://www.mas.gov.sg/regulation/acts/payment-services-act.
15. For example, cryptocurrency-backed stablecoins bear a far greater risk than stablecoins backed using reserves or central bank RTGS accounts.
16. For example, see Minwalla, C., "Security of a CBDC", *Bank of Canada*, June 2020, https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/.
17. Referred to by the European Central Bank (ECB) as "tokenised funds" in: Bullmann, Dirk et al., *In search for stability in cryptoassets: are stablecoins the solution?,* European Central Bank, 2019, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf.
18. It should be noted that there is always a potential risk of a run on a traditional currency, although this is not specifically mentioned.

19. The definition of e-wallet here includes e-wallets that rely on SMS messaging and app-like e-wallets.

20. Oliveros, Rosa and Pacheco, Lucia, *Protection of Customers' Funds in Electronic Money: a myriad of regulatory approaches*, BBVA Research, 28 October 2016, https://www.bbvaresearch.com/wp-content/uploads/2016/10/Safeguardingelectronicmoneyfunds_en.pdf.

21. Ehrentraud, Johannes, et al., *Policy responses to fintech: a cross-country overview,* Bank for International Settlements, January 2020, www.bis.org/fsi/publ/insights23.pdf.

22. Oliveros, Rosa and Pacheco, Lucia, *Protection of Customers' Funds in Electronic Money: a myriad of regulatory approaches*, BBVA Research, 28 October 2016, https://www.bbvaresearch.com/wp-content/uploads/2016/10/Safeguardingelectronicmoneyfunds_en.pdf.

23. "The Direct Debit Guarantee: What Does it Really Mean?" *ClearDebit*, 18 February 2013, https://cleardirectdebit.co.uk/the-direct-debit-guarantee-what-does-it-really-mean.

24. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

25. "Electronic money token" or "e-money token" means a type of cryptoasset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender.

26. European Commission, *Payment services (PSD2) – Directive (EU) 2015/2366*, 12 January 2016, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

27. HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence,* January 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf.

28. "Deep Dive: The Benefits And Challenges Of Real-Time Push Payments", *PYMNTS.com*, 26 September 2019, https://www.pymnts.com/news/faster-payments/2019/benefits-challenges-real-time-push-payments-pull/.

29. G7 Working Group on Stablecoins, *Investigating the impact of global stablecoins*, October 2019, https://www.bis.org/cpmi/publ/d187.pdf.

30. Powers, Benjamin, "'Digital Mercenaries': Why Blockchain Analytics Firms Have Privacy Advocates Worried", *CoinDesk*, 14 September 2021, https://www.coindesk.com/tech/2020/11/04/digital-mercenaries-why-blockchain-analytics-firms-have-privacy-advocates-worried/.

31. As was experienced with MakerDAO's DAI when the price of the cryptocurrency ether (ETH) rapidly fell in March 2020, despite DAI being pegged 1:1 to the US dollar and over-collateralized with ETH.

32. European Commission, *Payment services (PSD2) – Directive (EU) 2015/2366,* 12 January 2016, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

33. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, 24 September 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

34. "Top Stablecoin Tokens by Market Capitalization", *CoinMarketCap*, https://coinmarketcap.com/view/stablecoin/. As of 19 October 2021, the market capitalization for stablecoins had reached over $130 billion.

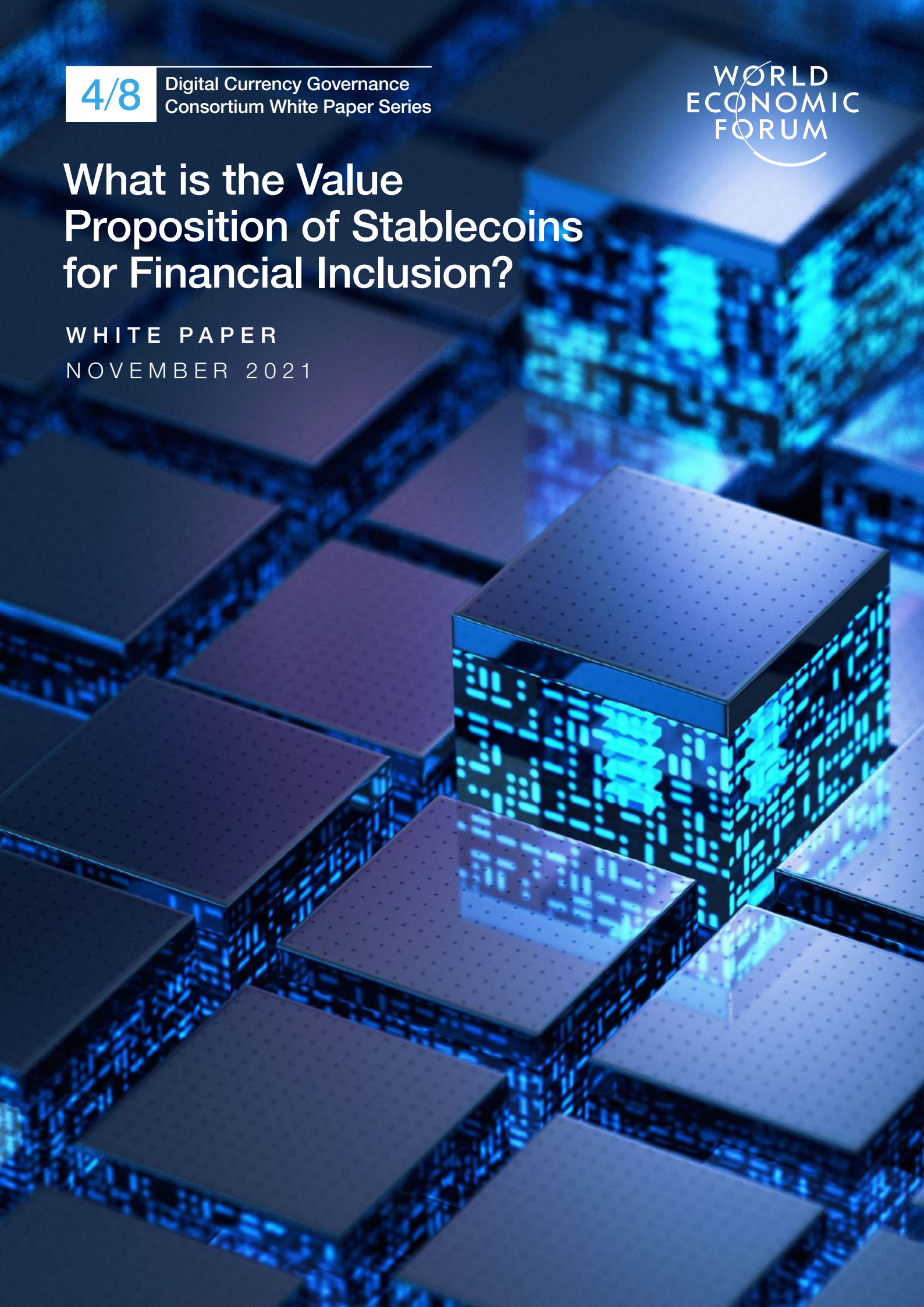
4/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

What is the Value Proposition of Stablecoins for Financial Inclusion?

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

Preface 87

1 Context and approach 89

1.1 Existing barriers to financial inclusion 89

1.2 Questions addressed by this white paper 90

1.3 Three case studies – three scenarios 90

1.4 Defining stablecoins 91

2 Key findings 92

2.1 Stablecoins currently offer limited benefits 92

2.2 Special characteristics of stablecoins for financial inclusion 94

2.3 Future opportunities related to DLT 95

2.4 Limitations of stablecoins for financial inclusion 97

2.5 Risks of stablecoins in the financial inclusion context 98

2.6 Stablecoins and cross-border transactions 100

3 Requirements for stablecoins to improve financial inclusion 101

3.1 Conditions specific to stablecoins and related infrastructure or other digital payment providers 101

3.2 General conditions for a jurisdiction to achieve financial inclusion, independent of the nature of the offering 101

4 Cross-border remittances to Honduras (scenario 1) 102

4.1 Background to remittances 102

4.2 A contemporary remittance story: José 102

4.3 Existing barriers assessment 104

4.4 Potential impact of stablecoins: filling unmet needs 105

4.5 Potential impact of stablecoins: addressing barriers to inclusion 107

5 Financial inclusion for SMEs in India (scenario 2) 109

5.1 Background: unmet needs of SMEs in India 109

5.2 Challenges of a small business in India: Gita 109

5.3 Existing barriers assessment 110

5.4 Potential impact of stablecoins: filling unmet needs 111

5.5 Potential impact of stablecoins: addressing barriers to inclusion 112

6 International wages in the online labour economy (scenario 3) 114

6.1 Background: international wages and the gig economy 114

6.2 Wages for a remote worker based in a developing economy:Yannick 114

6.3 Existing barriers assessment 116

6.4 Potential impact of stablecoins: filling unmet needs 117

6.5 Potential impact of stablecoins: addressing barriers to inclusion 118

Conclusion 120

Endnotes 121

Preface

This white paper investigates the benefits and limitations of stablecoins for supporting financial inclusion in historically excluded or underserved populations. It explores whether and how stablecoins can address common roadblocks to financial inclusion, and it examines the potential new opportunities and risks that stablecoins could introduce.

Financial inclusion is a well-recognized global issue: 1.7 billion people are "unbanked" – lacking an account at a financial institution or mobile-money provider – according to the World Bank.[1] Meanwhile, many small- and medium-sized businesses face challenges in realizing benefits from the current financial system. Individuals and small businesses may not be able to access financial services; if they can, those services may not be of high quality, suitable or affordable. The World Bank defines financial inclusion as the ability of individuals and businesses to access "useful and affordable financial products and services that meet their needs".[2] Financial inclusion is a complex global problem that existing systems and offerings have so far failed to solve.

It is often suggested that stablecoins could address the challenges and unlock some of the opportunities around financial inclusion globally.[3] Yet very little extensive analysis on the subject has been conducted. This white paper examines real-world case studies and builds on existing research to assess the benefits and risks of stablecoins for financial inclusion for historically excluded or underserved populations. The case studies or scenarios, while necessarily limited, attempt to capture the breadth as well as the nuances of the challenges faced by these communities. Although they clearly cannot represent the full slate or complexity of all situations, we hope that the conclusions we draw from our scenarios will be applicable to a range of contexts and regions.

To complete the analysis, we compare stablecoins' capabilities and limitations with those of pre-existing forms of money that do not typically employ blockchain technology, both electronic (e.g. commercial bank money, mobile money and e-money) and physical (e.g. cash). We assess the current barriers facing each scenario to determine if stablecoins overcome, circumvent or aggravate those barriers.

Our aim is to clarify the conditions and prerequisites for providing financial inclusion, and to provide policy-makers, businesses, civil society organizations and digital currency issuers with a better understanding of

the opportunities, risks and benefits that stablecoins currently offer and could in the future bring to financial inclusion. Notably, this paper does not assess the merits of stablecoins outside the context of financial inclusion, and our intent is not to make normative statements about whether individuals, communities or jurisdictions should or should not engage with stablecoins as a general matter.

This white paper is organized into six chapters. Chapter 1 presents the wider context of challenges to financial inclusion and our approach to analysing the capabilities of stablecoins to address those challenges. Chapter 2 highlights the key findings from our research, including both the advantages and limitations that stablecoins offer in the context of financial inclusion. Chapter 3 presents some requirements and conditions for stablecoins to improve financial inclusion. Chapters 4-6 detail three case studies around which our research is focused and offer a potential framework which future researchers could use to analyse the capabilities of different types of stablecoins in specific contexts and geographies.

> **Financial inclusion means that individuals and businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit and insurance – delivered in a responsible and sustainable way**
>
> The World Bank

1 Context and approach

1.1 Existing barriers to financial inclusion

Many well-known barriers prevent the financially excluded from obtaining access to and meaningfully using formal financial services.[4] A subset of barriers pertinent to this analysis, identified from *The Global Findex Database 2017*, published by the World Bank, can be grouped into three broad categories as follows: socio-cultural/demographic barriers, infrastructure barriers and financial barriers.

Socio-cultural and demographic barriers

These factors, which are unique to a particular nation, demography or culture, influence both access to and adoption of financial services. They can include:

- Distrust of financial services providers and/or government (including privacy concerns)
- Challenges around digital and financial literacy, as well as general literacy and numeracy challenges
- Physical safety concerns around accessing services
- Social, cultural and political barriers (including religious and gender-based barriers, and cultural views of money)

Infrastructure barriers

These factors relate to the broader capacity of the environment within which an individual lives. They can include:

- Weak or unreliable electricity supply
- Limited internet connectivity
- Limited access to mobile phones (smartphone or feature phone)
- Lack of government-issued personal identity documentation
- Lack of physical proximity to a bank or availability of services that fit needs

Financial barriers

These factors revolve around the lack of high-quality, affordable and relevant financial services, and include barriers such as:

- High prices and fees for financial products and services
- Minimum balance requirements
- Lack of digital financial history

1.2 Questions addressed by this white paper

It is suggested with some regularity that stablecoins can meaningfully address financial inclusion barriers. These claims tend not to reference specific known barriers in a region or explain in detail how stablecoins would address them. This paper aims to address that gap and evaluate in an objective manner whether stablecoins as currently deployed overcome specific barriers to financial inclusion, and to identify the principal benefits, risks and limitations of using stablecoins for this purpose.

Specifically, this white paper seeks to answer the following questions:

1. How, if at all, do stablecoins improve financial inclusion, compared to other pre-existing options; and what conditions must be met for stablecoins to succeed in supporting financial inclusion among underserved individuals and communities?

2. What new challenges or risks, if any, might stablecoins introduce?

3. What is the net conclusion for stablecoins' current value proposition, considering benefits, trade-offs and limitations?

1.3 Three case studies – three scenarios

> It makes sense to evaluate the impact of stablecoins on financial inclusion based not on which financial services they can enable, but on whether they help meet the fundamental needs of those who are financially excluded

Our research investigation is grounded in three case studies from different parts of the world, each of which is intended to represent a different real-world financial scenario or challenge. These are described in Chapters 4-6. Stablecoins are evaluated in terms of their ability to address the specific needs and challenges in each case study. The countries were selected to capture a range of geographic, regulatory and other differences. However, they carry their own unique considerations that do not scale across geographic barriers. The challenges in scaling solutions across different contexts are not unique to stablecoins but are reflected across a variety of pre-existing options.

The three case studies or scenarios are as follows:

Scenario 1: An undocumented individual in an urban area of the United States (US), sending remittances home to Honduras

Scenario 2: A small business in India, making domestic payments

Scenario 3: A digitally savvy "gig economy" individual in urban Cameroon, receiving wages from the US

Consumers of financial services are driven by unmet needs in their lives. As such, it makes sense to evaluate the impact of stablecoins on financial inclusion based not on which financial services they can enable, but on whether they help meet the fundamental needs of those who are financially excluded. Each persona represented by our case studies has multiple financial needs, which can be summarised in line with the ground-breaking "financial needs framework" commissioned by the Bill & Melinda Gates Foundation in partnership with The MasterCard Foundation as follows:[5]

- **Transferring value**: the ability to transfer value for activities such as making a purchase, paying a supplier or sending remittances or wages

- **Maintaining liquidity**: the ability to meet one's expenses at any point in time

- **Resilience to financial shocks**: the ability to handle unexpected expenses and return to the same financial position as before the shock

- **Meeting future goals**: the ability to afford irregular but planned expenses that meet consumptive expenses (e.g. wedding), life-cycle costs (e.g. education) or productive needs (e.g. expanding one's business assets)

In each of our three scenarios, the pre-existing conditions that limit financial access and inclusion are identified up-front. These conditions are based on those that are likely for the persona, drawing from personal interviews, the World Bank's *Global Findex Database* (latest available data from 2017), additional online research materials and a site visit in the case of Cameroon.[6] The scenarios were constructed in advance of the analysis, when results were not yet known. They were not adjusted over the course of the analysis. That said, a scenario written about an individual in rural Kenya, which sought to explore the role of stablecoins in an area of high mobile-money penetration, was removed after finding that there were too few significant barriers to inclusion in the specific scenario's context to be applicable to other jurisdictions (fintech innovations, rapid uptake of mobile money and government initiatives have significantly improved financial services access in Kenya).[7]

All scenarios involve a developing-market economy, since developing economies generally face higher rates of unbanked and financially underserved populations than developed economies.[8] However, many of the findings may be applicable to historically excluded communities in developed markets as well.

To evaluate the value proposition of stablecoins for inclusion in another country (whether developed or developing), a researcher may apply the framework in this paper, identifying the specific barriers to inclusion that are present and considering the potential for stablecoins to address or bypass them within the relevant context.[9]

1.4 Defining stablecoins

There are several types of stablecoin, each of which differs in its economic and technical design, risk management procedures, quality of backing and legal protections for users.[10] Our research takes a broad approach and includes within its scope any stablecoins conforming to the following definition:

Digital currencies, most often cryptocurrencies, operating primarily on distributed ledger technology (DLT), that are designed to maintain a stable value relative to a reference asset or a basket of assets.

A stablecoin's price may, for example, be pegged to the price of fiat currency such as the US dollar (achieved using US dollar collateral, typically held in banks). It may be backed by the value of other crypto-assets or commodities, or it may be supported by algorithms. Depending on the effectiveness of the stabilization mechanism and backing, the digital currency may or may not hold a stable value relative to its reference asset.

We consider all major current or potential future stablecoins, including the following, organized by market capitalization: Tether, USD Coin, Binance USD, DAI, TerraUSD, TrueUSD, Pax Dollar, Celo Dollar and Diem (formerly the Libra token; not issued at the time of writing).[11] Stablecoins are far from monolithic. In addition to varying design and stabilization mechanisms, the degrees of regulatory compliance and prudence in financial and operational risk management vary greatly. Another distinction is the extent to which the stablecoin operates on a public, permissionless blockchain ledger, which is the case for most stablecoins listed above, versus a closed and permissioned blockchain ledger as is anticipated with Diem.[12]

This high degree of variance between stablecoins makes it hard to generalize. Nevertheless, the conclusions in this white paper are likely to apply across the class of stablecoins described above, while leaving space for meaningful diversity among them. Risks such as the loss of user funds from lost wallet access, insolvency at the stablecoin issuer or technical failure of the stablecoin protocol stand out as varying substantially. While these risks are significant, a detailed analysis of them is beyond the scope of this paper, which focuses specifically on issues unique to financial inclusion.[13] The intention of this paper is to draw preliminary conclusions, based on our case studies, as to the currently visible capabilities of stablecoins, as a class of digital currency, to contribute towards financial inclusion. Readers are encouraged to employ the framework presented in this paper to evaluate the pros and cons of various types of stablecoins in other geographies and contexts.

2 Key findings

2.1 Stablecoins currently offer limited benefits

The principal finding of this white paper is that stablecoins are subject to many of the same barriers that constrain citizens from accessing other financial products and services, such as bank accounts, mobile money accounts or fully digital remittance providers. Where stablecoins are accessible, they generally address financial inclusion barriers to a similar degree as other digital financial services. They may also introduce new risks, which vary depending on the specific system. While different from stablecoins and not the focus of this paper, similar conclusions may be applicable for cryptocurrencies such as bitcoin that are not price-stabilized.

Overall, in the scenarios studied in this report, stablecoins as currently deployed would not provide compelling new benefits for financial inclusion beyond those offered by pre-existing options. Whether this changes over time will depend partly on how stablecoins are regulated and how much attention is paid by stablecoin providers and services to addressing specific barriers to financial inclusion. Even then, success is not guaranteed given the complexity and scope of the problem and potential requirements related to the use of stablecoins.

Table 1 presents an analysis of how stablecoins help or fail to address existing barriers to financial inclusion in each of the three scenarios or case studies. A green-coloured box would denote that stablecoins are likely to add significant new benefits in overcoming the challenge – however, no boxes are currently coloured green for the three scenarios. A yellow-coloured box indicates mixed or uncertain potential for stablecoins to address financial inclusion challenges. A red-coloured box denotes that stablecoins do not solve the problem and could (in certain cases, depending on design choices) aggravate the situation. Meanwhile, blank boxes indicate that the barrier does not clearly arise in the scenario's specific context.

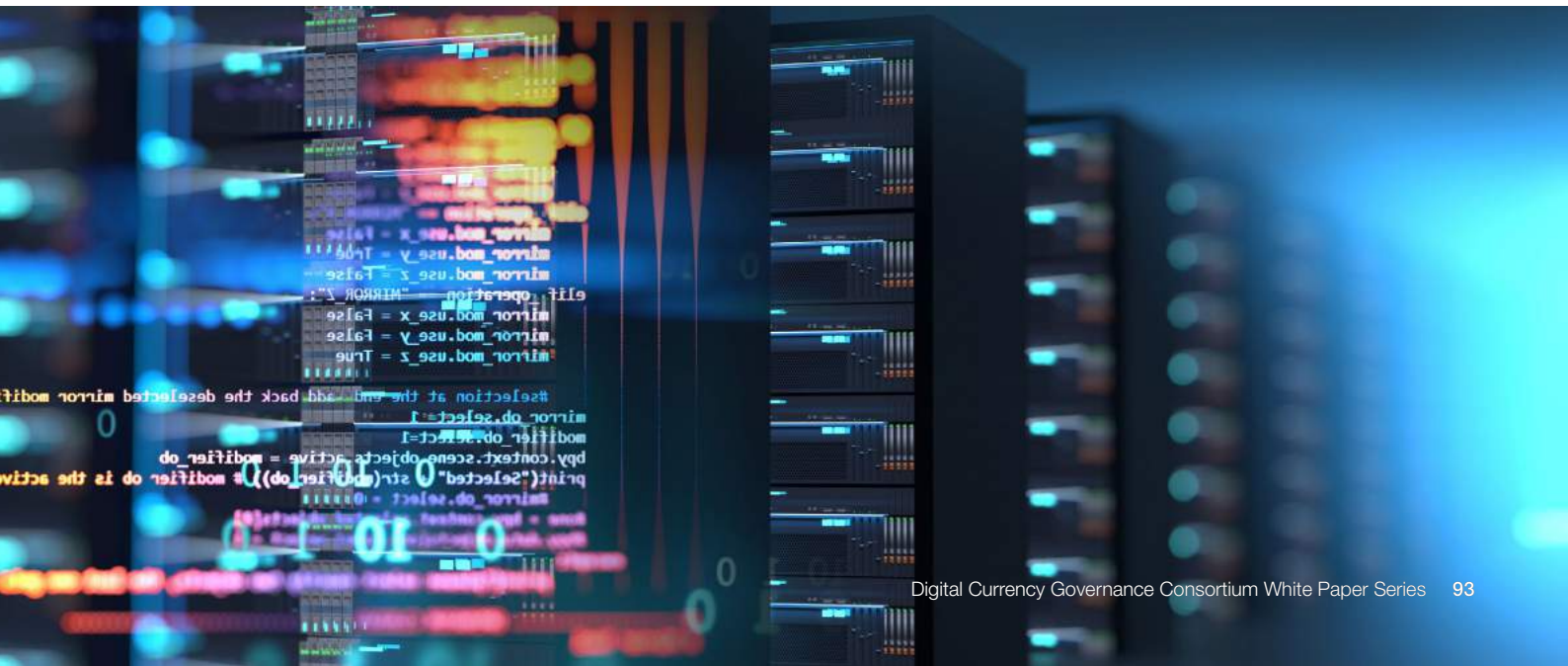
TABLE 1 **Impact of stablecoins on financial inclusion barriers, by scenario**

Financial inclusion barrier	**Scenario 1:** Individual in US sending remittances to Honduras	**Scenario 2:** Small business in rural India	**Scenario 3:** Digitally savvy, "gig economy" individual in urban Cameroon
Socio-cultural/Demographic barriers			
Distrust of financial service providers and/or government (incl. privacy concerns)	✕		
Digital, financial and/or general literacy & numeracy challenges	✕	✕	
Physical safety concerns accessing services	✕	✕	✕
Social, cultural & political barriers (incl. religious & gender-based barriers, cultural views of money)		✕	

Infrastructure barriers			
Weak or unreliable electricity supply			✕
Limited internet connectivity	✕	✕	✕
Limited access to mobile phones (smartphone or feature phone)		✕	
Lack of government-issued identity documentation	✕		
Lack of physical proximity to or availability of services that fit needs	✕	✕	✕
Financial barriers			
High prices & fees for financial products & services	✕		✕
Lack of digital financial history	✕	✕	
Minimum account balance requirements			✕

The remainder of this chapter analyses both the benefits and risks of stablecoins for financial inclusion through the following sections:

- Special characteristics of stablecoins for financial inclusion
- Future opportunities related to DLT
- Limitations of stablecoins for financial inclusion
- Risks of stablecoins in the financial inclusion context
- Stablecoins and cross-border transactions



2.2 Special characteristics of stablecoins for financial inclusion

Despite the general finding that stablecoins are subject to the same challenges as pre-existing options that this paper focuses on, with respect to the barriers to financial inclusion that we have identified, there are two special characteristics of stablecoins relative to pre-existing options.[14] First, stablecoins may side-step issues related to consumer mistrust in traditional financial services. Second, they may uniquely provide digital financial accounts that malicious or untrustworthy actors cannot steal from.

These characteristics are shared by non-stabilized cryptocurrency such as bitcoin. While they do not meaningfully address barriers in the specific scenarios studied, these characteristics could present benefits in other situations. That said, they may be two-sided, offering advantages to financial inclusion in some cases but also suffering from drawbacks.

1. Stablecoins (and cryptocurrency) may side-step issues related to consumer mistrust in traditional financial services

In some cases, consumers and merchants who do not trust local financial service providers or the government in their jurisdiction may trust stablecoins more, due perhaps to their more decentralized nature and management. However, further evidence through surveys or other data-gathering is necessary to determine this perspective, which is likely to vary heavily across regions. It is also possible that end-users will be more suspicious of stablecoins if they are associated with fraud or other issues. In other words, trust may also turn out to be weaker for stablecoins.

The type of stablecoin issuer could be a consideration, since a large tech firm such as Facebook, which initiated the Diem project (formerly Libra), could issue stablecoins where their brand may be more trusted than local brands. However, the reverse may also be true. In these cases, the issuer's brand-value drives the level of trust more than fundamental elements of stablecoin technology (end-users may not even be aware they are employing a stablecoin).

2. Stablecoins (and cryptocurrency) may uniquely provide digital financial accounts that malicious or untrustworthy actors cannot steal from

Cryptocurrency accounts operating on public, permissionless DLT through self-custody (or "non-custodial") wallets may be unique in their ability to protect user funds from outside theft, as funds cannot be moved from an account without the correct private key or password. That said, for many end-users today, the overall risk of losing funds through user error, or through financial or technical problems with the digital currency issuer or wallet, is likely to be higher with stablecoins (and cryptocurrency) than with accounts held at regulated financial institutions or providers.[15]

Users who have sole knowledge of their private key information would lose access to their funds if they were to lose that information. Thus, while stablecoins and their wallet infrastructure present a unique characteristic regarding account security, they currently do not necessarily resolve barriers related to insecure or unreliable financial services. This might change over time as user interfaces and safeguards are further developed, and as more stablecoins come under regulatory purview.

2.3 Future opportunities related to DLT

If we look towards the future, stablecoins and other DLT-based cryptocurrency could bring certain additional opportunities with respect to reducing barriers to financial inclusion, depending in large part on how the ecosystem develops. This section presents four such potential benefits or opportunities.

Today, however, such identifiable opportunities come with the following limitations:

- They are sub-scale, undemonstrated or unproven, and require further research or technology development
- They are reliant on an absence of clear regulation on stablecoins (which is likely to be a temporary situation in most regions)
- They are also available through other fintech innovations.[16]

1. Highly open and interoperable DLT-based ecosystems (which could involve stablecoins) could drive higher competition and more open-loop payment options

> Public, permissionless blockchains (on which many stablecoins operate) enable fully open access, by default, to the blockchain network and its data

This opportunity centres on the notion of blockchain-based ecosystems (in which stablecoins operate) enabling the growth and development of high-quality and accessible financial products that would not otherwise arise. Higher competition could promote lower-cost services that are better able to meet the needs of end-users.

Public, permissionless blockchains (on which many stablecoins operate) enable fully open access, by default, to the blockchain network and its data. This feature (which is also possible, although uncommon, using centralized technology) may lower barriers to entry and stimulate competition. Research points to lower overall costs of networking in a marketplace based on public, permissionless DLT, because rents from network effects are shared more widely among participants rather than owned by one firm, and no single firm fully controls or has access to underlying data assets.[17]

That said, the following unresolved questions remain:

- Will DLT prove over time to support greater openness and access for financial technology innovation and product development than centralized technology infrastructure, which can also employ open-source software or open API access? Open banking and open architectures, where APIs enable information- and data-sharing access to non-bank financial firms and technology start-ups, are examples of pre-existing opportunities for lowering barriers to entry and supporting innovation in retail payments. These are predicated on trust in the institutions involved and on the underlying information, which may vary depending on context.
- How might currently challenging aspects of DLT infrastructure influence the development of financial products and services? Such challenges include constrained scalability, network transaction fees, necessity to operate in cryptocurrency, and security vulnerabilities to smart contracts and underlying networks. Some of these challenges are the subject of intense activity in stablecoin and related ecosystems, but the outcomes are yet to be determined.

2. DLT platforms could offer new, publicly accessible and visible data sources for payment histories and account balances, facilitating credit and insurance underwriting

The premise of this notion is that the public ledgers of stablecoins (and cryptocurrencies) can serve as highly accessible digital payment histories that loan and insurance providers can use to underwrite a customer's risk profile more accurately. With more data and accurate risk profiling, loan and insurance providers could offer more affordable and plentiful services to end-users.

Notably, this activity requires users to employ stablecoins for a sufficiently high quantity of payments to ensure their payment history is informative. It would also require strong privacy protocols, as it implies publicly viewable end-user payment histories. However, such privacy protocols could increase the cost and impede the ability of providers to use such data for underwriting. For

this benefit to materialize, credit bureaus would need to recognize such payment histories, while standardized payment data formats and methods to import or aggregate data would be required.

While payment solutions based on centralized technology could also share payment history about a customer with loan or insurance providers, cryptocurrency (including stablecoins) operating on public ledgers present information publicly by default and are not subject to the decision of an institution regarding whether to share this information.

3. DLT offers opportunities related to decentralized digital identity and compliance

DLT may potentially enable solutions related to "decentralized digital identity", or identity credentials controlled by end-users that are verifiable and revocable within distributed ledger technology. Users could employ this digital identity in certain payments and operations conducted with stablecoins or other cryptocurrency. It could also be possible for the analysis of transactions conducted on public ledgers such as blockchains to flag risky activity and "blacklist" certain users, helping mitigate illicit and harmful activity without requiring traditional identity documentation.

The ability for these schemes to meaningfully reduce identity-documentation barriers while meeting compliance goals, and without compromising user data privacy or creating other issues, must be more thoroughly investigated and demonstrated.

Stablecoins today that do not yet follow regulatory requirements imposed on other payment providers and money transmitters in a given jurisdiction may offer lower-cost transactions. This benefit will almost certainly dissipate when regulatory requirements are imposed, while unregulated activities can present higher risks related to fraud, illicit activity and other issues. For detailed discussions on existing regulatory and policy gaps with respect to stablecoins, refer to the white paper in this series, *Regulatory and Policy Gaps and Inconsistencies of Digital Currencies*.

4. DLT platforms may fill a gap where financial services are not available in the region

In some regions, stablecoins might fill a gap for a "payment rail" or service that is not fully operational or able to receive transactions domestically or from across borders. This opportunity is highlighted by our case study from India in Chapter 5, where mobile payment services that do not require bank accounts remain under-developed. Stablecoins could serve as an alternative where other solutions have not been developed. In this case, stablecoins are filling a gap that has not been met by existing systems – but they do not necessarily present a unique capability.

In other regions, the gap may result from so-called "de-risking" by international banks or payment service providers, where those institutions deliberately terminate relationships with local financial institutions or money transfer operators, resulting in a dramatic reduction in access to financial services and a commensurate increase in the cost of completing basic financial transactions, particularly in a cross-border context. Providers often engage in this behaviour because of the cost of compliance with regulations aimed at reducing financial crimes, which can be particularly high in smaller economies. The effects can be profound.[18] This issue may be present in our Cameroon case study in Chapter 6, although it is difficult to confirm. In these cases, stablecoins might fill a gap effectively. That said, future regulation imposed on stablecoins or inadequate first- and last-mile digital infrastructure for the use of stablecoins in those regions may limit this opportunity, as seen in our Cameroon case study. If such infrastructure (also known as "on and off ramps", for example, local banking) begins to proliferate, this scenario might prove significant.

2.4 Limitations of stablecoins for financial inclusion

Stablecoins and their infrastructure, as they exist today, are subject to the following common barriers to financial inclusion:

- Lack of identity documentation
- Lack of first- and last-mile infrastructure for conversions between physical cash and digital money (given limited acceptance of stablecoin for payments)
- Limited digital and financial literacy and numeracy
- Limited internet or electricity access
- Limited access to smartphones or personal computers[19]
- Currency conversion costs in cross-border payments
- Lack of wealth to afford basic financial services

In general, where regulation is evenly applied, stablecoins are subject to the same adoption and inclusion hurdles as other forms of retail finance. Exceptions may be fleeting in nature: for instance, it may currently be possible in some jurisdictions to access and use stablecoins without meeting compliance requirements. However, it appears likely that stablecoins will eventually be subject to similar regulatory requirements as other digital payment services within a country.

It is often suggested that stablecoins (or cryptocurrency in general) can address problems related to hyperinflation or price instability for citizens in some economies. This challenge was not a meaningful barrier in any of the case-study scenarios, as price levels in the countries studied have remained steady.[20] Stablecoins might offer an easy and helpful way for an individual in a country experiencing high inflation to save funds in a hard currency such as the US dollar or Euro. That said, this ability may not be available at scale as it would entail a movement by citizens out of the domestic currency into the hard currency, which could lead to a currency crisis and escalate the price for citizens to purchase the hard currency using the local currency (as the value of the local currency relative to the hard currency would continue to decline).

Such currency substitution could also create other de-stabilizing effects in the economy and interrupt the effectiveness of monetary policy aimed at stemming the crisis (to the extent that any such policy were introduced).[21] Moreover, the ability for stablecoins to provide easier access to major foreign currencies in local economies with capital controls may be limited by regulation. For economies without capital controls, more research is needed to assess why access to these currencies is more available through stablecoins versus other financial services.

While generally beyond the scope of this white paper, DeFi applications, which extensively operate with stablecoins, are assessed for their ability to meet financial needs, particularly as they relate to lending and insurance.[22] While this space is in its early days, DeFi applications do not presently address identified gaps or meet the needs of the individuals and communities contemplated in the scenarios in this paper. It is conceivable that DeFi may provide value to the financially underserved in the future, although the relative benefits and risks will need to be assessed as the space develops, and their value-add relative to centralized financial services, assuming regulatory compliance, is not clear.[23]

2.5 Risks of stablecoins in the financial inclusion context

Stablecoins, depending on their design, may introduce new – possibly serious – risks to users. The risks and downsides listed below (divided into financial/technical and non-financial/non-technical risks) are each present in at least one of the three scenarios in this report, with many present in multiple scenarios. The extent to which these risks exist in various stablecoins depends on their specific management and operations. While some stablecoins are demonstrating prudent financial management and are seeking and gaining regulatory approval, others have not yet succeeded in doing so.[24] These differences in the regulatory management of stablecoins are highly relevant to the consideration of risks. Some prominent examples of such differences include the following:

- In 2018 the New York Department of Financial Services approved Gemini Trust Company LLC and Paxos Trust Company LLC to issue dollar-pegged stablecoins (namely, Paxos Standard, now called Pax Dollar, and Gemini Dollar), conditional on robust policies regarding anti-money laundering, anti-fraud and consumer protection measures.[25]

- Meanwhile, Tether, the largest stablecoin in issuance which is most often used by traders to trade into and out of cryptocurrencies, is pegged to the US dollar and has $68 billion of outstanding tokens as of the time of writing.[26] However, Tether has not historically fully backed its tokens with highly liquid US dollar reserves and has at times held significant reserve shortfalls; it has also been found to repeatedly deceive clients about its reserves and is not permitted to operate in New York State.[27]

Financial and technical risks

Stablecoins bring financial risks and downsides. The risk of losing stablecoin funds or losing access to those funds can arise from a number of factors, including:

> While some stablecoins are demonstrating prudent financial management and are seeking and gaining regulatory approval, others have not yet succeeded in doing so

- Financial failure at the stablecoin provider, due to illiquidity or insolvency caused by a digital "run" on stablecoin reserves, or mismanagement or other failure of the reserve assets or stabilization mechanism[28]

- Lost access to move funds (e.g. from losing one's private key or passwords, particularly if the wallet is "self-custody")

- Stolen access to funds (e.g. if one's private key or passwords are compromised), where bad actors steal funds

- Accidentally sending funds to the wrong recipient (transactions are irreversible)

- Falling prey to fraudulent schemes (stablecoins do not generally offer fraud protections or the ability to address such issues with human intervention)

- Technical failure at the base-layer blockchain protocol or stablecoin smart contracts, due to software bugs, smart contract exploitation, cyber-attack or other issues[29]

Some of these financial risks are worth examining in more detail:

Lack of deposit insurance and full protections

Several stablecoins today lack important provisions and guarantees that protect users' funds. As a result, funds with these issuers are likely to be at greater risk of loss than if they were held by regulated financial institutions. Unlike with domestic banking services in many countries, stablecoins are generally not subject to deposit insurance or the full protections offered by regulatory systems with respect to financial management and consumer protection.

Not all stablecoins are fully backed

Reserve and stability management are of particular concern. For stablecoins pegged to a fiat currency, users may lose their funds if the stablecoin issuer is not fully backing the stablecoin with that cash or other highly liquid and high-quality assets denominated in the stablecoin's currency and held in bankruptcy-remote accounts. Digital "runs", where an escalating number of users lose confidence and rapidly sell and redeem stablecoins, are a risk for all types of stablecoins.

Even where stablecoin issuance is fully backed by fiat deposits at the issuer's account at a commercial bank, a run on the stablecoin, if large enough, could

force the commercial bank to rapidly unwind its loan portfolio to meet its deposit redemptions, causing stress to multiple banks. Deposit insurance would generally not be able to cover the stablecoin issuer's entire account (in the US, deposit insurance currently covers up to $250,000 of deposits per depositor).

Accidental loss of funds

In the absence of consistent education around new stablecoin services, including the differences in how they operate, individuals may be at higher risk of mistakes that could lead them to accidentally lose their funds.

Higher costs

Depending on infrastructure and system design (particularly the consensus algorithm and degree of decentralization in transaction validation), stablecoins in particular and cryptocurrency in general may involve higher costs per transaction than non-blockchain-based payment infrastructure. Higher costs arise from network-level transaction fees to incentivize validators in a public network, and from higher security requirements involved in decentralized transaction verification (for instance, energy-consuming computations in proof-of-work consensus algorithms and locked-up-capital in proof-of-stake consensus algorithms).[30]

Non-financial and non-technical risks

Stablecoins also present a number of non-financial risks and downsides, outlined below.

Widening the digital divide and gender gap

> Unless the ecosystem focuses deliberately on building inclusive models at scale... stablecoins may risk increasing inequality in financial services and technology access, rather than addressing it

Rather than strengthen equality, it is possible that stablecoins and their surrounding ecosystems and infrastructure, as well as blockchain-based financial applications in general, could widen the "digital divide" and "gender gap" in access to financial services between those who are digitally and financially savvy, with smartphones and internet access, and those who lack these skills and technology.[31]

Early research indicates that users of cryptocurrency currently tend to be young, educated, male individuals who are already experienced in digital finance.[32] Unless the ecosystem focuses deliberately on building inclusive models at scale, this trend may continue and stablecoins may risk increasing inequality in financial services and technology access, rather than addressing it.

Privacy risks

Stablecoins can create privacy risks for users owing to the public visibility of the ledger. While public addresses of users are often "pseudonymous" (where numbers rather than names are used to identify accounts), the identity of account owners could be compromised if the accounts are associated with certain transactions or patterns. Adequate privacy protections and practices may help to mitigate or even eliminate this risk.

Concerns around illegality

Users may be subject to regulatory penalties if their use of stablecoins is or becomes illegal in a country, or if they improperly report their stablecoin activities for tax or other purposes.[33] Merchants may hesitate to accept stablecoins where they are not confident in their backing or they are suspicious of fraudulent activity.[34]

Higher complexity

Stablecoins may include an intangible or time-valued "cost of complexity" for individuals who are not accustomed to engaging with stablecoins and cryptocurrency, where individuals perform steps such as visiting a cryptocurrency exchange, setting up a digital wallet and provisioning it with funds, and other new activities. These barriers could be addressed through technical and educational efforts, but in the absence of such efforts, these barriers may prove to be significant.

2.6 Stablecoins and cross-border transactions

Research indicates that the following factors correlate with lower-price remittances for a given corridor: remittance volumes, competition in remittance providers (particularly from money transfer operators) and accommodating AML/CFT regulations.[35]

While it is true that disintermediation from expensive parties involved with cross-border transactions can reduce costs, doing so does not necessarily require the use of decentralized systems and can also occur through competitive payment providers operating with centralized ledgers. Moreover, payments based on DLT may entail higher costs per transaction than those based on centralized technology, as discussed in section 2.5.

Said otherwise, the decentralization of payment transactions and settlement (in terms of the operations, agents and ledgers involved) does not fundamentally reduce or eliminate currently unavoidable, and high, costs related to currency exchange and regulatory compliance in cross-border payments. This analysis assumes that any service complies with regulation; further, should regulations change, it is assumed that any potential cost savings would apply across all providers rather than favouring those that operate on decentralized infrastructure. Stablecoin providers thus may look to the world's most inefficient remittance corridors to provide beneficial services where other providers do not yet operate (including intra-continental corridors such intra-African).

For additional discussion on the risks and downsides of stablecoins, see the white paper in this series *Digital Currency Consumer Protection Risk Mapping*.

3 Requirements for stablecoins to improve financial inclusion

For many of the scenarios discussed in this paper, the following requirements and conditions are necessary to achieve financial inclusion via the introduction of stablecoins. They are expected to be relevant in most jurisdictions.[36] Several are also relevant requirements for existing digital payment solutions to enable wider access.

3.1 Conditions specific to stablecoins and related infrastructure or other digital payment providers

- High-quality and highly liquid reserve assets that fully back stablecoin issuance, paired with legal protections for users from issuer bankruptcy or insolvency, operational risk, market risk (volatility in cryptocurrency or other asset prices) and cybersecurity risk
- Minimum privacy, account recovery and/or other consumer protection standards and capabilities so the potential for irreversible user error is reduced, particularly for those new to engagement with digital systems
- Infrastructure to provide on-ramps and off-ramps (e.g. physical agent locations or digital services for the transition from digital or physical fiat money to the stablecoin and back again)[37]
- Adequate transaction scalability and processing speeds[38]
- Sufficient technical resilience and robustness
- Very low transaction fees for payments
- Sound financial governance and management, including safe and regularly audited custody of fiat or other assets backing stablecoins
- Regulatory clearance and compliance for all relevant activities (e.g. money transmission, reserve fund management, consumer protections etc.) in the country or countries in which the sender and receiver live[39]
- Acceptance with merchants (for purchases), government (for paying taxes or receiving benefits), employers (for receiving wages) or other relevant parties; interoperability with other payment rails and services[40]

3.2 General conditions for a jurisdiction to achieve financial inclusion, independent of the nature of the offering

- Adequate internet availability and access
- Adequate smartphone penetration (or ability for the financial service to operate on feature phones or other devices)[41]
- Education aimed at achieving digital and financial literacy and numeracy, including awareness of digital and financial risks
- Trust in digital and financial products
- Cultural acceptance of digital payments and other financial services
- National ID system or other ID solutions to meet KYC requirements
- Regulatory clarity on the new technologies and financial products that may improve financial inclusion. Specifically for stablecoins, regulatory clarity on their treatment and a comprehensive regulatory framework that governs both domestic and international use cases is necessary in many jurisdictions. This includes guidance on cryptocurrency exchanges and whether banks can connect with them or other businesses engaging with cryptocurrency or stablecoins.

4 Cross-border remittances to Honduras (scenario 1)

4.1 Background to remittances

> According to the World Bank... the global average cost of sending $200 was 6.4% in the first quarter of 2021, which is more than double the Sustainable Development Goal target of 3.0% by 2030

Remittances represent a significant source of livelihood for much of the world and several papers have studied the impact of remittances on economic development.[42] Remittance flows to low- and middle-income countries reached $540 billion in 2020 – more than the sum of FDI and overseas development assistance combined – and they are projected to reach $553 billion in 2021.[43] Migrant inflows account for more than 6% of GDP (on average) for developing market economies, with some as high as 40% of GDP.[44] The traditional costs of securely and efficiently managing and moving money across borders have been relatively high. According to the World Bank's Remittance Prices Worldwide Database, the global average cost of sending $200 was 6.4% in the first quarter of 2021, which is more than double the Sustainable Development Goal target of 3.0% by 2030.[45]

In addition to monetary cost, the time-cost of remittances is also high. Research has measured the time-costs associated with sending and receiving remittances by surveying recipients in Mexico and senders in the US. The average time spent standing in line for people who *send* funds using traditional remittances is 30 minutes – this adds up to 10 days over a lifetime.[46] For people *receiving* traditional remittances, the spent waiting per transaction is 41 minutes or 15 days over a lifetime. On aggregate, Americans spend nearly 300 million hours standing in line and walking to and from a remittance-sending location. On the receiving end, Mexicans spend over 100 million hours standing in line and walking to and from a remittance pick-up location.[47] Remittances also entail an aspect of physical danger for the individuals who send or pick up physical cash from a designated location, especially for women and the elderly.

This scenario will explore the challenges associated with remittances and whether stablecoins can mitigate them in meaningful ways.

4.2 A contemporary remittance story: José

José is an immigrant from Honduras who currently lives in Houston, Texas. He emigrated to the United States recently. José's wife Maria and their children did not make the journey north with him and live with Maria's family in a rural village approximately 30km outside of San Pedro Sula in Honduras.

Every week, José sends money back to Maria to support their family and save up to buy a house.[48] However, as José is an undocumented worker in the US, without a government-issued ID, social security number or credit score, he faces barriers to opening a local bank account. Maria does have a bank account, but the closest commercial bank is approximately one hour away from her home.

Both José and Maria have access to smartphone devices and are reasonably comfortable with using technology.[49] Coverage of electricity and cell service is not an issue for José, as he's located in a large, urban area. Meanwhile, Maria generally has adequate electricity but occasionally experiences internet connectivity outages in her village.

José and Maria have enough general wealth to engage in financial services (namely remittances), although many other Hondurans are not as fortunate. Honduras is one of the poorest countries in the world, with more than 66% of its population living in poverty and approximately one in five of its rural residents living in extreme poverty (less than $1.90 per day), according to the World Bank.[50] Indeed, 46% of adults report not having a bank account due to insufficient funds or lack of money.[51]

The need to transfer value

With his wages paid in physical cash and without access to a bank account to transfer value across international borders, José must use a money transmitter in the US that accepts physical cash, such as MoneyGram or Western Union. On the receiving end, Maria can receive the remittances to either her bank account or her mobile phone. She uses TIGO Money, a popular mobile money platform operated by one of the country's largest telecom providers. MoneyGram and Western Union serve as agents for TIGO Money in the US, enabling José to send US dollars in cash through the agents to Maria, who receives the funds to her TIGO Money account.[52] The remittance generally arrives within the hour or on the same day and costs about 2-4% depending on how much money José sends.[53]

The need to maintain liquidity

As an undocumented worker in the US, José's income stream is cash-based and dependent on his ability to find and maintain regular employment. Given his reliance on cash, José needs to carry a certain amount to meet his expenses at any point in time. Thus, José's ability to maintain enough liquidity requires constant cash management, balancing the risk of carrying extra cash should it be needed, compared to the time it would take to retrieve additional cash.

Maria's job at the local textile factory provides a more reliable and steady stream of income, but it is insufficient to support her family and save for a house, so she is reliant on the remittances from José each week. Additionally, despite access to a traditional bank account, Maria is also highly reliant on cash; the use of credit and debit cards remains rare in Honduras and she does not have one.[54]

The need to stay resilient to financial shocks

Due to the lack of credit facilities available to them, José and Maria rely on family and friends in Honduras for support during times of unexpected financial hardship, caused for example by illness or job loss. Neither José nor Maria can afford private health insurance, so if either of them (or their children) become ill they are reliant on public health services and may suffer lost wages (or even unemployment) if they cannot get treatment in a timely manner that allows them to return to work.[55]

Additionally, José requires a car to commute to work as he often needs to drive to job sites not served by public transport, while carrying equipment and tools. As such, should José lose access to a car, he may also lose wages or even his job.

The need to meet goals

As they save money to buy a house, Maria can take advantage of her bank access to put money (including funds received from remittances) into a savings account that earns a modest amount of interest. However, Maria has limited access to credit for large purchases, as retail loan markets are very limited in Honduras, with siloed credit scoring programmes and often punitive interest rates.[56]

Meanwhile, José does not have a bank account, but the large Honduran community in Houston affords him the opportunity to join a *tanda* – a community savings and lending circle that allows him to save towards various goals. *Tandas* typically do not offer interest, but they do allow José to save towards known goals or for unexpected expenses that may arise.

4.3 Existing barriers assessment

Socio-cultural/demographic barriers

Financial literacy: José and his wife Maria are digitally and generally literate and comfortable working with numbers, but they have low financial literacy. While they understand the mobile money and savings programmes they engage with, they are unaware of additional financial services that could benefit their family. Although more than 87% of adult Hondurans (age 15+) are literate, the issue of financial literacy remains a serious concern.[57] According to Standard & Poor's Rating Services Global Financial Literacy Survey, Honduras ranks 123 out of 144 countries, with a financial literacy rate of 23% compared to the world average of 33%.[58]

Distrust and privacy preferences: As an undocumented immigrant, José is wary of engaging with formal financial services for fear that the US government could learn about his status as an undocumented worker and deport him.

Physical security challenges: For Maria, the issue of security is extremely relevant. Honduras is one of the most violent and dangerous countries in the world, especially for women.[59] While Maria can receive her remittances digitally and use TIGO Money for some payments, she must still use cash for several day-to-day transactions with merchants in her town. While she carries small amounts of cash, she may be targeted for theft in her daily life, especially after visits to the bank.

Infrastructure barriers

Internet connectivity: Living in a major urban area, José does not typically have issues related to internet connectivity or electricity outages. However, Maria's remote rural location can result in common internet connectivity challenges. Access to electricity has been improving and is no longer an issue: rural populations in Honduras reached 81% electricity access in 2018.

Identity documentation: Access to identification is not an issue for Maria (84% of the Honduran population has a national identity card).[60] For José, the issue is more complicated. As a non-resident living in the US, he may be eligible for an Individual Tax Identification Number (ITIN) that he could use as a form of ID, which would allow him to open a bank account. However, José's preference is to preserve his privacy, given his immigration status and concerns around deportation. He has therefore chosen not to explore this possibility.[61]

Lack of physical proximity or availability of services that fit needs: For Maria, her bank is one hour away, creating a challenge of physical access and proximity when she needs to conduct banking transactions such as withdrawing cash from the bank to use in town.

Honduras lacks a developed market for retail loans where individuals can access credit for large purchases or expenses and develop a credit history that can be applied nationally. While health insurance is not required to access public healthcare in Honduras, the country lacks an effective public healthcare system that can reliably treat citizens in the event of serious healthcare needs.

Financial barriers

Affordability: José and Maria face some affordability challenges. First, they cannot afford private health insurance. Second, money transmitters in the US that accept cash charge about 3.6% in fees on average to send about $200 from the US to Honduras.[62] While this amount is much lower than the 6.4% global average, if José were to remit $200 a week, he would pay about $7 per week or $375 per year in remittance fees, which equate to one or two weeks' worth of income for the average Honduran.[63] The average cost of sending $500 at a time from the US to Honduras is even lower at 2.1%.[64]

Digital financial history: Only about 34% of Honduran adults borrowed money in the past year, lower than the Latin American and Caribbean average of 38%, and well below the average for low-income countries of 46%.[65] The fact that Hondurans are unlikely or unable to borrow money limits their ability to build a credit history. While both Maria and José take advantage of community-based financial programmes, lending activity in these programmes is unlikely to be reported to credit bureaus.

4.4 Potential impact of stablecoins: filling unmet needs

Areas of unmet need are listed below, followed by a discussion of the benefits that stablecoins could bring to each area.

Unmet need #1: The ability for José to send remittances to Maria at lower cost

José faces barriers – most notably, the lack of a government ID – that currently prevent him from owning and operating a stablecoin account from the US. If some of these barriers were addressed and he were able to open a bank account (allowing him to fund stablecoin purchases) or to access an exchange to purchase stablecoins, then José would also be able to send money using digital remittance services (e.g. World Remit, Remitly or Xoom). Both the stablecoin service and the fully digital remittance service would save José time by eliminating the need to visit a physical agent in Houston. Thus, once certain financial inclusion barriers related to the fiat-to-digital "on-ramp" are addressed, multiple options for smoother digital remittances are available to José, including but not limited to stablecoins.

Stablecoins can serve as an alternative method for sending funds internationally, particularly where there is a lack of competition from remittance providers. In José's case, the average cost of sending remittances from the US to Honduras is 2-4% and funds arrive often within the hour or the same day.[66] Once José can access stablecoins, he could compare the total costs of sending remittances through stablecoins versus available blockchain-based money transmitters. If he were able to access stablecoins, they might provide a cheaper method for remittances than the 2-4% he is currently paying.

Assuming stablecoins are subject to regulation and compliance requirements, it is not axiomatic that sending remittances through a decentralized payment network would be cheaper than with payment networks based on centralized technology. While decentralized technologies such as stablecoins may offer an alternative payment platform and corridors where efficient ones do not exist, centralized and decentralized technologies are equally able to operate payment networks in a manner that includes few intermediaries (i.e. the centralized payment provider may serve as the sole major intermediary in the process, if it is able to operate internationally).

Moreover, in both cases, current AML/KYC/CFT compliance and other regulatory costs are irreducible, and currency exchange costs are unavoidable. Stablecoins might entail an additional currency exchange where users are unable to exchange the stablecoin with local fiat currency. Table 2 displays the cost components of sending a cross-border remittance through stablecoins.[67]

TABLE 2 **Cost components of sending a cross-border remittance through stablecoins**

	Any on-ramp fees (e.g. from agents, banks, credit cards etc.) necessary for moving fiat money (digital or physical) onto an exchange or other service that enables the purchase of stablecoins
+	Potential exchange cost for converting starting fiat currency to stablecoin *(only relevant if stablecoin is denominated in another currency)*
+	Network or service-provider transaction fee
+	Potential exchange cost for converting stablecoin to recipient's fiat currency *(only relevant if stablecoin is denominated in another currency)*
+	Any off-ramp fees that may be necessary for moving funds from the exchange or other service into fiat money (digital or physical) that can be readily spent in the economy *(this could be lessened if stablecoins obtained wide use, including with merchants)*
=	Total cost of sending a remittance through stablecoins

Unmet need #2: Availability of loan options with affordable pricing and ability to develop a credit history that can be used across many loan providers in Honduras

Currently, neither stablecoins themselves nor applications developed in blockchain and DLT ecosystems (such as DeFi applications) offer lending services that meet this need for Maria and José.

While DeFi applications exist on blockchain technology that allow users to engage in peer-to-peer lending and borrowing, loans are denominated in cryptocurrency (including stablecoins) and usually require over-collateralization due to volatility in collateral assets (particularly in non-stabilized cryptocurrency) and absence of credit evaluation. They also typically entail non-trivial transaction fees and borrowing interest rates (for instance, the current cost to borrow the USD Coin stablecoin in Aave and Compound, two leading DeFi lending protocols, is approximately 8%).[68] Some DeFi services are starting to perform credit evaluation on borrowers, with a goal to draw from data and financial history outside the blockchain ecosystem in the future.[69]

Assuming consistent regulation is enacted, the advantages these services may present relative to those based on centralized technology infrastructure are unclear (while disadvantages related to consumer protection and the use of cryptocurrency are present), although they may serve to fill a gap where other lending services do not exist because of a failure to provide such services on the part of existing institutions.

It is also possible that a publicly visible payment history from using stablecoins could be used for credit-underwriting. However, this would require extensive use of stablecoins for payments, which is currently unfeasible in Honduras owing to factors including highly limited acceptance, requirements to employ a smartphone, on/off-ramp and currency exchange frictions and the presence of transaction fees. It also entails privacy risks, as user transactions are generally visible on the public ledger. Lastly, it is possible for payment histories to become visible or shareable using data from mobile money providers operating on centralized technology, which could address this problem without the need for a new system.

> Biases that can result from data gathering [for insurance and loan underwriting] can arise with both centralized and decentralized technology infrastructure

Unmet need #3: Access to affordable and suitable health and automotive insurance

Currently, neither stablecoins themselves nor decentralized finance applications developed in blockchain and DLT ecosystems (such as DeFi applications) offer suitable health or automotive insurance policies that fit this need for José and Maria. As a result, they are unable to meet this need today.

Overall, the insurance market suffers from both a lack of data on individual customers for risk assessment and on market data from which to derive risk models. It is possible in the future that if individuals utilize a stablecoin for a wide array of financial activities, that data could potentially be leveraged by insurance companies to offer tailored services while better understanding the broader environment. That said, this activity can entail privacy risks and is predicated on the extensive use of stablecoins, as discussed above.

Regardless of the technology infrastructure that underlies the insurance solution, data collection for insurance underwriting could create discrimination against those with little activity as they grow their profile or against those with unfavourable activity, resulting in exclusion or high premiums. There is the risk of bias as data informing risk models needs to be representative. Biases that can result from data gathering can arise with both centralized and decentralized technology infrastructure.

4.5 Potential impact of stablecoins: addressing barriers to inclusion

In addition to their ability to address gaps for products and services, stablecoins can also be assessed against their ability to address barriers to financial inclusion. Table 3 describes whether stablecoins meet and address the specific financial inclusion barriers and challenges in this scenario.

TABLE 3 **Do stablecoins address financial inclusion barriers in scenario 1?**

Financial inclusion barrier	Challenges present in scenario 1	Do stablecoins address the challenges for this scenario?
Socio-cultural/Demographic barriers		
Distrust of financial service providers and/or government (incl. privacy concerns)	×	MAYBE – Stablecoins often enable transactions from pseudonymous accounts, which could alleviate some of José's privacy concerns related to deportation. That said, from a technical perspective they are currently no more able to do so than other financial services. In both cases, compliance requirements necessitate José's identity and documentation to be provided, offsetting this opportunity.
Digital, financial and/or general literacy & numeracy challenges	×	NO – Stablecoins generally require higher digital literacy than pre-existing services and have weaker consumer protections. They may especially pose a risk to those who are not financially or digitally savvy.
Physical safety concerns accessing services	×	MAYBE – While Maria has access to mobile and bank payments, she must still use cash for many daily purchases. Any digital payment services (including but not limited to stablecoins) that are widely adopted by merchants and thus reduce Maria's need for cash would reduce her physical safety risks.
Social, cultural & political barriers (incl. religious & gender-based barriers, cultural views of money)		This barrier is not present in this scenario.
Infrastructure barriers		
Weak or unreliable electricity supply		This barrier is not present in this scenario.
Limited internet connectivity	×	NO – Stablecoins do not meaningfully resolve barriers related to low internet connectivity. Usually, the internet is needed for transactions with stablecoins. However, as with other financial technology, Bluetooth and near-field communication (NFC) networking could be employed for offline transactions in proximity, and the payment network may tolerate a limited number of offline transactions during short periods. Double spending risk is often present in these activities, as it is hard to account for ownership changes in the digital money.

Limited access to mobile phones (smartphone or feature phone)		This barrier is not present in this scenario.
Lack of government-issued identity documentation	×	MAYBE – Stablecoins will generally be subject to compliance requirements for identity documentation for AML/CFT purposes, particularly for transaction sizes that exceed certain thresholds. Small transaction sizes may not require identity documentation, for stablecoins or pre-existing money transmitter services (no unique value-add of stablecoins, assuming regulation is applied equally to them and pre-existing services).
Lack of physical proximity to or availability of services that fit needs	×	NO – Stablecoins are not currently accessible to José and thus do not solve these barriers. Once accessible, they may resolve Maria's physical proximity challenges, to the extent they serve as a substitute for banking activities. They may also support the development of credit or insurance services in the future, although this possibility is uncertain and it is not clear that such services would be more suitable or available than with centralized technology infrastructure.
Financial barriers		
High prices & fees for financial products & services	×	MAYBE – It is possible, though not guaranteed, that the total cost of a stablecoin transaction for the case of the US-Honduras corridor is cheaper than José's current options, which cost approximately 2-4%. Once stablecoins become accessible to José and Maria, the costs of each method can be identified and compared.
Lack of digital financial history	×	MAYBE – A publicly viewable stablecoin transaction ledger could be used as a new form of information on payment/financial history and account balances to underwrite loans and insurance. That said, the stablecoin would need to be heavily used and this practice entails privacy concerns.
Minimum balance requirements		This barrier is not present in this scenario.

José currently cannot access stablecoins as he lacks identification that would allow him to open a bank or other financial account that would serve as the on-ramp for him to convert his US dollar cash wages to stablecoins. If fiat-to-stablecoin exchange were unnecessary (for instance if José's employers pay him in stablecoin), José may need to have government ID to legally use a stablecoin wallet due to the AML/CFT compliance requirements. In short, the benefits of using stablecoins for remittances will be limited by many of the same financial inclusion barriers José already faces. Moreover, once the barriers that allow for stablecoins are addressed, José would also be able to access a bank account from which he could send funds to Maria using a digital remittance provider.

Applying this scenario to cases around the world, the value proposition for lowering the cost of remittances depends on an analysis of the total costs of sending a stablecoin transaction versus remittances using pre-existing options. High-potential regions are those where pre-existing remittance costs are high and where local conditions enable the use of stablecoins (e.g. presence of requisite digital infrastructure, regulatory clarity etc.). In these cases, sending remittances through stablecoins might be cheaper. Corridors with low competition from remittance providers, such as intra-African corridors, appear more likely to benefit from new remittance options.

Where remittance corridors are already efficient, the total cost of stablecoins coupled with risks such as accidental loss of funds or private keys may make them less favourable than pre-existing options. Moreover, careful recognition of the pre-requisites for individuals to realistically access stablecoins is necessary. Once many of those are met, pre-existing fully digital remittance options are also likely to become accessible and may provide a viable or even preferable alternative.

5 Financial inclusion for SMEs in India (scenario 2)

5.1 Background: unmet needs of SMEs in India

Despite the importance of SMEs to economic growth, access to finance is a key obstacle they face as they attempt to grow their businesses

Small and medium enterprises (SMEs) constitute about 90% of businesses and more than 50% of employment worldwide.[70] In developing economies, formal SMEs contribute up to 40% of GDP and create 7 out of 10 jobs. These numbers are likely to be significantly higher when informal SMEs are included. Despite their importance to economic growth, access to finance is a key obstacle facing SMEs as they attempt to grow their businesses. It is estimated that 40% of these enterprises in developing countries have unmet financing needs amounting to $5.2 trillion every year. This funding gap often leaves them relying on personal funds or funding from friends and family.

India has more than 63 million SMEs, accounting for over 80% of all industrial enterprises in the country. The credit gap for Indian SMEs amounts to $230 billion, posing serious working capital challenges.[71] These challenges are a result of a working capital cycle where SMEs are required to pay upfront for their inputs and employees, while waiting for sales to result in payment. In times of stress, the likelihood that payments are delayed increases and exacerbates an already vicious cycle.[72]

These troubles are felt even more strongly by women in India. Social attitudes and biases, difficulty in securing collateral-based loans and low financial literacy are often cited as reasons for a lack of access to institutional finance. As most women do not hold property, they are often excluded from collateralized loans. And since most women-owned SMEs (95%) are unregistered, they are not eligible for institutional finance. Plus, women are turned down for credit at a rate twice that of men. Finally, according to survey data, Indian females leading SMEs that do receive funding are often underserved, with a sanctioned loan amount averaging just 68% of the amount required.[73]

This scenario will explore whether stablecoins could help bridge the SME funding gap and overcome the gender bias currently evident in access to institutional finance for SMEs in India, among other challenges.

5.2 Challenges of a small business in India: Gita

Gita is an entrepreneur operating an international kitchenware reseller that has enabled last-mile delivery to rural areas a few hours north of New Delhi. Her company sells international goods, typically sourced from China, that she buys in New Delhi and transports to communities around her hometown. Gita leverages intermediaries as her suppliers since her current order sizes are not sufficient to justify freighting separate containers directly from China.

Gita's company currently employs five people: three drivers, an employee responsible for sourcing located in New Delhi and an administrative assistant. Gita focuses on gaining new clients in her surrounding villages while defining the strategy of the company. The company has a small office in Gita's village, rents a small office in New Delhi, and owns two small trucks and a car, which are available to her drivers.[74]

The need to transfer value

Gita has three main needs when it comes to transfer of value. First, Gita needs to pay her employees. This is typically done in cash for deliveries that have already been completed, when the drivers pick up inventory for a new delivery. It is difficult for the drivers as they typically do not return to the company's headquarters soon after a delivery, leaving them without payment for a period. As the team grows, finding a solution to manage the payroll has become increasingly critical.

Second, Gita needs a convenient way to receive payments from her clients. Payments are typically collected in cash by the drivers at the time of delivery. As a result, her drivers can sometimes be carrying large sums of cash over long distances,

which can put them in danger of theft. They also only deliver the cash to Gita when her town is close to their route, which means she does not have immediate access to those funds. India is very much a cash-economy. Consequently, while Gita would prefer digital payments from her clients, they still prefer to pay in cash. Motivations for cash use by consumers in some regions of India appear to include the avoidance of sales taxes and expectations that digital payments made to small retailers will entail higher fees than cash payments.[75]

Third, Gita must pay her suppliers, which she typically does by bank cheque. This can occur when she or her drivers visit New Delhi to purchase inventory from the suppliers.

The need to maintain liquidity

Cash usage causes a delay between the time at which Gita pays for her goods from the suppliers to the point at which she receives cash payment for the same goods from her drivers. Gita thus often struggles with cash flow issues. In addition, there is seasonality to her business with summer sales being much higher than winter sales. While she can lower purchase of inventory during those times, she still has fixed costs she needs to cover such as rent and internet service. Gita wishes she had access to loans or a line of credit that could help her cover costs while she awaits payments.[76]

The need to stay resilient to financial shocks

Gita's primary business risk is her vehicles. They are dated and only have the minimum required third-party liability insurance. This leaves her vulnerable to costs associated with accidents caused by her drivers. She is also unsure whether the personal vehicles that her drivers sometimes use are covered. Many Indians stop purchasing mandatory car insurance after the first few years of car ownership, with over half of vehicles registered still uninsured.[77]

Road accidents are common in India, and they can not only damage the car but also damage the merchandise and injure her driver. In addition, the roads to the villages she serves are of low quality and have damaged her vehicles. If a car needs repair, Gita must worry about paying repair costs as well as dealing with a delay in deliveries or the need to pay her drivers extra to use their own cars. Vehicle theft is also on the rise.[78]

The need to meet goals

When Gita first started her business, she did so with the financial support of her family. However, now that she's looking to expand, her family cannot help her cover the amounts required. Looking to the future, she would first like to start upgrading her vehicles and buying more of them. She needs financing for new vehicles.

Gita would also like to be able to offer faster delivery and more selection by holding an inventory of products. This would require her to rent storage space as well as obtain the capital to purchase additional inventory.

5.3 Existing barriers assessment

Socio-cultural/demographic barriers

Digital and financial literacy: While Gita is digitally and financially literate, some of the people with whom she engages in financial operations may not be (this could include customers, drivers and suppliers). Across India there is a low financial literacy rate of 24%, which is below the world average.[79]

Socio-cultural factors: India has a cultural preference for cash over digital payments (see section 5.2), limiting the popularity of mobile and bank payments.

Gender inequality, particularly regarding financial access, is a significant issue in India. World Bank Findex data shows that females in India lag their male counterparts in numerous financial areas, including account ownership, debit card ownership, mobile phone subscriptions and access

to emergency funding.[80] Women also repeatedly report having more difficulty in obtaining financial services. Loan applications of female entrepreneurs are more likely to be delayed or rejected. Over 70% of the total finance requirement of women entrepreneurs in the country is considered unmet.[81]

Physical security concerns: Receiving her payments in cash makes Gita very aware of security issues. She is worried for the safety of her drivers that are collecting the cash. Carrying large sums of money makes them vulnerable to theft and physical harm.

Infrastructure barriers

Internet connectivity: Gita, like 95% of Indians, has access to electricity. However, only about 50% of the country has internet access. Gita's small New Delhi office has internet access and she travels there when she needs to perform monthly business activities.[82] However, many of her clients have limited or no internet access, challenging their ability to engage with internet-based digital payments.

Mobile phone access: Gita does not currently have a smartphone, but she's been considering upgrading to one from a feature phone for her business. While there is a trend that Indians are moving from feature phones to smartphones, only about 26% of Indians (and 14% of Indian women) own a smartphone.[83]

Lack of availability of services that fit needs: India has a growing mobile payment industry; however, mobile payment transactions remain under 20% of point-of-sale transactions.[84] India's Unified Payments Interface (UPI) supports mobile money activity; UPI is a banking industry-sponsored protocol that allows for mobile payments to move funds directly to and from an individual's bank a ccount. Mobile money systems that do not require a bank account have slowed down in growth, leaving those without bank accounts with few, if any, options.[85] Thus, Gita's clients without bank accounts are less able to leverage the mobile payment systems available.

Financial barriers

Lack of financial history: More than 80% of all retail outlets in India – most of them sole proprietorships or "mom-and-pop" shops – operate in the cash-driven economy. Gita's business is included, although she pays cheques to her suppliers. Because a large part of their trade happens in cash, owners of these businesses often do not generate the strong financial records needed to apply for a bank loan.[86]

5.4 Potential impact of stablecoins: filling unmet needs

Areas of unmet need are listed below, followed by a discussion of the benefits stablecoins could bring to each.

Unmet need #1: Ability to receive sales revenues and to pay employees electronically, in order to maintain cash flow and liquidity, and reduce safety and security risks

With digital payments of any kind (including but not limited to stablecoins), Gita could receive sales revenues and pay employees electronically rather than with cash. Currently, preferences for cash usage instead of digital payments, and barriers related to internet availability, digital and financial literacy, mobile phone access and other factors inhibit Gita's ability to use pre-existing mobile and bank payment options with her employees and customers. These barriers are not necessarily overcome or avoided by stablecoins.[87]

Unmet need #2: Loans to grow the business and manage liquidity during sales seasonality

Currently, Gita cannot take out loans due to her limited financial history and, potentially, gender biases. As discussed in scenario 1, transaction history as captured by stablecoins could

possibly be shared with credit providers for loan underwriting. For an SME, this practice would be similar to cashflow-based loans suitable for SMEs with limited collateral. Other forms of digital payments also have this capability and this practice can entail privacy risks.

New DeFi projects and applications might possibly provide Gita with access to suitable and affordable lending services in the future, notwithstanding the challenges related to DeFi listed in scenario 1. However, assuming even regulation and wide access for both, it is currently unclear (particularly given the nascency of DeFi offerings) in what manner such DeFi lending applications would reduce biases stemming from gender or offer more suitable or accessible services than lending solutions operating on centralized infrastructure. As DeFi evolves, this clarity may emerge.

Unmet need #3: Affordable and suitable insurance options for Gita's delivery vehicle fleet

As seen in scenario 1, neither stablecoins themselves nor applications developed in blockchain and DLT ecosystems (such as those in the DeFi ecosystem) currently offer insurance policies that suit this need of Gita's. While such services may be developed in the DeFi ecosystem in the future, it is not evident that insurance products and services operating on DLT will offer benefits relative to traditional or centralized-technology options (assuming even regulation). They may also present risks to user privacy, as transactions operating on public blockchains are generally publicly visible.[88]

5.5 Potential impact of stablecoins: addressing barriers to inclusion

In addition to their ability to address gaps for products and services, stablecoins can also be assessed against their ability to address barriers to financial inclusion. Table 4 describes whether stablecoins meet and address the specific financial inclusion barriers and challenges in this scenario.

TABLE 4 **Do stablecoins address financial inclusion barriers in scenario 2?**

Financial inclusion barrier	Challenges present in scenario 2	Do stablecoins address the challenges for this scenario?
Socio-cultural/Demographic barriers		
Distrust of financial service providers and/or government (incl. privacy concerns)		This barrier is not present in this scenario.
Digital, financial and/or general literacy & numeracy challenges	✕	NO – Stablecoins generally require higher digital literacy than pre-existing services and have weaker consumer protections. They may especially harm those who are not financially or digitally savvy.
Physical safety concerns accessing services	✕	MAYBE – Any digital payment solutions that are widely adopted, including but not limited to stablecoins, could address this issue for Gita's firm. Cultural preferences towards cash are likely limiting adoption of pre-existing mobile and digital payment solutions.

Social, cultural & political barriers (incl. religious & gender-based barriers, cultural views of money)	×	MAYBE – Stablecoins may enable more equal lending access for Gita in the future, although not necessarily in a manner that is better relative to other technologies. Apart from potentially supporting tax avoidance (which is contradictory to public policy goals and may disappear with mandatory KYC procedures), stablecoins do not generally address cultural preferences in India towards cash.
Infrastructure barriers		
Weak or unreliable electricity supply		This barrier is not present in this scenario.
Limited internet connectivity	×	NO – Stablecoins do not meaningfully resolve barriers related to low internet connectivity (see scenario 1 for further information).
Limited access to mobile phones (smartphone or feature phone)	×	NO – Stablecoins currently require smartphone (or personal computer) access.
Lack of government-issued identity documentation		This barrier is not present in this scenario.
Lack of physical proximity to or availability of services that fit needs	×	MAYBE – Stablecoins might serve as an alternative for mobile money payments in the absence of mobile money options in India for those who lack a bank account. Non-blockchain based mobile money services, to the extent they become available, could equally address this gap.
Financial barriers		
High prices & fees for financial products & services		This barrier is not present in this scenario.
Lack of digital financial history	×	MAYBE – A publicly viewable stablecoin transaction ledger could be used to share payment and financial history and account balances to underwrite loans or insurance. That said, the stablecoin would need to be heavily used and this practice entails privacy concerns.
Minimum balance requirements		This barrier is not present in this scenario.

Overall, stablecoins in their current form generally do not resolve acute areas of unmet need and barriers to financial inclusion for Gita and her small business. They could serve as a method for Gita to engage in digital payments with her clients and staff (in the absence of other digital payment services), but not in a manner that is necessarily more appealing or beneficial (while still being compliant with tax policy) than other pre-existing or future mobile or bank payment options. The benefits that stablecoins can provide largely relate to filling a gap for digital payment infrastructure and product options available to those without a bank account.

A final and critical issue to consider is that usage of a stablecoin in India could put Gita at risk of legal difficulties. This is due to recently proposed legislation that would criminalize possession, issuance, mining, trading and transferring of crypto-assets within India.[89] While this legislation may not be passed, it could be risky for Gita to currently adopt any stablecoin that is not officially sanctioned by the Indian government.

6 International wages in the online labour economy (scenario 3)

6.1 Background: international wages and the gig economy

Could stablecoins help overcome the current wage payment challenges faced by individuals who work remotely and receive payment for their services from overseas?

The internet has given rise to a widespread global online labour economy. Also known as the "gig economy", it has enabled previously non-existent employment opportunities for millions around the world, including in developing economies. The online labour market in professional services, which engages a significant number of contracted workers from developing nations, constituted $7.7 billion in gross volume in 2018. It is estimated to grow to $17.4 billion in 2023.[90]

In particular, the increase in internet penetration on the African continent has meant young Africans, who make up over 60% of Africa's population,[91] have found paths to employment across national borders. According to GSMA data from 2019, 272 million people in sub-Saharan Africa are mobile internet users, correlating to a penetration rate of 26%. It is predicted that by 2025, the penetration rate will reach 39%, resulting in 475 million mobile internet users.[92]

This uptick in internet penetration has led to skilled Africans, especially in the domains of technology, graphic design and website design, providing their skills to the global labour marketplace. With half of the demand for such labour originating from the US, followed by the United Kingdom, Canada and Australia,[93] one challenge this new landscape presents is that of international wage payments.

This scenario will explore whether stablecoins could help overcome the current wage payment challenges faced by individuals who work remotely and receive payment for their services from overseas. Do stablecoins improve the ability for tech-enabled "gig economy" workers on the African continent to be paid across borders?

6.2 Wages for a remote worker based in a developing economy: Yannick

Yannick is a 25-year-old web and graphic designer who lives in his own apartment in Yaoundé, Cameroon.[94] He comes from a lower-middle class family and has three siblings. Apart from fulfilling his own financial needs, he has financial obligations toward his family. He has an elder brother who lives in the US and together they provide financial support for the education of their younger siblings, one of whom is in secondary school and the other at university. They also support their parents financially in meeting all other family needs.

For the past three years, Yannick has been doing freelance work for a variety of companies based abroad. Most recently, he's been working with a real estate development company headquartered in Florida, US. Yannick renders his services and gets paid on a per project basis. Therefore, payment is received upon completion of a project, or on the completion of milestones for longer-term projects. This averages out to monthly payments for his services given the nature of most projects.

Yannick is digitally and financially savvy. He has a bank account, government ID and smartphone. He is among the 30% of Cameroonians with an account at a financial institution and his educational status, steady work and urban dwelling allow him greater access to financial services than most of his compatriots.[95]

The need to transfer value

Yannick's employer pays his wages in US dollars to an account at an international payment service provider (PSP), as this is most convenient for the employer. With this, Yannick faces an obstacle: in Cameroon, the PSP does not allow customers to link their PSP account to their domestic bank accounts, which would enable withdrawals. Thus, Yannick cannot directly transfer his wage payments from the PSP to his bank account. Given the need for a workaround solution, the company pays the wages to his brother's US-based PSP account.

Yannick's brother withdraws and sends the money to him in Cameroon through a money transmitter. He can use fully digital or in-person remittance providers. He often makes the choice of provider based on the most favourable exchange rate at the time of sending. To reduce time and expense (the time to travel and wait in line for the in-person money transmitter and the higher fee percentage for sending smaller amounts), his brother typically bundles Yannick's salary and transfers it to him every two months, unless there is an urgent need. Yannick picks up the money at a money transmitter location in Cameroon (e.g. Western Union or MoneyGram).

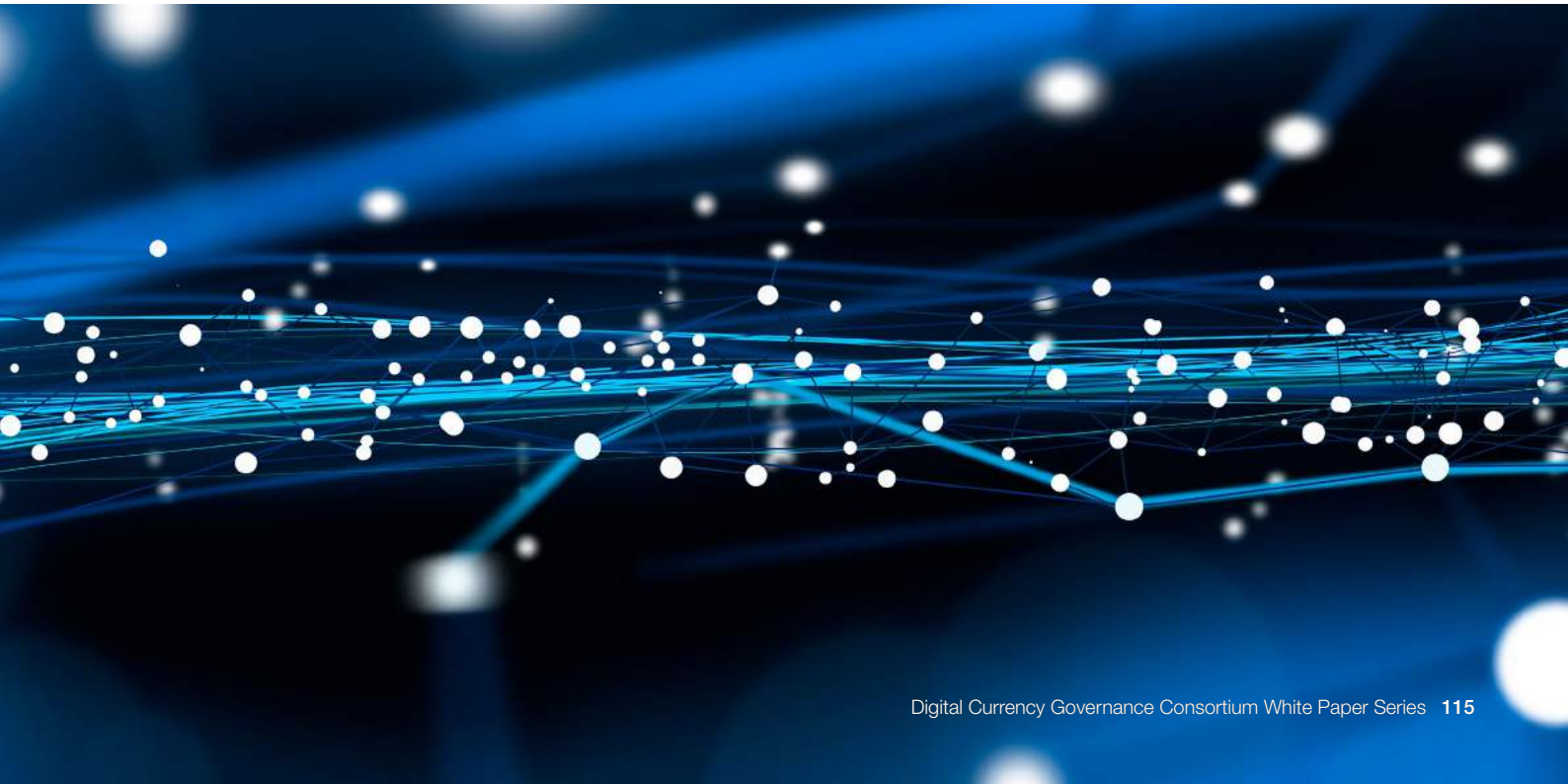
Yannick incurs a transportation cost as he pays for his ride to and from the location by taxi (approximately 4-6 km away). Sometimes, on arrival at the money transmitter, Yannick is informed they do not have an internet connection and they are unable to process his transaction. When this occurs, Yannick is forced to go to another location to pick up his money. When the exchange rate is more favourable or equivalent through a digital remittance provider, Yannick's brother sends the money directly to Yannick's bank account, eliminating the need for Yannick to go to a physical pick-up location.

Yannick's employer could alternatively use a digital money transmitter service (e.g. World Remit or Xoom) that would allow Yannick's wages to be sent directly to his Cameroonian bank account. His employer would need to go through the extra steps potentially involved and pay the transfer and foreign currency exchange fees (these extra costs may be deducted from Yannick's wages). Unfortunately, for the US-to-Cameroon corridor, these options tend to have less favourable exchange rates than remittance providers that operate with in-person, cash-in and cash-out processes.

The need to maintain liquidity

As a freelancer, Yannick sometimes has periods where he has no work and is searching for new contracts. At times he faces gaps in income for which he must save. He also needs a safe and reliable place to save his money for the two-month period between receiving the wages that his brother sends to him.

Yannick has a checking and savings account at BICEC (Banque International du Cameroun pour l'Epargne et le Crédit). His savings account at BICEC requires him to contribute a minimum of 20,000 FCFA (XAF) a month (approximately $37 US dollars). This is because he chose a savings account type that is helping him save towards future purchases such as a home. Yannick also holds short-term savings in his MTN Mobile Money account to plan for the utility bills that he pays using MTN Mobile Money. For this, he can transfer funds directly from his BICEC checking account to his MTN Mobile Money account (and vice versa).



The need to stay resilient to financial shocks

A little over a year ago, Yannick had a serious accident on a motorcycle taxi, a popular means of urban transportation in Cameroon. Fortunately, his brother in the US took care of all the hospital bills, which he was unprepared for. Out of this experience, he has been investigating health insurance. However, Cameroon lacks a reliable and accessible marketplace for health insurance, and individuals who do not work for major corporations are generally unable to attain it.[96] Generally, an individual's family and community help to cover their medical costs in the event of a substantial bill.

The need to meet goals

Yannick continually invests in his professional development by taking online courses in web and graphic design. He must save towards these expenses. Yannick also wants to purchase an upgraded laptop within the next year, which will help him to improve the quality and efficiency of his work. If he has not saved enough money, he will take out a small loan. He can access loans through his bank, BICEC, but for small amounts such as the amount needed for a laptop, he and Cameroonians prefer to borrow from a savings and lending group, called a *Njangi*. He can borrow from the *Njangi* without paying interest. In the *Njangi*, he pools money together with a group of friends and each can draw the total sum contributed on a rotating basis.[97] Cameroon is among the top seven sub-Saharan African economies where informal savings clubs such as *Njangi* groups are most used.[98]

6.3 Existing barriers assessment

Socio-cultural/demographic barriers

Physical security challenges: Although Yannick does not typically feel unsafe in Yaoundé, he has concerns about transporting the cash picked up at the money transmitter to the bank for deposit. Therefore, he does his best to conceal the cash, but carrying it remains a risk.

Infrastructure barriers

Internet connectivity: In general, there is high-speed internet connectivity in Yaoundé, but it is expensive and prone to network issues. Yannick relies heavily on his internet connection and thus is willing to pay high fees to ensure access. He subscribes to a monthly internet plan from MTN and connects to the internet on his laptop through a mobile wi-fi modem. Despite subscribing to this monthly plan, he has daily caps on his data usage.[99] Beyond this, he is at times subject to internet outages that disrupt his connectivity.

Electricity: Electricity outages occur in Yaoundé and across Cameroon, leading to a disruption in some of Yannick's financial activities. If a money transmitter branch is closed due to a power outage, he cannot withdraw funds with it. If his mobile phone or laptop are out of power from an outage, he cannot use them to conduct financial transactions.

Lack of availability of services that fit needs: Cameroon has a scarcity of health insurance providers that serve individuals.[100] Health insurance is very difficult to obtain for individuals who do not work for major multinational corporations. Relatedly, the historic absence of insurance results in low acceptance by health service providers.

Financial barriers

Affordability challenges: The current process for Yannick to receive his wages from the US is costly in terms of time and price. At a minimum, the process entails foreign exchange costs and fees paid to the money transmitter service used.

Minimum balance requirements: As a freelancer and someone banked under an institution that requires him to contribute a minimum of 20,000 FCFA (about $37 US dollars) per month to his savings account, Yannick is under some pressure to maintain a consistent income to keep up with account minimums. The contributions he makes to maintain his BICEC account also limit his funds for an account at a secondary institution that might have provided him a good loan for his laptop.

6.4 Potential impact of stablecoins: filling unmet needs

Areas of unmet need are listed below, followed by a discussion of the benefits stablecoins could bring to each.

Unmet need #1: Ability to receive wages affordably and efficiently for overseas freelance work

Once certain barriers are addressed, stablecoins could serve as an alternative method for Yannick to receive his wages from the US. As with scenario 1, the total cost of sending the wage through stablecoins should be compared with sending wages through other existing options. Most simply, Yannick's employer could open a stablecoin account and transfer Yannick's wages from that account (which would include an exchange operation to the stablecoin from US dollars) to a stablecoin wallet in Cameroon that Yannick could use.[101] However, the difficulty of this transaction for Yannick appears to be in the "off-ramp".

Yannick would need to identify an exchange in Cameroon where he could send the funds, exchange them to local currency and transfer those funds to a financial account from which he could spend them. This "off-ramp" would be necessary because cryptocurrency and stablecoins are not currently accepted for payment at the places where Yannick needs to spend money. Moreover, cash is used for most daily purchases in Cameroon and is more prevalent than mobile money or commercial bank money.

"On-ramp/off-ramp" issues exist with cryptocurrencies (including stablecoins) in Cameroon. There is a limited set of cryptocurrency exchanges and they do not connect with bank or other financial accounts. In today's environment in Cameroon, Yannick faces great difficulty converting his wages from stablecoins into spendable local currency. The Government of Cameroon has not yet issued legislation on cryptocurrencies, so there is currently no regulation or framework for their use.[102] The lack of regulatory clarity has limited the existence of local cryptocurrency exchanges and the willingness of banks and mobile money providers to connect with them.[103] Regulation is currently underway and may resolve these issues in the future.[104] Notwithstanding, Yannick is relatively privileged, as most Cameroonians would struggle with the basic digital infrastructure needed for stablecoins. Most still use 2G feature phones and lack access to the internet. Many also struggle to meet basic financial needs.

If he received his wages more frequently, Yannick could address some of his current liquidity-management challenges. One challenge results from the fact that his bank requires minimum balances. Stablecoins could potentially serve as an alternative place to store his savings, enabling him to avoid the bank account. However, Yannick may need a bank account for various purposes in his daily life, and he is likely to prefer the safety (e.g. through deposit insurance[105] and other protections) that it provides. Another potential solution for this challenge would be for Yannick to consider alternative bank or account types with easier minimums.[106]

Unmet need #2: Ability to obtain affordable and suitable personal health insurance

As discussed in the first scenario, it is unclear how stablecoins would directly benefit Yannick in terms of insurance, aside from the possibility in the future that globally available insurance products and services might arise in the DeFi and blockchain ecosystems. This possibility may not necessarily occur and it is important to identify why, assuming even regulation, such a gap would be better filled with the presence of a blockchain-based ecosystem rather than the pre-existing environment.

Unmet need #3: Availability of loan options

Yannick currently has some access to loans, although more options could be beneficial to him (for instance, he can currently only take out loans from his community *Njangi* at certain periods). As mentioned in the first scenario, stablecoin and the blockchain-based DeFi ecosystem might develop capacities to support this in the future (e.g. through DeFi lending protocols), but it is unclear why they would necessarily be more available or suitable than lending based on centralized technology.

6.5 Potential impact of stablecoins: addressing barriers to inclusion

In addition to their ability to address gaps for products and services, stablecoins can also be assessed against their ability to address barriers to financial inclusion. Table 5 describes whether stablecoins meet and address the specific financial inclusion barriers and challenges in this scenario.

TABLE 5 **Do stablecoins address financial inclusion barriers in scenario 3?**

Financial inclusion barrier	Challenges present in scenario 3	Do stablecoins address the challenges for this scenario?
Socio-cultural/Demographic barriers		
Distrust of financial service providers and/or government (incl. privacy concerns)		This barrier is not present in this scenario.
Digital, financial and/or general literacy & numeracy challenges		This barrier is not present in this scenario.
Physical safety concerns accessing services	×	MAYBE – If Yannick were eventually able to conveniently access stablecoins for receiving wages, he would no longer need to carry cash from a money transmitter office. Note: This is also possible using a digital money transfer service.
Social, cultural & political barriers (incl. religious & gender-based barriers, cultural views of money)		This barrier is not present in this scenario.

Infrastructure barriers		
Weak or unreliable electricity supply	✕	NO – Stablecoins depend on availability of electricity.
Limited internet connectivity	✕	NO – Stablecoins do not meaningfully resolve barriers related to low internet connectivity (see scenario 1 for further information).
Limited access to mobile phones (smartphone or feature phone)		This barrier is not present in this scenario.
Lack of government-issued identity documentation		This barrier is not present in this scenario.
Lack of physical proximity to or availability of services that fit needs	✕	NO – Currently, stablecoins do not present suitable insurance or lending products for Yannick.
Financial barriers		
High prices & fees for financial products & services	✕	MAYBE – Currently, stablecoins cannot address this barrier owing to "off-ramp" challenges from cryptocurrency to local currency in Cameroon. However, in the future, they may serve as an alternative method for Yannick to receive overseas wages, depending on regulatory guidance, and digital and cryptocurrency infrastructure development in Cameroon. That said, it is not self-evident that stablecoins would enable Yannick's wages to be sent in a way that is cheaper than or superior to technology based on traditional or centralized infrastructure.
Lack of digital financial history		This barrier is not present in this scenario.
Minimum balance requirements	✕	MAYBE – Once Yannick can access stablecoins, a stablecoin account can serve as an alternative deposit account without balance minimums. This may prove beneficial, although it is also available with other bank account options accessible to Yannick today.

Stablecoins are currently unable to solve Yannick's financial challenges. In the future, depending on regulatory clarity and the development of digital infrastructure and local cryptocurrency services in Cameroon, they may be able to offer an alternative method for him to receive his wages from the US. In this case, convenience relative to pre-existing digital transfer services must be considered, as digital remittance providers today allow for Yannick to receive his wages to his bank account, although in Cameroon they sometimes have unfavourable exchange rates.

Both stablecoins and digital remittance providers would require Yannick's employer to undergo an additional step of performing a foreign exchange transaction and sending funds to a new service.

Ultimately, to evaluate the options for the most convenient and least expensive manner for Yannick to receive his wages, further study must be conducted comparing the total costs of all three options: money transmitter with in-person offices, digital money transmitter and stablecoins.

As a reminder, Yannick is not representative of the average Cameroonian in his financial access. He has an ID, bank account, strong digital and financial literacy, and sufficient resources to engage in financial services. He does, however, remain partially excluded due to a combination of domestic and international financial infrastructures that limit his ability to access financial services that would meet his needs, particularly without reliance on intermediaries.

Conclusion

In response to strong interest and claims regarding the ability of stablecoins to promote financial inclusion around the world, this white paper builds off prior research and new interviews to investigate the value proposition of stablecoins for this purpose, using three realistic and data-driven case studies.

This paper seeks to answer the following questions:

1. How, if at all, do stablecoins improve financial inclusion, compared to other pre-existing options?

2. What new challenges or risks, if any, might stablecoins introduce, and what conditions must be met for them to be successful in supporting financial inclusion among underserved individuals and communities?

3. What is the net conclusion for their current value proposition, considering benefits, trade-offs and limitations?

Overall, at the present time stablecoins do not present features or capabilities that significantly reduce the specific barriers to financial inclusion in the scenarios studied – compared to pre-existing options, once accounting for consistent legal and compliance requirements. Stablecoins are subject to many of the same adoption and inclusion hurdles as other forms of retail finance, such as reliable internet and electricity, digital and financial literacy, and government identity documentation.

Decentralization in technology infrastructure itself does not reduce the cost of cross-border transactions. Generally, competition in remittance providers, remittance volumes and accommodating AML/CFT and other regulations are among the leading factors that correspond with lower remittance prices.

To the extent stablecoins are accessible to the financially underserved, they may introduce important risks, including financial failure at the stablecoin provider from illiquidity or insolvency, lost or stolen access to funds in digital wallets or exchanges, and technical failure at the underlying blockchain or smart contract levels. Many of these risks are currently the subject of extensive remedy efforts, but the outcomes are not certain. In addition, without significant investment in education, individuals may be at higher risk of suffering losses from user error or of purchasing stablecoins with riskier technical and financial management practices.

The blockchain, cryptocurrency and stablecoin ecosystems are continuously evolving, and certain capacities may develop in the future that present more benefits to end-users that are unbanked or unable to access relevant and suitable financial services. These opportunities might relate to open and interoperable DLT-based ecosystems, publicly visible payment histories, innovations with decentralized digital identity and compliance, or simply filling gaps where other services do not yet exist. That said, further research or demonstration of stablecoins' abilities to offer these opportunities and address complications (e.g. those related to privacy for publicly visible payment histories) is needed.

Endnotes

1. "Unbanked" individuals, usually the very poor, do not have a bank account or a transaction account at a formal financial institution or mobile money provider. "Underbanked" individuals are those who may have access to a basic transaction account with a formal financial institution but still have financial needs that are unmet. For instance, while they may be able to send or receive money, it may not be in a safe or affordable manner. For further discussion, see: The World Bank, *The Global Findex Database 2017*, https://globalfindex.worldbank.org/.
2. "Financial Inclusion", *The World Bank*, https://www.worldbank.org/en/topic/financialinclusion.
3. For instance see: Thomason, Jane, "Stablecoin adoption and the future of financial inclusion", *CoinTelegraph*, 19 August 2021, https://cointelegraph.com/news/stablecoin-adoption-and-the-future-of-financial-inclusion.
4. The extent and complexity of the factors contributing to financial exclusion are beyond the scope of this paper. For further discussion, see: The World Bank, *The Global Findex Database 2017*, https://globalfindex.worldbank.org/.
5. Makuvaza, Leonard, et al., *Means to an end: A conceptual framework for outcomes of financial service usage,* insight2impact, July 2018, https://cenfri.org/wp-content/uploads/2018/08/A-conceptual-framework-for-outcomes-of-financial-service-usage_i2i_July-2018.pdf.
6. As of the time of writing, the latest version of *The Global Findex Database* is from 2017. As a result, the data may be outdated and does not capture the effects of the COVID-19 pandemic. Where available, the authors have attempted to identify more recent data using other sources.
7. Central Bank of Kenya, Kenya National Bureau of Statistics (KNBS) and Financial Sector Deepening Kenya (FSD Kenya), *2019 FinAccess Household Survey*, April 2019, https://www.centralbank.go.ke/uploads/financial_inclusion/1035460079_2019%20FinAcces%20Report%20(web).pdf.
8. The World Bank, *The Global Findex Database 2017*, https://globalfindex.worldbank.org/.
9. The researcher should consider validating the relevance of the framework and assumptions in this white paper to other scenarios on a case-by-case basis.
10. For additional information and a detailed discussion of the risks associated with different types of stablecoins, see: Catalini, C. and de Gortari, A., *On the Economic Design of Stablecoins*, SSRN, Elsevier, 5 August 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499.
11. "Today's Cryptocurrency Prices by Market Cap", *CoinMarketCap*, https://coinmarketcap.com/. Accessed 15 September 2021.
12. For deeper discussion on technology differences and risks among stablecoins, see: Narula, Neha, "The Technology Underlying Stablecoins", *Neha's Writings*, 23 September 2021, https://nehanarula.org/2021/09/23/stablecoins.html. For an explanation of Diem, see: "Diem White Paper v2.0 – Cover Letter", *Diem Association*, https://www.diem.com/en-us/white-paper/#cover-letter.
13. For further discussion, see the white paper in this series: *Digital Currency Consumer Protection Risk Mapping*.
14. In India, stablecoins and cryptocurrency may also overcome a cultural preference towards cash that results from an effort to evade taxes. This could occur where individuals are not required to submit identifying information in stablecoin wallets or exchanges, allowing them to utilize stablecoins without necessarily being subject to tax reporting or other oversight. As this issue strengthens illicit activity and is contradictory to public policy goals, it is not listed as a benefit in this report.
15. Abramova, Svetlana, et al., *Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users*, Association for Computing Machinery, May 2021, http://lersse-dl.ece.ubc.ca/record/337/files/bits_mattress.pdf. For example, see p.13: "Cypherpunks opt for self-managed security solutions, whereas hodlers and rookies appear to face a non-trivial dilemma between risk-prone but convenient custodial solutions and secure but more burdensome non-custodial wallets."
16. The World Economic Forum's Global Future Council on Cryptocurrencies issued a paper that includes examples of opportunities relating to cryptocurrencies; the same opportunities may exist for stablecoins. For further discussion, see: World Economic Forum, *Crypto, What Is It Good For? An Overview of Cryptocurrency Use Cases*, December 2020, https://www3.weforum.org/docs/WEF_Cryptocurrency_Uses_Cases_2020.pdf.
The Forum's newly launched Crypto Impact & Sustainability Accelerator (CISA) will engage in research focused on assessing under what circumstances cryptocurrency systems might provide increased social benefit.
17. Catalini, Christian, and Joshua S. Gans, *Some Simple Economics of the Blockchain*, 2016, https://www.nber.org/system/files/working_papers/w22952/w22952.pdf.
18. "Remittances to Developing Countries Decline for Second Consecutive Year", *The World Bank*, 21 April 2017, https://www.worldbank.org/en/news/press-release/2017/04/21/remittances-to-developing-countries-decline-for-second-consecutive-year?utm_content=buffer0dcae&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

19. Stablecoins currently require the use of smartphones rather than feature phones because of their large transaction byte size. For example, the average bitcoin transaction size is 732 bytes (calculated over a 30-day period ending 15 June 2021, by dividing a 1.3MB average block size by the 1,774 average number of transactions over the same period). Feature phones typically employ Unstructured Supplementary Service Data (USSD) for mobile money and instant messaging. USSD only supports 160-byte transactions.
See:

    1) "Average Transactions Per Block", *Blockchain.com*, https://www.blockchain.com/charts/n-transactions-per-block.

    2) Calabia, Christopher, *Could the Poor Bank on Stablecoins?*, July 2020, p.4, https://www.findevgateway.org/sites/default/files/publications/submissions/72141/Calabia_Could_the_Poor_Bank_on_Stablecoins_20200721_Final.pdf. Note that hardware options that are not reliant on smartphone technology, such as cards, are the subject of much development activity.

20. The price levels of Honduras, the US, India and Cameroon have all been subdued in recent years, as of the time of writing.

21. See:

    1) Auer, Raphael et al., *CBDCs beyond borders: results from a survey of central banks*, Bank for International Settlements, June 2021, https://www.bis.org/publ/bppdf/bispap116.pdf.

    2) Berg, Andrew and Borensztein, Eduardo, *The Pros and Cons of Full Dollarization*, International Monetary Fund, 2000, https://www.imf.org/external/pubs/ft/wp/2000/wp0050.pdf.

22. "Use of stablecoins in DeFi has risen sharply in the last year, with more than 25% of a top USD stablecoin's supply locked in the top DeFi protocols such as Uniswap, Sushiswap, Curve, MakerDAO, Aave, and Compound." Source: Catalini, Christian and de Gortari, Alonso, *On the Economic Design of Stablecoins*, SSRN, 5 August 2021, p.6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499:

23. For more information on DeFi, see: World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, June 2021, https://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.

24. This discussion focuses on first-order impacts to individuals and small businesses; any macroeconomic challenges and risks that may exist are outside the scope of this white paper.

25. "DFS Continues to Foster Responsible Growth in New York's Fintech Industry with New Virtual Currency Product Approvals" [Press release], *Department of Financial Services*, 10 September 2018, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1809101.

26. "Today's Cryptocurrency Prices by Market Cap", *Coinmarketcap*, https://coinmarketcap.com/. Accessed 15 September 2021.

27. See:

    1) "Reserves Breakdown at March 31, 2021", *Tether*, https://tether.to/wp-content/uploads/2021/05/tether-march-31-2021-reserves-breakdown.pdf.

    2) "Independent Accountant's Report – Tether Holdings Limited", *Moore Cayman*, 6 August 2021, https://tether.to/wp-content/uploads/2021/08/tether_assuranceconsolidated_reserves_report_2021-06-30.pdf.

    3) "Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities In New York" [Press release], *Letitia James, NY Attorney General,* 23 February 2021, https://ag.ny.gov/press-release/2021/attorney-general-james-ends-virtual-currency-trading-platform-bitfinexs-illegal.

28. For illustration, see: Catalini, Christian and de Gortari, Alonso, *On the Economic Design of Stablecoins*, SSRN, 5 August 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899499.

29. For deeper discussion on technology differences and risks among stablecoins, see: Narula, Neha, "The Technology Underlying Stablecoins", *Neha's Writings*, 23 September 2021, https://nehanarula.org/2021/09/23/stablecoins.html.

30. See:

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

    2) Auer, Raphael, *Beyond the doomsday economics of "proof-of-work" in cryptocurrencies*, Bank for International Settlements, January 2019, https://www.bis.org/publ/work765.htm.

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

31. Additional information on the "gender gap" in access to digital or financial services can be found in the following resources:

    1) Kuroda, Reiko, *Policy Brief: The Digital Gender Gap*, GSMA, 2019, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Equity-Policy-Brief-W20-Japan.pdf.

    2) GSMA, *The Mobile Gender Gap Report 2020*, 2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf.

32. Based on an analysis of cryptocurrency users in the US. The report further finds no evidence that cryptocurrency is sought as an alternative to mainstream finance. For further discussion, see: Auer, Raphael and Tercero-Lucas, David, *Distrust or speculation? The socioeconomic drivers of U.S. cryptocurrency investments,* Bank for International Settlements, July 2021, https://www.bis.org/publ/work951.html.

33. DeFi applications that are unregulated and lack consumer protections can leave individuals at risk of harm from loss of funds related to those applications. These include the risks listed in this section, as well as issues related to lending, leveraged investment and other activities available in DeFi.

34. Gorton, Gary B. and Zhang, Jeffery, *Taming Wildcat Stablecoins*, SSRN, September 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888752.

35. For further discussion, see:

    1) Tito Nícias Teixeira da Silva Filho, "No Easy Solution: A Smorgasbord of Factors Drive Remittance Costs", *International Monetary Fund*, 30 July 2021, https://www.imf.org/en/Publications/WP/Issues/2021/07/30/No-Easy-Solution-A-Smorgasbord-of-Factors-Drive-Remittance-Costs-462130.

    2) Beck, Thorsten et al., "What explains the cost of remittances", *VoxEU*, 28 September 2009, https://voxeu.org/article/what-explains-cost-remittances.

    3) Martinez Peria, Maria Soledad, "What Drives the Price of Remittances?: New Evidence Using the Remittance Prices Worldwide Database", *World Bank Blogs*, 6 August 2010, https://blogs.worldbank.org/allaboutfinance/what-drives-the-price-of-remittances-new-evidence-using-the-remittance-prices-worldwide-database.

36. For additional discussion on this topic, see: Calabia, Christopher, *Could the Poor Bank on Stablecoins?*, July 2020, https://www.findevgateway.org/sites/default/files/publications/submissions/72141/Calabia_Could_the_Poor_Bank_on_Stablecoins_20200721_Final.pdf.

37. For stablecoins to succeed in financial inclusion today, off-ramps to fiat money are necessary as stablecoins are not currently generally accepted for payments.

38. For additional discussion on this topic, see: Calabia, Christopher, *Could the Poor Bank on Stablecoins?*, p.3, July 2020, https://www.findevgateway.org/sites/default/files/publications/submissions/72141/Calabia_Could_the_Poor_Bank_on_Stablecoins_20200721_Final.pdf.

39. Regulatory approval of stablecoins and cryptocurrency also enable infrastructure development related to exchanges and banking connections that can enable greater convenience and access to stablecoins in a jurisdiction. For additional discussion on the topic of whether stablecoins will comply with local e-money regulations that are meant to protect customer funds, see: Calabia, Christopher, *Could the Poor Bank on Stablecoins?*, p.6, July 2020, https://www.findevgateway.org/sites/default/files/publications/submissions/72141/Calabia_Could_the_Poor_Bank_on_Stablecoins_20200721_Final.pdf.

40. Acceptance can be driven by success in the aforementioned issues in this list. As a separate issue, increasingly in the US, major technology providers like PayPal, Visa and Mastercard are enabling more cryptocurrency-to-fiat interconnections. Related to merchant acceptance, PayPal now allows US users who purchase cryptocurrency within its platform to spend that cryptocurrency on purchases with many US merchants. Merchant acceptance in this case does not change as merchants receive fiat currency that is converted from cryptocurrency by PayPal. That said, users are able to spend the cryptocurrency with merchants. Such early examples may point to the ability to side-step issues related to merchant acceptance of cryptocurrency.

    For further discussion, see: Fleishman, Glenn, "PayPal now lets you spend cryptocurrency at millions of U.S. merchants", *Fast Company*, 30 March 2021, https://www.fastcompany.com/90620101/paypal-cryptocurrencybitcoin?partner=rss&utm_source=rss&utm_medium=feed&utm_campaign=rss+fastcompany&utm_content=rss.

41. See Celo with Pesabase and Toca for an example of efforts to enable stablecoin payments on feature phones. For further discussion, see: Calabia, Christopher, *Could the Poor Bank on Stablecoins?*, p.4, July 2020, https://www.findevgateway.org/sites/default/files/publications/submissions/72141/Calabia_Could_the_Poor_Bank_on_Stablecoins_20200721_Final.pdf.

42. See:

    1) Sobiech, Izabela, "Remittances, finance and growth: Does financial development foster the impact of remittances on economic growth?", *World Development*, Elsevier, vol. 113, 2019, pp. 44-59, https://ideas.repec.org/a/eee/wdevel/v113y2019icp44-59.html.

    2) Fayissa, Bichaka, and Nsiah, Christian, "The Impact of Remittances on Economic Growth and Development in Africa", *The American Economist*, 2008, www.researchgate.net/publication/5182511_The_Impact_of_Remittances_on_Economic_Growth_and_Development_in_Africa.

    3) Portes, Luis San Vicente, "Remittances, Poverty And Inequality", *Journal Of Economic Development*, vol. 34(1), 2009, pp. 127-140, https://ideas.repec.org/a/jed/journl/v34y2009i1p127-140.html.

43. "Defying Predictions, Remittance Flows Remain Strong During COVID-19 Crisis" [Press Release], *The World Bank*, 12 May 2021, https://www.worldbank.org/en/news/press-release/2021/05/12/defying-predictions-remittance-flows-remain-strong-during-covid-19-crisis.

44. The World Bank, *Remittance Prices Worldwide Quarterly*, Issue 37, March 2021, https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q121_final.pdf.

45. The World Bank, *Remittance Prices Worldwide Quarterly*, Issue 37, March 2021, https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q121_final.pdf.

46. Xoom (a PayPal Service), *Time is Money: How Digital Remittances Save Valuable Time for Americans and their Families around the World*, 2020, https://publicpolicy.paypal-corp.com/sites/default/files/policy/Time_is_Money_Xoom_Report.pdf.

47. Xoom (a PayPal Service), *Time is Money: How Digital Remittances Save Valuable Time for Americans and their Families around the World*, 2020, https://publicpolicy.paypal-corp.com/sites/default/files/policy/Time_is_Money_Xoom_Report.pdf.

48. Remittance inflows into Honduras constitute a significant source of income for many people. World Bank data estimates that migrant remittance inflows totalled more than $5 billion in 2020, representing 23% of the country's GDP. For further discussion, see: "Personal remittances, received (% of GDP) – Honduras" [infographic], *The World Bank*, 2020, https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=HN.

49. World Bank data shows there are 78 mobile phone subscriptions in Honduras per 100 people, which is well below the averages in Latin America and the Caribbean (100) and the World (109). For further discussion, see: "Mobile cellular subscriptions (per 100 people) – Honduras" [infographic], *The World Bank*, https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=HN&name_desc=false.

    Additionally, the GSMA notes that although 72% of Hondurans have access to mobile broadband, only 22% subscribe. Security concerns, especially for women in Latin America, are linked to limited cell phone usage, as many cite fears of being robbed due to the possession of mobile phone devices.

    For further discussion, see: Sharma, Akanksha and Arese Lucini, Barbara, *Connected Society: Digital inclusion in Latin America and the Caribbean*, GSMA, 2016, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/02/Connected-Society-Digital-inclusion-in-Latin-America-and-the-Caribbean-1.pdf.

50. "The World Bank in Honduras", *The World Bank*, https://www.worldbank.org/en/country/honduras.

51. "Honduras, 2017," *Global Financial Inclusion (Global Findex) Database 2017*, The World Bank, 2018, https://microdata.worldbank.org/index.php/catalog/3357.

52. Tigo Money, https://www.tigo.com.hn/tigo-money/remesas-internacionales.

53. "Sending money from United States to Honduras", *Remittance Prices Worldwide*, The World Bank, https://remittanceprices.worldbank.org/en/corridor/United-States/Honduras.

54. Only 17% of Hondurans (age 15+) own a debit card, while only 14% used a credit card (or borrowed from a financial institution) in 2017. For further discussion, see: "Honduras, 2017", *Global Financial Inclusion (Global Findex) Database 2017*, The World Bank, 2018, https://microdata.worldbank.org/index.php/catalog/3357.

55. The public health system in Honduras suffers from significant challenges related to underfunding, corruption and lack of medical and physician resources. For further discussion, see:

    1) Carmenate-Milián, Lino, et al. "Situation of the Health System in Honduras and the New Proposed Health Model." *Archives of Medicine*, IMedPub, 2017, https://www.archivesofmedicine.com/medicine/situation-of-the-health-system-in-honduras-and-the-new-proposed-health-model.php?aid=19759.

    2) Palencia, Gustavo. "Honduras Arrests Ex-Social Security Chief in $200 Million Graft Bust," *Thomson Reuters*, 9 September 2014, www.reuters.com/article/uk-honduras-crime-idUKKBN0H41XA20140909;

    3) Eppenauer, Alexandra, "Six Facts About Healthcare in Honduras", *The Borgen Project*, 12 August 2018, https://borgenproject.org/healthcare-in-honduras/.

56. Personal interview, Lucia Gallardo, 26 April 2021 (virtual).

57. "Literacy rate, adult (% of people ages 15 and above) – Honduras" [infographic], *The World Bank*, September 2021, https://data.worldbank.org/indicator/SE.ADT.LITR.ZS?locations=HN.

58. "S&P Global Finlit Survey", *Global Financial Literacy Excellence Center (GFLEC)*, 2021, https://gflec.org/initiatives/sp-global-finlit-survey/.

59. See:

    1) "Intentional homicides (per 100,000 people) – Honduras" [infographic], *The World Bank*, https://data.worldbank.org/indicator/VC.IHR.PSRC.P5.

    2) "Honduras - Events of 2020", *World Report 2021*, Human Rights Watch, https://www.hrw.org/world-report/2021/country-chapters/honduras#.

60. "Honduras, 2017", *Global Financial Inclusion (Global Findex) Database 2017*, The World Bank, 2018, https://microdata.worldbank.org/index.php/catalog/3357.

61. According to research by the American Immigration Council, citing data from the IRS, 4.4 million people used an ITIN to pay taxes in 2015. However, the Office of Immigration Statistics estimated almost 12 million undocumented immigrants were in the US as of January 2015, according to a Brookings report. For further discussion, see:

    1) "The Facts About the Individual Taxpayer Identification Number (ITIN)", *American Immigration Council*, 15 September 2021, www.americanimmigrationcouncil.org/research/facts-about-individual-taxpayer-identification-number-itin.

    2) Kamarck, Elaine and Stenglein, Christine, "How many undocumented immigrants are in the United States and who are they?", *Brookings*, 12 November 2019, https://www.brookings.edu/policy2020/votervital/how-many-undocumented-immigrants-are-in-the-united-states-and-who-are-they/.

62. "Sending money from United States to Honduras", *Remittance Prices Worldwide*, The World Bank, https://remittanceprices.worldbank.org/en/corridor/United-States/Honduras.

63. According to survey data, the average monthly income for a person working in Honduras is HNL 28,100 (equivalent to approximately $1,158), including housing, transport and other benefits. For further discussion, see: "Average Salary in Honduras 2021", *Salary Explorer*, 2021, http://www.salaryexplorer.com/salary-survey.php?loc=96&loctype=1.

64. "Sending money from United States to Honduras", *Remittance Prices Worldwide*, The World Bank, https://remittanceprices.worldbank.org/en/corridor/United-States/Honduras.

65. "Honduras, 2017", *Global Financial Inclusion (Global Findex) Database 2017,* The World Bank, 2018, https://microdata.worldbank.org/index.php/catalog/3357.

66. "Sending money from United States to Honduras", *Remittance Prices Worldwide*, The World Bank, https://remittanceprices.worldbank.org/en/corridor/United-States/Honduras.

67. Note that if cryptocurrency that is sent as a remittance has appreciated in value since the user received or purchased it (for instance if the holder is sending bitcoin and the price of bitcoin has risen), that gain may be subject to tax in certain jurisdictions. Stablecoins seek to maintain a stable value and, if successful, would not generally generate significant price appreciation or capital gains.

68. See Compound, https://app.compound.finance/ and Aave, https://aave.com/. Accessed 26 October 2021.

69. TrueFi is one example. It offers uncollateralized loans and in the future hopes to incorporate data generated outside the blockchain ecosystem. For further discussion, see: "Introducing TrueFi, the DeFi Protocol for Uncollateralized Lending", *TrustToken*, 5 November 2020, https://blog.trusttoken.com/introducing-truefi-the-defi-protocol-for-uncollateralized-lending-9bfd6594a48.

70. "Small and Medium Enterprises (SMEs) Finance", *The World Bank*, https://www.worldbank.org/en/topic/smefinance.

71. "Understanding the impact of loans on small businesses in India", *CDC Group*, 20 July 2020, https://www.cdcgroup.com/en/emerging-markets-investment/understanding-the-impact-of-loans-on-small-businesses-in-india/.

72. Ranade, Ajit, "Opinion: The big funding challenge that small businesses face", *Mint*, 2020 [Updated 20 April 2020], https://www.livemint.com/opinion/columns/opinion-the-big-funding-challenge-that-small-businesses-face-11587400832891.html.

73. See:

    1) Singh, Roshika and Chhabra, Pratibha, *Financial Inclusion for Women-Owned Micro, Small & Medium Enterprises (MSMEs) in India*, International Finance Corporation, World Bank Group, 2021, https://www.indiaspend.com/uploads/2021/02/20/file_upload-417397.pdf.

    2) Singh, Shalini, "Why women run fewer than 13% of India's small businesses", *Scroll.in*, 2 March 2021, https://scroll.in/article/988166/why-women-run-fewer-than-13-of-indias-small-businesses.

74. Digital identity is not a challenge in this scenario. An "Aadhaar" is the unique ID number issued to all Indian residents, who obtain their Aadhaar card by providing their fingerprints, retina scans and face photos. This underlying biometric database holds the information of 1.2 billion enrolments or about 89% of India's population. See: Aadhaar, https://uidai.gov.in/.

75. See:

    1) Bhat, Swati, and Jadhav, Rajendra, "Love of cash hinders India's move to digital economy", *Thompson Reuters*, 14 November 2019, https://www.reuters.com/article/us-india-demonetisation/love-of-cash-hinders-indias-move-to-digital-economy-idUSKBN1XO05J.

    2) Ligon, Ethan et al., "What explains low adoption of digital payment technologies? Evidence from small-scale merchants in Jaipur, India", *PLoS ONE*, vol. 14, no. 7, 2019, https://doi.org/10.1371/journal.pone.0219450. According to p.1: "Therefore, low rates of adoption do not appear to be the result of supply-side barriers, but due rather to demand-side factors or taxes. We find direct evidence of such demand-side factors, such as a perceived lack of customers wanting to pay digitally, and concerns that records of mobile payments might increase tax liability."

76. A line of credit is a pre-set borrowing limit that can be used at any time. The borrower can take money out as needed until the limit is reached. As money is repaid, it can be borrowed again.

77. Jain, Aashika, "Motor Insurance In India Has A New Hope In Digital", *Forbes Advisor*, 2020 [updated 17 December 2020], https://www.forbes.com/advisor/in/car-insurance/motor-insurance-has-a-new-hope-in-digital/.

78. Narang, Sharad, "Vehicle Theft in India is the Fastest Growing Type of Crime in India", *BO Herald*, 18 July 2019, https://boherald.com/vehicle-theft-in-india-is-the-fastest-growing-type-of-crime-in-india/.

79. Klapper, Leora, et al., *Financial Literacy Around the World: Insights from the Standard & Poor's Ratings Services Global Financial Literacy Survey*, 2015, https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf?x27564.

80. See:

    1) 2017 Findex data: 24% of women and 40% of men report having a debit card; 38% of women vs. 50% of men cite being able to come up with emergency funds; 76% of women and 82% of men report having an account at a financial institution; 1.3% of women and 3.1% of men report having a mobile money account. Source: "India, 2017," *Global Financial Inclusion (Global Findex) Database 2017*, The World Bank, 2018, https://microdata.worldbank.org/index.php/catalog/3362.

    2) According to 2020 GSMA data, 63% of women and 79% of men own or are a primary user of a mobile phone. Moreover, 21% of women and 42% of men are mobile-phone internet users. Source: GSMA, *The Mobile Gender Gap Report 2020*, 2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf.

81. Singh, Shalini, "Why women run fewer than 13% of India's small businesses", *Scroll.in*, 2 March 2021, https://scroll.in/article/988166/why-women-run-fewer-than-13-of-indias-small-businesses.

82. Keelery, Sandhya, "Internet usage in India – statistics & facts", *Statista*, 2 August 2021, https://www.statista.com/topics/2157/internet-usage-in-india/.

83. See:

    1) McKinsey Global Institute, *Digital India: Technology to transform a connected nation*, March 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/MGI-Digital-India-Report-April-2019.pdf.

    2) GSMA, *The Mobile Gender Gap Report 2020*, 2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/05/GSMA-The-Mobile-Gender-Gap-Report-2020.pdf.

84. S&P Global, *2020 India Mobile Payments Market Report*, 2020, https://www.spglobal.com/marketintelligence/en/documents/indiamobilepayments_2020finalreport.pdf.

85. S&P Global, *2020 India Mobile Payments Market Report*, 2020, https://www.spglobal.com/marketintelligence/en/documents/indiamobilepayments_2020finalreport.pdf.

86. McKinsey Global Institute, *Digital India: Technology to transform a connected nation*, March 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/MGI-Digital-India-Report-April-2019.pdf.

87. Stablecoins might address the reasons why Indians prefer cash – for example, avoidance of taxes or of higher prices for goods purchased at smaller merchants. For the former, stablecoin-based payments may aid in the avoidance of taxes, where tax reporting and customer identity and compliance controls at wallets and exchanges are not effective at reporting taxable transactions to authorities. Of course, from a policy perspective, this activity would be detrimental. In relation to Indians' latter preference for cash, it is not axiomatic that small businesses would be able to process stablecoins more cheaply than other electronic payment processing, as the stablecoins may involve network transaction fees or new merchant acceptance technology. Merchants may also be hesitant to accept stablecoins if they are not confident in their backing.

88. See discussion in scenario 1 on additional risks and issues with insurance operated on decentralized applications.

89. Nahar, Pawan, "Future of Cryptos in India: A blanket ban or birth of a new age asset class?", *The Economic Times*, 20 August 2021, https://economictimes.indiatimes.com/markets/cryptocurrency/future-of-cryptos-in-india-a-blanket-ban-or-the-new-age-asset-class/articleshow/85489406.cms?from=mdr.

90. Mastercard and Kaiser Associates, *The Global Gig Economy: Capitalizing on a ~$500B Opportunity*, May 2019, https://newsroom.mastercard.com/wp-content/uploads/2019/05/Gig-Economy-White-Paper-May-2019.pdf.

91. Africa Growth Initiative at Brookings, *Foresight Africa: Top Priorities for the Continent in 2019*, 2019, p. 11, https://www.brookings.edu/wp-content/uploads/2019/01/BLS18234_BRO_book_007_WEB.pdf.

92. GSMA, *The Mobile Economy: Sub-Saharan Africa 2020*, 2020, p. 6, www.gsma.com/mobileeconomy/wp-content/uploads/2020/09/GSMA_MobileEconomy2020_SSA_Eng.pdf.

93. Kässi, Otto, and Lehdonvirta, Vili, "Online labour index: Measuring the online gig economy for policy and research", *Technological Forecasting and Social Change*, vol. 137, 2018, pp. 241-248, https://www.sciencedirect.com/science/article/abs/pii/S0040162518301331?via%3Dihub.

94. This scenario is informed by a series of virtual and on-the-ground interviews with Cameroonians by World Economic Forum staff between February and May 2021. Interviewees are anonymous to preserve their privacy.

95. "Cameroon, 2017", *Global Financial Inclusion (Global Findex) Database 2017*, The World Bank, 2018, https://microdata.worldbank.org/index.php/catalog/3331.

96. Micro-insurance only has a 1.8% coverage rate in Cameroon. For further discussion, see: Nana Djomo Jules Médard and Ngouana Koudjou Serges Rodrigue, *Determinants of Demand for Micro-insurance in Cameroon*, African Economic Research Consortium, No. 728, 2020, http://publication.aercafricalibrary.org/bitstream/handle/123456789/1199/PB_728_Nana%20%26%20Ngouana.pdf?sequence=1&isAllowed=y.

97. Also known as tontine, a *Njangi* is a community savings and lending group where individuals pool money together to help each other meet their goals. A fixed amount is contributed by each member of the *Njangi* every month and is held by the treasurer. Each month, one member of the Njangi draws the full amount contributed by all members. Therefore, it functions as an interest-free loan because an individual may take the full amount pooled in January but pays it off throughout the rest of the year through his or her monthly contributions to the *Njangi*. The conditions surrounding each *Njangi* may differ according to the established purpose. Many *Njangis* have an account at a formal financial institution and can therefore offer additional access to credit, hence loans, for members.

98. The others are Rwanda, Kenya, Liberia, Malawi, Sierra Leone and Uganda. Source: The World Bank, *The Global Findex Database 2017*, 2018, p. 77, https://globalfindex.worldbank.org/.

99. "Data Bundles: Giga Surf", *MTN Cameroon*, 2021, https://mtn.cm/personal/internet/data-bundles/giga-surf/.

100. There are initiatives such as Izikare (a start-up that enables Africans in the diaspora to purchase health insurance policies for their family members on the continent) that are trying to fill this gap. However, it is largely insufficient. Izikare is not a local solution that would enable someone like Yannick to purchase his own insurance. See: "L'Assurance santé facile pour mes proches en Afrique", *Izikare*, 2021, https://izikare.com/.

101. Coinbase presents one example. It supports limited functionality for receiving, exchanging and sending cryptocurrency. See: Coinbase, https://www.coinbase.com/places/cameroon.

102. Baker McKenzie, *Blockchain and Cryptocurrency in Africa*, 2018, p. 18, https://www.bakermckenzie.com/-/media/files/insight/publications/2019/02/report_blockchainandcryptocurrencyreg_feb2019.pdf.

103. The cryptocurrency ecosystem in Cameroon is evolving. Some services (e.g. Uphold) allow individuals to purchase cryptocurrency using their debit or credit cards in Cameroon. See: Uphold, https://uphold.com/en-us.

104. The high energy consumption of cryptocurrencies and associated costs might hinder supportive policy, as demonstrated by the energy concerns that emerged following the government's pilot of a digital currency called Trest in 2015. For further discussion, see: Baker McKenzie, *Blockchain and Cryptocurrency in Africa*, 2018, p. 18, https://www.bakermckenzie.com/-/media/files/insight/publications/2019/02/report_blockchainandcryptocurrencyreg_feb2019.pdf.

105. The Central African Deposit Guarantee Fund (FOGADAC) guarantees up to 30 million FCFA in banks and 5 million FCFA in non-deposit collecting financial institutions. For further discussion, see: International Monetary Fund, *Central African Economic and Monetary Community (CEMAC): Financial Stability Assessment*, April 2016, https://www.imf.org/external/pubs/ft/scr/2016/cr16106.pdf.

106. An option could be Afriland First Bank which requires a minimum account balance of 50,000 FCFA for a basic savings account. See: "Passbook Savings Account", *Afriland First Bank*, https://www.afrilandfirstbank.com/index.php/en/individual1/individuals-account/savings-account.

5/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Blockchain-Based Digital Currency and Tools for Cross-Border Aid Disbursement

WHITE PAPER

NOVEMBER 2021

Images: Getty Images

Contents

Preface 130

Context of humanitarian aid 131

1 Priorities for blockchain-based digital currencies in humanitarian aid 132

- 1.1 Last-mile connectivity and device accessibility 132
- 1.2 Digital identity gap 133
- 1.3 Know Your Customer (KYC) challenges 133
- 1.4 Ethics 134
- 1.5 Programmable aid 134
- 1.6 A humanitarian stablecoin? 135
- 1.7 CBDC for cross-border humanitarian aid 135

2 Pilot projects for blockchain-based digital humanitarian aid 136

- 2.1 Benefits and challenges of digital aid pilot projects 136
- 2.2 A selection of blockchain-based digital aid pilot projects 137

Conclusion 146

Appendix 147

Endnotes 153

Preface

This paper explores the applications of digital currencies and blockchain-based tools for cross-border development and humanitarian aid delivery and disbursement.

The biggest challenges facing cross-border aid disbursement are human, process and geopolitical challenges, which technology alone cannot remedy. The introduction of a blockchain-based digital currency will, at most, only ever solve a piece of a much larger problem. Nevertheless, with this reality in mind, there is a range of cross-border aid pilots that are being conducted using blockchain-based digital aid solutions. Serious ethical questions and nuances arise regarding the testing of emerging technologies on people who may be caught up in crisis or find themselves in a vulnerable state, as there are considerable risks to tracking targeted groups of people.

However, vulnerable populations risk being left behind as technology advances. Humanitarian organizations can mitigate this risk by gaining a deep understanding of the possibilities offered by the future of money and new technologies, and by committing to bring the value of those technologies to underserved people. Given the current momentum and volume of pilot projects, it is likely that cross-border aid disbursement will continue to include and even increase the use of blockchain-based digital aid over the next 10 years. It is therefore important to keep exploring ways in which these technologies can deliver benefit to people who are underserved and in vulnerable situations. This is particularly true as legacy financial systems begin to incorporate digital currencies, which in turn may inadvertently enhance the digital divide.

This white paper examines both the promise and challenges posed by blockchain-based digital currencies, such as cryptocurrency and stablecoins, as well as blockchain-based tools and platforms, which create infrastructure aimed at improving cross-border humanitarian aid disbursement. The paper also examines whether these digital currencies and distributed ledger platforms could have a viable long-term net benefit to the way in which aid is disbursed to people in need globally. The paper does not focus on central bank digital currencies (CBDC), although this community may explore the use of CBDC for cross-border aid in the future.

Specifically, this white paper explores examples of pilot projects conducted by humanitarian aid organizations, which aim to test whether blockchain-based tools and currencies can enable cross-border aid transfers in a more efficient, transparent and less costly way than cash, commercial bank payments, or e-money. After a short section framing the context of cross-border humanitarian aid, the paper is divided into two chapters:

1. **Priorities for cross-border humanitarian aid** disbursement in which blockchain plays a role

2. **Examples of blockchain-based pilot projects** for cross-border humanitarian aid currently underway

This work is based on a review of literature describing the value and utilization of stablecoins and blockchain in humanitarian aid, as well as on primary research – including semi-structured interviews with leaders from major humanitarian organizations.

The target readership for this white paper includes:

– Individuals and organizations involved in the delivery of cross-border aid, such as humanitarian and development agencies, policy-makers, health authorities, private-sector investors and technologists who wish to learn about the value proposition of stablecoins for aid delivery and disbursement.

– Blended-finance investors, institutions and aid organizations that are keen to enhance ways of assessing the impact of aid projects.

Context of humanitarian aid

The primary objective of humanitarian assistance is to save lives, alleviate suffering and maintain human dignity during and after man-made crises and disasters associated with natural hazards, as well as to prevent and strengthen preparedness for when such situations occur. Today, over one billion people live in countries that are affected by long-term humanitarian crises.[1] The COVID-19 pandemic has exacerbated existing vulnerabilities, putting those living in fragility and poverty at even higher risk.

According to the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), 235 million people needed humanitarian assistance and protection in 2021. The UN estimated that it would require $35 billion to serve the 160 million of those in greatest need.[2]

Further, the humanitarian aid system itself is under pressure. The pandemic has further exposed its vulnerabilities and challenged its capacity to serve the growing numbers of those affected by crises. One positive development is the shift from in-kind assistance to cash transfers, which paves the way for the digitization of aid disbursements.[3]

Current challenges to cross-border aid are related to the cost of delivery and resource flows, inequality of access to global aid, and challenges with the accuracy of traceability and reporting. These are some of the ongoing challenges that organizations face as they assess the value of blockchain-based technologies and digital currencies in this space.

> **The potential traceability offered by stablecoins and distributed ledger technology opens the door for unprecedented innovations to monitor and assess the impact of aid-funded projects. However, such opportunity comes in tandem with the need to address complex human behaviour and judgement. Hence, it is important to study all interlinked dimensions including the technical, operational, legal and ethical aspects.**
>
> Rania Al-Mashat, Minister of International Cooperation, Ministry of International Cooperation of Egypt

1 Priorities for blockchain-based digital currencies in humanitarian aid

Based on our primary research and interview conversations, there is a consensus that human, process and contextual factors – such as collaboration between agencies and governments – have a greater impact on the effectiveness of humanitarian aid disbursement than the role new technologies are likely to play. Bearing that in mind, this chapter examines key priorities and questions which will need to be considered if blockchain-based tools and digital currencies are to be used for cross-border aid disbursement.

Blockchain-based currencies, such as stablecoins, cryptocurrencies and central bank digital currency (CBDC), should be used where they would have a net benefit for people in need of aid. For this reason, the future of blockchain-based technologies in aid should be grounded in a sound analysis of the benefits and risks as well as regulatory compliance.

In navigating the future of aid disbursement and the applicability of blockchain-based digital currencies, the following are some key barriers and issues to address. These need to be prioritized to realize the full value and effectiveness that digital technologies can bring to aid disbursement in the coming decades.

1.1 Last-mile connectivity and device accessibility

The breadth and reach of digital currency systems will depend on the strength of last-mile connectivity. This challenge will create major inequalities between places that invest in infrastructure and those that do not. Coverage of and access to internet systems in low-connectivity regions will be an important factor in the next 5-10 years.

Given disparities in access, most of the poorest customers are unlikely, for example, to be able to send and receive cryptocurrency via a device, until the costs of smartphones fall or the capabilities of feature phones rise.

Failing to consider the technology gap may, in turn, unintentionally reinforce the existing gender inequity in access to financial services. Women in lower- and middle-income countries are 8% less likely to own a mobile phone and 20% less likely to own a smartphone than men. Smartphone ownership rates may mean that historically excluded or underserved women could lag behind men in their ability to use stablecoins. This disparity in device accessibility could further the digital divide.[4]

1.2 Digital identity gap

New digital currencies in humanitarian aid could create the potential for financial inclusion, since the digital aid given to historically excluded people could incentivize them to join the financial system. However, over 1.1 billion people do not have government-issued IDs.[5] This ID gap is one of the key reasons why restrictive Know Your Customer (KYC) requirements present a significant barrier to financial inclusion. People lack government-issued IDs for a variety of reasons, but mainly because of government capacity failures. Other significant groups lacking official identity documentation include refugees and populations displaced by natural disasters and conflict. The provision of identity documents for such people will be a critical factor in advancing digital financial inclusion in the coming decade.

1.3 Know Your Customer (KYC) challenges

Often the most vulnerable people lack addresses or identification and are therefore excluded from financial services. Many have cell phones, they regularly communicate with relatives around the world and they may have some level of access to the internet. Yet they are unable to receive digital aid due to a lack of proper identification or because the cost of accessing that aid is exorbitant. Given the financial reality that disbursing digital aid entails facilitating smaller transaction amounts and account balances, it is imperative for policy-makers, entrepreneurs and innovators to enable and promote screening measures that are proportional to the context. One potential example from blockchain-based digital payments is an "unhosted wallet", a digital wallet that is not hosted by a financial institution, which can potentially serve the needs of many of the world's most vulnerable. However, it should be noted that unhosted wallets bear the risk of lost funds if passwords or keys are lost.[6]

The Bahamas CBDC, known as the "Sand Dollar", provides an example of pre-KYC onboarding. The network is designed to "provide non-discriminatory access to payment systems without regard for age, immigration or residency status, [so] government-issued identification is not an enrolment requirement". The limit for account balances is set at $500.[7]

KYC requirements in the context of digital humanitarian aid raise an important policy question, in which policy-makers should carefully weigh the advantages of lowering barriers to entering the financial system for the historically excluded against the potential risks of failing to prevent illicit activity. Another important policy consideration is the management of de-risking,[8] a practice in which financial institutions terminate or restrict business relationships with clients or categories of clients to avoid, rather than manage, risk.[9] De-risking digital aid in this way would largely block off the potential inclusion of the 1.7 billion people who are already historically excluded, simply creating a new digital version of a system that is already in place.

1.4 Ethics

Aid agencies operate according to commonly agreed humanitarian principles, although the application and interpretation of those principles may vary across organizations (see Table 1). Donors and implementing agencies will need to navigate ethical risks, responsibilities and trade-offs in the application of rapidly scaling technologies in the financial sector, such as digital currencies. These trade-offs include:

- Privacy and data protection risks *vs.* traceability and auditability
- The power of conducting remote aid disbursement *vs.* the potential of a new digital divide, which excludes populations that lack the requisite digital devices or literacy
- The risks for testing emerging technologies on already vulnerable populations *vs.* the importance of enabling access to financial services
- The positive impact of providing vulnerable populations with access to new digital currencies and stablecoins *vs.* the policy risks to governments from currency substitution and capital flight, particularly in smaller economies and those experiencing hyperinflation
- The potential to expand digital financial innovation to aid disbursement *vs.* the risk of crowding-out other means of payment (e.g. cash) that aid recipients currently have more access to and find to be relatively more secure

For further discussion of the potential risks posed by digital technology to beneficiaries in humanitarian aid contexts, refer to the subsection in the Appendix entitled Ethical considerations and the risk of digital harm.

TABLE 1 **Humanitarian Principles**[10]

Humanity	Neutrality	Impartiality	Independence
Human suffering must be addressed wherever it is found. The purpose of humanitarian action is to protect life and health and ensure respect for human beings.	Humanitarian actors must not take sides in hostilities or engage in controversies of a political, racial, religious or ideological nature.	Humanitarian action must be carried out on the basis of need alone, giving priority to the most urgent cases of distress and making no distinctions on the basis of nationality, race, gender, religious belief, class or political opinions.	Humanitarian action must be autonomous from the political, economic, military or other objectives that any actor may hold with regard to areas where humanitarian action is being implemented.

Source: United Nations Office for the Coordination of Humanitarian Affairs (OCHA)

1.5 Programmable aid

Advances in innovation make possible the concept of "programmable aid", which leverages software to automatically disburse digital aid to a set of predetermined ("pre-vetted") aid recipients' destination accounts. An example of this would be an aid agency account that can be programmed to rapidly distribute digital aid to all the households in a disaster-affected region within hours of the event. This would prevent the lengthy timelines and delays that are typical of aid programme fundraising, disbursement setup and delivery. As is currently possible with digital tokens such as food stamps, blockchain-based digital aid could also be programmed to be spent at certain qualified vendors or within certain geographic areas.

1.6 A humanitarian stablecoin?

Digital technologies have begun to disrupt the traditional model for one-off physical cash distributions by providing aid recipients with the infrastructure (digital wallets) for more financial services beyond basic consumption. Typically, aid organizations rely heavily on third-party banking and financial institutions, particularly for digital aid delivery. However, new fintech platforms and API-based designs open the possibility for humanitarian aid organizations to operate as regulated financial institutions (e.g. virtual asset service providers or VASPs). Related to this, our interview respondents raised the potential value that lies in a consortium of aid organizations creating a global stablecoin for aid disbursement. This idea remains largely hypothetical, although some aid organizations have expressed support for the concept.

One point of concern is that a global stablecoin for aid could centralize humanitarian delivery, thereby exacerbating the divide between well-resourced multilateral organizations and their smaller local counterparts. If such an offering were considered the principal unit or vehicle of delivery, it could further entrench a digital divide between international organizations with the means, access and capacity to use a humanitarian stablecoin, and small, local and civil society organizations without the means or the access. It also remains unclear what the specific advantages of a global humanitarian stablecoin might be over the status quo.

1.7 CBDC for cross-border humanitarian aid

Over the next decade, central bank digital currencies (CBDCs) will become operational in various countries. While CBDCs for cross-border humanitarian aid are not the focus of this white paper, they may play a role in the future. Domestic aid use-cases for CBDC are more obvious (e.g. for domestic stimulus) than cross-border use-cases, although pilots in this space may arise in the coming years.

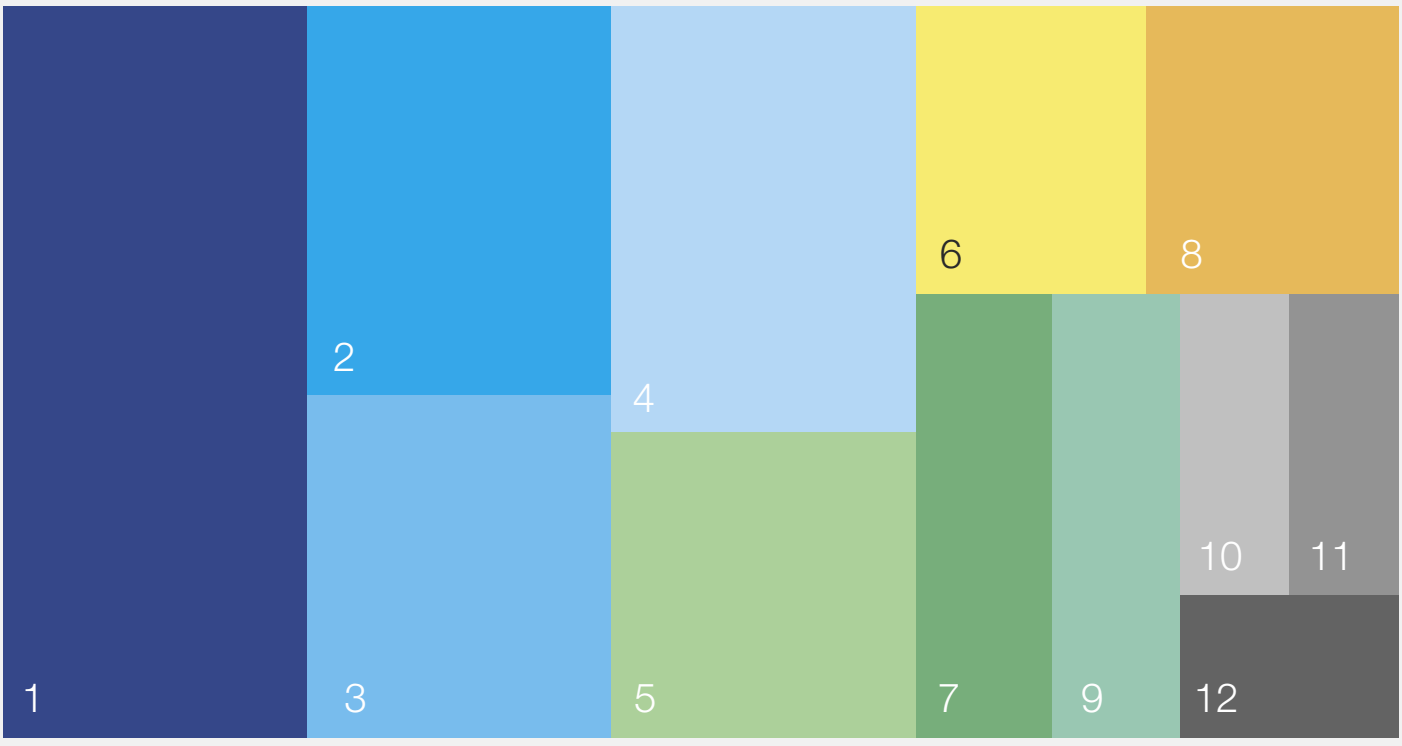
2 Pilot projects for blockchain-based digital humanitarian aid

2.1 Benefits and challenges of digital aid pilot projects

This chapter focuses on examples of blockchain-based cross-border humanitarian aid being piloted globally. Information was obtained through primary research and interviews with leaders from humanitarian aid organizations. Each leader showcased how their initiative or pilot is testing the applicability of blockchain to make progress towards delivering aid more efficiently and effectively. This research aims to inform dialogue among organizations, to bring visibility to the range of possibilities for digital currencies, and to encourage continued discussion and debate as to whether blockchain-based digital currencies and platforms can provide value in cross-border aid distribution and delivery.

Table 2 illustrates the benefits arising from digital aid pilot projects, as cited during project interviews with leaders of major humanitarian aid organizations, organized in the table by frequency of mentions during interviews.

TABLE 2 **Benefits by number of mentions across pilot interviews**

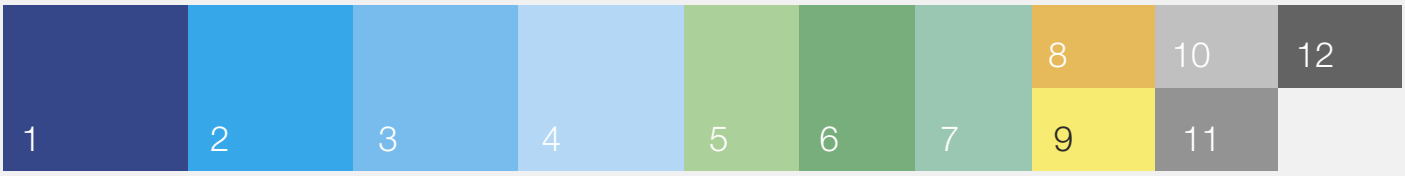


Source: Interviews conducted by World Economic Forum, January-March 2021

Table 3 illustrates the challenges arising with digital aid pilot projects, as cited during project interviews with leaders of major humanitarian aid organizations.

TABLE 3 **Challenges by number of mentions in pilot interviews**

1 Digital divide
2 Data protection for end-users
3 Lack of regulation
4 Security for end-users
5 Fraud detection
6 Internet connectivity
7 Volatility of cryptocurrencies
8 Allure of cryptocurrencies
9 Bad data
10 Blockchain talent
11 Collaboration across humanitarian organizations
12 Country specificity



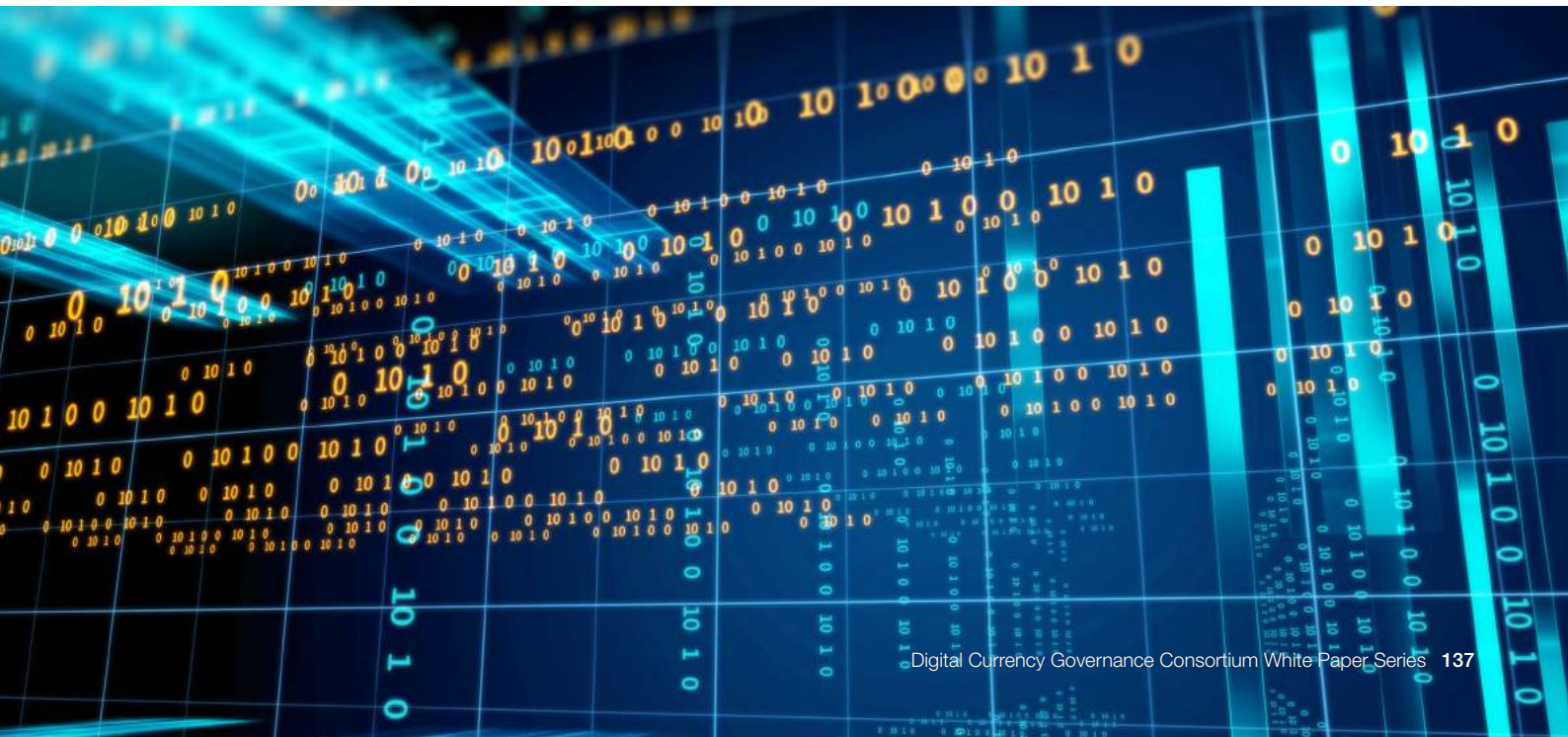
Source: Interviews conducted by World Economic Forum, January-March 2021

2.2 A selection of blockchain-based digital aid pilot projects

This section presents a selection of prominent pilot projects, with a focus on the cited benefits and challenges arising from the use of blockchain in cross-border humanitarian aid disbursement. The analysis below reflects the information provided by interviewees and is not the assessment or opinion of the World Economic Forum. This selection does not reflect the full slate of projects in the world, nor should inclusion of a project be taken as endorsement by the World Economic Forum. However, this sampling is intended to reflect the variety and diversity of projects around the world.

Further analysis is needed to determine the incremental value and efficacy of digital aid over pre-existing options for cross-border aid. The Forum's recently launched Crypto Impact & Sustainability Accelerator plans to dive deeper into topics related to humanitarian issues and financial inclusion.

For more detail on the pilot projects referenced, please refer to the Appendix for project summaries as explained by each organization. Project descriptions in the section below are also hyperlinked to each organization's website.



Circle Partners with Bolivarian Republic of Venezuela and Airtm[11]

Blockchain-based solution:	– Stablecoin
Project description:	– Unique private-public partnership – Dollar-backed, open, internet-based digital currency payments direct to frontline medical workers battling COVID-19 in Venezuela
Benefits:	– Direct distribution of funds avoiding censorship by Maduro regime – Helps recipients cope with hyperinflation and geopolitical insecurity, by bypassing state-controlled banking system – Airtm's network supports half a million users
Challenges:	– Airtm may need to be accessed via VPN due to Maduro government blocks on Airtm website and app

Red Cross blockchain-based credit system in Kenya[12]

Blockchain-based solution:	– Tradable digital tokens
Project description:	– Humanitarian response and recovery solution that enables communities to create and trade digital tokens for essential goods and services, using mobile networks – Users self-register to receive Community Inclusion Currencies (CICs), created on blockchain and guaranteed by reserves seeded by donors – Donors airdrop CICs into users' mobile wallets, enabling donors to remotely pay salaries, transfer aid and conduct training
Benefits:	– Communities trade CICs to access scarce goods and services – CIC transactions are recorded on blockchain, analysed and displayed in a web-based dashboard – Aid workers access analytics to improve field activities – Blockchain helps record aid provided to the region and enables increased transparency and accountability for distribution – Traceability enables aid workers to collect real-time data, useful for prompt response to crisis (e.g. during COVID response in Mukuru, an informal settlement in Nairobi)
Challenges:	– Need for more focus on governance in this space – Policy procurement side of aid is an important area in which problems need to be addressed

Diem payment system

Blockchain-based solution:	– Stablecoin
Project description:	– Decentralized programmable database (private, permissioned blockchain), designed to support a stablecoin – No current aid pilot, but included here as it is a possible future currency that may be considered for aid disbursement
Benefits:	– Intends to be a digital payment network accessible to a much larger swathe of the historically excluded population, through mobile app integration (e.g. WhatsApp) for individuals and businesses – Within-country and cross-border payment services on the network intended to be extremely low cost, with a focus on generating value from more complex services

Challenges:	– As with other pilots listed here, Diem does not overcome common roadblocks to inclusion for the historically excluded and underserved, including:
	  – lack of identity documentation
	  – lack of first or last mile digital infrastructure
	  – weak digital and financial literacy
	  – limited internet or mobile phone access
	  – currency conversion costs (which increase the price of cross-border payments)
	– May aggravate digital divide and gender gaps in finance and technology

GoodDollar by eToro[13]

Blockchain-based solution:	– Cryptocurrency backed by value of other cryptos
Project description:	– Crypto-asset freely distributed as a digital universal basic income, backed by the value of other cryptocurrencies – Decentralized impact investment tool to sustainably fund and scale a digital basic income for recipients, while delivering a financial and social return to financial sponsors
Benefits:	– Used smart contracts to autonomously create and distribute cryptocurrency to 250,000 people in 181 countries, with 80,000 daily active users (based on a $58,000 principal) – GoodDollar has performed as an appreciating asset with relative stability
Challenges:	– As with other pilots listed here, some digital literacy is required to use this app – App users face verification to ensure “one person-one account”, but verification is influenced by quality of cell phone camera

Grameen Foundation and the Celo Platform[14]

Blockchain-based solution:	– Stablecoin (cUSD)
Project description:	– Mobile payments app, built on the Celo Platform, to provide emergency cash relief – cLabs developed a blockchain-powered disbursement dashboard for tracking, monitoring and reporting on transfers and balances
Benefits:	– Each transaction on Grameen's disbursement to the Philippines costs less than $0.01. This represents a 99.5% reduction in costs, compared to the 2-3% cost of the average Filipino remittance – Blockchain-powered dashboard serves as a simple tool for tracking, monitoring and reporting on transfers and balances, which facilitates transparency
Challenges:	– As with other pilots listed here, technological literacy, internet connectivity and trust-building are barriers – The account key (Valora's security feature) is too long and the words are currently only in English – Self-custody has proved to be risky, as 1% of users eventually lost access to their funds

Inter-American Development Bank (IDB) and LACChain Blockchain Network[15]

Blockchain-based solution:	– Custom stablecoin
Project description:	– The LACChain Blockchain Network enables cross-border payments from the US to countries in Latin America and the Caribbean, using blockchain and tokenized money to enhance traceability of transactions, exchange rates and fees – LACChain is intended to be used by IDB for project fund disbursement
Benefits:	– LACChain is categorized as public-permissioned under ISO/TC 307, enabling it to provide free regional infrastructure as a public good – Open to all, with a requirement for users to follow local regulations governing their behaviour on the platform – Allows for cross-border payments with fewer intermediaries (avoids correspondent banking) – Enables greater traceability, which helps ensure that donor dollars reach the intended recipient
Challenges:	– When you use a public blockchain like LACChain or Ethereum you are using a trace, which may violate privacy preferences, although use of mixing software can alleviate this – As with other pilots listed, LACChain needs to ensure that KYC and AML are achieved – In common with all blockchain-based aid distribution solutions, the system requires a device with access to the internet – Does not overcome foreign currency conversion costs

Islamic Development Bank (IsDB) and the Global Coordination Platform (GCP)[16]

Blockchain-based solution:	– Online platform for aid tracking
Project description:	– Tracks aid given in Senegal, Maldives, Chad and other IsDB member countries – Allows interaction between stakeholders and development partners, in which registered countries can view services offered by various providers worldwide (e.g. suppliers of financial or advisory services)[17] – Aims to ensure greater efficiency, transparency and better governance in COVID-19 response efforts[18]
Benefits:	– Connects members to six UN agencies to help acquire masks and vaccines from other member countries – Enables inter-agency cooperation, boosting trust between agencies that participate – Blockchain has created trust within this platform that the data has not been tampered with – Ethereum ensures no vendor favouritism – No interoperability issues
Challenges:	– Underdeveloped countries have challenges with technology development – Different countries are structured differently, so the platform configuration had to cater to each country's needs; however, blockchain itself didn't pose a challenge with this – Finding advisors and experts with skills in blockchain was not easy

The Kiva Protocol for rapid eKYC verification[19]

Blockchain-based solution:	– National digital identity platform (NDIP)
Project description:	– Enables identity verification to help Sierra Leone's 7 million citizens access financial services
Benefits:	– Speed: citizens perform electronic Know Your Customer (eKYC) verifications in about 11 seconds, using just their national ID number and a fingerprint – With Kiva Protocol's verification system, the nation's historically excluded can open a savings account and move into the formally banked population
Challenges:	– As with other pilots listed here, users must be digitally literate enough to hold the wallet

Mercy Corps' blockchain-enabled vouchers[20]

Blockchain-based solution:	– Blockchain-enabled digital tokens
Project description:	– Digital tokens pegged against the value of the local currency, used for value transfers under field conditions
Benefits:	– Potential for fraud is lower, because vouchers have no secondary market value – Beneficiaries can spend without revealing payment account information – Blockchain's auditable data trail allows near real-time tracking of funds' movement – Eases the burden of reconciliation
Challenges:	– High quality connectivity is required for blockchain-enabled cash transfers – Digital literacy and security training is essential in the onboarding phase – Scaling-up would require additional compliance and regulatory requirements – Protection of participants' data is critical.

Project Unblocked Cash: Oxfam, Sempo and ConsenSys in Vanuatu[21]

Blockchain-based solution:	– Cash and voucher assistance (CVA) pilot built on the Ethereum blockchain mainnet – Initiative implemented on behalf of the Australian Government by Oxfam, in partnership with Sempo and ConsenSys
Project description:	– The objective is to enhance CVA programmes in areas which are highly prone to natural disasters, so that aid can in future be distributed with greater speed and traceability – The current iteration uses a local (fiat) currency token due to the volume of humanitarian response, now exceeding $7 million
Benefits:	– The blockchain-based system allows donors to see their donation arriving with Oxfam and its subsequent disbursement to the addresses of the recipients – Joining the programme gives vendors access to a new customer base – This method of transfer is cheaper for small donations
Challenges:	– Even with blockchain records, it is still possible to defraud the system by entering bad programmatic data (e.g. local field-officer typos or targeting etc.). Bad data stored immutably is still bad data. – As with many reserve banks, the Reserve Bank of Vanuatu has yet to regulate cryptocurrency and blockchain

UNICEF's CryptoFund[22]

Blockchain-based solution:	– Bitcoin and Ethereum
Project description:	– The CryptoFund is a financial vehicle through which UNICEF makes investments directly into early-stage start-ups in emerging and developing economies using cryptocurrencies – It enables UNICEF and its stakeholders to track where aid money is going – The fund is a way for UNICEF to learn and explore blockchain and cryptocurrencies
Benefits:	– By using cryptocurrency, donors, recipients and the public can track where the money is going and how it is being spent, providing an unprecedented level of transparency in the funding framework and NGO space
Challenges:	– The volatility of investment dollars associated with ether and other cryptocurrencies

World Bank's disbursement traceability initiative[23]

Blockchain-based solution:	– DLT platform
Project description:	– Tracks and traces use of World Bank project funds – Explores use of blockchain/DLT technology for automating traceability of disbursements, and capturing evidence of payments and work performed related to World Bank projects
Benefits:	– Provides the World Bank, its member countries, donors and auditors visibility into disbursements beyond the borrowers – Improves efficiency through business process engineering and automated tracking of the flow of funds using smart contracts – Ensures and verifies that project funds are delivered to intended beneficiaries and are disbursed for the purpose intended, with and without the use of tokenization
Challenges:	– Depending on the operation DLT Platform Operating model, the question of ownership and maintenance of the platform would need to be addressed – Challenge around how client countries would adopt track and trace on the blockchain platform and how it would integrate with their legacy systems – Further exploration is required to ensure that funds only flow between approved participants, as well as flag any suspicious activities with AML capabilities through smart contract enabled fraud detection

World Food Programme's Building Blocks[24]

Blockchain-based solution:	– DLT platform based on Ethereum
Project description:	– The project's aim is to provide a neutral network to improve collaboration between humanitarian organizations – The blockchain technology allows cash transactions between participants and the World Food Programme, without requiring a financial intermediary to connect the two parties
Benefits:	– For those organizations on the platform, it provides common visibility of the people they serve – Goal is to avoid duplication of aid through common visibility across organizations of what is being disbursed and to whom
Challenges:	– Scaling requires working with other organizations, but collaboration is difficult to foster – Organizations prefer to build their own platforms, sometimes with differing system architecture

Cash Learning Partnership (CaLP)

Finally, while not a project as such, the Cash Learning Partnership (CaLP) is global network of over 90 organizations engaged in the areas of policy, practice and research in humanitarian cash and voucher assistance (CVA) and financial assistance more broadly. CaLP places a strong focus on questions around the safety, dignity and preferences of people in crisis while exploring the efficiency and effectiveness of new technologies.

For more detailed descriptions of the pilot projects referenced above, refer to the Appendix, which organizes the projects in two thematic areas:

– Digital currency payment initiatives

– Digital systems to enhance humanitarian aid infrastructure

Conclusion

> Greater efforts are needed to speak directly with those the technology aims to serve at the core of the aid mission

While there are serious ethical considerations to consider when conducting technology pilots with vulnerable people, iterative learning about the benefits and challenges of blockchain-based digital tools for cross-border aid is key to shaping the future of humanitarian assistance. Human issues, such as collaboration among international organizations, political cooperation and process changes are what will transform this space. To that end, greater efforts are needed to speak directly with those the technology aims to serve at the core of the aid mission.

The goal for testing blockchain-based tools and technologies for cross-border aid is to extract the value of new technologies for the underserved and to ensure that they are not left behind. Digital humanitarian aid opens up new possibilities to connect the historically excluded to online financial services and it promotes financial inclusion. However, the pre-requisite infrastructure and digital and financial literacy, as underlined by the pilots highlighted in this white paper, are challenges that must be solved to unlock these possibilities.

This summary of findings should serve to inform future pilots in this space, which are anticipated to continue.

The application of blockchain-based technologies to humanitarian aid offers the opportunity for creative collaboration between donors, aid agencies, tech firms and host governments. This research and analysis have brought to the surface some key priorities for each of these groups:

- **Donors** (both governmental and private sector): encourage responsible innovation – especially where it can create cost efficiency.
- **Aid agencies:** build internal capacity to engage with emerging technology, to be able to adapt it effectively to humanitarian models, principles and standards.
- **Tech firms:** engage a diversity of local voices in developing digital solutions and infrastructure. This will enrich the innovation process and product adoption, as well as mitigating the risk of increasing the digital divide.
- **Host and donor governments:** harness technology to improve aid transparency, reduce corruption (leakage) and forge stronger links between humanitarian innovation and long-term development, especially in terms of increasing the access of the underserved to financial services.

Appendix: Detailed aid project summaries, by technology application

This appendix provides additional detail on the aid projects presented in this white paper, organized according to the following thematic areas:

- Digital currency payment initiatives
- Digital systems to enhance humanitarian aid infrastructure
- Ethical considerations and the risk of digital harm

These summaries are descriptions of each project as provided by interviewees and do not necessarily reflect the assessment of the World Economic Forum. Not all projects mentioned in this white paper are summarized below.

Digital currency payment initiatives

A report entitled *The Next Generation Humanitarian Distributed Platform*, published in November 2020 by the Danish Red Cross, Mercy Corps and hiveonline,[25] highlighted that "for traditional INGOs [international non-governmental organizations], the broad expansion of Cash and Voucher Assistance (CVA) programs stemming from commitments established in the 2016 Grand Bargain has led to an overall sector shift from distribution of in-kind aid to CVA. CVA totalled $5.6bn in 2019, doubling 2016 levels and accounting for 17.9% of total humanitarian assistance". This increase in the use of CVA has been coupled with further exploration into digital currencies and tokens.

Grameen Foundation and the Celo Platform in the Philippines[26]

In June 2020, the Grameen Foundation launched a project to provide emergency cash relief to women micro-entrepreneurs. Working with local microfinance institutions, Grameen identified 3,500 women in Manila and Cebu to receive immediate relief support for groceries and medical packages, via digital vouchers. COVID restrictions significantly hampered traditional aid disbursement processes and Grameen wanted to explore sustainable financial support for this cohort.

Following the successful pilot in 2019, Valora, the mobile payments app built on the Celo Platform, was selected. cLabs, a team building on Celo, designed the programme to meet the beneficiaries' needs and their level of digital and financial literacy. This was achieved through user research, iteration and close partnership with several other members of Celo's Alliance for Prosperity, including Beam and Go, Anchorage, Altonomy and Keyko.

A dedicated call centre was set up to contact each beneficiary. Call centre agents then provided step-by-step guidance in Filipino or Cebuano, to ensure that the women entrepreneurs knew how to use the app, learned to trust it and understood its use and value. Once the women had successfully downloaded the Valora app, Grameen directly topped up their Valora wallets with the full peso equivalent of Celo Dollars ("cUSD").

What made this initiative stand out?

- Beyond the much-needed financial support during COVID restrictions, the application of financial models of customer engagement, training and retention were used to build trust in the Valora app and self-confidence in the women's ability to use it.
- The use of call-centre agents who spoke the local language, the accessibility of these agents and the women's ability to spend the aid locally created a benefit loop of financial support, digital literacy and micro-business sustainability.
- The deployment of customer-centric tools ensured that 98% of beneficiaries successfully onboarded to Valora.

In terms of sustainability, feedback from beneficiaries suggested that beyond the instant

financial support, they enjoyed the convenience and safety of cashless transactions, despite their initial fear of using digital money. To further trust the technology, it would help if using and accessing the digital currency were to feel more like handling cash. Other beneficiaries suggested the possibility of using Valora to build up savings, with a view towards borrowing money from their microfinance institutions to invest in their businesses. This would preserve the financial and digital knowledge gained from this project and apply it to helping local entrepreneurs generate their own income.

Project Unblocked Cash: Oxfam, Sempo and ConsenSys in Vanuatu[27]

Vanuatu comprises an archipelago of more than 80 scattered volcanic islands in the South Pacific Ocean. The domestic payment network is highly fragmented, as the underlying technical and network infrastructure does not reach remote areas. The area is prone to cyclones and recurrent natural disasters. Access to cash, whether from an ATM or a micro-loan, can therefore be a challenge. Equally challenging is the availability of bank branches to safely deposit or lodge cash.

From October 2020, over 25,000 residents of three provinces affected by multiple crises – Cyclone Harold in Sanma province, Yasur Volcano ash fall in Tafea province and COVID-19 in Shefa province – can use digital tokens to buy relief goods through over 350 local vendors. The tokens are part of Oxfam's Unblocked Cash project, a partnership with the Vanuatu Business Resilience Council, Australian fintech company Sempo and a consortium of 17 local and international NGO and private sector partners.

According to project data, aid recipients were given a biodegradable and unbranded Near Field Communication (NFC) card topped up with tokenized Vatu (Vanuatu's national currency), via DAI, an Ethereum based stablecoin. The total value of DAI is collateralized by Vatu deposited at the Reserve Bank of Vanuatu (at a ratio of 4 tokens:1 Vatu). Local businesses can accept payment by simply tapping the NFC cards on a mobile phone that has the correct application. Prior to this initiative, 80% of vendors did not own a smartphone, so the learning curve was steep yet fast. Sempo's open-source blockchain-enabled system supports SMS, Android apps and tap-to-pay card transfers that work offline. It offers a real-time analytics dashboard to monitor cash disbursements and the overall programme. Using this innovative digitized token approach, Oxfam Australia reduced their aid delivery time in Vanuatu by 96%.

What made this initiative stand out?

In 2020, the project won the EU Horizon2020 Blockchains for Social Good Prize, providing €1 million to fully open-source the solution and to scale the initiative globally, via Oxfam International's network of civil society and INGO partners. The project has now been piloted in three countries.

Red Cross blockchain-based credit system in Mukuru, Kenya[28]

In November 2019, the Red Cross societies of Denmark, Kenya and Norway, together with Kenya-based NGO Grassroots Economics, launched a two-year project called Community Inclusion Currencies (CIC) to deploy blockchain-based "local currencies" to bolster trade within vulnerable communities of the Mukuru informal settlement of Nairobi, Kenya. The aim of the CIC initiative is to create a credit loop within the communities instead of purely donating cash. After an initial airdrop of digital credits (tokens) seeded from cash assistance, community members can earn digital credits through, for example, their work or completing micro-tasks and trainings. These credits can be exchanged for local goods and services. The aim is for villagers to become more self-sufficient and resilient, not only receiving aid, but earning an income through working, in turn incentivizing local economies through local spending of these tokens and strengthening community businesses. Because these tokens continue to circulate within the community for many months, rather than being extracted (as is the case with fiat currency), the initial funding achieves a multiplier ratio of 5x. In other words, for every $1 invested in the CIC reserve, $5 in economic value is realized. The system is like Kenya's popular M-Pesa mobile phone-based money transfer service. However, for the CIC initiative the user only needs a feature mobile phone without needing to hold Kenyan shillings.

What made this initiative stand out?

– Ability to turn aid disbursement into income creation, in turn s trengthening local businesses and building community resilience.

– Ability to monitor in real-time the impact of the programme (every transaction is written to the blockchain ledger), and to course-correct if the intervention is not

achieving its required goals and outcomes. Ability to toggle between response, recovery and resilience interventions without re-programming and within a few days.

– Ability to quickly enrol and continuously engage hundreds of thousands of users all linked together by digital wallets, so that when there is a disaster or conflict, aid can travel seamlessly to communities. (As of April 2021, there were over 200,000 users on the network, up from a few thousand in December 2019).

– Open-source solutions that enable other organizations to launch their own initiatives. For example, Germany's development agency (GIZ), France's development agency (AFD), the UN Children's Fund (UNICEF) and the World Food Programme (WFP) are all working with the Red Cross on versions of CIC.

Digital systems to enhance humanitarian aid infrastructure

The cash disbursement process in a humanitarian setting tends to have additional layers of complexity when compared to other cross-border cash transactions, such as trade or supply chain management. Obtaining funds, managing liquidity pools safely and adequately allocating aid are all part of the disbursement process. Our research aims to showcase how blockchain technology can enhance these processes and help to deliver tangible impact.

Inter-American Development Bank (IDB) and LACChain Blockchain Network[29]

In 2018, the Inter-American Development Bank (IDB) Group and representatives of the world's leading technology and consulting companies, announced the launch of LACChain Blockchain Network. The network was established to promote the open and inclusive use of blockchain by national consortiums in Latin America and the Caribbean, and comprises actors from the public sector, private sector and academia.

In Latin America, conditional cash transfers (programmes that provide financial assistance to households on the condition that they comply with certain predefined requirements) are the most used type of humanitarian assistance. By strengthening the infrastructure for cash disbursements in the region, and potentially using stablecoins or digital vouchers, the benefits of blockchain technology (traceability, smart contracts) would bring improvements to the conditional cash transfers in the region.

What made this initiative stand out?

This initiative aims at collectively developing robust, scalable and trusted technology layers that can increasingly be deployed and adapted for wider societal use. As of 2015, approximately half of all adults in Latin America and the Caribbean (LAC) were historically excluded, ranging from more than 80% in Haiti and Nicaragua to less than 35% in Brazil, Jamaica and Costa Rica.[30] The development of sustainable and scalable digital platforms in the region has been challenging. For example, there are nearly 40 mobile money services in 19 countries across LAC. By collaborating with financial institutions, such as Citigroup, to build LACChain, dual benefits can be achieved:

– Enabling faster, cheaper and more secure aid disbursement when needed

– Creating a digital financial services network that can be used to deploy humanitarian aid on a wholesale or individual basis

Through collaborations with financial institutions, the project teams at IDB are exploring the capabilities of the technology, working to solve big design questions such as: self-sovereign identity, KYC/AML checks and smart contracts for foreign exchange rates. Lack of regulatory and legal clarity in relation to stablecoins and tokenized fiat money may slow acceptance, but the fundamental roadblock will be the lack of technical infrastructure in the form of broadband and mobile services.

The Kiva Protocol for rapid eKYC verification[31]

Kiva has been supporting the historically excluded for over 15 years, making more than $1.6 billion in loans through the Kiva marketplace in over 90 countries, with borrower repayment

rates of 98%. This default rate of 2% is nearly identical to US credit card default rates.

In 2018, Kiva started to focus on initiatives that would connect emerging technologies with vulnerable populations as the last mile continues to rapidly digitize. Part of this mandate was to find ways that Kiva could address underlying barriers to inclusion within the financial system. Underpinning these efforts is the belief that digital inclusion can lead to financial inclusion, but only if foundational data – specifically, identity and transaction history – becomes broadly accessible alongside digital access.

Formal financial institutions may hold a perception that historically excluded individuals are inherently higher-risk customers than banked individuals, especially when it comes to lending products.[32] In the informal sector, individuals typically borrow between a few hundred and a few thousand dollars at a time, often with a short repayment term of about 12-18 months. Despite excellent repayment rates for these informal-sector loans, they remain unserved by local formal financial institutions. This is because the data from informal transactions is essentially invisible: the formal-sector institutions either do not trust the data sources or are unable to verify the provenance of the data. Solving this challenge is not possible without establishing verifiable identity credentials for these individuals and attaching that identity to their informal-sector transactions.

Kiva's solution – called Kiva Protocol – is built using Hyperledger, an open-source technical framework supported by the Linux Foundation. Kiva Protocol allows users to perform electronic Know Your Customer (eKYC) verifications in a matter of seconds, using just their national ID number and a form of authentication (typically biometric). With this verification, it is possible for historically excluded individuals to open a savings account and move into the formal economy.

What made this initiative stand out?

The first implementation of Kiva Protocol has gone live in Sierra Leone, as the National Digital Identity Platform. While Sierra Leone may not typically be a place where emerging technologies are piloted, the country offered the necessary conditions to deliver a successful population-scale intervention with the support of key stakeholders, who included:

- Regulatory and government enablers
- Private-sector financial service providers
- End-users

In Sierra Leone, the regulator had an existing digital financial inclusion strategy, and there were pre-existing efforts targeted at national-scale identity registration as well as consumer protection and privacy frameworks in development. Engagement from these stakeholders was instrumental in establishing a user-centric consent framework to digitize personal and financial data and make it usable in the financial sector.

Additionally, ensuring data sovereignty to prevent unintended consequences, such as broad surveillance or user profiling outside of the intended use-cases, was paramount to the system's architecture.

Kiva Protocol prompts the question as to how financial inclusion is measured and extended, especially in an era of rapid digitization of last-mile financial products and services. If we can provide fast, cheap and secure account access to all, and if we can assess credit worthiness based on lending transaction histories – then it is possible to add straightforward interventions for savings, insurance and other initiatives, thus increasing people's financial cushion for future crises.

Kiva Protocol was one of 193 blockchain initiatives included in Stanford Graduate School of Business' report *Blockchain for Social Impact: Moving Beyond the Hype*, because of its potential to generate accretive social impact that would not be possible without the use of blockchain in the first place.

Finally, initiatives like Kiva Protocol have demonstrated viability in very low-capacity environments, and provide a pathway for KYC and AML/CFT.

UNICEF's CryptoFund[33]

In October 2019, UNICEF launched the CryptoFund, a new financial vehicle allowing UNICEF to receive, hold and disburse cryptocurrency, the first such fund for the UN. The CryptoFund is part of UNICEF's Innovation Fund and comprises a pool of funds of bitcoin and ether. It enables the UN Children's Agency to receive cryptocurrency donations via four official UNICEF fundraising entities or national committees: Australia, France, New Zealand and the United States. Donors can contribute to the CryptoFund in either bitcoin or ether.

The fund has three main goals:

- The prototype fund is a vehicle for UNICEF to explore and learn more about blockchain and cryptocurrencies.
- UNICEF, donors, recipients and the public can track where the money is going. This is an unprecedented level of transparency in the funding framework. Transfers can be made to investors around the world in minutes, for a fraction of the cost of an international cross-border bank transfer using banking networks.

– The fund offers an additional way for UNICEF to make investments directly into early-stage start-ups in emerging and developing economies.

UNICEF has also rolled out Juniper,[34] a web-based visualization tool created to help the general public understand how and why UNICEF is using cryptocurrencies (and the CryptoFund).

The CryptoFund has invested in over 10 projects, including the following which are using blockchain applications:[35]

– Democratizing social impact financing with blockchain – Argentina

– Seeking to make sensitive clinical data portable, safe and private with blockchain – Mexico

– Using blockchain technology to inspire young people to become local changemakers – Tunisia

– Using a low-cost Interactive Voice Response platform to send key information about COVID-19 – Cambodia

– Utilizing virtual reality (VR) technology to address phobias and social anxieties – Turkey

What made this initiative stand out?

According to UNICEF, one of the most challenging aspects of the launch of the CryptoFund has been generating a sense of personal ownership over an asset that isn't associated with a familiar entity, like the government. A critical challenge was user trust in an asset that is not backed by a public authority.

The CryptoFund enables research and experimentation on blockchain platforms (and other disruptive technologies) while laying the foundations of a use-base of knowledge on the technology. This allows for talent proficient in these technologies to develop on the ground, thus minimizing lack of humanitarian personnel or related process frictions in future initiatives.

World Food Programme's Building Blocks[36]

WFP's Building Blocks project uses a private instance of the Ethereum blockchain network. The aim is to improve collaboration across the aid ecosystem.

The original pilot project in Jordan in 2017 reached more than 100,000 people. It was then rolled out to Bangladesh where, by September 2020, over 500,000 of the 855,000 Rohingya refugees in Cox's Bazar, a town on the southeast coast of Bangladesh, had access to food assistance via a QR code. The Building Blocks project has processed $162 million of cash-based transfers (including $85 million in 2020) and saved $1.8 million in bank fees.

Building Blocks is integrated with the existing authentication technology of the UN High Commissioner for Refugees (UNHCR). This not only saves on financial transaction fees in the refugee camp setting, but also ensures greater security and privacy for refugees. The Building Blocks initiative has the potential to collect assistance from multiple humanitarian organizations and offer it as one package to each refugee.

Feedback received during interviews found that collaboration across aid organizations is difficult, as they are rife with many process duplications and there is a proliferation of similar platforms that are not integrated.

What made this initiative stand out?

The success of WFP's Building Blocks project rests strongly on its integration with UNHCR's existing authentication technology, which provides trust and identification credentials for the distribution and use of voucher-based aid disbursements. It is not clear if the same benefits of speed and low-cost transactions would apply to the project if another technology was used alongside the authentication technology.

The project is continuing to explore ways to offer beneficiaries more choice and more control over how and when they receive and spend their cash benefits. This raises the question: will blockchain be the technology that welcomes humanitarian actors to collaborate on a network to improve cooperation, reduce fragmentation and bolster efficiency?

Ethical considerations and the risk of digital harm

Cash Learning Partnership (CaLP)[37]

The Cash Learning Partnership (CaLP) is a global network of humanitarian actors engaged in policy, practice and research in cash and voucher assistance (CVA). What makes CaLP unique is its diversity. CaLP members currently include local and international NGOs, UN agencies, the International Red Cross and Crescent Movement, donors, specialist social innovation, technology and financial services companies, researchers and academics, and individual practitioners. CaLP enables collaboration between organizations to increase the scale and quality of CVA. Their technical advisory group contributes to research into how to best achieve scale and quality in CVA within the humanitarian sector.

CaLP places a strong focus on questions around the safety, dignity and preferences of people in crisis while exploring the efficiency and effectiveness of new technologies.

Digital technology is transforming the way we respond to emergencies. Digital payment systems, including mobile devices, electronic vouchers and cards can deliver timelier and more secure, cost effective and inclusive assistance. Other digital innovations help ascertain which beneficiaries are eligible for assistance, collect data for assessments and monitoring, communicate with crisis-affected communities and even enable forecast-based financing, using weather forecasts to trigger aid disbursements to help soften the impact of natural disasters. As the volume of data collected, stored and shared grows, CaLP's members are working to ensure that data protection and payment systems are fit for purpose and that risks to beneficiaries are mitigated.

Humanitarian organizations have been researching and trialling the use of blockchain for aid disbursement for over five years. Within this context, CaLP has raised concerns regarding responsible data management in general, not just related to blockchain. CaLP is encouraging more rigorous questioning about the amount of data collected, bearing in mind beneficiaries' fundamental rights of choice and dignity, as well as the need for better data management.

Are the rights of beneficiaries protected? Are they part of the project or initiative and do they have a choice as to which data is given and stored? In cases of emergency aid and extreme situations, where beneficiaries may be particularly vulnerable, how do we ensure that beneficiaries are sufficiently well-informed of their rights and data protection choices, and that those choices are available to them in practice? How should we balance the imperative to reach out to beneficiaries with these inherent technological risks? The benefits of using a digital currency to disburse humanitarian aid may outweigh these risks, for example in cases of hyperinflationary economies.

Digital technology allows vast amounts of personal data to be collected (with transparency and immutability qualities), but does it mean that we should do so? Do we need to collect so much data? Are principles of data minimization being followed so that only data that is essential to an intervention is collected? Just because something is technically possible does not mean it is ethically appropriate.

Where is the data stored – is it managed by a humanitarian organization or outsourced to a cloud provider? Who is controlling the use of algorithms on such data? How is data protected against illicit access or cyber-attacks? Predictions as to use of cash, movements and location can be retrieved and potentially used against aid beneficiaries. For example, a personal digital record can be used and exploited.

The risk of digital harm in any context is real, with risks exacerbated when working with vulnerable communities. Digital and personal identification could be a tool to identify and target people in multiple ways: their digital presence and financial affairs could be exploited (e.g. targeting of loans), they could lose access to savings, or their profiles could be sold on the darknet. In extreme scenarios, data could be used to guide attacks on specific communities.

Any developments and proposals to use blockchain in aid disbursement must consider how to adhere to humanitarian principles (see Table 1 above) and how to preserve beneficiaries' fundamental rights today and in the future.

> **The use of stablecoins for aid situations raises a lot of interesting challenges. The specific scenario will matter greatly: delivering aid in the aftermath of a natural disaster/pandemic to individuals who want support could vary quite a bit from delivering aid to, say, political refugees who may not be able to prove who they are – or may not want to identify themselves if they fear reprisals against family members they may have left behind in their home countries**

Endnotes

1. Development Initiatives, *Global Humanitarian Assistance Report 2020,* 22 July 2020, https://devinit.org/resources/global-humanitarian-assistance-report-2020/.
2. United Nations Office for the Coordination of Humanitarian Affairs, *Global Humanitarian Overview 2021*, https://gho.unocha.org/.
3. Emerging Impact & Celo, *Future-Proof Aid Policy – Executive Summary,* 2021, https://drive.google.com/file/d/195h3oyR2LRwKOSIg_H2uwlHE1YVn9W0Z/view.
4. "Digital Divide", *Pew Research Center*, 2021, https://www.pewresearch.org/topic/internet-technology/technology-policy-issues/digital-divide/.
5. "Global Identification Challenge by the Numbers", *The World Bank, Identification for Development*, 2021, http://id4d.worldbank.org/global-dataset/visualization.
6. See:

   1) Sheth, Alpen, "The Digital Divide at the Heart of Financial Inclusion", *Mercy Corps Ventures* – FinX.vc, 9 January 2020, https://medium.com/finx-vc/the-digital-divide-at-the-heart-of-financial-inclusion-8eeb29933fe.

   2) Ramaswamy, Jai, "How I Learned to Stop Worrying and Love Unhosted Wallets", *Coin Center*, 18 November 2020, https://www.coincenter.org/how-i-learned-to-stop-worrying-and-love-unhosted-wallets/.
7. "Individual Sand Dollar", *Sand Dollar*, 2021, https://www.sanddollar.bs/individual.
8. "FATF takes action to tackle de-risking", *Financial Action Task Force (FATF)*, 23 October 2015, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html.
9. "De-risking", *U.S. Department of State*, 2021, https://www.state.gov/de-risking/.
10. "OCHA on Message: Humanitarian Principles", *United Nations Office for the Coordination of Humanitarian Affairs (OCHA),* June 2012, https://www.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf.
11. "Circle Partners with Bolivarian Republic of Venezuela and Airtm to Deliver Aid to Venezuelans Using USDC", *Team Circle*, 20 November 2020, www.circle.com/blog/circle-partners-with-bolivarian-republic-of-venezuela-and-airtm-to-deliver-aid-to-venezuelans-using-usdc.
12. Goering, Laurie, "Red Cross boosts disaster-prone communities with blockchain 'cash'", *Thomson Reuters Foundation*, 26 November 2019, https://news.trust.org/item/20191126123058-xtxvz/.
13. "Opening The Digital Economy, For You", *GoodDollar*, 2021, https://www.gooddollar.org/.
14. Kalaw, Angelo Paolo, "How the Grameen Foundation Successfully Delivered Humanitarian Aid to 3,500 Micro Entrepreneurs Using Celo's Blockchain", *The Celo Blog*, 10 February 2021, https://medium.com/celoorg/how-the-grameen-foundation-successfully-delivered-humanitarian-aid-to-3-500-micro-entrepreneurs-2bb3d5b78ca9.
15. "LACChain", *LACChain*, 2021, https://www.LACChain.net/home.
16. Hajjar, Bandar M.H., "102nd Meeting of the Development Committee", *Islamic Development Bank Group*, 16 October 2020, https://www.devcommittee.org/sites/dc/files/download/Statements/2020-10/DCS2020-0040-IsDB.pdf.
17. "Revealing The 80 Selected Projects to be Showcased in 2021", *Paris Peace Forum*, 21 July 2021, https://parispeaceforum.org/2021/07/21/revealing-the-80-selected-projects-to-be-showcased-in-2021/.
18. "UNOPS and Islamic Development Bank partner to help countries respond to COVID-19 pandemic", *Islamic Development Bank*, 14 July 2020, https://www.isdb.org/news/unops-and-islamic-development-bank-partner-to-help-countries-respond-to-covid-19-pandemic.
19. "Kiva protocol", *Kiva*, 2021, https://www.kiva.org/protocol.
20. Shreves, Ric, "Lessons Learned from Field Trials of Blockchain-Enabled Vouchers", *Mercy Corps*, 21 September 2020, https://medium.com/mercy-corps-technology-for-development/lessons-learned-from-field-trials-of-blockchain-enabled-vouchers-a8c7608f939c.
21. ConsenSys Solutions, *Project Unblocked Cash: Revolutionising Humanitarian Cash Transfers in Vanuatu*, 2021, https://cdn2.hubspot.net/hubfs/4795067/Project%20Unblocked%20Cash%20/Project-Unblocked-Cash-ConsenSys.pdf.
22. Lomazzo, Christina, and Hydary, Mehran, "The UNICEF CryptoFund", *UNICEF Office of Innovation*, 23 December 2020, https://www.unicef.org/innovation/stories/unicef-cryptofund.
23. World Bank Group, *Exploring Blockchain for Disbursement Traceability*, November 2020, https://documents1.worldbank.org/curated/en/717681616478065638/pdf/Exploring-Blockchain-for-Disbursement-Traceability-Outcome-Report.pdf.
24. "Building Blocks: Blockchain for Zero Hunger – Graduated Project", *World Food Programme*, 2021, https://innovation.wfp.org/project/building-blocks.
25. Blakstad, Sofie, et al., *The Next Generation Humanitarian Distributed Platform*, Danish Red Cross, Mercy Corps and hiveonline, November 2020, https://www.mercycorps.org/sites/default/files/2020-11/The-Next-Generation-Humanitarian-Distributed-Platform-v3.pdf.

26. Kalaw, Angelo Paolo, "How the Grameen Foundation Successfully Delivered Humanitarian Aid to 3,500 Micro Entrepreneurs Using Celo's Blockchain", *The Celo Blog*, 10 February 2021, https://medium.com/celoorg/how-the-grameen-foundation-successfully-delivered-humanitarian-aid-to-3-500-micro-entrepreneurs-2bb3d5b78ca9.

27. ConsenSys Solutions, Project Unblocked Cash: *Revolutionising Humanitarian Cash Transfers in Vanuatu*, 2021, https://cdn2.hubspot.net/hubfs/4795067/Project%20Unblocked%20Cash%20/Project-Unblocked-Cash-ConsenSys.pdf.

28. See:

    1) Goering, Laurie, "Red Cross boosts disaster-prone communities with blockchain 'cash'", *Thomson Reuters Foundation*, 26 November 2019, https://news.trust.org/item/20191126123058-xtxvz/.

    2) Danish Red Cross, Mercy Corps, hiveonline, *The Next Generation Humanitarian Distributed Platform*, November 2020, p.16, https://www.rodekors.dk/sites/rodekors.dk/files/2020-11/The%20Next%20Generation%20Humanitarian%20Distributed%20Platform%20Final%20Version%20Nov%202020%20%28002%29.pdf.

29. "LACChain", *LACChain*, 2021, https://www.LACChain.net/home.

30. Almazán, Mireya and Frydrych, Jennifer, *Mobile financial services in Latin America & the Caribbean*, GSMA Mobile Money for the Unbanked, May 2015, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/09/2015_GSMA_Mobile-financial-services-in-Latin-America-the-Caribbean.pdf.

31. "Kiva protocol", *Kiva*, 2021, https://www.kiva.org/protocol.

32. Durner, Tracey and Shetret, Liat, *Understanding bank de-risking and its effects on financial inclusion*, Global Center on Cooperative Security with Oxfam International, 2015, https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf.

33. Lomazzo, Christina, and Hydary, Mehran, "The UNICEF CryptoFund", *UNICEF Office of Innovation*, 23 December 2020, https://www.unicef.org/innovation/stories/unicef-cryptofund.

34. "The UNICEF CryptoFund", 2021, https://cryptofund.unicef.io/track.

35. "The UNICEF CryptoFund", 2021, https://cryptofund.unicef.io/track.

36. "Building Blocks: Blockchain for Zero Hunger – Graduated Project", *World Food Programme*, 2021, https://innovation.wfp.org/project/building-blocks.

37. CaLP homepage, 2021, https://www.calpnetwork.org/.

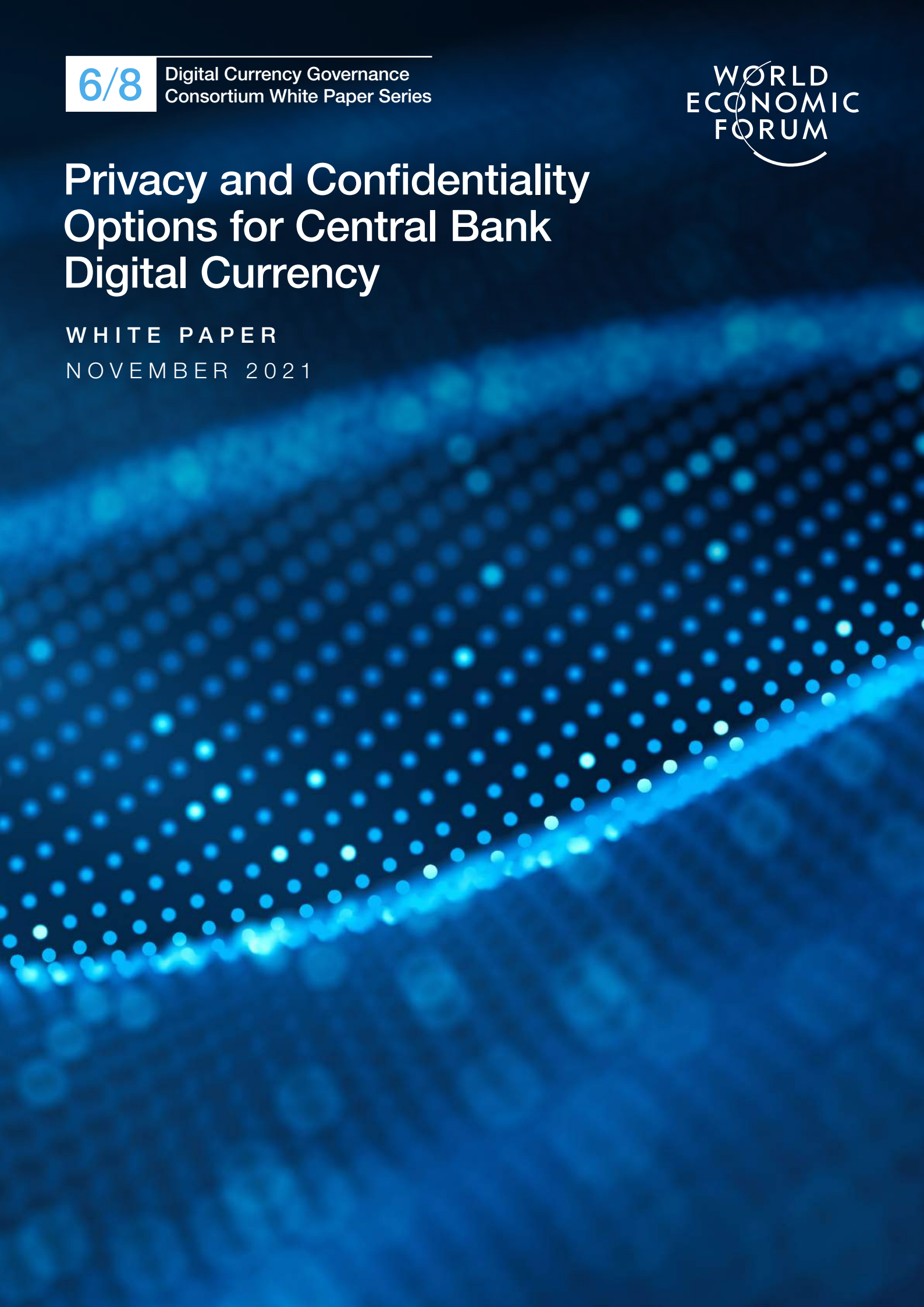
6/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Privacy and Confidentiality Options for Central Bank Digital Currency

WHITE PAPER

NOVEMBER 2021



Images: Getty Images

Contents

Preface 157

1 Privacy technology choices 158

- 1.1 Privacy architecture examples in use today 158
- 1.2 The frontier of privacy-enhancing techniques for financial systems 159
- 1.3 Requirements for a privacy-preserving financial system 160
- 1.4 The cryptography 162
- 1.5 Advanced features 166
- 1.6 Cyber threat protection considerations 166

2 Policy and regulatory considerations relevant to privacy technology choices 167

- 2.1 The current state of trust 167
- 2.2 Privacy principles and data subject rights 168
- 2.3 Privacy regulations 169
- 2.4 Policy choices for privacy 170
- 2.5 Balancing privacy and financial crime management in a CBDC world 171
- 2.6 The role of digital identity in privacy for CBDC 171

Conclusion 172

Endnotes 173

Preface

This paper explores the spectrum of technology-based privacy and confidentiality options for designing central bank digital currency (CBDC), with a focus on cryptographic techniques. It discusses the range of technologies that central banks have available to support the implementation of CBDC and outlines the principles and policy choices that lie behind those options, without making recommendations.

As more central banks begin researching the possibilities of issuing a CBDC, there is a common concern around the impact this will have on privacy. Of the 8,200 comments received by the European Central Bank (ECB) during its consultation period on the potential for a Euro-denominated CBDC, 41% of all replies centred around privacy.[1] CBDC acceptance will therefore depend in part on users' trust in the privacy offered by CBDC. However, the notion of privacy is not consistent across the globe and privacy preferences, policies and laws vary significantly by culture and region. Privacy is not a binary choice – there is a spectrum of configurations to enable varying levels of privacy. In many jurisdictions, privacy rights need to be considered in light of the disclosure requirements of policies aimed at combatting money laundering or terrorism.

In comparing CBDC to current alternatives, physical cash is typically used as a benchmark. Physical cash is generally unrivalled in its ability to provide a high degree of privacy and anonymity to its users. This feature is not limitless, however, as many countries have transactional reporting thresholds and payees often see a payer's identity. Understanding the technology choices available may allow policy-makers to better replicate the privacy-enhancing features of cash in CBDC architecture, if desired. Privacy-enhancing techniques can be configured or designed to maximize the potential of CBDC for achieving policy goals while providing privacy.

This white paper is divided into two chapters. Chapter 1 examines the current technology options, beginning with examples of privacy architectures in use today, before setting out the requirements of a privacy-preserving financial system. This is followed by an exploration of cryptography methods and how they could be employed in CBDC.

Chapter 2 examines the current state of trust in governments and why this is relevant to privacy. Such trust is the bedrock of CBDC adoption. The chapter then highlights important policy and regulatory aspects relevant to the technology options described in Chapter 1, calling out some of the policy and regulatory challenges that policy-makers face.

This paper takes a technology-first approach, clarifying the options available to policy-makers without recommending one option over another. The guidance can be used to implement successful CBDC design that respects user privacy while reducing risk and meeting regulatory requirements.

1 Privacy technology choices

1.1 Privacy architecture examples in use today

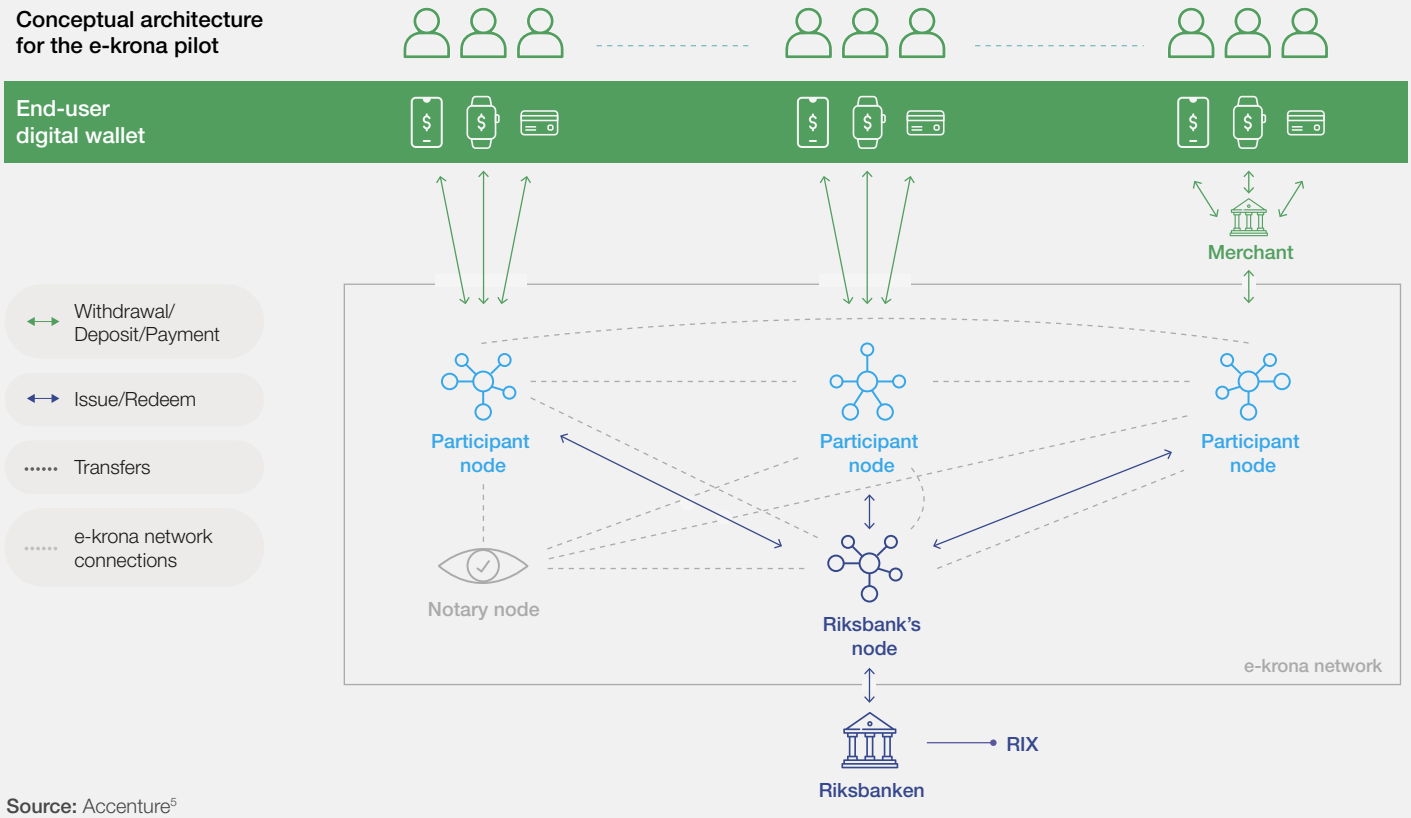
To identify the current state of privacy design in CBDC systems, it is worth mentioning privacy architectures already in use today. Below are some important examples.

The Riksbank's e-krona on Corda – "need-to-know basis"

Corda is an open-source distributed ledger project developed by R3. Currently, Corda uses a need-to-know data distribution model, which provides a degree of physical separation between transactors and the central bank or regulatory actors. Only the transactors receive the data for that transaction (i.e. the Corda nodes themselves).[2] This method provides both privacy and confidentiality (see Glossary for definitions). The e-krona pilot is a CBDC with a direct claim on the Riksbank.[3] This is a two-tiered model: in the first tier, the Riksbank will issue or redeem SEK (Swedish krona) to intermediaries in an e-krona network such as banks. In the second tier, the intermediaries will distribute SEK to end users, granting them pseudonymous identities that are used as network addresses for CBDC payments (see Figure 1).

Participants will be able to obtain or redeem SEK against the debiting or crediting of reserves held directly by the participants or via a representative in the Riksbank's real-time gross settlement funds transfer system (RTGS), known in Sweden as the RIX. Corda's network architecture, in which information is only shared to central bank and financial regulatory authorities and financial intermediaries on a need-to-know basis, allows for a level of privacy that is akin to the two-tiered model used by central banks today. To prevent double-spend in this model, notaries keep track of inputs and outputs of transactions and double-spending attempts by noting transaction IDs.[4]

FIGURE 1 **Conceptual architecture for the e-krona pilot**



Source: Accenture[5]

China's Digital Currency Electronic Payment – "controlled anonymity"

China's CBDC system, the Digital Currency Electronic Payment (DC/EP), uses a concept known as "controlled anonymity" in its current trials to ensure transactions remain confidential.[6] This method ensures that transactions remain private to those outside the system, except for the People's Bank of China (PBOC), which can trace DC/EP movements. The corresponding relationship between addresses and user identity is known to PBOC only through a KYC (Know Your Customer) process.

Commercial banks will play a key role in the issuance and redemption of DC/EP and will be responsible for implementing KYC checks. DC/EP transactions only involve DC/EP senders, DC/EP receivers and the PBOC. Differing standards can be applied depending on whether users are institutional or low-volume users. Public-key infrastructure (PKI) creates digital certificates and manages public-key encryption. PKI can be used for authentication of financial institutions or other similar high-volume users, while identity-based cryptography, which uses a string of identifiers (e.g. IP address, email address, etc.) to represent a user, can be used for authentication of low-volume users.

1.2 The frontier of privacy-enhancing techniques for financial systems

With the advancement of cryptography, newer systematic and mathematical methods to achieve privacy, confidentiality and anonymity in a wide range of financial systems and applications are being developed. Although many of these methods are at the frontier and require further development to be used at scale and without impacting system performance, they could be developed to increase privacy from outside parties or to enhance the robustness of the privacy features of a CBDC system.

The tools introduced in the cryptography section of this paper could be applied to various aspects of or entities involved in CBDC implementation. This text is strictly meant to explore technology options and possibilities, rather than to recommend or imply the appropriate degree of privacy from various parties, potentially including the central bank itself. The actual CBDC privacy scheme would depend on local policies, laws and regulations and other constraints, along with policy-makers' preferences.

Importantly, cryptography techniques alone cannot prevent failures such as hacking, unwanted data dissemination and leakage, censorship, corruption of information, privacy subversion or other issues that can affect financial and communication systems. Rather, a robust and holistic protocol that ensures the properties of the security model will need to be built.

> **"Cryptography techniques alone cannot prevent failures such as hacking, unwanted data dissemination and leakage, censorship, corruption of information or privacy subversion**

For more insights into these techniques, refer to the following publications:

- World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, White Paper, September 2019.
- Tinn, Katrin and Dubach, Christophe, *Central bank digital currency with asymmetric privacy*, McGill University, 11 February 2021.
- Miers, Ian, "Blockchain Privacy: Equal Parts Theory and Practice", *Zcash Foundation*, 2021.
- Ben-Sasson, Eli et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)", *Cryptology ePrint Archive, Report 2014/349*, 18 May 2014.
- Solomon, Ravital and Almashaqbeh, Ghada, "smartFHE: Privacy-Preserving Smart Contracts from Fully Homomorphic Encryption", *Cryptology ePrint Archive, Report 2021/133*, 6 February 2021.
- Ma, Shunli et al., "An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain", *Cryptology ePrint Archive, Report 2017/1239*, 22 December 2017.

1.3 Requirements for a privacy-preserving financial system

To assess which cryptography methods may be useful, central banks must first make decisions about the level of privacy they would like to create and enforce within their financial system. These decisions can be divided into three main technical components or features:

1. The **functionality** that enables the features of the system (e.g. minting, transferring, governance, etc.)
2. The **privacy guarantees** that ensure the privacy and confidentiality of the information, and the anonymity of the participants (e.g. sender anonymity, amount confidentiality, etc.)
3. The **integrity or security requirements** that ensure the system's robustness to attacks and fraudulent activity (e.g. stealing funds, double spending of the digital currency, etc.)

One of the most important aspects to consider when moving to a privacy-preserving system is ensuring the preservation of integrity requirements. In a transparent system, the operators of the system ("validators") usually verify the integrity requirements by looking at the transaction data and accepting transactions that are integral and follow the established rules, for example transactions that are not attempting to double spend. However, when building a privacy-preserving system, where the information is hidden even from the validator itself, the validator needs a way to accept the correct transactions without seeing the transaction data. This is where the power of cryptography reveals its potential.

Functionality

The points below set out the basic functionality and integrity requirements of a CBDC system as they relate to privacy.

Onboarding of individuals and institutions

This is particularly relevant for a system that requires unique identification of participants. A PKI system, for instance, could be used to identify every entity in the system (both institutions and individuals).[7] Such a protocol will ensure that all transactions are sent by someone identified in the PKI. However, privacy guarantees could ensure that third parties to the transaction will not be able to associate the transaction with a particular key (which represents a user) in the PKI. Furthermore, if auditing is required by law (e.g. for disclosure of fraudulent or illicit activity), additional functionality could uncover which key and identity are tied to a certain suspicious transaction.

Issuance

Only central banks are responsible for issuing CBDC. The issuance action can be both public, where all the issuing details are public, or private, hiding the amount issued.

Transfer currency between participants

The transfer transaction is where a sender (e.g. CBDC owner) transfers CBDC to the receiver of the transaction.

Privacy guarantees

The following is an overview of some basic privacy options within a CBDC system.

Sender and receiver anonymity

Sender and receiver anonymity are achieved if the sender and receiver details are kept private from various participants in the transaction. In the case of a CBDC, the receiver may not need to know who the sender is. The cryptography section below sets out the way in which identities can potentially be revealed to the central bank or a government authority, in the event of a fraudulent transaction or criminal activity. However, the central bank authority may have the power to de-anonymize at their discretion.

Funds and owner confidentiality

In a privacy-preserving financial system, each participant could be enabled to keep their funds and accounts private and confidential. The authority and even intermediaries might not initially need access to account information until it is determined necessary to address fraudulent or criminal behaviour.

Transaction unlinkability

This is the property that ensures that two transactions by the same participant cannot be connected to each other. Unlinking every pair of transactions ensures that the transaction graph is hidden, enabling the highest form of privacy.[8] Formally, this property is called "ledger indistinguishability",[9] since any two transactions look the same to an external party to the transactions.

Integrity or security requirements

Lastly, for the system to maintain its integrity and functionality, any CBDC should ensure that the following basic guarantees are fulfilled.

Ownership

This fundamental requirement ensures that funds cannot be transferred by an identity other than the legitimate owner of the funds. To own funds, a transaction with you as a receiver must have been verified and validated by the network. In a privacy-preserving setting, the address could be ensured while keeping hidden both the identity of the transacting parties and the amount transferred.

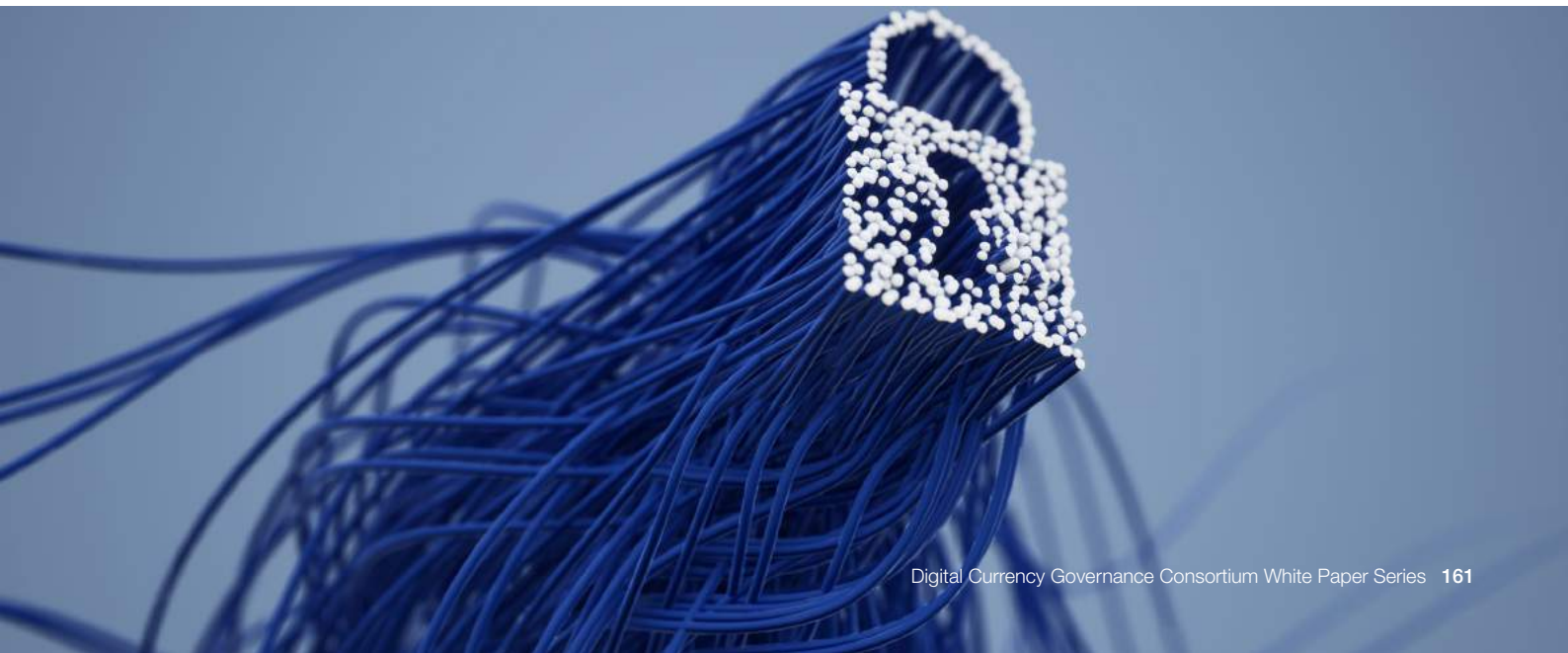
Balance preserved

This is the concept that the amount of money sent by the sender is the same as the amount of money received by the receiver. It is a basic requirement that prevents parties from spending more money than they have by creating money out of thin air. In a privacy-preserving setting, the balance of the transaction must be preserved in a hidden manner.

No double-spend

Similar to the concept of "balance preserved" above, this requirement prevents participants from spending the same money twice, ensuring they cannot spend more money than they own.

The above requirements are only a sample of features, options and guarantees relevant to a privacy-preserving financial system. A more extensive study should be conducted for any cryptographic protocol to be built securely.



1.4 The cryptography

In this section, the relevant advanced cryptographic techniques are described at a high level, together with examples of how they could be used to enhance privacy in CBDC and a review of their readiness for use.[10] As noted above, regulatory requirements with respect to privacy and the specific role of central banks and various authorities in CBDC differ across jurisdictions and are critical in determining the privacy tools employed in CBDC. The discussion below is exploratory and focuses solely on technology possibilities, rather than recommendations for specific CBDC architecture or privacy choices.

Zero-knowledge proofs (ZKPs)

This technique enables an individual to share the output of some computation with a second party, without sharing the inputs to the computation, while ensuring that the output is valid according to a publicly available function. This maintains the privacy and confidentiality of the data. ZKPs are viewed by both academics and open-source experts as a fundamental cryptographic tool to enhance the privacy and confidentiality of financial systems, for three reasons:

- Unlike other cryptographic techniques, ZKPs enable verifiability of local computations
- ZKPs enable auditability and prevention of fraudulent activity, even within the scope of private transaction data
- ZKPs are efficient enough to be used for verifying all the protocol rules in a blockchain-based financial system with auditing capabilities

Potential uses for CBDC

Zero-knowledge proofs can be used to prove that a transaction is legitimate, while hiding the data, or for revealing information about a CBDC account balance without revealing the balance itself. For instance, the central bank could calculate an interest payment or benefits for a stimulus payment for a certain account, without seeing the size of the account balance. ZKPs can indicate to the central bank whether an account balance is within certain ranges (for remuneration or KYC/AML purposes), without revealing the specific balance and while hiding information from all other parties.[11] ZKPs allow parties to transact in a private manner but also allow the central bank to conduct audits to extract insights about the economy.

Readiness for production

ZKP cryptography is being standardized through ZKProof, an open-industry academic initiative. ZKP has caught the attention of organizations such as the Defense Advanced Research Projects Agency (DARPA), part of the US Department of Defense, which cited in 2019 that zero-knowledge proofs have seen an uptick in use and efficiency in recent years, particularly in cryptocurrency. In 2019, DARPA launched an initiative called SIEVE (Securing Information for Encrypted Verification and Evaluation). SIEVE aims to develop computer science theory and software that can generate mathematically verifiable statements that can be shared publicly without giving sensitive information away.[12] Today, the technology can take millions of lines of code, input this to a zero-knowledge system and quickly identify whether there is a bug in the code. ZKP is also being used by Mozilla and Cloudflare, which implemented a scheme called Privacy Pass.[13]

Symmetric-key cryptography

This form of cryptography refers to those schemes that require a single key to perform the algorithms. One basic building block (known as a "cryptographic primitive") of a cryptographic system involves commitment schemes.

Cryptographic commitments allow a party to irreversibly pledge to a message or data in a private manner. A commitment scheme has two fundamental security properties: it must be *hiding* so that the message itself is private (by making the commitment random-looking) and *binding* so that, once the message is revealed, anyone can verify that the message is indeed the one that was originally intended and was not modified. In order to send a commitment message, a "commit algorithm" is employed that uses a random key to hide the message securely, even when the commitment output is shared publicly. A "reveal algorithm" is then used to reveal the underlying message, with the assurance that it was not changed since the time of commitment. Commitments are one of the most fundamental tools used to hide information that must be used as a reference for future verification.

Hash functions

Mathematic hash functions are a type of deterministic algorithm that generates a unique random-looking fingerprint of the input message. Any two computations of the same message will give the same hash result and no other message would give that result, which is how the unique fingerprint is generated. The algorithm has the property that it is relatively easy to compute the hash given the message, but it is almost impossible to find the input message given the output hash. Put another way, a huge amount of computation is required to *invert* the function. Hash functions are used everywhere in cryptography: to build commitment schemes, to enable non-interactivity in zero-knowledge systems, to hide information with a unique fingerprint and for integrity checks.

Public-key (asymmetric-key) cryptography

In a public-key cryptographic system (also referred to as asymmetric-key cryptography), there is a secret-public key pair that enables two parties to perform cryptographic operations (such as sending and receiving messages, authenticating data, etc.) without having to share private keys.[14]

Digital signatures

Digital signatures serve to authenticate the origin of data by providing a cryptographic connection between the identity (some public key) and the data, represented as a message. A signature algorithm allows the address of the secret key to sign a message, indicating that they are authenticating the message. A verification algorithm then takes the associated public key and verifies that the signature is correct. In a CBDC system, signatures can serve to authorize the transfer of assets. Mainly, once a transaction has been verified to come from the rightful owner of the assets, then it is validated.

An aggregate signature scheme can aggregate many signatures on a single message, making the resulting signature look like a single entity signed, maintaining the anonymity of the signing parties.

Encryption

An encryption algorithm allows parties to share messages by privately communicating over insecure networks. They can be employed with symmetric or asymmetric-key cryptography (for the former, the same key is used for both encryption and decryption; for the latter, different keys are used). Encryption systems enable peer-to-peer communication where, in the case of asymmetric-key cryptography, for a given key-pair the communication is directed to a single individual. This means that anyone who has a public key can encrypt any message, but only the address of the secret key associated with the public key will be able to decrypt and read the message. In a privacy-preserving financial system, this property is used to "warn" a receiver that there is a transaction for them. This is achieved by the sender encrypting some secret information using the public key of the receiver. Once the receiver sees the transaction, he or she will try to decrypt the message and, if successful, read the transaction data.

Symmetric-key cryptography, hash functions and public-key cryptography are used to put together different components of a financial system. One example is to derive a one-time address from the initial identity in a public-key infrastructure (PKI): for every new transaction, a receiver can derive a new address by computing a hash of the secret key associated with the public key in the PKI. This then allows a zero-knowledge proof to be used to prove the relationship and legitimacy of the identity. Another example is where hash functions are used to burn a token.

Potential uses for CBDC

In a privacy-preserving CBDC, transactions may not contain data in-the-clear, but instead contain commitments to the relevant data, such as the identity of the sender or receiver and the amount of currency transferred. When a transfer is being executed, the sender can "use" an existing commitment and create a new commitment, which would contain the address of the receiver of the transfer.

To ensure the *balance* of the transaction is preserved without revealing the amount transferred, the system can use a third functional property of certain commitments called "homomorphism".[15]

PKI enables individuals to send and receive funds while keeping account information secure. It can work together with a digital signature scheme, which enables a CBDC account owner to sign a transaction to send funds with his or her private key (a process that demonstrates his or her ownership of the account). The recipient would see the transaction incoming and verify its origin using the sender's public key. Signatures can be used to identify people on a CBDC as they enable verification of the origin of a transaction. Encryption can be used to communicate between two parties in a private manner, where encrypted information such as for a receipt or invoice can be sent alongside the transaction. Using encryption (with asymmetric keys), a receiver can be made aware that the transaction is meant for them and can use a private key to decrypt it.

Readiness for production

The cryptography functions described above are already in common use or are extensively available for production. Computing a hash function within a CPU is very fast. However, computing a hash function within a zero-knowledge proof is not as efficient and entails slower computation, depending on the number of functions being executed.

Multi-party computation (MPC)

MPC enables several parties to jointly compute some function on their individual inputs, without revealing their inputs to the other participants. The output is visible to all parties. In the academic realm, there are fully generic schemes that allow us to compute any such function or program. However, these generic schemes are not yet efficient and their implementation is not easy to use. On the other hand, there are "specific-purpose" schemes which allow computation of one type of function and are extremely efficient.

Secure secret sharing

One such function is secure secret sharing (SSS), and it is widely used in the blockchain space. SSS is a method for breaking down a secret into random-looking pieces, such that the secret can be reconstructed if and only if all the pieces are put back together. Importantly, the reconstruction itself can be done in a private way, where no single individual reveals his or her random piece. The most basic security assurance from secret sharing is that no subset of the parties with the individual pieces can reconstruct the full secret, maintaining its privacy. Private keys, as part of public-key cryptography, are fundamental to the functionality of financial systems, enabling assets to be fully controlled by the entity or entities in possession of the private keys. Secret sharing can be used today both to ease the recoverability process of a lost private key without losing security and to enable multi-signature accounts.

By combining SSS with public-key cryptography, different parties that are onboarded in the PKI can create a shared account by using secret shares derived from each other's public keys, such that the transactions from this shared account will not leak the identities of the owners.

Potential uses for CBDC

MPC can be used for multi-party wallets to generate secrets in a distributed way. Another potential application could involve multiple central banks in a multi-CBDC or cross-border CBDC arrangement contributing suspicious transaction data from their operations and jointly computing on such data. The data they contribute is kept private from the other central banks. They could determine whether transactions are illegal (by benefiting from a greater amount of data), without seeing the details of the transactions occurring in another country's CBDC.

Readiness for production

Although secure multi-party computation (SMC) is generally computationally inefficient, several research efforts are underway to improve its performance. Some schemes, like secret sharing, are being used widely in production within internet protocols and in some blockchain spaces. The more generic protocols, which allow computation on any function (e.g. machine learning or AI in a private computer) are not quite ready for production because they do not yet generally meet desired expectations for efficiency. There may be insufficient tooling to make the development easy for deployment. There are several companies, such as Inpher and Tripleblind, focusing on MPC and they are working to make this form of cryptography scalable.

Differential privacy (DP)

Differential privacy allows for one entity to keep the low-level data within a dataset private while sharing publicly the higher-level patterns, statistics or model outputs based on the data. It is well known that when analysing large sets of data, a minimal change in the underlying data can be identified only by looking at the results of analysis. This is called privacy leakage. Although not original to cryptography, differential privacy has become one of the most important tools to formally measure the amount of privacy leaked from a system as well as to hide the actual leakage from it. Data privacy comes in many flavours, but the general method is to add randomness to specific parts of the data set that are queried. This generates a fundamental trade-off to be considered between the amount of leakage permitted and the exactness of the results in the analysis.

Potential uses for CBDC

DP could potentially be used in a CBDC to aggregate data on the total amount transacted in a time period, while not leaking the individual data entries used across aggregations. Additionally, central banks may want to analyse transaction data to generate information, for example, on the

state of the economy. Differential privacy will allow analysis of datasets without allowing leakages of the original datasets. While DP enables statistical inference, it is still difficult to identify an individual.

Readiness for production

DP is efficient and usable today; there are several open-source implementations available, either for use or as reference. Mozilla Firefox is using differential privacy to do large scale analytics on users in Firefox browsers today. Differential privacy is working with legal departments in universities to explore the intersection between data and law. This technology is currently ready for production and will continue to improve in efficiency and in robustness of result, while minimizing leakage of information from the original dataset.

Homomorphic encryption (HE)

Homomorphic encryption is one of the most promising methods to enable computation on encrypted data. HE makes it possible for a party to compute on, analyse or manipulate encrypted data and never see the data in readable plain-text.

Homomorphic encryption can be partially or fully employed. Partially homomorphic encryption keeps sensitive data secure by only allowing select mathematical functions to be performed on encrypted data.[16] Fully homomorphic encryption (FHE) enables analytical functions to be run directly on encrypted data and yields encrypted results, which can then be decrypted by the appropriate parties or owner of the data.[17]

The client can encrypt their data, send the encryption to a server that will perform some computation, and then the client can decrypt the output to get the actual result of the computation on their data stored unencrypted (in clear). Even if HE is not currently efficient enough to run large computations on encrypted data, it can be used to do some basic operations. The Homomorphic Encryption consortium has produced a set of standard secure parameters to be used in production systems.[18] Several research efforts are underway to improve the efficiency of HE.

Potential uses for CBDC

HE could be used to aggregate and compute on encrypted data across accounts in a private manner, for example to check that the sum of a set of accounts does not exceed a certain amount. It could also be used to aggregate and analyse encrypted identity data from different transactions for KYC or anti-money laundering (AML) purposes. The central bank could also provide encrypted CBDC account or transaction data to a regulator, law enforcement organization or private firm that could compute to generate findings from it for various purposes.

On a cautionary note, HE is an encryption scheme, so one must consider who holds the secret key that enables eventual decryption. If multiple parties want to aggregate their data using HE, or perform a complicated function on it privately, they can certainly do it. For example, two parties could create joint HE keys using secret sharing, or using a "multi-key HE" scheme, and then separately encrypt their inputs. They would then have to cooperate to decrypt the result, using their respective pieces of the key. One must be mindful of where the eventual decryption happens.

Readiness for production

HE is being standardized. The most efficient schemes are quantum-secure. Quantum-secure cryptography refers to algorithms that are resistant to attacks by future quantum computers. For certain function types or small functions, HE is doable and efficient. There are many companies today that are using HE; however, it has not reached full maturity. For central banks, this may be ready for use today for simple computations. DARPA, part of the US Department of Defense, is leading interesting efforts around HE hardware acceleration, among other organizations.[19]

1.5 Advanced features

Advanced cryptography can enable several kinds of functions, for example:

- Auditing of specific transactions, addresses or entities by central banks and regulatory bodies
- Automated transaction flagging: preventive features that automatically enforce certain restrictions or behaviour on the participants, such as maximum transaction amount auditing keys

Auditing

Central banks and regulatory bodies (e.g. the US Securities and Exchange Commission) will most likely require some visibility on transactions of specific types, as well as on specific "tagged" people and on transactions between specific individuals. Techniques such as ZKP and MPC could be used to provide this kind of auditability, while minimizing the details shared and ensuring that the control is fully in the hands of the user.

Automated transaction flagging

Most countries impose a limit on the maximum transaction size that can be completed with cash. With CBDC, a similar control can be programmed, where a flag is raised on an attempted transaction that is larger than the permitted amount. The flag could even reveal some secret about the transaction that would allow an authority (such as an auditor or regulator) to see the sender's identity. The CBDC system could also be programmed to prevent certain transactions from occurring altogether.

1.6 Cyber threat protection considerations

It is not easy to design a CBDC protocol in a fully secure manner. Each cryptographic scheme has its own security requirements and putting them together can add more complexity.[20] One needs to keep in mind the size of the anonymity pool (the number of users or entities conducting transactions). The smaller the pool of users, the less privacy the whole system will have.

While privacy and security are two different concepts, it must be acknowledged that data loss prevention is also an important component of privacy preservation. Drawing from the World Economic Forum's Presidio Principles[21] and the Privacy Principles for Digital Development,[22] central banks will need to do the following:

- Assess the risks of unauthorized access to or leakage of any stored data
- Investigate which groups may be motivated to acquire your data and how capable they are
- Determine the sufficiency of information and access controls around data
- Track personal or sensitive information captured and create a plan for potential mid- and post-project destruction if necessary

Additional information on cybersecurity for CBDC can be found in the white paper in this report series entitled *CBDC Technology Considerations*.

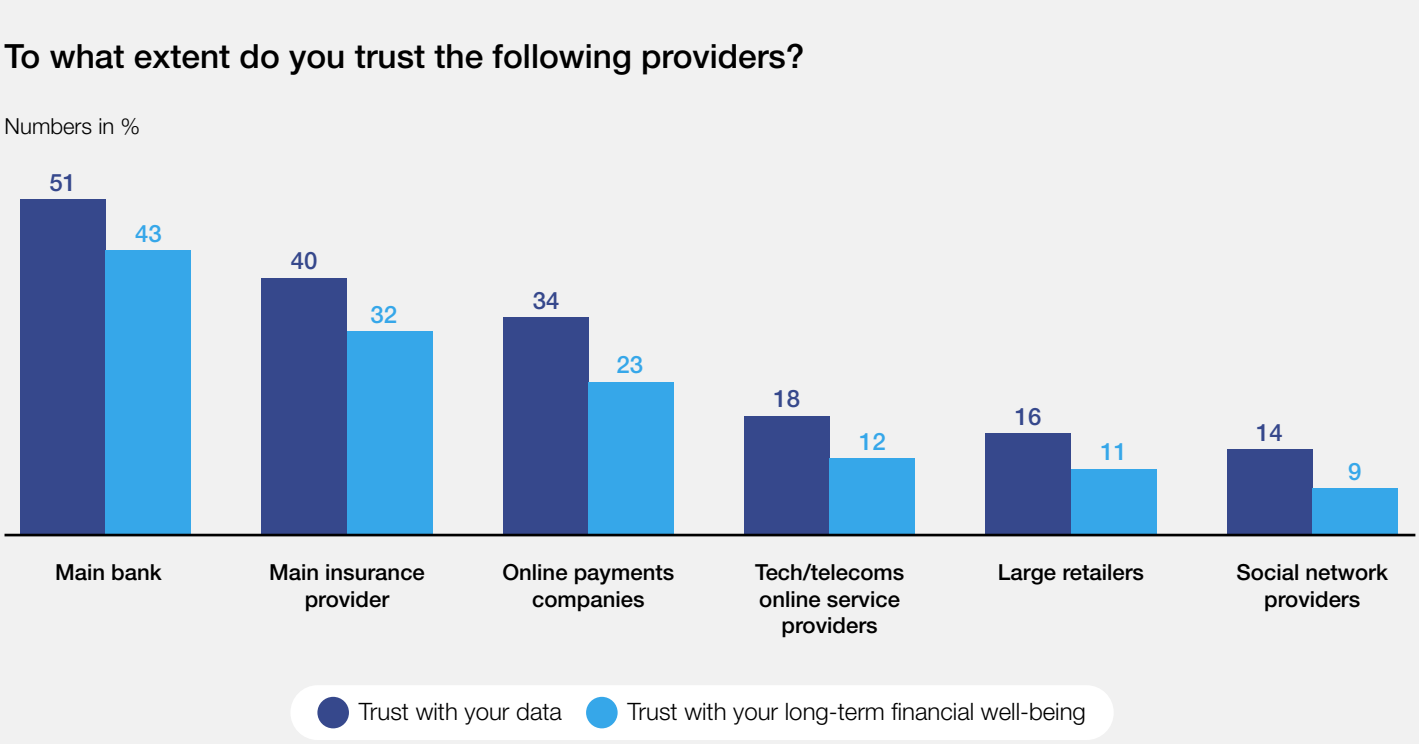
2 Policy and regulatory considerations relevant to privacy technology choices

2.1 The current state of trust

Consumers are becoming increasingly aware of and concerned about to whom they entrust their data and how it is used. According to Accenture's *2019 Global Financial Services Consumer Study*,[23] which surveyed 47,000 banking and insurance customers across 28 markets, the percentage of consumers who trust financial service providers with their data ranges from 14% (social network providers) to 51% (main bank) – see Figure 2.

In addition, many citizens do not trust their government to use their data to their benefit. A survey of 18,800 adults in 26 countries on consumer acceptance of information technology, commissioned from Ipsos by the World Economic Forum, found that only a minority of citizens trust their own national governments (39%), while trust in foreign governments is lower still at 20%.[24]

FIGURE 2 **The state of consumer trust in financial services**

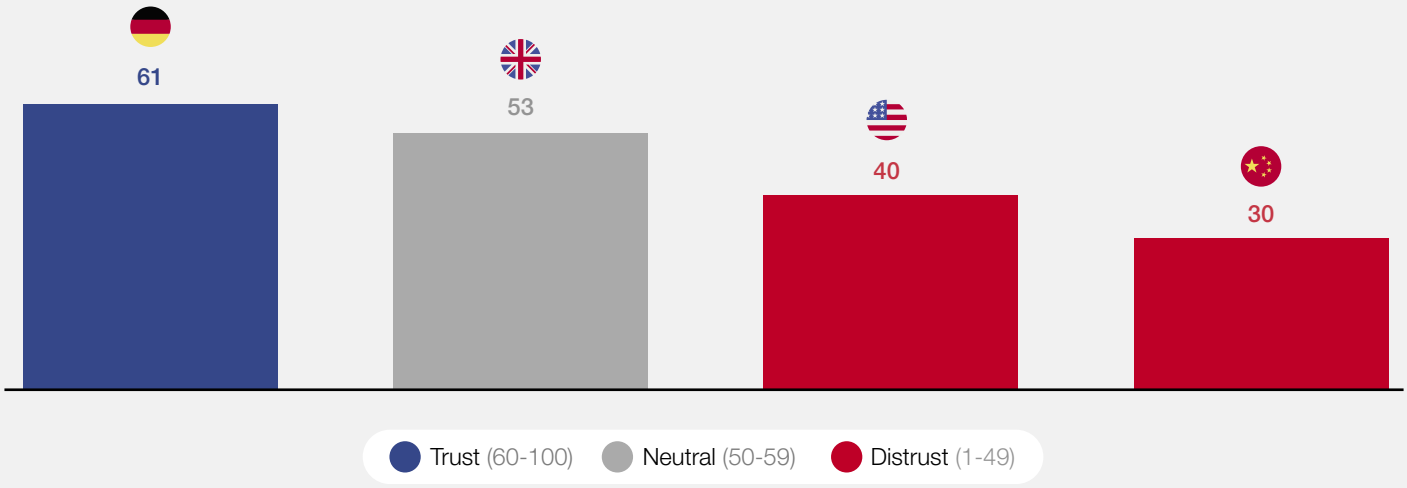


Source: Accenture *Global Financial Services Consumer Study*, 2019

The *2021 Edelman Trust Barometer* shows that businesses have become the most trusted institution, helping fuel the rise of stakeholder capitalism.[25] Business is more trusted than government in 18 of 27 countries, while some major governments registered neutral or negative trust levels (see Figure 3).

Successful adoption of CBDC requires a level of trust in the central bank – or trust in the government, for individuals who do not distinguish between the two or where the central bank lacks independence.[26] A primary concern of policy-makers is therefore to develop CBDC in a way that fosters user trust, particularly in how data is gathered and used.

FIGURE 3 **Percent trust in the national government of foreign countries**



Source: *2021 Edelman Trust Barometer*

2.2 Privacy principles and data subject rights

When it comes to safeguarding the privacy of data, there are three core principles – informed by the World Economic Forum's Presidio Principles[27] and the Principles for Digital Development project[28] – which central banks may adopt to inform their policies:

1. Prioritize the best interests of citizens, especially vulnerable populations, when collecting data
2. Limit the collection of personal identifiable information to what is necessary
3. Use data only for the purpose for which it was provided

For example, with respect to a possible future United States CBDC, the Digital Dollar Project proposes the following guiding principles for privacy:

1. People should be able to use a US CBDC without making themselves subject to undue corporate tracking or government surveillance
2. People may opt to benefit from legitimate, contractual sharing of information with financial services providers, or they may refuse it
3. Law enforcement access to CBDC usage data should be controlled by applicable US law, due process and the Fourth Amendment

Beyond any consideration of principles such as these, there remains the question of trust around a government's or institution's ability to instil and uphold consumer trust in the process.

2.3 Privacy regulations

Regulators across the world are introducing increasingly strong data protection regulations due to growing consumer awareness and demand. According to global research and advisory firm Gartner, 65% of the world's population will have its personal information governed under modern privacy regulations by 2023, up from 10% today.[29] By 2024, more than 80% of all organizations globally will need to comply with privacy and data protection requirements.[30] The European Union's (EU) General Data Protection Regulation (GDPR) and other privacy regulations improve institutional accountability and enforcement around data protection for consumers and citizens. Yet many of the privacy rules vary depending on geography and lack standardization across privacy mandates.

CBDC designers must negotiate varying national baselines of privacy regulation, especially when considering cross-border CBDC interoperability. They may benefit from designing architectures based on the stricter regulations (e.g. GDPR) to ensure longevity and standardization.

Table 1 summarizes personal data principles and rights, as dictated by three examples which have a considerable impact on data privacy and confidentiality discussions and regulatory developments around the world:[31] the EU's GDPR,[32] the California Consumer Privacy Act (CCPA),[33] and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).[34]

TABLE 1 **Data subjects' rights as protected by GDPR, CCPA, PIPEDA**

Data subjects' rights over their personal data	GDPR	CCPA	PIPEDA
Informed and expressed consent needed to process the data	Yes	No	No
Possibility of objecting to the processing of data	Yes	Yes	No
Special categories of personal information	Yes	Yes	Yes
Access to data	Yes	Yes	Yes
Correct incomplete or incorrect data	Yes	Limited	Yes
Right to be forgotten (data erasure)	Yes	Yes	No
Obligation to designate a data privacy officer	Yes	No	Yes
Obligation to provide transparency in data processing	Yes	Yes	Yes
Obligatory security measures	Yes	Yes	Yes
Breach notification	Yes	Yes	Yes
Privacy by design	Yes	No	No
Privacy by default	Yes	No	No
Employees' data protection	Yes	Limited	No

Source: Accenture

2.4 Policy choices for privacy

When enacting policies, policy-makers choose what rights they believe to be fundamental for their citizens and craft policies intended to protect those rights. This is especially important in the context of privacy, as policy concerns surrounding privacy differ across jurisdictions and can also differ in respect of private versus public actors. Some important considerations include the following:

- Many jurisdictions have laws which are geared towards the processing of personal information. If a CBDC drastically increases the scope of citizens' personal information being processed by the public sector, then new policy considerations will be raised. There will need to be consideration around whether such information will be shared between different government departments or bureaus.
- The approach that a country takes in its surveillance laws may have a cross-jurisdictional impact. This has been acutely experienced in respect of the GDPR's adequacy requirements and the invalidation of the EU-US privacy shield by the Court of Justice of the European Union due to the surveillance laws of the US.[35] Taking significantly different policy positions in respect of CBDC architecture could result in similar issues in privacy regulation being ported into the policy concerns of CBDC.
- Many of the regulatory regimes are designed around governments taking positive action to gain access to private transactional data, such as through a court-issued warrant. A change in this position resulting from CBDC architecture choices may require consideration on how these approaches are mimicked in CBDC frameworks.

Table 2 lists further considerations for policy-makers in the context of surveillance and CBDC adoption.

TABLE 2 **The spectrum of privacy**

Surveillance disincentivizes adoption	Opportunity cost of surveillance prevention and nuance	Most extreme risks of surveillance
– Lack of trust in government could hinder CBDC adoption, due to fear and ease of digital surveillance – Populations more engaged with the informal economy might be financially excluded	– Citizens may prefer that their data be used in an anonymous way for certain purposes, such as the advancement of science and research – Citizens may not want their data used for commercial marketing purposes	– Aggregated and anonymized data still presents the possibility of surveillance, such as the monitoring of demographic migrations based on transactional data

2.5 Balancing privacy and financial crime management in a CBDC world

In addition to data privacy laws, there are multiple regulations and policy obligations related to data privacy and financial services that must be considered when designing for CBDC. These regulations include anti-money laundering (AML) and counter-terrorist financing (CTF).

Central banks will have to make choices that balance privacy with law enforcement. This debate centres around the societal trade-offs between zero monitoring and stringent laws, as a CBDC operating at either extreme is likely to face significant adoption challenges.

At the foundational level, CBDC systems verify the uniqueness, security and settlement of a transfer of a CBDC by answering the questions: "Is this money genuine?", "Has the user spent this money before?" and "Did a transfer of money occur successfully?" The operators of the system (e.g. the central bank and/or its designated regulated entities) may not necessarily need to have visibility into account balances, identity information or other transaction-related information. The choice to have visibility into that information is a policy choice and can be limited, threshold-based and audited.

From the government perspective, one of the most promising advantages of privacy-preserving techniques applied to CBDC is the potential to enable more effective AML and CTF activities. Depending on the choices made, CBDC could enable appropriate regulatory entities to develop a topographical view of aggregated monetary flows and more effectively identify suspicious outlier transactions. This could be achieved in an aggregated way, by utilizing techniques (e.g. differential privacy) that would protect the privacy of individuals while providing the appropriate tools to regulators.

Lastly, the roles of the central bank and other institutions that engage with the CBDC, regarding maintenance, control, custody and other activities, will determine their requirements with respect to AML/KYC/CTF and other policies and the privacy requirements and protocols they adhere to.

2.6 The role of digital identity in privacy for CBDC

The design choices related to privacy need to allow for adequate identification mechanisms to meet national policy and legal requirements associated with, for example, anti-money laundering laws. The Bank for International Settlements (BIS) report, *Central bank digital currencies: foundational principles and core features*,[36] written in collaboration with a group of central banks, asks: "Digital identity is an emerging field in many jurisdictions. In the absence of digital identity infrastructure, what are efficient approaches to KYC/ AML/CTF?" The UK has proposed a digital identity and attributes trust framework,[37] which seeks to govern how organizations use digital identities.

This highlights a number of questions. Do national digital identity systems exist to support CBDCs? Will CBDC be implemented with standards closer to physical cash, for which typically no identification is required? Will central banks need to account for full population identification schemes, which some jurisdictions may require for their resilience and inclusion requirements?[38]

A middle ground solution is that central banks would connect to externally managed sources of digital identity information, such as a national digital identity scheme. These would need frameworks for integration with CBDC administration. Non-centralized solutions have also been considered, such as credential-based, "self-managed" or "self-sovereign" alternatives, which leverage digital wallets, generally in the form of mobile applications, to build digital identities off decentralized identifiers and verifiable credentials.

CBDC policy-makers will need to be keenly aware of developments in respect of digital identity architecture and how choices made in respect of CBDC frameworks impact or are impacted by these developments.

Conclusion

As with all technology innovation and advancements, there will be significant learning and evolution in CBDC over the next decade. Early designs and implementations will need to support constant modernization. Several frontier technology developments, while still requiring scalability, already reveal that privacy in CBDC will require a dynamic and nuanced approach to technical design and choices.

Core needs such as privacy may be central to CBDC designs. “Privacy by design” can be integrated with “security by design” to enable higher CBDC adoption and responsible deployment.

However, keeping pace with the variety of techniques to support the privacy objectives of a nation’s CBDC system is critical and requires constant engagement across the public and private sectors. Policy-makers will need to develop forums in which governments and other stakeholders can accurately communicate their goals, while exploring the potential of cryptographic, security, identity and other technology solutions. Without such a space, policy-makers will run the risk of adopting an approach without a full view of non-regulatory tools available to achieve desired privacy and compliance goals.

Endnotes

1. "ECB digital euro consultation ends with record level of public feedback", *European Central Bank*, 13 January 2021, https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html.
2. "Corda Documentation", *R3 Ltd*, 2021, https://docs.corda.net/docs/corda-os/4.6/key-concepts-ecosystem.html#admission-to-the-network.
3. "The e-krona pilot – test of technical solution for the e-krona", *Riksbank*, 2021, https://www.riksbank.se/en-gb/payments--cash/e-krona/technical-solution-for-the-e-krona-pilot/.
4. "Spending Corda State on Different Notaries", *Corda*, 27 July 2020, https://www.corda.net/blog/spending-corda-state-on-different-notaries/.
5. "The Riksbank in Sweden launches e-krona pilot", *PaymentsCM LLP*, 26 February 2020, https://www.paymentscardsandmobile.com/the-riksbank-in-sweden-launches-e-krona-pilot/.
6. Kharpal, Arjun, "China has given away millions in its digital yuan trials. This is how it works", *CNBC*, 4 March 2021, https://www.cnbc.com/2021/03/05/chinas-digital-yuan-what-is-it-and-how-does-it-work.html.
7. This could alternatively be achieved by designs such as a central authentication service in other architectures.
8. Miers, Ian, "Blockchain Privacy: Equal Parts Theory and Practice", *Zcash Foundation*, 2021, https://www.zfnd.org/blog/blockchain-privacy/.
9. Ben-Sasson, Eli et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)", *Cryptology ePrint Archive*, Report 2014/349, 18 May 2014, https://eprint.iacr.org/2014/349.
10. It is important to note that such cryptographic schemes are based on abstract mathematical models that provide a basis for the security of the schemes. Where necessary, cryptographic schemes can be modernized to account for evolving security threats, such as those that may arise from advances in quantum computing technology.
11. World Economic Forum, *CBDC Policy-Maker Toolkit – Appendices*, 2020, http://www3.weforum.org/docs/WEF_CBDC_Policymaker_Toolkit_Appendices.pdf.
12. "Generating Zero-Knowledge Proofs for Defense Capabilities", *DARPA*, 2019, https://www.darpa.mil/news-events/2019-07-18.
13. "Using Privacy Pass with Cloudflare", *Cloudflare Help Center*, 2021, https://support.cloudflare.com/hc/en-us/articles/115001992652-Using-Privacy-Pass-with-Cloudflare.
14. Tinn, Katrin and Dubach, Christophe, *Central bank digital currency with asymmetric privacy*, McGill University, 11 February 2021, https://www.mcgill.ca/engineering/files/engineering/central_bank_digital_currency_with_asymmetric_privacy_mcgill_tinn_dubach.pdf.
15. "Homomorphism, mathematics", *Encyclopaedia Britannica Inc.*, 2021, https://www.britannica.com/science/homomorphism.
16. Marr, Bernard, "What Is Homomorphic Encryption? And Why Is It So Transformative?", *Forbes*, 15 November 2019, https://www.forbes.com/sites/bernardmarr/2019/11/15/what-is-homomorphic-encryption-and-why-is-it-so-transformative/?sh=452d426c7e93.
17. "What Is Fully Homomorphic Encryption?" *Inpher*, 2021, https://inpher.io/technology/what-is-fully-homomorphic-encryption/.
18. Albrecht, Martin et al., "Homomorphic Encryption Security Standard", *HomomorphicEncryption.org*, 2018, https://homomorphicencryption.org/standard/.
19. "Building Hardware to Enable Continuous Data Protections", *DARPA*, 2020, https://www.darpa.mil/news-events/2020-03-02.
20. ZKProof, *ZKProof Community Reference, Version 0.2*, Chapter 4: Applications, 31 December 2019, https://docs.zkproof.org/pages/reference/reference.pdf.
21. World Economic Forum, Global Blockchain Council, *Presidio Principles: Foundational Values for a Decentralized Future*, http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf.
22. Principles For Digital Development, *Principle 8: Address Privacy & Security*, https://digitalprinciples.org/principle/address-privacy-security.
23. Accenture, *2019 Global Financial Services Consumer Study: Discover the patterns in personality*, 4 March 2019, https://www.accenture.com/us-en/insights/financial-services/financial-services-consumer-study-2019.
24. Ipsos and World Economic Forum, *Global Citizens & Data Privacy*, 2019, https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/ipsos-wef_-_global_consumer_views_on_data_privacy_-_2019-01-25-final.pptx_lecture_seule_0.pdf?mod=article_inline.
25. Edelman, *Edelman Trust Barometer 2021*, https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf.
26. Casey, Michael, "Money Reimagined: Warnings From an Argentine Tragedy", *CoinDesk*, 7 August 2020, https://www.coindesk.com/money-reimagined-warnings-from-an-argentine-tragedy.
27. World Economic Forum, Global Blockchain Council, *Presidio Principles: Foundational Values for a Decentralized Future*, http://www3.weforum.org/docs/WEF_Presidio_Principles_2020.pdf.

28. Principles For Digital Development, *Principle 8: Address Privacy & Security*, https://digitalprinciples.org/principle/address-privacy-security.

29. Moore, Susan, "A proactive approach to privacy and data protection helps organizations increase trust", *Gartner*, 20 January 2020, https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/.

30. Moore, Susan, "A proactive approach to privacy and data protection helps organizations increase trust", *Gartner*, 20 January 2020, https://www.gartner.com/smarterwithgartner/gartner-predicts-for-the-future-of-privacy-2020/.

31. Although not an extensive sampling, the examples chosen in Table 1 are based on some of the stricter privacy regimes in place today, with similar regimes in Australia, Brazil, Chile, China, India, Japan, New Zealand, South Africa, South Korea and Thailand. See: Simmons, Dan, "13 Countries with GDPR-like Data Privacy Laws", *comforte AG*, 2021, https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws.

32. European Commission, *Data protection in the EU*, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

33. State of California Department of Justice, Office of the Attorney General, *California Consumer Privacy Act (CCPA)*, 2018, https://oag.ca.gov/privacy/ccpa.

34. Office of the Privacy Commissioner Of Canada, *The Personal Information Protection and Electronic Documents Act (PIPEDA)*, 2021, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda.

35. "Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems", Case C-311/18, *ECLI:EU:C:2020:559*, 16 July 2020, https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

36. Bank for International Settlements, *Central bank digital currencies: foundational principles and core features*, 2020, https://www.bis.org/publ/othp33.pdf.

37. Department for Digital, Culture, Media & Sport, UK Government, *The UK digital identity and attributes trust framework*, 2021, https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework.

38. Such as the Bank of England.

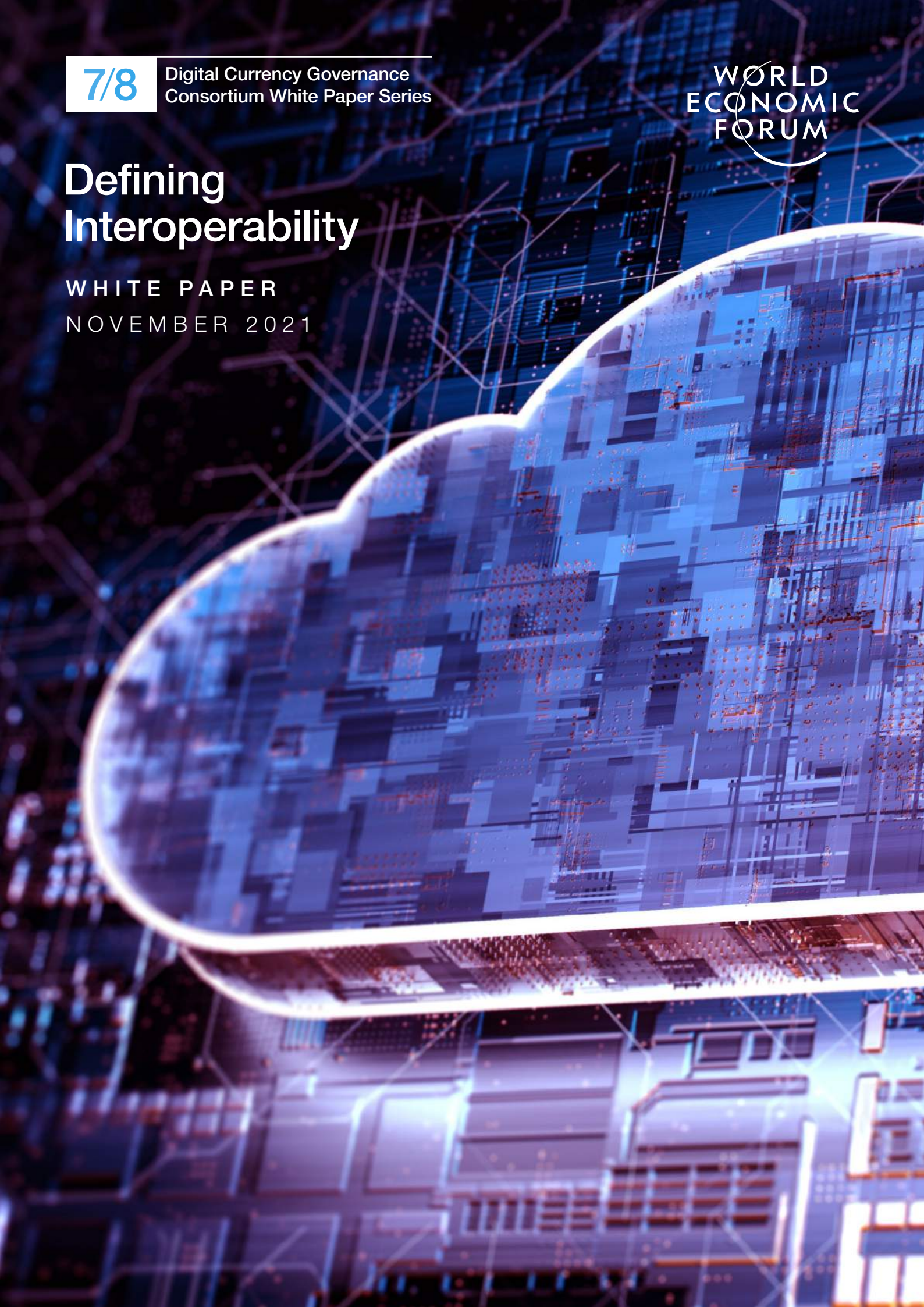
7/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Defining Interoperability

WHITE PAPER

NOVEMBER 2021



Images: Getty images

Contents

Preface 177

Definition of interoperability 178

1 Interoperability design principles and priority outcomes 179

2 Interoperability for central bank digital currency (CBDC) 181

- 2.1 Retail and wholesale CBDC 181
- 2.2 Implementation scenarios for CBDC 182
- 2.3 Examples of implementation in CBDC pilots 183

3 Interoperability scenarios for stablecoins 185

- 3.1 Interoperability challenges for stablecoins 185
- 3.2 Examples of stablecoin interoperability solutions 186

4 Technical standards for CBDC and stablecoin interoperability 187

5 Other considerations for interoperability 191

- 5.1 Integration between digital currencies and existing payment systems 191
- 5.2 Vendor neutrality as a design goal for interoperability 191
- 5.3 Impacts of security and resilience considerations on interoperability 192
- 5.4 Technology build approaches for interoperability 193

Conclusion 194

Endnotes 195

Preface

This paper explores various forms of digital currency interoperability and considers a definition for what the term should mean. It considers the implications of various forms of interoperability for users and other stakeholders and summarizes efforts currently underway.

As various providers and systems for digital payments and currencies enter the market, the challenge of how well these systems can interact, exchange and transact with each other will become more complex. Interoperability is key to spurring coordinated industry development and cross-border financial connections. The interoperability of different digital currency networks across the globe could facilitate adoption and reduce cross-border transaction costs in global commerce. Interoperability of digital currencies with existing payment systems could improve the convenience they offer users.

Consumers and businesses will be more likely to use a given digital currency if it:

- leverages existing acceptance infrastructure
- is supported by known and identifiable payment methods (physical or digital) that are linked to the user's existing devices and accounts
- provides a quantifiable advantage over the existing methods

An advantage could take the form of a new capability, better accessibility (such as for the unbanked), lower transaction cost, or faster completion time.

Interoperability is valuable to achieve the global efficiencies generally desired from digital currencies. However, there are also trade-offs associated with interoperability, such as the benefits or incentives arising from maintaining friction between systems, or the extra time it takes to develop and conform to software or data standards.

This white paper focuses on the interoperability of blockchain-based digital currencies, including central bank digital currency (CBDC) and stablecoins. The paper defines interoperability, identifies the key principles and outcomes for interoperability and highlights existing cases and standards. It also explains important technical considerations for interoperability, such as privacy, digital identity, security and vendor neutrality. The paper is intended for central banks, stablecoin operators and policy-makers.

Definition of interoperability

> Consumers will expect a global digital money system that is as interoperable as an email system

There are existing definitions of interoperability framed by the Bank for International Settlements (BIS)[1] and the World Economic Forum.[2] The following definition of interoperability for blockchain-based digital currency acknowledges that any definition should include both technical aspects (such as the need for systems to be able to exchange information) and expected outcomes.

1. **From a business perspective:** interoperability for digital currency would work towards enabling digital currency issuers to interact with various types of payment systems (potentially including systems of a foreign country) to offer end-users a resilient digital payment infrastructure and efficient payment instruments that are open, standards-based, universally accessible, affordable, secure and always available.

2. **From a technical perspective:** interoperability means that digital currency systems leverage common messaging formats, protocols and/or identifiers which enable seamless payment transfers between users holding different digital currency types.

3. **From a regulatory perspective:** interoperability entails regulatory interchange and a deep consideration of what regulatory differences and nuances exist outside the borders in which the technology and systems are being developed. To ensure interoperability, differences in regulatory guidelines will need to be accounted for.

4. **From a legacy perspective:** interoperability in terms of compatibility with legacy systems should also be considered, as there will be a transition period during which new systems will need to interact with the existing financial infrastructure where value in the form of spendable assets exists today.

1 Interoperability design principles and priority outcomes

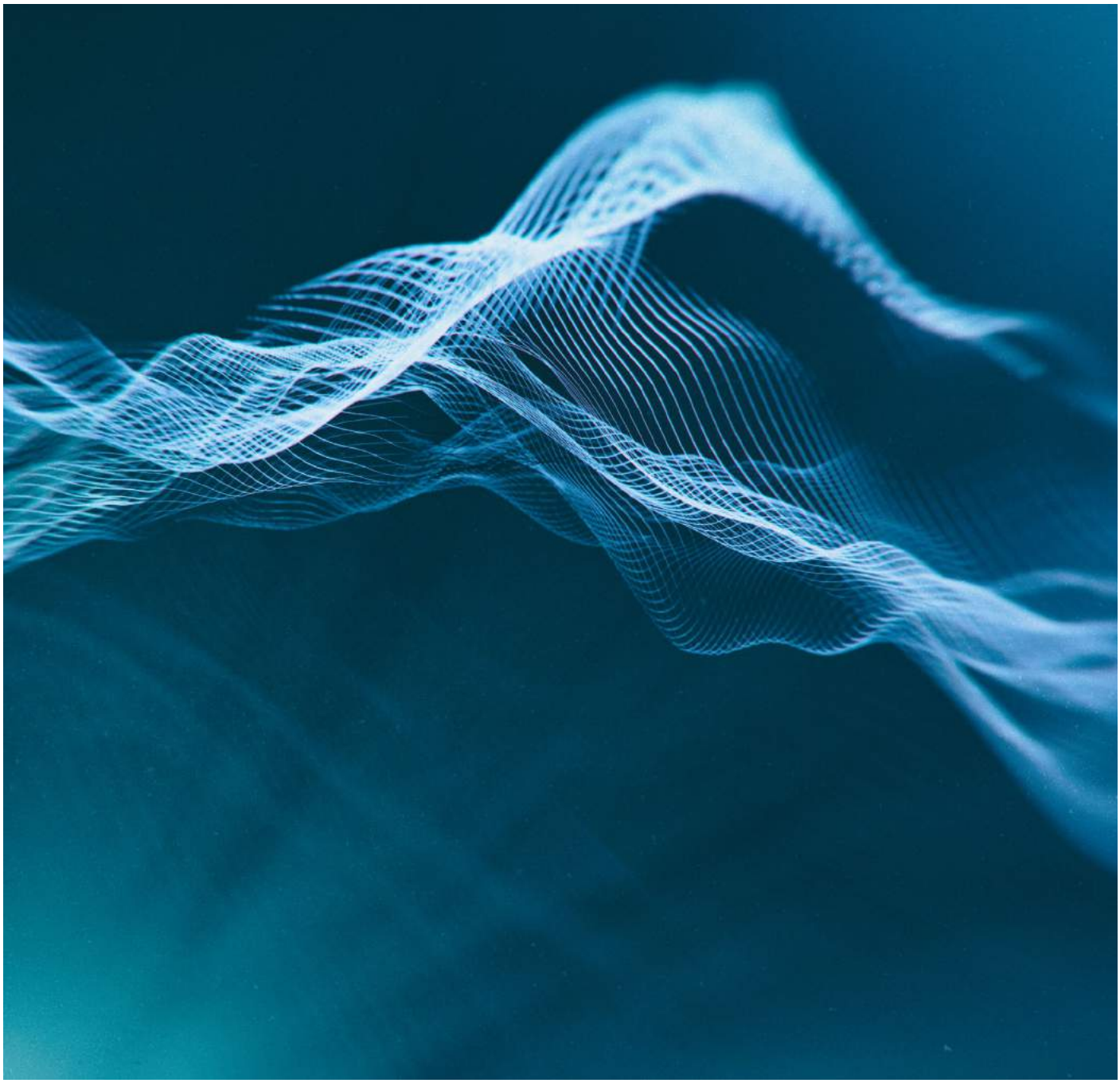
Even though our focus is on blockchain-based digital currency, some key design principles and outcomes for interoperability would be desirable for digital currency in general. These are summarized in the tables below.

TABLE 1 **Key design principles for interoperability**

Interoperability design principle	Description
Universality	Broad acceptance and exchange (as individuals or as commercial entities) via different payment instruments; integration with existing and new payment systems.
Privacy	Common privacy requirements across different networks as most blockchain technologies have their own ways of handling privacy, which makes it much harder to work across ledgers.
Resilience[3]	Enhanced resilience of payment settlements infrastructure to survive shocks to the system (including cyberattacks and counterfeiting), comparable to current conditions or other extraordinary events such as natural disasters.
Security	Secure interoperability mechanisms; minimal risk propagation across interoperable systems (i.e. a weakness, outage, bug or cyberattack on one CBDC should not be able to propagate to another CBDC).
Friendly competition	A level playing field for competition and avoidance of closed-loop payment systems (in which payments can only be made between users of the same payments provider).
Vendor neutrality	Avoidance of locking into specific proprietary technologies or technology providers.
Availability	End-user ability to make payments 24/7/365 via an efficient transaction settlement across networks facilitated by the interoperability of those networks.
Standards compliance	Compliance with appropriate technical and regulatory standards (e.g. data formats, APIs, AML and data privacy).
Durability/Finality	Once a transaction is committed, it remains so.
Atomicity	If one leg of a transaction that involves payment for an asset fails, the whole transaction fails. Ensuring atomicity guarantees delivery upon payment (i.e. Delivery versus Payment, DvP), without the risk of handing over the asset in question if the payment fails.
Predictability	Payment settlement in a predictable time frame (predictable finality). While transfer is occurring, ownership cannot be modified. When it comes to stablecoin, transfer (commit or fail) always results in the token located in one distributed ledger technology (DLT) only.

TABLE 2 | **Priority outcomes for interoperability**

Interoperability priority outcome	Description
Local efficiency	Linkage of domestic digital currencies in a way that enables fast and efficient national payments, reduces transaction and set-up costs and widens direct participation.
International efficiency	Efficient and more affordable cross-border payments, especially for emerging economies. Transactions should be completed as fast as or faster than traditional methods for the same operation.
Low cost	Low or no cost payments for end-users.
User trust and adoption	Improved user experience and confidence in using the system.
Risk reduction	Reduction of counterparty risk in the payments chain.



2 Interoperability for central bank digital currency (CBDC)

2.1 Retail and wholesale CBDC

This section considers both retail and wholesale CBDC types. There are similarities and differences in the issues related to interoperability when comparing both CBDC options. In a domestic setting, it is important for CBDCs to be able to interact with other domestic payment systems.

In a retail setting, the "digital wallet" is one of the elements that impacts the adoption of a system of payment since it is likely to be the main interface for the user to interact with the system. The consumer may expect to use a digital wallet that can hold multiple forms of digital money and digital identity documents, just as their actual physical wallets could today. For retail CBDCs, standards for wallets and how they store, manage and exchange become important for interoperability at a cross-border setting. The integration of retail CBDC with other types of retail payments is another area of interoperability that needs to be considered.

In a wholesale setting, transactions are between banks rather than end-users. Many banks will deal with more than one currency, so – as with wallets – common standards for their representation are desirable. However, when engaging in cross-border transactions, banks will sometimes deal with different networks for each major currency they hold. Here, interoperability between networks becomes important. Being able to conduct exchanges of assets in coordinated transactions across two different ledgers (centralized or decentralized), without requiring an intermediary, will help enhance efficiency and mitigate risk. Coordination among central banks on the conditions to be satisfied before the payments can be executed will also be required.

An example of wholesale CBDC involving different currencies is the BIS innovation hub project involving the central banks of China, Hong Kong, United Arab Emirates and Thailand collaborating on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project.[4] The aim of this project is to develop an international settlement platform through which central banks can utilize CBDC for transactions by financial institutions. The mCBDC project would enable cross-border payments that can be done real-time between the four jurisdictions 24/7, with the foreign exchange leg settled in real time. This project would also provide an example of a retail CBDC being used for cross-border payments, but policy-makers would have to decide whether non-residents could hold CBDC and what foreign exchange controls should be implemented.

According to the BIS's June 2021 report to the G20, *Central bank digital currencies for cross-border payments*,[5] under the mCBDC project a retail CBDC currency conversion can be made so that the other party receives the payment in another retail CBDC. The paper also proposes that an alternative approach would be to consider using wholesale CBDCs as settlement assets in payment versus payment (PvP) mechanisms – both for the settlement of cross-currency retail CBDC transactions and also for the foreign exchange (FX) settlement of cross-currency transactions, either in commercial bank money or in central bank money.

2.2 Implementation scenarios for CBDC

The three key requirements for CBDC interoperability are as follows:

1. **Universality:** interoperability principles must enable CBDC to be accepted across different payment systems (e.g. accepted as a means of payment by different domestic merchants and payment service providers).

2. **Technical standards:** there must be technical standards for interactions between payment systems and CBDC platforms enabling executing transactions in (and across, if permitted) CBDCs.

3. **Payment settlement:** CBDC must integrate with a specified payment settlement system provided by the central bank.

In terms of implementation technology, central bank digital currencies can make use of a combination of different technologies such as traditional centralized databases and systems, shared databases or distributed-ledger technologies. In this context, achieving interoperability is complex given the different technology options being used. For additional discussion, see the white paper in this series entitled *CBDC Technology Considerations*. In addition, the architecture designs need to take into account trade-offs when implementing requirements for privacy, governance and electronic Know Your Customer (eKYC) processes.

Each individual central bank will determine the rules and policies that best suit its domestic market for CBDC, as well as whether to allow foreign access to the CBDC. If the central bank decides to grant cross-border access to the CBDC and it wants to support interoperability with foreign CBDCs, then it needs to create communication protocols and standards to enable domestic and foreign CBDCs to exchange information seamlessly. Such a network would enable different CBDCs to function in a coordinated way and could make cross-border value exchange faster, cheaper and more reliable for businesses and consumers.

In its report to the G20, *Central bank digital currencies for cross-border payments*, the BIS identifies three possible models for multi-CBDC arrangements:

Model 1: mCBDC arrangements based on compatible systems

– In this model, the system might rely on compatible messaging systems and governance arrangements. This could provide additional means for banks and non-banks to settle payments.

Model 2: mCBDC arrangements based on interlinked CBDC systems

– In this model, central banks can interlink their system with others and provide similar functions to model 1 and additional measures, such as safety features (e.g. PvP) and efficiency (e.g. a common clearing mechanism linked to foreign exchange trading).

Model 3: single mCBDC multi-currency system

– This model would provide similar features to model 2 but better integration for foreign exchange and payment settlements for cross-border payments.

Other issues to consider are monetary policy implications and financial stability associated with issuing foreign CBDCs, which may require policy-makers to make accommodations around governance arrangements and system design. There will need to be international coordination among central banks to facilitate the implementation of such arrangements.

In the Visa Research paper *Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies*,[6] the authors propose an offline payment system (OPS) protocol for CBDC that could allow a user to make digital payments to another user while both users are temporarily offline and unable to connect to payment intermediaries (or even the internet). OPS may be used to instantly complete a transaction involving any form of digital currency over a point-to-point channel without communicating with any payment intermediary. The OPS protocol could ensure funds cannot be double-spent during offline payments as no trusted intermediary is present in the payment loop to protect against replay of payment transactions. There would also need to be transaction limits as no one is able to verify the amount held in wallets. Even then, there is still a double-spend risk inherent in offline transactions with this technology.

For additional discussion on these issues, refer to the white paper in this series *The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth*.

2.3 Examples of implementation in CBDC pilots

The examples below show the different implementation pathways and designs adopted by central banks in rolling out CBDCs.

Digital Currency/Electronic Payment (DC/EP) and m-CBDC project

Context

The issuance and circulation of DC/EP by the People's Bank of China (PBOC) for its pilot CBDC is based on a two-tier architecture.[7] The first layer is the central bank and the second layer includes commercial banks and third-party online payment platforms. PBOC issues DC/EP to commercial banks in a wholesale approach. Commercial banks then distribute DC/EP to the public for retail use. A centralized ledger managed by PBOC records all DC/EP transactions and corresponding users. It also records all DC/EP transactions, including the whole lifecycle of issuance, circulation and redemption.

DC/EP is considered as legal tender and is intended to be universally accepted. Commercial banks are heavily involved in the DC/EP wallet setup and KYC processes. The DC/EP wallet supports offline transfers between users, recharge by ATM and mobile POS payments using QR codes. Commercial banks and third-party payments companies play a key role in the distribution and redemption of DC/EP and are responsible for KYC. The wallet establishes a custodian relationship between commercial banks and retail users.

Interoperability design

DC/EP is leveraging existing payment channels for distribution domestically. As noted above, PBOC is developing a Multiple Central Bank Digital Currency (m-CBDC) Bridge Project[8] jointly with the Hong Kong Monetary Authority (HKMA), Central Bank of the United Arab Emirates (CBUAE) and Bank of Thailand, supported by the BIS Innovation Hub, to explore the global adoption of DC/EP. The Bridge Project aims to explore the capabilities of distributed-ledger technology (DLT) through developing a proof-of-concept prototype to facilitate real-time, cross-border foreign exchange PvP transactions in a multi-jurisdictional context and on a 24/7 basis. The m-CBDC Bridge Project will also explore business use-cases in a cross-border context using both domestic and foreign currencies.

Bank of Thailand pilot CBDC project[9]

Context

The Bank of Thailand (BoT) CBDC pilot project is a public-private partnership to explore the efficiency of CBDC payments in the business sector. The prototype is based on a two-tiered model where BoT issues the CBDC to the commercial banks and payment service providers that handle the distribution to the business sector. The goal for interoperability in this case was to communicate between two or more blockchain/distributed-ledger systems.

Interoperability design

- **Asset-level:** the "universal token" (the main token standard used in the Codefi Assets API) is interoperable with other Ethereum-based ERC token standards[10] and compatible with services currently supported by wallets and key custody solutions.
- **Network-level:** the prototype is based on Ethereum protocol using Hyperledger Besu, which makes it interoperable with any private Ethereum network as well as with the Ethereum Mainnet.
- **Application-level:** for the CBDC platform to be interoperable with other applications, the open application programming interface (API) layer must be standardized and well-designed to ensure seamless interoperability.

Riksbank e-krona

Context

The Riksbank e-krona pilot project is a two-tiered CBDC model. In the first tier, the Riksbank will issue Swedish Krona (SEK) to, or redeem SEK from, participants in an e-krona network of intermediaries, such as banks. In the second tier, the first-tier participants will distribute SEK to end-users.

Interoperability design

The e-krona pilot project is expected to be linked with the real-time gross settlement (RTGS) system in the future and this will enable it to integrate with other payment systems.[11]

Table 3 compares some of the design features of the CBDC pilots mentioned above. As can be seen, there are differences in how different elements of the systems are approached and implemented.

TABLE 3 **Design features of select CBDC pilots and proposals**

Implementation/ design features	DC/EP – PBOC, China	e-krona – Riksbank, Sweden	Bank of Thailand CBDC
Purpose	Retail CBDC	Retail CBDC	Business to business payments
Architecture	Two-tier model	Two-tier model	Two-tier model
Nature of intermediary	Commercial banks and payment service providers	Commercial banks and payment service providers	Commercial banks
Role of intermediary	Circulates DC/EP to public and performs onboarding and eKYC process	Circulates e-krona to public and performs onboarding and eKYC process	Circulates CBDC to businesses and performs eKYC
Digital wallet	Activated after eKYC	Activated after eKYC	Activated after eKYC
Privacy	Controlled anonymity	Pseudo-anonymous transactions supported. AML authority issues anonymity vouchers that enable anonymous transactions up to a certain volume within a time period.	Private transactions supported
Identity verification	Public Key Infrastructure (PKI) is used for high-end users and organizations. Identity-based cryptography used for small value payments.	PKI used	PKI used
Support offline payments	Yes	Yes	Out of scope, did not test as part of this project
KYC/AML	Performed by intermediary	Anti-money laundering (AML) authority performs AML checks	Out of scope, did not test as part of this project
Interoperability	A DC/EP wallet is needed for all transactions involving payments made with DC/EP. DC/EP wallets can be linked to accept payments from other private sector payment systems. The m-CBDC Bridge Project is being conducted to evaluate the feasibility of cross-border exchange.	Expected to be integrated with RTGS system	Compatible with Ethereum-based networks

3 Interoperability scenarios for stablecoins

3.1 Interoperability challenges for stablecoins

The goal of stablecoins is to provide an alternative form of cryptocurrency with relatively stable value. In this paper, the focus is mainly on the collateralized stablecoin model, where stability is achieved by linking the digital currency to a reserve of stable real assets, such as fiat currencies or commodities.

There are two key interoperability challenges with stablecoins:

1. **Transfers on the same blockchain:** to enable transfers (e.g. sending USDC stablecoin) implemented on the same blockchain type. Decentralized swapping services or exchanges facilitate the execution of a stablecoin swap (i.e. the transfer from one stablecoin asset to another digital asset type) to a single blockchain without an intermediary. This change from one asset type to another within the same blockchain could involve smart contracts, automated payment paths, or a decentralized exchange function.

2. **Transfers on different blockchains:** to enable transfers of different stablecoins implemented on different blockchain types (e.g. from Tether to Fnality Utility Settlement Coin). The interoperability of token transfer for different stablecoin types on different blockchains is possible through centralized exchanges,[12] decentralized atomic cross-chain swaps,[13] or other cross-chain protocols. For interoperability between different stablecoins over different blockchain types, atomic cross-chain swaps[14] enable token transfer between different blockchains without an intermediary. This is an area which has attracted a lot of research and is still evolving.

Most stablecoins are generally based on a distributed-ledger technology architecture. Blockchain interoperability will play a key role in interoperability for stablecoins. Interoperability scenarios for stablecoins would encompass the following:

- **Scenario 1:** transfer of different stablecoin types between sender and receiver implemented on the same blockchain

- **Scenario 2:** transfer of the same stablecoin type between sender and receiver – but their blockchains are different

- **Scenario 3:** transfer of different stablecoin types between sender and receiver – and they belong to different blockchains

For implementations based on public blockchains, interoperability can be achieved through sidechains,[15] hash-locks[16] and notary schemes.[17] When it comes to enabling interoperability across different blockchain types, cross-chain interoperability comes into play.

Cross-chain protocols provide one possible option to create an interoperable network for private chains, where a third blockchain acts as a bridge for other chains.[18] This middle layer maintains a cryptographically secured, time-stamped ledger of the various activities between different blockchains. It is like a single chain hosting a network of chains, making the whole process more efficient. Cross-chain technology seeks to facilitate atomic swap between different blockchains without an intermediary, although the technology is generally yet to be implemented in a manner that is fully functional.

3.2 Examples of stablecoin interoperability solutions

Some projects that are currently working on research in the area of cross-chain interoperability are provided below as examples.

Canton[19]

Developed by Digital Asset, Canton is a DAML ledger interoperability protocol whose smart contract language and synchronization protocol guarantees data is reliably shared only with entitled parties despite the presence of malicious actors. DAML is a smart contract programming language with built-in models of authorization and privacy. By partitioning the global state, it solves both the privacy problems and the scaling bottlenecks of public blockchains allowing developers to balance auditability requirements with GDPR compliance.

ChainBridge[20]

ChainBridge is an open source (LGPL) token bridge developed by ChainSafe. It provides the ability to transfer a token from an Ethereum-compatible or substrate (Polkadot), by using a smart contract deployed on each chain and a set of relayers.

Cosmos[21]

Cosmos Network and Interchain Foundation developed the inter blockchain communication (IBC) protocol, which acts like an interoperability bridge between all the chains that follow Tendermint consensus protocol. The IBC protocol functions as a messaging protocol for blockchains, similar to TCP/IP.

Hyperledger Cactus[22]

Hyperledger Cactus is a blockchain integration tool designed to allow users to securely integrate different blockchains. This pluggable architecture helps enable the execution of ledger operations across multiple blockchain ledgers, including Hyperledger Besu, Hyperledger Fabric, Corda and Quorum, with the aim of continually adding support for new blockchains in the future.[23]

Interledger Protocol (ILP)[24]

Interledger Protocol aims to promote an equitable web with an open-source protocol that connects different payment networks to each other via a series of escrowed payment transfers.

Liquality[25]

Liquality launched a cross-chain application that lets users transact between Ethereum and Bitcoin in a trustless and decentralized manner. Liquality also implemented cross-chain atomic swap between ether, bitcoin and stablecoin DAi.

Optics[26]

Developed by cLabs, Optics is a cross-chain communication protocol which enables Celo stablecoin to communicate with other blockchain systems (such as Polkadot, Cosmos and Ethereum amongst others).

Polkadot[27]

Like Cosmos, Polkadot has developed specialized chains for each blockchain application and implemented interoperability between them using the Polkadot protocol. Polkadot unites a network of heterogeneous blockchain shards called parachains to address scalability issues. These chains connect to and are secured by the Polkadot relay chain. They can also connect with external networks via bridges. Interoperability in Polkadot enables cross-blockchain transfers of any type of data or asset. The protocol can transfer data across public, open, permissionless blockchains as well as private, permissioned blockchains. This makes it possible to build applications that get permissioned data from a private blockchain and use it on a public blockchain.

Syscoin[28]

Syscoin developed an interoperability bridge known as Sysethereum bridge that enables exchange between SPT (a token on Syscoin blockchain) and ERC-20 (a token standard on the Ethereum blockchain).

4 Technical standards for CBDCs and stablecoin interoperability

Technical standards for the following processes or issues are required to enable interoperability across different levels:

- Messaging
- Privacy
- Anti-money laundering and combating the financing of terrorism (AML/CFT)
- Identity and authentication
- Distributed-ledger technology (DLT) protocols
- Certification of interoperability for CBDC and stablecoins
- Inter-currency exchange rate standards

In addition to standards, coordination between central banks would be a key factor in fostering interoperability for CBDCs to address areas such as KYC, privacy, data exchange and messaging formats for cross-border payments. Below we outline some existing initiatives aimed at setting standards and framing high-level principles.

Standard-setting efforts

There are several standard-setting initiatives underway with respect to digital currency:

- Global Standards Mapping Initiative,[29] led by the Global Blockchain Business Council and the World Economic Forum to survey blockchain standards
- Tokenization and smart-contract standards, led by InterWork Alliance
- Market and conduct standards and best practices for digital currency, led by Global Digital Finance

One notable cross-disciplinary standard-setting initiative is the Digital Currency Global Initiative (DCGI).[30] DCGI is a collaboration between the International Telecommunication Union (ITU) and Stanford Digital Currency Program of Stanford University to study the requirements for technical standards for central bank digital currency and stablecoins. The DCGI has set up three working groups on policy and governance, architecture, interoperability and use-cases, and security. The working groups are composed of stakeholders from the information and communications technology (ICT) sector, financial services sector, central banks, digital currency providers, academia and fintech companies. The DCGI is also working towards developing metrics that could be used to benchmark performance of CBDC and stablecoin systems and to provide test criteria for assessing and certifying the level of interoperability of these systems.

Messaging standards

Messaging standards that are compatible with ISO 20022 will be important for integration with existing payment systems for CBDC and stablecoins. Entrenched as a common business language for the financial marketplace, ISO 20022 is firmly positioned as an element of coalescence for new and contrasting fintech innovations, such as DLT, smart contracts and APIs. For example, the ISO 20022 standard is widely used in payments automation in the RTGS and trade finance networks. The standard allows payments to contain more structured data, standardizes payment formats that were previously inconsistent and includes information needed by banks to comply with AML requirements. To enable integration with existing payment systems, there will be a need to package the instructions to be sent from the CBDC or stablecoin system into an ISO 20022-compatible structure for hand-off to the client by a smart contract present on the distributed ledger.

Standards for privacy

The degree of privacy/anonymity could vary from country to country depending upon the governance, regulations and implementation of the system. When interoperating, the level of privacy would default to the lowest common level of privacy used. One way to ensure interoperability is for regulators to come together to form some level of standardization across different privacy rules.

A number of new developments in zero-knowledge cryptography and other technologies in privacy research may offer a different approach to ensure interoperability in a fragmented regulatory world. Such privacy-preserving technology promises to allow for truly secure privacy in transactions, even in account-based models and automation of the implementation of the privacy rules. There are efforts underway with the US Department of Commerce's National Institute of Standards and Technology (NIST) and ZKProof, an open-industry academic initiative, to standardize zero-knowledge proof to create reference and guidelines in privacy-preserving cryptography studies. There is also a standardization effort underway on homomorphic encryption with guidelines for how to use the schemes.

More detailed discussions on privacy-preserving technologies, such as zero-knowledge proofs and homomorphic encryption, can be found in the white paper in this series entitled *Privacy and Confidentiality Options for Central Bank Digital Currency*.

Standards for AML/CFT

Laws and regulations on anti-money laundering and combating the financing of terrorism (AML/CFT) are crucial in maintaining the safety of the payments system. As with privacy, the laws and regulations on AML/CFT vary from country to country. Global coordination on AML/CFT is required to create a more interoperable environment when it comes to cross-border payments using digital currency. In addition, such regulations have not been collated into a standardized data format to allow for automation. One possible solution to achieve more interoperability is for a given government or intergovernmental organization to provide a centralized database for digital currency service providers to obtain a risk score regarding illicit activity with respect to a particular transaction or individual.

Standards for identity and authentication

Interoperable identification and authentication schemes will be key to enable organizations to meet the Financial Action Task Force (FATF) AML/CFT guidelines for customer due diligence.[31] The digital identity community has begun to unify around a common set of standards for presenting, exchanging and validating digital credentials, so that credentials issued by one can be consumed by another. A standard is needed for a unified digital identity protocol for DLT to communicate with off-chain systems. Currently different DLT platforms use different methods for this. The Worldwide Web Consortium (W3C), the ITU Study Group 17 on security and the International Organization for Standardization (ISO) are all working towards developing international standards for decentralized identifiers that enable verifiable digital identities in a decentralized way using DLT and PKI. This will eliminate the need for centralized registries or identity providers, allowing users the flexibility of having control over their personal data. The South Korea-based DID Alliance, an open-industry association for decentralized identity (DID) services, has developed the Global Architecture for Digital Identity (GADI)[32] which uses a digital address.

Leveraging recent advancements in the field of digital identity with identity-credentialing will enable wallets to exchange within jurisdictions and outside of them as well. There are currently two approaches for users to prove who they are so that they can transact from endpoint to endpoint.

One approach is to use self-sovereign identity (SSI),[33] where a user generates their own decentralized identifier(s)[34] and an institution issues documents called "verifiable credentials" that attest to facts attached to that individual by binding to their decentralized identifier. Those credentials are held by the individual, who presents them when asked for. They can be verified for accuracy, such as proof of employment or the result of a KYC check. SSI provides a common identity system without defaulting to any government or one institution to be the sole source of truth. It offers a potential path to harmonizing KYC standards.

The second approach is a more traditional account-based or token-based model with identity established by trusted institutions, which can be a national government or financial institution. A digital wallet would therefore not only need to hold funds in a given digital currency, but also potentially other types of verifiable credentials such as credit score, national ID etc. A user can move their credentials from one "identity wallet" to a competing one with better features.

Standards for DLT protocols

> DLT interoperability can be defined as the ability of a DLT network to exchange information with other networks and to use the information that has been exchanged

DLT protocols will also require common standards for interoperability. A DLT interoperability solution must propose a universal method to read data and update it for all types of blockchains. DLT interoperability can be defined as the ability of a DLT network to exchange information with other networks and to use the information that has been exchanged. In CBDCs and stablecoins based on DLT, the issues identified in the previous sections on cross-chain data exchange among different DLT systems are areas where standards are required. For example, a DLT platform should implement locking, secret-key disclosure and timeout to successfully build a Hashed Time Lock Contract (HTLC)[35] functionality. However, there are no standards to govern how HTLC is implemented on each of the DLT platforms, so HTLC implementation may differ from one platform to another.

To address the lack of standards for DLT protocols, a DLT interoperability bridge layer – which can be considered as a kind of DLT API – is required to provide a controlled and common method for exchanging and processing data across DLT networks and legacy systems. The interoperability layer would need to contain standard methods to achieve interoperability for the following functions:

- Different governance rules
- Unified messaging
- Atomicity of transactions
- Secure end-to-end transactions
- Facilitate off-chain data exchange (e.g. for digital identity verifications)

Standards for certifying interoperability of CBDCs and stablecoins

A common method for assessing and certifying the interoperability of CBDC and stablecoin systems would help level the playing field and consolidate attention on projects that meet an agreed standard, thereby facilitating interoperability.

In the ITU standardization sector, ITU-T Study Group 16 (SG16)[36] started work on DLT interoperability and standards in 2019. The scope of this group's work includes making standards for DLT platforms and for applications and services built on top of these platforms. In particular, the group is working on approaches to technical DLT interoperability that would also be applicable to digital currencies and payment systems based on DLT architecture.

The first type of interoperability is named by ITU-T SG16 as "north-south interoperability" and includes two subtypes:

- Communication between applications and the underlying DLT platform – which may involve promoting the compatibility of different DLT system interfaces and simplifying the adaptation work between applications and DLTs.
- Communication between DLT and off-chain systems acting as input or output to DLT computation (like financial, governmental or industrial systems); this focuses on safe and trustworthy interaction between off-chain systems and DLTs.

The second type of interoperability is called "east-west interoperability", or inter-chain interoperability, and may involve DLT systems using the same protocol or different ones. This type of interoperability involves a cross-chain communication protocol as well as identification and governance, which include malicious nodes punishment and abnormal transaction rollback. Some technologies used to implement atomicity in this type of interoperability include "two-phase commit" and "time lock". ITU-T SG16 has already published recommendations that directly relate to technical interoperability, including:

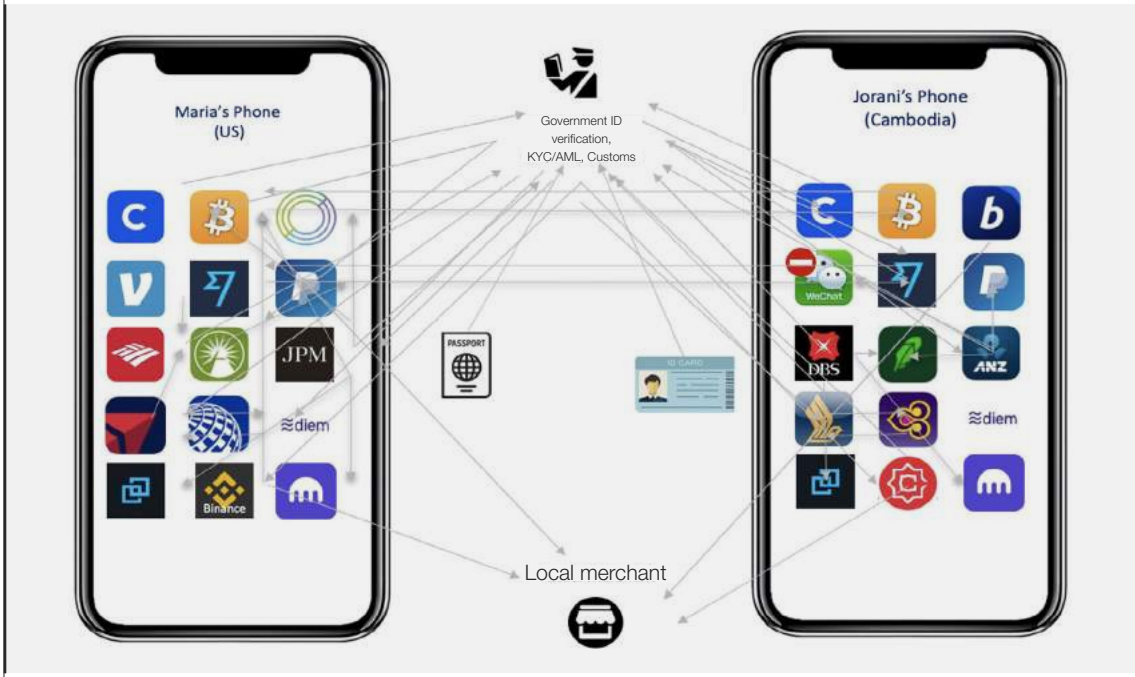
- ITU-T F.751.0 "Requirements for distributed ledger systems"[37]
- ITU-T F.751.1 "Assessment criteria for distributed ledger technologies"[38]
- ITU-T F.751.2 "Reference framework for distributed ledger technologies"[39]

Standards for digital wallet interoperability

For most consumers, interoperability will be most sharply felt at the level of a wallet application on their mobile device that holds at least one payment instrument, though likely more. A combination of unified experience, optionality, widespread and open standards adherence and other qualities may be the best embodiment of the interoperability design principles stated earlier. To understand what the consumer expects of interoperability of their digital wallet, a good guide would be the interoperability of internet email systems and e-mail clients. People can send emails to one another using many different types of email service providers. Most people use one particular email client on their phone, from which a user can access multiple accounts on different mail providers and send mail from any of those accounts to any other email account on the internet. You can even use a different email client on a different device, such as a web-based interface or local mail client while sitting at your laptop, accessing the same message store and even the same preferences.

Figure 1 is an illustrative wallet and application example scenario, which is currently tolerated by consumers but begs for simplification.

FIGURE 1 **A view of the current user experience for consumers**



Source: The Linux Foundation, Karen Ottoni

Today, wallets may be built across protocols, around particular protocols, or around particular exchanges and custodians. As the variety of options and providers for digital payments increases, consumers will most likely want to simplify the number of applications and wallets they engage with and have a unified user experience when purchasing goods globally or travelling across borders. Consumers will expect a global digital money system that is as interoperable as an email system. To meet such expectations, we need to think about how digital money is converted among providers and exchanged, and also how the consumer wallet ecosystem could be shaped to meet the principles set forth in this white paper.

5 Other considerations for interoperability

5.1 Integration between digital currencies and existing payment systems

Standardized common protocols are critical for integrating stablecoins and CBDCs into existing payment systems. For example, according to the ISO, currencies are supposed to be represented by three characters (e.g. CNY, EUR, USD). To implement a stablecoin such as the Pax Dollar (USDP)[40] or Gemini dollar (GUSD)[41] and integrate it within a core banking system would require current banking systems to handle a four-character currency unit.

To avoid creating payment silos, public-private sector partnerships could work towards enhancing integration. For example, in February 2021, Mastercard and Island Pay launched the Bahamas Sand Dollar prepaid card, giving people the option to instantly convert the Sand Dollar CBDC to traditional Bahamian dollars and pay for goods and services anywhere Mastercard is accepted on the islands and around the world.

5.2 Vendor neutrality as a design goal for interoperability

Vendor neutrality is an interoperability design goal. When there are multiple substitutable and competitive providers of products and services leveraging a common network or platform, it is *prima facie* evidence that interoperability has been achieved to at least some degree. The greater the number of providers and network/platform participants, the greater the degree of interoperability. However, there exists a tension between vendor neutrality and a government's desire for autonomy and data-residency (whereby data is required to be stored inside a given country).

In the short term, a vendor-specific solution can be attractive because closed-loop interoperability is always easier to achieve in a single-vendor solution. However, there are both technology and business risks to a single-vendor platform in the long term. For example, if there are any changes to the vendor's ability to manage or deliver, then that puts each implementation at risk. The goal of vendor neutrality helps focus deployment efforts on outcomes and strategy rather than rely on a specific vendor's claims of compatibility. The diversity of vendors or other support and service providers involved in the deployment of a CBDC or stablecoin network might support business and operational resiliency.

Examples of vendor neutrality

The European Union's Connecting Europe Facility (CEF)[42] recognizes that a lack of cross-border interoperability of digital tools and services is a barrier that inhibits market potential. Its aim is to provide regulatory conditions and cross-border digital infrastructures which facilitate interoperability.

Some CBDC and stablecoin research and pilots are taking a vendor-neutral approach. One example is Project Ubin.[43] Initiated by the Monetary Authority of Singapore, vendors representing various platforms were invited to participate along with 11 financial institutions in a five-phase project over five years. Along the way they shared their findings in published reports and shared their source code[44] as well, contributing to the public knowledge on how best to build a digital monetary system. The MIT Digital Currency Initiative is currently working with the Federal Reserve Bank of Boston on research to evaluate the requirements for a US CBDC design based on first principles.[45] They have stated they will release a report and make what they develop available as open-source material. The Stellar Development Foundation supports projects building on the open-source Stellar network that leverages over a dozen interoperable world currency stablecoins to improve financial access and inclusion, especially in emerging markets. There are many examples of efforts like these that demonstrate that an open, vendor-neutral approach helps to create systems that integrate across competitors and platforms, enabling industry-wide transformation.

5.3 Impacts of security and resilience considerations on interoperability

Security and resilience are imperative for any system that is managing payment transactions and holding funds for companies and users, but this is perhaps even more critical when the system is tied to a national currency. What happens when bad or irrational actors attempt to corrupt or steal? How can a central bank prevent and guard against this?

Any large-scale digital currency initiative will become a serious target for attack, which is why security is an essential characteristic of any digital currency to be proven and tested before its launch. For more discussion on cybersecurity considerations for CBDC, refer to the white paper in this series entitled *CBDC Technology Considerations*.

Wallet software security

> There are many ways to design a CBDC or stablecoin but as yet no broadly accepted standard for ensuring the security of digital currencies

It is evident that security considerations for interoperability are both crucial and complex, in part because there are many ways to design a CBDC or stablecoin but as yet no broadly accepted standard for ensuring the security of digital currencies. Any CBDC developed on a DLT would need to be assured of the secure design of any other digital currency it may interoperate with. Given the motivation of many CBDC projects for financial inclusion, end-users will most probably need to access currencies via a smartphone, as discussed in the section above. However, current software security is insufficient to secure a CBDC in a smartphone, even though there are technologies in development that have potential for this in the medium to long term, according to the Bank of Canada.[46]

Wallet software security will need to be strong and central banks should take abundant caution when designing how wallets are built and audited, ensuring timely updates as needed. Certifications could play a role in assuring security for blockchain-based digital currency networks, by establishing an approved base of characteristics which wallets and networks must meet to be able to operate and transact with CBDCs. Like web browser software, it seems preferable from a security point of view to see a relatively small number of widely used wallets that can handle multiple kinds of CBDCs and stablecoins, so that each can be better built, more thoroughly vetted and well certified, rather than a separate wallet app per CBDC or token.

Network collaboration for security

Given the global nature of exchange and commerce, there is an incentive for CBDCs and stablecoins to interoperate and to be connected to the internet despite the range of risks it presents. Networks are frequently subject to shocks and attacks, so interoperability between networks can enhance overall resilience, by providing alternative paths for sharing states and allowing transactions across different networks. Software diversity can be valuable, too: having a diverse set of clients implementing the same protocol but in different languages or by wholly separate teams, as we see in the Ethereum ecosystem (e.g. Go-Ethereum, Quorum, Hyperledger Besu etc.), provides assurance that defects in one implementation would be tougher to exploit across the entire network at once.

One form of interoperability will be about getting network participants talking with the same protocol. However, a monoculture of technologies is not the goal either and would actually reduce security and resilience. What could help, while reducing complexity, is a small set of protocols to facilitate interoperability and a diversity of networks and implementations leveraging those protocols so that if something goes wrong in one network, it does not necessarily affect the whole system. The objective is to leverage the benefits of decentralization and distribution of networks while also enabling those disparate networks to communicate. CBDC and stablecoin settlement networks should strive to reproduce that phenomenon, which is why using common software advancing the work of standards is so important. Generally, software that is developed in the open with multiple stakeholders involved tends to be more secure and resilient.[47]

As security technology develops, so will the skills of those who seek to undermine security systems. Interoperability can introduce new vulnerabilities. Future-proofing security and resilience is an important consideration for central banks and private companies embarking on launching digital currencies. In practical terms, central banks will need to set aside research and development funds on hardware and software to ensure both are more secure than average and establish insurance policies against breaches as well.

5.4 Technology build approaches for interoperability

There are three ways in which organizations and governments can come together to leverage technology for digital currencies: buy, build, or co-create. Buying is quick and easy. Building allows you to control and customize. Both have advantages and disadvantages, depending on the situation. However, there is a third path that the open-source community has paved for the last 20 years: co-creation.

Co-creating technology in the open can serve to achieve the goals of interoperability: multiple requirements and perspectives can be incorporated, while the process can leverage the benefits of a vendor-neutral solution. Common needs are best served by building common solutions and the interoperability of CBDC and stablecoin networks will need an approach that reflects the end goal.

The benefits of an open-source solution

The telecommunication industry has demonstrated the benefits of competitors collaborating openly on ecosystem-wide technology to advance scalability, efficiencies and user experience. Open cellular standards, developed in vendor-neutral settings, have enabled the evolution of mobile wireless technology, as well as being a driver of innovation and multi-vendor interoperability. The return on investment is far greater than any one organization could generate on its own. According to the Linux Foundation's annual report for 2020, over 70% of global telecom subscribers are built on LF Networking's open-source projects. "The investment to recreate LFN's 87 million lines of source code would exceed 700,000 person-months of development time, or $7.3 billion of capital", says the report.[48]

In the race to 5G wireless technology, the public and private sectors are embracing open collaboration. Governments and enterprises face similar challenges, where integration can become an operational burden if solutions are incompatible. The Defense Advanced Research Projects Agency (DARPA), part of the US Department of Defense, is enabling US government suppliers to collaborate on a common open-source platform that will enable the adoption of 5G wireless and edge technologies.[49] The Open Radio Access Network (O-RAN) alliance challenges Huawei's proprietary *modus operandi* in 5G by simply bringing operators together to build openly, thereby diminishing the secrecy of proprietary hardware.[50] Open-network architecture is often described as a "white box", replacing the secret solutions that infrastructure vendors use to keep customers locked into their equipment.

There are potential downsides to mandating the use of open-source licensed software, or even releasing bespoke or highly customized software as open-source code to the public. Open-source software, like all software, can contain both inadvertent defects and intentional back doors. The only fix for this is greater investment into the code and greater scrutiny by auditors and end-users. It may be easier to obtain the source for open-source code, making it easier to audit. This in turn could drive greater adoption and commercial support opportunities, resulting in a more competitive marketplace around it. But releasing code as open-source does not automatically lead to such additional scrutiny, investment or competition. So a thoughtful strategy around open-source must include the engagement of additional stakeholders (e.g. central banks, commercial banks, regulators, software vendors and systems integrators) – and enough of them to matter. Most governments already use and understand the benefit of open-source technology; in the case of CBDCs there is an opportunity to collaborate early on in the experimentation process with others, which can accelerate the development of interoperable solutions.

Conclusion

It is critical to reiterate the importance of having a common definition of interoperability for digital currencies. The definition presented in this paper covers both technical aspects (such as the need for systems to be able to exchange information) and the expected outcomes of interoperability.

In a globalized world, the consumer's desire to easily use different types of digital payment and access basic financial services is likely to increase. While there are numerous business, technical and regulatory challenges to achieving interoperability of a currency, we encourage businesses and central banks to consider the factors mentioned in this paper in their early design decisions. This will require collaboration between business operators, policy-makers, technologists and regulators throughout early conceptual conversations and planning.

Many of the factors considered in this paper would benefit from standard-setting and there are governing bodies and institutions already engaged in this work. We encourage business operators and central banks to contribute to efforts in setting standards and defining a common taxonomy. Adopting shared standards would create common ground for the implementation of interoperable digital currencies and technical aspects of their exchange.

Endnotes

1. Bank for International Settlements, *Central bank digital currencies: foundational principles and core features*, 2020, https://www.bis.org/publ/othp33.pdf.
2. World Economic Forum, *Bridging the Governance Gap: Interoperability for blockchain and legacy systems*, White Paper, December 2020, http://www3.weforum.org/docs/WEF_Interoperability_C4IR_Smart_Contracts_Project_2020.pdf.
3. Auer, Raphael and Böhme, Rainer, *The technology of retail central bank digital currency*, Bank for International Settlements, 2020, www.bis.org/publ/qtrpdf/r_qt2003j.pdf.
4. "Joint statement on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project", *Hong Kong Monetary Authority*, 23 February 2021, www.hkma.gov.hk/eng/news-and-media/press-releases/2021/02/20210223-3.
5. Bank for International Settlements, *Central bank digital currencies for cross-border payments*, Report to the G20, July 2021, https://www.bis.org/publ/othp38.pdf.
6. Christodorescu, Mihai et al., *Towards a Two-Tier Hierarchical Infrastructure: An Online Payment System for Central Bank Digital Currencies*, Visa Research, December 2020, https://arxiv.org/pdf/2012.08003.pdf.
7. Kong, Shuyao, "DCEP: An inside look at China's digital currency", *Decrypt*, 28 June 2020, https://decrypt.co/33866/dcep-an-inside-look-at-chinas-digital-currency.
8. "Joint statement on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project", *Hong Kong Monetary Authority*, 23 February 2021, www.hkma.gov.hk/eng/news-and-media/press-releases/2021/02/20210223-3.
9. Bank of Thailand, *Central Bank Digital Currency: The Future of Payments for Corporates*, https://www.bot.or.th/English/FinancialMarkets/ProjectInthanon/Documents/20210308_CBDC.pdf.
10. "Token Standards", Ethereum, 2021, https://ethereum.org/en/developers/docs/standards/tokens/.
11. Financial Stability Board, *Enhancing Cross-border Payments, Stage 1 report to the G20*, 9 April 2020, www.fsb.org/wp-content/uploads/P090420-1.pdf.
12. See Glossary in Compendium Report
13. See Glossary in Compendium Report
14. Hammond, Matthew, "Blockchain Interoperability Series: Atomic Swaps", *Medium*, 23 September 2019, https://medium.com/@mchammond/atomic-swaps-eebd0fa8110d.
15. Ray, Shaan, "What are Sidechains?", *Hacker Noon*, 22 January 2018, https://hackernoon.com/what-are-sidechains-1c45ea2daf3.
16. Min, Alex, "Hash Time Locked Contracts (HTLCs) Explained", *Liquality*, 3 April 2019, https://liquality.io/blog/hash-time-locked-contracts-htlcs-explained/.
17. Buterin, Vitalik, *Chain Interoperability*, R3 Research, September 2016, https://www.r3.com/wp-content/uploads/2018/04/Chain_Interoperability_R3.pdf.
18. Pillai, Babu et al., *Cross-chain interoperability among blockchain-based systems using transactions*, The Knowledge Engineering Review 35, June 2020, https://www.researchgate.net/publication/341791407_Cross-chain_interoperability_among_blockchain-based_systems_using_transactions.
19. Canton, *Canton: A Daml based ledger interoperability protocol*, 2020, https://www.canton.io/publications/canton-whitepaper.pdf.
20. "Chainsafe / ChainBridge: Modular Multi-Directional Blockchain Bridge to interact with Multiple Networks; Ethereum, Ethereum Classic, Substrate, based Chains", *GitHub*, 2021, https://github.com/ChainSafe/ChainBridge#installation.
21. Belchior, Rafael et al., *A Survey on Blockchain Interoperability: Past, Present, and Future Trends*, arXiv, 2021, https://arxiv.org/pdf/2005.14282.pdf.
22. "Hyperledger Cactus", *Hyperledger*, https://www.hyperledger.org/use/cactus.
23. "Interoperability and Integration Developments in the Hyperledger Community", *Hyperledger*, 28 May 2020, www.hyperledger.org/blog/2020/05/28/interoperability-and-integration-developments-in-the-hyperledger-community.
24. "About Us", *Interledger Foundation*, 2021, https://interledger.org/about-us/.
25. Huillet, Marie, "BTC, ETH, DAI Cross-Chain Atomic Swaps Launched By Liquality on Mainnet", *Cointelegraph*, 25 June 2019, https://cointelegraph.com/news/btc-eth-dai-cross-chain-atomic-swaps-launched-by-liquality-on-mainnet.
26. Nyzio, Joe, "Announcing Optics: A Gas-efficient Interoperability Standard for Cross-Chain Communication", *Celo*, 21 April 2021, https://medium.com/celoorg/announcing-optics-a-gas-efficient-interoperability-standard-for-cross-chain-communication-e597163b2.
27. Wood, Gavin, *Polkadot: Vision for a heterogenous multi-chain framework*, Draft 1, Polkadot Network, https://polkadot.network/PolkaDotPaper.pdf.
28. "Syscoin Bridge & How It Works", *Syscoin Platform*, 2021, https://syscoin.readme.io/docs/what-is-sysethereum-bridge-how-does-it-work.

29. "Global Standards Mapping Initiative (GSMI)", *Global Blockchain Business Council*, 2021, https://gbbcouncil.org/gsmi/.
30. "Digital Currency Global Initiative", *International Telecommunication Union (ITU)*, 2021, https://www.itu.int/en/ITU-T/extcoop/dcgi/Pages/default.aspx.
31. Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations*, June 2021, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
32. "An Introduction to GADI: the Global Architecture for Digital Identity", *Goode Intelligence*, 15 September 2020, https://www.good-id.org/en/articles/introduction-gadi-global-architecture-digital-identity/.
33. "What is self-sovereign Identity?", *Sovrin*, 6 December 2018, https://sovrin.org/faq/what-is-self-sovereign-identity.
34. "Decentralized Identifiers (DIDs) v1.0", *W3C*, 3 August 2021, www.w3.org/TR/2021/PR-did-core-20210803/.
35. "Hashed Timelock Contract (HTLC)", *Corporate Finance Institute*, 2021, https://corporatefinanceinstitute.com/resources/knowledge/other/hashed-timelock-contract-htlc/.
36. "Question 22: Multimedia aspects of distributed ledger technologies and e-services", *ITU*, 2021, https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/q22.aspx.
37. "F.751.0: Requirements for distributed ledger systems", *ITU*, 13 August 2020, https://www.itu.int/rec/T-REC-F.751.0-202008-I/en.
38. "F751.1: Assessment criteria for distributed ledger technologies", *ITU*, 13 August 2020, https://www.itu.int/rec/T-REC-F.751.1-202008-I/en.
39. "F.751.2: Reference framework for distributed ledger technologies", *ITU*, 13 August 2020, https://www.itu.int/rec/T-REC-F.751.2-202008-I/en.
40. "Pax Dollar", *Paxos*, https://www.paxos.com/usdp/.
41. "Gemini dollar", *Gemini*, https://www.gemini.com/dollar.
42. "CEF Telecom", *Innovation and Networks Executive Agency, European Commission*, https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom.
43. "Project Ubin: Central Bank Digital Money using Distributed Ledger Technology", *Monetary Authority of Singapore*, December 2020, www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.
44. "Project-Ubin/Ubin-Corda", *GitHub*, https://github.com/project-ubin/ubin-corda.
45. "digital currency initiative", mit media lab, 2021, https://dci.mit.edu/.
46. Minwalla, Cyrus, "Security of a CBDC", *Bank of Canada*, June 2020, https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/.
47. Wheeler, David, "Is Open Source Good for Security?", *Dwheeler.com*, https://dwheeler.com/secure-programs/Secure-Programs-HOWTO/open-source-security.html.
48. The Linux Foundation, *Annual Report 2020, Advancing open collaboration amid the challenges of a lifetime*, https://www.linuxfoundation.org/wp-content/uploads/2020-Linux-Foundation-Annual-Report_120520.pdf.
49. Smith, Jonathan, "Open, Programmable, Secure 5G (OPS-5G)", *DARPA*, https://www.darpa.mil/program/open-programmable-secure-5g#.
50. "The O-RAN Alliance, Open RAN Architecture, 5G, and Testing Solutions", *Viavi*, https://www.viavisolutions.com/en-us/solutions/service-providers/wireless/o-ran.

8/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

CBDC Technology Considerations

WHITE PAPER

NOVEMBER 2021

Images: Getty Images

Contents

Preface 199

1 CBDC policy goals and technical design considerations 200

1.1 Continued access to central bank money 201

1.2 Financial inclusion 202

1.3 Payment system efficiency (domestic or cross-border) 203

1.4 Payment system safety and resilience 204

1.5 Mitigation of currency substitution risk 206

1.6 Improvement of payments and banking competitiveness 206

1.7 Monetary policy implementation 207

1.8 Household fiscal transfers 208

2 Trade-offs for blockchain-based CBDC 209

2.1 The benefits and downsides of DLT-based CBDC 209

2.2 Examples of nodes in DLT-based CBDC 212

3 Cybersecurity considerations for CBDC systems 213

3.1 Credential theft and loss 213

3.2 Users with privileged roles 214

3.3 Denial of service 214

3.4 Double spending 214

3.5 Quantum computers 215

Conclusion 216

Endnotes 217

Preface

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

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

1. CBDC policy goals and technical design considerations

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

3. Cybersecurity considerations

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

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

1 CBDC policy goals and technical design considerations

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

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

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

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

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

– Strong cybersecurity, technical stability and resilience

– Sound technical governance

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

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

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

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

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

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

1.1 Continued access to central bank money

Background

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

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

Technology considerations

The following technology considerations stand out for this policy goal:

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

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

1.2 Financial inclusion

Background

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

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

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

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

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

Where does CBDC enable a capability or service that –

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

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

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

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

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

Technology considerations

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

Low cost

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

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

– Provide CBDC devices or applications for free

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

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

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

Accessibility and convenience

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

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

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

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

Additional resources on this topic

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

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

1.3 Payment system efficiency (domestic or cross-border)

Background

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

Domestic payments

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

Cross-border payments

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

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

Technology considerations

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

Cross-border payment efficiency

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

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

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

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

Additional technology considerations

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

Technical trade-offs for this policy goal

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

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

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

1.4 Payment system safety and resilience

Background

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

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

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

Technology considerations

The following technology considerations stand out for this policy goal:

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

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

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

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

1.5 Mitigation of currency substitution risk

Background

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

Technology considerations

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

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

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

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

1.6 Improvement of payments and banking competitiveness

Background

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

Technology considerations

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

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

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

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

1.7 Monetary policy implementation

Background

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

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

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

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

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

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

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

Technology considerations

The following technology considerations stand out for this policy goal:

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

1.8 Household fiscal transfers

Background

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

This activity has multiple challenges, including:

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

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

Technology considerations

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

2 Trade-offs for blockchain-based CBDC

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

2.1 The benefits and downsides of DLT-based CBDC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Examples of nodes in DLT-based CBDC

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

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

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

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

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

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

3 Cybersecurity considerations for CBDC systems

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

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

3.1 Credential theft and loss

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

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

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

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

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

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

3.2 Users with privileged roles

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

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

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

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

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

3.3 Denial of service

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

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

3.4 Double spending

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

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

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

3.5 Quantum computers

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

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

Conclusion

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

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

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

3. It presents some key cybersecurity vulnerabilities for CBDC

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

Endnotes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

28. See:

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

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

29. See:

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

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

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

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

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

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

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

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

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

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

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

39. See:

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

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

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

40. For further discussion on this topic, see:

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

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

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

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

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

44. See:

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

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

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

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

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

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

For further discussion, see:

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

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

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

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

    For further discussion, see:

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

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

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

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

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

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

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

    For further discussion, see:

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

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

    Related to higher security costs, see:

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

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

    See:

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

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

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

58. See:

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

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

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

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

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

See:

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

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

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

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

See:

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

For additional discussion on cost, see:

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

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

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

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

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

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

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

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

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

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

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

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

71. See:

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

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

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

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

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

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

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

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

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

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

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

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