7/8 Digital Currency Governance Consortium White Paper Series

WORLD ECONOMIC FORUM

Defining Interoperability

WHITE PAPER

NOVEMBER 2021

Images: Getty images

Contents

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

Preface

This 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

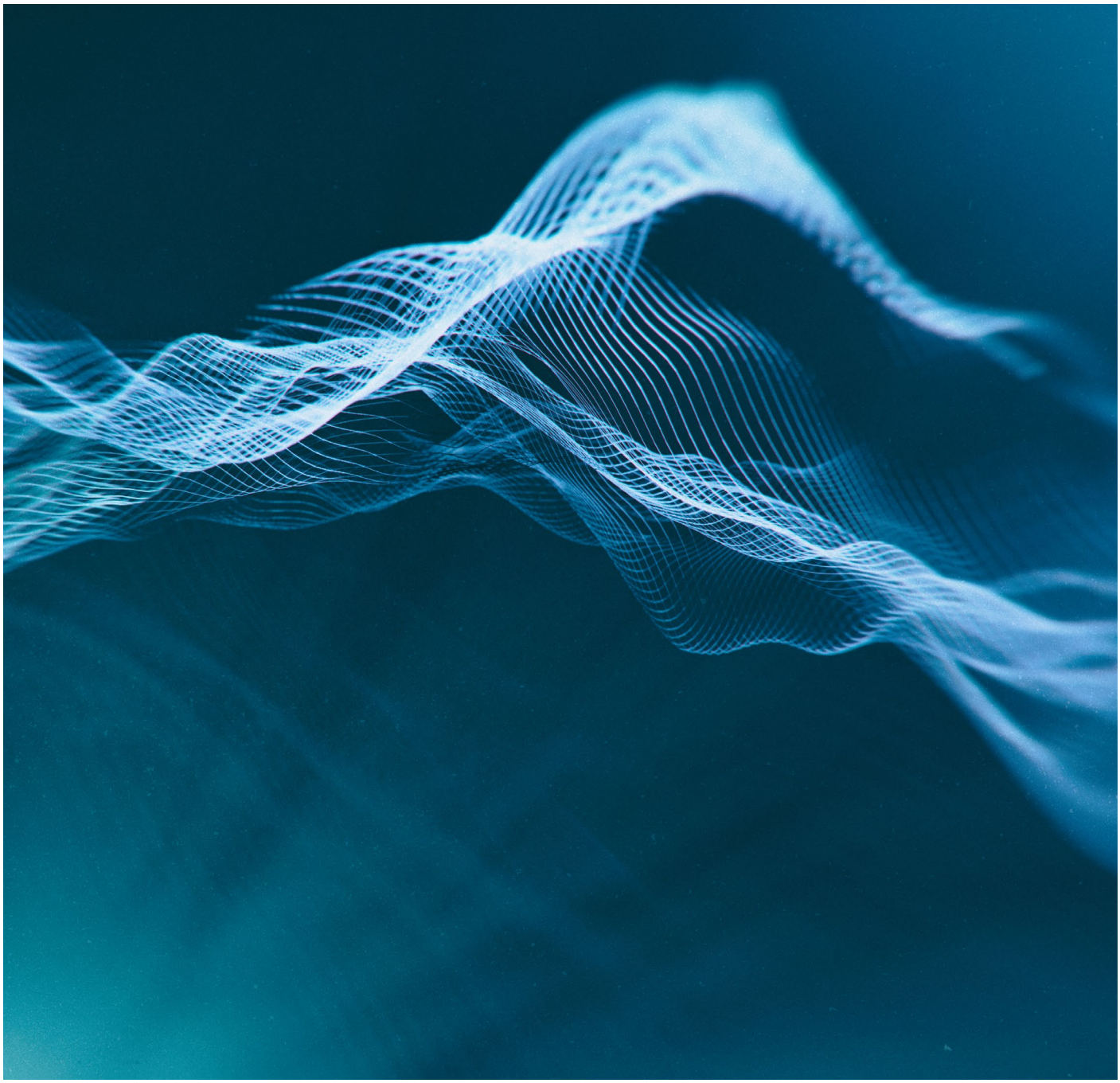
Even though our focus is on blockchain-based digital currency, some key design principles and outcomes for interoperability would be desirable for digital currency in general. These are summarized in the tables below.

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

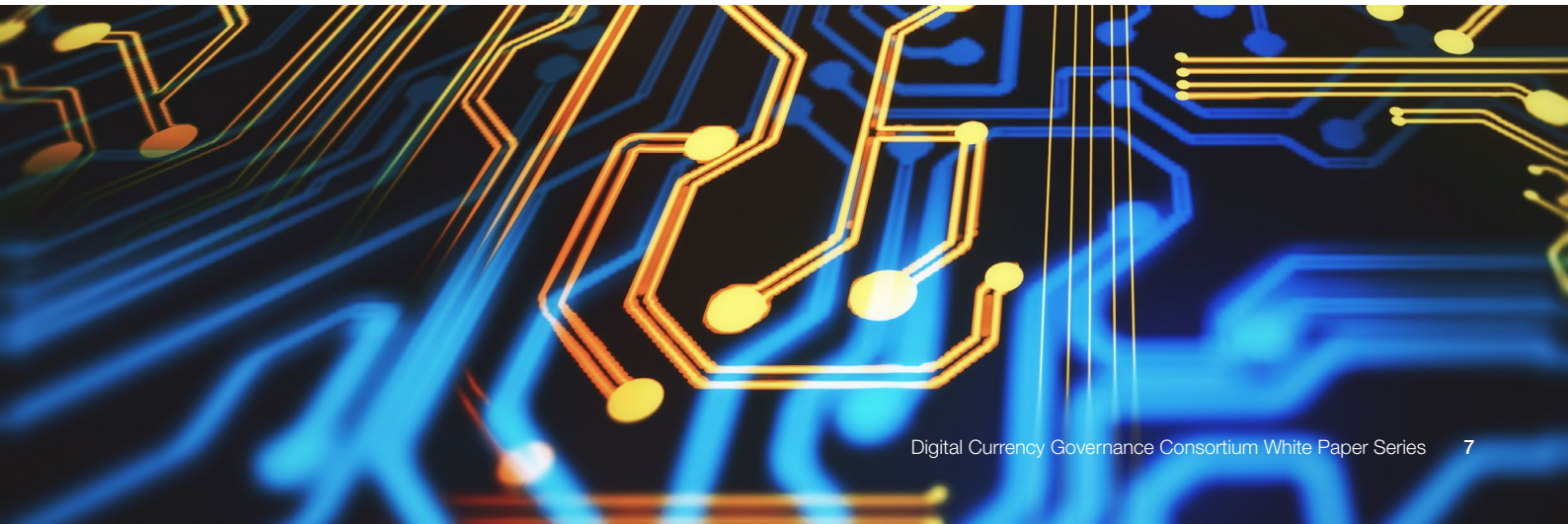
This section considers both retail and wholesale CBDC types. There are similarities and differences in the issues related to interoperability when comparing both CBDC options. In a domestic setting, it is important for CBDCs to be able to interact with other domestic payment systems.

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:

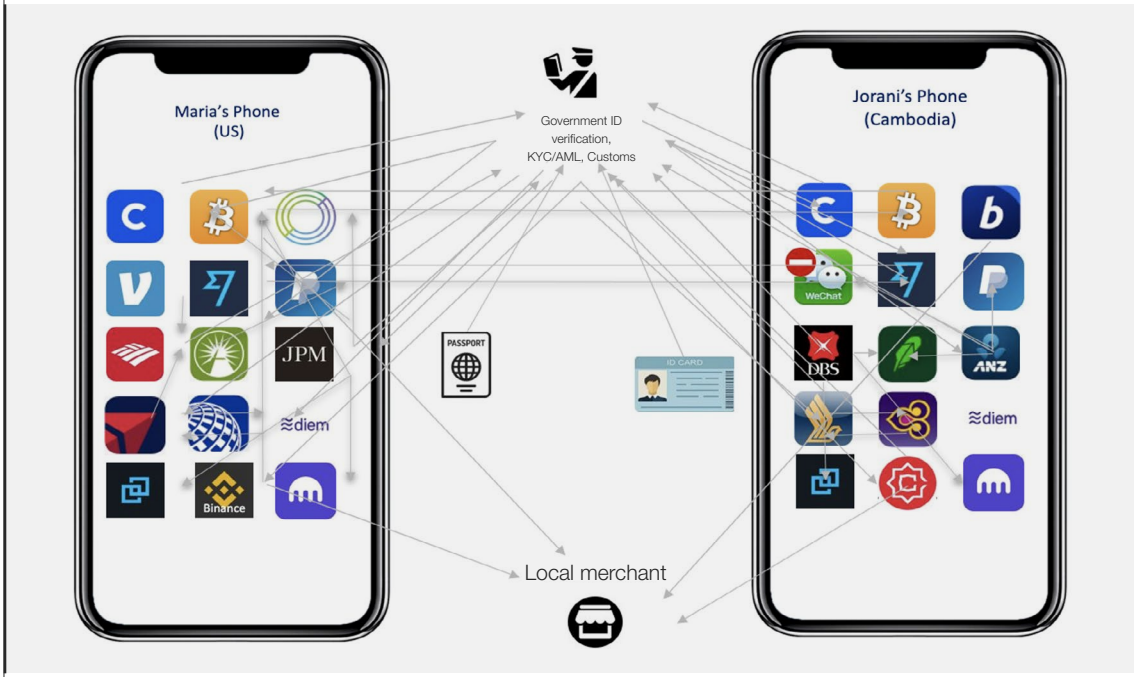
- ITU-T F.751.0 "Requirements for distributed ledger systems"[37]
- ITU-T F.751.1 "Assessment criteria for distributed ledger technologies"[38]
- ITU-T F.751.2 "Reference framework for distributed ledger technologies"[39]

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.

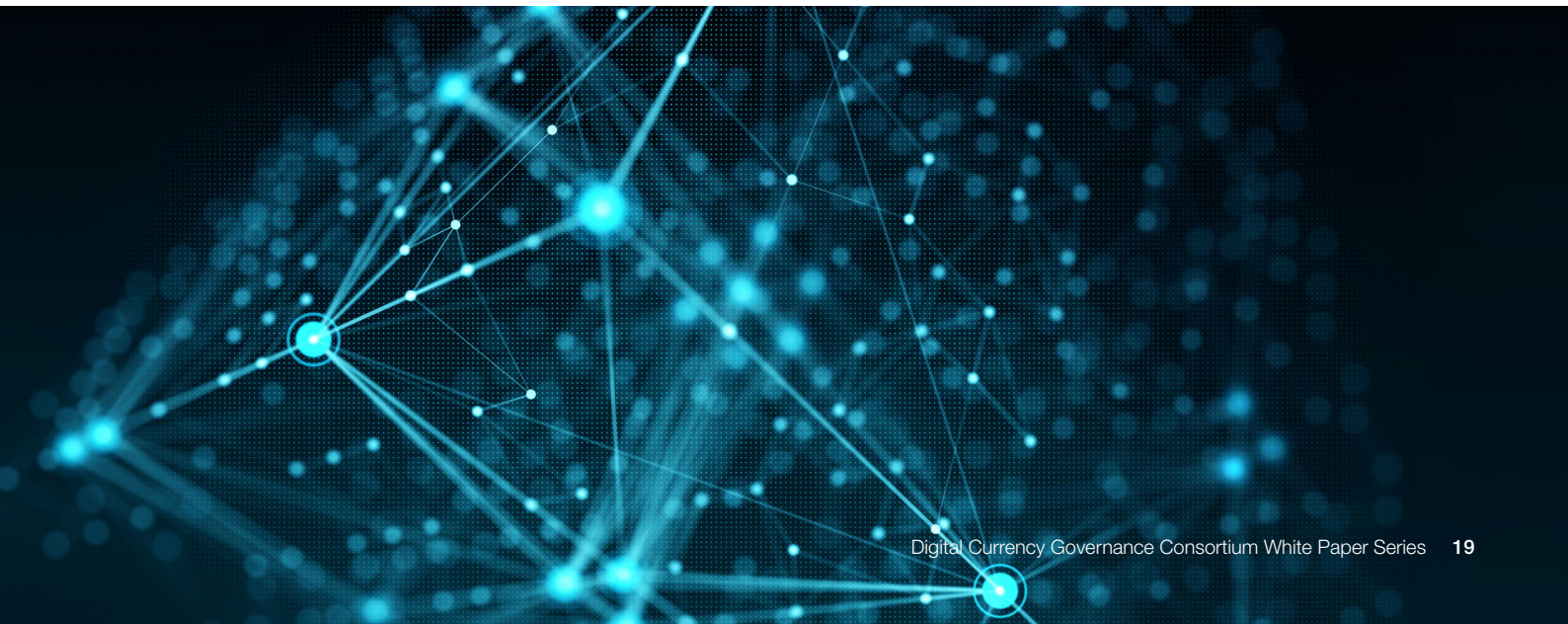
Co-creating technology in the open can serve to achieve the goals of interoperability: multiple requirements and perspectives can be incorporated, while the process can leverage the benefits of a vendor-neutral solution. Common needs are best served by building common solutions and the interoperability 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.

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