

Impact of Distributed Ledger Technology

in Global Capital Markets

Contacts



Allison Parent

GFMA
Executive Director
aparent@gfma.org



Elise Soucie

AFME
+44 (0)7990 558 659
elise.soucie@afme.eu



Laurence Van Der Loo

ASIFMA
+65 6622 5972
lvanderloo@asifma.org



Charles DeSimone

SIFMA
+1 212-313-1262
cdesimone@sifma.org



About GFMA

GFMA represents the common interests of the world's leading financial and capital markets participants to provide a collective voice on matters that support global capital markets. It also advocates on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows to end users. GFMA efficiently connects savers and borrowers, thereby benefiting broader global economic growth. The Association for Financial Markets in Europe (AFME) located in London, Brussels, and Frankfurt; the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong; and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian, and North American members of GFMA.

Authors



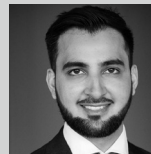
Roy Choudhury

Boston Consulting Group (New York)
Managing Director & Senior Partner
Choudhury.Roy@bcg.com



Kunal Jhanji

Boston Consulting Group (London)
Managing Director & Partner
Jhanji.Kunal@bcg.com



Humza Samd

Boston Consulting Group (London)
Project Leader
Samad.Humza@bcg.com



Simon Gleeson

Clifford Chance
Consultant
Simon.Gleeson@CliffordChance.com



Scott Bennett

Cravath, Swaine & Moore LLP
Partner
sbennett@cravath.com

Additional Authors: Ninad Nirgudkar, Boston Consulting Group (New York), nirgudkar.ninad@bcg.com

Foreword

Trust remains a foundational element of effective and robust capital markets. Regulatory policy is a core component of trust, ensuring market participants operate within a set of common rules that appropriately protect all stakeholders and meet the regulatory outcomes of policymakers. Balanced regulatory policy involves weighing growth and innovation with safety and soundness, market integrity, consumer protection, and overall financial stability.

The development of Distributed Ledger Technology (“**DLT**”) and the digital asset ecosystem motivates all market stakeholders to look to the future. Regulatory policy should seek to instill the same stability and protections in digital asset markets that exist in traditional, regulated financial markets, whilst allowing and supporting innovation. DLT holds promise for unlocking efficiencies, driving growth, and harnessing such innovation. Payments, settlement, and lifecycle events may be accomplished with greater safety and more efficiency; access may be expanded to a broader set of participants; and markets and market infrastructure may operate more effectively with improved liquidity. At scale, these developments could benefit the real economy. Where regulatory oversight and institutional risk management exists, this potential should not be ignored nor prohibited.

With this goal in mind, the research published in this report was prepared on behalf of GFMA members by Boston Consulting Group, Cravath, Swaine, and Moore LLP, and Clifford Chance to **evaluate the opportunities and risks of DLT and DLT-based Securities and DLT-based Payment Instruments used in conjunction with such securities**. Based on a ground-up, global analysis across the securities lifecycle, this report assesses the applicability of existing legal, regulatory, and risk management frameworks and outlines the possible benefits of a DLT-based ecosystem in capital markets, one of many potential areas for the application of DLT in financial services. Evaluating the potential of DLT includes ensuring that risks continue to be appropriately managed, and issuer, market, and investor protections are in place for all participants.

Our analysis shows that market participants make decisions around technology across a range of use case–specific considerations, leading to risk profiles that vary depending on these decisions. The selection of appropriate DLT network archetypes carry varying risk implications. “Private-permissioned” networks present limited incremental risk that can be mitigated by leveraging existing regulatory processes and therefore are analogous to technology operating in capital markets today. They introduce efficiencies and a platform for innovation, such as programmable security products. Where the legal nature of a service or a function does not change, the use of DLT-based systems to support or record the provision of that service or function should not result in incremental risk, nor necessitate a change in the regulation or regulatory characterization of that service or function. Policymaking should allow such networks to exist and flourish if demand warrants. Public networks (public-permissioned, public-permissionless) have their own set of network-specific risk considerations that should be evaluated in the context of applicable use cases.. These network archetypes may enable potential benefits for specific use cases, such as expanding broader access to capital markets and increasing levels of interoperability between participants. Capital market participants have developed applications on private-permissioned, public-permissioned, and public-permissionless networks, choosing the specific configuration best suited for their business needs to serve clients efficiently, within their own risk management frameworks. Regulated financial institutions have a continuous track record, from dematerialization, digitization, to off-premises cloud computing, of adopting new technology and implementing appropriate governance, controls, and processes to adequately manage risks as they evolve. Key to the success of DLT-based solutions is support for responsible innovation and flexible best practices for institutions to set controls based on the size, scope, and complexity of a given use case.

To illustrate the potential of DLT in capital markets, we examine three emerging uses cases within (1) Collateral Management; (2) Tokenization of Assets; and (3) Sovereign and Quasi-Sovereign Bonds.

The objective of this report is to support policymakers and market participants across jurisdictions to align on risk management tools and supervisory practices that ensures appropriate stability and protections for both regulated and unregulated market participants, but also allows the industry and economy to harness the benefits of DLT.

Leonardo Arduini
Chairman, GFMA
Markets Chief Operating Officer,
Citi



Adam Farkas
CEO, GFMA
CEO, AFME



Roy Choudhury
Managing Director & Senior Partner,
Boston Consulting Group



Simon Gleeson
Consultant
Clifford Chance



Scott Bennet
Partner
Cravath, Swaine & Moore LLP



Scope of this Report

This report explores two different implementation models of DLT for use across the securities lifecycle by regulated financial institutions: “Books and Records”, and “Tokenization”. They are defined as follows:

1. **“Books and Records”**: Existing internal recordkeeping, accounting, reporting, and other back-office functions centrally administered by a financial institution(s), which can be supported by DLT-based infrastructure; and
2. **“Tokenization”**: Digital representation of regulated financial instruments and money on a distributed ledger, reflecting an ownership right of the underlying asset, and its transfer between entities intermediated using the ledger. The report assumes that DLT is the enabling technology and catalyst for Tokenization. Although some features of Tokenization can be achieved without DLT (e.g., real-time settlement and fractionalization), this is out of scope for this report given market adoption of DLT.

The core asset classes in scope are the DLT-based forms of traditional equities, fixed income (including asset-backed securities), and derivatives.¹ These assets can exist on a distributed ledger in two formats:

1. **“Tokenized Securities”**, which are issued and custodied traditionally, but also converted onto a distributed ledger through a digital twin token that represents the underlying traditional security; and
2. **“Security Tokens”**, which are issued and custodied natively on a distributed ledger only, and therefore do not have a traditional security as an underlying basis.

It is important to distinguish between the two because they pose significantly different implications across the securities lifecycle. Where a distinction is not required, they are collectively referred to as **“DLT-based Securities”**.

In addition to the core scope of this report, traditional forms of money that are represented on a distributed ledger through Tokenization or otherwise are also considered.² These are defined as tokenized commercial bank money, DLT-based deposits (where the ownership of commercial bank deposits is reflected natively on a distributed ledger) and, as may be applicable, special purpose forms of central bank digital currencies (**“CBDCs”**) that may be designed for specific use by wholesale market participants. They will be collectively referred to as **“DLT-based Payment Instruments”**. GFMA members underline the importance of DLT-based Payment Instruments to realize the benefits of Delivery-versus-Payment (**“DvP”**) settlement for DLT-based Securities transactions, the distribution of coupons, dividends, and other proceeds on a distributed ledger.³

These in-scope assets either meet the classification conditions for **Group 1a** digital assets as set out by the Basel Committee on Banking Supervision (**“BCBS”**) under its new **“SCO60: Cryptoasset exposures”** standard in the Basel Framework⁴, or are acknowledged as out of scope for this framework.⁵ In line with this, there is a crucial difference between DLT-based Securities and DLT-based Payment Instruments as defined above, and other digital assets, such as cryptocurrencies, that do not represent traditional assets or fail to effectively link value at all times to traditional assets. Such digital assets are out of scope and not considered in this report.⁶

1 Tokenization also includes the representation of other tangible assets (e.g., commodities) and intangible assets (e.g., copyrights and patents) on a distributed ledger, but this is out of scope for this report. Additional use cases for Tokenization also exist but are out of scope for this report.

2 The use of money and deposits as an asset class in this report does not include Foreign Exchange.

3 ASIFMA, “Tokenised Securities: A Roadmap for Market Participants and Regulators”, 2019.

4 The Basel Framework is the full set of standards of the BCBS, which is the primary global standard setter for the prudential regulation of banks.

5 BCBS, “Prudential treatment of cryptoasset exposures,” December 2022; see SCO60.3 for specific detail on CBDCs etc.

6 Ibid.

A decorative graphic consisting of numerous thin, white, wavy lines that flow horizontally across the page, creating a sense of movement and depth. The lines are layered and overlap, giving the impression of a dynamic, fluid motion.

Executive Summary

This report provides a comprehensive assessment of the opportunities and risks posed by Distributed Ledger Technology (DLT) – including DLT-based Securities (both Tokenized Securities and DLT-native Security Tokens) – and associated activities across the end-to-end securities lifecycle. Co-developed with Global Financial Markets Association (GFMA) member firms, the report represents the perspectives of industry practitioners who are pioneering research and real-world applications of DLT use cases across the world.

Innovation continues to redefine the art of the possible. Progress in distributed computing and data encryption – brought together in DLT and the emerging digital asset ecosystem – could play a fundamental role in the next major wave of developments in capital markets. Examined through ground-up analysis in this report, market participants have identified areas where new technology could play a pivotal role in the coming decade and beyond. These areas include new approaches to deliver operational efficiency, cost efficiencies, product innovation, broader market access, and new liquidity pools.

Current discourse is rightly focused on ensuring DLT applications satisfy regulatory requirements and mitigate against any potential risks associated with the use of new technology. To this end, several jurisdictions are rolling out sandboxes or pilot regimes that facilitate firms to experiment with and issue DLT-based products to their clients. At the same time, there are live use cases in capital markets, such as those profiled in this report, that are already starting to capture opportunities and realize benefits for clients, while remaining compliant with applicable rules and regulations.

The emergence of DLT and the digital asset ecosystem presents a critical inflection point. As regulators globally are forming policy to govern the ecosystem, it is essential that policymaking seeks to instill consistent stability and protections in digital asset markets for market participants. The objective of this report, therefore, is to support policymakers and market participants across jurisdictions in identifying regulation, supervision, and risk management practices that support appropriate stability and protections for all industry stakeholders, but also allow the industry and economy to harness the DLT's benefit. To further this objective, the key findings explored in this report, and summarized in the Executive Summary, include the following:



1 | Emerging use cases are proving the benefits possible from a complementary, DLT-based ecosystem. DLT could unlock transformative benefits (e.g., ~\$20B USD annually in global Clearing and Settlement costs)⁷, and innovation (e.g., a ~\$16T USD global market for tokenized illiquid assets by 2030)⁸. Use cases are centering around asset classes, such as corporate bonds (e.g., Project Mars, a European Investment Bank bond issuance), which stand to benefit from the efficiency and liquidity benefits DLT could offer. In the long-term, this could enable a phased evolution towards a complementary, DLT-based capital markets ecosystem, coexisting alongside existing infrastructure. This ecosystem could be marked by broader market access (e.g., through fractionalization that reduces minimum ticket sizes), tailored value propositions to the needs of issuers and investors (e.g., faster time-to-issue for select asset classes), and enhanced risk mitigation (e.g., reduced operational risk throughout post-trade processes) when operating at scale. [See Executive Summary Section 1, page 10.](#)



2 | DLT-specific risk management can build on existing oversight frameworks. DLT-specific risk must be assessed across three dimensions, driven by the unique requirements of the use case being developed: (1) the chosen implementation model (Books and Records vs Tokenization); (2) lifecycle activity (Primary Market vs Secondary Market vs post-trade); and (3) the chosen DLT network archetype (private-permissioned, public-permissioned, public-permissionless). Private-permissioned networks are the closest analogue to traditional financial market infrastructure (e.g., settlement systems), but may have limited built-in interoperability. Public networks have a clear scope for broader connectivity and increased access, and therefore have distinguishing risk considerations for which mitigations are in various stages of development and implementation. Financial institutions have a successful track record of integrating transformative technological innovation. Existing regulatory and prudential policy (e.g., liquidity and capital requirements), existing risk management frameworks (e.g., operational and cyber resiliency), and newer DLT-specific risk mitigations as outlined in this paper, provide robust risk management that enables safe and secure innovation. This paper therefore cautions that any punitive, DLT-specific prudential treatment is unnecessary and could serve to be counter-productive, increasing both the regulatory and financial burden of DLT-related innovation by regulated financial institutions. [See Executive Summary Section 2, page 15.](#)



3 | Resolving legal and regulatory ambiguity could enable a level playing field that promotes safe and sound innovation. The resolution of legislative constraints and legal ambiguity in the scope and application of regulation, which necessarily varies by jurisdiction, is critical to prevent unintended consequences on the evolution of a DLT-based capital markets ecosystem that is compliant with global regulatory perimeters. A globally-harmonized approach, with jurisdiction-specific nuance and risk-specific distinctions, can help ensure policy development occurs in parallel with an early focus on interoperability to build and improve upon the standard of traditional markets, while protecting from the development of federated and siloed “digital islands”. [Explored in Executive Summary Section 3, page 30.](#)

Despite the growing momentum in developing DLT use cases, there is still no widespread adoption of DLT-based Securities. DLT-based issuances have been largely experimental, and liquidity in Primary and Secondary Markets remains far below levels of institutional adoption anticipated in the long-term once barriers to adoption are addressed. While experimentation is a necessary intermediate stage in this evolution, there is a danger that siloed approaches, as well as diverging regulatory regimes, could undermine progress towards the tangible, coordinated outcomes required to establish a broader DLT-based ecosystem.⁹ Absent this necessary alignment, market participants may have varying degrees of expertise in the operational capabilities required to plan, research, and launch larger-scale initiatives.

⁷ Santander, Innoventures, Oliver Wyman, Anthemis Group, “The Fintech 2.0 Paper: rebooting financial services”, 2015.

⁸ BCG and ADDX, “Relevance of on-chain asset Tokenization in crypto winter”, 2022.

⁹ ASIFMA, “Tokenised Securities in APAC—A State of Play”, 2021.

To build confidence among industry participants a cross-industry consensus is necessary, both to promote development around specific use cases, and encourage stakeholders to work proactively to shape the emerging ecosystem in this foundational state of development. The GFMA and its members have therefore set out five calls to action, for industry participants and regulators alike, to overcome existing barriers to adoption and advance the development of DLT-based capital markets.

Recommendations – five imperatives to achieving network effects.



1 | Harmonize global regulatory and legal frameworks: Current laws and regulations applied to DLT assets are generally those developed for traditional assets, creating inadvertent outcomes - either de facto prohibitions or an imposition of contradictory requirements. Considering adaptations to existing legal and regulatory structures is fundamental in promoting the development of transparent, disciplined, risk-focused, and effective market infrastructure. While different jurisdictions are facing individual and global challenges and as such, legislation is at different levels of maturity, we believe that the development of harmonized and risk-consistent policy positions across different jurisdictions would be a significant benefit both for the market and for governments and regulators.



2 | Enable interoperability | Build consensus on common standards & vision for DLT-based markets: To enable interoperability, participants must build on existing processes and broaden alignment on a framework of standards to guide market-level compatibility. This alignment would include participants agreeing on key areas including technology architecture design, smart contract standards and governance, linkages with traditional infrastructure – alongside risk identification, mitigation, and management – and specific roles and responsibilities. This would also entail exploring initiatives that cover public networks as well as private-permissioned networks, with appropriate risk mitigation.



3 | Pool liquidity | Focus on viable Primary & Secondary Markets for high potential asset classes: By focusing on specific assets and expanding to the full security lifecycle, financial institutions can design solutions that pool more sources of liquidity and increase the chances of attaining a viable market. Industry participants can focus on assets where the inefficiencies are well-documented and the cost of conversion is less onerous.



4 | Technology | Collaborate on the advancement of DLT to promote new technical solutions: Industry practitioners, in collaboration with authorities, are coming together to promote, sponsor, and collaborate on further research and development of DLT-specific solutions. Cross-industry participation distributes the cost behind a joint-venture and can accelerate the timeline to key outcomes, which can encourage smaller institutions with less appetite for capital expenditure to participate, generating positive externalities for capital markets at large.



5 | DLT-based Payment Instruments | Achieve true DvP settlement with DLT-based commercial bank money: DLT-based payment mechanics are a key enabler for settlement for any form of DLT-based capital markets. While DLT-based technology can align settlement of legacy payment tools with delivery of securities, DLT-based Payment Instruments in the form of tokenized commercial bank money and deposits (where representation of deposit account balances at commercial banks are reflected on a distributed ledger to support settlement) should be broadly developed to support more efficient and effective payment tools.

Full report preview

The comprehensive report that follows includes: a detailed overview of DLT, including the infrastructure and the digital assets represented on this infrastructure; a phase-by-phase impact assessment across the securities lifecycle; an exploration of live use cases; legal and regulatory considerations and recommendations; and barriers to adoption. To close the report, GFMA members present critical calls to action from all market participants to drive progress towards network effects, working in dialogue across key areas. For regulators, it could help inform efforts around emerging legal and regulatory frameworks, with an aim of protecting markets and promoting innovation. For industry, it provides detailed potential areas for further dialogue to accelerate ongoing research and development.

As an overarching guiding principle, legal and regulatory frameworks should be designed in line with the “same risk, same activity, same regulatory outcome” and “technology-agnostic” risk-based guiding principles that support, rather than deter, industry innovation and adoption. The GFMA and its members underline the importance for all market participants to contribute toward ongoing research and development of DLT, and the representation of regulated financial instruments and money on this infrastructure. Punitive penalties for the use of a particular technology, without clearly defined risk-based justification, could be detrimental to innovation in the market and have unintended consequences on the evolution of a future DLT-based market structure within the regulatory perimeter.

Significant contributions have been made by a wide selection of GFMA members and non-members across the financial services ecosystem, together with industrial and legal advisers. Analysis has also reflected upon regulatory publications across jurisdictions to ensure central areas of concern are evaluated. We hope this provides a value-added perspective that drives public-private dialogue and advances progress on the topic.

For further details, please see the following chapters of this report:

- **Chapter 1: Distributed Ledger Technology (DLT) and Tokenization** | Providing a clear and unambiguous definition of the key terms and concepts required with the goal of providing a consistent cross-industry framework for discussions of DLT, Tokenization, technology, and infrastructure.
- **Chapter 2: Impact of Tokenization Across the Securities Lifecycle** | Examining the impact across the end-to-end securities lifecycle on roles and responsibilities, workflows and activities, technology and infrastructure, financials, and existing levels of risk and potential for DLT to enable incremental mitigation.
- **Chapter 3: Use Cases** | Exploring real-world use cases, developed with GFMA members, to provide insights and best practices on how existing risk-management governance and processes are being used to drive decisions around the role of technology for specific use cases.
- **Chapter 4: Legal and Regulatory Landscape** | Demonstrating where existing regulations sufficiently addresses DLT-enabled operations and Tokenized Securities and highlighting gaps in legal and regulatory frameworks based on the “same risk, same activity, same regulatory outcome” and “technology-agnostic” risk-based guiding principle.
- **Chapter 5: Towards a Future DLT Ecosystem and Barriers to Adoption** | Outlining the additional barriers to adoption cited by GFMA members and other market participants.
- **Chapter 6: DLT Ecosystem Recommendations and Calls to Action** | Pragmatic next steps proposed by industry participants to work toward a desirable DLT ecosystem. Prioritizing focus areas that require cross-industry collaboration and public-private dialogue to unlock and drive progress.

1 | Unlocking Benefits Across the Securities Lifecycle

The case for DLT in traditional capital markets has typically been focused on operational efficiencies in Clearing and Settlement and post-trade activities. However, our research suggests DLT offers technical capabilities that could support broader developments across the end-to-end securities lifecycle. This includes clear opportunities for growth and value creation, as well as incremental risk mitigation. Through a detailed impact assessment, these opportunities have been reviewed across implementation models (Books and Records and Tokenization) and qualitatively scored based on the degree of positive impact. This is synthesized in Exhibit ES.1 below, with an extensive discussion in Chapter 2 of the report.

Exhibit ES.1
Impact of DLT-based Securities on Workflow Efficiency, Financials and Value Creation, and Risk Mitigation Across the Securities Lifecycle

| Implementation models | Books and Records + Tokenized Securities | | | | |
|--|--|-------------------|-------------------------|---------|-----------------|
| | Primary Markets | Secondary Trading | Clearing and Settlement | Custody | Asset Servicing |
| Overall DLT Impact | Medium | Medium | High | High | High |
| Workflow Efficiency | Medium | Low | High | High | High |
| Financial Opportunity & Value Creation | High | High | High | High | High |
| Incremental Risk Mitigation | Low | Low | High | Medium | Medium |

■ Low degree of positive impact
 ■ Medium degree of positive impact
 ■ High degree of positive impact

Source: BCG analysis

- 
Primary Market Issuance (MEDIUM): Primary issuances include manual and bespoke processes that could benefit from digitization and automation to drive operational efficiencies and mitigate risk.
- 
Secondary Market Trading (MEDIUM): Platforms with features such as Tokenization and fractionalization could help pool and deepen liquidity in Secondary Markets, particularly for illiquid assets.
- 
Clearing and Settlement (HIGH): DLT-based Clearing and Settlement could emerge as a complementary channel alongside infrastructure in traditional markets, with automated processes & risk mitigation.
- 
Custody (HIGH): DLT offers technical capabilities that could help establish “golden-source” records and workflow automation in post-trade processes, mitigating operational risk in Custody.
- 
Asset Servicing and Lifecycle Management (HIGH)¹⁰: DLT could automate Asset Servicing and Lifecycle Management workflows for corporate actions, tax withholding, & regulatory reporting that mitigates operational & compliance risk.

¹⁰ Asset Servicing & Lifecycle Management in this report includes other lifecycle activities such as regulatory reporting for the sake of analysis.

Our research points to the potential for financial outcomes that include lower operating costs, financial resource efficiencies, and innovation-led growth. The gains in operating margin could facilitate broader access to capital markets by issuers and enable smaller-size issuances (e.g., bond origination is traditionally for deal sizes above \$300 million USD¹¹). This could be particularly impactful in emerging markets where capital market ecosystems are in the early stages of development, broadening access and accelerating innovation. These financial outcomes are broken out below, with figures that should be considered as illustrative and based on a DLT-based ecosystem operating at scale.^{12, 13}



1 | Operating Cost Efficiencies: *Back-office efficiencies from workflow automation.*

~\$15-20 billion (USD) in annual global infrastructure operational cost savings have been estimated, driven by smart contract-driven process automation in areas such as settlement and corporate action administration.¹⁴ The opportunities for savings are particularly concentrated in fixed-income and private market assets.



2 | Financial Resource Efficiencies: *Freed collateral and other balance sheet efficiencies.*

At the end of 2022, there was an estimated ~\$19 trillion (USD) worth of addressable global collateral outstanding across repurchase agreements (repos), OTC derivatives, and securities lending.¹⁵ This opportunity could therefore range well beyond ~\$100+ billion (USD) annually in freed financial resources that could be redeployed to generate incremental returns.¹⁶



3 | Innovation-Led Growth: *New product innovation, expanded liquidity pools, and market access.*

Emerging investor demand for DLT-based Securities is likely focused on two areas. The first is fixed-income, such as corporate bond markets (currently worth ~\$41 trillion USD¹⁷, where the transparency and fractional issuance enabled by DLT could broaden access to wider pools of liquidity in “off the run” or non-standardized areas. The second is the Tokenization of illiquid and private asset classes like investment funds. The global value of tokenized illiquid assets is estimated to be worth ~\$16+ trillion USD by 2030, from a base of ~\$0.3 trillion USD today.¹⁸ New instruments (e.g., tailored frequency income payments) through product innovation may also act as a key value driver to serve client needs.¹⁹

Use Cases are Demonstrating Early Real-World Benefits

Market participants have been exploring DLT for several years. As of December 2022, ~85% of GFMA members had a use case either at pilot stage or in production, with product innovation and workflow efficiencies the most common drivers cited.²⁰ Through these developments, an array of DLT-based solutions and platforms are emerging, ranging from proof-of-concepts to full market deployment. These are providing early validation on the value that DLT could unlock while operating within existing regulatory and risk frameworks. A non-exhaustive list of select projects are summarized below:

11 ASIFMA, “Tokenised Securities: A Roadmap for Market Participants and Regulators”, 2019.

12 For more details see, for example, an E.U. study on economic benefits: European Parliament, “Increasing European added value in an age of global challenges”, 2023.

13 On April 20th, 2023, Mr. Christopher J. Waller, Member of the Board of Governors of the Federal Reserve System remarked on the “considerable promise” of Tokenization citing its ability to be “programmable” and enable “atomic settlement” with use of smart contracts. Waller, Speech at the Cryptocurrency and the Future of Global Finance, April 2023.

14 Santander and Innoventures, “The Fintech 2.0 Paper: rebooting financial services”, 2015.

15 SIFMA repo factsheet end 2022; ICMA Survey June 2022; ICMA Survey December 2022; ICMA APAC Survey 2022 and 2021; International Securities Lending Association (“ISLA”) website; BIS ORC Derivatives statistics at end June 2022; BCG analysis 2023.

16 Security Tokenization survey of GFMA members, November to December 2022; n=39.

17 International Capital Markets Association (ICMA), “Bond market size”, 2020.

18 BCG and ADDX, “Relevance of on-chain asset Tokenization in crypto winter”, 2022.

19 Security Tokenization survey of GFMA members, November to December 2022; n=39.

20 GFMA member surveys, Nov-Dec 2022.



Collateral mobility | HQLA's Books and Records Digital Collateral Registry is a platform built on a private-permissioned DLT network provided by R3 Corda. It records the ownership transfers of securities, while the underlying securities remaining in the Custody location of the participating triparty agents and custodians. When collateral needs to be exchanged between participants, the platform enables instant and simultaneous transfers on the platform, so-called Delivery vs. Delivery Delivery ("**DvD**"), swapping ownership of securities and avoiding the traditional Custody chain and settlement cycle. Transactions can be predetermined to occur at precise times through the day. This reduces intraday credit exposures and liquidity requirements to enable capital savings and minimize the scope for trade fails.



Intra-day repos | J.P. Morgan's Digital Financing Application, running on the Onyx Digital Assets DLT platform built on a private-permissioned DLT network, enables true DvP settlement for repurchase agreements ("**repos**"). The platform enables the simultaneous exchange of tokenized deposits and collateral, and settled over \$500 billion USD in transaction value by the end of 2022. Precise, and more frequent, intra-day settlement cycles, free collateral that would otherwise be subject to longer, traditional, settlement cycles (e.g., T+2) for productive redeployment. The 24/7 availability of the platform enables borrowers and lenders with uninvested cash or securities at the end of traditional business hours to benefit from its use. J.P. Morgan has also reported operational efficiency gains through a near-zero trade fail rate.



Digital bonds | In January 2023, the European Investment Bank ("**EIB**") issued the digitally-native, £50 million GBP three-year floating 'Mars' bond on the private-permissioned HSBC Orion platform. The Security Token issuance was mirrored with anonymized details on the public-permissionless Ethereum Mainnet. Along with HSBC, BNP Paribas and RBC Capital Markets were joint-lead managers. The banks reported that the EIB benefitted from a significantly lower issuance cost compared with traditional Primary Markets bond issuance and instant and simultaneous (atomic) DvP settlement. Additionally, in February 2023, the Hong Kong Monetary Authority ("**HKMA**") announced the successful offering of a \$800 million HKD tokenized green bond using the Goldman Sachs GS DAP™ Tokenization platform. HKMA leveraged a private-permissioned network with a special purpose CBDC designed expressly for the purpose of settling the primary placement of this bond.²¹ Additional detail on digital bond issuances, and the variety of network archetypes that been used to do so, is included for reference in [Annex 2: DLT-based Security Issuances](#).

As demonstrated by these use cases and those profiled later in the report (see [Chapter 3 | Use Cases](#)), implementations of DLT have largely focused on specific asset classes and transaction types such as bonds, over-the-counter ("**OTC**") derivatives and repo. These share two common drivers: (1) a clear financial opportunity from efficiency gains or innovation; and (2) market readiness for innovation and adoption around specific market structure attributes (e.g., shallower liquidity, relative "opaqueness" trading OTC, long issuance processes), workflow inefficiency, and the maturity of electrification. These projects provide early insights into the expected pattern of DLT adoption in capital markets, which could follow these drivers.

A recent BIS Bulletin report, *The Tokenization Continuum*, provides a similar perspective citing that "Tokenization could bring benefits" to assets and the way transactions and transfers occur, but adoption will occur on a "continuum and highlight a trade-off: where Tokenization is easiest, per-unit gains are likely to be modest" and

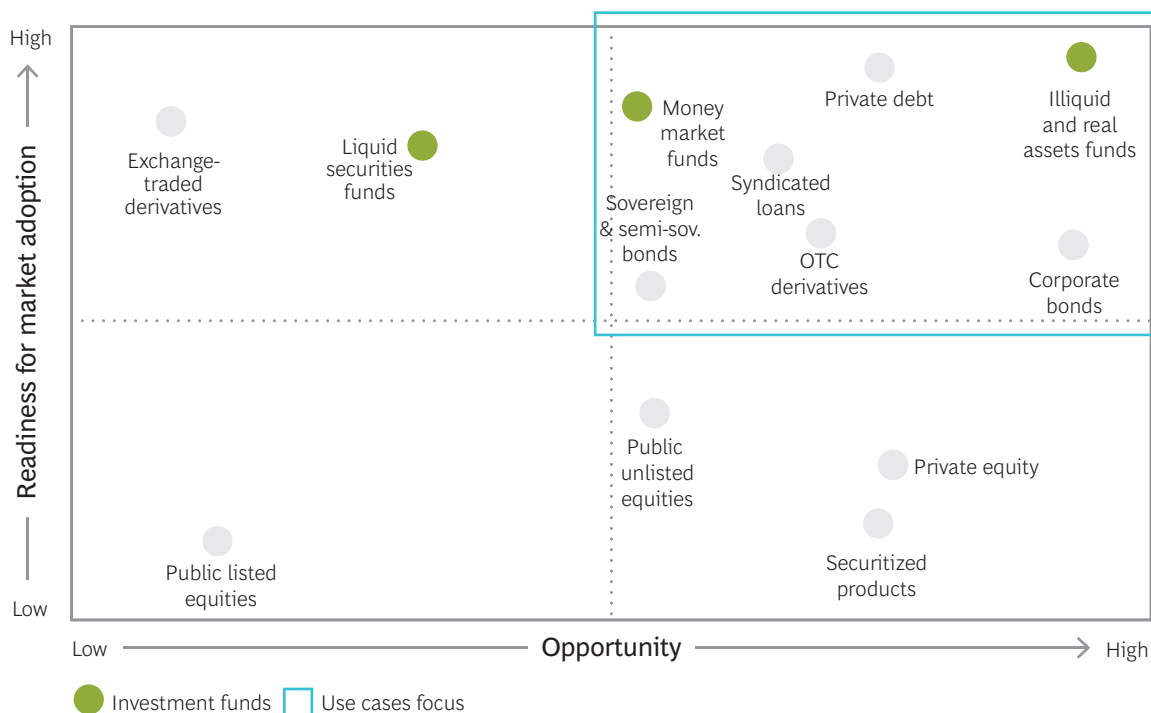
21 Additional information regarding the transaction can be found at the following link: Hong Kong Monetary Authority - HKSAR Government's Inaugural Tokenised Green Bond Offering (hkma.gov.hk).

conversely “where Tokenization is difficult the potential benefits are the largest”.²² As a result, the authors suggest Tokenization efforts to “focus on identifying assets that are suitable for Tokenization” and have enough volume for a sizeable impact.²³

Liquidity in a DLT ecosystem may therefore pool in specific asset classes where there is clear opportunity and market readiness (see top right quadrant of Exhibit ES.2 below). Homogeneous adoption may be less likely in high-volume, efficient markets such as public equities, where the incremental opportunity is limited.

Exhibit ES.2

Asset-Classes Show Varying Suitability For Adoption Onto DLT



Source: BCG analysis; Adapted from JP Morgan and BCG, 'The Future of Distributed Ledger Technology in Capital Markets', November 2022

22 Aldasoro, Doerr, Gambacorta, Garratt, Wilkens, BIS Bulletin No 72 “The Tokenization continuum”, April 2023.

23 Ibid.

Toward a Complementary DLT-Based Ecosystem

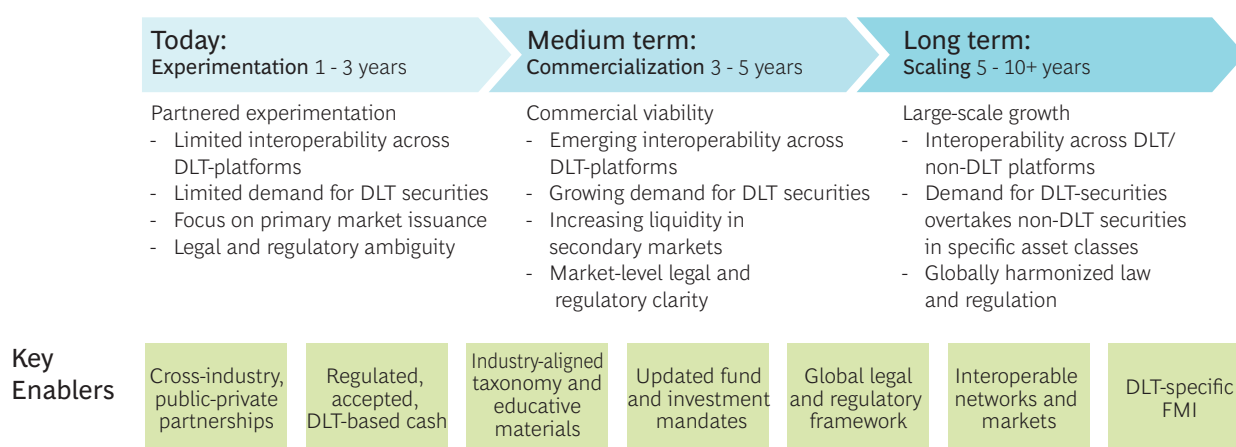
The concentration of use cases in specific asset classes and transaction types are marking the early beginnings of a phased evolution toward a complementary ecosystem that exists alongside traditional capital markets. This ecosystem could offer broad access and value propositions that are responsive to the needs of issuers and investors, underpinned by operational efficiency, financial resource efficiency, new products and services, improved competition, and new risk mitigation approaches when operating at scale.

The evolution is likely to be a phased development, enabled by advancements in technical capabilities, clarity around legal and regulatory frameworks, ongoing lessons learned from live use cases, established approaches to risk management for new considerations, and other areas. These enablers, which could develop in parallel, could significantly impact the speed of progress.

Three major phases are expected along this journey, beginning with **(1) Experimentation** – the current state of play, marked by ongoing research and development with a focus on technical capability development, Primary Market Issuances, and legal and regulatory ambiguity; **(2) Commercialization** – marked by emerging Secondary Market liquidity as issuer and investor demand scales, and ambiguity is resolved; and **(3) Scaling** – marked by the predominance of DLT-based Primary and Secondary Markets for specific asset classes and transaction types with legal and regulatory frameworks that are harmonized across jurisdictions, and interoperability across platforms. This is set out in Exhibit ES.3 below.

Exhibit ES.3

Possible Future Developments of a DLT Ecosystem



Source: BCG analysis, GFMA Member Interviews

To guide the formation of a viable and differentiated DLT ecosystem, consensus is required among all stakeholders on **(1) robust risk management, (2) globally harmonized legal and regulatory frameworks; and (3) key calls to action to achieve network effects.**

2 | A Holistic Understanding of DLT-Specific Risk

The GFMA and its members strongly advocate that the implementation of DLT be operationalized in a manner that meets the high existing standards of regulated capital markets. Safeguards must be ensured for all market participants and mitigants must similarly protect financial markets more broadly. To this end, the GFMA and its members have developed a detailed risk assessment, with preliminary risk mitigations for the introduction of DLT Books and Records and DLT-based Securities related to the use case components outlined above. These recommendations build upon existing governance and control processes in line with the International Organization of Securities Commissions (“**IOSCO**”) *Principles for Financial Market Infrastructure*,²⁴ *Operational Resilience of Trading Venues and Market Intermediaries During the COVID-19 Pandemic*,²⁵ *BCBS Principles for Operational Resilience and Principles for Sound Management of Operational Risk*,²⁶ and related principles from the Financial Stability Board (“**FSB**”),²⁷ that all collectively provide the tools necessary to (1) explore the potential for DLT-specific risk, and (2) provide mitigations to ensure risks can be mitigated and managed to ensure safe and secure development of DLT. The GFMA and its members recognize the considerable progress in global alignment of operational and cyber resilience frameworks and seek to aid regulators in a journey towards a harmonized, technologically-agnostic, approach for the in-scope digital assets based on the legal and regulatory analysis contained herein..

We believe DLT can play diverse roles in capital markets across three use case considerations that can differ significantly based on (1) implementation model (‘Books and Records’ vs ‘DLT-based Securities’), (2) digital asset type (Group 1a vs. Group 1b/2 in the BCBS crypto asset framework), and (3) lifecycle activity (Primary Markets, Secondary Markets, and post-trade).

A blanket regulatory approach anchored on a specific type of technology could therefore fail to distinguish use cases that are analogous to similar technology and financial market infrastructure already being used in capital markets today. Similarly, regulatory requirements should consider the risks and mitigants entailed in based on the particular use cases of a technology, not on the characteristics of the technology alone.

To help disaggregate this conflation and enable a focused regulatory approach on the associated risk, the research published in this report includes the following findings on key risk drivers:

(1) Implementation Model, (2) Lifecycle Activity, and (3) DLT Network Archetypes.

Market participants will need to adjust their assessment of risk management implications accordingly depending on how each of these three components are configured.

(1) Implementation Model



Books and Records

DLT Risk Assessment: DLT-based Books and Records systems are focused on internal recordkeeping (e.g., collateral management), accounting, reporting, and other back-office operations on private-permissioned networks. Books and Records, along with the book entries recorded on such systems, are operated with risk management that is analogous to traditional Books and Records systems (set out under “DLT Risk Mitigation”

24 BIS-IOSCO, “Principles for Financial Market Infrastructure”, April 2012.

25 IOSCO, “Principles on Outsourcing” October 2021, and “Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic”, January 2022.

26 BCBS, “Principles for Operational Resilience”, March 2021, and “Principles for Sound Management of Operational Risk”, March 2021.

27 Such as: FSB, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting”, and Format for Incident Reporting Exchange (FIRE), April 2023; and the FSB’s Guidance on “Operational Continuity while in Resolution”, August 2016.

below). In line with these characteristics, where the legal nature of a service or a function does not change, the use of DLT-based systems to support or record the provision of that service or function should not result in incremental risk, nor necessitate a change in the regulation or regulatory characterization of that service or function. Indeed, the BCBS have deemed DLT-based Books and Records for: “dematerialized securities that use electronic versions of traditional ledgers and databases that are centrally administered” as out of scope for additional prudential treatment.²⁸

DLT Risk Mitigation: Regulated financial institutions are exploring and implementing DLT-based technologies and systems to support their existing internal electronic recordkeeping, accounting, reporting, and other back-office functions (“Books and Records”).

Where the legal nature of a service or a function does not change, we do not believe that the use of DLT-based technology to support or record the provision of that service or function should result in a change in the regulation or regulatory characterization of that service or function. The Books and Records systems of regulated financial institutions, and the adoption and use of any new replacement technology, are subject to existing regulatory requirements and ongoing comprehensive supervisory oversight frameworks wherein financial institutions have integrated governance and controls to help identify and mitigate risks.

As regulated financial institutions innovate using DLT protocols to enhance Books and Records capabilities, this should not result in a change in the regulatory characteristics of the assets recorded on such Books and Records systems – including additional punitive capital treatment or creating barriers for responsible innovation. A reclassification of such assets to “tokens” should only be applied where there is a change in the legal nature of the service provided or the function for which it is used. Where one or more firm(s) uses a private-permissioned, internal DLT-based system, the regulatory focus should be on whether the use of that system satisfies the financial institution’s regulatory obligations to maintain efficient and effective systems and controls, in a safe and sound manner.

DLT-based Books and Records systems along with the book entries recorded are analogous to currently used Books and Records systems and their records where the following criteria are satisfied:

- The control environment is private-permissioned and internal, with proper security ringfenced within the regulated financial institution’s technology and security control environment, in line with regulatory requirements, subject to appropriate supervisory governance standards, and where the regulated financial institution is the only entity with direct read/write access²⁹;
- The Books and Records systems record debits, credits, and other asset transfers on behalf of the financial institution, consistent with existing approved traditional book entries that record changes to customer positions. In such circumstances, third parties cannot directly affect changes without the approval and vetting of such instructions by the regulated financial institution under its supervisory approved governance and controls;
- The Books and Records may also provide reporting and statements of account to the regulated financial institution’s customers, as permissioned by the financial institution, without direct third-party access; and
- The Books and Records provide a mechanism for regulated financial institutions to reconcile and to unilaterally correct any mistakes in line with internal governance control protocols.

²⁸ Ibid.

²⁹ It is important for supervisors to differentiate a Books and Records system from an open or even a private, permissioned, but shared ledger. Specifically, no third party may directly access a bank’s Books and Records system without express approval and permission from the bank.

The introduction of new technology alone, such as the use of DLT protocols by regulated financial institutions for Books and Records capabilities, akin to traditional banking activities, should not, in itself, give rise to additional regulation or capital charges that could impede the ability of well-regulated and supervised banking institutions to invest and to adopt innovative technologies. Regulated financial institutions have a history of demonstrating competency in evaluating and mitigating the risk of incorporating new technology, especially operationally-related solutions.

Tokenization

DLT Risk Assessment | Group 1a assets, as defined in the BCBS consultation for the prudential treatment of cryptoasset exposures, include the tokenized formats of regulated financial instruments (equities, fixed income including asset-backed securities, derivatives), with payment for such assets accomplished with DLT-based Payment Instruments (commercial bank money and deposits, and central bank money) that can be represented on a distributed ledger. As acknowledged by the BCBS standard, this does not alter the credit or market risk of the underlying assets and therefore carries the same risk profile.³⁰ This has also been demonstrated by the credit rating to the City of Lugano’s recently issued unsecured municipal bond in January 2023. Assigning a Aa3 rating, Moody’s commented:

“The Aa3 debt rating mirrors the City’s long-term issuer rating of Aa3 and is equal to debt ratings assigned by Moody’s to Lugano’s traditional bond issuances. The notes will have the same status of the issuer’s senior unsecured rated bonds and, in Moody’s view, the different technology will not add materially higher risks compared to a traditional issuance.”³¹

DLT Risk Mitigation | Regulated financial instruments and commercial bank money are subject to comprehensive regulatory, prudential capital, and liquidity frameworks, as applicable. The tokenized forms of these assets can therefore be governed by existing policies and procedures. Similarly, DLT-based Payment Instruments used as payment for such assets comprise either commercial bank money subject to prudential regulation, or central bank money as a liability of the central bank, subject to central bank policy, and available only to regulated participants. Group 1a DLT-based Securities and DLT-based Payment Instruments can also be clearly identified based upon the classification conditions that are distinct and separate from Group 1b/2a/2b digital assets. The GFMA developed an approach to classification of digital-assets to support our response to the BCBS discussion paper on *Designing a Prudential Treatment for Crypto-Assets*³² and Financial Stability Board’s (“FSB”) consultation on the *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets*.³³

The classification approach reflects the principle that the treatment of digital-assets should be underpinned by clear methodology for identifying different types of digital-assets’ risk which will allow for tailored regulatory treatment, as appropriate, to mitigate reputational risks by conflating use cases of DLT, promoting legal clarity and confidence for asset managers, investors, and issuers (see Annex 1).

30 BCBS, “Prudential treatment of cryptoasset exposures”, December 2022. We note that there are network specific considerations, and we have reviewed these risks separately to avoid overlap.

31 Moody’s, “Moody’s assigns Aa3 rating to City of Lugano’s upcoming digital bond”, 2023.

32 Joint Trades Comment Letter – Second Consultation on Prudential Treatment of Cryptoasset Exposures, 2022. Please reference page 4, 29-37 for additional detail on the proposed infrastructure risk add-on for Group 1 cryptoasset exposures.

33 FSB, *Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets*, October, 2022.

(2) Lifecycle Activity

DLT-based Securities could lead to significant mitigation of operational, counterparty credit and systemic risks, but a limited number of additional risk considerations (generic across DLT network archetypes) will also require mitigations. Regulated financial institutions are well-placed to manage these through existing BCBS capital and liquidity supervisory frameworks and guidelines, which provide a proven basis to manage known financial and nonfinancial risk, as well as unforeseen risks through the imposition of buffers and other charges.³⁴ In addition, new risk mitigations are being developed and proven through live use case testing and market implementations. These risk considerations across the lifecycle are summarized below, along with mitigations:



Primary Market Issuance

DLT-Lifecycle Risk Assessment: Given the ongoing development of policymaking to support the growth of DLT-based Securities, the level of participation in DLT-based Primary Markets remains relatively low compared to traditional capital markets. As a result, DLT-based Primary Markets could face increased levels of liquidity risk, challenging or impairing the ability of Transaction Managers³⁵ to place initial offerings. This could be compounded by the potential for fragmentation across multiple DLT platforms and lack of interoperability between them. Non-financial risk impacts will also need to be accounted for, including operational risk (e.g., integrations between DLT and non-DLT platforms and interoperability between DLT platforms) and compliance with additional disclosure requirements (e.g., offering documents required for DLT-based issuance).

DLT-Lifecycle Risk Mitigation: Transaction Managers can launch dedicated efforts to source liquidity and generate interest, alongside broader industry initiatives to pool liquidity in high potential asset classes and in this way support the formation of DLT-based Primary Market liquidity and mitigate potential liquidity risk. Similarly, interoperability across DLT-based platforms will be crucial to prevent fragmentation and ensure sufficiently liquid markets. Existing operational risk and operational resilience frameworks can provide a basis for achieving sound integrations between DLT and non-DLT platforms for non-financial risk considerations. Regulatory clarity would be helpful to inform the necessary legal documentation for Primary Markets issuances.



Secondary Market Trading

DLT-Lifecycle Risk Assessment: The potential bifurcation of trading liquidity between traditional and DLT-based Secondary Markets, as well as across different DLT-based trading platforms, needs to be managed. This could primarily affect native Security Tokens that, as a new security format, are likely to require new liquidity pools. Secondary Markets for Security Tokens are likely to exhibit poorer liquidity conditions for some time, until critical mass is reached. Traditional and Tokenized Securities may also provide an imperfect hedge to support market-making; however, it is likely that a spread between traditional and DLT-based Securities may form, especially as Secondary Market Trading activity increases. The potential need to immediately pre-position securities and cash for Clearing and Settlement for DLT-based Securities could impact liquidity in DLT-based Secondary Markets, acting as a barrier to entry for investors by tying up assets in pre-funding requirements.

DLT-Lifecycle Risk Mitigation: The development of bridges across traditional and DLT-based trading venues, and interoperability between DLT-based platforms could resolve fragmentation and mitigate trading liquidity risk. Technical on/off ramp solutions with conversion mechanisms (e.g., Tokenization/deTokenization) will play a central role, with precedents in the approach taken today between Depositary Receipts and ordinary shares. Incentivization for liquidity provision in DLT-based Securities (e.g., fee discounts) could also serve as

³⁴ Such as liquidity, capital, and funding requirements as set out in Basel III frameworks.

³⁵ The term Transaction Manager is used in this report to generalize across asset classes and subfunctions; it covers a subset of roles including Coordinator, Bookrunner, Arranger, Underwriter, and Placement Agent.

an important mitigant. Security Tokens can be integrated into existing workflows to broaden participation, and automated market makers can provide liquidity in return for pricing cross-format risk.

As broader initiatives develop across the industry, it is likely that interoperability will be greatly enhanced, along with required operational changes to support the formation of secondary liquidity and adaptation of existing workflows. Existing trading systems have leveraged the Financial Information Exchange (“FIX”) protocol to standardize messaging and integration. There is a risk that competing protocols and standards could hinder the goal of interoperability, which could have a significant impact on the ability to integrate liquidity pools, automate trades, and simplify the trading ecosystem. This should be addressed through an early and broad alignment on technical standards. Liquidity risks around pre-positioning can be mitigated by ensuring pre-funding requirements are set at levels that avoid trapping capital for time periods equivalent to or exceeding traditional Clearing and Settlement cycles. Broker-dealers can also lend liquidity to pre-funding requirements and earn a return.

Clearing and Settlement

DLT-Lifecycle Risk Assessment: DLT-based settlement may result in (although does not necessitate) higher levels of gross settlement in specific asset classes and transaction types. All else being equal, this could require more liquidity on-hand and increase “aggregate liquidity requirements” when operating at scale, contributing to liquidity risk.³⁶ This is in addition to the liquidity impacts from the need for pre-positioning of securities and cash discussed above in Secondary Market Trading. Finally, there is uncertainty and limited alignment across jurisdictions regarding the legal basis of Security Tokens and determination of settlement finality³⁷. This creates legal risk, particularly in the context of cross-border transactions.³⁸ Settlement finality, however, could also give rise to complex legal considerations in achieving DvP that vary by DLT network archetypes (further explored under “DLT Network Archetypes” below).

DLT-Lifecycle Risk Mitigation: In approaching these risks, it should be noted that DLT does not necessitate a gross settlement model and could be configured to support Deferred (or real-time atomic) Net Settlement where this could generate efficiencies or process advantages. However, regulatory guidance has begun to encourage real-time gross settlement in some jurisdictions outside the U.S..³⁹ Existing regulatory and risk frameworks can therefore provide applicable guidance for DLT-based Clearing and Settlement risk management. Legal clarity across jurisdictions will be required to clarify the status of Security Tokens. Regarding settlement finality, the use of private-permissioned or public-permissioned networks could help mitigate risk (refer to the discussion below under “DLT Network Archetypes”).

Custody

DLT-Lifecycle Risk Assessment: Differentiated operational risks could stem from new lifecycle management workflows, including private key management (to the extent applicable to the relevant asset) and data integrity between distributed and traditional ledgers.

DLT-Lifecycle Risk Mitigation: Qualified custodians are already implementing processes and standards (e.g., compliance with jurisdiction-specific account segregation requirements) to mitigate these risks. Private key management mitigants could include split keys (with quotas for signatures), account abstraction smart contracts (e.g., timelocks and social recovery) as upgrades to externally owned accounts developed by self-custodial wallets

³⁶ BIS, “On the Future of Securities Settlement”, 2020.

³⁷ The BCBS, in its paper entitled “Prudential Treatment of Cryptoasset Exposures”, has specified that an essential element of classification of a digital asset as a Group 1 asset is that “the applicable legal framework(s) ensure(s) settlement finality” SCO 60.14. As the BCBS states further: “Banks are required to conduct a legal review of the cryptoasset arrangement to ensure this condition is met, and make the review available to their supervisors upon request”. Id.

³⁸ Ibid.

³⁹ BIS-IOSCO, “Principles for Financial Market Infrastructure (Part 8, Annex D)”, 2012.

like MetaMask, parachute recovery functions (that sends keys or tokens to a pre-programmed governance address), and location-based signing. We note that as technology evolves, so too will risk mitigants, and the above is not an exhaustive list of such mitigants. Data integrity between distributed and traditional ledgers can be enabled through new, automated reconciliations, with recourse processes where erroneous transactions are recorded. This is equivalent to existing data reconciliations processes between non-DLT systems.

Asset Servicing and Lifecycle Management

DLT-Lifecycle Risk Assessment: DLT introduces additional risk considerations centered on data residency and privacy, regulation, and smart contracts.

DLT-Lifecycle Risk Mitigation: On data residency and privacy, participants may need to align on technology and governance architecture to protect sensitive corporate action, tax, and regulatory data from other members of the distributed ledger while still maintaining core efficiencies. It should be noted that DLT platforms can also play a crucial role in enabling data consolidation and control. Market participants may need to establish clear accountability, governance, and recourse for errors in smart contract execution (refer to the discussion below under “DLT Network Archetypes” for more details).

(3) DLT Network Archetypes

DLT network archetypes present differing profiles of risk that require specific mitigation approaches. Regulated financial institutions bring a proven track record of responsible innovation, drawing on the high standards of proven institutional-grade technology and operational risk management, operational resilience, cybersecurity, data protection processes, client suitability frameworks, and established know-your-customer (“**KYC**”)/anti-money-laundering (“**AML**”)/combating the financing of terrorism (“**CFT**”) procedures. Together, these can help protect market participants and ensure safe innovation across global capital markets.

There are three archetypes of distributed ledgers:



Private-permissioned: Closed-loop, private networks, which restrict access to only predetermined users and are typically governed by rules agreed to by, and that apply to, all users. Authentication can be used to determine privileges. This is the most common archetype used in capital markets today, and is characterized by its security and central control, which has proven to be well-suited to certain capital markets use cases. They may be less suited to use cases requiring large-scale interoperability given the closed nature of these networks and limited user bases, but interoperability can be achieved if required.



Public-permissioned: By using permissioned network-level participants, effectively created closed access networks that can vary by design, given defined selective restriction of access through authentication for certain governance, administration, or other privileges. They can also include designs with more open or publicly-available access (i.e., access is open, but authentication is used to restrict privileges to pre-determined users only). In these instances, public access could introduce new considerations around security and risk mitigations for use in capital markets use cases, while balancing the benefits of offering access to a broader user base and stronger network effects as adoption scales. There can also be benefits around operational resilience given the potential for broader distribution across a greater number of nodes.



Public-permissionless: Open, public networks that do not restrict access for privileges. These include some of the largest distributed ledger networks adopted at scale today, and therefore offer proven potential for significant network effects. For example, the leading public-permissionless networks have demonstrated strong operational resilience given distribution across many nodes. However, the absence of defined restrictions of access gives rise to heightened levels of potential risks and therefore the need for market participants' to leverage and adopt appropriate governance and control frameworks.

DLT network archetypes therefore have differing defining characteristics and technical attributes which impacts their suitability for different use cases. For example, private-permissioned networks are particularly well-suited to use cases that prioritize a closed network of permissioned participants for confidentiality and defined finality of settlement, rather than requirements for broad interoperability and access. The largest public-permissionless networks, on the other hand, offer a proven channel to reach a mass market that may be advantageous in the development of Secondary Market liquidity for some asset classes.

Each network-type has advantages and trade-offs that should be optimized for the specific requirements of a given use case.

Exhibit ES.4

Comparison of Defining Characteristics Across Distributed Ledger Network Archetypes

| | Private-permissioned | Public-permissioned | Public-permissionless |
|------------------------------------|---|--|--|
| Governance | Centralized | Centralized (for the relevant application) | Decentralized |
| Accessibility to users | Closed | Closed (for the relevant application) | Open |
| Control over privileges | Can be defined as required | Users authenticated for specific roles | All users can perform all roles |
| Identification requirements | All users known | All users known (for the relevant application) | Pseudonymous |
| User base | Very Limited (by design) | Limited (for the relevant application) | Broad |
| Interoperability | Can be developed as required but lower ease of implementation | Can be designed as required (for the relevant application) | Higher interoperability given existing DLT-based ecosystem |

Source: BCG Analysis, GFMA Member Interviews

GFMA and its members have taken a principles-based approach to create a preliminary industry framework assessing the primary risk implications of each DLT network archetype being deployed against key risk categories. These were developed with the goal of substantiating that DLT-specific infrastructure risk is not unforeseeable, but instead can be mitigated and managed through an industry-agreed framework to promote the safe, coordinated development of DLT.

Operational Risk — Technology Robust cybersecurity including permissioning (network access, user privileges), operational resilience, smart contracts, data confidentiality, scalability, and delivery of secure interoperability across DLT-based and traditional capital markets systems.

Operational Risk – Technology: Cybersecurity

Ensuring security of the network as a whole and the integrity of specific nodes from cyberattacks from bad actors.

Existing cyber resilience, cryptography, and consensus mechanisms, correctly developed and deployed, have the potential to guard against bad actors. While cyberattacks (e.g., hacks, ransomware) are not unique to DLT, the industry has worked to develop and implement more robust regulatory frameworks exist and remain applicable for these generic, technological risk considerations.

Example of DLT-specific cyber security considerations to account for include:

- “Crypto bridge attacks”: bad actor(s) exploit vulnerabilities in integrations between DLT networks known as “bridges”.
- Sybil attacks: bad actor(s) gains influence over the network by controlling the consensus mechanism.⁴⁰
- “51%” attacks: majority of the network’s power is controlled by bad actor(s).



Private-permissioned networks: Closed and permissioned access, together with centralized governance over user privileges, significantly reduces exposure to cyberattacks. While risk of collusion-type cyberattacks are technically possible on private-permissioned networks, they remain highly unlikely given both (a) the robust permissioning required to access and participate on the network and (b) the high-degree of centralized network control. These considerations can be managed by existing cyber resilience risk frameworks.⁴¹



Public-permissioned network: Comparable to private networks (when permissioning occurs at the network layer), with closed and permissioned access and potential for centralized governance over user privileges, but potential for the network to be larger can increase exposure to cyberattacks. Like private-permissioned networks, effective permissioning can aid in preventing or mitigating the likelihood of a successful cyberattack. These considerations can be managed by existing cyber resilience risk frameworks.⁴²



Public-permissionless networks: Open and permissionless access, decentralized governance over user privileges, as well as the potential for the largest-scale user bases, potentially increases the risk of malicious cyber events, attacks, or incidences. In practice, the interaction of cryptography and consensus mechanisms has been effective in mitigating these specific cyberattack risks in the largest public-permissionless networks. For example, there have never been any successful attacks on Bitcoin or Ethereum.⁴³ There have been a series of “crypto bridge hacks” on other such networks. Other cybersecurity threats include data privacy breaches and theft, operational breakdowns, counterparty risk management failures, and financial losses worth ~\$21 billion USD in 2022.⁴⁴

While network-based attacks like “Sybil” and “51%” described above are possible they are (a) rare, with a low probability of occurring due to the economic cost of securing the validators required to execute such an attack and (b) yet to be successful against established public-permissionless networks like Bitcoin or Ethereum with a diversified and large network of validators.

⁴⁰ BIS, “Cryptocurrencies and Decentralized Finance”, 2022.

⁴¹ Such as: FSB, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting”, and Format for Incident Reporting Exchange (FIRE), April 2023.

⁴² Such as: FSB, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting”, and Format for Incident Reporting Exchange (FIRE), April 2023.

⁴³ BIS, “Cryptocurrencies and Decentralized Finance”, 2022.

⁴⁴ Chainalysis, “The 2023 Crypto Crime Report”, 2023. Note: This figure may include a portion of financial losses from other DLT network archetypes.

Regulated entities could use governance controls as risk mitigants even on established public-permissionless networks such as those with a track record of proven cryptography and effective consensus mechanisms (e.g., Ethereum Mainnet). For example:

- Selecting public, permissionless DLT networks with a track record of proven cryptography and effective consensus mechanisms, and a wide network of validation nodes (e.g., Ethereum Mainnet);
- Defined criteria for permissioned applications on the network to identify users.⁴⁵ Société Générale – Forge built a permissioned application on Ethereum Mainnet for the first EIB bond issuance as part of Project Mercure that authenticated relevant parties; and
- Whitelisting of tokens to desired users through smart contracts (e.g., broker-dealers and investors).

Operational Risk – Technology: Common Mode Failure

Simultaneous failure of multiple nodes, validators, or components due to software bugs that lead to system-wide disruption.

Cross-industry coding standards and partnered development of infrastructure-level protocols, such as redundancy and failover mechanisms, should be used to enable transparent, auditable, and well-tested software and processes to prevent common mode failures.



Private-permissioned networks: Given the relatively smaller size of the network, failure resilience and fault tolerance are achieved through established technology resilience practices such as redundancy and failover approaches, rigorous testing and proven IT operational maintenance procedures (simulations, audits). Additionally, consensus mechanisms can be designed to prevent network outages in an event where multiple nodes are compromised.⁴⁶ This can be managed through adaption of existing FI cyber resilience frameworks.⁴⁷



Public-permissioned network: Fault tolerance may be enhanced given the need for a greater number of nodes to be compromised to bring about network outages. Developer communities can also be larger, which can increase the resilience of code and reduce bugs. This can be managed through adaption of existing FI cyber resilience frameworks to public networks.⁴⁸



Public-permissionless networks: The leading networks offer proven, historical resilience to failures and strong fault tolerance because the ledger is replicated by the largest number of nodes (e.g., Ethereum had more than 14,400 active nodes in March 2023)⁴⁹, reducing the likelihood of network outages even in the event nodes are compromised by failures and faults. These networks also have the largest developer communities. This can be managed through adaption of existing FI cyber resilience frameworks in tandem with the banks assessment of a public-permissionless networks own cyber resiliency standards.

45 This should not be conflated with a ‘public-permissioned’ network. Though counter-intuitive, it is possible to achieve permissioning on public-permissionless networks through permissioned applications. As an analogy, this is conceptually similar to a secure portal on the internet (which is also public-permissionless) but requires authentication to access the web application.

46 For example, the practical byzantine fault tolerance consensus mechanism (PBFT). PBFT is a fault-tolerant protocol used in DLT networks to ensure that a consensus can be reached even when a certain number of nodes in the network are compromised or fail. In PBFT, validators are randomly selected to propose new blocks, and other validators use a voting process to reach a consensus on whether the proposed block should be added to the DLT. If a certain number of validators agree on the proposed block, it is added to the DLT network. PBFT can prevent network outages when multiple nodes are compromised because it requires a two-thirds majority of validators to reach a consensus, which makes it difficult for malicious actors to disrupt the network by compromising a large number of nodes.

47 Such as: FSB, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting”, and Format for Incident Reporting Exchange (FIRE), April 2023.

48 Such as: FSB, “Recommendations to Achieve Greater Convergence in Cyber Incident Reporting”, and Format for Incident Reporting Exchange (FIRE), April 2023.

49 <https://nodewatch.io/>, node count figure taken in March 2023.

Operational Risk – Technology: Smart Contract Risk

Running a viable technical infrastructure to coordinate smart contract activity, and the prevention of undesired outcomes including self-execution of errors and violation of terms and conditions.

Smart contract infrastructure requires the extension and operation of a technical infrastructure which pose new considerations including, but not limited to, updates to data models, changes in calculation methods or other market conventions, and the resolution of valuation differences on the ledger. Clear governance and standards are required both within financial institutions and across industry to ensure common approaches.

Additionally, smart contracts pose a new form of ‘automation’ risk given their self-executing nature, and the design of some DLT network archetypes that use immutability that prevents editing post-execution (although conducting additional transactions may have the effect of ‘reversing’ erroneous transactions). Multifaceted approaches are required to mitigate these smart contract risks across all DLT network archetypes, which broadly do not fall under existing operational risk and cyber resilience frameworks.

These key risk mitigations are applicable on all three types of DLT networks defined above and are listed below:

- Cross-industry smart contract format standards (including but not limited to ERC-20⁵⁰ and others) and templates.
- Pre-deployment code review that includes user acceptance testing and scenario testing to identify issues or vulnerabilities prior to the go-live date to ensure smart contracts perform as intended, across business, legal, and technology stakeholders.
- Independent audit/verification before deployment conducted by reputable practitioners (such as professional service firms and technology providers) for smart contract code and oracles. This involves the use of mathematical models of the code logic applied against predetermined criteria to ensure execution is as intended and should be paired with industry-accepted standards for audit procedures and common pass/fail criteria.
- Ability to edit and redress erroneous code, and render a smart contract void (e.g., due to errors, breached terms).
- Multi-signature authentication to prevent pre-mature or inadvertent execution by requiring multiple parties to approve a transaction in advance.
- Timelocks, kill switches, failsafes, and monitoring to delay execution, enable manual interventions, and use APIs to enable real-time oversight (e.g., confirming correctness of wallet address, minimize operational “fat finger” errors) and ongoing transaction verification.
- Conduct due diligence on technology, operational, and legal considerations specific to a smart contract before its use (e.g., network upgrades, legal terms, jurisdictional applicability).
- Insurance and dispute management: Enable protection from unforeseen events and resolution of disputes between affected parties.



Private-permissioned networks: Closed and permissioned access, together with centralized governance over user privileges, significantly reduces the risk of bad actors accessing the network to potentially exploit vulnerable code. This also enables the central governance entity to verify the integrity of smart contracts and to provide for a rule-based approach to identify and remedy transaction-based errors. Most private-permissioned networks typically allow for editing and redress of erroneous code.

⁵⁰ Ethereum Request for Comment 20 (“ERC-20”) is a token standard that allows for the creation and issuance of smart contracts on the Ethereum DLT.



Public-permissioned network: Comparable to private networks, with closed and permissioned access and potential for centralized governance over user privileges, however the propensity for a larger network can increase exposure to bad actors exploiting vulnerabilities in smart contract code. Like private-permissioned networks, these networks typically allow for editing and redress of erroneous code.



Public-permissionless networks: Open and permissionless access, decentralized governance over user privileges, and large-scale user bases amplify the risks of bad actors exploiting vulnerabilities in smart contract code. Immutability also prevents editing and redress of erroneous code. To mitigate these risks, networks like Ethereum have code verification tools to ensure confidence in smart contracts executed.

Although existing cyber resilience frameworks provide a basis for approaching risk management, the differentiated nature of smart contract execution could require many of the mitigants listed above.

Operational Risk – Technology: Interoperability

Ensuring the security of connections and integrations between DLT systems and existing traditional systems.

Connections and integrations should be secured against bad actors and other cyberattack threats across the full range of solutions adopted including APIs, middleware, bridges, oracles and smart contracts. These solutions should mitigate against the risks of transferring security vulnerabilities between systems, instability from interference with consensus mechanisms, and maintaining KYC/AML/CFT regulatory compliance.



Private-permissioned networks: Closed and permissioned access significantly reduces the risk of exposure of transmitted data to bad actors. Interoperability can be achieved through adoption of common standards such as APIs, and single-common infrastructure, to bridge information flows, but distinguishing risks need to be mitigated to preserve the high standards of security and privacy. This includes unauthorized access, data leakage, and regulatory compliance (in the case of integrations with public, permissionless DLT networks). Depending on design, technical risks could also exist, stemming from incompatibility of data formats, consensus mechanisms, and scale requirements. To mitigate these risks, bespoke infrastructure and security protocols are being implemented by market participants to block unauthorized access, encrypt transmitted data and avoid interactions that could breach KYC/AML/CFT regulatory compliance (see KYC/AML/CFT risk for more details further below). Integrations with ‘public, permissionless’ networks are often also avoided altogether, to prevent the transfer of security vulnerabilities. Existing operational risk and cyber resilience frameworks provide a basis for risk management but require supplementation by these new infrastructure and security protocols to mitigate these risks.



Public-permissioned networks: Comparable to private networks, with closed and permissioned access, however these networks are typically designed for broader interoperability use cases ‘out of the box’. The implication of a larger network also increases the risk of exposing transmitted data to bad actors. In addition to the mitigants described for private-permissioned networks, these networks should also consider mitigants set out for public-permissionless networks under Cybersecurity risk.



Public-permissionless networks: Open and permissionless access, decentralized governance over user privileges, and large-scale user bases increases the risk of exposing sensitive data (e.g., OTC security transactions) to bad actors during transmission. The distinguishing risks these networks present must be taken into account when implementing interoperability solutions to ensure safety and security.

Operational Risk – Technology: Scalability

Ensuring DLT-based capital markets can meet (a) processing throughput requirements and (b) digital storage requirements.

Sufficient processing throughput should be provided by the network to meet demand through a combination of techniques in the design of the DLT network including consensus mechanisms, data compression, and approaches to storage capacity requirements. Network operators should differentiate between different node types based on operational user requirements and storage capacity needs: from full-copy nodes, to lighter access-only nodes.



Private-permissioned networks: Scalability and processing speed is typically highest in these networks, given that there are far fewer nodes participating in the validation of transactions. These networks can also use more efficient consensus mechanisms such as Practical Byzantine Fault Tolerance (pBFT), Raft, Proof of Stake-derived models, and others. Custom node types can be defined to differentiate between requirements (e.g., from full-copy to access-only). This can be managed through existing cyber and IT resilience frameworks.



Public-permissioned network: Similar to private-permissioned networks, though the potential for more nodes could decrease scalability and processing capacity depending on the design of the network and use case. This can be managed through existing cyber and IT resilience frameworks.



Public-permissionless networks: Scalability and processing speed have presented ongoing challenges for these networks.⁵¹ To mitigate these risks, workarounds on networks such as Ethereum spread storage workload (known as sharding) and bandwidth compression using layer 2s (like zero-knowledge rollups) have been successful in increasing capacity.⁵² Proof of stake consensus mechanisms, such as that debuted by Ethereum in 2022, are increasingly common and significantly faster. These features could help provide the throughput required to meet scalability requirements. Can be managed through existing cyber and IT resilience framework.

Operational Risk – Technology: Settlement Finality

Ability to identify precise settlement and achieve designation as a securities settlement system.

The basis of settlement finality law is the identification of a precise moment after which the transaction (defined as discharge of an obligation by transfer of funds and transfer of securities) becomes irrevocable and unconditional.



Private-permissioned networks: Have the operational capability to identify the precise moment of settlement and can define the settlement finality moment in their rules (subject to availability of legal or regulatory frameworks that make such finality irrevocable).



Public-permissioned network: Can be designed to define the moment of settlement finality similar to private-permissioned networks set out above.



Public-permissionless networks: Use “probabilistic settlement” because any transaction must be validated through the consensus mechanism before it can be deemed completed. This makes the determination of the exact moment of operational finality relatively less precise to demonstrate settlement finality.⁵³

51 For example, the Ethereum proof of work blockchain averages ~15 transactions per second (“TPS”) and Bitcoin ~7 TPS.

52 Zero-knowledge roll ups are protocols with of state updates off-DLT while storing transaction data on-DLT to improve scalability.

53 The use of permissioning to provide requisite settlement finality is discussed further in Chapter 4.

Compliance and Financial Crimes Risk | Permissioned and permissionless networks can comply with existing KYC / AML, data privacy regulations, settlement finality and reputational risk (avoiding Group 1b/2a/2b cryptoasset exposures).

Compliance and Financial Crimes Risk: KYC/AML/CFT Compliance

Ensuring the standards of KYC/AML/CFT implemented in regulated financial markets are upheld.

DLT networks can use authentication, verifiable credentials, and other relevant controls to ensure interaction with KYC'd accounts and ensure transactions are validated by KYCed nodes. Additionally, market solutions for real-time DLT transaction monitoring can be used to ensure KYC/AML/CFT standards are continuously being applied and upheld.



Private-permissioned networks: Enables a model with the closest equivalence to regulated capital markets infrastructure. Nodes are restricted to regulated financial institutions who would be responsible for ensuring counterparty compliance in each transaction (with anonymous counterparties but known institutional sponsors); governance is managed by a central entity, preventing rule-changes or “forks” of rules.⁵⁴ This can be managed through existing compliance frameworks.



Public-permissioned network: Can enable a model that operates similarly to private-permissioned networks. Although there is potential for unverified nodes on the network, central governance over user privileges and the use of authentication to deliver this can facilitate compliance with KYC/AML/CFT. This can be managed through existing compliance frameworks.



Public-permissionless networks: These networks present the most significant challenges to achieving KYC/AML/CFT compliance due to the absence of permissioning and central governance. To mitigate these risks, several practices are emerging. To achieve KYC/AML/CFT compliance on public-permissionless networks, applications can be built to use authentication so nodes and users can be identified. Users can also be equipped with verification markers, such as verifiable credentials, to support KYC/AML/CFT verification by decentralized applications. Furthermore, KYC/AML/CFT noncompliance only occurs if transactions are broadcast publicly for validation. However, on public networks, block-builder software can be used to hold transactions back from the public pool of unverified transactions and sent directly to validators subject to KYC/AML/CFT checks. It should be noted that this may result in slower processing times.⁵⁵ In respect of sanctions, smart contracts that screen transactions against sanctions lists such as Office of Foreign Asset Control (OFAC) and other due diligence requirements could be developed, though this is not currently in widespread usage. Additionally, qualified custodians have made investments in sophisticated DLT monitoring software to enable effective know-your-transaction (KYT) capabilities and ensure compliance with applicable rules and regulations.

As per the latest drafting of the Financial Action Task Force’s (FATF’s) *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, transaction fees paid to validators as part of a virtual asset transfer on a public-permissionless network are not subject to the same personally-identifying-information requirements as the originator and recipient of the same transaction.⁵⁶

⁵⁴ A “fork” is a technical term to describe when a blockchain splits into two separate branches, sharing history up until the point of the “fork”.

⁵⁵ GFMA member input.

⁵⁶ FATF, “Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers”, Oct 2021. For specific detail see: Recommendation 16.180 and footnote 43.

Compliance and Financial Crimes Risk: Data Privacy

Replicating existing market confidentiality and data laws on DLT (e.g., General Data Protection Regulation (GDPR) right to be forgotten).

Data privacy and confidentiality of financial transactions can be protected to the same standards as traditional financial markets.



Private-permissioned networks: Privacy and confidentiality of financial transactions can be appropriately safeguarded across the network. Can be managed through existing Data Management frameworks.



Public-permissioned networks: Privacy and confidentiality of financial transactions can also be safeguarded to a similar standard as private-permissioned networks. Can be managed through existing Data Management frameworks.



Public-permissionless networks: The safeguarding of privacy and financial transactions pose challenges that require incremental risk mitigants, because transactions are publicly available on the ledger by default. Approaches like zero-knowledge proofs (“ZKPs”) can achieve data partitioning and keep transactions private (as seen on the Polygon distributed ledger). With ZKPs, the identities and value of the transaction would not be displayed on the ledger.⁵⁷ ZKPs could provide the nodes on the platform with RAG indicators (based on commonly agreed thresholds among participants) on the risks related to the beneficial owner, thereby reducing challenges relating to data protection. Zero-knowledge testing in the transition of on- and off-chain information can mitigate GDPR⁵⁸ risks.

Compliance and Financial Crimes Risk: Reputational Risk

Ensuring Group 1a DLT-based Securities and DLT-based Payment Instruments are clearly ringfenced from Group 1b/2a/2b digital assets, to protect market participants from unwanted exposures.

Regardless of network archetype, exposure to Group 1b/2a/2b digital assets as defined in the BCBS framework should be eliminated or minimized as appropriate to ensure regulatory compliance, create confidence for issuers and investors, and be appropriately ringfenced from Group 1a digital assets.



Private-permissioned networks: It is possible to limit digital asset classes and enable strict management of exposures to Group 1b/2a/2b digital assets in the context of the Basel Framework by expressly designing the network to prohibit use of any non-Group 1a digital assets.



Public-permissioned networks: Depending on the design and use case, these networks can similarly limit exposure to Group 1b/2a/2b digital assets.



Public-permissionless networks: The majority of public-permissionless DLT networks have a native cryptocurrency (Group 2b digital asset, in the context of the BCBS framework) token. On networks such as Ethereum and others that use EIP-1559, and similar, fee structure modifiers, a transaction validator is paid a transaction fee in the native network token (e.g., Ether for the Ethereum network) for posting its stake as collateral to validate the transaction (i.e., proof of stake). This creates significant risk of exposure to Group 1b/2a/2b digital assets. To eliminate this exposure risk, GFMA members have highlighted several methods of participating on public-permissionless networks, *without* paying a transaction fee in the native network token, including:

⁵⁷ Ibid.

⁵⁸ Chainalysis, “The 2023 Crypto Crime Report”, 2023. Note: This figure may include a portion of financial losses from other DLT network archetypes. BIS, “Cryptocurrencies and Decentralized Finance”, 2022.

The EIP-2771 based Biconomy “gasless product” | A contract interface protocol that separates the signer and the payer of the transactions, thus allowing a third party to pay transaction fees. These are called meta transactions. In December 2022, J.P. Morgan executed its first-ever cross-border decentralized finance (DeFi) trade on Ethereum using Biconomy’s gasless relay.^{59, 60}

Block builder software | Transactions do not have to be shared publicly for validation and can instead be directed to specific validators. Custom block builder software could pull transactions from a private group of transactions (which are not shared to the publicly accessible mempool) to which only financial institutions are allowed to contribute and direct them to validators that are being run by an organization that has been KYC’d in return for a premium or subscription payment (a KYC’d subset of the whole) that would be paid in DLT-based Payment Instrument or traditional cash offline.⁶¹

Our assessment shows that private-permissioned networks, which retain control over network access and user privileges, provide a model that is comparable to existing infrastructure used in capital markets. As highlighted above, these qualities enable robust management of cybersecurity risk as well as KYC/AML/CFT and data privacy compliance. These networks also offer arguably the strongest potential for scalability, and settlement finality in line with traditional payment systems. Some private-permissioned networks may have reduced resilience to common mode failure and ease of achieving interoperability compared with public networks. However, these remain in line with attributes of existing centrally administered systems, and can be managed by existing standards around operational and cyber resilience frameworks and supported by developing bespoke integrations with other distributed ledgers (e.g., through APIs). They can, therefore, be managed in line with established regulatory and risk management frameworks. As with all DLT networks, differentiated risk considerations exist around smart contract risk, for which mitigations have been substantiated and outlined above.

Though public networks raise questions on oversight, our assessment suggests that public-permissioned networks could potentially offer similar benefits around security and control to private-permissioned networks provided that appropriate risk mitigants are implemented. Public networks must contend with issues particularly around cybersecurity, KYC/AML/CFT and data privacy compliance, and settlement finality. However, public-permissioned networks can enable cybersecurity risk mitigation and KYC/AML/CFT compliance through permissioning, centrally-controlled governance, and through technology solutions that allow participants to share information and enter into agreements in ways similar to private-permissioned networks. Public-permissioned networks are also not exposed to the same level of cybersecurity as larger public-permissionless networks (e.g., 51% attacks, Sybil attacks) given they remain centrally controlled. These networks can also be designed to deliver settlement finality in line with traditional settlement systems. In addition to these mitigations, public-permissioned networks can offer potential for broader interoperability and market access to mitigate liquidity risks from fragmentation across bespoke DLT platforms in Primary and Secondary Markets. For example, leading DLT technology provider R3, which developed the private-permissioned Corda platform, has also developed ‘Corda Network’, a public-permissioned platform to meet use case requirements for interoperability.

Finally, the assessment suggests market participants and regulators should remain open to public-permissionless networks in the longer-term, as risk mitigants are further developed and proven. Key drivers include the potential for interoperability to access larger liquidity pools, the operational resilience of leading public networks, and reduced financial overhead of achieving economies of scale. However, differentiating risk considerations including cybersecurity concerns (cyberattacks on “crypto bridges” with other networks, 51% attacks, Sybil attacks, and

59 Biconomy, 2022: <https://www.biconomy.io/post/jpmorgan-makes-history-with-first-ever-on-chain-defi-trade-using-biconomy-transaction-infrastructure>.

60 “Gas” is a unit of measure referring to the computational resources required to complete a transaction, which manifests as a fee. A “gasless relay” refers to a service where a third party (the ‘relay’) pays the gas on the behalf of a user, thereby allowing the user to forego payment of the gas fee required to submit a transaction.

61 A “mempool” is an organized queue of pending, but not yet validated transactions that have yet to be added to a block-entry on a DLT.

other attempted network collusion), KYC/AML/CFT regulatory compliance (given unverified nodes are present), and exposure to Group 1b/2a/2b digital assets (native cryptocurrency tokens are used) could require technology workarounds, as described in the table of findings above.

An additional issue for public-permissionless networks arises in relation to settlement finality. Unlike private, permissioned DLT networks and traditional Clearing and Settlement infrastructure – which can define specific rules as to finality of payment and delivery, as well as backstops in relation to potentially failed transactions – these networks raise the issue of “probabilistic finality” in settlement due to the need to validate any transaction on the public network before it can be deemed completed. This makes the determination of the exact moment of operational finality relatively less precise. In practice, it is unlikely at present, to be possible for any fully permissionless DLT framework to obtain status as a securities or payment settlement system, which must demonstrate settlement finality.

To address these differentiated risks, market participants have been testing and developing mitigants as outlined in the risk mitigation framework and profiled in this report. Recent digital issuances (including those detailed in [Chapter 3 | Use Cases](#)) have experimented with these mitigants (e.g., whitelisting, privacy controls), finding success in their real-world application, paving a way forward for further adoption and exploration of new use cases.

3 | Legal And Regulatory Certainty: A Level Playing Field That Promotes Safe Innovation

Legal and regulatory certainty is a significant requirement for wholesale market development. The current position is that the laws and regulation applied to DLT-based Securities and DLT-based Payment Instruments are those developed for traditional assets. In some cases, this is effective, in others it can either operate as an inadvertent prohibition of certain types of business, or as a destabilizing influence undermining legal certainty as to the effectiveness of ownership and transfer of assets.

Both regulators and legislators are aware of this situation, and there are several initiatives around the world aimed at removing inadvertent barriers and improving legal certainty for investors and others. It is important to recognize that this updating of legal and regulatory functions involves engaging with difficult policy issues, and therefore requires significant resource input for the public sector.

This is an area where we would urge regulators and legislators to increase their focus and resourcing and to continue engaging in ongoing dialogue with the private sector to work towards solutions. This is not only because of the extreme undesirability of markets and practices developing outside the scope of the existing regimes, but also because the timely establishment of these structures will promote transparent, disciplined, and effective development of markets and infrastructures.

The legal challenges and barriers preventing or delaying the adoption and use of DLT and tokenized representations of securities in capital markets can be divided into three broad categories, which are discussed below.

It is important to note that both legislation and regulation or enacted on a national or, in the case of the E.U., supranational basis. Different jurisdictions are facing individual as well as global challenges and as such, legislation is evolving at different paces. It is unlikely that the development of different approaches in this area will benefit either individual jurisdictions or the market as a whole, and we believe that the development of coordinated policy positions across different jurisdictions would be a significant benefit both for the market and for governments and regulators.

(1) Legislative Constraints: In each jurisdiction, there may be specific legislation or regulatory requirements, almost always put in place for other reasons, which are incompatible with the use of DLT and the issuance or trading of DLT-based Securities by regulated entities. By way of example, in the E.U. and the U.K. it is a requirement that for a security to be traded on a trading venue (an exchange or a multilateral system) it must be recorded in book-entry form in a centralized securities depository (“CSD”). In practice, this does not prohibit the issuance of DLT-based Securities, but in the absence of a CSD that operates a DLT platform, such securities cannot be made fully available to investors. Where such outcomes are unintended consequences of existing legislation, they should be addressed as a matter of priority.

(2) Legal Uncertainty: While legal and regulatory requirements are often presented as being technology agnostic, in practice the decentralized nature of some DLT networks create legal uncertainty. For example, in many jurisdictions there is as yet no positive legislative instrument that permits the issuance and confirms the ownership status of holders of DLT-based Securities. This can lead to unacceptable levels of legal uncertainty as to what issuers are permitted to do, how issuances and transactions are to be treated for tax and settlement finality purposes, and the risk of invalidity for failure to comply with requirements established for report-based issuances. Some countries, notably Luxembourg and Germany, have passed laws establishing legal and regulatory clarity, and there is progress towards updating legal frameworks in many countries. Generally, we acknowledge that there is progress towards updating legal frameworks in many countries. However, there is a common thread as to the need for further development of an internationally-agreed approach to these issues, and to the development of the legal certainty that forms the foundation of trust necessary to support a capital markets framework and to meet the express expectations outlined in BCBS guidance regarding crypto assets. Regulators legitimately require regulated institutions to satisfy themselves as to the legal certainty and settlement finality in the transactions in which they engage, but this cannot happen unless regulators themselves co-operate with legislators and with the private sector to develop that legal certainty.

As usage of DLT increases, it will become increasingly necessary to (i) remove legislative constraints (such as rules requiring paper or mechanical processing of transactions); and (ii) create a legal and regulatory environment with clear guidelines that provide legal certainty to market participants. Some work is underway in certain jurisdictions, including the EU and the UK, to develop “sandbox” or pilot regimes that would create test environments in order to foster adoption of DLT. These measures are welcome. However, a sandbox is only useful where, once a concept has been proven within it, that concept is permitted within the relevant law – if necessary, by changing it. Sandboxes do not provide a long-term stable legal framework for market developments. It is particularly important in this context to note that the aim of such experiments is ultimately to provide legal and regulatory certainty to the entire securities value chain.

With regard to creating guidelines for legal certainty, an essential starting point is clarification of regulatory expectations as to the level of finality required to meet the BCBS requirement. As a first step, it should be clarified that the intended scope of the finality requirement should apply to the settlement process. Settlement finality is a legal technique used to cover delays in settlement systems – where a transaction involves an exchange of DLT-based Securities for payment in DLT-based Payment Instrument (or a fiat currency), this should be recognized as final is accomplished in a manner that is final. We note that payment in a form of DLT-based Payment Instrument may give rise to the sort of cross border payment issues identified in the BCBS paper “Enhancing cross-border payments: building blocks of a global roadmap” of July 2020. This clarification would be consistent with comparable settlement finality requirements in foreign exchange and regulated financial market infrastructures.

In this regard, we believe that the same approach should be adopted as for Foreign Exchange. In paragraph 3.6.5 of its *Supervisory guidance for managing risks associated with the settlement of foreign exchange*,⁶² the BIS explains that the basis of this requirement is that “A bank should obtain legal advice that addresses settlement finality with respect to its settlement payments and deliveries. The legal advice should identify material legal uncertainties regarding settlement finality so that the bank may assess when key financial risks are transferred.” This makes

62 BIS (BCBS), “Supervisory guidance for managing risks associated with the settlement of foreign exchange transactions”, Feb 2013.

clear that the ultimate assessment of the legal protection available is a risk decision for the reporting institution and would avoid unintended extension to other lifecycle elements of capital markets (such as issuance or safe-keeping). It would also be helpful to clarify that finality applies to settlement within the given network or platform that governs the relevant DLT-based Security and DLT-based Payment Instruments, which would also be consistent with the CPMI/IOSCO Principles. Such clarity would help promote ecosystems that are designed to result in free and clear ownership that is not impacted by events external to the relevant network or platform, including events on an unrelated network or platform.

It would also be helpful to underscore the importance of applying such guidance consistently, so that a global legal framework is developed in such a way as to promote the harmonization of rules and standards across jurisdictions. With clearer and consistent guidance, DLT's potential benefits outlined in this report can be effectively realized.

Market participants invite regulators to engage in a dialogue with the private sector and with legislators to develop legal infrastructure that meets expectations as to legal certainty and finality. Recent discussion of a “unified programmable ledger”⁶³ which could enable the creation of a DLT-based golden source for record-keeping, may be a potential starting point for this endeavor.

(3) Avoidance of Legal Frictions: As of today, there are significant frictions – referring to contradictory requirements or inconsistent obligations - which arise from divergent legislation and regulation regarding DLT-based Securities and DLT-based Payment Instruments. These frictions arise both within jurisdictions and between them. The process of updating legal and regulatory frameworks will take time, and whilst it is ongoing the occurrence of such frictions is likely inevitable. However, we believe that it is important that a process for identifying and addressing such frictions is established as part of the ongoing policy work in this area. We believe that the process of updating and enhancing wholesale market capabilities using new technologies will be an ongoing development which will have no clearly identifiable end point. This therefore needs to be a continuing process rather than a one-off project.

Recommendations: Legal and Regulatory Framework

Existing securities laws ideally should be refined and modified to apply optimally to DLT-based Securities. For example, existing disclosure requirements may not capture all the pertinent information or address all the risks that are most relevant to investors of DLT-based Securities. Examples of information that may benefit from more specific disclosure requirements include the processes by which new investments can be created or existing investments redeemed. Thus, the challenge is not as simple as just bringing these assets within the scope of existing laws – the detailed requirements of those regimes should be revisited to ensure that they capture information most relevant to an investment decision.

The existing rules of engagement for investors of DLT-based Securities with service providers and intermediaries (such as transfer agents, broker-dealers, and custodians) also pose an impediment to the development of the DLT-based Securities marketplace. Currently, investors may be effectively required to deal with one set of providers for traditional securities and another for DLT-based Securities, thereby increasing cost, adding complexity, while decreasing utility, and impeding interest. These rules should be revised to reflect the emerging structure of a DLT-based Securities ecosystem and reduce the number of providers DLT-based market participants must interact with. Additionally, it is critically important to ensure that DLT-based Securities are fully protected by qualified and well-regulated custodians. Here too, existing rules can be revised to ensure an equivalent standard of investor protection, while acknowledging the specific nuance of a DLT-based framework.

63 Carstens, “Innovation and the future of the monetary system”; speech at the Monetary Authority of Singapore, Feb 2023.

Settlement standards also should be revisited. The existing regime was put in place to further the goal of dematerialization of securities and the promotion of paperless settlement given problems experienced with a paper-based system. Today's regulated service providers work on systems that contemplate a robust, but intermediated, electronic settlement process and the migration to systems that contemplate a DLT-based environment requires analysis and modifications. Given the success and protections of the current settlement processes for traditional securities, regulators and legislators may be hesitant to seek changes. However, the question of how regulation should be reconfigured to facilitate the settlement of DLT-based Securities without losing legal and regulatory protections for users will require detailed policy analysis. This will include, in some jurisdictions, reviewing and revising mandates relating to clearing and related functions.

Where DLT-based Payment Instruments are intended to perform a money-like function, the regulatory issues are also complex. As a core principle, customers should benefit from the same protections when dealing with banks and "legacy" assets or payment instruments and when dealing with DLT-based Payment Instruments. Similarly, regulations and other standards should be rationalized to ensure that banks can provide the services that customers are accustomed to receiving from banks, with prime examples being Custody and transaction facilitation. Tokenized commercial bank money and deposits therefore should be subject to similar rules as traditional commercial bank money and not differentiated due to technology.

For a comprehensive exploration of the topics covered in this Executive Summary, we encourage you to refer to the full report.

The GFMA and its members acknowledge the increasing significance of DLT and the extensive research that underpins its implementation. We hope to encourage further study and exploration in the Closing Remarks, where we identify additional areas for examination.

We trust that the report will serve as a valuable resource for policymakers, regulators, and government officials, and we are confident that it will help foster a greater understanding of the impact DLT can have in global capital markets.