

## Agenda item 3: Members' presentations on topics related to new technologies for settlement of wholesale financial transactions in central bank money

**Background:** in line with the NTW-CG's purpose of information sharing and following interest expressed by some members to discuss certain themes, members will be invited to present useful topics related to new technologies for settlement of wholesale financial transactions in central bank money.

Themes that have been put forward in a recent NTW-CG survey were:

- What can be done to reduce the risk of refragmenting financial markets?
- Management of KYT/AML when using smart contracts
- Standardisation and interoperability between different DLT platforms (continued)
- Governance and risk assessments of DLT platforms

8th NTW-Contact Group meeting  
18 June 2024

# Presentation to NTW-CG

June 2024

DIGITAL ASSET SECURITIES CONTROL PRINCIPLES: A FRAMEWORK FOR ADOPTION

**DTCC**

clearstream

DEUTSCHE BÖRSE  
GROUP

 euroclear

In collaboration with **BCG**

Note: This presentation is an extract of the document that can be accessed from any of the companies' sites

## How to support adoption and overcome fragmentation

The aim is to support the industry's efforts to unlock the transformative nature of DLT in the realm of Digital Asset Securities (DAS i.e. does not cover cryptoassets or CBDC used as means of payments).

We all see the potential but also the risk of fragmentation that comes with the rapid evolution of the domain.

## This proposal looks at:

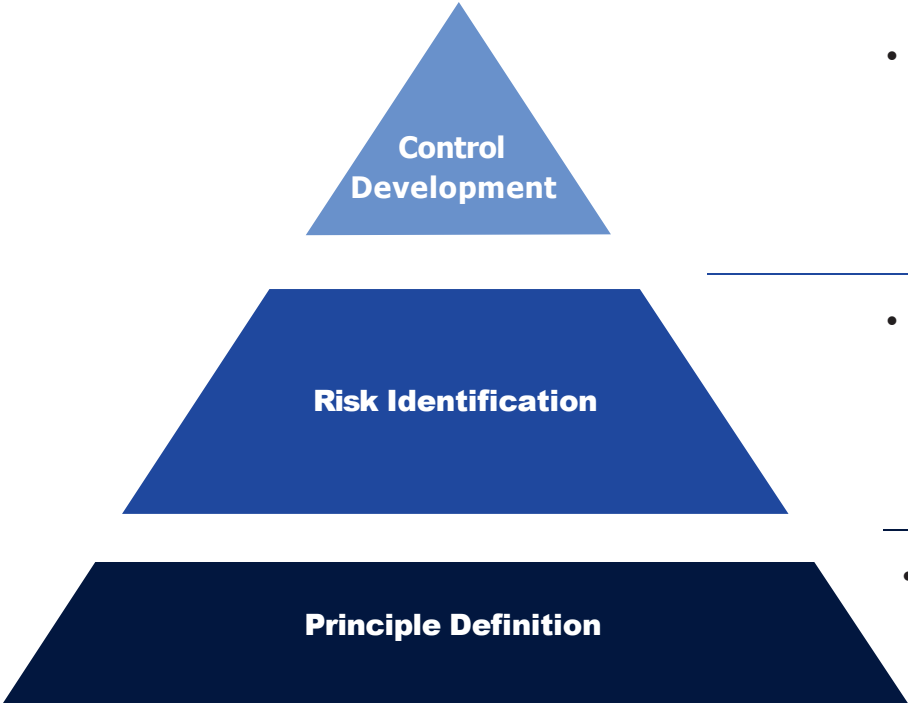
- **Fostering a common language**
- **Supporting efforts to enable regulatory clarity**  
Over 100 regulations reviewed by BCG and engaged with more than 20 key market participants)
- **Proposing a blueprint for industry-wide alignment**  
Developing capabilities to form an aligned view on controls to get alignment on industry wide processes
- **Designed to be asset class agnostic and technologically neutral**  
so it can be adopted across different organisation across the ecosystem
- **Next step is to transition to industry association(s)**  
as neutral third party(ies) to foster wider engagement.

# Structured layered approach

**The framework (DASCP) was developed in multiple layers along foundational principles, risks, and controls.**

At this juncture, the DASCP is not about creating fixed standards; rather, it is laying the necessary groundwork that will inform the development of comprehensive industry standards in the future.

We start from the ground by laying out a set of foundational principles for secure and efficient financial ecosystems.



- **Control Development Design:** Controls for each identified risk are then designed, emphasizing flexibility to allow them to serve as adaptable guidelines rather than rigid rules.

- **Risk Identification Compilation:** a comprehensive list of risks associated with each principle is compiled, incorporating traditional finance risks adapted for DAS and new risks unique to this sector.

- **Principle Definition:** a set of foundational principles that function as overarching objectives guiding the entire framework.

# Principles

The rise in DLT initiatives signifies a shift in financial market infrastructure, reminiscent of the robust standards set forth by the Principles for Financial Market Infrastructures (pFMIs) issued by BIS and IOSCO. As tokenization becomes increasingly prevalent, the DASCP has been proactively established to address the challenges of widespread adoption. The DASCP is formulated with an understanding of the core objectives that pFMIs champion: integrity, stability, and confidence in the financial system.

**The principles below are listed in order of priority, but all are vital to building a secure DAS ecosystem:**



## **Legal Certainty:**

Ensuring operations comply with existing laws and regulations to maintain market integrity and investor confidence.



## **Regulatory Compliance:**

Encouraging alignment with regulatory frameworks to build a foundation of trust and safety in digital asset markets.



## **Resilience and Security:**

Developing robust infrastructure capable of resisting disruptions, while protecting sensitive data and ensuring the continuous operation of digital asset services.



## **Safeguarding Customer Assets:**

Implementing governance over smart contracts to manage and protect customer assets within the digital asset ecosystem securely.



## **Connectivity and Interoperability:**

Facilitating transactions and flexible settlements across diverse networks to enable the seamless transfer and settlement of DAS.



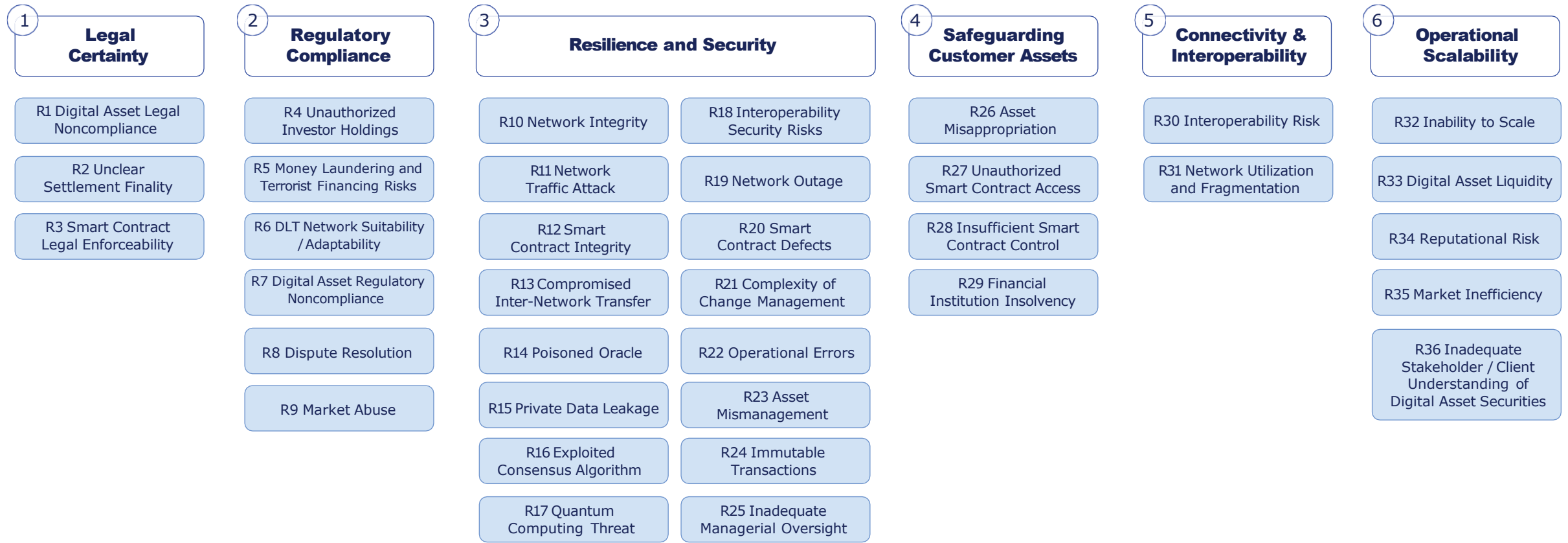
## **Operational Scalability:**

Striving for efficiency and cost-effectiveness through standardized roles and smart contract functions to accommodate market growth.

# Risks

Building on the foundational principles outlined above, it is crucial to systematically manage a wide range of risks. Adopting a risk-first approach ensures that emerging risks associated with DAS are proactively identified and effectively mitigated. This establishes a solid basis for safeguarding market integrity and building investor trust, which are critical for the adoption and growth of digital asset markets.

These risks, spanning the entire value chain, were identified along with the outlined principles to ensure robustness and exhaustiveness of the framework. Some risks inherently impact multiple principles. For conciseness, they were assigned to the principle with the highest importance, as depicted in the figure below.



**Immediate priority**  
Minimum requirements



**Subsequent priority**  
Unlock full potential

# Controls

The comprehensive risk inventory establishes a foundation for developing targeted controls essential for managing identified risks, thereby supporting the transition toward a DAS ecosystem aligned with our foundational principles.

These controls are designed to be adaptable, serving as a broad framework. Thus, they function more as guidelines rather than rigid controls and are crafted to address multiple risks, offering flexibility to adjust to different technologies and products. These controls are also dynamic, allowing for iterative updates to keep pace with the changing risk landscape and emerging technological advancements.

The following controls have been derived and mapped to the risks they are mitigating. Each control mitigates at least one risk, with many controls addressing multiple risks.

## A secondary layer of control categorization organizes controls into four distinct groups, each distinguished by a unique suffix appended to the control number:

### **L** → **Legal:**

Addresses adherence to regulatory requirements and legal frameworks, ensuring that DAS operations comply with applicable laws and compliance standards.

### **S** → **Smart Contract Governance:**

Ensures the accuracy, authorization, and performance of smart contracts.

### **R** → **Resilience and Data Protection:**

Protects systems against disruptions and secures sensitive information.

### **N** → **Network Settlement:**

Fosters reliable and timely transaction processing within the DLT network.

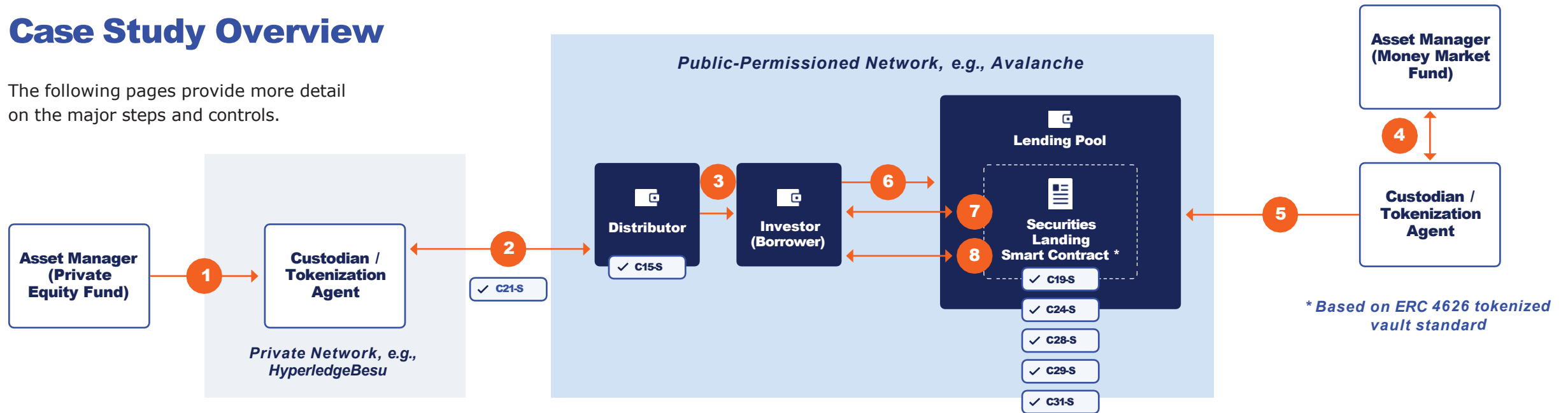
As illustrated in the figure below, controls also have been organized into a taxonomy comprised of four categories – Legal, Smart Contract Governance, Resiliency and Data Protection, and Network Settlement – each categorized according to its required mitigating measures to enhance clarity. The specific risk that the control mitigates is listed below the control.

Legal		Smart Contract Governance		Resilience & Data Protection		Network Settlement	
C1-L Participation Guidelines R1, R35	C7-L Governance R1, R6, R35	C13-S Smart Contract Auditing Guidelines R3	C23-S Data / Properties R22, R32	C32-R Audit Trail R2, R12, R14, R16, R23, R24, R26, R27	C39-R Recovery Testing R10, R19, R21	C46-N Data Lineage R1, R12, R15, R21, R23, R27	C52-N Compliance and Policy Management R4, R5
C2-L Product Eligibility R1, R7	C8-L Rule Enforcement and Arrangements R1, R9	C14-S Certification R3, R12	C24-S Functions / Behaviors R22, R32	C33-R Data Life Cycle Management R7	C40-R Private Data Segregation R15	C47-N Encumbrance Mechanism R2	C53-N Continuous Management Education R5
C3-L Network and Oracle Vetting R1, R6, R10, R14, R35	C9-L Regulatory Approval and Oversight R1	C15-S Investor Compliance and Access Control R4, R5	C25-S Bookkeeping R22, R29, R32	C34-R Data Subject Access Rights Enforcement R7, R24	C41-R Anonymization and Pseudonymization R15	C48-N Settlement Proofs R2	C54-N Legacy Infrastructure Integration R30, R32
C4-L Participant Roles, Responsibilities, and Obligations R1, R3, R8, R25, R26	C10-L Asset Safeguarding and Segregation R4, R23, R25, R26, R27, R29	C16-S Multiparty Transaction Validation R4, R5, R7, R12, R23, R26, R28	C26-S Account Structure R22, R29, R32	C35-R Event Monitoring and Alerts R9, R14, R16, R19, R22, R25, R30, R33	C42-R Identity Verification R15	C49-N Fail to Settle Process R2	C55-N Third-Party Integration Guidelines R30
C5-L Service Providers Responsibilities / Limitation of Liability R1	C11-L Policies and Procedures R7, R35	C17-S Dispute Resolution Mechanism R8	C27-S Key Life Cycle Management R26, R27	C36-R Redundancy and Concurrency R10, R11, R19	C43-R Geographical Distribution R19	C50-N Transaction Sequencing R2, R13	C56-N Community Engagement Framework R31, R34
C6-L Terms and Conditions R1, R29	C12-L Education and Training for Stakeholders on Digital Asset Securities R36	C18-S Code Auditing R12, R16, R20, R35	C28-S Smart Contract Roles R28, R32	C37-R Backups R10, R11, R19, R21	C44-R Feature Deployment Process R21	C51-N Cross-Ledger Data and Inventory Balances R2, R13	C57-N Liquidity Management Strategies R33
		C19-S Smart Contract Entitlements R16, R23, R24, R26, R27, R28	C29-S Emergency Stop R28, R32	C38-R Failure Prevention, Detection, and Recovery R10, R11, R19, R21	C45-R Data Integrity Correction R22		
		C20-S Quantum-Resistant Signature Algorithms R17	C30-S Account Pause R28, R32				
		C21-S Intraoperability between DLT Networks R18, R22, R30, R32	C31-S Token Pause R28, R32				
		C22-S Token Specification Model R22, R32					



# Case Study Overview

The following pages provide more detail on the major steps and controls.



## Major steps:

- 1 Asset Tokenization
- 2 Token Transfer
- 3 KYC Enforcement
- 4 Money Market Fund (MMF) Issuance
- 5 MMF Tokenization for Lending
- 6 Collateral Deposit
- 7 Lending Pool Transactions
- 8 Automated Lending Operations

Principle	Risk	Control
Connectivity and Interoperability	R30 Interoperability Risk	C21-S Intraoperability between DLT Networks
Regulatory Compliance	R4 Unauthorized Investor Holdings	C15-S Investor Compliance and Access Control
Resilience and Security	R23 Asset Mismanagement	C19-S Smart Contract Entitlements
Operational Scalability	R32 Inability to Scale	C24-S Functions / Behaviors
Safeguarding Customer Assets	R28 Insufficient Smart Contract Control	C28-S Smart Contract Roles C29-S Emergency Stop C31-S Token Pause

## Description of major steps:

### 1 Asset Tokenization:

An asset manager issues a private security, such as a private equity fund, which is then tokenized on a private blockchain by a custodian.

### 2 Token Transfer:

The custodian moves the newly created PE (Private Equity) tokens from the private ledger to a public-permissioned ledger for wider distribution.

### 3 KYC Enforcement:

As tokens are distributed, KYC compliance checks are performed to ensure all investors meet regulatory standards, despite the change in blockchain.

### 4 Money Market Fund (MMF) Issuance:

In parallel, an asset manager issues a Money Market Fund.

### 5 MMF Tokenization for Lending:

The custodian tokenizes the MMF shares and makes them available for lending in the Securities Lending Market.

### 6 Collateral Deposit:

Investors with tokenized PE fund shares deposit these tokens into the lending pool to serve as collateral.



### 7 Lending Pool Transactions:

Using the collateral provided, investors borrow more liquid assets (e.g., MMF shares) from the lending pool.

### 8 Automated Lending Operations:

The lending process, powered by smart contracts, automates the workflow, including the deposit, loan issuance, and approval, and upon maturity, manages repayment and interest distribution and returns the securities to their original owners.

The chart below presents a detailed illustration of the DASCP controls in action, delineating the specific methods used for its implementation. While these examples highlight the controls' functionality and the potential for smart contracts to reinforce the robustness of the DAS market, they are intended to serve as illustrations of what can be achieved. They are not prescriptive; organizations are encouraged to interpret and adapt controls to fit their unique environments, strategies, and compliance needs. This illustrative approach reaffirms the DASCP framework's commitment to flexibility and its capacity to accommodate a diverse range of technologies and operational scenarios, ensuring its broad applicability and relevance across the financial industry.

Principle	Risk	Control	Smart Contract Control Activities
<p data-bbox="115 516 585 545"><b>Connectivity and Interoperability</b></p> 	<p data-bbox="739 516 1298 805"><b>R30 Interoperability Risk:</b> The risk pertains to the complexities of integrating digital assets with traditional financial systems and, potentially, multiple blockchain architectures (e.g., public, public-permissioned, and private) to ensure seamless transactions across the entire financial spectrum.</p>	<p data-bbox="1365 516 1943 876"><b>C21-S Intraoperability Between DLT Networks:</b> Adhere to industry-accepted cross-network communication protocols specifically designed for blockchain interoperability. This includes standardized protocols for asset representation, transaction formats, and data exchange between different blockchain networks, ensuring seamless and secure interactions across diverse blockchain platforms.</p>	<p data-bbox="1986 516 2529 841">Specific smart contracts and token standards, along with cross-chain interoperability protocols (lock / mint), ensure token transferability from one chain to another, adhering to both internal compliance and industry-accepted cross-network communication protocols for asset representation, transaction formats, and data exchange.</p>
<p data-bbox="115 922 446 951"><b>Regulatory Compliance</b></p> 	<p data-bbox="739 922 1314 1211"><b>R4 Unauthorized Investor Holdings:</b> Potential for regulatory noncompliance and financial repercussions if a non-compliant or unauthorized investor holds or transfers a digital asset security. This includes breaches of investor accreditation, investment caps, or other regulatory standards not related to AML or CTF.</p>	<p data-bbox="1365 922 1946 1211"><b>C15-S Investor Compliance and Access Control:</b> Implement mechanisms that only allow authorized investors that are in good compliance standing (e.g., KYC, sanctions, etc.) to hold registered securities while restricting others who are not, which could be facilitated by allow-lists, verifiable credentials, or other relevant protocols.</p>	<p data-bbox="1986 922 2548 1062">Smart contract checks the client's wallet for required credentials and completes the transfer only if the investor is compliant with the fund terms.</p>

Principle	Risk	Control	Smart Contract Control Activities
<p><b>Resilience and Security</b></p> 	<p><b>R23 Asset Mismanagement:</b> Digital assets are at risk of being lost, stolen, or erroneously transferred due to breaches in operational controls, system vulnerabilities, or inadequate asset management protocols.</p>	<p><b>C19-S Smart Contract Entitlements:</b> Restrict access to smart contract data and functions based on standard roles using fine-grain entitlements.</p>	<p>A smart contract, combined with a specific token standard, grants the lending decision to the lending pool, ensuring that only the lending pool can issue and approve a loan. This ensures immutability of roles, entitlement, and processes, thus eliminating the risk of unauthorized use or access to the loan’s data and functions.</p>
<p><b>Operational Scalability</b></p> 	<p><b>R32 Inability to Scale:</b> DLT networks may not efficiently manage or scale to accommodate surging transaction volumes, impacting critical functions such as post-trade capture and overall transaction throughput (including suitable customer support), potentially degrading system performance and reliability.</p>	<p><b>C24-S Functions / Behaviors:</b> Conform to a common set of functions, behaviors, and service level agreements that support various security life cycle operations such as issuance and settlement.</p>	<p>Smart contracts enable automation and atomic settlement of transactions, which provides scalability to perform large volumes of standardized yet complex operations in seconds. For example, for the lending transaction, the smart contract performed six functions in one step (deposit, issuance, approval, deposit, hair-cutting, and pledging).</p>
<p><b>Safeguarding Customer Assets</b></p> 	<p><b>R28 Insufficient Smart Contract Control:</b> A custodian and/or relevant intermediary does not have the requisite control over the digital asset securities / tokens or smart contracts functions.</p>	<p><b>C28-S Smart Contract Roles:</b> Define standard roles to determine who can access smart contract data and functions.</p> <p><b>C29-S Emergency Stop:</b> Ensure that smart contracts have an embedded kill switch or process to halt all activity, which can be accessed by a role with elevated permissions.</p> <p><b>C31-S Token Pause:</b> Ensure that a user can freeze or pause activity for all or some of the token inventory, controlled by either the agent of the investor or a role with elevated permissions.</p>	<p>Token standard and smart contract configuration were used to bring off-chain KYC compliance rules into on-chain token configuration, enabling the operations to halt or pause any token activity when participants did not match KYC criteria (e.g., jurisdiction). This ensured that only a role with elevated permission (compliance officer) could freeze or unfreeze activity over the token factory.</p>

# NTW-CG

## On-chain deposit accounts using wCBDC for settlement

*a new model under experimentation*

FRANKFURT – JUNE 2024



Contact: Guénolé de Cadoudal  
digitalassetsgroup@ca-cib.com

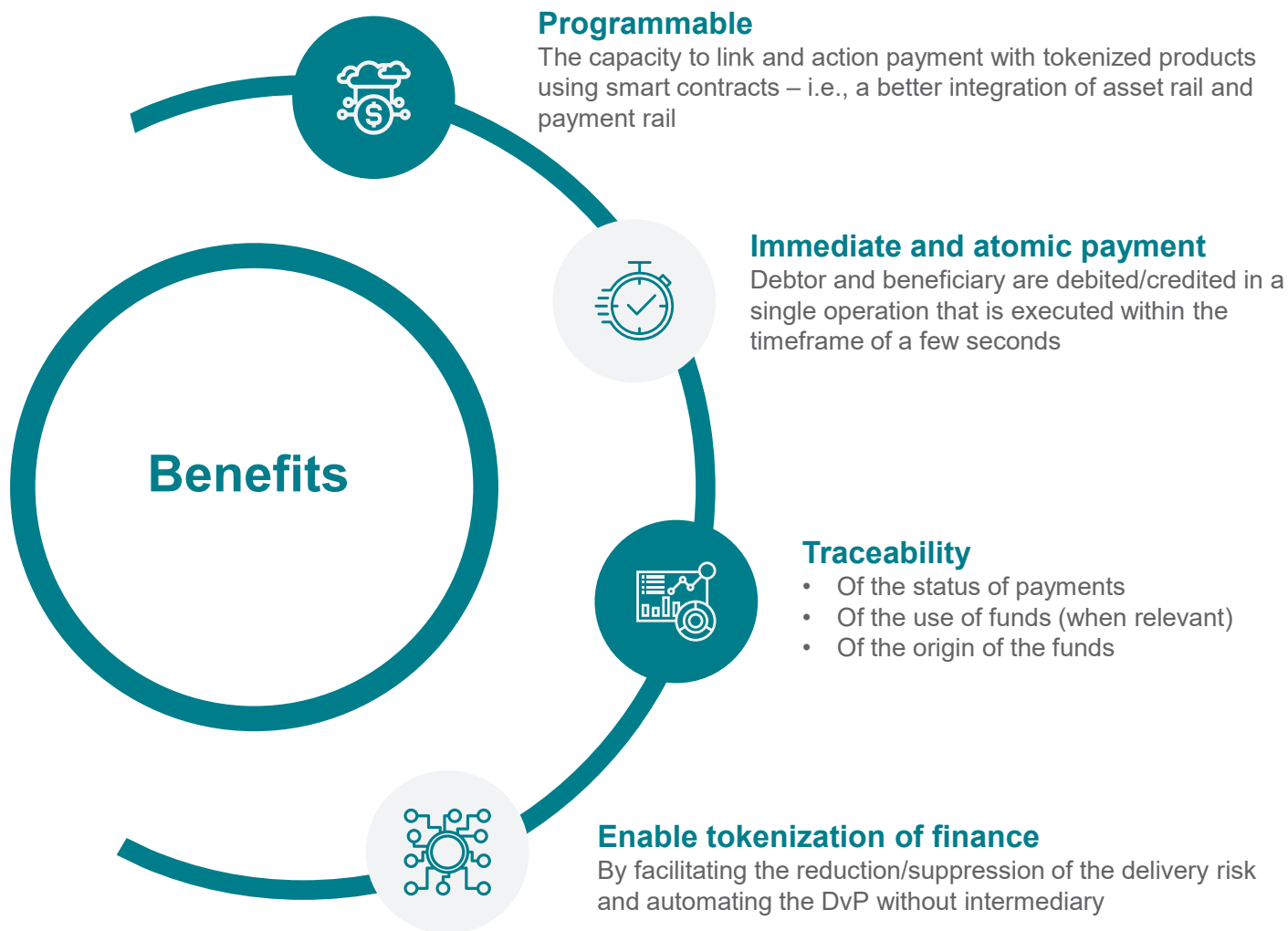
DISCLAIMER

This document is provided as is with no commitment from its authors that the information provided are verified or will not change. This document reflect the current state of reflection on this model and still requires further investigations and testing.

# Table of Contents

- 1 Benefits of wholesale payment rail on chain
- 2 so|cash : testing an alternative approach
- 3 Fragmentation of the liquidity and operational frictions
- 4 The history and status
- 5 The use cases under discussion

# 1. Main benefits of wholesale on-chain payment rail



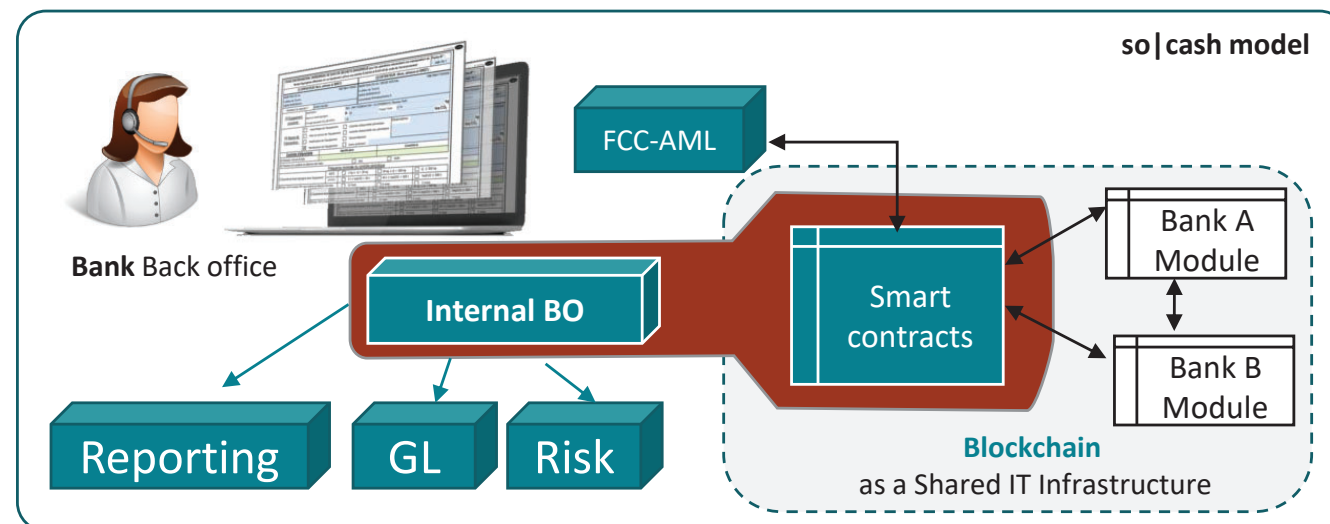
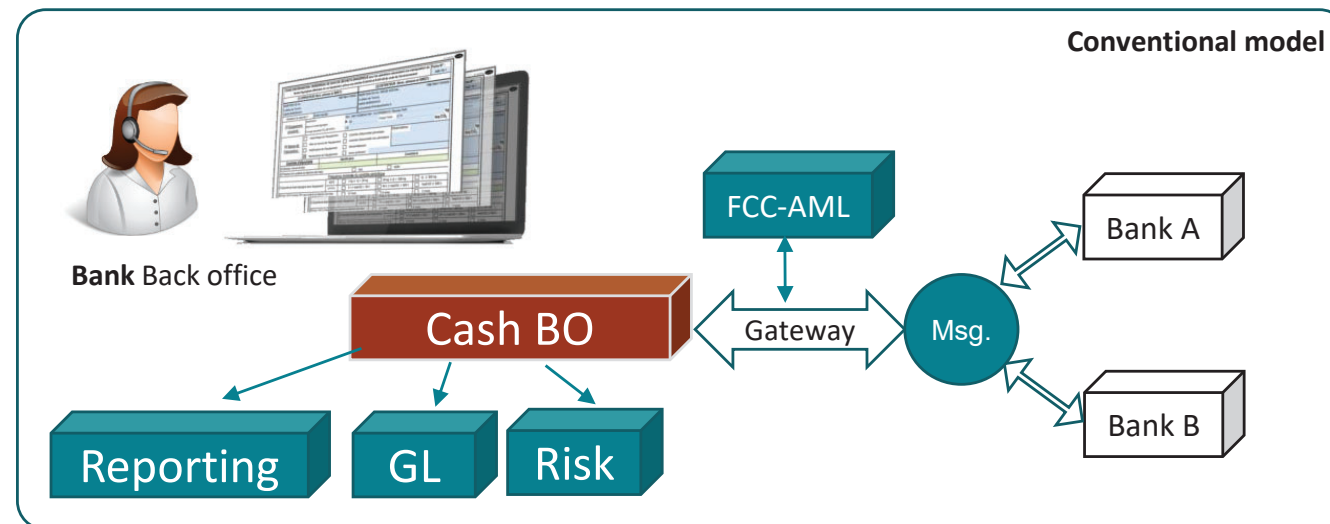
## WHILE



- Banks need the liquidity from their clients
- Banks expect to keep the commercial relationship with their clients (KYC)
- Not all banks' clients have access to Central Bank Money
- Banks prefer to avoid “vendor locking” solutions

## 2. so | cash: testing an alternative approach *(a standard - not a platform)*

Not tokenizing an asset or liability but using the DLT as an IT infrastructure



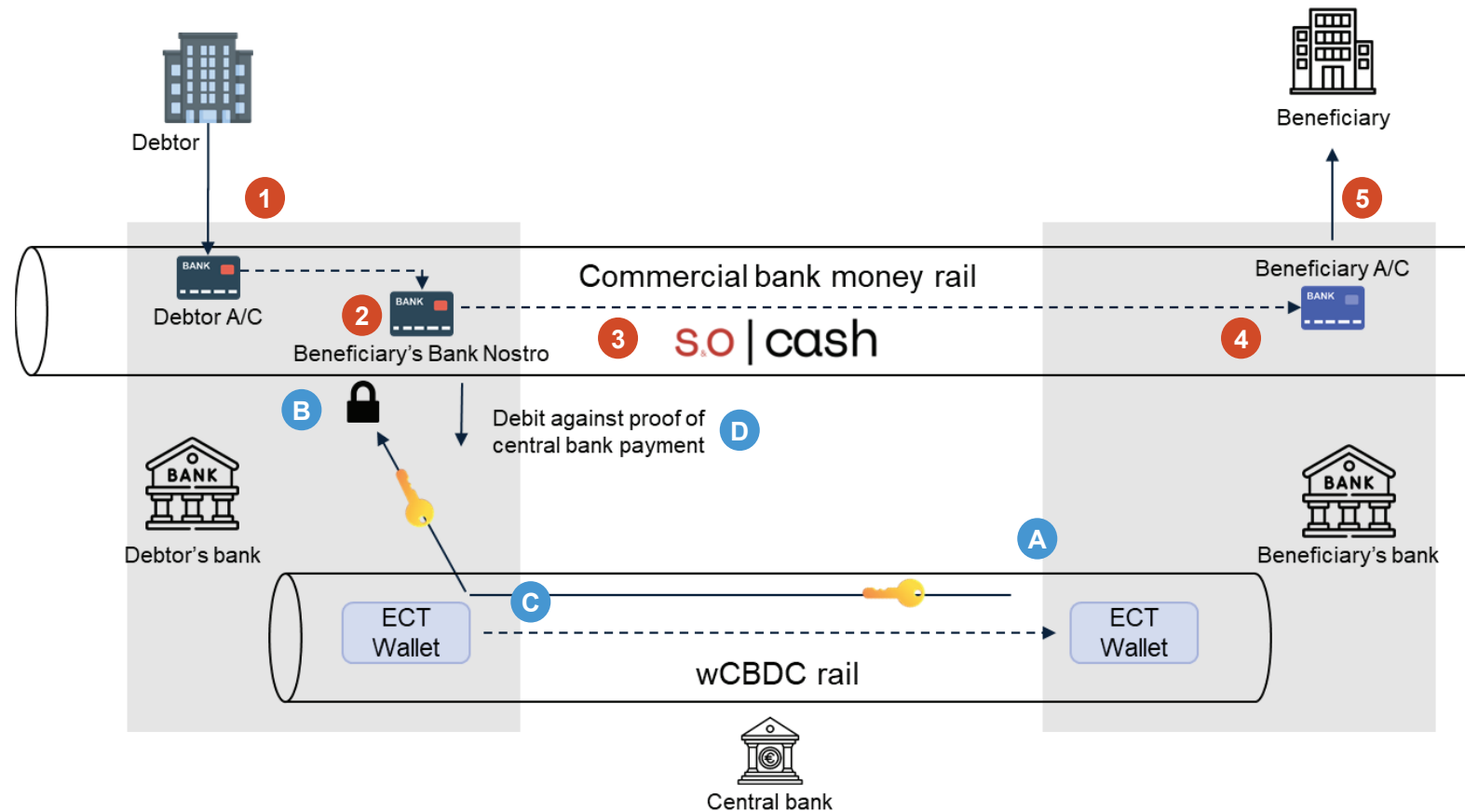
### What changes and what remains?

- **Banks back-office system** that manages the client's bank accounts is (partly) **on-chain** (accounts, transactions, acquisition ...)
- **Banks can communicate directly** inside the Blockchain instead of message-based communication.
- **Each bank remain responsible for its own smart contracts** (back-office module on-chain) – directly of using a provider
- **Account owners can view and access their account on-chain directly** (or via a provider) without going through the off-chain bank IT system
- **Architecture moves** from a message-based approach to a program call approach



## 2. **so** | cash: testing an alternative approach *(a standard - not a platform)*

Illustrating an end-to-end payment flow



### Process flow of the payment

- [so|cash atomic on-chain interbank transfer](#)
  - 1 Request for payment in Euro directly on its account (or via its bank)
  - 2 Debtor's bank smart contract debits the client account and credit the account of the beneficiary's bank
  - 3 Debtor's bank smart contract calls the smart contract of the beneficiary's bank
  - 4 Beneficiary's bank smart contract checks instantly its account is credited and credits the beneficiary's account
  - 5 Beneficiary is informed of the credit immediately by reading the chain
- 
- [HTLC process between so|cash and wCBDC](#)
  - A Beneficiary's bank initiates a payment request in CBDC (creating a secret)
  - B Beneficiary's bank locks its cash in its *nostro* account with the Debtor's bank (so it cannot be spent)
  - C Debtor's bank pays the beneficiary's bank in central bank money and receives the secret
  - D Debtor's bank unlocks the beneficiary's bank cash with the secret and debits the account

### 3. Fragmentation of the liquidity and operational frictions *(first level analysis)*

#### Liquidity fragmentation

- **Different issuers:** stablecoins (EMT in MiCA) from different issuers are not equivalent and could lead to the need of reserves in multiple coins
- **Non-transferable:** tokenized deposits (as crypto-assets) at one bank cannot be given to another bank (KYC compliance) leading to constraints in liquidity circulation
- **In Europe, non-interest bearable:** under MiCA, EMT usage will not likely be a treasury asset leading to needs to move positions back and forth.

#### Integration costs / Provider dependency

- **On-ramp/Off-ramp friction:** accessing the tokenized form of cash from conventional requires the purchase process before using them. Under MiCA, the lack of interest generation will lead to re-conversion
- **Multiple implementations:** dedicated payment networks are not all similar/compatible leading to either integration efforts or dependency on a provider

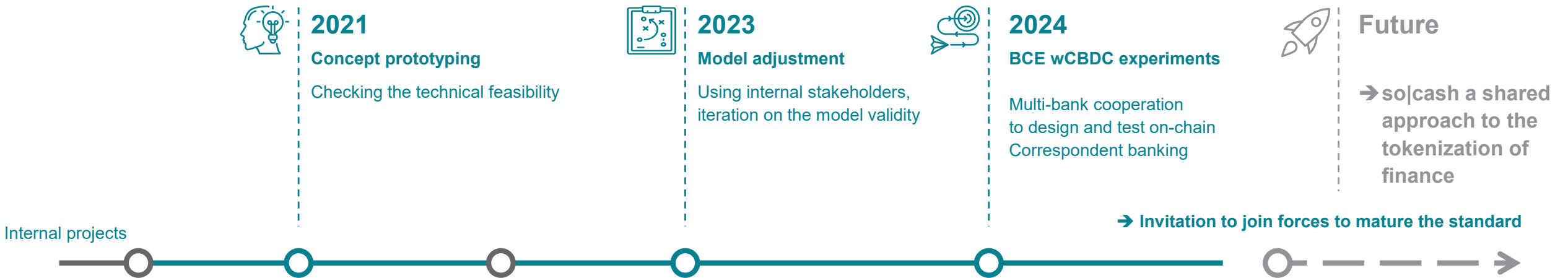


#### so|cash perspective on these issues



- **Copy of the current banking model:** so|cash accounts are the primary records of bank's liabilities toward clients and banks can use these deposits as part of their funding in accordance with liquidity ratios
- **Not a token:** with so|cash model, client deposits are recorded in accounts held on a Blockchain based back office system. Deposits are not transferred to any one, but accounting entries are made between accounts.
- **Compatibility with multiple interbank settlements:** banks transfer their liquidity in any currency that has an automatable (HTLC like) payment rail
- **An open-source standard:** any actor can use/implement the standard without a license cost, without a private IP.
- **Fostering competition and innovation:** tech providers can compete to offer tools to clients and banks. Banks can compete to leverage real time payment for cash management services. As an elementary brick of the financial system, new products and services can emerge.
- **Less friction:** as the chain exposes bank accounts (with real IBAN), payments can be done from and to any other existing accounts (on-chain and off-chain), and the model will be made ISO20022 compatible.

# 4. The history and status of s.o | cash model



# 5. Use cases under discussion that can be leveraged by s.o | cash

**Enhance ability** to manage and optimize liquidity in real-time, providing continuous access to funds and seamless financial operations



**24/7 Corporate Treasury**

**Immediate consolidation** and optimization of a company's cash resources across multiple accounts, enhancing liquidity management and reducing borrowing costs



**Real-time cash pooling solution**

**Immediate settlement** of cross-border transactions at competitive exchange rates, improving cash flow and reducing currency risk



**Instant payment with FX**

**Increase security** and efficiency in processing invoices, reducing fraud risk and enabling faster and more transparent transactions



**Tokenized invoices payment**

**Secure transfer** of funds, ensuring faster settlement and reduced counterparty risk (MLETR)



**Cash leg of tokenized trade finance documents**



# Governance & Risk at DLT- Infrastructures

Jonathan Leßmann, SWIAT

E-Mail: [jonathan.lessmann@swiat.io](mailto:jonathan.lessmann@swiat.io)

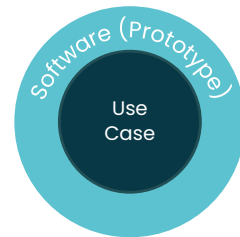
# Moving from PoC to full production



## World of Proof of Concepts

*From Zero to One*

Building up Know-How



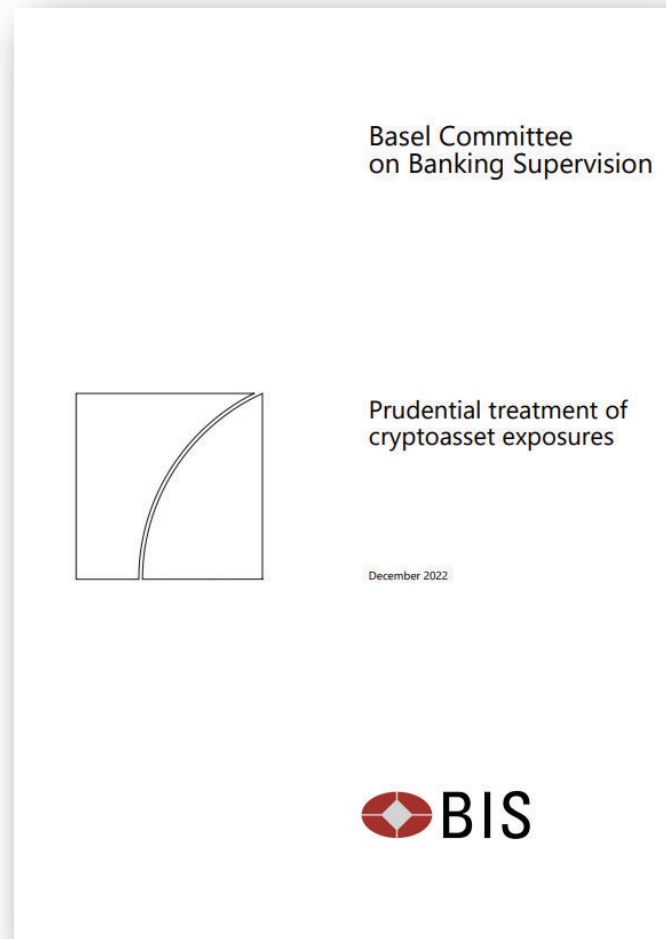
## Scaled Production

*From One to Many*

Competitive Advantage



# SC060, key for scaling digital assets



## **Focus:**

Prudential treatment of bank's exposures<sup>1</sup> to cryptoassets, including tokenized traditional assets, stablecoins and unbacked crypto assets.

## **Timeline:**

Scheduled for January 2026

1. "exposure" includes on- or off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks



# A full blockchain assessment is required



SCO60 requires banks to not only analyze the asset, but as well the blockchain network and it's involved entities on weaknesses, risks, and business continuity.

Can the network mitigate and manage material risks for:

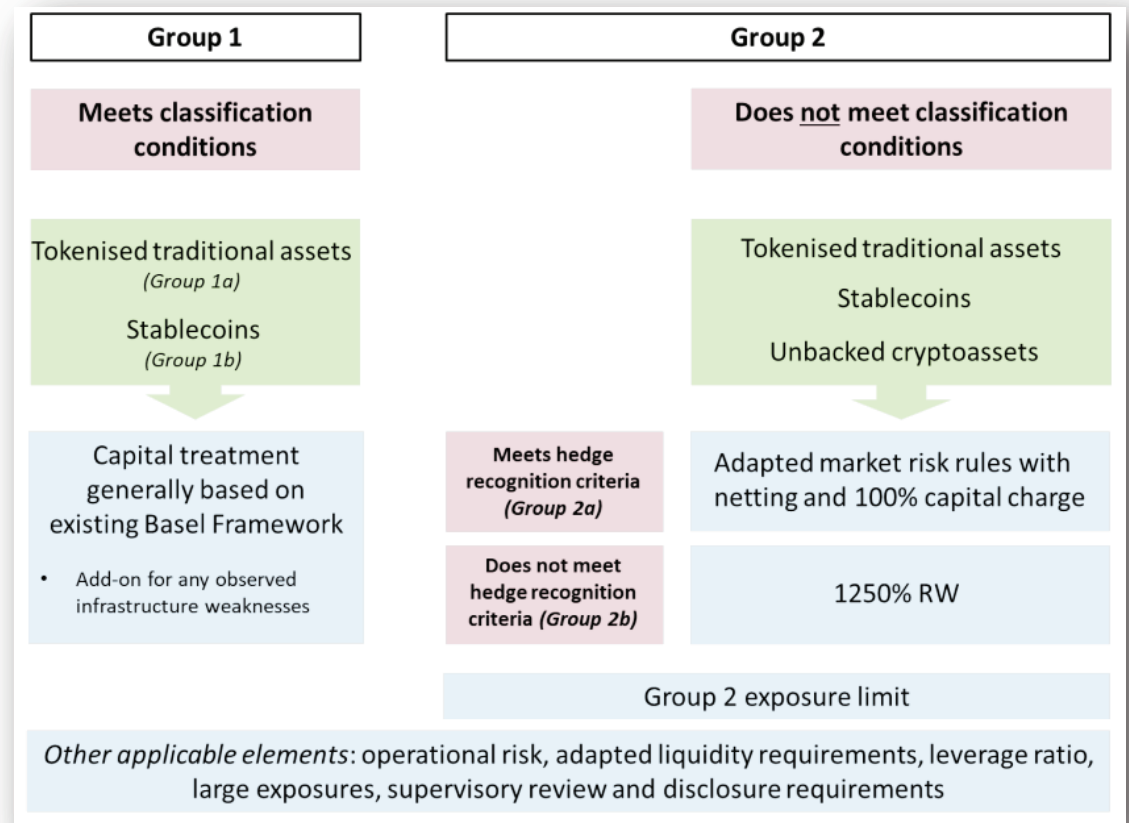
- Asset transferability
- Settlement finality<sup>1</sup>

Are there well-defined elements regarding operational structure, degree of access, technical roles of nodes, validation and consensus mechanism

Are entities with key roles regulated and supervised or have an appropriate risk management in place?

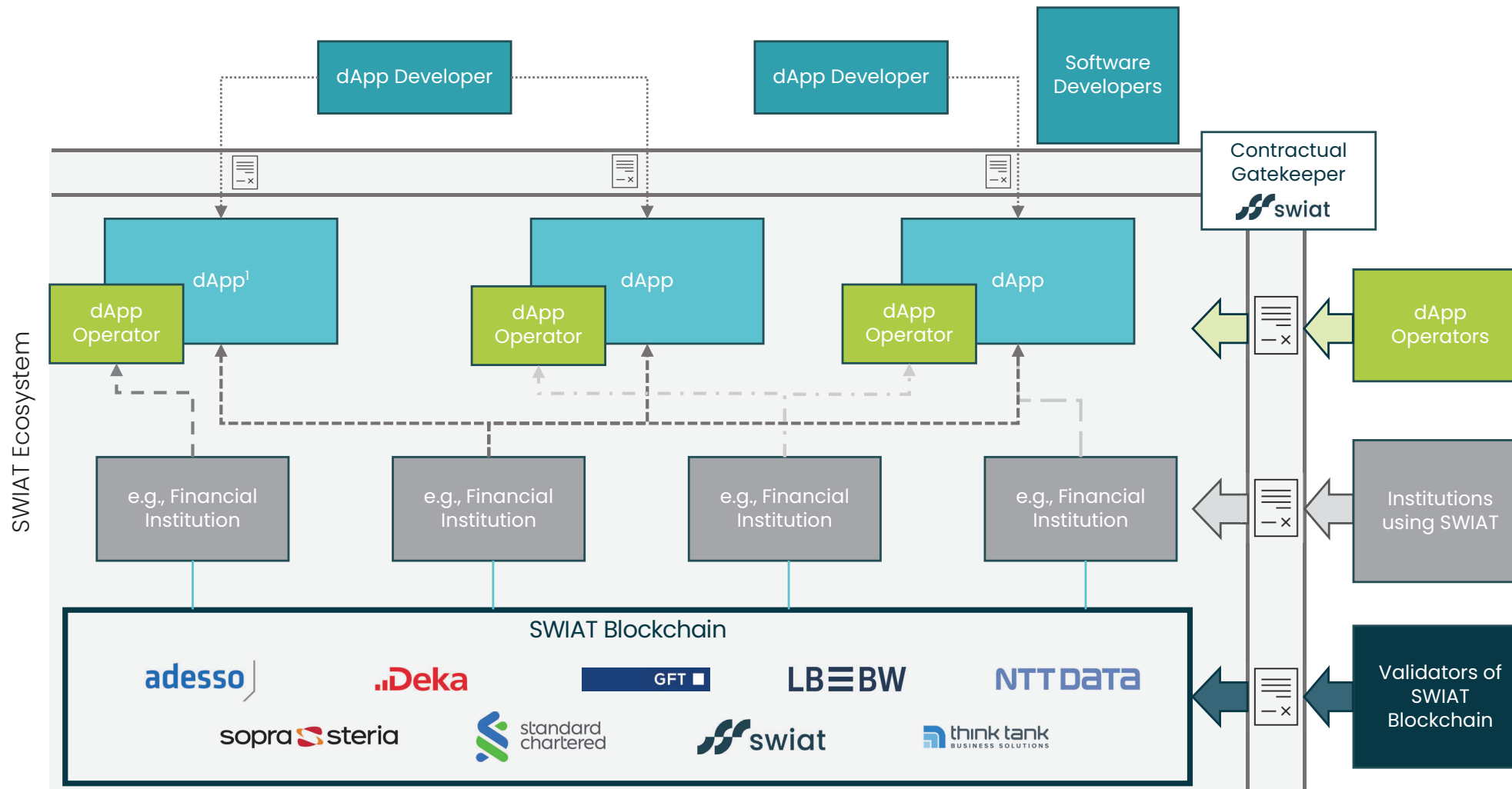
Is a comprehensive governance framework disclosed and in place?

*Different treatments based on classification criteria*



1. Analysis should differentiate between the legal term 'settlement finality' and settlement finality from a technological standpoint in a blockchain

# Ecosystem-Architecture of SWIAT



## Network Terms cover:

- Entry conditions
- Description of roles and responsibilities
- Consensus mechanism
- Reward description for validators
- Framework for policy changes
- Reliability and BCM and more ...

# SWIAT, a regulatory-compliant blockchain for the financial industry



- ✓ **Allowing for SCO60 classification into Group 1, avoiding additional RWA-requirements and capital charges for banks and allowing better secondary market activities**
- ✓ **Open for 3<sup>rd</sup> Parties to deploy their own solutions onto the SWIAT Ecosystem**
- ✓ **Clear distribution of roles and responsibilities – at any time**
- ✓ **Comprehensive and exhaustive governance framework**

More details like a Glossary or the full Ecosystem Diagram can be provided.

# Contact



## Jonathan Leßmann

CMO & Plattform Strategie

E-Mail: [jonathan.lessmann@swiat.io](mailto:jonathan.lessmann@swiat.io)

Web: [www.swiat.io](http://www.swiat.io)

# Digital Assets Experimentation: Interoperability Findings



Product and Innovation  
June 2024

## Since 2021, Swift has led a series of experiments to demonstrate interoperability with CBDCs and Tokenised Assets

June 2024  
Digital Currencies  
and Assets  
Experimentation:  
Recent Results

### CBDCs

**Q4 2021:** initial exploration of interoperability models for forthcoming CBDC networks (including a potential interlinking solution)

**Q3 2022:** CBDC Sandbox Phase 1: demonstrated an interlinking solution prototype ('Swift Connector') to connect CBDCs and payment systems

**H2 2023:** CBDC Sandbox Phase 2: explored additional use cases (DvP, Trade, FX, LSM) for interlinking solution with nearly 40 Central & Commercial banks

**Q1 2024:** Issued report with results of CBDC Sandbox Phase 2

### Tokenised Assets

**Q2 2022:** 1<sup>st</sup> set of experimentation to connect multiple private tokenization platforms (Citi, Clearstream, NT) using Swift messages to mint, burn, and transfer tokens

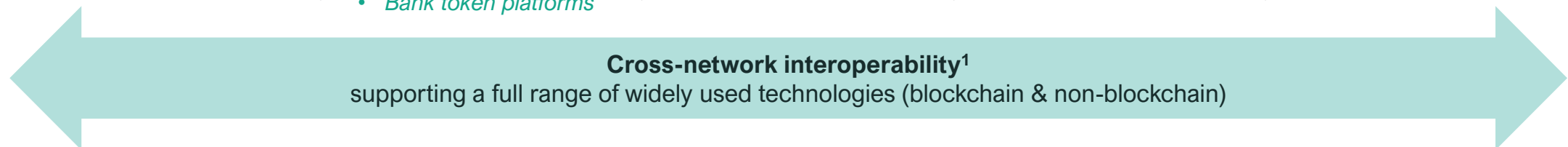
**Q2 2023:** follow-up 'Blockchain Interoperability' experiment w/ 13 FI/FMI and Chainlink to extend scope of our interop POCs to public blockchain (test) networks (*report published August 2023*)

# Our experimentation is active across CBDCs, tokenised deposits and tokenised assets

Whilst exploring cross-network interoperability as an enabling capability

June 2024  
 Digital Currencies  
 and Assets  
 Experimentation:  
 Recent Results

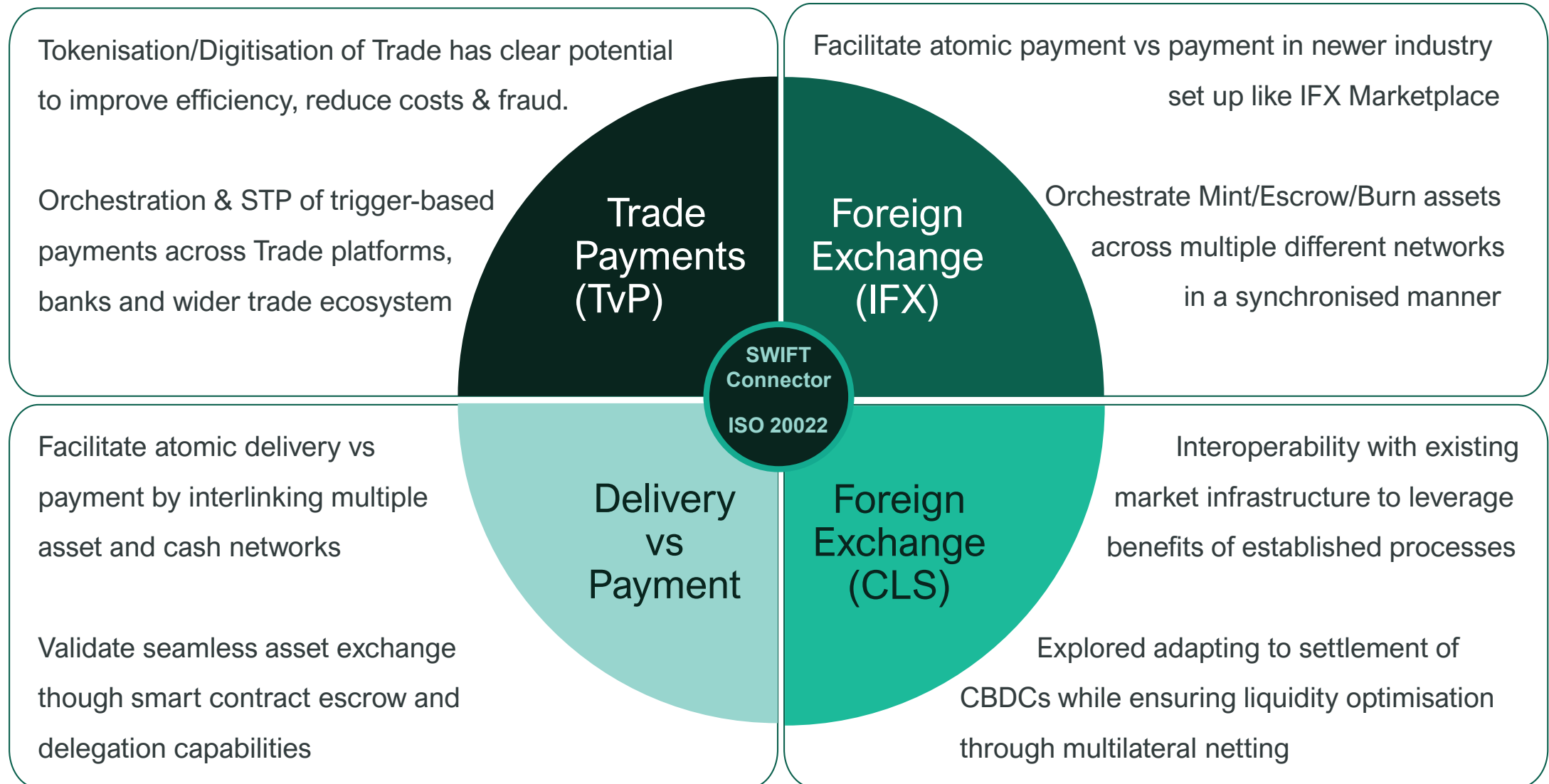
Public Sector		Private Sector		
Digital Currency		Digital Assets		
CBDC	Tokenised Deposits	Asset-backed Stablecoins	Tokenised Assets	Crypto assets
<ul style="list-style-type: none"> <li>✓ Regulated 'out of the box'</li> <li>✓ Strong engagement from the Swift community</li> <li>✓ Swift can connect into cross-border payment system</li> </ul> <ul style="list-style-type: none"> <li>• <i>Swift Connector</i></li> <li>• <i>Sandbox Phase 2</i></li> </ul>	<ul style="list-style-type: none"> <li>✓ Claim on issuer (regulated banks)</li> <li>✓ Compliance w/ existing legal &amp; regulatory</li> <li>✓ Reinforces role for commercial banks</li> <li>✓ Fragmentation of bank coins likely, potential Swift role</li> </ul> <ul style="list-style-type: none"> <li>• <i>Regulated Liability / Settlement Network (RLN / RSN)</i></li> <li>• <i>Bank token platforms</i></li> </ul>	<ul style="list-style-type: none"> <li>• Claim on issuer (unregulated non-banks mostly)</li> <li>• Lack clear regulation</li> <li>• Operate in closed-loop networks on public blockchains</li> <li>• Low interest from banks, but several starting to explore</li> </ul>	<ul style="list-style-type: none"> <li>✓ Existing regulated financial instruments</li> <li>✓ Growing global demand across the Swift community</li> <li>✓ Customers looking for Swift to be single access point</li> <li>✓ Potential to impact current Swift flows</li> </ul> <ul style="list-style-type: none"> <li>• <i>Tokenisation &amp; blockchain interoperability</i></li> </ul>	<ul style="list-style-type: none"> <li>• Unregulated assets lacking attributable value</li> </ul>



<sup>1</sup> can support other use cases (e.g., trade platforms)



## In our latest CBDC sandbox, we explored a range of additional use cases with 38+ central and commercial banks, demonstrating the potential value of interlinking new networks





## And our recent tokenised asset & blockchain interoperability experiment was based on findings from consultations with 25+ global institutions in the Swift community

Key Findings	Practicable Insights
<p><b>There is increasing investor demand for access to DLT networks and improve liquidity across these networks</b> For a range of benefits, institutional investors are increasingly looking for access to the assets, liquidity pools, and features enabled by blockchain networks</p>	<p>Over-time cross chain protocols and orchestration will be needed to unleash potential of DLT networks and liquidity optimization</p>
<p><b>The future will be “multi-chain”</b> To serve investors FI’s will need to connect and interact with multiple blockchain networks in a secure and cost-effective way,</p>	<p>There is a strong need to streamline how interactions with multiple DLT networks are done, and to decouple the technical aspects from business intents</p>
<p><b>Desire to re-use existing infrastructure where possible</b> Financial institutions prefer to leverage existing infrastructure to connect to a wide range of blockchain networks and applications where possible. This will help to simplify architecture and operations and minimize the cost of new investment and risk of tech obsolescence.</p>	<p>Adopting DLT networks will be a journey. Not every front, middle and back-office applications will be adapted at once, and interoperability with these applications is needed to enable progressive adoption</p>
<p><b>Preference for underserved and illiquid assets</b> Private market instruments and carbon credits represent the asset classes with the most potential benefit. While applicable for other assets including equities and bonds, existing infrastructure is relatively efficient.</p>	<p>It is not about migrating well-functioning market and instruments</p>
<p><b>Fundamental questions on security, privacy, compliance, and liability</b> More important than simply the technical transfer of tokens, addressing these more fundamental topics are what will enable institutions to securely and compliantly serve customers in a tokenized financial system.</p>	<p>Beyond technical aspects, there are questions to be addressed and framed around how we operate, how we define regulatory frameworks and how we bring institutional stability in the eco-system</p>

**Interoperability is hard – but necessary.** There is no single model, but this initiative gives us confidence that emerging networks can be supported through a standardised approach

**Guiding Principles for interoperability**

***Interlinked networks***

*Interlink new digital networks, agnostic to asset class and technology choices*

1

***Single point of access***

*Enable institutions to leverage existing channels to reach new networks and reduce overhead*

**Global Interoperability**

3

2

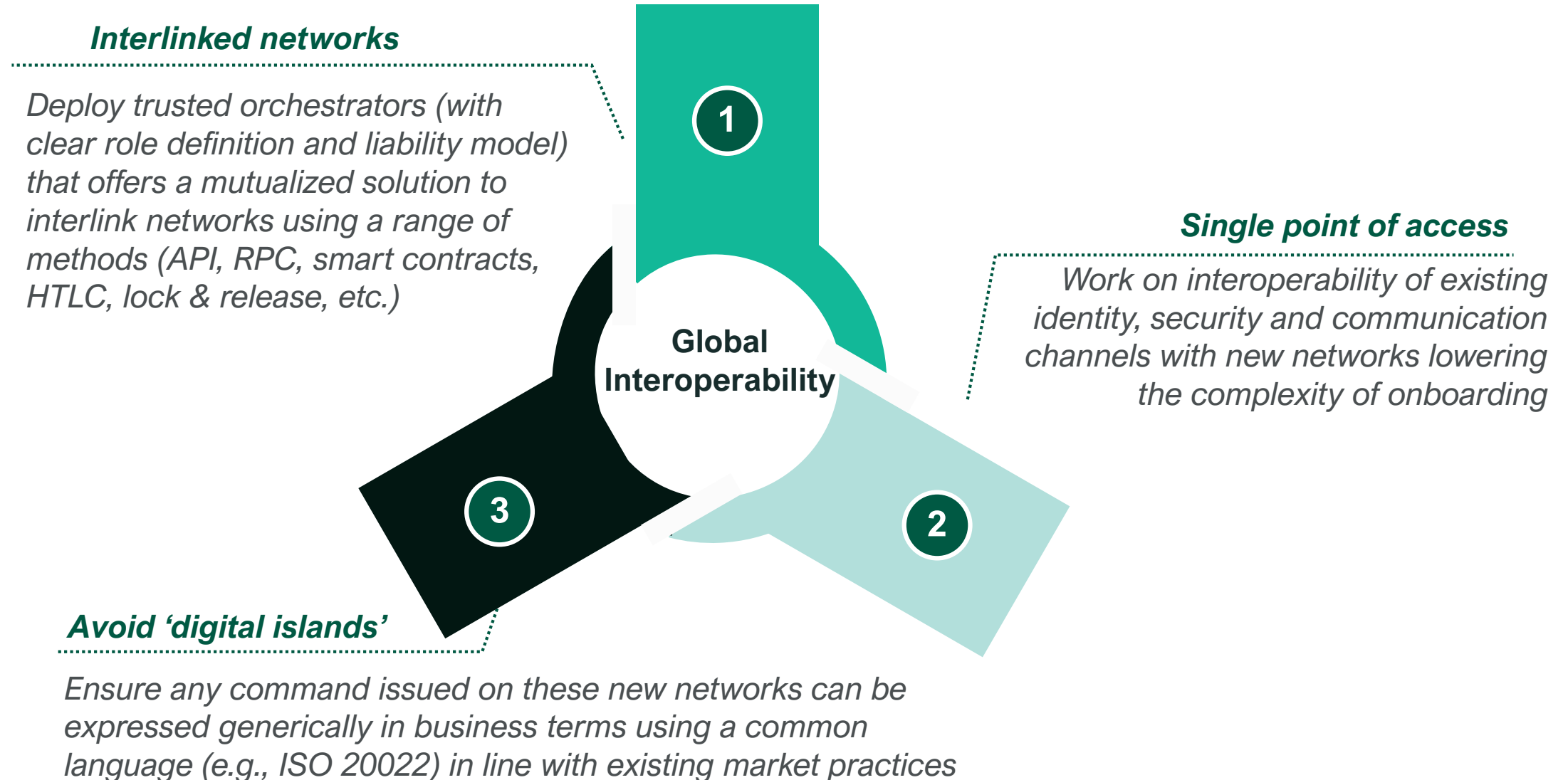
***Avoid 'digital islands'***

*Ensure new digital networks can not only connect to each other, but to the existing financial system*

June 2024  
Digital Currencies  
and Assets  
Experimentation:  
Recent Results

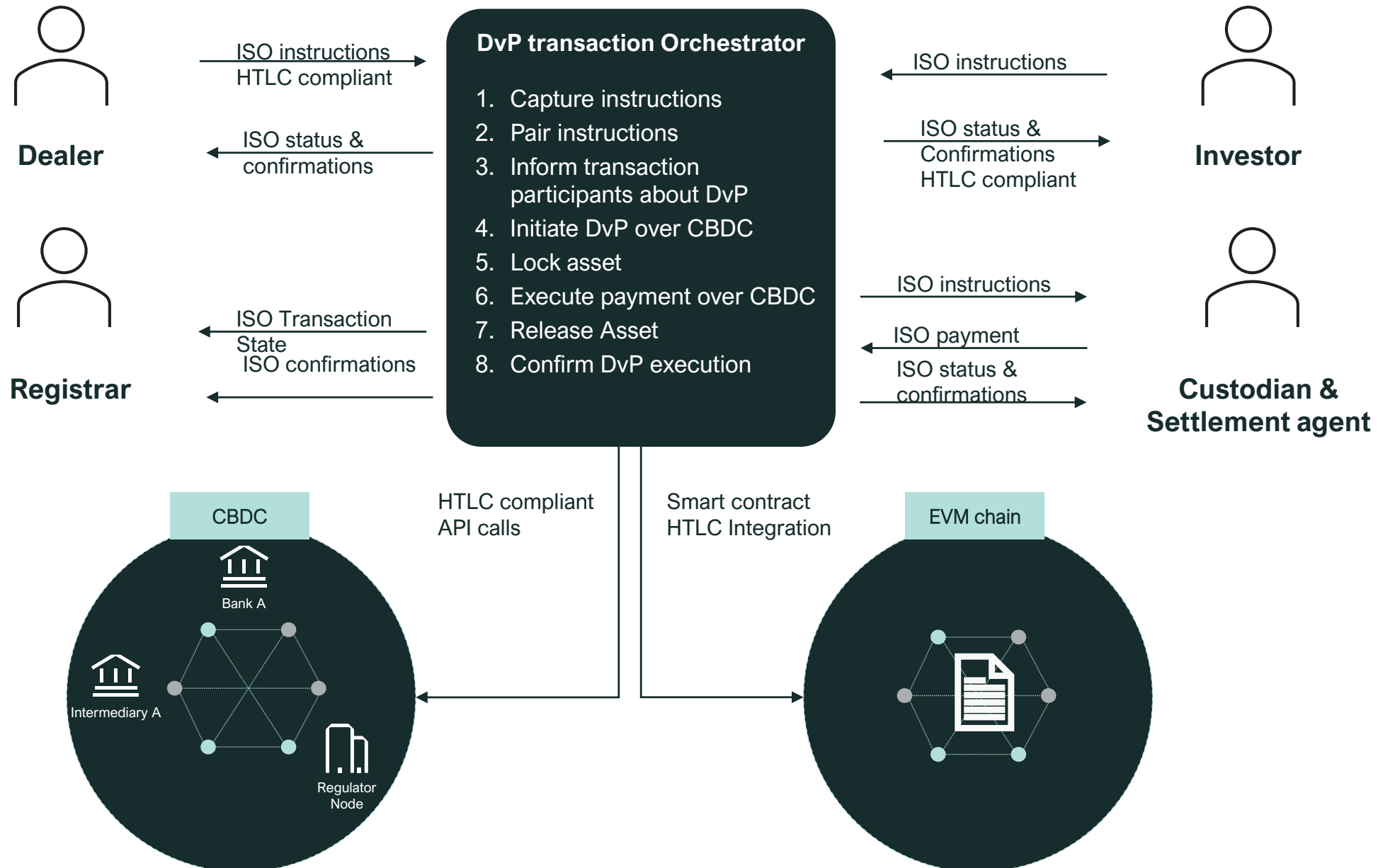
## What avenues is Swift exploring to satisfy these principles?

### Guiding Principles for interoperability

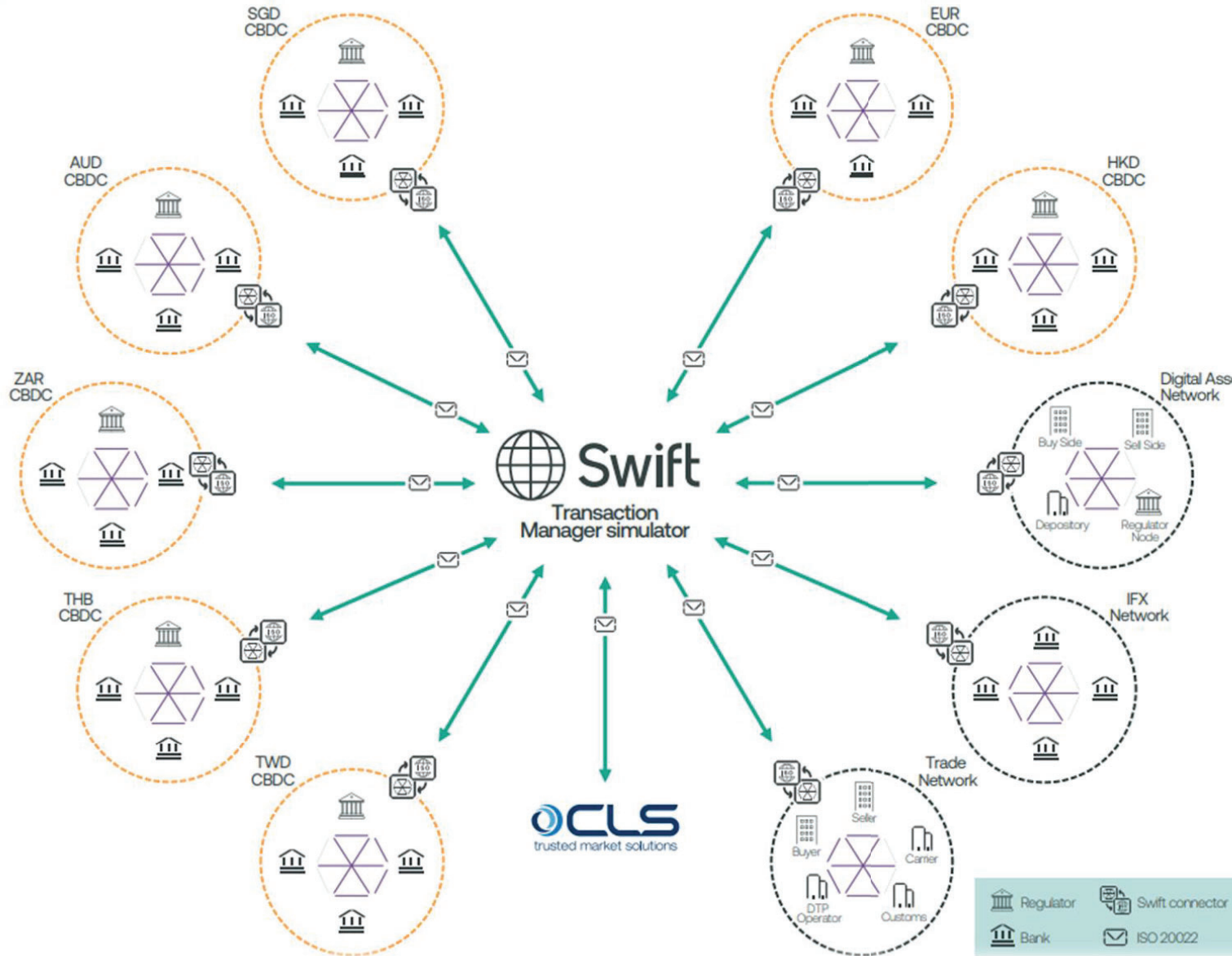


## Example of delivering on principles

ISO based orchestration of DvP among market participants with cash and asset ledger integration



## Sandbox set-up



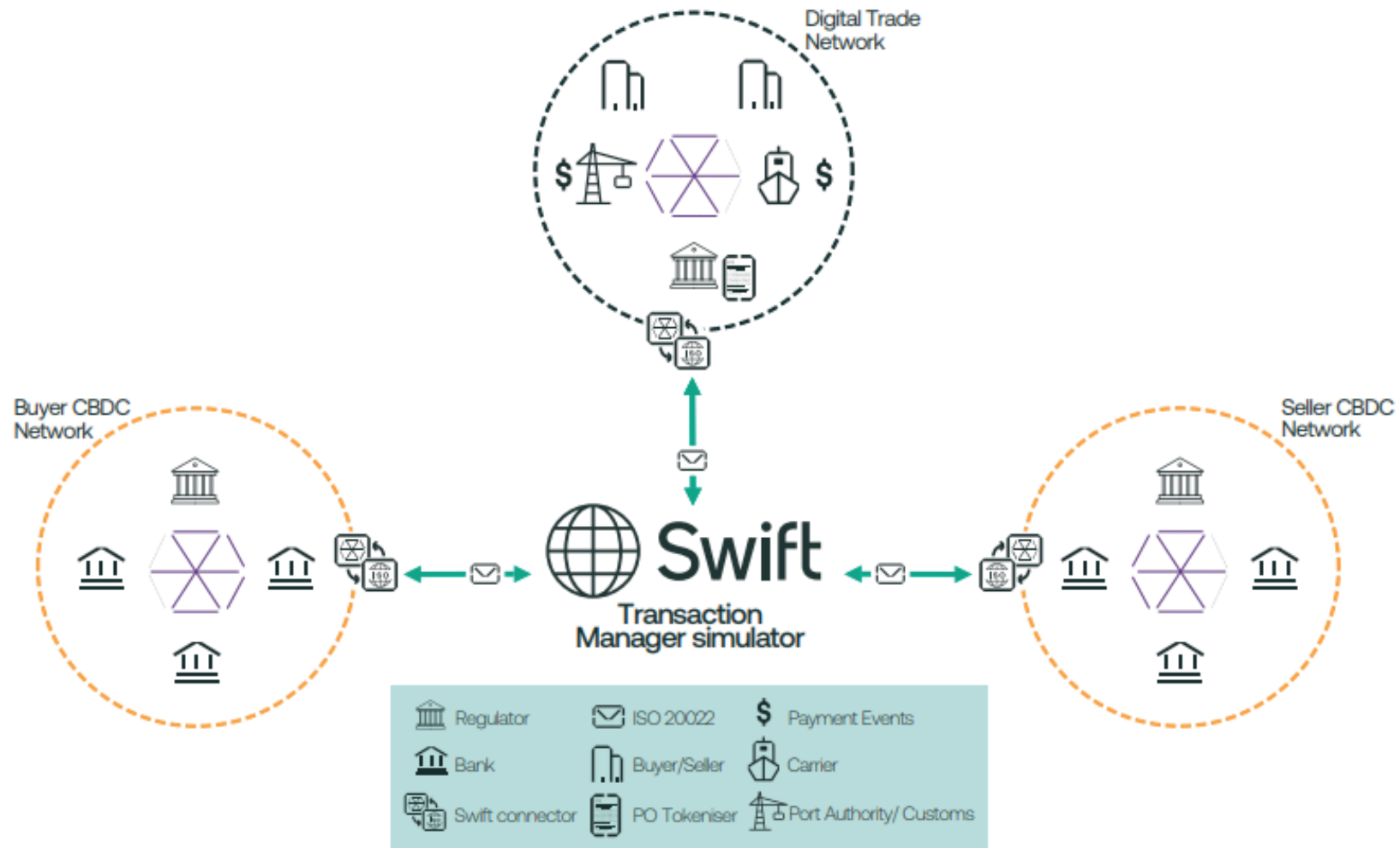
7 simulated CBDC networks

3 digital networks – Assets, IFX Network, Digital Trade Network

1 existing market infrastructure

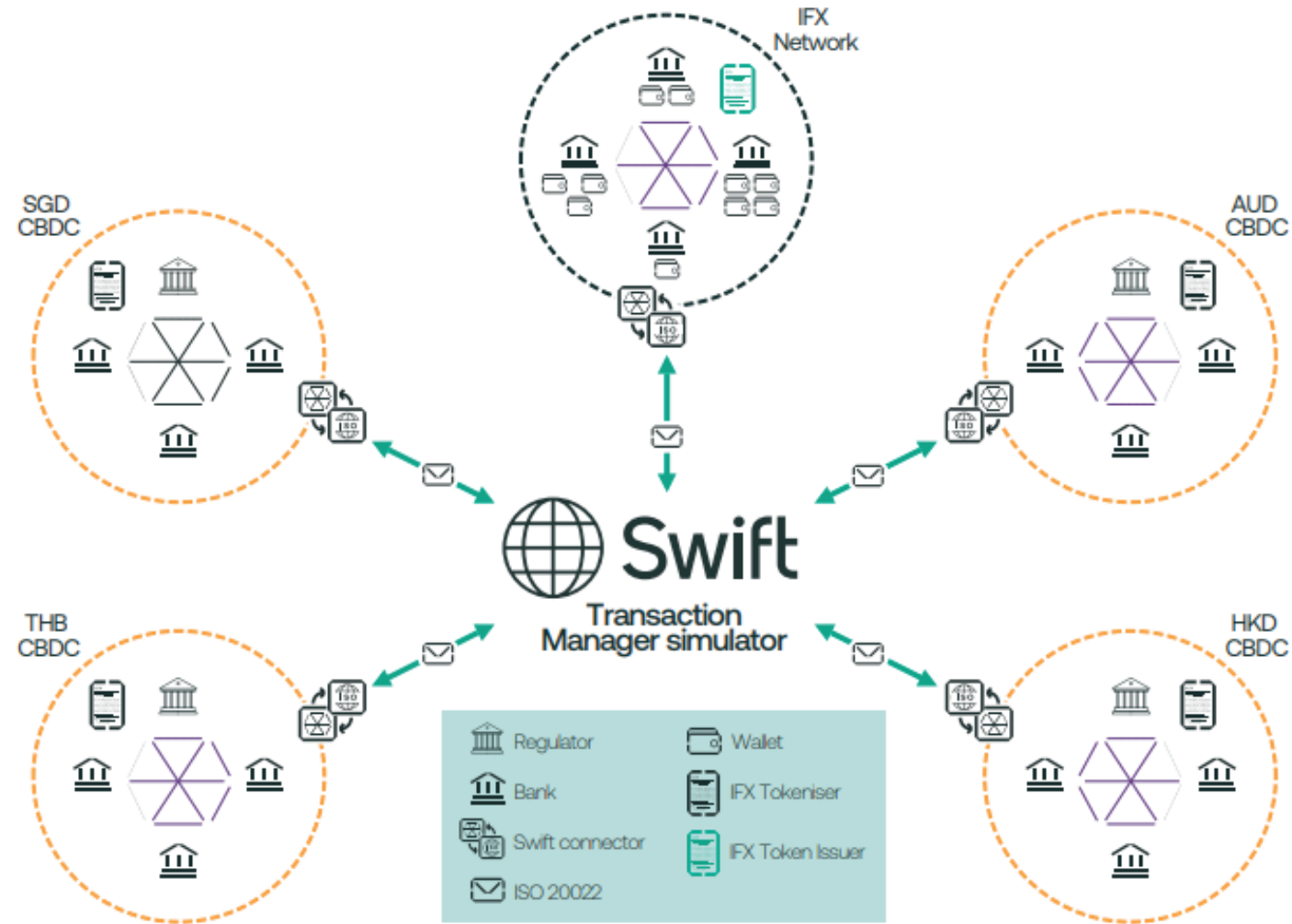
## Use Case1: Trade vs Payments

Explore interlinking and automation of complex trigger-based payment events across different networks.



## Use Case2a: FX – International Foreign Exchange Marketplace (IFX)

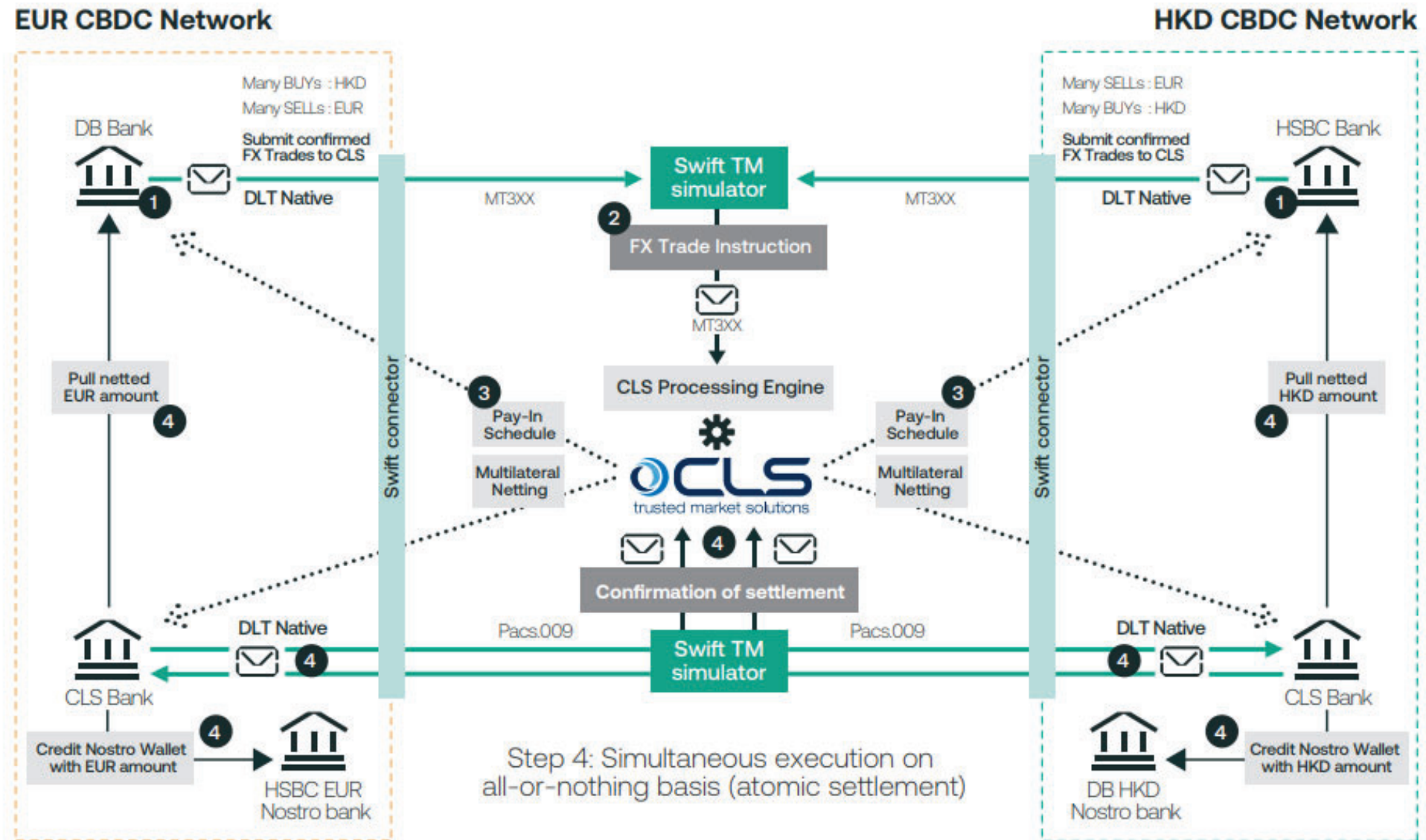
Explore a conceptual marketplace for trading and settlement of spot FX transactions between commercial banks using CBDCs



## Use Case2b: FX – CLS Processing and Settlement Engine

Leverages the capabilities of a CLS-like settlement engine to mitigate settlement risk for cross-CBDC FX settlement, with similar protection as for fiat currency.

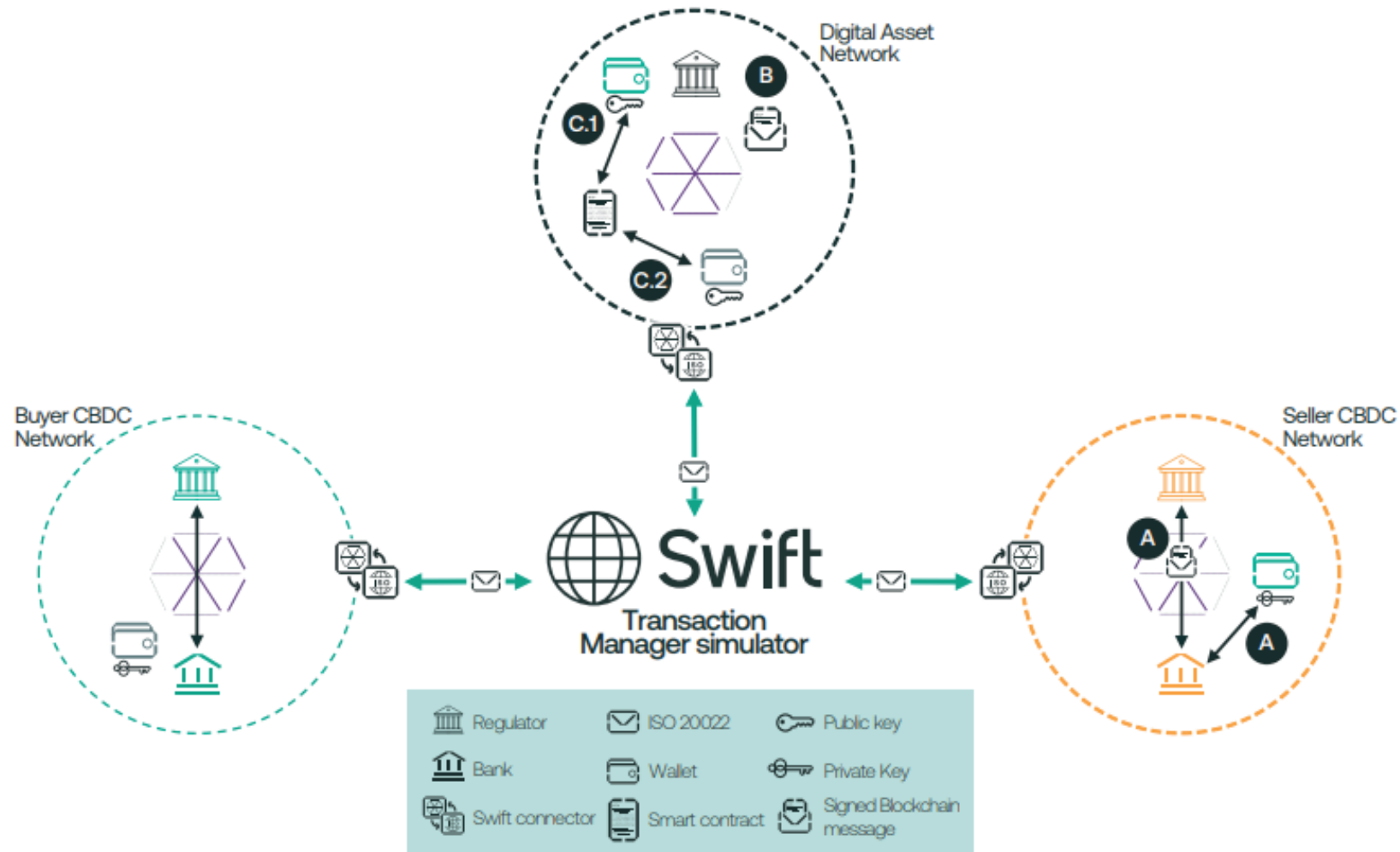
June 2024  
Digital Currencies and Assets  
Experimentation:  
Recent Results





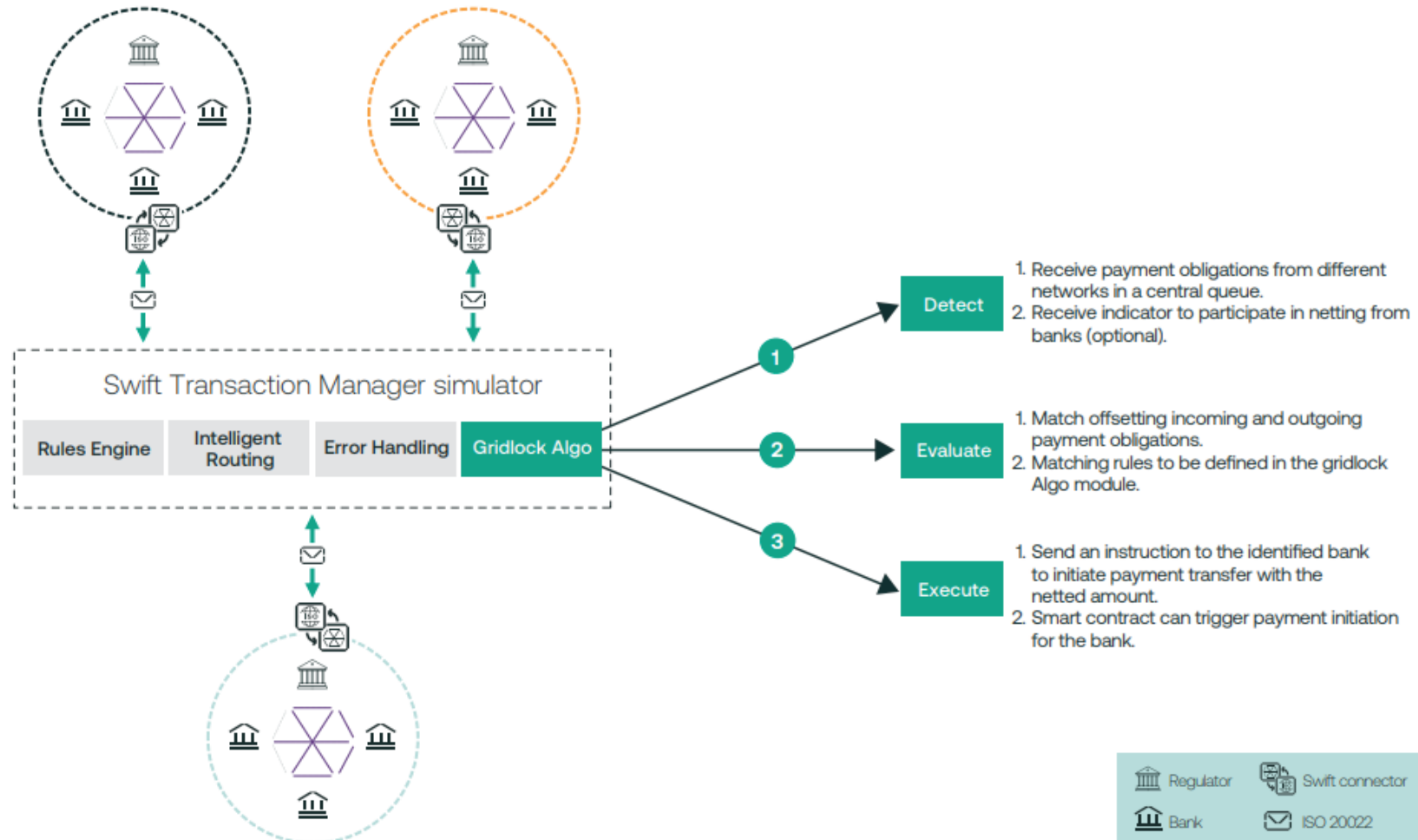
### Use Case3: Delivery vs Payments

Interlinking of multiple asset and cash networks to facilitate DvP in a cross-border setting where the buyer and seller are in different CBDC networks.



## Use Case4: Liquidity Savings Mechanism

Explore models which can help reduce the fragmentation of liquidity in the new digital paradigm. This was a paper-based exercise as the WG did not see this as an immediate priority.





**Swift**