CBW3B
Powered by LACChain

Governance Analysis for CBWebWeb3

CBWeb3

Version 0.1– 06/05/2025

System/Service	RG-T4567 Phase I (Take-Off): A Regional Solution for Accelerating the Deployment of Central Bank Digital Currencies (Cbdc's) for Inclusion in Latin America and the Caribbean		
Status	DRAFT		
Approved by owner			
Authors	CV	Carolina Velasquez	LACChain: Blockchain Solutions Architect
Contributors	NY	Nayam Hanashiro	LACChain Coordinator of Strategic Projects.

CBW3B
Powered by LACChain

Version history

Version	Date	Author	Description
0.1	05/06/2025	CV	First Draft.

CBW3B
Powered by LACChain

Content

CBW3B
Powered by LACChain

Introduction

CBWEB3 is an IDB Lab project that seeks to enable a regional test-network (Test Net) for Latin America and the Caribbean that will allow for the issuance of CBDCs and the tokenization of financial assets, with a focus on cross-regional interoperability between central banks and financial institutions. The Test Net will build upon the technological capabilities and infrastructure of IDB Lab's initiative LACChain[1] and LACNet[2] the Alliance for the Development of the Blockchain Ecosystem in Latin America and the Caribbean, and capitalize on the Korean experience on the topic including Korean entities from the public, private and academic sectors such as the Bank of Korea (BOK), Korea Exchange (KRX), KAIST Network Security and Privacy Lab and Sungkyunkwan University (SKKU).

Central banks worldwide are experimenting with wholesale Central Bank Digital Currencies (CBDCs) to improve cross-border and interbank payments. A critical success factor is **governance** both the technical governance of the platforms (how networks are managed, secured, and updated) and the institutional governance (the legal agreements, decision-making processes, and participation rules among stakeholders). Effective governance provides the **"trust and shared control"** needed for multiple central banks to confidently share infrastructure[3]. Without robust governance, even the most advanced technology will fail to gain adoption by diverse jurisdictions.

This report examines governance mechanisms across major wholesale CBDC initiatives, focusing on four interoperability models identified in BIS and IMF studies[4]:

- **Single Shared Ledger** – participating countries use one common DLT[5] platform hosting multiple CBDCs.
- **Hub-and-Spoke** – domestic CBDC systems remain separate, connected via a central hub or platform.
- **Bilateral Links** – pairs of CBDC systems interlink directly without a central coordinator.
- **Compatibility Standards/Interlinking Frameworks** – systems adopt common standards or external bridging solutions to enable interoperability.

For each model, we analyze **technical governance** (node roles, consensus and software control, privacy/security configurations) and **institutional governance** (legal frameworks,

[1] LACChain is a global alliance for the development of the blockchain ecosystem in LAC by IDB Lab.
[2] LACNet is the third-party organization that orchestrates LACChain Networks. LACChain Networks are blockchain networks developed by the LACChain Alliance and orchestrated by LACNet.
[3] BIS Innovation Hub and central banks of Australia, Malaysia, Singapore and South Africa develop experimental multi-CBDC platform for international settlements.
[4] Options for access to and interoperability of CBDCs for cross-border payments. Report to the G20.
[5] Distributed Ledger Technology (DLT) is a decentralized database managed by multiple participants, commonly used in blockchain systems for maintaining a shared and immutable record of transactions.

rulemaking bodies, onboarding processes, dispute resolution). We draw on official documentation from the Bank for International Settlements (BIS), International Monetary Fund (IMF), and central bank pilot reports including Projects *DREX* (Brazil), *mBridge* (multi-country), *Dunbar*, *Icebreaker*, *Ubin*, and others to illustrate how these governance models are implemented in practice. We emphasize permissioned DLT platforms (e.g., Hyperledger Besu, Quorum) prevalent in these projects, as their design inherently ties into governance (through permissioned node access, smart contract[6] rule enforcement, etc.). Finally, we compare the models against BIS recommendations for cross-border CBDC design and discuss trade-offs in scalability, resilience, compliance, and inclusivity.

Single Shared Ledger Model

Under this model, multiple central banks and participants transact on a **single shared ledger** a common blockchain network hosting the digital currencies of each participating jurisdiction. All jurisdictions share one technical infrastructure, as seen in platforms like **Project mBridge** and **Project Dunbar**. The appeal of a single system is straightforward: by consolidating payments into one network, cross-currency transactions become direct and instantaneous, approaching the efficiency of domestic settlements. However, this model is also "*the most challenging to achieve*" because it requires a high degree of **coordination and trust** among sovereign entities. Governance is therefore central, it must ensure that no single party dominates, that each central bank retains control over its own currency, and that the system operates securely and fairly for all members.

Technical Governance in a Shared Ledger

On a shared multi-CBDC ledger, technical governance is often enforced through the blockchain's design and smart contract rules:

- **Node Roles and Consensus:** Each participating central bank typically operates one or more validator nodes on the network, so that validating power is distributed. For example, in Project mBridge's MVP, four founding central banks each deployed a validating node to run the **mBridge Ledger**[7]. Consensus algorithms (usually a form of proof-of-authority[8] or BFT consensus) are configured such that a quorum of validator nodes (controlled by different central banks) must approve transactions and blocks. This prevents any single authority from unilaterally altering the ledger and creates a built-in check and balance. In short, **the network's integrity is jointly maintained** by

[6] Smart contracts are self-executing contracts where the terms of the agreement are written into code and automatically executed when predefined conditions are met. In the context of CBDCs, they are used to automate transactions and enforce rules on the ledger.

[7] Project mBridge reached minimum viable product stage.

[8] Proof-of-Authority (PoA) is a consensus algorithm in blockchain systems where a set of trusted nodes (authorities) are designated to validate transactions, as opposed to using Proof-of-Work or Proof-of-Stake.

all members; a technological enforcement of shared control. (In Project Dunbar's prototypes, this principle was demonstrated on two different DLT platforms, R3 Corda and Partior/Quorum, both showing that no central bank alone could validate a transaction without others' consent.)

- **Permissioning and Identities:** Because the ledger is permissioned, an agreed list of entities is authorized to run nodes or transact. Central banks govern the onboarding of participants at the network level (e.g., deciding which commercial banks or PSPs can hold and use the CBDCs on the platform). Fine-grained permissions can be coded for instance, only a given central bank's node can invoke the function to issue or destroy its national CBDC token, ensuring each currency's **minting rights remain with the issuer**. Similarly, participants may be restricted to certain roles; Project Dunbar defined different tiers of bank access (some banks could be "selected" node hosts vs. others transacting through those nodes) to align with jurisdictional policies.

- **Protocol for Upgrades and Changes:** Software upgrades, parameter changes, or new features on the shared platform require collective agreement. Typically, a **technical committee** composed of members' IT leaders would propose and test updates, but implementation on the live network would need approval from the governance body (as discussed below) and a coordinated rollout to all validating nodes. This ensures no unilateral changes disrupt others. The network might even enforce version checks – if a node is not updated per the agreed schedule, it could be removed from the validator set to maintain protocol consistency.

- **Embedded Policy Rules:** Smart contracts on the shared ledger can encode policy decisions. For example, if participants agree on transaction limits or require certain checks, the smart contract handling transfers can include those constraints. In Project Dunbar, the design had to respect that **each jurisdiction's rules (e.g., FX[9] controls, AML requirements) should apply to their currency** even on the shared platform. Thus, the system included features like currency-specific transaction restrictions and the ability for each central bank to approve or reject transactions involving its CBDC if needed. These controls are part of technical governance; they are automated enforcement of institutional agreements.

- **Privacy and Data Segregation:** By default, a single ledger means all validators see all transactions, raising privacy concerns for banks and jurisdictions. Governance of a shared ledger often involves configuring privacy features. Enterprise DLTs like Hyperledger Besu support private transaction groups or use of cryptographic techniques (e.g., zero-knowledge proofs[10]) to hide transaction details from non-involved parties. Deciding on the privacy model is a governance question: for instance,

[9] Foreign Exchange (FX) refers to the trading of one currency for another, essential for international payments and settlements between central banks participating in CBDC projects.

[10] Zero-Knowledge Proofs (ZKPs) are cryptographic methods that allow one party to prove to another that they know a value without revealing the value itself. This is important for privacy in blockchain networks, ensuring transaction confidentiality.

do all central bank nodes see every transaction, or only those relevant to their currency or institutions? In current multi-CBDC pilots, a common approach is that **all transactions are visible to the central banks (for oversight/audit),** but commercial entities' transaction details can be shielded from other commercial. The network may integrate an off-chain enclave or utilize an overlay network for confidential data, which then becomes part of the governed infrastructure.

- **Security and Resilience:** Technically, the shared platform must meet critical infrastructure standards. Cybersecurity policies (patch management, node hardening, etc.) are agreed and followed by all node operators. Incident response is coordinated if a breach or fault occurs, procedures dictate how nodes can be isolated, or the network halted to protect the whole. For resilience, nodes are likely geo-distributed across jurisdictions so that the ledger doesn't rely on one data center. Some projects consider a **"federated operator" model** where an entity (or the group collectively) manages backup nodes or cloud instances to ensure uptime. All these measures are codified by the technical governance policy and require trust and verification among the members.

Institutional Governance in a Shared Ledger

Because a single ledger inherently blurs jurisdictional boundaries, institutional governance is perhaps most complex in this model. Key elements include:

- **Legal Structure and Agreements:** Participants usually formalize their cooperation via a **multilateral agreement or memorandum of understanding (MoU)**. This lays out the legal nature of the shared platform (e.g., is it a jointly owned utility, a series of contractual obligations, or simply a consortium network). In some cases, a new entity might be created to administer the platform; for example, the mBridge project formed a steering committee that developed a *bespoke governance and legal framework including a rulebook* for the platform[11]. That rulebook would cover the rights and obligations of each party. Project Dunbar likewise devoted significant effort to governance design, asking *"What governance arrangements could give countries sufficient comfort to share critical national infrastructure such as a payments system?"*. In its experiment, governance remained an open question to be refined, but the project demonstrated that a combination of legal agreements and technical controls can make a shared platform viable.

- **Governance Bodies:** Typically, a **Steering Committee or Governing Council** is established, comprising representatives of each member central bank (and possibly major banks or international institutions if they are stakeholders). This body makes high-level decisions: admission of new members, system upgrade roadmaps, setting of transaction fees or limits, etc. It operates on a consensus or voting basis defined in the rulebook. For day-to-day oversight, sub-committees might exist (e.g., an

[11] Project mBridge reached minimum viable product stage.

Operations Committee, a Compliance Committee). **Equal representation** is often a principle, governance structures are designed to ensure all stakeholders are fairly represented in decisions[12]. For example, no single country should be able to impose changes without others' agreement, reflecting the shared sovereignty of the platform.

- **Participant Onboarding and Roles:** Institutional governance defines who can participate in the platform and how. In wholesale contexts, this means which commercial banks or financial institutions from each jurisdiction are allowed to access the multi-CBDC ledger. Typically, **central banks retain authority to nominate or approve participants from their jurisdiction** (ensuring alignment with domestic policy)[13]. Project Dunbar segregated participants into roles: central banks (issuers/regulators), "selected" commercial banks (large banks hosting nodes with broader access), "other" commercial banks (with more limited privileges via selected banks), etc., each with defined onboarding criteria. The governance framework must spell out these categories and the process for onboarding (and offboarding) members. It also covers cross-border participation: e.g., can a bank from Country A directly hold or transact in Country B's CBDC on the platform? In Dunbar's prototype, the answer was yes, authorized banks could directly hold multiple CBDCs, but subject to each central bank's policies and the shared rules. Thus, a foreign bank might need approval from the issuer's central bank (perhaps via an access tier or licensing).

- **Jurisdictional Autonomy and Policy Application:** A crucial governance aspect is preserving each central bank's policy prerogatives. Even on a common network, **each central bank must retain control over its currency and regulatory requirements**. Institutional arrangements often formalize this by stating, for instance, that each CBDC on the platform is a liability solely of the issuing central bank, and that issuer has the final say on transactions involving its CBDC (within agreed constraints to prevent arbitrary refusal). Moreover, compliance with local laws (such as AML/CFT checks or sanctions) is maintained: banks from each jurisdiction are still bound by their national regulators. The shared platform's rulebook might require participants to certify compliance with their home regulations and include mechanisms for information-sharing or joint audits to support that compliance in a cross-border context. In other words, the platform doesn't override local laws, it coordinates them. This was affirmed in Dunbar's findings: *"any such arrangement should be subject to governance deemed appropriate by central bank participants, including allowing them to retain control of the application of rules on a jurisdictional and currency level."*.

- **Dispute Resolution and Liability:** With multiple independent authorities operating together, disagreements or incidents are inevitable (e.g., a disputed transaction, an outage on one node, or a compliance breach). The governance framework must define how disputes are handled. Often a tiered approach is used: operational issues are resolved by the Operations Committee or by central banks involved consultatively;

[12] Project Dunbar. International settlements using multi-CBDCs.
[13] Project Dunbar. International settlements using multi-CBDCs.

major disputes can be escalated to the Steering Committee. In extreme cases, an arbitration clause might be included in the legal agreement, possibly referring issues to an external arbitrator or court if central banks cannot agree. Liability for losses (say, due to a technical failure) is a sensitive topic typically, central banks are reluctant to indemnify each other. The rulebook might state that each party bears its own risks or that the platform operator (if a separate entity) has limited liability. Insurance or guarantee arrangements could be considered if significant financial exposure exists on the shared ledger. Clarity on these points is vital for trust.

- **Operational Oversight and Audits:** Institutional governance may set up audit rights and monitoring. Central banks could conduct joint audits of the platform's operations or require independent assurance reports on the system's security and performance. For example, if a common entity runs aspects of the network (perhaps a secretariat or technical operator coordinating between nodes), that entity would periodically report to all central banks. Additionally, any rule violations by participants (e.g., a bank misusing the platform) would be addressed through predefined sanctions (ranging from warnings to suspension of access), enforced by the collective decision of the governing body.

Challenges and Trade-offs Single Ledger

A common platform maximizes efficiency – *Project Dunbar showed that a shared multi-CBDC network can enable direct cross-currency settlements, reducing reliance on intermediaries*. It can also simplify liquidity management (consolidating reserves on one platform) and enable innovative automation via smart contracts (for instance, cross-border delivery-vs-payment for securities). However, these benefits come with significant governance challenges:

- **Scalability vs. Decentralization:** Technically, a single ledger can face scalability limits as participants grow. Accommodating many currencies and banks on one chain may strain throughput and data management. To scale, the governance might need to permit upgrades (sharding, layer-2 networks, etc.), which requires unanimous agreement. There is a tension between broad inclusion (many members) and the efficiency of decision-making. A larger committee of central banks could slow down governance processes, making it hard to adapt quickly.

- **Operational Resilience:** The single ledger is a **common point of failure** if not properly managed. An outage or cyber-attack on the platform could impact multiple countries' payment operations simultaneously; a systemic risk. Mitigating this requires joint investments in redundancy and robust security. It also means that **trust is mutual**: each member must trust that others are securing their nodes to a high standard, since a weak link could threaten the whole. The governance framework likely mandates minimum security standards and information-sharing on incidents. Nonetheless, some central banks may be uncomfortable tying their core payments so directly to another's operational rigor. This is partly why Dunbar was a pilot – proving this can be handled but acknowledging more work is needed on risk management.

- **Compliance and Legal Complexity:** Hosting multiple CBDCs on one platform raises legal questions: Which jurisdiction's law governs the platform itself? How are differences in data protection, or in insolvency treatment of CBDC, reconciled? The governance solution might be to treat the platform as *jointly governed under a bespoke legal regime* (perhaps through a contract under neutral law). But until international legal frameworks catch up, this is complex. Moreover, anti-money laundering (AML) compliance has to be collective, if a suspicious transaction routes from Bank A in country X to Bank B in country Y on a shared ledger, both sides' authorities may need to coordinate on investigation. The platform's rulebook can require information exchange but executing that seamlessly is challenging. **No single model code exists yet** for such multi-sovereign payment systems, meaning each project must negotiate its own legal governance structure; a time-consuming process.

- **Sovereignty and Inclusivity:** Politically, a fully unified system may be seen as compromising monetary sovereignty. Every central bank will ask: do the benefits outweigh the loss of full control over infrastructure? The Dunbar report noted this as a key question: how to give countries "sufficient comfort" to share critical infrastructure. Strong governance mechanisms are the answer, by giving each country veto rights or clearly delineated control over its currency. Even so, some may opt out. This suggests that while a single system could be extremely efficient for those who join, it might end up limited to a coalition of the willing. Others might prefer a looser model initially (like hub-and-spoke or just compatibility). Thus, inclusivity could suffer if the world fragments into a few separate single-ledger groups rather than one global platform.

In summary, the single shared ledger model is **technically viable**, prototypes like mBridge and Dunbar proved that financial institutions can transact directly using multiple CBDCs on one network. They also showed that governance tools (rulebooks, permissioning, and smart contract controls) can address trust issues and allow **"countries [to] retain control"** at the jurisdiction level. The remaining challenges revolve around scaling this model beyond pilots: crafting legal agreements for production, ensuring resilience, and convincing a broad set of central banks to sign on. The model embodies a trade-off: maximum integration for maximum efficiency, versus the complexity of collective management of what used to be national infrastructure.

Hub-and-Spoke Model

The hub-and-spoke model aims to achieve interoperability while preserving independent domestic systems. In this model, each central bank runs its own CBDC ledger or payment system (the "spokes"), and a **central hub** connects them to facilitate cross-border transactions. The hub typically does not issue currency itself; rather, it **links or mediates transactions** between CBDC systems. This approach was explored in **Project Icebreaker** which connected three prototype retail CBDC systems via a BIS-run hub[14] – and is analogous

[14] Project Icebreaker concludes experiment for a new architecture for cross-border retail CBDCs.

to the **"Nexus"** scheme proposed by the BIS for linking national payment systems[15]. The IMF's vision of a global or regional cross-border payment platform also aligns with a hub concept.

The hub-and-spoke model can be seen as a form of "interlinking" in BIS terminology: a common platform (hub) **connects multiple separate CBDC systems**, as an alternative to a single shared system. Each jurisdiction maintains its autonomy over its ledger, and the hub provides the *interoperability layer*. This has two key advantages: (1) Each system only needs **one connection (to the hub)** to reach all others, rather than many point-to-point links, simplifying integration; (2) Domestic ledgers can be designed and governed primarily by the national central bank, with the hub handling only what's necessary for cross-border exchange. Essentially, it minimizes the required coordination on the core infrastructure, focusing governance on the linking mechanism.

Technical Governance of Hub-and-Spoke Model

In a hub-and-spoke architecture, technical governance is split between the hub and the local (spoke) systems:

- **Hub Functions and Design:** The hub is usually a middleware or message routing system, possibly itself a limited DLT or a conventional application. In Project Icebreaker, the hub's role was to route payment messages between countries and to coordinate foreign exchange (FX) rates by collecting bids from competing providers. Importantly, *the Icebreaker hub did not hold any CBDC funds*; each cross-border payment was broken into two domestic payments (payer to FX provider in country A, FX provider to payee in country B), so the CBDCs never left their national ledgers. The hub needed only to pass along the minimal data to link these two halves and ensure the trade was synchronized. In this principle **the hub is an information coordinator, not a settlement entity** strongly influences governance. It means the hub can be simpler and lower risk (not a bank or custodian), focusing on reliability of message delivery and perhaps an algorithm to match/choose FX rates.

- **Node Roles and Connectivity:** Each participating CBDC system integrates with the hub via a **gateway** or adapter. Technically, this might be a server or node that translates between the domestic ledger's API and the hub's protocol. For example, if one country's CBDC runs on Corda and another's on Quorum, a gateway at each end can interface with its ledger and send/receive standardized messages through the hub (the approach taken by the recent SWIFT CBDC interoperability experiments)[16]. These gateways must be developed according to common specifications so that all spokes "speak" to the hub in a unified way. Part of technical governance is maintaining these specifications (message formats, encryption standards, etc.). In many designs, the hub

[15] Project Icebreaker. Breaking new paths in crossborder retail CBDC payments.
[16] Connecting digital islands: CBDCs – Results of SWIFT experiments interlinking CBDC networks and existing payments systems to achieve global interoperability.

operates on a **request-response model**: a bank in country A requests a payment to country B's system via the hub; the hub finds a corresponding liquidity provider offer and instructs payment in country B. Because each domestic system might have different technology, the hub likely uses a technology-neutral approach (e.g., REST APIs or ISO 20022[17] XML/JSON messages) to interface. That makes it **agnostic to the underlying DLT** – indeed, Icebreaker demonstrated integration of three different DLT platforms through minimal common standards.

- **Consensus and Data Handling:** The hub itself may not need a complex consensus mechanism if it's not a ledger, but it still must be highly reliable. It could be centralized (run on redundant servers by the hosting entity) or distributed (run as a small consortium network by a few central banks or international organizations). If distributed, the hub might run a simple consensus among its nodes to agree on message ordering and FX quote selection. Since the hub's operations are relatively straightforward (essentially a **router and matcher**), the consensus can be lightweight. Project Icebreaker's report indicates the hub only acts on FX provider data to pick the best rate, and otherwise *"only routes payment messages and does not act upon them"*, minimizing its involvement[18]. This design choice – limiting the hub's intelligence – simplifies technical governance: the hub doesn't need to interpret or validate domestic compliance rules; it just moves data and coordinates timing.

- **Atomicity and Settlement Mechanism:** A critical technical governance aspect is how the hub ensures that a payment in one system only occurs if the corresponding payment in the other system occurs i.e., no half-completed transfers. This can be achieved via various interlinked payment protocols. One approach is **coordinated conditional payments**: for example, country A's system could escrow the CBDC payment until a confirmation from country B's system (via the hub) is received, then both legs finalize (similar to a Payment-versus-Payment lock). Icebreaker effectively did this by using the hub to orchestrate a form of atomic settlement: if no valid FX quote was found or the second leg failed, the first leg would not execute[19]. The technical governance must define this process clearly whether through a custom protocol or using something like **Hashed Time-Locked Contracts (HTLC)** (which were used in Jasper-Ubin's bilateral experiment[20] and could also be applied in a hub scenario). Ensuring atomicity typically requires synchronized clocks and a common understanding of timeouts across systems, which the hub can manage.

- **Security and Reliability of the Hub:** Since the hub becomes a critical piece for cross-border transactions, its security is paramount. Technical governance will set requirements for the hub's operation: encryption of all data in transit (likely using

[17] ISO 20022 is an international messaging standard used in financial services for exchanging electronic data. It is widely adopted for payment messages, including those for cross-border transfers.
[18] Project Icebreaker. Breaking new paths in crossborder retail CBDC payments.
[19] Project Icebreaker concludes experiment for a new architecture for cross-border retail CBDCs.
[20] Jasper–Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies.

established PKI or TLS standards), authentication of all connections (only authorized gateways can send to the hub), and perhaps transaction signing so that the hub cannot falsify instructions. Moreover, because the hub could be a **single point of failure** for cross-border linkages, redundancy is needed[21]. This could mean running mirrored hub infrastructure in multiple geographic locations or even having multiple hubs that can take over if one fails (though that introduces additional complexity of keeping hubs in sync). At minimum, robust failover and disaster recovery plans are part of the hub's technical governance. Unlike a single shared ledger, a hub failure doesn't affect domestic systems' internal function, but it would halt new cross-border transactions. Participants will demand extremely high availability.

- **Standards and Interoperability Maintenance:** Over time, the hub and spoke interfaces may need updates (for example, adding support for a new message type or upgrading cryptographic algorithms). A technical governance process is needed to roll out changes in a coordinated way so that all spokes remain compatible. This often involves versioning of APIs and backward compatibility support while members transition. It's likely that changes to the hub protocol must be agreed upon by all or a majority of participants (institutional governance covers that), but technically, the hub operator would implement and publish the new standards, and each domestic platform team would adapt their gateway. Ensuring continued **interoperability** is an ongoing governance task akin to how SWIFT maintains message standards yearly and banks must update their systems accordingly.

Institutional Governance of Hub-and-Spoke.

Institutional arrangements in a hub-and-spoke model focus on the governance of the hub and the **contracts linking each jurisdiction to the hub**. Key considerations:

- **Hub Operator and Ownership:** A fundamental question is: who operates the hub? Often, the vision is that an international neutral party does so (e.g., BIS for Icebreaker, or potentially a new entity under multilateral governance). In Icebreaker, the BIS Innovation Hub acted as the operator during the experiment. For production, one could imagine LACChain/LACNet or even a coalition of central banks jointly operating it through CEMLA[22]. The governance model could range from **a centralized service** (operated by one entity with advisory input from members) to **a jointly owned utility** (like SWIFT's cooperative model where central banks or commercial banks collectively own and govern it). The choice will shape the legal structure: it could be an extension of an existing institution (leveraging BIS's legal infrastructure and immunity, for instance) or a new company/consortium with a board of directors from member banks.

[21] Project Icebreaker: Breaking new paths in crossborder retail CBDC payments.

[22] CEMLA is the Center for Latin American Monetary Studies, a regional body focused on promoting the development of monetary and financial systems in Latin America. It may play a role in governance models for CBDC interoperability in the region.

- **Participation and Rulemaking:** Each participating central bank likely signs a **participation agreement** or MoU with the hub operator. This document would set out each party's responsibilities. For central banks: to ensure their domestic system follows the protocols, to manage their end of FX or liquidity provision if relevant, and perhaps to pay a share of the hub's costs. For the hub operator: to provide agreed services (routing, FX matching), maintain confidentiality, and follow any rules set by participants. A **Hub Steering Committee** may be established where all participating central banks have a seat, guiding the evolution of the hub. However, governance here can be lighter than in a single shared ledger: since domestic ledgers remain under national control, the steering committee's scope is limited to the hub's functionality and the terms of cross-border engagement. Many policy matters (like who can access each CBDC) remain national decisions, the hub just connects systems once those decisions are made locally.

- **FX Providers and Third Parties:** An interesting institutional element in hub models is the inclusion of **third-party service providers** such as foreign exchange dealers. Icebreaker's model introduced competitive FX providers that submit quotes to the hub for each cross-currency payment. Governance must define how these entities participate: e.g., criteria to qualify as an FX provider on the hub (must be licensed in at least one participating jurisdiction, meet capital requirements, etc.), and rules they must follow (quoting behavior, no collusion, etc.). The hub operator might vet and onboard these providers under guidance from the central banks. There may also be a need for an oversight mechanism for them – perhaps central banks collectively monitor market activity on the hub to ensure it remains fair. The upside is this adds a market-driven element (improving rates for users), but it introduces non-central bank actors into the governance mix.

- **Transaction Governance and Liability:** The hub-and-spoke setup simplifies some legal issues each leg of a cross-border transaction is essentially domestic. So, each central bank continues to apply its jurisdiction's laws to its leg. The hub never takes custody of funds, which avoids questions of the hub needing a banking license or being a counterparty. However, there is still the need for a legal framework to handle the *cross-border link*. Suppose a payment fails because the hub malfunctioned or gave bad info – who is liable to the transacting parties? Likely, the hub operator will have limited liability by contract, given it's not moving money itself. The banks involved in the payment will probably bear or mutually reconcile any loss (similar to correspondent banking today where errors are resolved bank-to-bank). Nonetheless, **dispute resolution** clauses are needed for cases where one central bank's system says, "we paid" and the other says "we never received". The hub's transaction logs (which should record message timestamps and confirmations) would be the arbiter of truth. The governance framework might establish that if the hub log shows a fault, the operator compensates for certain costs, but if a domestic system failed to execute after receiving a proper instruction, that central bank (or its commercial banks) bear the consequence. These details require careful agreement to prevent finger-pointing in a live scenario.

- **Data Governance and Privacy:** Because the hub routes transaction data, participants must trust the hub operator with potentially sensitive information (even if limited). For retail payments (Icebreaker's case), personal data ideally does not travel to the hub and indeed the project ensured the hub only saw anonymized payment amounts and technical addresses, not user identities. For wholesale, data is less personal, but still could be market-sensitive (e.g., large interbank transfers). Governance should enforce that the hub *only* uses data for the intended purpose (e.g., matching FX) and does not retain or misuse it. Audits or oversight of the hub's data handling might be part of the agreement, possibly with central banks having the right to inspect the hub systems. Also, if the hub is global, data protection laws come into play – data is flowing between jurisdictions. A common approach is to specify that each participant is responsible for ensuring it can lawfully send data to the hub (perhaps treating it like an international data transfer under existing payment messaging rules).

- **Onboarding New Spokes:** One strength of hub-and-spoke is easier expansion. The governance model should outline how a new country can join. This likely involves approval by existing members (to ensure the hub can technically support the new system and that the newcomer will abide by the rules). Once approved, the new central bank signs the standard participation agreement, sets up the gateway, and joins the steering committee. Contrast this with a single ledger, where adding a new member might be more intrusive (they need to run a node and integrate into consensus, etc.). The hub model is **modular**, so inclusivity is high any system that meets the technical requirements can plug in. This is crucial for global adoption: it means even if not all central banks coordinate at once, smaller groups can interlink, and others can opt in overtime. The IMF has suggested that such models could allow regional hubs that later interconnect, building toward global reach gradually.

Challenges and Trade-offs – Hub-and-Spoke.

The hub model offers a **middle ground** between isolated national systems and a single unified system. It can deliver many of the benefits of interoperability while keeping national systems decoupled. Still, it has its own set of trade-offs:

- **Efficiency vs. Complexity:** A hub introduces one extra step in transactions (two domestic payments instead of a single on-platform transfer). However, this is still far leaner than today's correspondent chains, and Icebreaker showed transactions can complete "within seconds" even with the hub mediation. The FX conversion becomes an added component efficiency depends on competition among FX providers and sufficient liquidity. Governance must ensure the hub mechanism (like the FX auction) is efficient. If it is not well-designed, a hub could add latency or cost. Technically, though, the overhead is small (message passing). The complexity lies more in the business process than the technology.

- **Single Point of Failure and Risk Concentration:** As noted, the hub is a critical node. If it fails, **all cross-border links through it are cut off**. This is a concentration of

operational risk. Mitigations like robust architecture and possibly having a backup hub operator are needed. There is also some concentration on decision-making: if the hub operator (say BIS) sets certain standards or fees, participants need to agree or negotiate through governance channels. Some countries might worry about over-reliance on an external hub. One possible remedy is a **federated hub** e.g., multiple regional hubs that interoperate, or a hub that is itself run by multiple institutions together. Those variants complicate governance but distribute trust. The straightforward single-hub model assumes trust in the entity running it. In practice, central banks already trust entities like BIS and SWIFT for critical roles; extending that trust to a CBDC hub is plausible but would require clear accountability and oversight arrangements.

- **Legal and Regulatory Alignment:** While simpler than a single ledger, hub-and-spoke still needs participating jurisdictions to align on some basic principles. For example, there needs to be legal recognition that a payment made via two domestic systems (with an FX trade in between) constitutes a valid discharge of cross-border obligation. This is akin to the legal underpinnings of correspondent banking, but now the hub coordination brings an added wrinkle: what law governs the FX contract? Possibly the hub's terms specify that (e.g., governed by English law or some neutral choice). Additionally, each jurisdiction must be comfortable allowing its CBDC to be used by foreign intermediaries (the FX providers likely straddle jurisdictions). Some regulatory adjustments might be needed to authorize non-resident financial institutions to open accounts or use APIs in the domestic CBDC system, if not already allowed. **However, local autonomy is largely preserved,** each central bank can impose its own participation criteria and compliance checks for any transaction going through its system. As BIS noted, this model "might be easier in the short run" since it lets each country pursue its CBDC design independently, then connect later[23].

- **Scalability and Network Effects:** A major strength of the hub model is scalability in terms of connectivity. The number of connections grows linearly with the number of systems (n systems = n connections to hub) instead of exponentially. This makes it far more feasible to link, say, 50 countries. It avoids the **"spaghetti junction"** of bilateral links. In terms of throughput, the hub has to handle aggregate traffic, which could be heavy if dozens of countries do high-volume trades. But since the hub deals mostly in lightweight messages (not value storage), it can likely scale with modern cloud infrastructure. The governance must plan for scaling: e.g., adding processing power or spinning up multiple hub instances that share load. Another factor is that the hub model can **foster competition and innovation** in services. Because the hub is modular, new features (like additional currency swap services or liquidity management tools) could be built on top without altering the core ledgers. The governance would need to decide what additional services the hub might provide versus leaving it minimal.

[23] BIS G20 report explores practical lessons from CBDC projects.

- **Inclusivity vs. Control:** This model is arguably the most **inclusive** in that it imposes minimal demands on joining members. Each central bank keeps "almost full autonomy in designing a domestic CBDC" and then can connect internationally when ready. This was highlighted as a unique strength of Icebreaker it allows divergent national designs but still enables cross-border use. For regions like Latin America & Caribbean, a hub approach could allow each country to roll out CBDC at its own pace and tech, then connect to a regional hub for interoperability. The trade-off is that because domestic systems differ, the hub can only provide a lowest-common-denominator interface. Some richer features of one CBDC system might not transmit over the hub if others can't support them. For instance, if one system supports highly granular transaction metadata and another doesn't, the hub standard might ignore that metadata for consistency. Thus, interoperability may be **partial**. Governance bodies might try to harmonize certain features across systems over time to improve this.

In summary, the hub-and-spoke model provides a **pragmatic balance**. It reduces the governance burden by localizing most decisions and requiring only a focused set of agreements for the hub's operation. Empirical results are promising: *Project Icebreaker concluded that a hub-and-spoke model can "reduce settlement and counterparty risk" (through coordinated PvP in central bank money) and achieve fast, cost-effective transfers*[24]. It also showed that integration requirements for domestic systems can be kept minimal, aiding scalability. The key challenges revolve around making the hub itself ultra-reliable and ensuring that its limited scope is still sufficient to meet user needs (e.g., providing a mechanism for competitive FX so users get good rates). With proper governance likely through a collective oversight of the hub by participating central banks, this model can significantly enhance cross-border payments without demanding countries to surrender control of their own CBDC infrastructure. Indeed, many observers see the hub approach as a practical stepping stone: it can be implemented with fewer hurdles, and if successful, could either expand or inform future more integrated systems.

Bilateral Links Model

The bilateral links model connects CBDC systems **pairwise**, without any central hub or common platform. In this scenario, two central banks establish a direct interoperability channel between their CBDC infrastructures, enabling cross-border payments for that currency pair. This approach can be considered a specific case of the "interlinking" models defined by BIS – essentially the *"bilateral link"* option (as opposed to single access point or hub). It is the digital age analogue of correspondent banking relations, but with the goal of using technology to automate trust between two ledgers.

In practice, bilateral CBDC links have been tested on a limited basis. A notable example is the **Jasper–Ubin experiment** (2019) between the Bank of Canada and Monetary Authority of Singapore, which connected their prototype DLT networks to do cross-border atomic

[24] Project Icebreaker concludes experiment for a new architecture for cross-border retail CBDCs.

transactions[25]. Another is **Project Aber** (2019) between Saudi Arabia and UAE, where the two central banks actually created a single dual-issued digital currency on a shared ledger for their corridor[26]; a slightly different flavor (more like a mini shared system for two, which can be seen as an extreme form of bilateral arrangement). Generally, a bilateral link could also be implemented through a **gateway node** that links two systems (for example, if one country runs on Corda and another on Quorum, they might set up a special node that is a member of both networks to transfer assets between them).

Technical Governance of Bilateral Links

In a bilateral link, technical governance is highly specific to the two systems involved:

- **Interoperability Mechanism:** The two ledgers must have a protocol for atomic exchange of assets across them. Jasper-Ubin accomplished this using **Hashed Time-Locked Contracts (HTLC)**, which allowed transactions on two separate DLTs to be synchronized without a trusted intermediary[27]. In simplified terms, a cryptographic hash lock was used so that Bank of Canada's network would release funds if and only if Singapore's network did the same, using a shared secret and time-out to rollback if the second leg didn't happen. This *"trust in the technical solution rather than in a third party"* was a breakthrough. The governance of this mechanism involves agreeing on the parameters (hash functions, time lock durations, etc.) and implementing compatible smart contracts on each ledger. Both sides must maintain those contracts and ensure they remain secure. If the two systems are based on different technology, additional work is needed to bridge them (e.g., an adaptor that can listen to events on one chain and trigger actions on the other). Technical governance here is essentially **joint software development**: Canada and Singapore had to collaborate to write and test the HTLC contracts that worked on Quorum (in Singapore) and Corda (in Canada)[28]. This included ensuring each platform's consensus and finality properties align with the atomic swap needs.

- **Node and Infrastructure Setup:** In some bilateral arrangements, the central banks might run a **notary or observer node** on each other's systems to facilitate monitoring of the link. Or they might establish a new intermediate node that interfaces with both. Technical governance decisions include where this bridging code runs and who operates it. In a pure HTLC scenario, no third node is needed; the logic is in each ledger, and they communicate through public cryptographic triggers (one side posts a hash, the other side uses it, etc.). That is elegant, but in practice, it may require a communication channel to transmit the secret when the time comes. Jasper-Ubin possibly used an out-of-band channel or a simple API for one contract to inform the

[25] Options for access to and interoperability of CBDCs for cross-border payments.
[26] Project Aber – Reimagining domestic and cross border settlement.
[27] Jasper–Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies.
[28] How cross-border payments are evolving.

other. If such a channel exists, it needs to be secured and agreed upon. Generally, each side will maintain its own infrastructure and just expose an interface or contract endpoint to the other. So, governance is about defining those interfaces clearly and making sure they are robust to errors.

- **Upgrades and Compatibility:** Since only two parties are involved, coordinating upgrades is simpler than in multi-party networks but it still requires explicit agreement. If one central bank wants to change something in its CBDC system that affects the link (say, change the way UTXOs are managed, or update the smart contract language), it must notify the other and possibly jointly update the bridging protocol. A governance protocol could be as simple as a clause: “each side will not modify the interoperability contract or related settings without prior consultation and mutual agreement”. They might schedule joint testing whenever an upgrade is planned.

- **Performance and Scalability:** A bilateral link might be very high capacity if, for example, two major economies link their CBDCs and large volumes flow through. The technical governance would need to address performance tuning of the link e.g., if using HTLC, ensuring that time locks are set such that network latency doesn’t cause unnecessary expiries. If the connection is too slow or unreliable, it could create backlogs. Monitoring systems to watch the success/failure rates of cross-ledger transactions would be put in place by both parties’ technical teams. Essentially, each pair takes on the *integration engineering* that a hub would otherwise centralize for many.

- **Security Measures:** With direct links, each system is exposing an entry point to an external party. That heightens the need for security governance. Each central bank will carefully firewall what the other can do, for instance, the Singapore ledger will only accept incoming instructions or proofs from the Canadian side that meet the agreed protocol, and vice versa. There is no *general* access for the foreign system. If using a cryptographic protocol like HTLC, compromise would require breaking the crypto or one ledger’s integrity, which is unlikely if both are secure. However, if an attacker did compromise one ledger (or got hold of the hash preimage in an HTLC flow), they could potentially steal funds from the other ledger; thus, trust is mutual in securing their environments. Auditing each other’s security might be part of the arrangement (or at least sharing audit results). Also, revocation: if a security issue is discovered, how to pause the link? They might build a **“kill switch”** where either side can suspend cross-ledger transactions temporarily. This is a technical governance safety feature to prevent misuse during issues.

- **Privacy:** In a two-party link, data exchange is limited. Likely, only transaction hashes, amounts, and maybe pseudonymous addresses are exchanged as needed to coordinate the transfer. Each ledger keeps its transaction details internally. Thus, privacy is easier to manage – it’s one-to-one data sharing under an NDA or MoU. Technically, they ensure no more data is exposed than necessary. For example, the Singapore side doesn’t need to know the identities behind the Canadian transaction; it

just needs cryptographic proof that funds were locked for the right amount. Privacy considerations are therefore mostly organizational (the central banks might learn some aggregate info about each other's flows, but those are expected in any cross-border payment context).

Institutional Governance of Bilateral Links

When only two parties are involved, institutional governance can be simpler and more flexible, though it lacks the neutrality of a multilateral arrangement:

- **Bilateral Agreement:** The two central banks will enter into a **bilateral agreement or MoU** outlining the CBDC link. This likely specifies the purpose (e.g., to facilitate payments between their currencies for banks in each jurisdiction), the technical method (referencing the protocols they've implemented), and roles/responsibilities. It may detail operational procedures, for instance, how to coordinate maintenance times so one system isn't sending transactions while the other is down. It will also handle legal liability: each side probably agrees to fulfill its obligations on a best-effort basis but disclaims liability for technical failures beyond maybe reversing any incomplete transactions. Since no third party is involved, the two central banks have more freedom to shape terms to their mutual satisfaction.

- **Access Rules:** The agreement should clarify who can use the link. Is it only the central banks transferring balances between each other (like a crossholding of CBDC for liquidity)? Or are commercial banks in each country directly using the link to send payments to each other? In Jasper-Ubin's concept, the idea was **commercial banks could directly transact across ledgers** via the HTLC mechanism[29]. In practice, which means if Bank A (Canada) wants to pay Bank B (Singapore), it initiates a cross-ledger swap of CAD-CBDC for SGD-CBDC through the system. The central banks would oversee this but not intervene in each transaction. For that to happen, the central banks must agree on which commercial institutions are eligible. They might maintain a shared whitelist of participants. If, say, a new Canadian bank wants to use it, the Bank of Canada would inform MAS to trust transactions involving that bank's identity, and vice versa. Essentially, each central bank **vouches for its domestic participants**. They also need to decide whether participants need to separately sign any agreement (perhaps not, if they are just using their own CBDC systems normally, with the link handled in the background).

- **Regulatory Coordination:** Because this is a direct link, any **regulatory approvals** needed for cross-border flows must be sorted out. For example, capital controls or FX restrictions: if one country has rules about how much CBDC can be converted to foreign CBDC or sent out, the link must respect that. The two central banks would discuss these policies and possibly encode limits. If either side has concerns about

[29] BIS Innovation Hub and central banks of Australia, Malaysia, Singapore and South Africa develop experimental multi-CBDC platform for international settlements.

illicit finance, they might include clauses to share information on suspicious activities. They might also plan joint exercises or oversight meetings to ensure the link isn't being used to bypass regulations (like if one jurisdiction has stricter AML, criminals might try to route money via the other – cooperation is needed to prevent that arbitrage).

- **Decision-Making and Change Management:** With just two parties, governance is inherently **joint** – nothing changes unless both agree. This can make decision-making easier (only one counterpart to negotiate with) but also means if there's a disagreement, there's no third-party mediator by default. Typically, issues would be resolved through bilateral diplomacy: central bank heads or appointed liaisons would work it out. The agreement could establish a **Bilateral Working Group** that meets periodically to manage the project. This group would handle any enhancements to the system, review performance, and address problems. Because of the limited scale, this might not need a formal voting mechanism, it could operate on consensus (both sides must consent, essentially a veto power for each). This ensures sovereignty is fully respected: each central bank has ultimate say over its involvement.

- **Dispute Resolution:** If disputes cannot be solved amicably, the agreement might specify arbitration or a jurisdiction for legal recourse, but given central banks are often protected by sovereign immunity, it's likely they'd keep resolution in the diplomatic realm. They might specify escalation to higher authorities (e.g., deputy governors, then governors) to try to resolve any stalemate. The main disputes that could arise are technical failures causing loss or one side perceiving misuse. Since both have aligned incentives for a smooth link, dispute risks are relatively low; nonetheless, clarity in the MoU is important to avoid misunderstandings.

- **Termination and Exit:** Either party will want the right to turn off the link if needed (for instance, if trust erodes or if one country decides to join a different arrangement instead). Governance includes terms for termination, usually with notice, except in emergencies where a suspension might be immediate. If terminated, the agreement would outline how to settle any in-flight transactions or outstanding obligations. Ideally, the atomic nature means no half-done transactions, so termination just means stop accepting new ones. It's simpler than unwinding a multilateral platform membership, which could be messier.

- **Expansion to Multilateral:** One bilateral link is manageable, but what if each country wants links with others? For example, if Singapore links with Canada, and then separately with UK, and Canada also links with UK, you get a triangle of separate links. Each link has its own governance. Over time, this becomes **fragmented**. There is no central coordination, so differing terms or technologies could make it unwieldy, and monitoring systemic risk across many bilateral links is hard. BIS analysts have noted that without a hub, linking n systems leads to *n(n-1)/2 connections* which are unsustainable beyond a small number of jurisdictions[30]. Thus, bilateral governance

[30] Project Icebreaker: Breaking new paths in crossborder retail CBDC payments.

doesn't scale; it might be suitable for a few corridors (especially where there's strong bilateral cooperation already, like neighboring countries or key trading partners), but it could not easily extend to a global network. Central banks recognize this – Jasper-Ubin's authors themselves questioned *"What complications will arise with a large number of jurisdictions? How should such a system be governed, for example in updates to the protocol?"*[31]. Those questions imply that bilateral solutions become problematic as you multiply them.

Challenges and Trade-offs – Bilateral Links

As a model, bilateral CBDC links offer **maximum autonomy and tailoring** – each connection can be customized to the needs of the two parties. They also avoid creating new institutions or governance layers: it leverages direct relationships. But the downsides in a broader context are significant:

- **Limited Scale and Redundancy:** A bilateral link by definition only connects two currencies. If a bank needs to pay a third currency, it either goes through another link or falls back to old methods. This can lead to a patchwork where some corridors are efficient and others lag. It may concentrate liquidity in a few major links (for example, everyone links with a key currency like USD or EUR, forming a hub-and-spoke indirectly around that currency – but then we're back to a de facto hub, just not explicitly governed as one).

- **Complexity for Multiple Links:** If a country maintains many bilateral links, it has to juggle multiple governance agreements and possibly multiple technical protocols. One country's CBDC system might end up running different modules for each link, each with its own quirks. That increases operational complexity and risk of inconsistencies. Coordinating upgrades or changes then requires dealing with each partner separately. This could overwhelm smaller central banks if they attempt more than a couple such links.

- **High Initial Trust or Effort Requirements:** To link directly, two central banks either need a high degree of mutual trust or a very well-crafted trustless mechanism. Jasper-Ubin achieved trustless atomicity, which is encouraging, but such sophisticated implementation may not be within reach of all central banks without significant R&D. Lacking that, two countries might simply decide to trust each other's nodes or appoint an escrow agent – but that reintroduces a third party or weakens security. Thus, the bilateral model works best either for *close allies* (where legal trust and communication is strong) or when both invest in advanced cryptographic solutions. The former limits it to certain pairs; the latter is complex to develop (though results like Jasper-Ubin show it's feasible).

[31] Jasper–Ubin Design Paper Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies.

- **Resilience:** One could argue bilateral links reduce single point of failure risk (no central hub that can crash and take out all connectivity). Each link is independent – so a problem between A and B doesn't directly affect B's link with C, etc. This **decentralized topology** is more resilient in that sense. However, it's also harder to monitor. If something goes wrong in one link, there's no central overseer to quickly impose a fix across all; it depends on the two involved. Systemic oversight (by bodies like CPMI) would have to look at many connections individually. Furthermore, if one country's system fails, all its bilateral links fail at once (which is similar to any model, but here there's no alternative path – unless perhaps others route around via different links which gets complicated).

- **Innovation and Future Compatibility:** Bilateral links may lag in adopting innovations compared to a centralized hub or single system. If a new standard for interlinking emerges, each bilateral pair has to incorporate it. There's a risk of fragmentation where different pairs use different standards, hindering any future consolidation. With a hub, you could update once; with bilaterals, you update many times. That said, bilateral links could serve as **learning testbeds** – e.g., two countries pilot a new feature which could later inform multilateral designs.

In summary, bilateral CBDC links are a **tactical solution** suitable for early experiments or specific partnerships, but they do not present a scalable long-term framework for global CBDC interoperability. They shine in situations requiring minimal multilateral coordination – just two parties hashing out an arrangement. Indeed, such links might emerge first, as neighboring countries or key trade partners pair up to solve urgent pain points (similar to how some central banks have bilateral currency swap lines). Over time, however, there will be pressure to migrate to a more scalable model (hub or shared platform) as the network of links becomes too cumbersome. The BIS has effectively suggested that while bilateral interlinking can enhance cross-border CBDC use, it "may not necessarily require direct access or the establishment of new technical components" but also **"may not achieve similar scalability"** as more centralized models. The Jasper-Ubin trial was successful in proving technical viability *"a cross-border, cross-currency, cross-platform atomic transaction without a trusted third party"*, but even its authors acknowledged open questions on governance and scalability for more jurisdictions. Thus, bilateral links are likely to complement, rather than replace, broader interoperability strategies.

Compatibility Standards and Interlinking Frameworks

The fourth model is less about a specific network architecture and more about an overarching strategy: ensuring CBDC systems are built to common **standards** and utilizing interoperability frameworks so that they can **"plug in"** to each other or to existing payment networks when needed. This can be thought of as the *compatibility* approach (in BIS terms, "CBDC systems using common standards" to reduce friction[32]) and the use of *interlinking frameworks* (toolkits

[32] Options for access to and interoperability of CBDCs for cross-border payments July 2022 Report to the G20.

and protocols that facilitate communication between disparate systems). Unlike the previous models, which establish explicit connections or shared infrastructure, this approach prepares the ground for interoperability without necessarily activating it through a dedicated platform. It emphasizes **coordination, not integration**.

Examples of this approach include the use of **standardized messaging protocols** for CBDCs (so any system can understand payment instructions from another) and the exploration of technologies like **API gateways, blockchain interoperability protocols (e.g., Hyperledger Cacti, Chainlink CCIP)**, or even leveraging existing networks like **SWIFT** as a carrier for CBDC transactions. A real-world instance is SWIFT's recent experiments interlinking CBDC networks on Quorum and Corda using ISO 20022 messages and a *"CBDC connector"* gateway, effectively showing that with proper standards, a CBDC on one platform can be transferred to another through the existing SWIFT communication network[33]. Another example is **Brazil's DREX (Digital Real) project**, which is building its CBDC on an Hyperledger Besu platform and explicitly prioritizing interoperability: the Central Bank of Brazil's guidelines call for *"interoperability with legacy domestic systems and ... integration with systems in other jurisdictions, with a view to making cross-border payments"*[34]. In line with that, Brazil is piloting Chainlink's CCIP (Cross-Chain Interoperability Protocol) to connect DREX with foreign platforms in trade finance use cases[35], a showcase of an interlinking framework in action.

Technical Governance via Standards and Frameworks

In the compatibility approach, technical governance is diffuse. Instead of one network to govern, the focus is on governing the **standards and interfaces** that many networks will implement:

- **Common Standards (APIs and Message Formats):** Central banks and international bodies (like BIS, IMF, ISO) collaborate to define technical standards for CBDC interoperability. This can include message schemas (payment requests, settlement confirmation, etc.), identity formats, and transaction data elements. For example, using the existing ISO 20022 standard for payments as a base, SWIFT's CBDC experiment did exactly that, encapsulating a CBDC transfer instruction in an ISO 20022 message that any system could parse[36]. The governance of such standards is typically through working groups and committees. Once published, adherence is voluntary but encouraged. Each CBDC system built to comply with these standards will inherently be easier to connect to others. The role of governance here is ensuring the standard is kept up to date and that central banks actually adopt it. There might be a monitoring function (e.g., an international dashboard of who has implemented which API version).

[33] Connecting digital islands: CBDCs – Results of SWIFT experiments interlinking CBDC networks and existing payments systems to achieve global interoperability.
[34] Brazil central bank details CBDC pilot guidelines.
[35] Brazil's Central Bank to Leverage Chainlink CCIP In Key CBDC Project.
[36] Connecting digital islands: CBDCs – Results of SWIFT experiments interlinking CBDC networks and existing payments systems to achieve global interoperability.

Yet, there's no enforcement beyond consensus and possibly moral suasion via fora like the G20.

- **Interoperability Frameworks and Middleware:** A variety of technical **bridges or middleware solutions** are emerging that can connect different DLT or payment systems. Hyperledger Cacti (formerly Cactus) is one open-source example aiming to provide interoperability between blockchains via a plugin architecture. Chainlink CCIP is a service that can pass value and data between chains through a decentralized network of oracles[37]. In a standards approach, a central bank might not build such a bridge itself but ensure its CBDC system can interface with them. For instance, if many CBDCs run on variants of Ethereum, they might agree on using a common bridge contract or oracle network for cross-chain transfers. Technical governance in this context often falls to the **providers or maintainers of the framework**. For Cacti, a Linux Foundation project, a committee of contributing organizations governs its roadmap. For Chainlink, Chainlink Labs and the node operators collectively govern its oracle network (which is a decentralized but not centrally bank-governed system). Thus, the challenge is that central banks must **trust external tech governance** or be part of it. To mitigate this, they may form public-private partnerships or consortia to have a say in these frameworks' development. Alternatively, central banks might collectively fund an open interoperability solution (like a public domain protocol) to avoid dependence on private networks.

- **Legacy Infrastructure Integration:** Compatibility also implies integrating CBDCs with existing payment rails. Many wholesale CBDC pilots ensure they can interact with RTGS systems and SWIFT from day one. For example, one design might allow a CBDC transfer to be initiated via a SWIFT message and vice versa[38]. Technical governance here involves coordination with the governance of legacy systems (like SWIFT's own standards release cycle, or national RTGS operating hours). A concrete governance tool is the adoption of **ISO country and currency codes** for CBDCs, ensuring that any messaging network can route CBDC transactions just like any currency. We already see proposals for unique identifiers (e.g., "Digital Real" might get a currency code so it can be referenced in international messages).

- **Decentralized vs Centralized Interlinking:** Some compatibility solutions may be decentralized (like cross-chain atomic swaps) and others centralized (like using a global message hub). SWIFT's solution is somewhat centralized (it uses the SWIFT platform as the intermediary carrying messages), whereas an atomic swap via HTLC or Chainlink is decentralized across nodes. Each has different technical governances. With a centralized intermediary (SWIFT), technical governance is easier to manage (SWIFT can roll out a new feature and all users update their interface). With decentralized protocols, updates are more community-driven and require agreement to adopt new versions. Central banks will likely prefer controlled evolution – hence

[37] Brazil's Central Bank To Leverage Chainlink CCIP In Key CBDC Project.
[38] Connecting digital islands: CBDCs – Results of SWIFT experiments interlinking CBDC networks and existing payments systems to achieve global interoperability.

SWIFT advertising itself as a "global hub" for CBDCs[39], implying it can be a stable backbone. SWIFT's governance (a cooperative of financial institutions) is something central banks are already involved in (through oversight groups). So, leveraging it means leaning on an existing governance structure rather than creating one anew. We see that in October 2022, SWIFT published results of interoperability tests and indicated readiness to support multiple CBDCs on existing infrastructure[40].

- **Security and Identity Frameworks:** Compatibility across systems also hinges on shared approaches to security. For example, digital signatures used by participants should be mutually recognizable. Perhaps a **global PKI or digital identity framework** will be needed so that a bank in one CBDC system can be authenticated when interacting with another. Efforts like W3C's DID (decentralized identifiers) or other PKI bridging might come into play. Governance of identity standards would ensure that each CBDC platform's identity management (often tied to national digital identity or licensing of institutions) can map to others. A practical step is agreeing on certificate authorities or trust anchors that all systems honor. This again would be handled in committees or mutual agreements, not by a single network's code.

Institutional Governance of the Compatibility Approach

Without a single platform or formal link, institutional governance is more about **cooperative arrangements and policy alignment**:

- **Policy Coordination and Principles:** Central banks may agree on high-level principles for interoperability. For example, the BIS Innovation Hub published reports and principles advocating that *"for cross-border payments, central banks should work together to establish common standards, protocols and frameworks"*[41]. These principles aren't binding but serve as a governance benchmark. Forums like the G20, BIS committees (e.g., CPMI), the IMF, and World Bank facilitate this coordination. They produce guidance documents and model frameworks. One could view the **"BIS CBDC interoperability principles"** as a soft governance tool – central banks publicly endorse them and commit to consider them in design. This way, even without a single network, there is a concerted push for compatibility (do no harm, ensure coexistence with other systems, etc.). The July 2022 BIS report on CBDC interoperability options is one such guidepost, comparing compatibility, interlinking, and single system approaches and highlighting implementation challenges to anticipatebis.org.

- **Bilateral/Multilateral MOUs for Access:** In lieu of technical integration, central banks might sign MOUs to open access of their CBDC systems to foreign institutions or to recognize each other's users. For example, Central Bank A could allow approved banks from Country B to hold and transact in A's CBDC, under certain conditions. Country B reciprocates. This essentially recreates a *"correspondent"* relationship but directly in CBDC. Institutional governance then is case-by-case agreements ensuring

[39] Swift finds role as global hub for CBDCs and tokenised assets.
[40] Swift Makes Strides in Interoperability Testing of CBDCs Across 200 Countries.
[41] Central Bank Digital Currency. Global Interoperability Principles. WHITE PAPER.

foreign participants abide by local rules. Unlike a bilateral link which is technical, this is just policy – e.g., allowing a foreign bank to open a wallet on A's CBDC system. There might be **legal conditions** (the foreign bank has to be supervised equivalently, info-sharing on any enforcement actions, etc.). Such agreements could be standardized regionally: a template for mutual access could be developed so that any central banks can plug in bilaterally without renegotiating from scratch every time. This approach was hinted at in some studies as *"indirect access"* for non-residents as a complement to interoperabilitybis.org. It increases compatibility by overlapping participation rather than linking infrastructure.

- **Role of International Networks (SWIFT, etc.):** If existing international networks are used (SWIFT, CIP, etc.), then those networks' governance serves as part of the institutional framework. For instance, if SWIFT is the carrier of CBDC interconnection, central banks might formalize that by an arrangement (maybe through the PMPG – Payments Market Practice Group or SWIFT's board) to prioritize CBDC support. They could form a user group within SWIFT for CBDCs that steers the needed changes. Essentially, they inject their governance requirements into SWIFT's processes. Similarly, if a regional network like LACChain (which underlies LAC CBDC experiments) is used as a common base, the governance of that network (LACNet consortium etc.) would intersect with central bank oversight. In fact, the IDB's LACChain initiative provides a permissioned blockchain infrastructure governed as a public-good consortium; if multiple LAC central banks deploy CBDCs on LACChain, they benefit from a shared governance layer for the base infrastructure, achieving compatibility by default. They would then likely enter into an agreement with LACNet on performance, security, and so forth, and among each other on usage norms.
- **Regulatory Harmonization Efforts:** Compatibility also requires harmonizing certain regulatory aspects across borders so that even if systems aren't directly linked, transactions can flow smoothly. This might include aligning messaging for compliance information (e.g., a standard format for attaching travel rule data about originators/beneficiaries for cross-border CBDC payments). Institutional governance in this sense takes the form of regulatory cooperation: central banks and finance ministries aligning anti-money laundering rules, foreign exchange laws, and reporting requirements. An example is the Financial Action Task Force (FATF) working on digital currency guidelines, if all CBDCs follow FATF's guidance for cross-border transactions, they will be more interoperable from a compliance standpoint. Such harmonization is slow but crucial; without it, technical compatibility might be moot if legal barriers prevent non-residents from using a CBDC or sharing data.
- **Market Practices and Adoption:** Another soft governance aspect is encouraging market players (banks, fintechs) to adopt bridges and standards. If, say, a group of major international banks decide to support a particular interoperability solution, that can drive global usage. Central banks might convene industry task forces to explore bridging between CBDCs and other digital asset networks, ensuring private sector readiness. The outcome could be industry guidelines that complement central bank

efforts. For instance, a consortium of banks might agree on a protocol to move liquidity between CBDCs and forex markets, which central banks could then endorse.

Challenges and Trade-offs – Compatibility/Standards

- **Lack of Immediate Coherence:** The compatibility approach doesn't deliver a singular functioning cross-border system; it provides building blocks. The actual interoperability still has to be achieved through participants leveraging those blocks. In the near term, this might mean cross-border CBDC transactions aren't much faster or cheaper than today unless private initiatives use the standards to create new services. There's a risk of a coordination problem: everyone is waiting for someone else to build the linking infrastructure.
- **Uneven Adoption:** Not all central banks may implement the standards uniformly. Some might use different technologies that don't fully adhere, or timeline differences could mean interoperability is patchy. This could create **"digital islands"**, where some CBDCs cluster around certain standards and others around different ones[42]. Without an enforcement mechanism, standard-setting relies on consensus and peer pressure. As a result, interoperability might improve incrementally, but some friction and conversion processes will remain (similar to how not all payment systems use ISO 20022 yet requiring translation in places).
- **Role of Third Parties:** While avoiding a new central intermediary, this model often ends up relying on existing intermediaries or new service providers (like oracle networks). This reintroduces trust considerations by the back door. For example, using Chainlink CCIP for interoperability means placing trust in a decentralized oracle network's security. Central banks might be cautious about that, they may demand audits or even run some of the nodes to gain trust. Meanwhile, using SWIFT involves trusting that SWIFT's governance will prioritize CBDC needs and keep costs reasonable (SWIFT will naturally seek to remain central by offering these services[43]). The cost model and control are then in the hands of an entity that is not explicitly governed by central bank consensus (though central banks influence SWIFT, they don't directly control it).
- **Gradual Efficiency Gains:** Compatibility alone might not dramatically cut costs or settlement times in the short run. It paves the way for improvements, but actual gains come when combined with either bilateral links or hub approaches on top. For instance, two compatible CBDCs could still use a correspondent bank to bridge them, with less friction due to standardization. That might be marginally better (fewer manual interventions, maybe straight-through-processing), but not the quantum leap of a multi-CBDC platform that eliminates intermediaries. Thus, one trade-off is **immediacy vs. readiness**: the standards-first approach emphasizes being ready for future integration

[42] Swift Makes Strides in Interoperability Testing of CBDCs Across 200 Countries.
[43] Swift finds role as global hub for CBDCs and tokenised assets.

("design for interoperability from day one"[44]), possibly at the expense of delivering a big cross-border impact right away.

- **Foundation for Other Models:** On the positive side, a strong compatibility framework is **complementary** to the other models. It's not either/or compatibility is indeed the baseline in the BIS classification. Even if you build a hub or shared ledger, you still benefit from common standards (for example, mBridge made its platform EVM-compatible to integrate with other systems more easily). Likewise, any hub could connect to other hubs via standardized APIs in future. So, investing in standards is a low regret move. The challenge is ensuring those standards don't lag behind technology; they must be somewhat future proof.

In essence, the compatibility and standards-based approach **emphasizes flexibility and long-term interoperability** over short-term centralized solutions. It acknowledges a world of diverse technologies and seeks to knit them together through agreed conventions and tools, rather than replacing them with one network. For policymakers, pushing this approach means funding collaborative R&D (for interoperability protocols), actively participating in international standard-setting, and requiring that any CBDC developed domestically has "hooks" for future connectivity. The Central Bank of Brazil's inclusion of interoperability requirements in its Real Digital pilot principles is a prime example, it ensures from the outset that DREX won't be a silo[45]. Already, Brazil's pilot with Chainlink shows how a domestic CBDC platform can connect to an external blockchain network securely to achieve cross-chain Delivery-vs-Payment[46]. Such experiments, if multiplied, could yield a web of interoperable CBDC ecosystems, not through one unifying network, but through **many bridges governed by common standards and reciprocity**.

Comparative Analysis and Key Trade-offs

Drawing the insights together, each interoperability model carries distinct governance implications and trade-offs. A useful comparative framework comes from the BIS, which notes that **"each of the CBDC interoperability models has different implications in terms of efficiency, resilience, complexity, and governance"**[47]. There is likely **no one-size-fits-all** solution, different regions or use cases may favor different models, and they may coexist. Here we summarize the models side-by-side, emphasizing wholesale CBDC contexts and drawing on BIS recommendations:

- **Single Shared Ledger:** This model can deliver the highest efficiency (near-instant cross-currency settlement with minimal intermediaries) and potentially the most innovative functionalities (since all players share one programmable platform). It also enforces a high degree of standardization by definition, one system means one set of rules. However, it scores lower on ease of implementation and sovereignty concerns.

[44] BCB issues multiple announcements for banks.
[45] Brazil central bank details CBDC pilot guidelines.
[46] Brazil's Central Bank To Leverage Chainlink CCIP In Key CBDC Project.
[47] Options for access to and interoperability of CBDCs for cross-border payments.

Governance is **highly centralized (collectively)**, requiring a formal structure to manage what is essentially a new multinational financial market infrastructure. The BIS has suggested that while a common platform is very promising for connectivity, it is *"the most challenging to achieve"* and would likely require robust governance mechanisms to ensure trust. The Dunbar project confirmed that these governance mechanisms can be built using both technology (permissions, smart contracts) and legal agreements to address concerns of shared control. But in practice, convincing multiple central banks to actually put a joint system into production will involve overcoming legal hurdles (e.g., enabling laws to allow a foreign entity to operate domestic critical infrastructure, if needed) and aligning political will. Thus, this model might emerge in scenarios where a strong regional bloc exists (perhaps a monetary union or very closely integrated economies) or under the aegis of a trusted international institution that can serve as an operator. The trade-off is essentially **efficiency vs. complexity**: you get the most streamlined processes at the cost of the most complex governance arrangement.

- **Hub-and-Spoke:** The hub model offers a modular approach; each jurisdiction keeps its system, and the hub does the minimal necessary bridging. It tends to rank high on **resilience and scalability** in terms of connections (fewer total links and localized failures), though the hub itself must be resilient. In BIS's view, a hub-and-spoke can bring significant improvements more easily than a single system, and indeed Icebreaker's success hints that even retail users could get better FX rates and faster service via this model[48][49]. For wholesale, a hub could similarly streamline interbank cross-currency trades and liquidity savings (especially if combined with a PvP mechanism). Governance in this model is partly centralized (the hub operation) and partly decentralized (each central bank governs its own CBDC). This split means governance tasks are also split technical and operational governance of the hub might be handled by one entity, while institutional governance is more about agreements between that entity and participants. The **inclusivity** is high; many countries can connect provided the hub is open, which for regions like LAC is attractive because smaller economies can join a larger scheme without negotiating dozens of bilateral deals. One major trade-off here is **trust vs. autonomy**: central banks retain autonomy over their own systems (a plus) but must trust the hub operator to be neutral and competent (a new dependency). Mitigating that trust issue often means giving them collective oversight of the hub (like a council). The BIS has pointed out that a hub model might be more feasible in the shorter term and can later be extended. It's a kind of **intermediate solution** that could gradually globalize (imagine multiple hubs interconnecting, perhaps via standard protocols, a network of hubs, which some have dubbed a "network-of-networks" approach).

- **Bilateral Links:** In terms of **policy control and simplicity**, bilateral links are top, each link is a contained project between two willing partners. For wholesale use, this could be useful for specific corridors (e.g., a deep financial relationship like US-Mexico or

[48] BIS Says 'Hub-and-Spoke' Cross-Border Transfers Offer Benefits to Retail CBDC.
[49] BIS G20 report explores practical lessons from CBDC projects.

Singapore-Eurozone) to pilot CBDC connectivity. Bilateral arrangements shine when just a pair of central banks want to achieve something quickly without waiting for broader consensus. They also might handle unique requirements of that corridor (for example, if two countries have a currency swap agreement, they could integrate that with a CBDC swap system easily). However, on **scalability and network effects**, bilateral links rank lowest. They do not inherently create a seamless network; they create siloed corridors. The more are added, the more complicated it gets to manage the web. This approach could inadvertently recreate the fragmented correspondent network, just with DLT pipes under it. The BIS report cautions that while interlinking via bilateral links can address some challenges, it may bring only incremental improvements and could falter with large numbers of participants. Governance of each link is straightforward, but governance of the *collection of links* is nonexistent, that's a key drawback if one aims for a global solution. One could imagine down the road; multiple bilateral links being replaced by a hub or shared platform as participants realize the need for consolidation. In essence, the bilateral model might be a stepping stone or a niche solution rather than an end-state.

- **Compatibility Standards/Interlinking Frameworks:** This approach is like **laying down rail tracks broadly, before deciding which train will run**. It's a necessary underpinning – indeed, all models benefit from common standards, but on its own, it's the least tangible for delivering faster/cheaper payments. Its strength is that it **reduces barriers to future interoperability** and ensures that, at a minimum, different CBDCs aren't completely siloed or incompatible. For wholesale CBDCs, having common technical standards (data formats, APIs) can ease integration with existing financial institutions' systems and with cross-border arrangements that may arise. The BIS calls this *"compatibility"* and notes it is the least costly form to implement (you basically design your CBDC to be compatible, which is just good practice). The trade-off is that it *"may not achieve similar efficiency benefits"* as actual interlinking or a single system. It's necessary but not sufficient for major performance gains. In terms of governance, the standards approach relies on **broad consensus and voluntary adoption**, which can be slow. But it scores well on **compliance and national preference**: each country can implement its CBDC in line with domestic needs while still adhering to common standards. Over time, if all follow compatibility principles, even if formal links are not in place, the system is more flexible, private sector or regional initiatives can bridge systems with less friction. A real risk is if standards are interpreted differently or updates cause divergence, which is why continuous coordination (through BIS, ISO, etc.) is needed. This model also encourages leveraging existing infrastructures to the fullest – an example being SWIFT essentially proposing to serve as an interlinking *"single access point"* for CBDCs globally, which could be seen as a hybrid of compatibility and a centralized hub (albeit using an existing hub).

Challenges and Trade-offs Summary

- *Scalability*: Single ledger can handle high volumes internally but is limited by how many members can effectively co-manage it; hub can scale to many members linearly;

bilateral doesn't scale beyond a few links; standards scale conceptually but require uptake.

- *Resilience*: Single ledger has unified security, but a bug or attack can be systemic; hub localizes failures to the hub (still critical), but domestic systems remain safe if hub fails; bilateral isolates issues to that link; standards alone have no "system" to fail, but rely on existing systems' resilience.
- *Compliance & Sovereignty*: Single ledger demands most compromise and unified governance (harder to accommodate divergent rules, though can be built in via smart contracts to some degree); hub allows national rules on each side with minimal shared rule set (FX and messaging), so easier to fit different legal environments; bilateral is two-party tailored, easier to satisfy each of the two, but doesn't solve differences beyond those two; standards allow each jurisdiction full control, just using common "language", so it's the most respectful of sovereignty, but in turn places more burden on each to enforce compliance at the borders of systems.
- *Inclusivity*: Standards and hub models rank high; they present low barriers to join the interoperable club. Single ledger could exclude those who are not ready or comfortable to join the shared platform. Bilateral links can leave many out unless proactively extended.

The BIS and other global institutions seem to converge on a view that a **portfolio of solutions** will be needed. In fact, they often suggest pursuing compatibility (common standards) as a baseline, and interlinking (via either hubs or specific connections) as needed to complement domestic CBDC development[50]. The end-state could even involve integration of models: for example, several countries might form a shared ledger union, which then connects to other such groups or standalone CBDCs through hub or standard-based links.

This analysis underscores that **governance choices are as crucial as technical choices**. A technically excellent platform without a viable governance model will not gain multi-country adoption. Conversely, a well-governed simple solution might beat a complex but poorly coordinated one. It will be important to **leverage international best practices**: use the BIS Innovation Hub findings as templates (e.g., adopt the rulebook structures from mBridge and Dunbar, adapt them regionally), follow IMF and World Bank guidance on legal frameworks, and participate in global standard efforts so that LAC CBDCs are compatible with others from day one. Initiatives like LACChain provide a ready-made governance and technical environment aligning with these principles (permissioned Ethereum, open governance, etc.), which can accelerate experimentation.

In conclusion, governance in wholesale CBDC projects entails a dual design problem: **designing the technology architecture and the cooperative framework** in tandem. Whether through a single cross-border ledger, a connector hub, direct bilateral arrangements, or simply smart use of standards, the success of these projects will hinge on how well governance mechanisms address the needs of scalability, resilience, legal compliance, and

[50] Options for access to and interoperability of CBDCs for cross-border payments. Report to the G20.

broad participation. Early pilots have proven that various models *can* work, now the task is to refine and combine them to build an interoperable future for CBDCs, where payments move seamlessly across borders with the same confidence and speed as within domestic systems. The choices made today in governance design will set the trajectory for how inclusive and effective the global CBDC ecosystem will become in the coming decade.