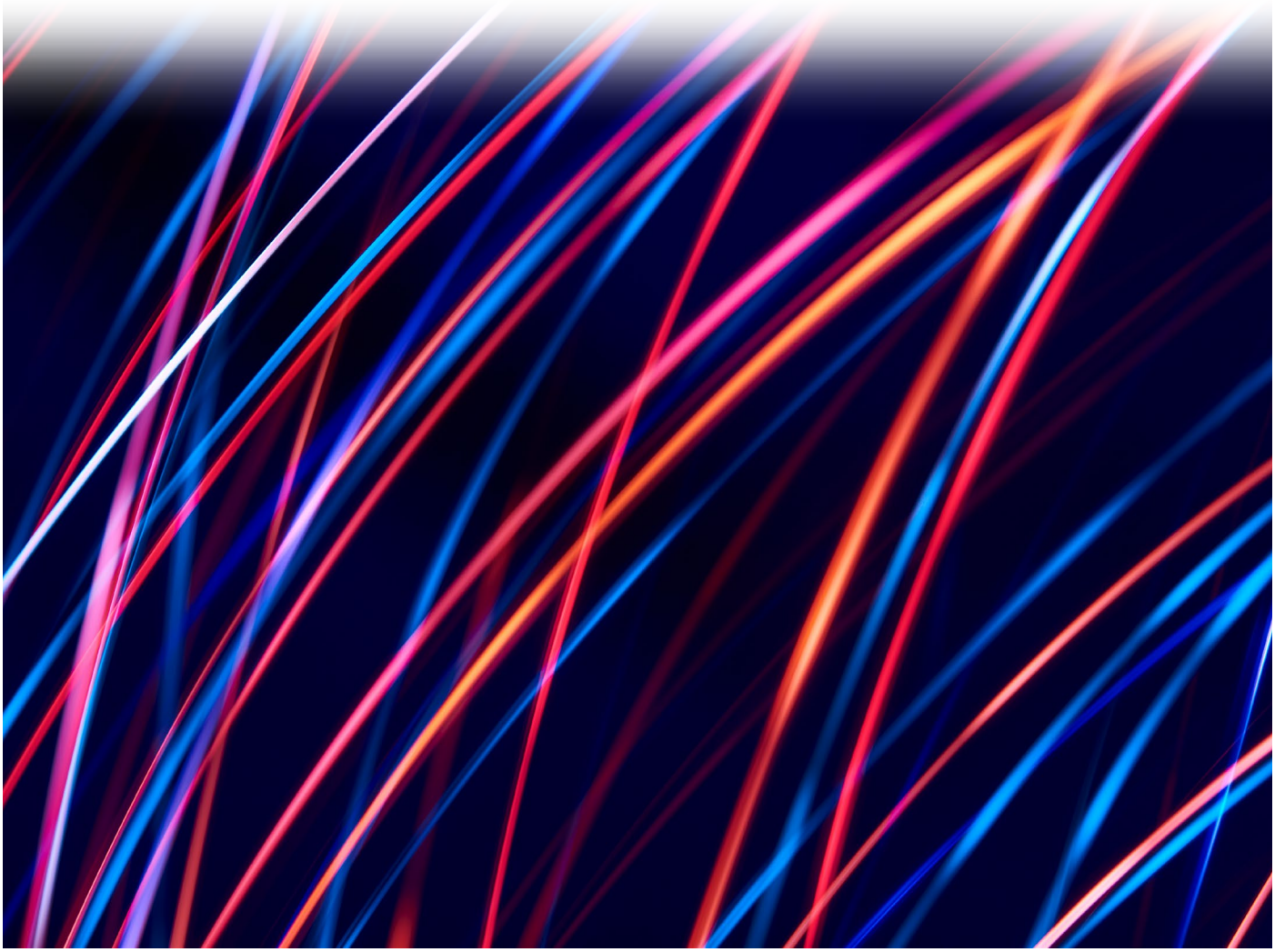


WHITE PAPER

# Building the Path Towards Digital Asset Securities Interoperability

February 2026

DTCC + CLEARSTREAM + EUROCLEAR + BOSTON CONSULTING GROUP

# Content

# Foreword

Dear industry colleagues,

Financial markets have long relied on **financial market infrastructures (FMIs)** to **reduce operational risk**, thereby providing **certainty in settlement**, **trust** in collateral management, and **market neutrality** in custody.

In that spirit, the Depository Trust and Clearing Corporation (DTCC), Clearstream, and Euroclear together with Boston Consulting Group (BCG) continue to collaborate to help the industry translate the promise of **Distributed Ledger Technology (DLT)** into **resilient**, **trusted**, and **market neutral production-grade services** for Digital Asset Securities (DAS). Our last joint effort introduced the Digital Asset Securities Control Principles (DASCP). These principles underpin our collective resolve to uphold the highest standards of integrity, security, and interoperability across the full lifecycle of DAS.

As is the case with other FMIs – **DTCC**, **Clearstream**, **and Euroclear have been crucial operators of the infrastructure that both enables and depends on interoperability** between markets to ensure effective and resilient capital market operations.

**Interoperability will be critical for the DLT markets to be successfully scaled** in the coming years. Without homogeneous treatment of assets across different infrastructures, the market may face significant challenges in adopting DLT rails at scale, potentially constraining global interoperability.

The framework presented in this white paper is a testimony of our day-to-day engagement for interoperability, to enable **harmonization**, drive **adoption**, and unlock **value**. It introduces a solution-neutral approach to interoperability, encompassing all dimensions such as data, processes, and roles/responsibilities.

We would like to help the market fully embrace the interoperability challenge in DLT, where – unlike in traditional finance – it remains an evolving frontier. This paper aims to give a **common taxonomy** to FMIs, regulators, market participants, and technology providers. Hopefully **interoperability** can guide discussions at every level. It will also provide a structure to classify initiatives, reveal gaps in interoperability coverage, and offer a reference point for further work on standards, required initiatives or operational risk management.

Our perspective is pragmatic – **traditional infrastructures and DLT will likely coexist for years**, market participants expect **continuity**, **inclusivity**, and uncompromised **security** as they connect. Ultimately, we believe that **industry collaboration remains the most effective way to build the ecosystem**.

We invite you to join us in advancing the work outlined here, so that tokenization improves outcomes for issuers and investors, while upholding the safeguards that underpin trust in global financial services.

Sincerely,


**Nadine Chakar**
*Managing Director and Global Head of DTCC Digital Assets*

**Jens Hachmeister**
*Managing Director and Head of Issuer Services and New Digital Markets at Clearstream*

**Isabelle Delorme**
*Managing Director and Head of Product Strategy and Innovation at Euroclear*

**Frédéric Brugère**
*Managing Director and Partner at BCG*

# Executive Summary

In 2024, DTCC, Clearstream, Euroclear, and BCG designed the **DASCP**[1], a comprehensive **risk control framework** to lay the foundation for safe and efficient adoption of DAS. Designed to be technology-neutral and asset-agnostic, the DASCP provided the industry with a common reference point to ensure legal certainty, operational resilience, and regulatory alignment. Since its publication, multiple market participants have leveraged the framework as a baseline for specific initiatives, helping to establish shared ground in an emerging ecosystem.

As **DLT adoption accelerates**, network **fragmentation has emerged** as one of the most pressing hurdles to adoption and the building of scale. Without interoperability, assets remain trapped in isolated pools, operations costs remain high for market participants, and both operational and regulatory risks remain elevated. **Market participants need rails that are safe, neutral and offer a high degree of reliability.**

**Interoperability is therefore essential for DAS to achieve their full potential** by simplifying basic use cases, scaling complex or siloed ones, and unlockin g new models, **while preserving mobility**, **liquidity**, **security**, **and fungibility** of assets.

This paper introduces an interoperability framework for capital markets. Based on five **capital market foundations**, **interoperability building blocks**, and concrete **use cases**, the framework is intended as a practical knowledge asset for FMIs, regulators, market participants, and technology providers. It offers a neutral reference to classify initiatives, reveal gaps and define priorities, while laying the groundwork for further standards and collaboration.

Digital asset securities are at an early stage of market development and provide a rare opportunity to **embed interoperability at the outset**, and **to accelerate progress** toward integrated TradFi and DLT networks.

## Key takeaways

### 1 Interoperability is a prerequisite for DAS adoption at scale.

The current interoperability limitations already create tangible frictions: operational costs are high, liquidity is fragmented, and both operational and regulatory risks remain while volume increases. Without overcoming these barriers, the expected benefits of digital asset securities will be difficult to achieve. Interoperability can enable the seamless execution of foundational use cases, facilitate the scaling of complex ones, and unlock entirely new opportunities. By ensuring the mobility, liquidity, security, and fungibility of assets, interoperability lays the foundation for widespread DAS adoption.

### 2 Interoperability extends beyond cross-DLT data integration.

Interoperability is built on 5 enduring capital market foundations: assets and liabilities, ownership, asset lifecycle and movement protocols, ledgers, and legal and regulatory compliance. These foundations have remained relevant for decades, and interoperability across all of them is essential to enable asset exchange across DLT or between DLT and traditional ledgers.

1. **DASCP**.

### 3 Interoperability requires industry-wide effort.

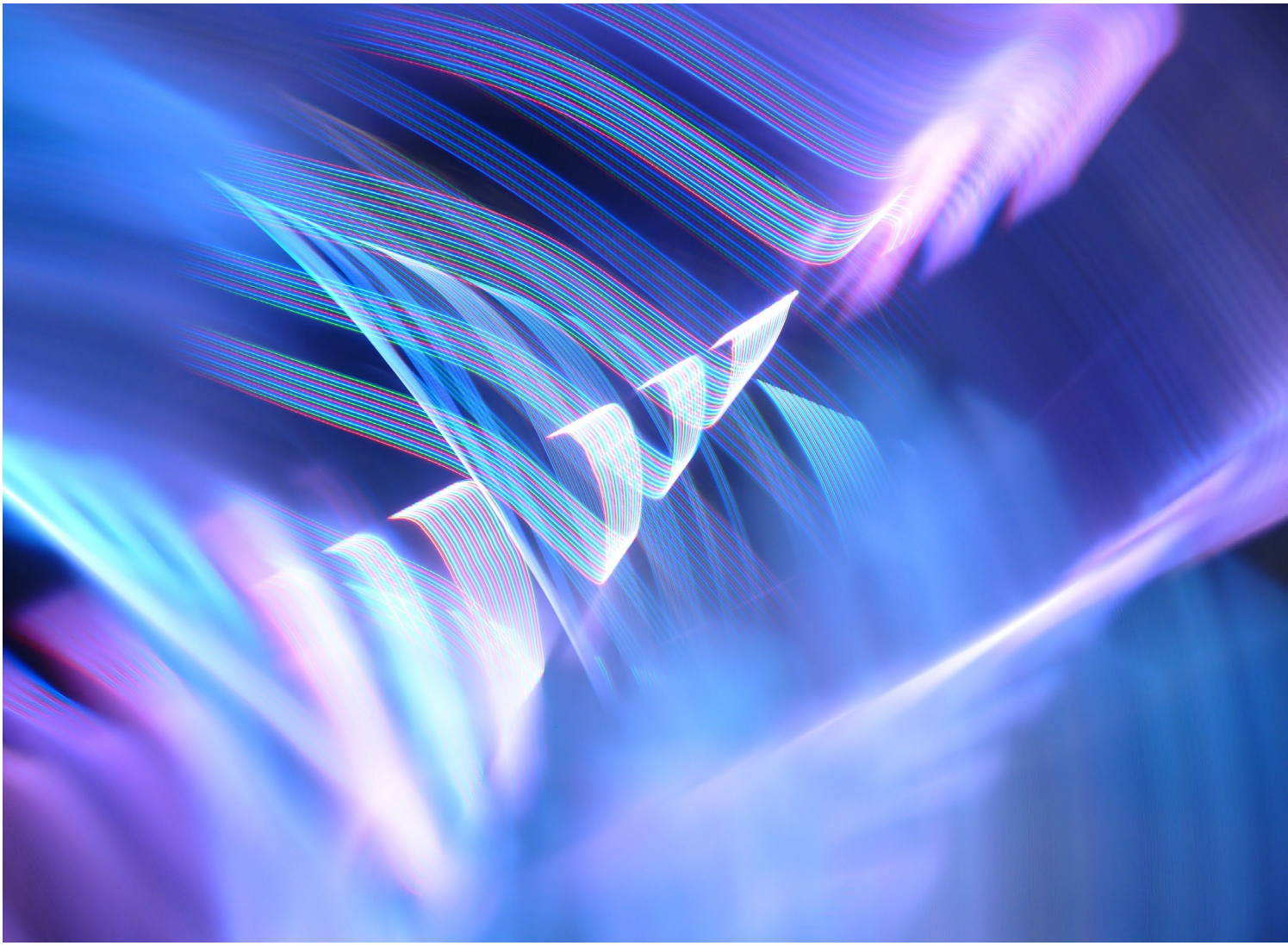
FMIs, regulators, market participants, and technology providers should build infrastructure and create standards around **data harmonization**, **process integration**, and **harmonization of roles** and critical functions. The framework described in this paper serves as a neutral reference point to convene this harmonization – helping establish a common taxonomy, anchor outcomes, classify initiatives, and highlight both coverage and gaps.

### 4 Interoperability should be advanced through a value-led approach.

Defining a market-level phased approach, with each phase focusing on a set of high-value use cases, enables actors to focus on the most critical interoperability areas and address the most important frictions. Each phase should be anchored in measurable outcomes and tested across multiple DLT and traditional finance ledgers. This prioritization leads the way to full scale interoperability over time.

### 5 Collective action today will shape resilient markets tomorrow.

In traditional finance, it took decades of effort and crisis management to harmonize market processes, data standards and integration approaches. To accelerate and reduce costs, market participants, technology vendors, regulators, and FMIs should come together to identify the salient priorities.



# The case for interoperability

## 2.1 The emergence of DLT in capital markets

While on-chain activity is still small versus traditional securities ($145.1 trillion for global FX and $126.7 trillion for global equity[2]), adoption is accelerating in specific segments.

Large-scale infrastructure is already in motion, with **$300+ billion in repo trades daily**, across the largest platforms.

**Regulatory momentum is also accelerating thanks to the intense effort of regulators.** Recent developments – including the U.S. GENIUS Act and U.S. CLARITY Act (both July 2025), the U.S. Securities and Exchange Commission's crypto rule overhaul (September 2025), and the EU's updates to the DLT Pilot regime and progress on the Wholesale Euro – can unlock key enablers and catalyze industry efforts for real-world adoption.

Underscoring growing institutional interest, **important market participants** from the existing financial market infrastructure and the largest financial institutions have not stayed on the sidelines.

At the same time, the underlying technology is evolving fast. In 2025 alone, both established players and newcomers launched new **Layer-1 (L1) and Layer-2 (L2) chains**, and tech actors **developed new solutions to support development**. Altogether, these developments could position "stablecoin rails" as foundational infrastructure across the full spectrum of DLT operations – from recording and settlement, to custody, asset servicing, and beyond. However, DAS are not at the core of these initiatives and it will be an issue going forward.

**$24B**

Depending on the source, the asset value of RWA tokens, enabling the investors to subscribe, hold and manage assets, is estimated at **$24 billion**[3].

**$1.3B**

Volumes for digital native securities are estimated to be around **$1.3 billion**[4].

**90%–120%**

Overall, the market has been expanding rapidly, with growth rates ranging between **90% and 120%** over the last year.

**Stablecoins**

**Stablecoins** – whose circulation **has grown by more than 75% year-to-date to $290 billion** – are increasingly filling the critical "cash leg" in transactions, linking tokenized instruments with real-world settlement.

2. **SIFMA**.
3. **rwa.xyz** ~$24B, retrieved on 4 Jan 2026.
4. **Business research insights**.

## 2.2 Strong potential, rising fragmentation

While momentum is building, and market activity has demonstrated the potential of DLT in capital markets, pilots and production implementations have also demonstrated that DAS can be issued, traded, and settled on-chain with a cash leg improving efficiency.

> Adoption is emerging across a fragmented landscape of DLT implementations within capital markets.

Today there are dozens of actively used public L1/L2 networks in capital markets pilots and products, alongside permissioned platforms. Each has its own smart contract language and runtime, consensus, and token standards, which multiplies risk and makes integration difficult.

This diversity is widening because **spinning up new chains keeps getting easier:** modular stacks and "rollup-as-a-service" providers allow institutions to launch bespoke L2s with configurable data availability, privacy, and permissions in weeks rather than years.

At the same time, legal and regulatory fragmentation remains. For example, the EU and the U.S. apply different supervisory philosophies – the EU generally pursues a "same activity, same risk, same rules" approach, while U.S. frameworks tend to rely more on activity-specific or state-level oversight – resulting in variations in how DAS activities are classified and supervised. This introduces additional complexity in managing the cross-border lifecycle of DAS.

**Interoperability is improving, but progress remains uneven.** A growing set of mechanisms now helps move assets and instructions across crosschain messaging and bridging, ecosystem native protocols, and institutional rails. Even so, DLT addresses only part of the workflow. DLT still needs to connect to TradFi infrastructure: the fiat **cash leg** on real-time gross settlement (RTGS) and automated clearing house (ACH) rails and the ledgers of CSDs, ICSDs, and custodians.

Given this reality, we see no clear signs that a "single ledger will rule them all." Rather, **the operating model is evolving into a network-of-networks**, **with standards**, **gateways**, **and regulated service providers** linking on-chain objects to off-chain finance.

> The operating model is evolving into a network-of-networks, with standards, gateways, and regulated service providers

## 2.3 Interoperability as the foundation for digital asset securities adoption

Without interoperability, fragmentation has introduced **structural inefficiencies across capital markets**. In traditional finance, decades of standardization and integration efforts have largely addressed fragmentation, but in contrast fragmentation is growing rapidly in DLT. To scale adoption, interoperability is needed not only to connect ledgers, contracts, and networks, but also to ensure seamless integration with the traditional infrastructure that continue to anchor global finance.

**Without robust interoperability, costs of operations on-chain might be higher than expected.** Firms will end up connecting to multiple permissioned DLTs and legacy rails, adding bespoke interfaces, duplicate KYC/AML checks and off-chain reconciliations that will keep post-trade processes largely manual and expensive. On a single platform, settlement can be atomic and near instantaneous, but when transactions span different ledgers, especially between TradFi and DLT, participants have to reintroduce coordination layers to move cash and assets in multiple steps.

## Interoperability gaps also diminish liquidity and create missed investment opportunities.

Assets and cash locked on isolated networks cannot be reused across venues, for example, in collateral management. Market makers struggle to operate in large markets, fragmenting order flow and slowing the emergence of efficient secondary markets. The remedy highlighted by central banks and market infrastructures is to link ledgers or provide a shared connectivity layer – an approach seen in BIS's unified ledger vision[5] – so assets can safely move between networks and into the broader financial system. Market participants, and reporters[6] likewise, note that common standards are needed for DAS trading to scale. The aim is a set of interoperable platforms that preserve co-existence while unlocking deeper liquidity.

**Interoperability challenges also increase regulatory uncertainty and operational risk.** Diverging regional frameworks, combined with inconsistent standards across ledgers, create compliance and process complexity that can stall cross-border adoption. Participants will face uncertainty around how assets are defined, how rights are recognized, and how obligations can be enforced – further deterring large-scale adoption. On top, the coexistence of multiple ledgers, custody chains, and intermediaries, introduces reconciliation challenges, gaps in entitlements, and increased points of failure. Without harmonized processes, trust in the finality of transactions and market operational resilience will be compromised, especially in times of stress.

5. **BIS, The next-generation monetary and financial system**.
6. **Reuters**, referring to the **Axelar report**.

# How to advance interoperability through the interoperability framework

## 3.1 Three objectives and five key principles to guide interoperability at industry level

The DASCP established a comprehensive, risk-based framework to guide the safe and efficient adoption of DAS. Designed to be technology-neutral and asset-agnostic, it outlined core risks and controls to help ensure legal certainty, operational resilience, and regulatory harmonization. Since its release, the DASCP has become a common reference point across the industry and is now being used as a shared ground for the development of more specific frameworks and initiatives.

Building on this first work and to support the next stage of digital asset adoption, **DTCC**, **Euroclear**, **Clearstream and BCG decided to regroup to highlight the importance of interoperability**. They aim to consistently describe the different dimensions of interoperability, highlight the issues which will be raised if they are not addressed, and illustrate how it will impact core use cases in capital markets.

This framework serves multiple objectives, each designed to accelerate adoption and reduce fragmentation:

**Objective 1: Create a common taxonomy and outcome;** provide the industry with a shared definition and taxonomy, anchored on the principle of "same asset, same rights, same outcome" across both DLT and traditional rails.

**Objective 2: Classify initiatives, reveal coverage and identify gaps;** Enable classification of existing and new efforts against the framework's capital markets foundations and interoperability building blocks. This makes coverage, overlaps, and gaps visible, guiding market priorities and investment decisions.

**Objective 3: Lay down a foundation for further work;** As with the DASCP, offer a starting point for development of standards, further analysis, and research. The framework is intended to inform design choices, discussions on risks, and regulatory engagement, while also facilitating broader industry collaboration.

As a result of these principles, we do not prescribe specific implementation approaches but aim to provide common objectives for the industry.

## 3.2 A framework for outlining market interoperability challenges

The interoperability framework is intended as a practical knowledge asset for FMIs, regulators, market participants, and technology providers. It offers a common reference point that can be used to define initiatives and guide regulatory dialogue.

## 5 principles to guide interoperability

### Solution neutrality

considers interoperability issues independently from the actor that solves it or the approach that is used to solve it

### Bridging networks, TradFi and DeFi

considers that TradFi and DeFi will work alongside each other for a long period, thus requiring assets to move seamlessly from DLT to traditional finance ledgers and back

### Business continuity at all times

prioritizes continuity and tolerance of change. Interoperable rails must withstand upgrades to assets, contracts and ledgers, ensuring engagements persist

### Inclusivity

fosters the inclusion of every market participant across the value chain in the solution for interoperability

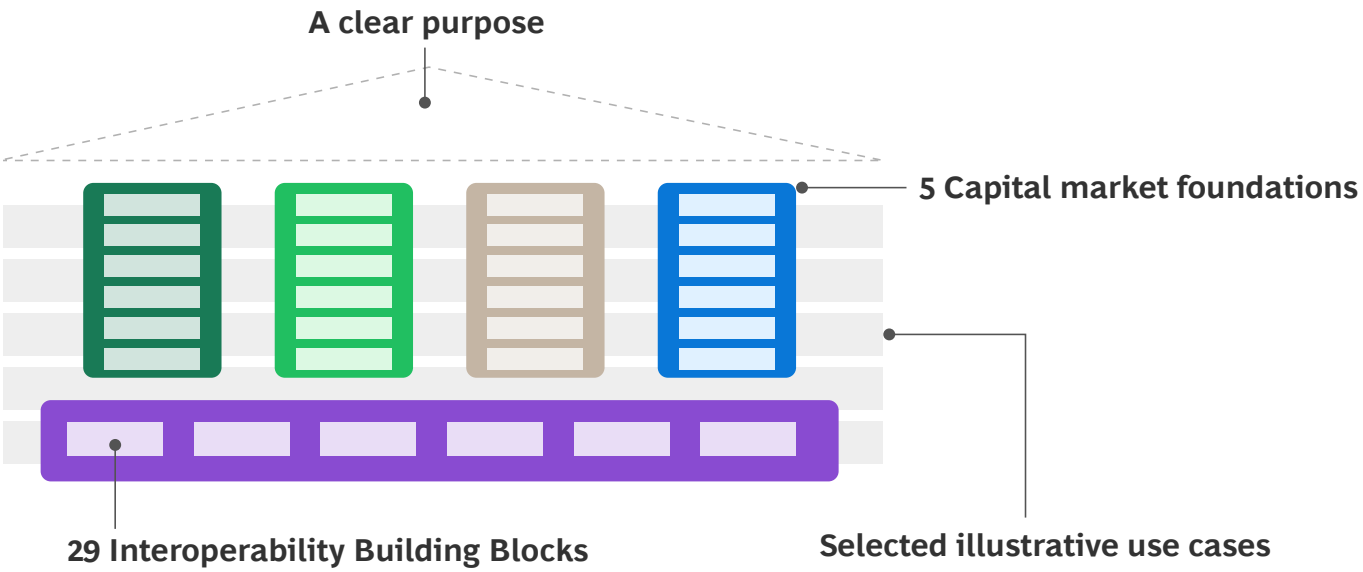
### FMI-grade security and resilience

ensures interoperability never weakens security – the number of ledgers or platforms connected must always meet single-ledger-grade standards

The framework is based on a structured, layered approach:

- **We start with a clear purpose:** to foster the safe and scalable adoption of DAS, with the aim of reducing residual risks for investors and strengthening operational resilience, market trust, and accessibility across the financial ecosystem.
- **Then we define interoperability and lay out capital market foundations:** critical layers that must be aligned to enable interoperability.
- **For each market foundation, we define interoperability building blocks:** specific interoperability areas within each foundation, that address practical requirements.
- **Finally, use cases illustrate the different interoperability issues:** end-to-end scenarios where interoperability can simplify processes, enable scale, and unlock new efficiencies.

This layered design ensures that the framework is both comprehensive, providing a path from principles to implementation, and is adaptable, allowing discussion with FMIs, regulators, market participants, and technology providers.




## 3.3 A clear purpose: Interoperability definition

We took a step back and first articulated what interoperability means today in capital markets, i.e., how it has been understood and applied so far.

Other sectors frame interoperability as systems that *work together end-to-end*. In **tech**, this means systems exchange and use information seamlessly, in **transport**, goods move smoothly across modes, and in **payments**, transactions flow across networks without friction.

In capital markets, especially with DLT coming, the conversation splits. **Technology vendors and teams** focus on ledgers, bridges, message formats and runtimes. **Business and risk teams focus** on rulebooks and responsibility in execution. We take a holistic view that spans data exchange, process and definition of roles.

**We believe that interoperability in capital markets can be defined as "the ability to exchange assets across ledgers – DLT and traditional – while preserving the asset's integrity, ownership rights and lifecycle, with full legal and regulatory compliance".** In other words: "same asset, same rights, same outcome".

> interoperability in capital markets can be defined as "the ability to exchange assets across ledgers – DLT and traditional – while preserving the asset's integrity, ownership rights and lifecycle, with full legal and regulatory compliance"

## 3.4 Capital markets foundations

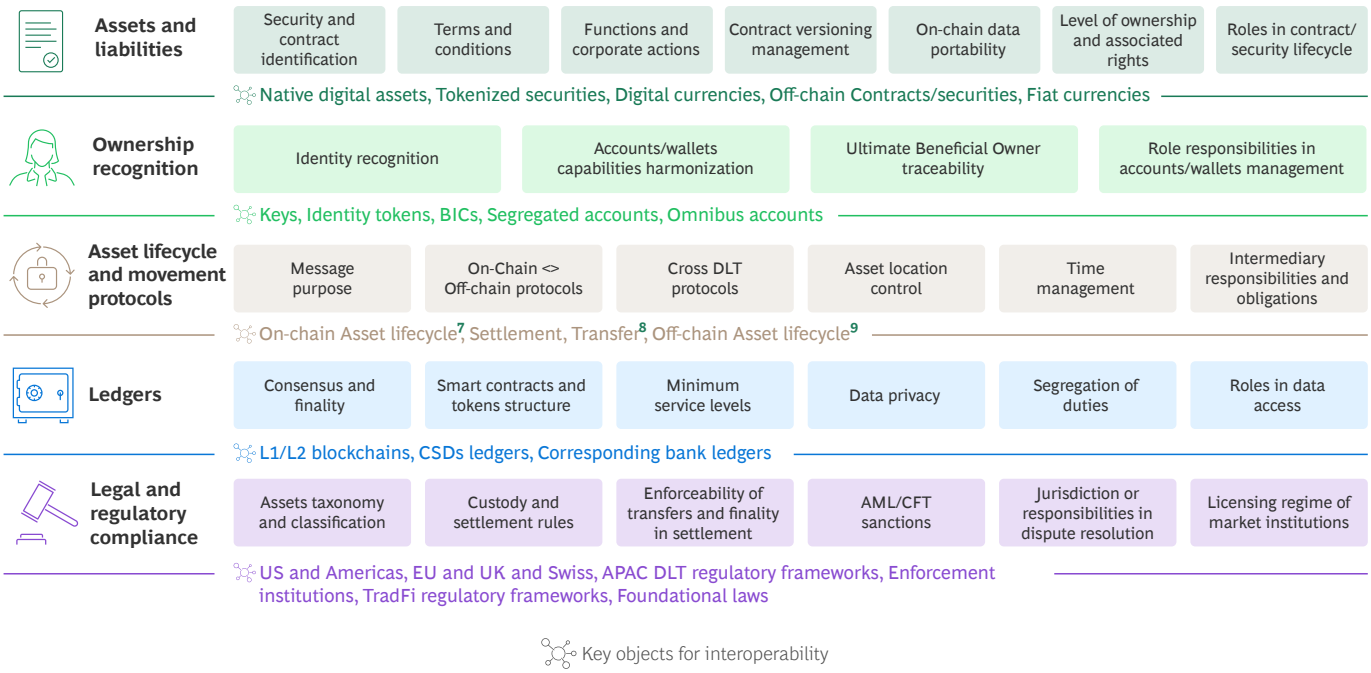
### Assets and liabilities, with market perspective

When talking about assets and liabilities from a market perspective (not from an accounting perspective), the different parties formalize their engagement in contracts and instruments in TradFi, or directly in smart contracts in DLT. On both sides, interoperability starts with ensuring the agreements between parties can be understood in the same way in every situation, starting with a unique identifier, similar to ISIN, UTI or LEI. Then, whether the transaction and/or the instrument is written in English or in French, in Solidity or in DAML, the outcome should be the same in every situation. This provides the market with stable identifiers and data schema to describe terms and conditions with standardized lifecycle logic for issuance, income, and corporate actions.

With a shared source of truth, the harmonization must go further: event semantics and versioning must be explicit, so upgrades do not distort flows across venues. When these elements are harmonized, an asset or a liability is portable and unambiguous across DLT and traditional systems, cutting exceptions and manual reinterpretation.

### Ownership recognition

Markets also need a consistent way to bind ownership rights to operational control. This requires portable, attestable identities (such as LEI/BIC/KYC credentials) mapped to keys, accounts, and roles; harmonized wallet/account multi-models (segregated and omnibus); and enforceable permissions and signing policies (Multi-signature/MPC) with auditability. Entitlements, freezes, recoveries, and beneficial-ownership attestations must operate the same way across platforms so “who may do what” is never in doubt. The result is continuous, compliant control of assets without bespoke ownership rules per network.




7. Mint, Burn, Freeze/Unfreeze, Lock/Unlock, Contracts upgrade.
8. Asset movement, Collateral mgmt., Lending and Borrowing.
9. Issuance, Corp. Actions, Redemption.

### Asset lifecycle and movement protocols

Asset lifecycle and movement are managed by exchanging messages. The most predictable events (format, sequences and origins, and expected dividend payments) are often pre-agreed between parties. This predictability is encoded in each financial institution's management of its assets. However, entities do not have a common language for messages. A common understanding of the meaning behind (i) messages (e.g., instruct, allocate, confirm, settle, cancel), (ii) agreed settlement protocols (DvP and PvP), and (iii) cross-DLT proofs and bridges that predicate actions on almost certainty of finality could eliminate the need to confirm that the action was properly executed at each stage.

To scale, responsibility for on- and off-chain orchestration needs to be explicit, with defined duties, SLAs, and obligations for intermediaries such as custodians, oracles, or bridge operators. Location control (lock/burn/mint/release) and robust error and reversal handling ensures an asset is in only one place at a time, thereby eliminating reconciliation disputes.

### Ledgers

The different ledgers of the market must agree when something is final. In addition, due to the shared source-of-truth paradigm, they must carefully manage what can be seen, how programs run, and when and from whom operations are accepted.

### Legal and regulatory compliance

Finally, interoperability is also concerned with harmonization of legal and regulatory compliance. This means establishing clear enforceability of transfers and finality in settlement by the law, and a clear escalation path to manage disputes, as this is a fundamental foundation of capital markets.

Moving out from these critical interoperability building blocks, the other steps are simpler. A shared taxonomy and classification would facilitate the anticipation of the impact of rules, harmonized custody and settlement rules would provide clarity for non-expert market participants, clear licensing and oversight for all roles – including novel ones like bridges and oracles – remove ambiguity concerning legal responsibility. Clearer responsibility for AML/CFT and sanctions will ensure compliance travels with the asset. Taken as a whole, these elements provide the operational and legal footing for cross-ledger activity across jurisdictions and institutions.

*Detailed explanation of each building block can be found in **Appendix (section 6.1)***

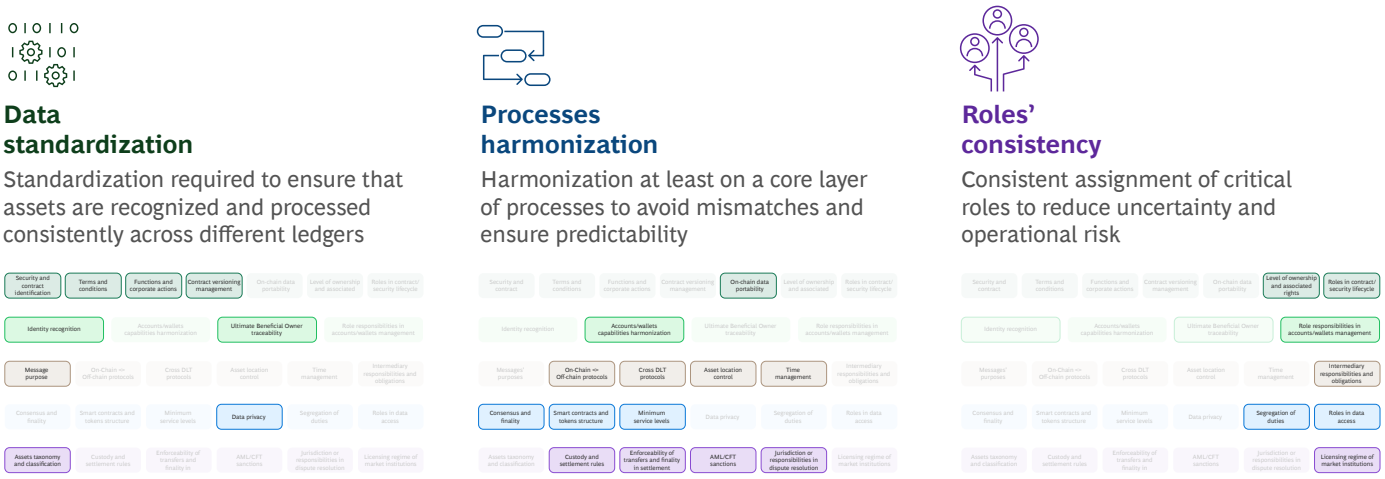
## 3.5 Minimum harmonization of data, roles, and processes

**The industry must ensure that the interoperability building blocks are consistently underpinned by three essential dimensions: data, processes, and roles.** These dimensions are fundamental to the effective management of interoperability. Every subsequent aspect can be mapped to one of these three, and their harmonization is key to ensuring consistency and predictability across infrastructures.

**Data standardization** has long been a prerequisite for market efficiency. In traditional finance, the introduction of the International Securities Identification Number (ISIN) in 1981, later recommended for adoption by the G30 countries in 1989, created a universal standard for identifying securities. The numerous iterations of this standard allowed assets to be recognized consistently across jurisdictions and infrastructures, paving the way for the globalization of financial markets, with most banks now able to run trading 24/7 across jurisdictions, issuers able to offer double quotation, and investors able to manage the risk of almost any payoff with OTC contracts. In the same way, DAS will require minimum harmonization of data structures, covering taxonomy, identifiers and message formats, to ensure that assets are recognized and processed consistently across different ledgers and networks.

**Process harmonization** is another critical enabler. In traditional markets, standardization of processes such as trade confirmation, clearing, and settlement cycles, including through SWIFT protocols, enabled the scaling of cross-border transactions and reduced operational risks. The market needs to harmonize processes to avoid mismatches and ensure predictability of operations.

**Roles' consistency** is equally important. Traditional finance achieved interoperability by clearly defining the responsibilities of critical actors such as custodians, central securities depositories (CSDs), and clearing houses. These roles are not only operationally defined but also legally codified, with custodians, CSDs, and clearing houses subject to specific licensing and supervisory regimes under frameworks such as CSDR, EMIR, and SEC/CFTC rules. This regulatory anchoring ensured clarity of responsibilities and accountability across the system. In digital assets, consistent assignment of critical roles – who validates transfers, who safeguards access to assets, or who provides regulatory oversight – could facilitate greater predictability and help reduce uncertainty and operational risk.



# Deep-dive in the role of data standardization as a major Interoperability enabler

Of the three kinds of harmonization required, the alignment of data is the most obvious, and there are multiple market initiatives underway. Capital markets exchange all types of business objects: contracts, transfers, payment, settlement, ledger entries... The way these business objects are exchanged defines the language used in the industry.

To increase interoperability, the industry would benefit from uniform data standards, whether the result of a joint industry initiative or from the regulators.

These standards will help increase the data quality in seven key dimensions:

**Uniqueness:** Although DLT could leverage existing standards like ISIN or UTI today securities may carry different identifiers depending on the chain where it was issued, requiring participants to maintain complex mapping tables to properly query current positions across ledgers. Similarly, with identification management, if DLT networks use different approaches to uniquely identify a beneficial owner, protocols are more complex and identity matching will be slower. **In addition**, identity theft risks increase.

**Accuracy:** Data must correctly reflect the capital market engagement, with the right level of precision and granularity, whether at asset or message level. For example, when a smart contract is issued on a ledger without proper control or certification for its programmability, the smart contract could be implemented with errors, leading to incorrect execution and loss of trust by the market participant.

**Consistency:** Integrity of data must be preserved throughout its lifecycle, with definitions respected across systems. Without this, transferring a security between ledgers could lead to translation errors, where the behavior of the smart contract changes unintentionally, or a beneficial owner of a security on one ledger may have a different outcome for a market operation on another.

**Completeness:** Considering the decentralization aspect of distributed ledgers shared by multiple market participants, it is critical that data is complete when being queried by a market participant. For example, if a security has different levels of completeness across chains, when a market participant queries the information of a smart contract, they could receive different levels of information, or when a market operation takes place, certain functions, such as default management or pricing, may be available in one ledger but not in another.

**Timeliness:** Timeliness is about ensuring that each event is recorded at the right pace and action occurs at the expected moment. Ledgers maintain an atomic approach to transfers and settlement. Without timeliness, different ledgers may update at different speeds, temporarily creating mismatches where smart contracts referring to the same asset operate with divergent definitions, or where smart contracts may send dividends or coupons to the wrong beneficial owners.

**Compliance:** Data access and market impact must be handled in line with internal policies and external regulations or standards, such as data privacy, AML, KYC. With programmability, the market has the capacity to embed automatic checks in protocols, or as in traditional finance, an institution can include compliance checks before triggering an action on DLT. If the protocols governing asset transfers or data access fail to meet compliance requirements, operational risks increase materially for the market participant.

**Accessibility and usability:** Data regarding ownership and movement must be accessible to all relevant and authorized stakeholders, whether based on owner contractual relationship, like Power of Attorney access, or based on regulatory roles such as market monitoring for Anti-Money Laundering, while respecting privacy, confidentiality, and sovereignty. Without this, different ledgers or smart contracts may implement inconsistently, creating interoperability risks if roles are not clearly defined.

Taken together, these dimensions make clear that interoperability cannot be achieved without rigorous harmonization of data. High-quality data definitions and processes ensure that assets retain their integrity across chains and infrastructures, enabling the seamless exchange of DAS while safeguarding mobility, liquidity, and investor rights.

# Conclusion and next steps for the interoperability framework

We invite all industry participants – FMIs, regulators, market participants, and technology providers – to continue leveraging the DASCP framework and this new Interoperability framework as practical foundations for their initiatives. Together, these frameworks provide shared principles and concrete reference points that can guide the design of solutions, inform executive or regulatory dialogue, and help scale adoption across capital markets.

Collaboration will be critical if the industry wants to reduce the cost of development and accelerate innovation beyond the pace of traditional finance. We are strongly convinced that interoperability is critical to scale DAS in the coming years. To truly move the market forward, we believe the industry should make key components interoperable through:

1. **Data standardization** – creating common identifiers, taxonomies, and message standards, as financial markets did in the past with ISIN.

2. **Process harmonization** – ensuring minimum definition of core processes such as settlement, reconciliation, and corporate actions, replicating the efficiency gains achieved in traditional finance through SWIFT standardized protocols.

3. **Consistent roles assignment** – clearly defining responsibilities for critical functions *(for example, custody, validation, oversight)*, as traditional finance achieved with custodians, CSDs, and clearing houses, to preserve accountability and trust.

By working together, the industry can build an integrated and resilient future for capital markets, where interoperability transforms fragmentation into connection and innovation into sustainable impact. We would encourage the formation of working groups across industry, under the sponsorship of FMIs and supervisors, to work on:

- **Governance:** Defining an industry-wide roadmap with the objective of guiding steps toward full interoperability

- **Interoperability and standards:** Defining standards on data, processes or roles or building guidebook for implementations in financial institutions. Opportunities could be, expanding on going initiatives on:

  - **Data model standards:** wallet model, smart contract model, corporate action model

  - **Process standards:** role assignment for wallet, corporate action execution on chain

- **Resilience and cybersecurity:** Developing guidelines on smart contract integrity and change management or industry wide resilience metrics and monitoring tools, designing controls for outage, error handling or cybersecurity risk management

- **Safeguarding customer assets:** Defining custody and settlement principles for FMIs, developing frameworks for asset and activity segregation of FMIs

# Case studies

## Interoperability to enable a large range of use cases across the value chain

To illustrate the impact of interoperability, we have looked at four families of use cases:

1

### Settlement

Exchanging value between parties across DLTs, payment networks (digital and fiat currencies), and traditional RTGS rails, including intraday and 24/7 operations

2

### Asset Lifecycle

Creating and maintaining an asset, including issuance, coupon/dividend/fee flows, redemptions, conversions, splits/mergers, and contract upgrades

3

### Collateral Management

Pledging, locking, valuing, and substituting assets to secure exposures (bilateral, tri-party, CCP), spanning digital twins and digital-native assets on single or multiple chains

4

### Custody Services

Safekeeping and record-keeping, potentially across multi-tier chains (sub-custodians, global custodians, CSDs) for digital-native and tokenized assets

The impact of interoperability can be understood across three levels. First, it can **simplify the execution of basic use cases** such as settlement on same chain or reducing friction in processes that today remain overly complex or duplicative. Second, it enables the **scaling of use cases currently operated in silos or with high complexity** (e.g., cross chain settlement), making it possible to consolidate liquidity and streamline fragmented operations. Finally, interoperability can **unlock the most complex use cases** (e.g., DAS-to-Fiat currency settlement) that are only at an exploratory stage today, paving the way for innovation that cannot emerge in a fragmented environment.

For each level of interoperability, we suggest a set of building blocks to prioritize, and we illustrate the frictions and added value of interoperability in one of the complex use cases.

## 5.1 Settlement: DAS-to-Fiat currency settlement

To gradually deliver all DLT expected value at settlement, a financial market needs a strong infrastructure to manage Delivery versus Delivery (DvD) and Delivery versus Payment (DvP) in all situations, with trust and neutrality at scale.

**At a simple level**, DAS settlement can be enabled when both asset and cash legs reside on the same chain, such as DAS-to-stablecoin transactions executed within a single ledger. This straightforward case already requires clarity in **consensus and finality**, enforceability of transfers, and consistent **asset taxonomy and classification** across jurisdictions. These building blocks ensure that transactions are final, legally enforceable, and universally recognized, reducing the risk of disputes or inconsistencies.

Scaling **beyond single-ledger** operations into cross-chain settlements requires additional blocks of interoperability. Here, the **definition of cross-DLT protocols** becomes critical to synchronize settlements across networks, as atomicity is not provided by default. Equally important are **custody and settlement rules**, which provide legal

recognition of tokenized asset transfers, and the definition of **accounts and wallets capabilities**, enabling consistent ownership structures and preventing mismatches across ledgers. In parallel, standardization of **message purpose** guarantees that settlement instructions carry the same meaning and intent across systems, avoiding complex integration layers, errors in message entries or reconciliation challenges. Together, these building blocks allow more complex settlement use cases to scale efficiently, consolidating liquidity that would otherwise remain fragmented.

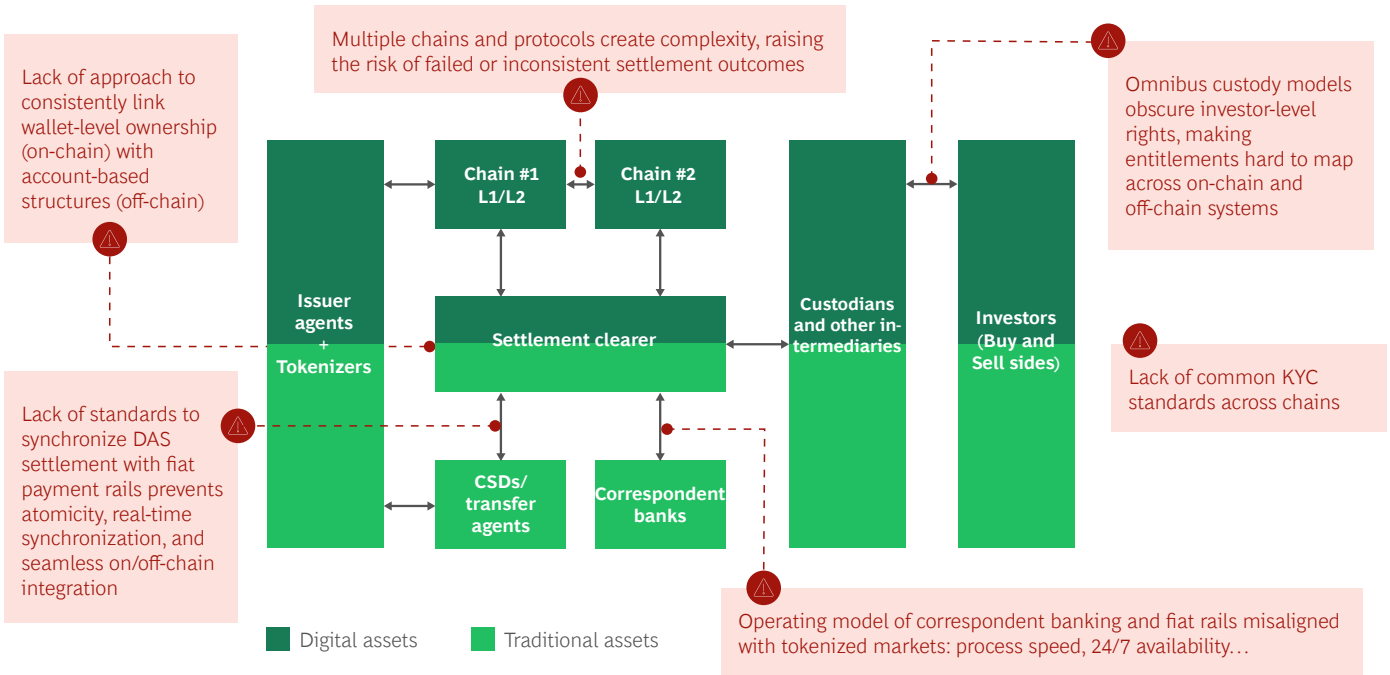
Finally, **to unlock new settlement use cases that are still at an exploratory stage** – such as DAS-to-fiat transactions where buyers may be recorded in omnibus accounts – interoperability must extend across digital and traditional environments. This requires robust **on-chain to off-chain and off-chain to on-chain protocols** to connect tokenized instruments with fiat payment rails, ensuring synchronization of asset and cash movements across infrastructures. Without such integration, settlement flows bridging DLT and traditional finance would remain inefficient, with important operational residual risk.

*Further details in **appendix (section 6.2)***

**In the coming years, the industry will have to manage seamlessly settlement between traditional finance and DLT. The DvP settlement of DAS-to-fiat amply illustrates the complexity.** Market participants will expect certainty in delivery and a higher level of success compared to what is available today.

The expected impact of interoperability for this use case would be to increase liquidity intraday, provide support for 24/7 operations, and reduce both counterparty and operational risk.

**Interoperability frictions:** the DAS-to-fiat currency settlement process will face multiple interoperability frictions across different stages and participants if interoperability is not offered. From issuers and tokenizers to custodians, intermediaries, and investors, challenges emerge both on-chain and off-chain, creating inconsistencies, inefficiencies, and misalignments between digital and traditional rails.



**Frictions reduction:** Providing interoperability on eight priority building blocks would remove most frictions, allowing investors to fully benefit from DLT advantage at scale.

- **Accounts/wallets capabilities harmonization:** Provide the equivalent of the different types of accounts developed in traditional finance are available on-chain, so all participants have the required capabilities to preserve the operational framework of their traditional finance vehicle of investment.
- **Message purpose:** Harmonize settlement messages so they carry consistent meaning across DLT and fiat rails, avoiding mismatches in asset/cash legs and enabling end-to-end synchronization.
- **On-Chain/off-chain protocols:** Provide smooth bridging protocols between fiat rails (correspondent banks, CSDs) and DAS rails, with clear responsibility of the different actors to reduce operational risk.
- **Cross DLT protocols:** Provide strong protocols to manage settlement in all situations across multiple chains.
- **Consensus and finality:** Define rules for final definition of DAS versus cash legs across chains and fiat rails and ensure no double-spending, with limited clearing requirements.
- **Assets taxonomy and classification:** Harmonize DAS regulatory status across jurisdictions and platforms, where possible, to avoid mismatches in how instruments are recognized.
- **Custody and settlement rules:** Ensure tokenized custody is recognized consistently across jurisdictions and custodians.
- **Enforceability of transfers and finality in settlement:** Ensure the ecosystem implements procedures for regulators and courts to enforce transfer of assets.

## 5.2 Asset lifecycle: Management of corporate actions on multiple chains

With DLT, the industry can expect a higher level of integration of the different parties. With programmability, smart contracts have the potential to automate most corporate actions, providing, for example, instant payments for coupon or dividends or a reduction in reconciliation requirements. In the coming years, the market will mature, delivering gradually the required interoperability requirements.

At a simple level, basic lifecycle events can already be managed on a single chain. To support this at scale, interoperability must ensure consistent **terms and conditions** across chains, which provide the baseline to express legal rights, obligations, and lifecycle triggers. In addition, clear definitions of **functions and corporate actions** are essential to encode how events such as coupons, dividends, or corporate splits operate, even when assets remain siloed within one ledger. These building blocks provide the necessary foundation for accurate event management within contained environments.

When positions are distributed across multiple chains, more advanced lifecycle challenges emerge. To address these, interoperability must support **identity recognition**, ensuring that entitlements can be attributed consistently across ledgers. **Cross-DLT protocols** are required to synchronize events when assets are split across chains, while **roles in data access** enable tiered visibility and reporting across issuers, CSDs, custodians, and investors. In parallel, **minimum service levels** are needed to align expectations when lifecycle events touch critical processes such as timing of entitlements, while **asset taxonomy and classification** ensure consistent treatment of digital-native versus off-chain equivalents in reporting. Finally, enforceability becomes key: **enforceability of transfers and finality in settlement** ensures that lifecycle-related transfers triggered by events are legally binding across rails, with flexibility in how responsibilities are assigned.

At the most complex level, interoperability must also incorporate corporate actions that involve both on-chain and off-chain components, such as major equity events. Here, additional building blocks are required. **Ultimate beneficial owner traceability** ensures entitlements can be reconciled across jurisdictions and fragmented custodial chains. Contract versioning management is needed to ensure that lifecycle events remain valid even as contracts evolve over time, providing consistency in event processing. **On-chain <> off-chain protocols** become essential to synchronize lifecycle events, such as, for example, coupon payments, when positions are partly managed across environments. Finally, the **licensing regime of market institutions** guarantees that only regulated and authorized entities can process and report lifecycle events, backed by contractual structures to enforce service levels.

*Further details in **appendix (section 6.2)***

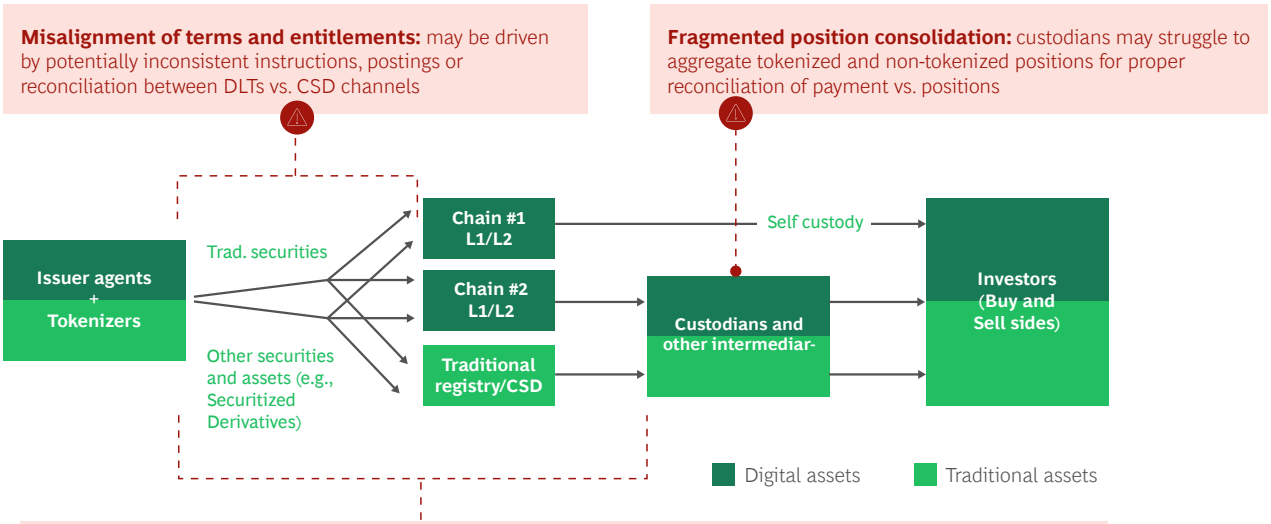
**Managing seamlessly simple corporate actions such as dividends and coupon payments with assets partially on-chain and off-chain (e.g., on-chain Digital asset, off-chain fiat currency) requires a high level of interoperability to identify asset holders accurately, trigger the event and efficiently send payments in fiat currency in the cash accounts.** Without interoperability, split positions across tokenized and traditional systems risk misaligned entitlements, inconsistent reporting, and investor confusion. The expected impact of interoperability for this use case is to enable consistent execution of corporate actions across rails, safeguard investor rights, and reduce reconciliation risk at scale.

**Interoperability frictions:** the processing of corporate actions faces multiple frictions across different stages and actors. From issuers and tokenizers to custodians, intermediaries, and investors, challenges arise both on-chain and off-chain, creating inconsistencies in entitlements, reconciliation gaps, and blurred accountability across digital and traditional systems.

**Frictions reduction:** Providing interoperability on ten priority building blocks would remove most frictions, allowing investors to fully benefit from DLT advantage at scale.

- **Terms and conditions:** Harmonize definition of coupon clauses and eligibility rules across all ledgers.
- **Functions and corporate actions:** Harmonize event types (dividends, mergers, splits) and definitions so the application can process them.
- **Contract versioning management:** Ensure smart contract amendments, expected and unexpected, can be executed by the issuer or regulatory bodies and propagated across all dependent smart contracts and chains.

- **Accounts/wallets capabilities harmonization:** Provide matched accounts/wallets across chains to prevent double-credit or missed entitlements, and intermediaries should be able to link wallets to cash accounts to allow receipt of payment in fiat currency for an on-chain asset.
- **On-Chain <> off-chain protocols:** Enable synchronizations for snapshots, elections, and payments between token ledgers and CSD books.
- **Cross DLT protocols:** Enable the coordination of events across the ledger to avoid timing skews or omissions.
- **Roles in data access:** Provide clear definitions of who can query and attest to entitlements across issuers, custodians, and investors.
- **Minimum service levels:** Manage timing asymmetry to ensure entitlements are recognized at the same moment.
- **Assets taxonomy and classification:** Manage the different tax/reporting framework for the different asset types and events across jurisdiction.
- **Enforceability of transfers and finality in settlement and the licensing regime of market institutions:** Necessary for regulatory bodies to be able to enforce impact of coupons payment and major corporate actions regardless of the chain.




**Timing asymmetry:** tokenized rails may operate in near-real-time, while legacy rails follow batch/market schedules — entitlements recognized at different moments

**Jurisdictional recognition gaps:** legal treatment of entitlements may differ between RWA and digital twins leading to coupon claim issues

*Considering more complex asset events:* **inconsistent event propagation with blurred accountability:** splits, mergers etc. may cascade inconsistently through multi-tier custody chains, creating gaps for end-investors – with **unclear accountability for finality** *(e.g., in a situation of self custody)*, **esp. when not clarified by regulator**

## 5.3 Collateral management: Substituting one digital twin for another

Collateral management is the most critical area of DAS and providing interoperability can unlock significant gains in efficiency. Activities such as securities lending, repo transactions and collateral substitutions all require precise coordination across ledgers and infrastructures. Without interoperability, these processes are complex, slow, and prone to error. As with other use case families, progressively more advanced interoperability building blocks are required depending on the complexity of the operations.

At a simple level, collateral management can be performed when both the collateral and the asset being lent are held on the same chain. To support this, interoperability must ensure that the **level of ownership and associated rights** is clearly defined, clarifying the rights to pledge, reuse, or reallocate collateral. In parallel, harmonization of **accounts and wallets definitions and capabilities** is needed so that collateral can be locked, moved, or released seamlessly. The consistency of **message purpose** is equally important, ensuring that instructions such as lock, release, or reuse incorporate identical semantics across platforms. Finally, enforceability must be ensured. **Enforceability of transfers and finality** provides the legal and operational certainty that collateral actions, such as those triggered by counterparty default, are binding.

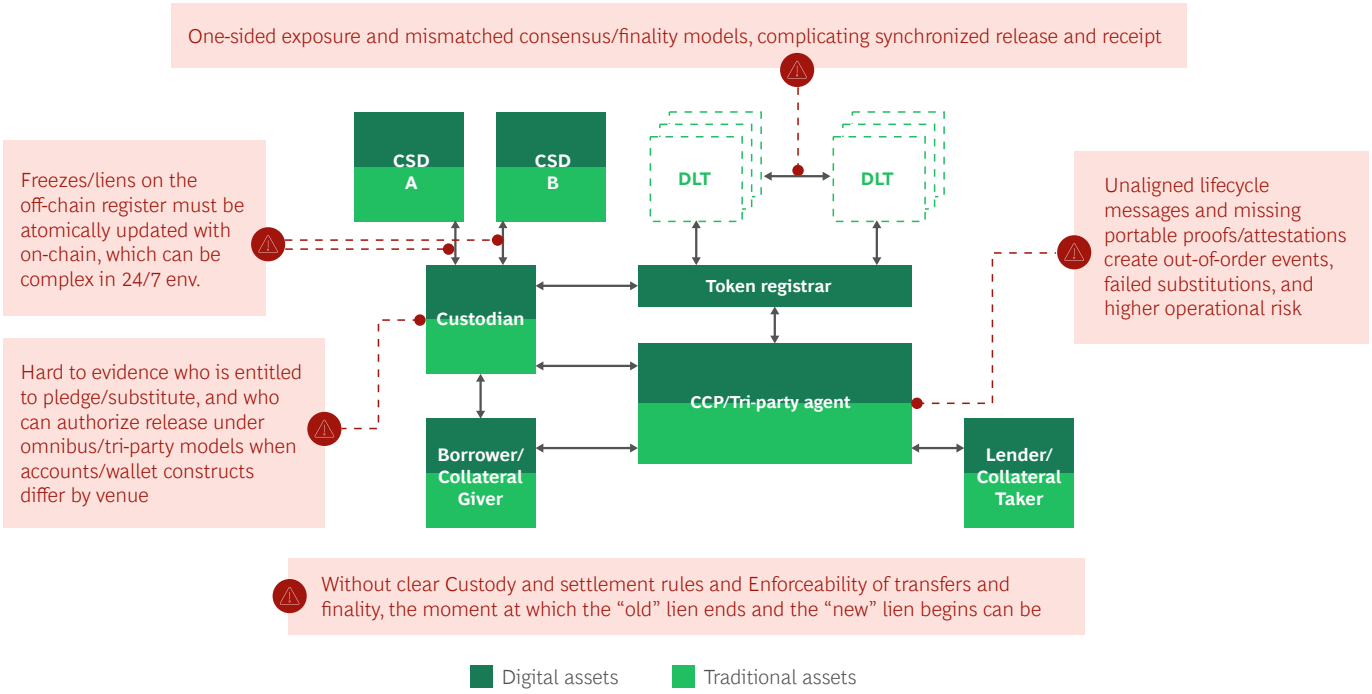
When collateral needs to move across chains or asset types, for example, in repo markets spanning multiple ledgers, additional building is required. **Security and contract identification** ensure that every collateral instrument is uniquely tracked and identified across environments. **Intermediary responsibilities in execution** must also be clearly defined, covering how custodians, CCPs and tri-party agents coordinate cross-platform collateral movements, confirmations, and exceptions. Synchronization of **consensus and finality** across chains is equally critical, enabling substitutions to take place without leaving one-sided exposures. To support seamless asset mobility, **cross-DLT protocols** are required to synchronize lock, unlock, or substitution events across chains, while **minimum service levels** ensure that ledgers deliver CCP-comparable resilience and continuity, making sure critical market functions remain robust end-to-end.

The most complex use cases arise when collateral substitution requires bridging between digital and traditional infrastructures – for instance, substituting one digital twin for another when positions are split across systems. Here, three additional building blocks become essential. **Custody and settlement rules** must be codified to define how client assets are held and segregated. **On-chain <> off-chain protocols** are necessary to bridge digital and traditional rails, ensuring freezes and releases are synchronized across both environments. Finally, **data privacy** safeguards must be in place, ensuring that beneficial ownership and position data remain private while still allowing selective disclosure, role-based access, and appropriate data controls.

*Further details in **appendix (section 6.2)***

**Substituting one digital twin for another requires a high level of interoperability.** This use case focuses on enabling a borrower to replace a digital twin posted as collateral with a different digital twin seamlessly during an ongoing securities lending or repo transaction. Without interoperability, such substitutions are operationally complex and often require unwinding the entire transaction. By enabling frictionless substitution, interoperability would allow lenders and borrowers to respond more efficiently to market needs, enhancing repo and lending market efficiency. The expected impact is to support collateral optimization, increase liquidity, and reduce funding costs.

**Interoperability frictions:** With limited interoperability, the substitution of collateral faces multiple frictions across different stages and participants. From borrowers and custodians to CSDs, tri-party agents and lenders, challenges arise both on-chain and off-chain, leading to mismatched finality, disputed liens, out-of-order events, and higher operational risk.




**Frictions reduction:** Providing interoperability on nine priority building blocks would remove most frictions, allowing investors to fully benefit from DLT advantage at scale.

- **On-Chain <> off-chain protocols:** Harmonize orchestration of lock/receive/release so the new twin is secured before the old twin is freed.
- **Cross DLT protocols:** Synchronize CSD/registry freezes, liens and releases in step with on-chain state during substitution, with callbacks, retries and cut-off handling.
- **Consensus and finality:** Define when each chain is final so release only triggers once both legs are irreversible.
- **Custody and settlement rules:** Define who may pledge/reuse/substitute, and define segregation and triparty/CCP duties, so that substitutions are operable across institutions (DvP/DvD logic across ledgers).
- **Enforceability of transfers and finality in settlement:** Make the swap legally binding at a clear moment so the old lien ends, and the new lien attaches without claw back risk.
- **Accounts/wallets capabilities harmonization:** Harmonize lock/escrow/pledge/reuse operations, approvals and allowlist, so the right party can substitute and control asset travel.
- **Message purpose:** Apply common semantics for lock/attest/accept/release/substitute, reducing out-of order events and manual monitoring.
- **Level of ownership and associated rights:** Model consistently the ownership of the security on-chain, the ownership of the twin and the ownership of claims, ensuring the lender's security interest attached to the new twin and the old twin is unencumbered on release.
- **Data privacy:** Ensure only necessary proofs are shared during substitution, while sensitive details remain confidential.

## 5.4 Custody Services: Custody models for tokenized assets

Custody is a cornerstone of capital markets, ensuring that assets are properly safeguarded, recorded, and serviced. As tokenization expands, interoperability becomes central to custody models, where fragmented ledgers and account structures can otherwise lead to gaps in reconciliation, unclear responsibilities, and risks to investor protection. Different levels of custody complexity require progressively broader sets of interoperability building blocks.

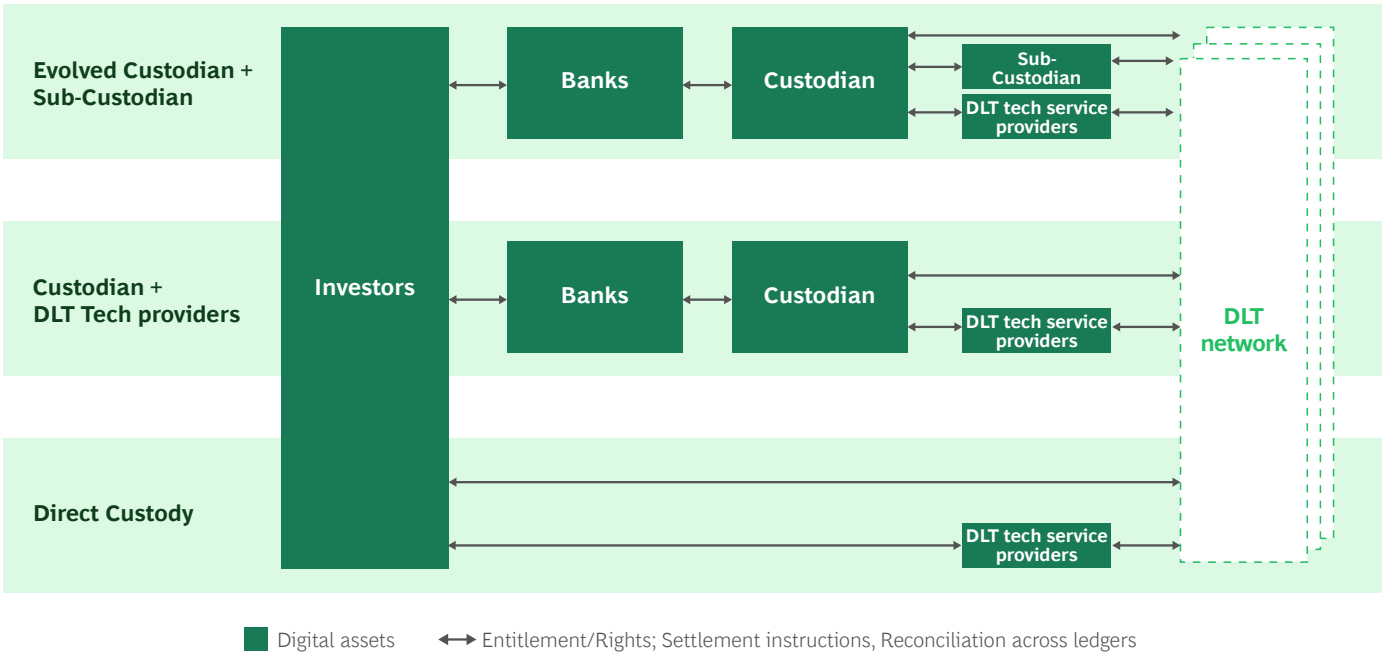
At the simplest level, interoperability enables the transfer of tokenized securities between custodians operating on different DLTs. To make this possible, **security and contract identification** must ensure instruments are recognized unambiguously across ledgers, so that positions reconcile consistently. Clear **roles and responsibilities in accounts and wallet management** are also required, providing similar ownership and sub-account models to those already used in traditional markets. In addition, interoperability must define **roles in data access**, clarifying who can see or attest to holdings across chains, thus enabling position queries and proofs. Finally, **custody and settlement rules** must be harmonized, allowing event taxonomies and servicing to be consolidated across multiple custodians. Together, these enablers provide the foundation for basic interoperability in custody.

When custody operations extend to account keeping across multiple DLTs, additional interoperability challenges emerge. At this stage, **data privacy** becomes essential, ensuring that proofs of positions and entitlements can be shared without disclosing client identities, relying instead on attestations and selective disclosure. Lifecycle servicing also requires harmonization through **functions and corporate actions**, ensuring that event definitions are consistent and can be executed across custodians. In parallel, **message purpose** must be harmonized, providing common semantics for instructions such as receive, deliver, internal transfers, statements, or servicing notices. By harmonizing these building blocks, custody operations can scale beyond silos and support more complex multi-ledger environments.

The most advanced custody use cases are still at an exploratory stage, such as multi-tier custody chains for tokenized assets. Here, interoperability must go further. **Ultimate beneficial owner traceability** becomes critical, providing regulators and market participants with visibility through multiple tiers of custody while still respecting privacy and regional constraints. In addition, **smart contracts and tokens** play a central role, embedding features such as freeze, allow-lists, or partitions directly into token designs to ensure control and proper servicing across custodians. Finally, **On-chain <> off-chain protocols** are required to enable hybrid custody, where some links in the chain may still rely on legacy books or CSD infrastructures. These protocols allow tokenized assets to remain fully serviceable even in mixed environments.

*Further details in **appendix (section 6.2)***

Three custody archetypes could potentially exist in the mature DAS ecosystem, where services would not be delivered by the same players:

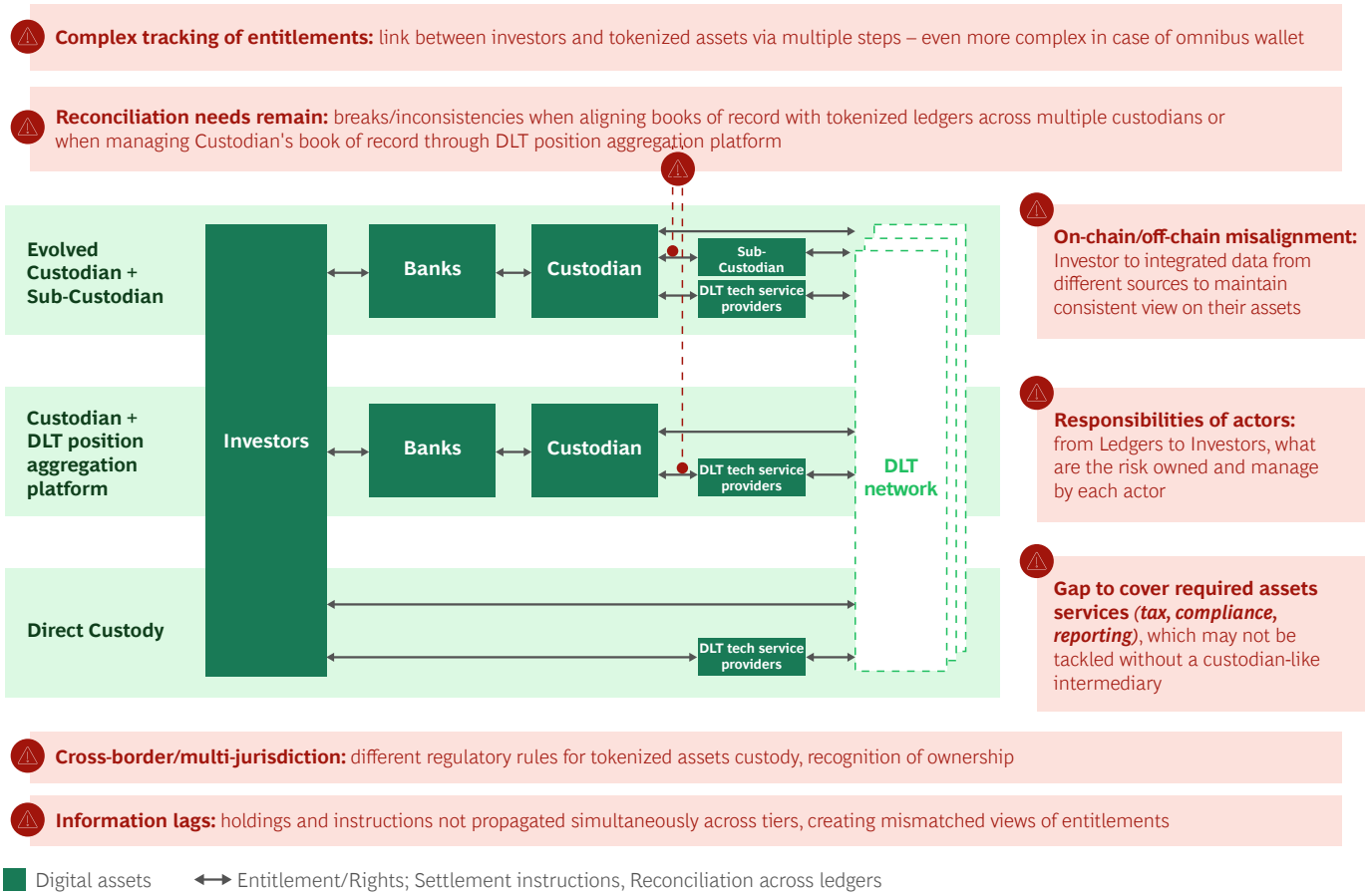



**The first archetype consists of multi-layer custody chains, to address fragmented market access.** In this archetype, custodians would rely on a mix of approaches, with direct integration, DLT tech service providers or sub-custodians for DLT access. The role of sub-custodians would evolve to focus on providing connectivity and services on specific DLT networks.

**The second archetype is based on an increased reliance on tech platforms for connectivity.** In this archetype, custodians would centralize risk management, entitlements, and reporting. Custodians could rely on tech service providers for access to specific networks instead of sub-custodians.

**The final archetype consists of shortened custody chains, shifting operational and regulatory exposure toward end-investors.** In this archetype, investors would mainly hold assets directly on tokenized ledgers. All services usually provided by custodians would be directly managed by investors or provided by DLT tech services, such as withholding tax management or compliance reporting, without risk ownership.

**Interoperability frictions:** With limited interoperability, custody of tokenized assets faces multiple frictions across different stages and participants. From investors and banks to custodians, sub-custodians, and DLT providers, challenges emerge both on-chain and off-chain, creating reconciliation gaps, misaligned entitlements, and inconsistent responsibilities. While most of these frictions occur regardless of the custody archetype considered, some issues, such as reconciliation across multiple custodians or the handling of specific asset services, are unique to particular models.




**Friction reduction:** Providing interoperability on ten priority building blocks would remove most frictions, allowing investors to fully benefit from DLT advantage at scale:

- **Security and contract identification:** Provide harmonized definitions of the tokenized assets across different custodians and DLTs.
- **Functions and corporate actions:** Allow corporate actions and investment actions to cascade correctly through multiple custody layers.
- **Role and responsibilities in accounts/wallet management:** Segregate the management of the chain of accounts/wallets to avoid conflict.
- **Ultimate beneficial owner traceability:** Always provide clarity to the regulator about the chain of ownership, despite layered beneficial owners.
- **Message purpose:** Guarantee instructions and requests have consistent meaning across custodians and DLT networks.
- **On-Chain <> off-chain protocols:** Bridge DLT with off-chain CSD books to maintain synchronized views, managing complex digital twin cases.
- **Roles in data access:** Segregate rights of intermediary to access and update asset records on ledgers, avoiding conflicts or blind spots.
- **Data privacy:** Ensure sensitive data remains protected when entitlements pass through multiple custodians.
- **Smart contracts and tokens:** Automate entitlement transfers and reconciliation of positions between custody layers, with transferability.
- **Custody and settlement rules:** Provide the legal framework for custody rights and obligations across jurisdictions.

# Appendix

## 6.1 Building Blocks definition and underlying issues

### Assets and Liabilities - Building blocks definition and potential issues of nonapplication

| Building blocks | Description | Issues (if not applied) |
|---|---|---|
| **Security and contract identification** | The market needs to uniquely identify security and transactions along their full lifecycle. As of today, some standards and market practices are set.<br>• ISIN and UTI are the most common ones:<br>• All publicly traded securities and most funds and other form of securities require an ISIN, available for OTC contracts securities and Derivatives can leverage ISIN<br>• All transactions are identified with a unique Transaction identifier<br>To ensure interoperability, an asset should follow the same conventions whether it is issues on-chain or off-chain, and conventions should be set up to manage the difference between RWA and its digital twin | If separate conventions are followed to identify assets, it will generate complexity along the value chain, esp. in the management of fungibility of positions. For example:<br>• **Cross-chain transfers:** maintenance of mapping rules is required between the codification of smart contracts in the different chains<br>• **Inventory of ownership:** transfer agents and other parties managing beneficial owners have more difficulties to track assets<br>• **Corporate actions:** payment agent can have difficulty tracking the corresponding positions in the different chains<br>• **Custody:** computing security inventory/balances is more complex<br>• **Digital twin tracking:** tracking the issuance of digital twins is more complex if they follow different standards<br>• **Compute position:** market actors will have difficulty in computing the resulting risk/trading position in their system<br>• **Market data management:** linking oracle data to the smart contract is more complex |
| **Terms and conditions** | When defining the assets, interoperability will be enhanced if all ledgers use similar standards to define assets/contracts, especially for:<br>• **Economic terms** (e.g., interest rate, conventions, payment schedule…) need identical schema anchored to the legal documents<br>• **Governing law and dispute resolution process**<br>• **References** to external documents (e.g., link to full contract definition) | Consistent definition of the terms and conditions will have critical impact in the lifecycle of the assets defined in multiple chains:<br>• **Functions encoding** – if the economic terms or the right and obligations are encoded following different logic, the function and corporate action encoding will be very specific to each blockchain<br>• **Integration in market actor systems** – the economic terms of the assets have to be replicated in the position keeping tools. If they follow different standards, the adoption by market actor will be slower (beyond the use of functions<br>• **Data request to ledger** – if economic terms are managed differently, request on Ledger data can have different level of performance |
| **Functions and corporate actions** | When defining functions, interoperability will be increased if all functions follow similar standards so all actors can operate their role similarly, across ledgers:<br>• **Standard lifecycle functions** (issue, redeem, exercise, etc.) must follow standard event types and semantic, as much as possible,<br>• **Economic/calculation functions:** coupon/interest calculation, conversion formula<br>• **Utility and Maintenance functions:** upgradeability, audit actions, exception management, etc. | Without interoperable approach in function definition across, the industry will run into different level of issues:<br>• **Corporate actions** will not be able to be instantaneous, as the issuer has difficulty to execute the function in every context<br>• **Issuer events/Credit event management** – impacting all the smart contracts could take months while no authority could block change of ownership movement<br>• **Not being interoperable would require re-implementation + reconciliation** mechanism in market actor systems |

| | | |
|---|---|---|
| **Contract versioning management** | As a security can remain active for 20 years or more, the on-chain securities and contracts will require versioning along their lifecycle, especially for:<br>• **Regulatory modifications**, e.g., after the creation of a new regulatory requirements<br>• **Change in corporate structure** of the issuers: e.g., merge with another company<br>• **Change in the roles in the security**, e.g., change of guarantor<br>• **Changes in the economic terms**, e.g., moving from USD to USDD or a potential USD CBDC for coupon payment<br>• **Change in the DLT tech**/ definition standards | The versioning of digital assets needs to follow similar approach across chains to prevent:<br>• **Co-existence on one-chain** – where one exchange runs v1 while another exchange runs v2<br>• **Co-existence across chains** – where one chain runs on v1 and another chain runs v2, thus breaking transferability<br>• **On-chain <> Off-chain incompatibility** – where on-chain and off-chain security are not aligned, thus breaking transferability |
| **On-chain data portability** | **A portable on-chain asset record** – identifier, terms, rights and event schema – that can be read and reused across ledgers without loss of meaning or legal effect. Practically, this means common identifiers, harmonized data taxonomies and token/ contract interfaces so "the same asset" is the same everywhere it appears | • **Fragmentation and venue lock-in** – one asset forks into incompatible versions per chain or venue; liquidity gets trapped. (ICMA warns against fragmentation and promotes shared data language for bonds)<br>• **Lifecycle breaks** – corporate action/rights interpretation diverges because terms and event data aren't modeled the same way everywhere. (CDM addresses uniform lifecycle semantics)<br>• **Heavy reconciliation and reporting risk** – positions and rights can't be computed consistently across books/ledgers without shared identifiers and schemas. (DTI provides chain-linked unique token IDs) |
| **Level of ownership and associated rights** | Across smart contract, securities and contracts, a harmonized definition of ownership level, and associated to increase the capacity of investor to optimize the cost and revenue of asset holding, starting with:<br>• **Legal ownership**, incl. title transfer in collateral management<br>• **Contractual claim** to restitution of the security, owner by the lender<br>• **Security interest of a collateral taker:** collateral-provider remains the legal owner | If those ownerships set up are not harmonized across the different ledgers and consistently implemented, the legal rights for the different levels of ownership could lead to:<br>• **Decrease of liquidity:** as the digital asset on a chain could not have anticipated the definition of contractual claim in security standard<br>• **Misappropriation of the underlying assets:** e.g., sale of a security on which a security interest claim remains<br>• **Error in corporate actions:** e.g., dividend sent to the security lender rather than the borrower |
| **Roles in contract/ security lifecycle definition** | Across smart contracts, securities and contracts, a harmonized definition of standard roles in security and contract lifecycle management, and associated permissions for each step should be implemented, starting with:<br>• **Long term issuance role:** Issuer, Guarantor<br>• **Servicing roles:** paying agents, registrars, transfer agents<br>• **Custody roles:** CSD<br>• **Regulators/Supervisors**<br>• **Tokenizer** | Harmonizing the standard of operations across all DLT would simplify the identity and access management across ledgers:<br>• **Error in role definition at issuance:** e.g., providing Issuer role to the guarantor<br>• **Prevent impersonation:** Transfer agents of security A being in a position to act as a CSD on that security<br>• **Misappropriation of the underlying assets:** e.g., paying agents being allocated regulator role and enforcing a change in ownership<br>• **Decrease of liquidity:** as the digital asset on a chain could have not anticipated the definition of CSD in security definition standard |

## Ownership recognition - Building blocks definition and potential issues of nonapplication

| Building blocks | Description | Issues (if not applied) |
|---|---|---|
| **Identity recognition** | To be interoperable, the markets have adopted standards for international asset movement to prove the identity of asset owner or intermediaries asking for payment, asset movement or settlement, or of intermediaries, with BIC and IBAN or in payment.<br><br>To increase interoperability, a harmonized approach to credential management rules and protocols could **bind legal entities/venues and persons to the key and wallets they control and be portable across venues or ledgers**, with standard crypto suites, revocation, and evidence<br>• Credentials that bind legal entities/persons to keys and wallets (e.g., LEI/BIC ⍰ DID/VC) with supported signature suites, key rotation, and revocation<br>• Portability of KYC/KYB allowlists and sanctions screening results across venues; common evidence format for onboarding decisions | If identify recognition is not harmonized across ledgers, the cybersecurity risk increases for on-chain actions:<br>• **Different Cybersecurity level in identity management implementation:** with ledgers having different level of security, cross-chain protocols will have different level of security, thus increasing the identity spoofing risk<br>• **Reduction of speed in asset movement:** if proof of identity is managed differently across blockchains, the speed at which asset movement can happen is slower<br>• **Compliance of account/wallet activities:** can be non-compliant, compromised, stall or rejected<br><br>In case of importability of KYC:<br>• **Each venue re-onboards the same client** and maintains its own lists; approvals diverge, cross-venue transfers fail, and collateral/liquidity get trapped – raising costs and delays |
| **Accounts/wallets capabilities harmonization** | Over multiple iterations of regulatory/standard adoptions, capital markets have developed different standard of accounts. Not all have to be reproduced in ledgers, but a harmonized approach on the implementation of their specificity would decrease adoption cost for large institutions:<br>• **Purpose of use:** cash vs security,<br>• **Types:** custodial, omnibus, segregated, nominee, trust<br>• **Regulatory treatment:** ISA/OSA<br>• **Market infrastructure layers:** CSD accounts/CCP accounts/sub-custody accounts<br>• **Capabilities:** e.g., freeze/unfreeze; lock/escrow; pledge/reuse; spending limits; recovery; multi-approval<br>• **Risk controls:** e.g., allowlist wallets | • **Liquidity reduction:** with no capacity to provide the equivalent of omnibus, nominee or trust accounts, some investment vehicles existing today will not be able to access blockchains, thus reducing investments<br>• **Segregation breaches, blocked transfers, ungoverned usage** if controls are misread or absent cross-systems<br>• **Operational and compliance risk** if there is no consistent way to enforce limits/allowlist/recovery |
| **Ultimate Beneficial Owner traceability** | To align with AML/travel-rule requirements, a set of components required to reveal beneficial ownership across custodian layers could be harmonized to reduce risks:<br>• **Attestation model and query protocol for UBO/ownership** across custodial layers, taking into account privacy and data residency constraints<br>• **Integration of identify with public registries** and relationship data where available (e.g., LEI Level 2 "who owns whom" for parent relationships) | With blockchain not aligning on approach to track UBO, the implementation costs of UBO tracing will increase, preventing some institutions to invest as it will increase the risk of On-chain transactions:<br>• **Settlement rejections, regulatory breaches**, since counterparties/regulators cannot verify UBO at receipt<br>• **Sanctions/AML exposure** from opaque chains of ownership<br>• **Duplicative KYB, slow onboarding**, and fragmented investigations |

| | | |
|---|---|---|
| **Role responsibilities in accounts/wallets management** | Over multiple iterations of regulatory/standard adoptions, capital markets have developed different standard of accounts and approach to operate accounts.<br>On-chain, they will need to be implemented either at wallet management level, at protocol level, or at ledger level. A harmonized approach on the following would increase interoperability:<br>• **Transaction authorization rules** – codify who can do what/when/to whom/how much (by user group, source wallet, destination, asset, amount, time)<br>• **Roles' definition**: harmonizing roles naming and associated rights<br>• **RBAC administration**, with technology enforcement of separation of admin and operations<br>• **Audit logs** for every privileged action (policy change, allowlist edit, transaction approval) is attributable and timestamped for audit/regulatory review | With multiple standards used across blockchains or with specific complex configuration set up, the cost and complexity of implementation will lead to:<br>• **Liquidity reduction**, with some intermediaries not able to able to implement their compliance rules and thus the right level of cybersecurity risk to their investors<br>• **Error in roles/rights assignment**, leading to misexecution (in case if wrong party acts), duty drift, unenforceable mandates<br>• **Audit failures**, client asset protection risk due to inability to evidence control/segregation<br>• **Higher fraud/operational losses** |

## Asset lifecycle and movement protocols - Building blocks definition and potential issues of nonapplication

| Building blocks | Description | Issues (if not applied) |
|---|---|---|
| **Message purpose** | A common message model defining **who sends what to whom** and the **intended legal and economic effect** of each instruction across systems. ISO 20022-style standard should be adopted – ensuring key instructions (e.g., DvP, derivatives novation) are the same on every platform.<br>Key dimension to harmonize include:<br>• **Message types** (trade confirmation, settlement instruction, corporate action, data queries, etc.) and their outcomes<br>• **Standard attribute** so that a message triggers identical processes on DLT networks and traditional systems (CSDs, RTGS, etc.)<br>• **Legal impact:** Alignment of enforceability on-chain with the equivalent of what exists off-chain (e.g. a token transfer message carries the same ownership change intent as a securities delivery message) | Without a unified purpose, format and engagement for messages, each system may interpret instructions differently, leading to breaks in lifecycle:<br>• **Conflicting books and records** if, for instance, one platform treats a message as final while another sees it as provisional<br>• **Settlement (incl. atomic) cannot be assured** in case of lack of standard DvP or DvD messages, reintroducing settlement risk<br>• **Manual intervention and reconciliation** – an untenable friction when bridging 24/7 blockchain environments with limited-hours legacy systems |
| **On-Chain <> off-chain protocols** | Deterministic linkage between on-chain and off-chain ledgers with well-defined callbacks, timing, data-level harmonization, and error handling to enable hybrid workflows (e.g., security token is delivered on a blockchain, an equivalent cash payment is triggered in a traditional RTGS).<br>The protocol must ensure **idempotency** (retries won't duplicate an outcome), **synchronized finality**, and clear **handling of failures** (rollbacks or compensating actions). Key considerations include:<br>• **Mapping of on-chain asset actions** (mint, burn, transfer) **to off-chain actions** (issue securities, update account balances, etc.)<br>• **Atomicity, for settlement** – one leg cannot finalize without the other, preventing ledger divergence. Trigger messages or atomic transaction mechanisms can be used to coordinate between smart contracts and institutions – e.g. a smart contract escrow that only releases tokens when a callback confirms fiat payment settled, within a given timeout | Without cross-domain protocols, there is a set of issues<br>• **Ledger desynchronization** (state drift) – on-chain and off-chain books can diverge (e.g., if token burned on chain, and bank leg fails, one party will lose asset, since books and records don't match)<br>• **DvP settlement could fail asymmetrically** – the digital leg settles but the cash leg doesn't – leaving participants and regulators in a precarious position; require manual intervention<br>• **Stalled workflows** – without time-bound callbacks and error handling, a 24/7 blockchain might await an action from a 9-5 system<br>• **Limited traceability** to manage disputes |

| | | |
|---|---|---|
| | • **Error recovery** – if one side fails (technical error or outside of operating hours), define how transactions abort or queue for later, and how parties are notified, and evidence is logged (to avoid orphaned instructions)<br>• **Security across each link in the chain** – Communication channels are protected against interception, messages are guaranteed to be authentic and tamper-proof, and authorizations reflect the right level of business risk<br>• **Legal responsibility** of the actor in the protocols<br>• **Auditability** | |
| **Cross-DLT protocols** | Harmonized protocols that move value and state across heterogeneous DLTs with security, finality, and data/contract compatibility, ensuring atomicity (or well-defined compensation) and survivability through upgrades/forks<br>Key elements:<br>• **Trust model and attestation tiers:** clarify whether claims are checked via light client proofs, decentralized oracles, MPC custodians, or vetted relays<br>• **Cross-chain agreement on recognition of trust events** (e.g. via cryptographic proofs or vetted intermediaries)<br>• **Mechanisms to eliminate partial completion** (e.g., no token gets minted or burned without the corresponding asset moving on the other chain)<br>• **Wrapped tokens and derived contract lineage:** (1) Manage the lifecycle of wrapped tokens to prevent double counting during cross-ledger transfers, (2) ensure traceability of the chain of related smart contracts (from Beneficial Owner to Ultimate Beneficial Owner), (3) reconcile derived entitlements (e.g., voting, dividends, collateral pledges) with the original underlying contract to preserve consistency across ledgers<br>• **Secure transport and endpoint posture**, such as e.g., mTLS/TLS 1.3 between bridge components; strict API authn/authz (e.g., OAuth/OIDC service accounts, token binding), network allowlisting, and DoS protection at gateways<br>• **Data semantics harmonization:** cross-chain asset identifiers, address/identity mapping, and message purpose taxonomy to avoid "same name/different meaning" errors<br>• **Other security measures** like sequence numbers or timeouts to prevent duplicated or rogue cross-chain instructions, and routing standards so messages reach the right chain and contract<br>• **Legal responsibility**<br>• **Auditability** | Absent robust cross-DLT protocols, blockchains remain isolated/unsynchronized "islands" of liquidity. Potential issues include:<br>• **Partial or failed transfers** (one network updates while the other doesn't, causing unbacked tokens or stuck funds)<br>• **Double-spend exploits** if a malicious actor capitalizes on lags between chains, and general fragmentation (users must resort to ad-hoc bridges, often vulnerable – evidenced by hacks like Harmony Bridge)<br>• **Undermined resilience** due to bespoke and error-prone integrations with each new blockchain<br>• **Double counting of wrapped assets** – if wrapped tokens and their control accounts are not reconciled; same assets can appear multiple times across ledgers<br>• **Loss of entitlement traceability** – without managing the chain of related smart contracts (Beneficial Owner → Ultimate Beneficial Owner), rights such as dividends, voting, or collateral can be duplicated, lost, or misallocated<br>• **Semantic drift in financial meaning** – failure to standardize representation of encumbrances, liabilities, and "value over time" contracts cause misinterpretation of obligations, leading to mispriced risk and systemic exposure.<br>• **Fragmented state visibility** – if cross-ledger transaction states are not tracked, in-flight transfers create blind spots where assets seem to exist on multiple ledgers simultaneously, enabling fraud or disputes over ownership<br>For institutions, lack of a secure cross-chain protocol means inefficiency, trapped assets, and operational risk when trying |
| **Asset location controls** | **A common ruleset that specifies the authoritative location of an asset at any moment** (the "source of truth") and how authority transfers between ledgers/venues – e.g., immobilize at a CSD and mirror on a DLT, or burn on Chain A and reissue on Chain B – without creating duplicate title and while satisfying venue/jurisdiction requirements. | • **Double representation/broken chain of title** – the same asset appears "live" in two places; entitlements and settlement become contestable (Bridge patterns that don't control source of truth have been a major risk vector)<br>• **Regulatory breach** – dematerialized/immobilized securities in the EU must be represented in book entry through a CSD, poor control location rules risk noncompliance<br>• **Operational/finality mismatches** – cash and asset legs settle on different systems unless control transfer is tightly coordinated with RTGS/central bank money rails. (Eurosystem trials and Helvetia address this integration) |

| | | |
|---|---|---|
| **Time management** | **Synchronized clocks: A unified time reference and snapshot mechanism** across ledgers in a multi-chain environment to ensure that at any given moment (a true "record time"), the system can clearly identify who owns what on each ledger. It extends the traditional record date concept into a precise, cross-ledger record timestamp, critical for functions like corporate actions in a 24/7 trading context.<br><br>**Coordinated timing** (potentially centralized): Achieving a coherent cross-ledger timeline may require a trusted time oracle or coordinating service so that every ledger abides by the same timeline for state changes. Completely decentralized networks struggle to reach a perfectly synchronized view of time and state, so time management often relies on a governance layer or central timekeeper to ensure all participants adhere to unified timing and snapshot rules. This guarantees that even as transactions occur continuously, there is a consistent temporal framework to track ownership and value over time across the ecosystem.<br><br>**Snapshot and state control: Coordinated state snapshots and transaction sequencing** so that asset movements between chains do not create ambiguity. For example, when an asset is in transit (being wrapped or moved to another chain), time management protocols capture that transitional state to prevent any double-counting of the asset. All ledgers agree on the exact moment an asset leaves one ledger and arrives on another, maintaining a single version of truth about asset location. | • **Uncertain ownership at a given time:** Without synchronized timing, it becomes difficult or impossible to definitively determine ownership and control "at this second" across ledgers<br>• **Double-counting and inflated asset counts:** If ledgers are not time-coordinated, an asset moving between chains can appear on two ledgers at once (on one as locked/reserved and on another as newly issued). In-flight assets may be counted twice, overstating total supply or exposures<br>• **Reconciliation Breakdowns:** Asynchronous clocks and unsynchronized state updates force participants to perform complex reconciliations after the fact. Records on different platforms won't match if one ledger's "end-of-day" snapshot doesn't line up with another's. These mismatches introduce operational risk – firms might find inconsistent transaction histories, or missing assets, requiring manual intervention to resolve<br>• **Settlement delays and failed corporate actions:** Simultaneous exchange on different networks may fail, as one network might process a transfer faster than another. Similarly, corporate actions could misfire – e.g. an investor could receive benefits on one chain while the source asset was already moved on another, or misses an entitlement because the snapshot was taken at different times<br>• **Weakened asset lifecycle integrity:** Key events – trades, collateral postings, margin calls, transfers, corporate actions – depend on knowing the exact state of an asset at specific times. If each ledger operates on its own timeline, ownership verification becomes unreliable, and risk management models break down (since exposures can't be pinpointed in time) |
| **Intermediary responsibilities and obligations** | Clearly defined roles, SLAs, and liability for each intermediary involved in cross-platform transactions. In an interoperable ecosystem, various actors – oracle providers, bridge relays, custodians, clearing houses, technology vendors – facilitate the end-to-end execution. Key components:<br><br>• **Service-Level Agreements (SLAs)** for uptime, response time, and processing throughput (e.g. an oracle network commits to report events within X seconds, 99.9% of the time)<br>• **High availability/automation** commitments to support 24/7 operations demand from traditionally 9–5 institutions<br>• **Liability and coverage** – agreements on who bears financial loss if an interoperability mechanism fails – e.g. if a bridge contract is hacked or a relay fails to deliver a message causing a settlement fail, is it the service provider, the user, or a mutualized fund that absorbs the loss?<br>• **Audit and evidence trails** – each intermediary must produce reliable logs/proofs of their actions (signed attestations, etc.) so that in dispute or failure scenarios, there's transparency. This also entails governance frameworks (possibly overseen by a consortium or regulator) to enforce these responsibilities | Absent clear responsibilities, accountability doesn't exist – a serious issue when something breaks in a complex transaction spanning multiple system.<br><br>Participants could be left blaming each other with no prompt resolution (e.g., if a cross-chain transfer fails to complete, the origin blockchain might point to the bridge operator while the bridge blames a custodian – meanwhile the assets are in limbo).<br><br>• **Losses from incidents** (hacks, downtime, errors) may not be compensated without predefined liability, deterring institutional adoption<br>• **Workflows can stall** – if an oracle is down or a relay runs slow during peak hours, and no SLA/back-up is in place, transactions queue up indefinitely. In a 24/7 market, this is untenable as it could freeze liquidity across ecosystems<br>• **Complicated regulatory oversight** due to lack of clear roles – regulators cannot easily determine who must fix an issue or who to hold responsible for compliance lapses. |

# Ledgers - Building blocks definition and potential issues of nonapplication

| Building blocks | Description | Issues (if not applied) |
|---|---|---|
| **Consensus and finality** | Finality is essential for trust in cross-ledger operations. In TradFi, finality is deterministic, error can happen but there is an action, and dispute can be managed on those actions.<br>**Different blockchains employ various consensus mechanisms** (e.g., PoW, PoS), which yield **different notions of finality** (probabilistic vs. immediate).<br>• On-chain settlement provider could harmonize their definition of finality<br>• **Interoperability solutions could interpret consensus differences and manage their complexity** – for example, detecting when a transaction is finalized on one chain before acting on another<br>• **Blockchain bridge/adapter could ensure a source transaction won't be reversed** (forked out) before it triggers actions on a target ledger | • **Double-spending and inconsistency:** without guaranteed finality, a transaction assumed successful on one ledger could be reversed, leading to duplicate asset usage or mismatched states across systems<br>• **Settlement uncertainty:** Relying on probabilistic finality (e.g., waiting for many confirmations in PoW networks) slows down cross-chain processes and still carries risk<br>• **Security vulnerabilities:** If consensus differences are not respected, attackers could exploit them – for instance, by reorganizing Chain A after a bridge has transacted on Chain B – resulting in fraud. Failing to wait for finality or to handle consensus faults can let bad data or invalid transactions propagate across networks |
| **Smart contracts and tokens structure** | Smart contracts encapsulate business logic on ledgers, and tokens represent digital assets or rights **standardizing these across platforms is critical for seamless interoperability**<br>• **Common standards provide consistent interfaces**, so wallets and applications can recognize and handle tokens across multiple ledgers, simplifying readability and portability<br>• **Establishing chain-agnostic frameworks** (like taxonomy models) helps bridge interoperability gaps by providing a common language for contracts and tokens<br>• **Establishing verifiable contract provenance and controlled change** (audited code, governed upgrades, explicit pause/kill semantics) as part of token/contract standards | • **Fragmented assets and liquidity:** Incompatible token standards prevent direct transfer of assets between ledgers<br>• **Security incidents:** The lack of a unified approach has led to many security incidents – often because custom bridge code introduces vulnerabilities<br>• **Increased cost and complexity of integration:** If smart contract languages and token models differ widely, developers must implement custom logic for every pair of interacting platforms<br>• **Governance issues:** Multiple versions of what should be the "same" token should be managed across different chains (e.g., wrapped tokens). Governance actions like token freezes, supply adjustments, or compliance checks might not carry over across networks, potentially violating rules in one environment even if enforced in another<br>• **Irreversible losses and inconsistent enforcement** across networks in case of exploitable logic/upgrade |
| **Minimum service levels** | DLT platforms for capital markets are expected to uphold stringent minimum service levels to match traditional financial market infrastructure. This means:<br>• **Very high availability** (often >99.95% uptime, with no single points of failure)<br>• **Fast and predictable processing**<br>• **Capacity for high throughput**<br>Platforms must be resilient, with defined recovery objectives (which is aligned with industry norms like the CPMI-IOSCO), for example abilities to:<br>• **Resume operations within 2 hours of a disruption** with near-zero data loss<br>• **Operate continuously** (24/7 service windows) | • **Settlement disruptions and delays:** If a DLT does not meet required uptime or latency, critical operations can fail (e.g., an outage or slow block confirmation could halt a DvP settlement or a collateral substitution, causing failed trades or missed margin transfers)<br>• **Participants will miss key cut-off times** for funding or collateral, losing access to liquidity windows and incurring penalties<br>• **Broken atomicity and synchronization:** Insufficient service levels undermine cross-system coordination → credit risk if one side of a payment or exchange completes while the other is stuck<br>• **Breach of regulatory and oversight expectations.** Financial authorities require FMIs to have robust continuity plans |

| | | |
|---|---|---|
| **Data privacy** | Protect sensitive data while preserving interoperability and verifiability:<br>• **Data minimization and placement:** store hashes/pointers; classify data (public/consortium/confidential) and tag with residency/retention rules<br>• **Selective disclosure and partitioning:** field/record/view level controls (encryption, redaction, ZK proofs) so observers/regulators see only what they are entitled to; support for read-only nodes/feeds with filtered data<br>• **Encryption and controls:** encrypt at rest/in flight; use threshold/MPC keying, envelope encryption, and key rotation policies<br>• **Retention per jurisdiction:** enforce data residency, timebound retention, and lawful disclosures; deletion/erasure paths (e.g., proofs on chain, data off-chain) | • **Legal breaches and fines:** immutable ledgers carry PII across borders; you can't honor erasure/minimization → GDPR/banking secrecy violations; sharing with partners becomes risky<br>• **Business leakage:** sensitive prices/positions/customer data visible to competitors; market abuse and profiling risks increase |
| **Segregation of duties** | **Define the cross-layer interface so that L2 execution is portable and verifiable by L1 and by external systems** – clarifying who is the source of truth (L1), who executes (L2), and which proofs/controls connect them. This makes L2 state consumable by other ledgers and by traditional finance systems.<br>• **L1 anchors final state** (state root/data availability), **while L2 provides scale**; outsiders verify L2 facts via L1 proofs (validity/fault proofs, inclusion commitments)<br>• **Finality mapping:** Define when an L2 event is final for others (e.g., after challenge window for optimistic rollups, or upon validity proof on L1 for ZK rollups) so DvP/DvD and cross-chain actions can trigger safely<br>• **Standard cross-layer messages:** Canonical "send/receive" and bridge semantics (lock, mint, burn, release) through L1 to avoid bespoke, risky L2↔L2 links | Assets and messages become unreliable across layers and networks: they get stranded, misaccounted, or used before they're truly final → bridges and DvP fail unpredictably<br>• **No canonical truth:** External systems can't tell which layer to trust<br>• **Finality mismatch:** L2 "final" is later reorged/challenged → asymmetric settlement and principal risk in cross-ledger flows<br>• **Fragile L2↔L2 links:** Bespoke bridges bypass L1 guarantees → higher exploit surface, fragmented liquidity |
| **Roles in data access** | Define a portable, role-based entitlement model so participants can read, write, observe, and administer ledger data consistently across networks – with least privilege, separation of duties, selective disclosure, and full auditability<br>• **Role taxonomy and scopes:** common actor classes (issuer, custodian, exchange, validator/operator, oracle/relay, auditor, regulator, etc.) and scopes (read, write/execute, configure/admin, observe)<br>• **Entitlement model (RBAC/ABAC):** roles bound to attributes (jurisdiction, instrument class, purpose, conflict of interest) with dynamic constraints (time windows, amount thresholds, velocity limits) | • **Data leaks and privacy violations:** Without proper role segregation, sensitive information may be visible to all participants, or unauthorized parties might access data. This not only erodes trust but can violate regulations, e.g., PII exposure will likely breach GDPR<br>• **Unauthorized actions:** If write permissions are not role-based, any participant could invoke critical transactions or modify smart contracts<br>• **Audit and compliance challenges:** Without defined observer or auditor roles, providing regulators or third parties selective access is difficult<br>• **Operational risk:** A system with no role separation lacks the checks-and-balances common in traditional systems (e.g., requiring two signatories for a wire transfer) |

# Legal and regulatory compliance - Building blocks definition and potential issues of nonapplication

| Building blocks | Description | Issues (if not applied) |
|---|---|---|
| **Assets taxonomy and classification** | **A harmonized mapping of assets into clear regulatory categories** (e.g. securities, commodities, payment tokens, etc.), **with common definitions across jurisdictions**. This ensures that each asset or token type is identified under a consistent legal class (with tags for its jurisdiction and governing law), so regulators and market participants know which rules apply globally | If no common taxonomy exists, the same instrument can be treated as entirely different products in different markets, leading to conflicting obligations and regulatory arbitrage. For example, one country might label a token as a security, another as a commodity, and another as currency<br>• **Legal uncertainty**<br>• **Duplicative or contradictory compliance requirements**<br>• **Limited cross-border issuance and trading** |
| **Custody and settlement rules** | Clear regulatory rules for **how assets are held and how trades are settled**, defining:<br>• Who is allowed to custody client assets<br>• How to segregate customer holdings from firm assets<br>• How DvP is achieved across ledgers<br>These rules ensure client assets are safeguarded (with proper segregation and insolvency protection) and that transfer of an asset occurs if and only if payment occurs | • **Client asset protection can fail** – customer holdings might be commingled or misused. If a custodian goes bankrupt, clients could lose their assets<br>• **One party could deliver value without receiving payment** (or vice versa)<br>• **Settlements may be later challenged as invalid** (e.g., courts might not uphold a blockchain transfer if property/settlement law standards weren't met), undermining confidence in the system |
| **Enforceability of transfers and finality in settlement** | Legal certainty that a digital asset transfer is valid and irrevocable at a defined point.<br>• **Recognition of electronic signatures, smart contracts and ledger records** as legally binding, and statutes or rules defining when a transfer "finalizes" (so that after that moment it cannot be reversed, even if a party becomes insolvent)<br>• **Establishing finality** is crucial so that participants and regulators know exactly when ownership changes and obligations are discharged | Parties cannot rely on "settled" trades – increasing credit risk, legal disputes, and compliance challenges (since it's not clear when an obligation is truly final).<br>• **Transactions on a ledger may not be legally upheld** without enforceability and settlement finality (e.g., if digital signatures or records aren't recognized by law, a transferring party could later repudiate the transaction, or courts might not honor the token transfer)<br>• If no finality rule exists, **a counterparty's bankruptcy could retroactively void a completed trade** (some insolvency laws have "zero hour" rules that would undo transfers lacking statutory finality protection, causing cascading losses) |
| **AML/CFT sanctions** | Implementation of AML/CFT controls and sanctions screening at each critical point of transfer in the market. This entails:<br>• **Customer due diligence** (KYC for issuers, investors, and intermediaries<br>• **FATF "Travel Rule"** (transmitting sender and beneficiary information with crypto transactions above certain thresholds)<br>• **Ongoing transaction monitoring**, and blocking of sanctioned persons or addresses<br>• **Record-keeping obligations** to ensure an audit trail of transactions | If these measures are not applied, **illicit finance can flow through interoperable networks, undermining trust and inviting regulatory crackdowns**.<br>• Institutions will be forced to "de-risk" by severing ties with unclear networks<br>• **Regulators will impose penalties** – heavy fines or even sanctions designations – on entities or networks that facilitate money laundering or sanctions evasion<br>• Even **legitimate users could find their transfers rejected or delayed if originating from non-compliant channels** |

| | | |
|---|---|---|
| **Jurisdiction or responsibilities in dispute resolution** | Pre-agreed mechanisms for resolving disputes and clarifying which laws apply in cross-border or cross-ledger transactions. This includes:<br>• **Specifying governing law and forum** (courts or arbitration) for contracts or platform rules before problems arise<br>• **Agreement on how to handle evidence from decentralized systems** (e.g. acceptance of on-chain records or oracle data as proof in court).<br>In essence, participants must decide which country's legal system (or arbitral rules) will handle any dispute, and who has authority to enforce outcomes. | If no jurisdiction or dispute forum is defined, conflicts can become chaotic:<br>• **Multiple courts might claim authority or no court may clearly have it**, given the borderless nature of DLT, which can lead to parallel proceedings, higher legal costs, and uncertainty about which ruling to follow<br>• **Delays in enforcement**, given assets could be in limbo during prolonged fights over jurisdiction. Furthermore, without standards for blockchain evidence, a party might be unable to prove a transaction in court or a judge might refuse to recognize an oracle's output, undermining smart contract arrangements. |
| **Licensing regime of market institutions** | **Coherent or at least non-conflicting licensing and oversight frameworks** for all key market roles is required – including issuers, exchanges/trading platforms, brokers, custodians, clearing/settlement providers, and even interoperability service providers (like cross-chain bridge operators or oracles that facilitate transfers).<br>In a globally interoperable market, **each type of service should be subject to equivalent regulatory authorization across jurisdictions**, ensuring they meet baseline prudential, conduct, and investor protection standards. This alignment will let legitimate firms operate across borders and maintains a level playing field | • Without aligned licensing regimes, what is legal in one jurisdiction may be illegal or unregulated in another, leading to market fragmentation and risk hotspots<br>• Inconsistent requirements also invite regulatory arbitrage – firms will gravitate to lenient jurisdictions, concentrating activities in places with weaker oversight |

## 6.2 Zoom on differentiated impact of Interoperability across use cases families

Gradually, interoperability will enable more **Settlement** use cases at scale:

**Settlement at scale**

### Blocks to solve primary interop. challenges and enable "simple" use cases

(e.g., DAS-to-StableCoin settlement on same chain)

**Consensus and finality**

Same-chain settlement needs clarity on finality definition on cash/asset exchange

**Enforceability of transfers (and finality in settlement)**

Grows in importance as settlements cross networks and require recognition by multiple regulators

**Assets taxonomy and classification**

Aligning definitions across jurisdictions, avoid mismatches in how instruments/assets are defined and recognized

### Blocks to scale use cases that are currently operated in silos or with high complexity

(e.g., DAS-to-StableCoin settlement on different chains)

**Cross DLT protocols**

Critical for synchronized settlement across different ledgers as atomicity is not provided by default

**Custody and settlement rules**

Required to legally recognize tokenized asset settlement, even in low-complexity pilot

**Accounts/wallets capabilities harmonization**

Different assets ownership and sub-account approach to be managed in similar fashion

**Message purpose**

Aligning the semantics and objectives of messages exchanged with applications, facilitates exchange of information

### Blocks to enable new use cases which are only at an exploration stage

(e.g., DAS-to-Fiat currency with buyer part of Omnibus Account)

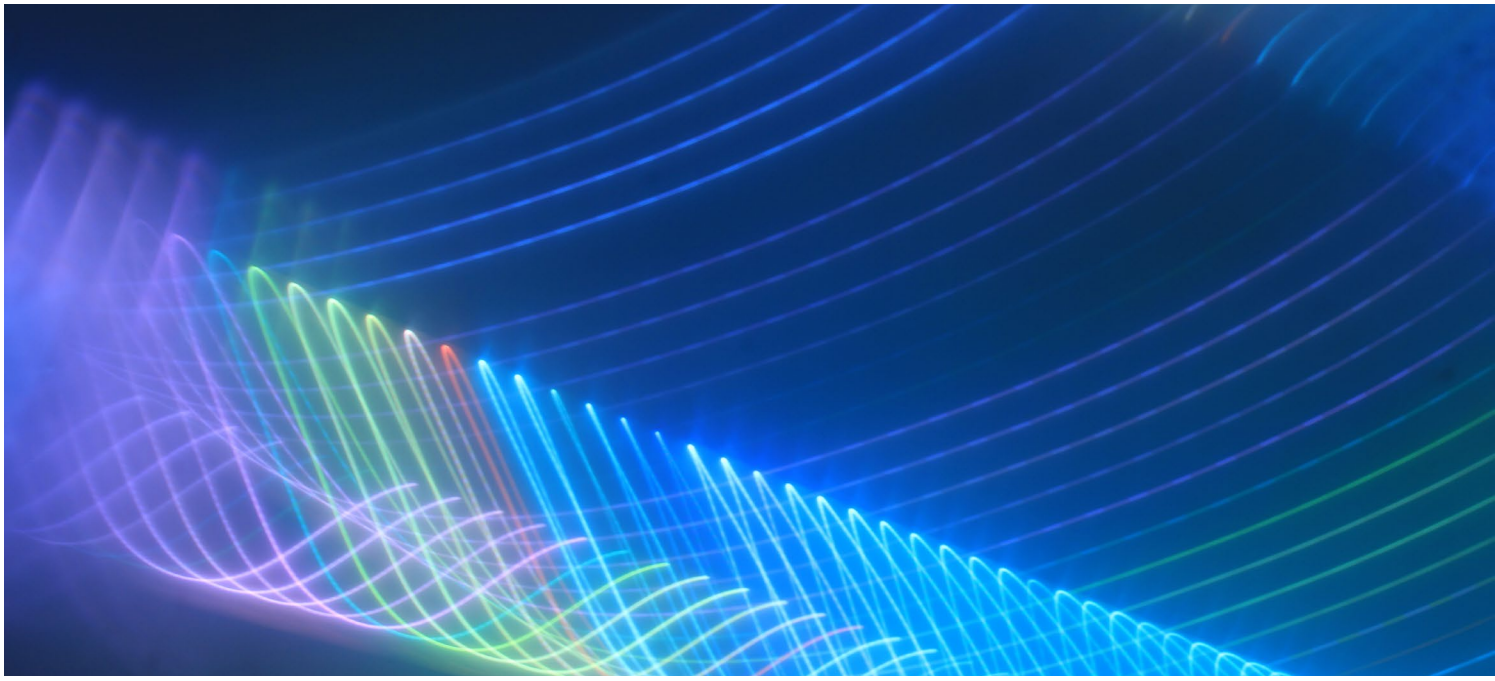
**On-Chain <> Off-chain protocols**

Important when trades touch both tokenized and traditional environments (e.g., in-house hedging)

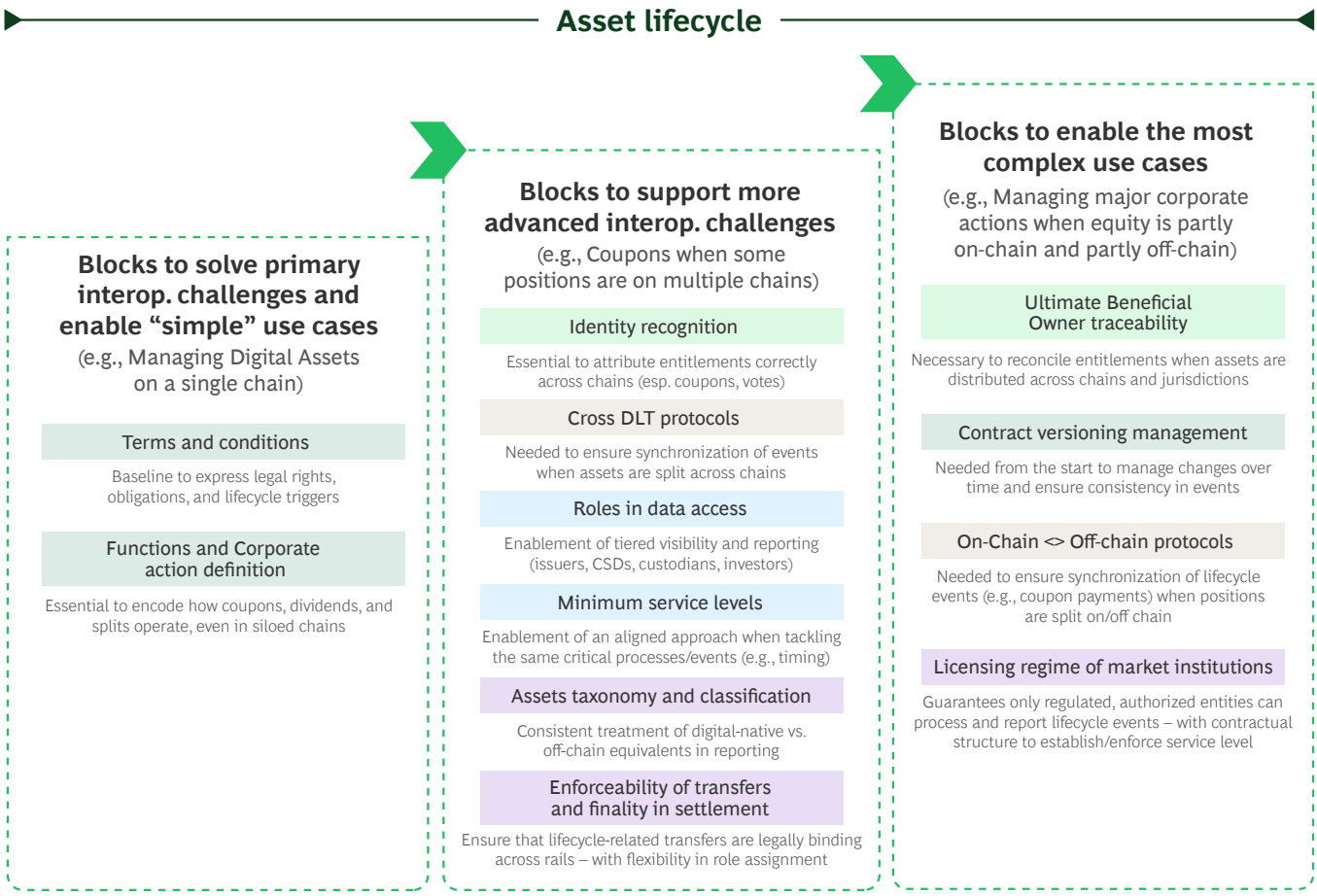
*Note: majority of Interoperability building blocks required for the use cases – analysis only highlights the most crucial enablers*

Building block category

Assets and liabilities | Ownership recognition | Asset lifecycle and movement protocols | Ledgers | Legal and regulatory compliance



Gradually, interoperability will enable more **Asset lifecycle** use cases at scale:




*Note: majority of Interoperability building blocks required for the use cases – analysis only highlights the most crucial enablers*

Building block category

Assets and liabilities | Ownership recognition | Asset lifecycle and movement protocols | Ledgers | Legal and regulatory compliance

Gradually, interoperability will enable more **Collateral Management** use cases at scale:

## Collateral management

### Blocks to solve primary interop. challenges and enable "simple" use cases

(e.g., Lending and borrowing with collateral and asset on the same chain)

**Level of ownership and assoc. rights**

Clarification of the rights to pledge/reuse collateral

**Accounts/wallets def. and capabilities**

Common accounts/wallet constructs so collateral can be locked, moved and released

**Message purpose**

Shared instruction semantics for repo, lending lifecycle events (lock, release, etc.)

**Enforceability of transfers and finality**

Management and standardization of actions for defaulting counterparty

### Blocks to support more advanced interop. challenges

(e.g., Repo market across chains, across assets)

**Security and contract identification**

Ensures each collateral instrument is unambiguously identified and tracked

**Intermediary responsibilities in exec.**

Definition of how custodians/CCPs/tri-party agents coordinate cross-platform collateral movements, confirmations and exceptions

**Consensus and finality**

Point of no return on each chain must be synchronized so substitution can happen without one-sided exposure

**Cross DLT protocols**

Synchronized asset movements across chains (e.g., lock/unlock or burn/mint during substitution)

**Minimum service level**

Underlying ledgers must deliver CCP-comparable resilience and continuity to ensure that critical market functions remain robust end-to-end

### Blocks to enable the most complex use cases

(e.g., Substituting one lent digital twin for another)

**Custody and settlement rules**

Codification of how client assets are held/segregated and how DvP/DvD is achieved across ledgers

**On-Chain <> Off-chain protocols**

Bridging DLs and TradFi ledgers, keeping freezes, liens and releases aligned

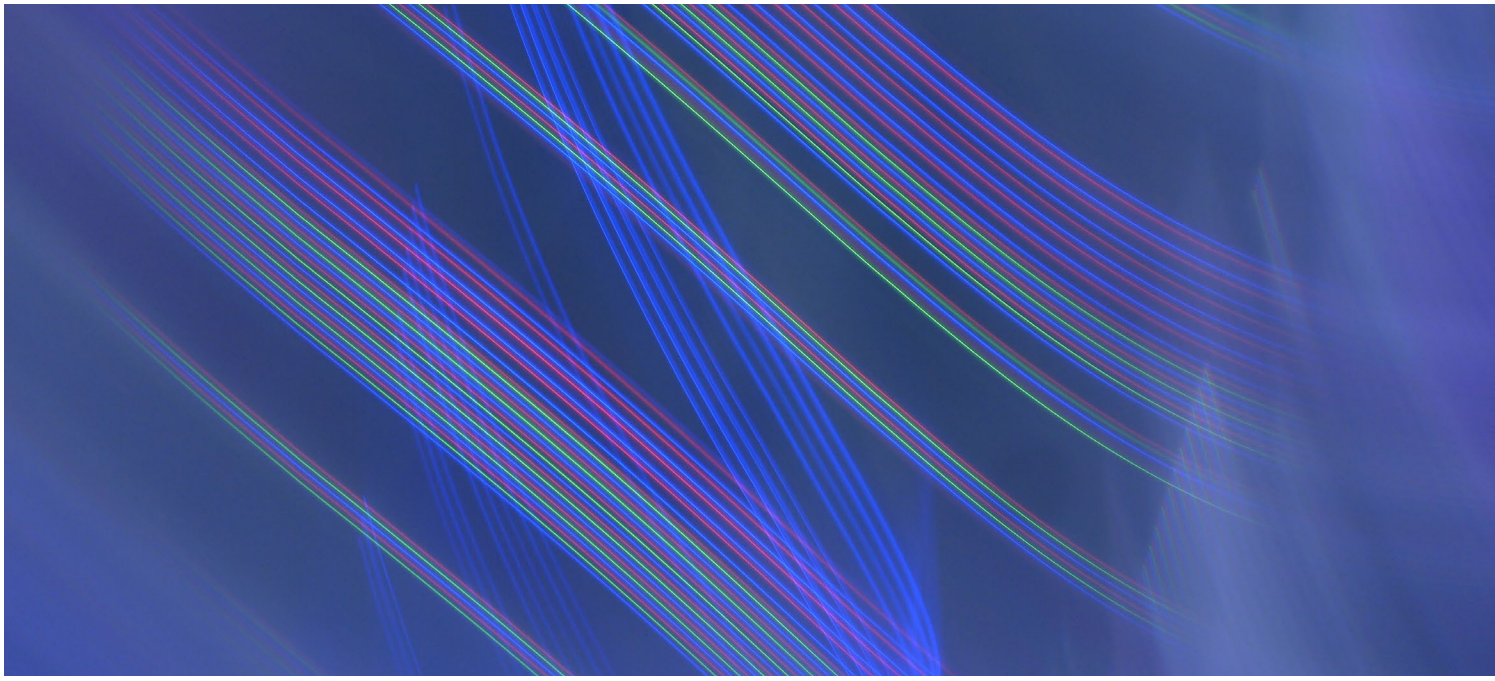
**Data privacy**

Keeps beneficial owner/positions data private with selective disclosure, role-based access, data controls

*Note: majority of Interoperability building blocks required for the use cases – analysis only highlights the most crucial enablers*

Building block category

Assets and liabilities | Ownership recognition | Asset lifecycle and movement protocols | Ledgers | Legal and regulatory compliance



Gradually, interoperability will enable more **Custody** use cases at scale:

## Custody

### Blocks to solve primary interop. challenges and enable "simple" use cases

(e.g., Transfer of tokenized securities between custodians on different DLTs)

**Security and contract identification**

Unambiguous instrument identity across DLTs so positions reconcile across ledgers

**Role responsibilities in accounts/wallet management**

similar ownership model for wallets as what exist today for accounts and sub-accounts

**Roles in data access**

Who can see/attest to holdings of wallets across chains; enables position queries and proofs

**Custody and settlement rules**

Harmonized event taxonomy so servicing can be consolidated across multiple custodians

### Blocks to scale use cases that are currently operated in silos or with high complexity

(e.g., Account keeping by custodian across multiple DLTs)

**Data privacy**

Share proofs of positions/entitlements without leaking client identities (e.g., ZK attestations, selective disclosure)

**Functions and corporate actions**

Harmonized event taxonomy so servicing can be consolidated across multiple custodians

**Message purpose**

Common instruction semantics for receive/deliver, internal transfer, statements, and servicing notices

### Block to enable new use cases which are only at an exploration stage

(e.g., multi-tier custody chains for tokenized assets)

**Ultimate Beneficial Owner traceability**

Look-through across tiers while respecting privacy/regional rules

**Smart contracts and tokens**

Token features custodians rely on (freeze/allow-lists/partitions) for control and asset servicing

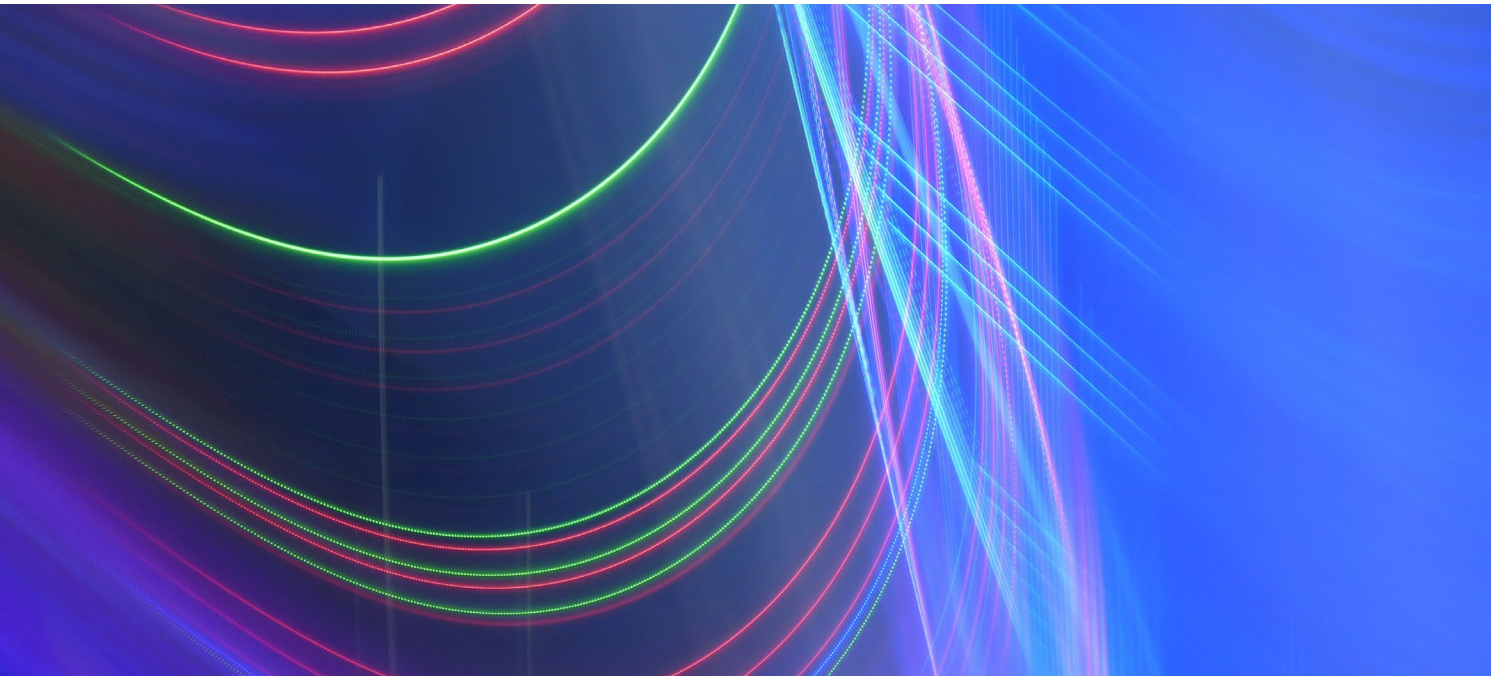
**On-Chain <> Off-chain protocols**

Hybrid custody where some links remain on legacy books/CSD

*Note: majority of Interoperability building blocks required for the use cases – analysis only highlights the most crucial enablers*

Building block category

Assets and liabilities | Ownership recognition | Asset lifecycle and movement protocols | Ledgers | Legal and regulatory compliance



## 6.3 Contributors

### Steering Committee:

– Nadine Chakar, Managing Director and Global Head of DTCC Digital Assets

– Jens Hachmeister, Managing Director and Head of Issuer Services and New Digital Markets at Clearstream

– Isabelle Delorme, Managing Director and Head of Product Strategy and Innovation at Euroclear

– Frédéric Brugère, Managing Director and Partner, BCG

### Working group:

**DTCC:**

– Otto Nino, Director, Technical Business Development

– Nitin Gaur, Senior Advisor

**Clearstream:**

– Thilo Derenbach, Head of Sales and Business Development, Digital Securities Services, Clearstream

– Vic Arulchandran, Director, Head of Digital Product and Market Design, Clearstream

– Patrick Kropp, Product Development Manager and Internal Readiness Lead

**Euroclear:**

– Jorgen Ouaknine, Global Head of Innovation and Digital Assets, Euroclear

– Stephanie Lheureux, Head of Digital Assets Excellence, Center at Euroclear

**BCG:**

– Frédéric Brugère, Managing Director and Partner

– Kaj Burchardi, Managing Director, BCG Platinion

– Tobias Wuergler, Managing Director and Partner

– Quentin de Waziers, Associate Director

### Acknowledgments

Special thanks to Quentin de Waziers for driving the structuration and the contribution of everyone.

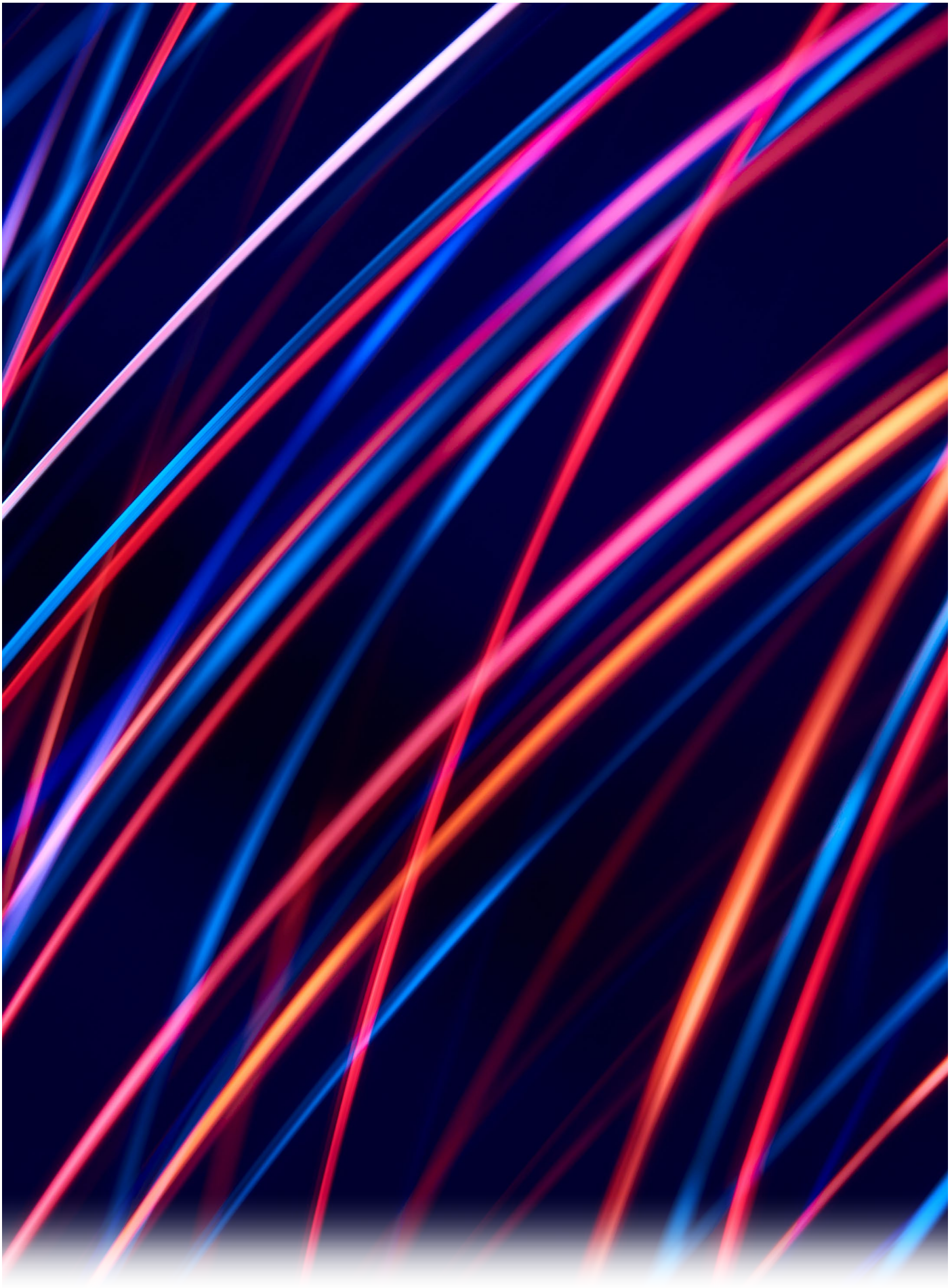
## 6.4 About DTCC, Clearstream, Euroclear, and BCG

With over 50 years of experience, DTCC is the premier post-trade market infrastructure for the global financial services industry. From 20 locations around the world, DTCC, through its subsidiaries, automates, centralizes, and standardizes the processing of financial transactions, mitigating risk, increasing transparency, enhancing performance, and driving efficiency for thousands of broker-dealers, custodian banks, and asset managers. Industry-owned and governed, the firm innovates purposefully, simplifying the complexities of clearing, settlement, asset servicing, transaction processing, trade reporting, and data services across asset classes, bringing enhanced resilience and soundness to existing financial markets, while advancing the digital asset ecosystem. To learn more, visit **dtcc.com**.

Clearstream is the innovative and trusted post-trade business for the global markets. It runs the leading securities and funds servicing ecosystems of tomorrow. The company operates the German and Luxembourg central securities depositories and an international central securities depository for the Eurobonds market. With 18 trillion euros in assets under custody, it is one of the world's largest settlement and custody firms for domestic and international securities. Its digital post-trade platform D7 provides a fully digital alternative to conventional physical issuance and processing of securities. It also delivers premier fund execution, distribution, data, and reporting services, covering over 55 fund markets worldwide. Clearstream is part of the Deutsche Börse Group, an international exchange organization and provider of innovative market infrastructures. To learn more, visit us at **clearstream.com**.

Euroclear group is the financial industry's trusted provider of post-trade services. Guided by its purpose, Euroclear innovates to bring safety, efficiency, and connections to financial markets to sustain economic growth. Euroclear provides settlement and custody to domestic and cross-border securities for bonds, equities and derivatives, and investment funds. As a proven, resilient capital market infrastructure, Euroclear is committed to delivering risk-mitigation, automation, and efficiency at scale for its global client franchise. The Euroclear group comprises Euroclear Bank, the International CSD, as well as Euroclear Belgium, Euroclear Finland, Euroclear France, Euroclear Nederland, Euroclear Sweden, Euroclear UK and International and MFEX by Euroclear. To learn more, visit **euroclear.com**.

Boston Consulting Group is a global consulting firm that partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG's success depends on a spirit of deep collaboration and a global community of diverse individuals determined to make the world and each other better every day. To learn more, visit **bcg.com**.



DTCC clearstream DEUTSCHE BÖRSE GROUP euroclear BCG