



HONG KONG MONETARY AUTHORITY
香港金融管理局

In collaboration with



Distributed Ledger Technology in the Financial Sector: A Study on the Opportunities and Challenges

March 2025



Supported by



QUINLAN
& ASSOCIATES

Contents

Foreword	3
Introduction	4
1. Executive Summary	6
2. Introduction to DLT	7
3. Adoption Use Cases	17
4. Practical Guidance for DLT Adoption	41
5. The Way Forward	60
6. Appendix	63

Foreword

In recent years, the financial services industry has witnessed a significant transformation, driven by the emergence of innovative technologies that are redefining the way institutions operate, interact with customers, and manage risk. Among these technological advancements, Distributed Ledger Technology (DLT) has garnered significant attention for its potential to enhance transparency, efficiency, and security in financial transactions.

The evolution of financial technology has been characterised by increasingly shorter innovation cycles. While the widespread adoption of traditional banking systems took decades, the emergence of digital payment systems, online banking, and mobile banking has accelerated the pace of innovation. Given the growing interest in DLT, it is likely that the adoption of this technology will follow a similar trajectory, with institutions and regulators needing to adapt quickly to harness its benefits while managing its risks.

The Hong Kong Monetary Authority (HKMA) has been actively promoting the development and adoption of Fintech in Hong Kong's financial services industry through its Fintech 2025 strategy, which aligns with the growing interest in DLT from industry participants. As part of this initiative, the HKMA has been working closely with financial institutions, Fintech firms, and other stakeholders to foster innovation while ensuring that the adoption of DLT is safe, secure, and aligned with supervisory expectations.

Effective risk management is critical to the sustainable development of the financial services industry. In this context, the HKMA has issued guidance to clarify its supervisory expectations and highlight those risk management considerations or areas that may prove particularly relevant as banks continue with their adoption of DLT.

DLT has emerged as a transformative force, reshaping industries and redefining traditional processes. However, its true potential lies not only in the technology itself but in the mindset with which it is approached. As we embark on this journey to harness the power of DLT, we must remember that innovation is not a destination, but a continuous process of evolution and improvement. By embracing this mindset, we can unlock the full potential of DLT and create a more efficient, secure, and resilient financial system.

This paper aims to provide a comprehensive overview of the role of DLT in the financial sector, including its potential use cases, benefits, and challenges. It also, building on earlier HKMA supervisory guidance, details practical guidance and strategies for institutions to consider when implementing DLT solutions while fostering an innovative and risk-centric mindset that aligns with supervisory expectations.

As we look ahead, the HKMA remains committed to creating an environment where financial institutions can leverage the power of DLT responsibly, while ensuring that Hong Kong continues to be a leader in Fintech innovation. By working together, we can unlock the full potential of DLT, while upholding the integrity, resilience, and stability of our financial system.

We would like to extend our heartfelt thanks to the Securities and Futures Commission (SFC), the Insurance Authority (IA), the Mandatory Provident Fund Schemes Authority, financial institutions, and industry stakeholders who provided their inputs for this paper. Collaboration is critical as we begin this journey to shape the future of financial services through DLT.



As we embark on this journey to harness the power of DLT, we must remember that innovation is not a destination, but a continuous process of evolution and improvement.

Mr Arthur Yuen, Deputy Chief Executive of the HKMA



Introduction

The financial services sector stands at a pivotal moment of technological evolution, with DLT emerging as a transformative force that complements traditional banking operations. As a leading international financial centre, Hong Kong is strategically positioned to harness innovations while maintaining its reputation for regulatory excellence and financial stability.

Recent advancements in DLT have accelerated its adoption among financial institutions. Notably, the development of new tokenisation standards has enabled the tokenisation of a broader range of asset classes and facilitated improved connectivity between on-chain and off-chain interactions via oracles, which play an important role in connecting digital and traditional ecosystems. These innovations are crucial for enhancing DLT's functionality and integrating its features into existing financial systems.

Following the HKSAR Government's "Policy Statement on Development of Virtual Assets in Hong Kong" in 2022, there has been growing interest from financial institutions in exploring DLT applications in traditional financial market operations.¹ The HKMA has observed an increasing number of Authorized Institutions (AIs) seeking guidance on their planned DLT initiatives, particularly in areas such as tokenised deposits and related financial services.

In response, the HKMA has taken a number of steps to support related developments, including issuing guidance to clarify its supervisory expectations, and launching facilitating initiatives, such as the Supervisory Incubator for Distributed Ledger Technology.^{2,3}



FINETech4 - Charting the New Frontiers of Finance with DLT

To enable the provision of even more targeted support based on the latest market developments, the HKMA conducted a study to assess the current adoption of DLT among financial institutions, and identify issues/ areas that may particularly merit attention. As part of this, it held in-depth interviews with 10 major players and surveyed 113 financial institutions. The findings reveal that most institutions leverage DLT for at least two of its core features, with programmability and transparency being the primary drivers for adoption. Use cases include improving user experience, automating previously manual operations, and providing a single source of truth for multiple parties.

¹ Financial Services and Treasury Bureau. 2024. *Policy Statement on Development of Virtual Assets in Hong Kong*. (https://gia.info.gov.hk/general/202210/31/P2022103000454_404805_1_1667173469522.pdf).

² Hong Kong Monetary Authority. 2024. *Risk management considerations related to the use of distributed ledger technology*. (<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240416e1.pdf>).

³ Hong Kong Monetary Authority. 2025. *Supervisory Incubator for Distributed Ledger Technology (DLT)*. (<https://www.hkma.gov.hk/media/chi/doc/key-information/guidelines-and-circular/2025/20250108c1.pdf>).

The study also shows that while the adoption of DLT offers significant benefits for financial institutions, it also presents novel challenges that hinder more widespread adoption including high integration and deployment costs.

In response, this research paper provides practical guidance and implementation strategies to help overcome the identified barriers. By exploring the key considerations for DLT implementation, risk management, and supervisory alignment, these collectively offer a roadmap for institutions looking to harness the potential of DLT while maintaining the stability and security of the financial system. By working closely with industry stakeholders and providing clear supervisory guidance, Hong Kong is well-positioned to lead the responsible integration of DLT within global financial markets.



By working closely with industry stakeholders and providing clear supervisory guidance, Hong Kong is well-positioned to lead the responsible integration of DLT within global financial markets.

Ms Carmen Chu, Executive Director (Banking Supervision) of the HKMA



1. Executive Summary

This research paper explores the transformative role of DLT in reshaping the financial sector. With attributes such as transparency, immutability, resilience, and programmability, DLT provides financial institutions with opportunities to modernise operations, automate processes, and enhance collaboration through a unified source of truth. The adoption of DLT is driven by advancements such as tokenisation standards and enhanced connectivity between on-chain and off-chain systems.

To illustrate the practical applications of DLT, this paper explores 10 real-world adoption cases from leading institutions, covering diverse use cases, such as programmable payments, trade settlement, and digital identity management. These examples showcase the technology's potential to enhance the existing financial market operations.

While DLT offers significant benefits, institutions face adoption challenges, such as lack of strategic alignment, emergence of novel risk, solution deployment and activation difficulties, and regulatory uncertainty, all of which hinder broader implementation. To help financial institutions overcome these hurdles, this paper provides practical guidance and strategies, including good practices, approaches and frameworks to:



Develop a firm-wide DLT strategy with a dedicated DLT team;



Deliver fit-for-purpose training programmes to ensure successful activation of DLT solutions;



Establish mitigation plans for identified risks and challenges, including those related to third-party, concentration risks, smart contract, immutability, key management, cybersecurity, data privacy, and interoperability; and



Advance DLT initiatives while ensuring compliance by adhering to established regulatory principles.

The paper also highlights initiatives by the HKMA to create an enabling environment for DLT adoption. These include supervisory guidance to ensure regulatory clarity, trial facilities to support implementation, and talent development efforts to foster DLT expertise. Collaborative research and innovation are emphasised to position Hong Kong as a global leader in the responsible integration of DLT.

Overall, this research paper aims to provide a comprehensive overview of the role of DLT in the financial sector, including its potential use cases, benefits, and challenges. By addressing challenges and leveraging opportunities, it aims to enable institutions to harness the full potential of DLT, ensuring innovation, resilience, and long-term stability of the financial sector.

2. Introduction to DLT

In an increasingly interconnected global economy, businesses are confronting heightened operational complexity, including navigating diverse time zones, managing multiple stakeholders, and dealing with intricate internal processes. This complexity typically leads to prolonged processing times and elevated costs, ultimately hindering operational efficiency.

In response to these challenges, companies worldwide are increasingly exploring technological innovations to streamline their operations. In this context, DLT stands out as a key solution that can enhance and/or augment traditional methods of storing, recording, and transferring financial information between parties, underpinned by its unique characteristics, such as immutability and programmability.

The financial services industry has been particularly proactive in its efforts to adopt DLT, focusing on a diverse range of applications, including the creation of financial data repositories, the tokenisation of real-world assets, atomic transaction settlement, and programmatic transactions. Notably, the top 10 financial services firms alone, ranked by the number of patents acquired in DLT, have secured over 700 related patents, underscoring the industry's commitment to harnessing this technology.⁴ The growing integration of DLT into the financial services industry signals a new era of adoption, marking a significant shift from initial interest to more widespread implementation and innovation.

2.1 DLT Architecture

According to the Bank for International Settlements (BIS), DLT is a method of proposing and validating records on a synchronised ledger system based on pre-agreed protocols between multiple entities from different locations.⁵ These records are stored and can be shared amongst different parties without the need for a central authority.

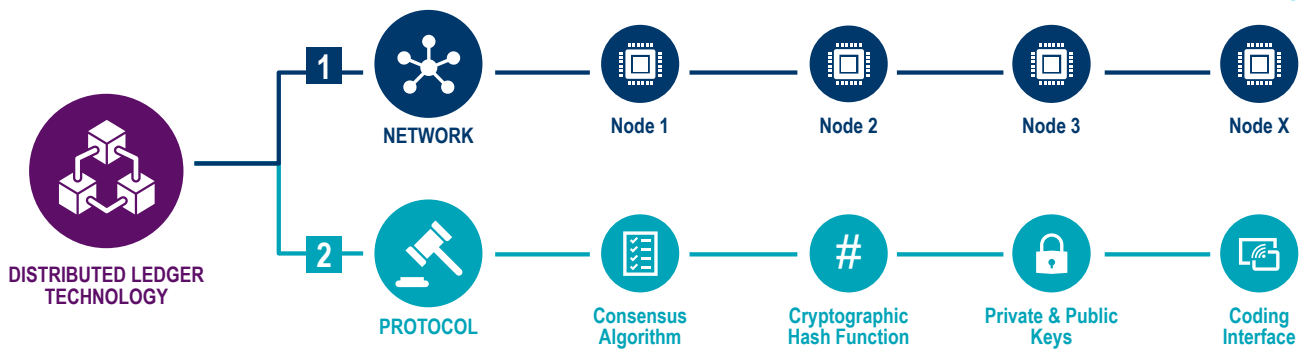
The most notable example of DLT is blockchain, characterised by a linear chain of information blocks that store transaction records. The DLT architecture consists of two primary components (see Figure 1):

1. **The network:** nodes managed by network participants; and
2. **The protocol:** guiding principles and relevant tools for participation.

⁴ Google. 2024. *Google Patent search results for "DLT", "Distributed Ledger Technology" and "Blockchain"*. ([https://patents.google.com/?q=\(DLT+OR+blockchain+OR+distributed+ledger+technology\)&oq=DLT+OR+blockchain+OR+distributed+ledger+technology](https://patents.google.com/?q=(DLT+OR+blockchain+OR+distributed+ledger+technology)&oq=DLT+OR+blockchain+OR+distributed+ledger+technology)).

⁵ Bank of International Settlements. 2017. *What is distributed ledger technology?* ([https://www.bis.org/publ/qtrpdf/r_qt1709y.htm#:~:text=Distributed%20ledger%20technology%20\(DLT\)%20refers,synchronised%20way%20across%20a%20network](https://www.bis.org/publ/qtrpdf/r_qt1709y.htm#:~:text=Distributed%20ledger%20technology%20(DLT)%20refers,synchronised%20way%20across%20a%20network)).

Figure 1: DLT Architecture



Source: Quinlan & Associates Report – Cracking the Code

2.1.1 Network

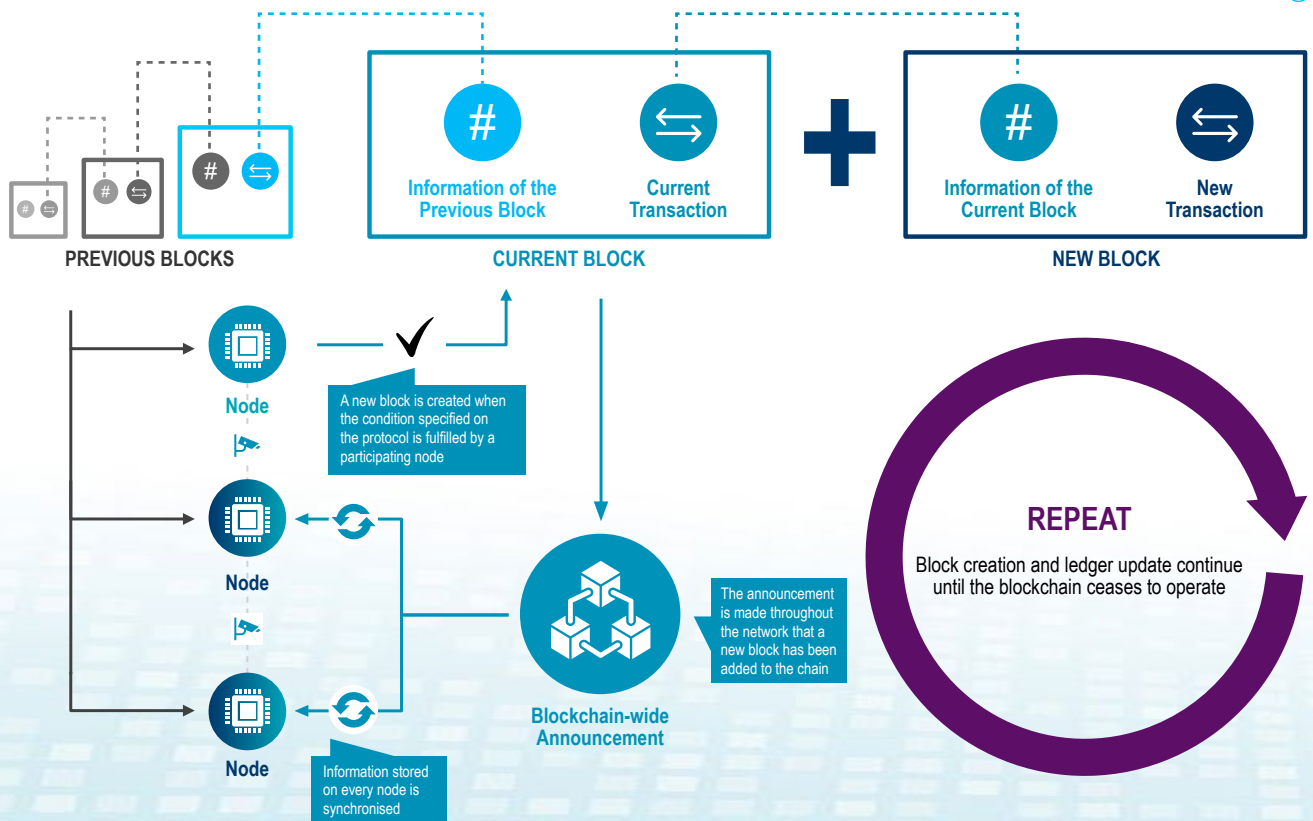
A DLT network consists of nodes, which are individual computers connected to a functioning DLT, each maintaining an updated copy of the ledger. Guided by an agreed set of protocols, each node monitors and interacts with other participating nodes to facilitate several key functions:

- Broadcasting transactions made to the ledger to all network participants;
- Validating the authenticity of the updates or transactions with one another;

- Creating new blocks containing data from previous and current transactions, thereby extending the chain securely through cryptographic links; and
- Synchronising the nodes to store up-to-date information on the ledger on each node, thus ensuring a consistent and accurate record of all transactions across the network (see Figure 2).

Collectively, the nodes support the ledger's accuracy and integrity while also reinforcing the decentralised nature of the DLT system.

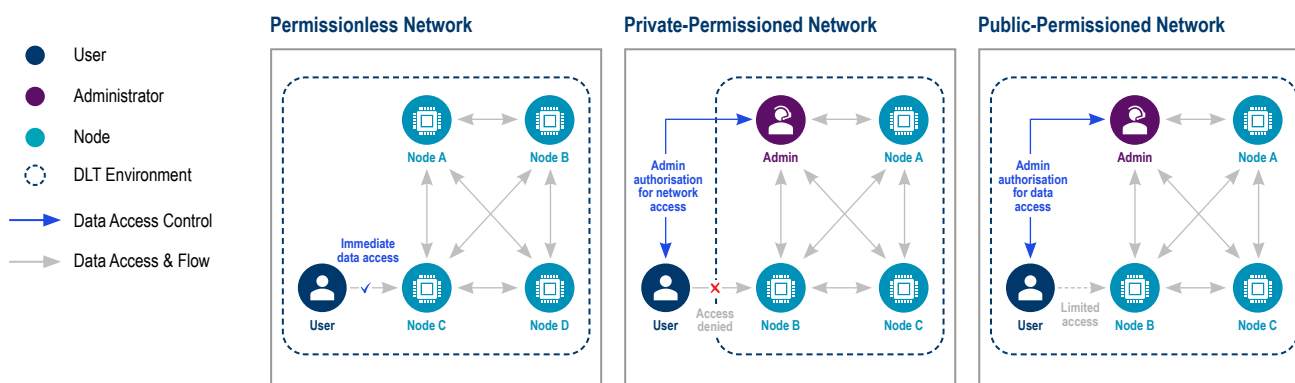
Figure 2: Role of Nodes



Source: Quinlan & Associates Report – Cracking the Code

DLT architecture types primarily differ in the levels of user participation in the network, resulting in three main categories: permissionless, permissioned, and hybrid networks (see Figure 3).

Figure 3: Types of DLT



General

Purpose	<ul style="list-style-type: none"> Public-facing networks that can be edited and accessed by anyone 	<ul style="list-style-type: none"> Networks for internal use within and among organisations 	<ul style="list-style-type: none"> Public-facing networks that can only be edited by approved parties
Ability to Read Information	<ul style="list-style-type: none"> Anyone 	<ul style="list-style-type: none"> Approved users only 	<ul style="list-style-type: none"> Anyone (Limited information)
Ability to Write Information	<ul style="list-style-type: none"> Anyone 	<ul style="list-style-type: none"> Approved users only 	<ul style="list-style-type: none"> Approved users only

Network Control

Responsible Entity	<ul style="list-style-type: none"> Network Users (Openly Shared) 	<ul style="list-style-type: none"> Individual(s) / Organisation(s) 	<ul style="list-style-type: none"> Individual(s) / Organisation(s)
User Identity Verification	Not Needed	Required	Needed (for approved users) Not Needed (for anyone)
Decentralisation	High	Low	Low

Scalability

Processing Time	Slow	Fast	Medium
Complexity in Adding Users	Easy	Difficult	Medium
Network Size (# of Users)	Large	Small	Small

Source: BIS, Global Financial Markets Association, Quinlan & Associates analysis

Permissionless Networks

Permissionless DLT networks offer an open environment where participation is unrestricted, and anyone can connect to the network. There are no restrictions on who can validate transactions, and access to past transaction information is visible to all participants.

One of the key advantages of permissionless networks is their ability to rapidly expand and increase in size, as user verification is not required. The large user base ensures network security, as multiple anonymised parties must agree on changes before new information is added to the ledger, preventing collusion by malicious parties.

While the user base grows and more transactions are conducted on the network, the general computational power of the network remains the same. Despite the potential addition of more validator nodes, the speed of the network is often limited by the average hardware specifications of nodes. Consequently, the processing time of transactions may be slower in permissionless networks, especially during periods of high network activity.

To mitigate this issue, permissionless DLT networks often utilise an additional network layer, known as Layer 2 solutions, on top of a Layer 1 network. In these cases, the Layer 1 network continues to securely validate transactions on the main chain, while the Layer 2 network enhances the network's capacity by processing additional transactions off-chain or in a more efficient manner, such as through sidechains or state channels. While most commonly observed in permissionless networks, these solutions may also be applied in both private- and public-permissioned DLT networks.

Private-Permissioned Networks

In contrast to permissionless networks, private-permissioned DLT networks are accessible only to approved entities and are commonly used for internal operations within a consortium or organisations with multi-market operations. In these networks, administrators oversee approvals for participation, restrict nodes' access to information, and maintain the validation of information, prioritising control to ensure security and privacy.

While private-permissioned networks offer robust security and control, they may face limited scalability and flexibility relative to permissionless networks. The size of the network is inherently restricted, and it is unable to quickly onboard new users due to the approval process. However, private-permissioned networks can accommodate faster transaction processing times, which may be beneficial in certain scenarios for financial institutions, such as real-time or high-frequency transactions.

Public-Permissioned Networks

Public-permissioned DLT networks combine features of public access from permissionless networks and restricted control from private-permissioned networks, making them a popular option for financial institutions seeking to capitalise on core DLT characteristics (i.e., transparency, immutability, resiliency, and programmability) while maintaining the level of control required for risk management purposes.

In hybrid networks, multiple tiers of users may coexist, including both approved and non-approved users. Unlike private-permissioned networks, where access to all kinds of information is restricted to approved users only, public-permissioned networks can grant limited access or editing privileges to non-approved users, depending on the design and requirements of the network. This tiered access control allows organisations to maintain a clear delineation between public information and sensitive data, ensuring that only authorised users can modify critical information. By incorporating elements of the first two models, public-permissioned DLT networks offer a level of flexibility and scalability required for enabling participants to have special permissions while maintaining a decentralised structure for others.







Regardless of such benefits, public-permissioned DLT networks are still affected by the issues encountered in both private-permissioned and permissionless networks. Scaling the network while ensuring security for approved users remains a challenge, and processing times may be affected if unapproved users gain access to writing privileges. Therefore, organisations must carefully weigh the benefits and drawbacks when designing and implementing hybrid networks.

2.1.2 Protocol

The consensus algorithm is the central component of the protocol, governing how participating nodes interact to validate, agree upon, and record transactions on the distributed ledger to ensure the consistency of entries. Prominent consensus algorithms include Proof-of-Work (PoW), where nodes compete to solve complex mathematical puzzles to validate transactions, and Proof-of-Stake (PoS), where a node's likelihood of validating transactions correlates with its stake (i.e., the number of tokens held in the network).

Beyond these established algorithms, the market has also seen the emergence of alternative consensus algorithms, including Proof-of-Activity, which secures the network through a combination of PoS and PoW mechanisms. These protocols exert a profound influence on DLT networks, as they also define the cryptographic hash functions and the keys necessary for accessing information stored on the ledger. Furthermore, some of the protocols enable advanced functionalities, such as virtual machines, which facilitate the computation and execution of smart contracts. By empowering users to autonomously execute transactions based on predefined conditions coded into the contract, these features effectively eliminate the need for intermediaries (see Figure 4).

Figure 4: Notable Consensus Mechanisms

Consensus Mechanism	First Instance in DLT	Launch Year	Description
 PROOF-OF-WORK (PoW)	Bitcoin	2009	Miners solve complex mathematical problems to validate transactions and create new blocks
 PROOF-OF-STAKE (PoS)	Peercoin	2012	Validators are chosen to create new blocks based on the number of cryptocurrencies they hold and are willing to "stake"
 PRACTICAL BYZANTINE FAULT TOLERANCE	Tendermint	2014	A consensus mechanism that ensures agreement among nodes even if some fail or act maliciously
 PROOF-OF-ACTIVITY	Decred	2016	A combination of PoW and PoS, miners solve complex mathematical problems and then stake cryptocurrencies to validate transactions
 PROOF-OF-ELAPSE TIME	Hyperledger Sawtooth	2016	Wait times are randomly assigned to nodes, with the node waiting the shortest time allowed to validate transactions
 PROOF-OF-AUTHORITY	Ethereum Testnet "Kovan"	2017	A few pre-approved validators are trusted to create blocks and maintain the network

Note: The mechanisms listed above have been shortlisted based on their relevance to the financial services industry and are not intended to be collectively exhaustive

Source: Institute of Electrical and Electronics Engineers Access, blockchain project websites, Quinlan & Associates analysis



The SFC will continue to work with the industry to identify the value of tokenisation and focus efforts on value enhancing. This collaborative approach aims to harness the potential of blockchain technology to improve efficiency, transparency and accessibility in financial markets. In addition to its efforts in tokenisation, the SFC continues to be at the forefront of virtual asset regulation, ensuring that the trading, custody and fund management of virtual assets are conducted with the highest standards of integrity and security.

Dr YIP Chee Hang, Eric, Executive Director, Intermediaries Division, SFC



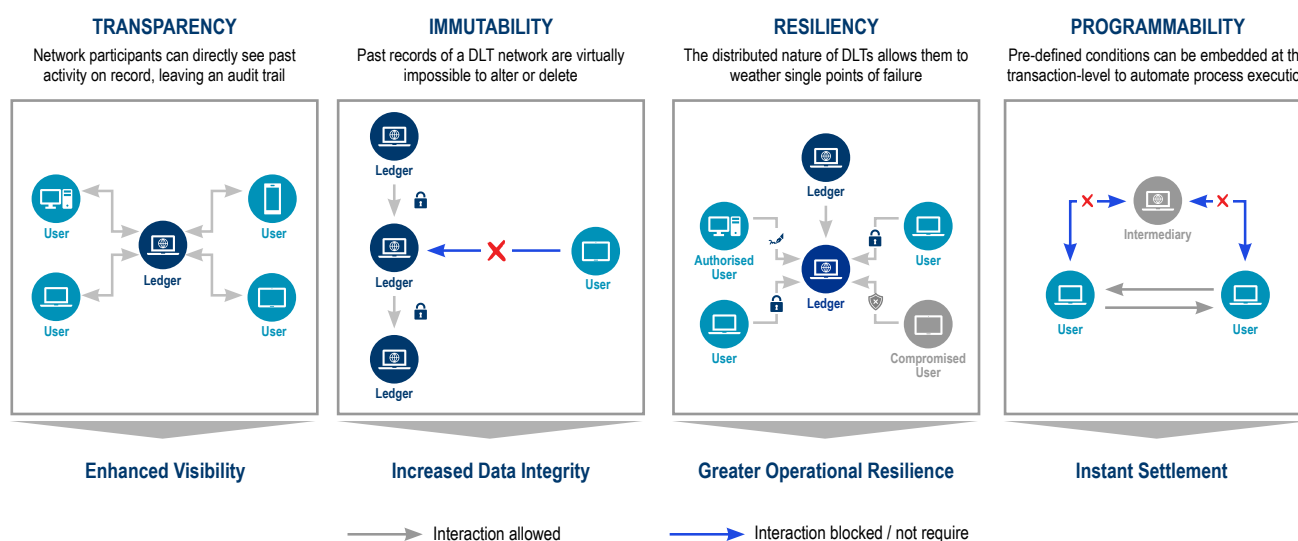
2.2 Core Characteristics

Drawing from its foundational components and building blocks, the DLT network embodies a range of advantageous attributes including transparency, immutability, resiliency, and programmability, all of which help to support diverse use cases across various industries (see Figure 5). These innate features enable DLT to offer significant benefits to industry participants, enhancing operational efficiencies and trust.

Transparency

A single source of truth is maintained and replicated across all participating nodes, ensuring that both historical and ongoing records are accessible to network participants as defined by the protocol. This characteristic can be leveraged for a more streamlined reconciliation of financial records and robust risk management practices.

Figure 5: Core Characteristics of DLT



Source: Blockchain Council, Alchemy, Quinlan & Associates analysis

Immutability

In contrast to traditional centralised systems, where data is typically under the control of a single entity or authority and susceptible to potential manipulation or unauthorised changes, DLT stores data in a decentralised manner. Participating nodes maintain the data, which is organised into “blocks,” containing batches of previously validated information agreed upon by network participants. Each block is linked to the preceding one using cryptographic hashes, starting from the genesis block. This structure makes any attempt to alter or delete previous records nearly impossible due to the interconnected and interdependent nature of the information stored on DLT. In certain types of DLT mechanisms (e.g., PoW), mutability may theoretically be possible under

extreme cases if more than 51% of the network is controlled by a single participant. However, this scenario is specific to some consensus mechanisms and is generally considered unlikely in well-secured networks. The immutable record, combined with transparent audit trails, ensures the integrity, security, and reliability of financial information.

Resiliency

DLT's decentralised architecture maintains a single source of truth across all participating nodes, with every change subject to mutual verification. This approach renders DLT resistant to a single point of failure, reducing the risk of data losses and potential security breaches – a critical feature for any financial institution.

Programmability

DLT, equipped with the smart contract feature, offers programmable capabilities that enable participants to configure and embed predefined conditions on their intended transactions. These transactions are executed and settled automatically once the

conditions are fully met. The programmability feature, ideally with a mechanism for intervention to manage contingencies, is poised to bring about a significant transformation to traditional financial operations by automating processes that do not require a certain degree of human judgement.



The IA keeps pace with the evolving Insurtech landscape and is dedicated to collaborating with stakeholders to build a robust ecosystem for better application of enabling technologies, such as DLT, that benefit policyholders and promote industry development.

Mr Clement Lau, Executive Director (Policy and Legislation), IA



2.3 Technology Development



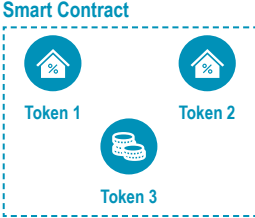
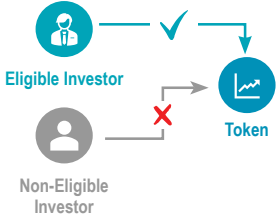
DLT has undergone substantial evolution, incorporating advanced features and capabilities to address technological hurdles commonly encountered by participants and enrich its strategic value across various sectors. Key advancements have been made in tokenisation and oracles to accommodate features that are required for broader cross-sector applications in the financial services industry.

2.3.1 Tokenisation Standards

Prior to the development of token standards, DLTs in their most basic form were limited to making transactions using endogenous cryptocurrencies (e.g., Bitcoin), as they were not designed to represent and/or trade exogenous assets (e.g., traditional financial instruments). Over the past decade, innovative protocols have emerged with advancements that enable exogenous assets to be represented, programmed, and traded on DLT platforms. While numerous cutting-edge protocol developments have been introduced, the following are highlighted for their broad adoption rate among financial institutions (see Figure 6).



Figure 6: Tokenisation Standards

	ERC-20 <i>Fungible Tokens</i>	ERC-721 <i>Non-fungible Tokens</i>	ERC-1155 <i>Fungibility-agnostic Tokens</i>	ERC-3643 <i>Security Token Contract</i>
				
Year	2015	2017	2019	2021
Description	Interchangeable digital assets that are identical and mutually interchangeable	Unique digital assets that represent ownership of a specific item	Digital assets with flexible traits (i.e., it could be interchangeable or unique)	Digital assets with capabilities to enforce regulatory restrictions
Traits	Interchangeable	Unique	Only requires a single smart contract for both unique and interchangeable tokens	Compliant to securities regulation
Use-cases	Non-distinguishable assets (e.g., securities, currencies, commodities, etc.)	Distinguishable assets (e.g., loans, real estate, art pieces, etc.)	Transactions that involve multiple assets (e.g., composite instruments)	Security trading (e.g., tokenised private credit, real world assets, etc.)

Source: Ethereum Improvement Proposal, Vegavid Technology, Tatum, BitKan, Quinlan & Associates analysis

The Ethereum network has introduced several token standards to facilitate the creation and trading of various asset types. These standards have evolved to address the limitations of earlier tokens and provide greater functionality and compliance.

- ERC-20 (i.e., Fungible tokens): Ethereum introduced fungible tokens that allowed network participants to mint interchangeable assets like securities and currencies. These tokens can embed transaction instructions with predefined conditions that are executed automatically and settled instantly, a capability now commonly referred to as a smart contract. However, the interchangeable nature of fungible tokens limited their ability to tokenise unique and high-value items.
- ERC-721 (i.e., Non-fungible tokens): In response to the limitations of fungible tokens, non-fungible tokens were developed to capture the scarcity of real-world assets. Financial institutions can use these tokens to represent high-value assets or collateral, such as art or mortgages. However, the incompatibility of ERC-20 and ERC-721 tokens on the same smart contracts hindered effective trading.
- ERC-1155 (i.e., Fungibility-agnostic tokens): The introduction of a fungibility-agnostic token addressed the limitations of previous tokens. Prior to the development of this token, trades involving multiple types of tokens (e.g., delivery versus payments (DvP) for unique assets) required separate smart contracts for each type. The fungibility-agnostic token reduced the number of smart contracts needed to one, enabling financial institutions to minimise redundancies and potential errors.⁶ Reducing documentation requirements further augmented the benefits of tokenised assets, compressing settlement times and streamlining transactions.
- ERC-3643 (i.e., Regulated security token contract): While previous token standards have streamlined the underlying infrastructure for direct peer-to-peer DvP processes, these standards are still inadequate for real-world asset tokenisation due to securities regulation. To address this, new security token standards have introduced tokens with inherent traits such as investor-type restrictions and ownership monitoring to ensure greater compliance. By integrating risk management within DLT infrastructure, these standards accelerate the adoption of tokenised assets in traditional financial services and markets.

⁶ Tatum. 2022. *Smart Contracts*. (<https://docs.tatum.io/docs/smart-contracts>).

2.3.2 Oracles

The development of oracles has been instrumental in advancing tokenisation, particularly when combined with token standards (see Figure 7).

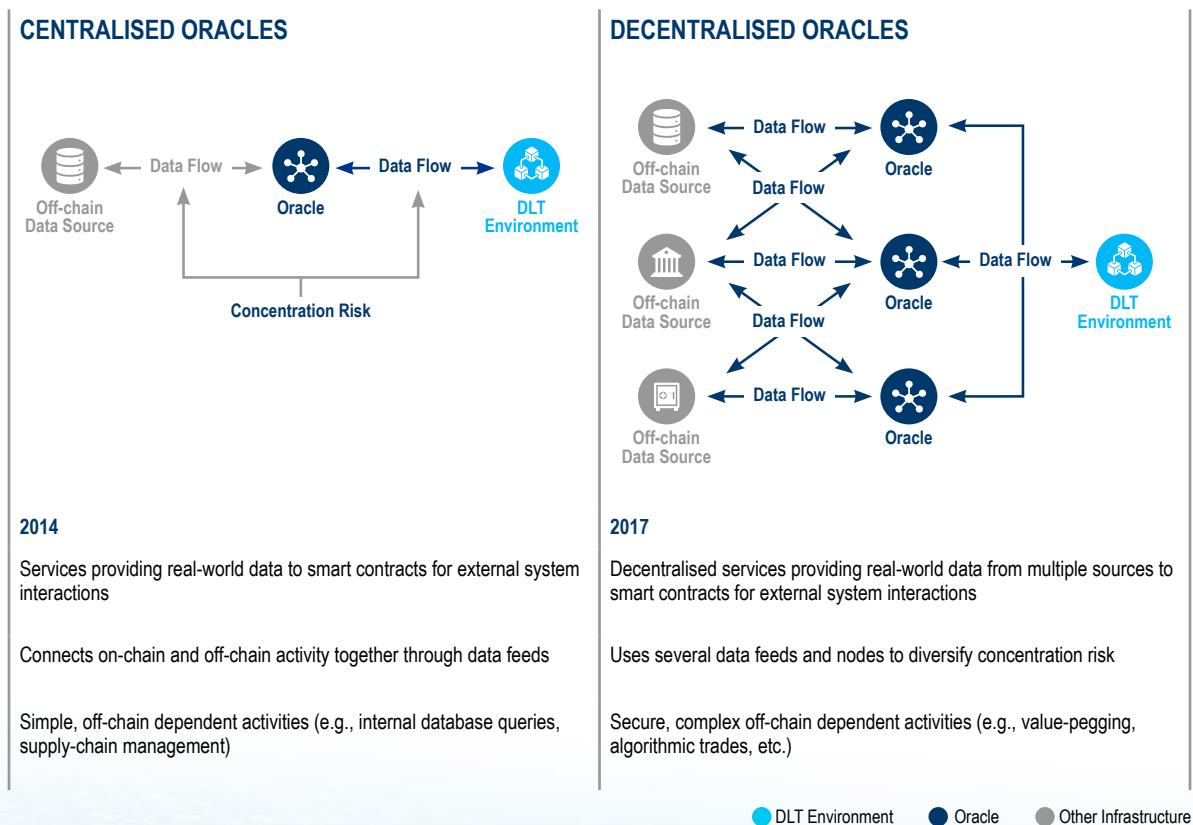
A key limitation of many DLT networks is their isolation from external data sources, which restricts their ability to extract or transmit data off-chain. Oracles act as intermediary protocols, that connect DLT networks to off-chain data sources, facilitating the secure retrieval and integration of real-world data, such as financial market prices, supply chain updates, or weather information. This capability enables DLT networks to interact with external systems, bridging the gap between on-chain and off-chain environments and even enabling proprietary enterprise data to be brought on-chain to support smart contract execution.

Traditional oracles, often centralised, rely on a single data source and are well-suited for use cases that require access to trusted, proprietary data.

However, their reliance on a single source can create vulnerabilities, such as single-point failures or data manipulation risks. To address these concerns, decentralised oracles have emerged as an alternative approach to enhance the resilience of off-chain connectivity. Decentralised oracles are particularly critical for use cases that demand high levels of reliability and trust, such as supporting tokenised assets with value pegging or facilitating broader financial applications.

Decentralised oracles ensure that tokenised securities accurately reflect real-world prices by pegging them to off-chain data while maintaining the resilience of DLT networks. By securely linking on- and off-chain information, decentralised oracles significantly enhance the functionality and utility of smart contracts, thereby expanding the potential applications of tokenisation. Together, centralised and decentralised oracles provide flexibility and adaptability for different types of DLT use cases.

Figure 7: Oracles



Source: Reality Keys, Chainlink, Quinlan & Associates analysis



The MPFA monitors the adoption of DLT in the MPF industry as it navigates the Fintech ecosystem and will continue to work together with other financial regulators to facilitate the healthy development of DLT in the financial services sector.”

Mr Kenneth Chan, Executive Director (Members and Supervision), MPFA



2.4 Conclusion

DLT has garnered significant interest in the financial services industry, driven by its unique benefits, including decentralisation, immutability, resiliency, transparency, and programmability. As a result, many financial institutions are exploring ways to leverage DLT in their current operations. Advances

in technology, from tokenisation standards to oracles, have now paved the way for financial institutions worldwide to consider, explore, and harness the transformative potential of DLT.



3. Adoption Use Cases

In recent years, the financial services industry has seen notable adoptions of DLT. To gain a deeper understanding of the practical applications of DLT, the HKMA has conducted a series of in-depth interviews with key stakeholders from 10 organisations across the banking, securities, and insurance sectors that

have implemented DLT in various capacities (see Figure 8). The interviews aimed to explore three key aspects: (1) the solution mechanism employed, (2) the rationale behind adopting DLT, and (3) the DLT-specific challenges encountered.

Figure 8: DLT Adoption Case Summary

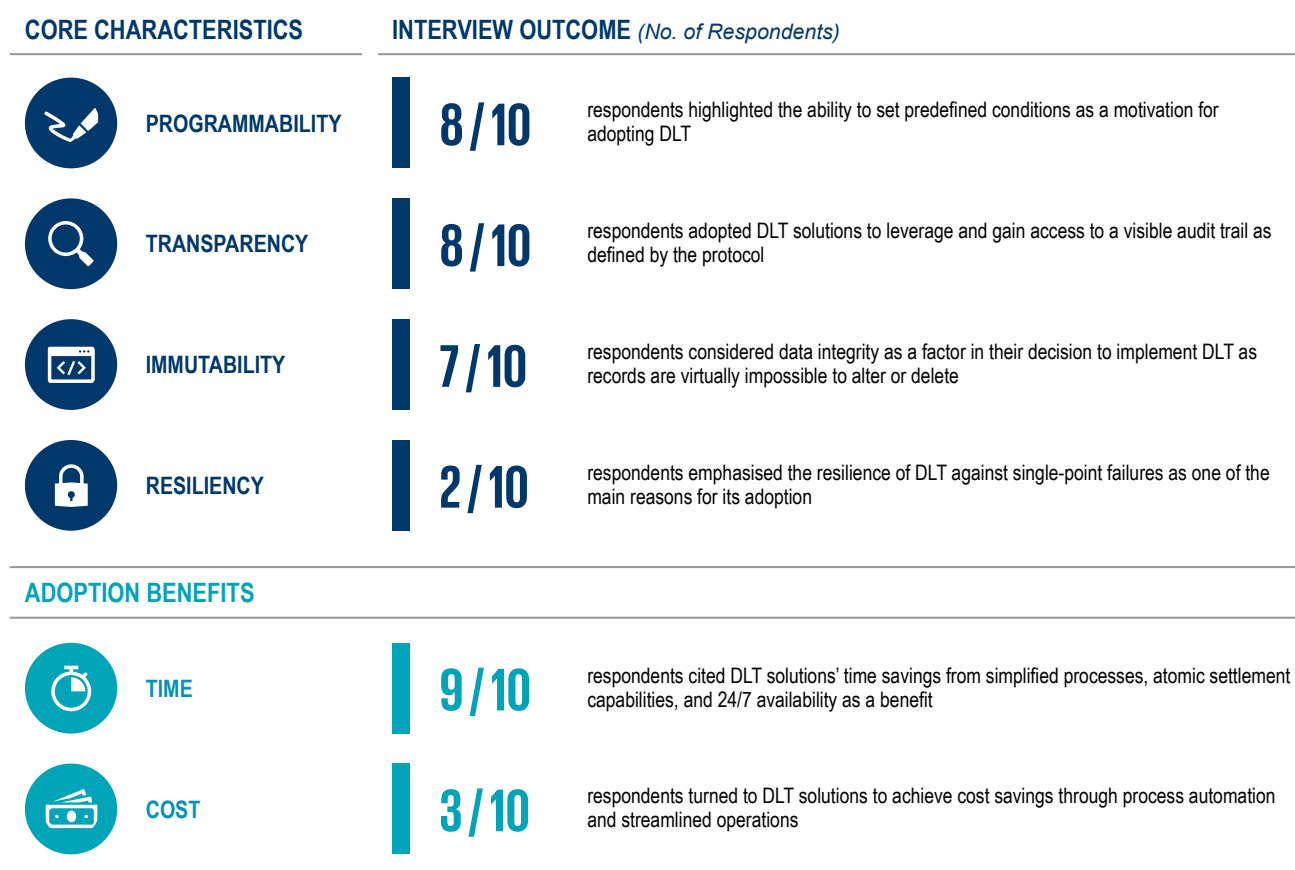
SECTOR	ORGANISATION / SOLUTION NAME	SOLUTION MECHANISM / UNIQUE PROPOSITION
BANKING	Hang Seng Bank Hypothetical e-HKD Use Case	Enhances user experience and eliminates manual processes within the reward lifecycle, from distribution to payment settlement, for merchants, users, and financial institutions via conditional payments, instantaneous settlements, and automatic reconciliation
	HSBC Experimental Tokenised Deposit Solution	Enables 24/7 fund transfers for customers through tokenised deposits, which enhances clearing capabilities and addresses the limitations of traditional clearing systems
	Linklogis Digital Trade Token	Provides deep-tier supply chain financing through stablecoin-based conditional payments, allowing anchor buyers to manage their supply chain ecosystem and banks to gain more visibility into their financed space's downstream payments
	Wecan Group Wecan Comply	Allows one party to share and update compliance-related data simultaneously with a network of permissioned counterparties, such as custodian banks and wealth managers, for KYC and KYB purposes
SECURITIES	Deutsche Bank & Memento Blockchain Digital Identity in Project DAMA 1	Utilises a KYC and digital identify solution as a feature of Project DAMA 1, which has the potential to be a one-stop digital fund investment servicing platform to reduce the effort for asset managers, transfer agents, fund administrators, and custodians to launch and service digital funds
	HKEX & Digital Asset Synapse	Enables global investors to more efficiently manage time zone constraints in Mainland China's A-shares market through Northbound Stock Connect by replacing traditional sequential settlements with simultaneous conditional approvals and incorporating buy-side and custodians into the process
	J.P. Morgan Digital Financing Application on Kinexys Digital Assets Platform	Provides secured financing against tokenised collateral on an intraday, overnight or term basis; integrating the execution and settlement, the solution adds precision, automation, and control in repos through the near-instantaneous settlement of tokenised assets and cash
	UBS UBS Tokenize	Allows issuers to tap new and flexible funding pools and enables investors to access new issuers, smaller ticket sizes, and more flexible product characteristics, via a DLT-based tokenisation service that supports issuance, distribution, and custody of digital assets
INSURANCE	Allianz Cross-border Claims Settlement Solution	Streamlines the end-to-end European cross-country motor claim business across 25 organisational silos while improving governance in a frictionless way
	HKFI & CryptoBLK Motor Insurance DLT-based Authentication System (MIDAS)	Allows parties to authenticate motor insurance without disclosing personal information as the first industry-wide DLT application in Asia for insurance

Source: Interview findings, Quinlan & Associates analysis

The interview participants provided a variety of reasons for adopting DLT. Core characteristics of the technology have sparked significant interest among financial institutions, with all interviewees citing at least two intrinsic features of DLT derived from its underlying technology and architecture. Beyond

the core characteristics, interviewees also shared supplementary benefits that result from the use of DLT but are not necessarily part of the fundamental structure, such as atomic settlement and low costs (see Figure 9).

Figure 9: DLT Adoption Rationale Summary



Source: Interview findings, Quinlan & Associates analysis

Core Characteristics

Programmability and transparency are two leading factors driving the adoption of DLT among financial institutions, with eight out of ten interviewees citing them as primary drivers.

Programmability enabled some financial institutions to experience improved efficiency and reduced error rates, while others reported streamlined operational processes as a major upside. Beyond operational improvements, programmability has granted

enhanced control to financial institutions, enabling a securities firm to customise at both the token and transaction levels, while enabling another institution to provide access to multiple investor groups by embedding conditional statements into their tokens.

Transparency, on the other hand, was often mentioned alongside immutability, another strong adoption driver cited by seven interviewees. These attributes create a visible and tamper-proof single source of truth, which is particularly valuable for shared information depository use cases such as

Know Your Customer (KYC) and authentication. The immutable nature of the record ensures data integrity, while the transparent ledger offers visibility into traditionally opaque financial transactions, providing institutions with enhanced control and insight into their operations.

Resiliency was highlighted by two interview participants as a key reason for adoption, thanks to DLT's distributed nature that mitigates the risk of single points of failure. One financial institution's solution focused on local encryption and decentralised data storage, ensuring users retain full control over their data. Similarly, another institution leveraged these security features to foster greater trust among its users. However, the relative lack of emphasis on resiliency suggests that many institutions may be assuming its inherent presence within DLT and hence may be overlooked. This underscores the importance of and need for a robust design approach (e.g., incorporating fault-tolerant consensus mechanisms, rigorous security protocols, effective recovery strategies, etc.) to strengthen system resiliency and mitigate operational failures from the outset.

Adoption Benefits

The time-related benefits enabled by the core characteristics of DLT emerged as the primary driver of adoption among financial institutions during our interviews. Nearly all interviewees cited time savings from simplified processes, atomic settlement, or reduced time restrictions as key advantages of adopting DLT.

More than half of the interviewees highlighted time savings resulting from simplified processes as a significant benefit. Compared to traditional systems, DLT enables faster and more efficient distribution of information and value, streamlining operations. For instance, one institution noted that shifting from traditional workflows to a DLT-based solution reduced delays by providing real-time information access.

In addition, half of the interviewees emphasised the importance of the atomic settlement capability of DLT, which allows transactions to be settled instantly and securely. For example, a few financial institutions highlighted how DLT accelerated transaction settlement times in their solutions, whether that be in payments or trading applications.

Furthermore, two interviewees highlighted the advantage of reduced time restrictions associated with DLT. Unlike conventional settlement systems constrained by operational hours, DLT-based transactions can support 24/7 service provision, enabling financial institutions to respond more flexibly to market demands and customer needs.

Beyond time savings, some institutions recognised DLT's potential for cost reduction. The transparency fostered by DLT reduces the need for manual human efforts typically required in traditional transactions to verify and process transactions. By streamlining these labour-intensive tasks, institutions may lower transaction costs. For instance, one financial institution reported that its DLT network helped to bridge information silos across the organisation, thereby reducing administrative overhead and increasing cost efficiency required for transactional operations. The cost-related benefit, however, was a secondary priority for most financial institutions. Many interviewees acknowledged that the costs associated with DLT adoption, such as integration and migration, may often exceed the expense of maintaining existing systems. Despite this, financial institutions are exploring DLT adoption as the time savings and other core characteristics, such as immutability, may easily outweigh the costs.

As financial institutions increasingly recognise the transformative potential of DLT, they are more inclined to explore and integrate it into their existing systems and operations. The following section will examine ten detailed case studies, exploring the solution mechanisms and rationale for adoption.

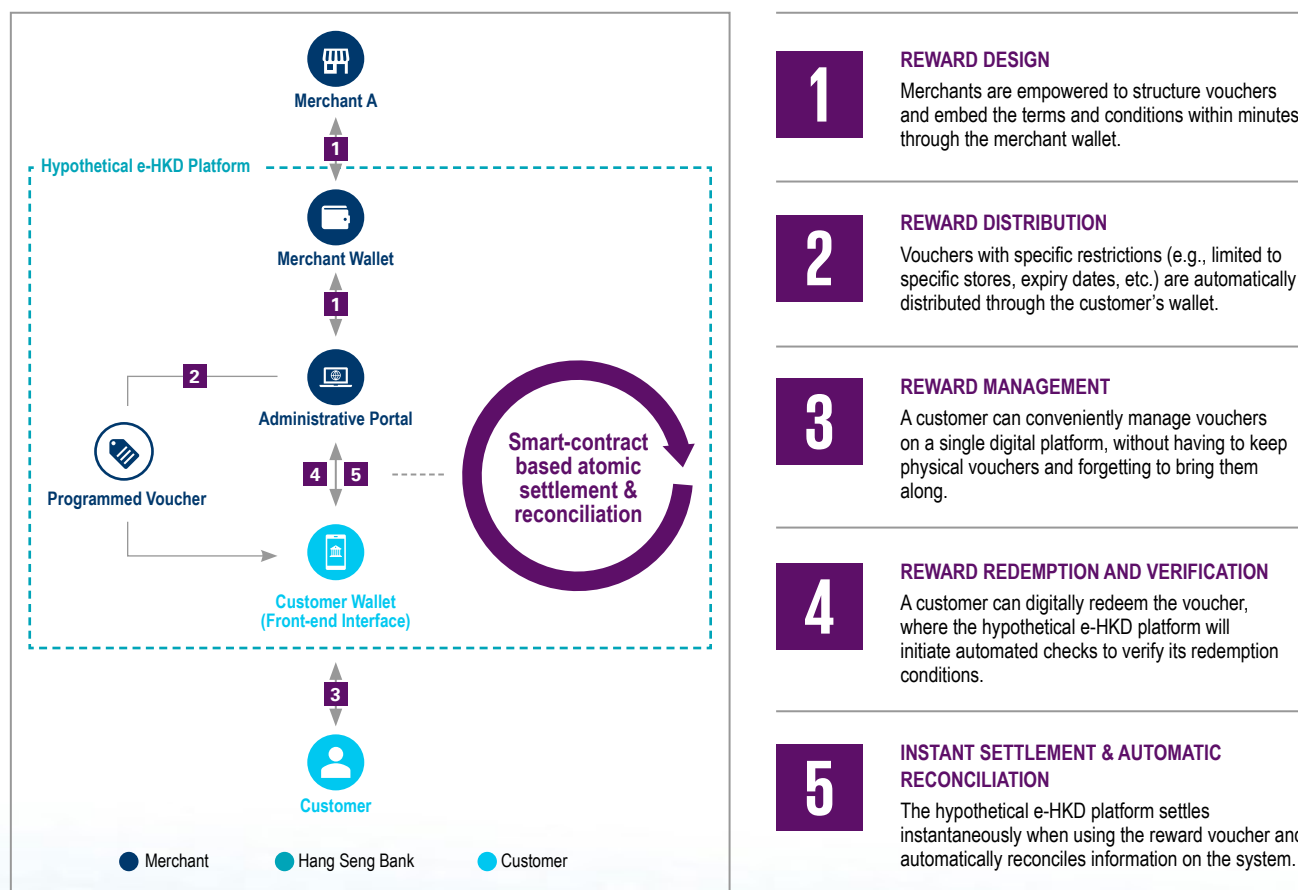
3.1 Hypothetical e-HKD Use Case by Hang Seng Bank for Merchant Payment and Rewards Programme

As part of the HKMA's Phase 1 of the e-HKD programme, Hang Seng Bank developed a platform for merchants that aims to test the effectiveness of a hypothetical e-HKD to streamline the issuance, distribution, and usage of vouchers in a digital reward platform by leveraging the programmability feature of smart contracts and the atomic settlement capability of DLT.

Solution Mechanism

Customers can conveniently manage vouchers from various merchants on a single platform within their banking application. When redeeming these vouchers, customers simply pay using hypothetical e-HKD via their customer wallets. By using smart contracts with pre-set conditions defined by merchants, the vouchers automatically apply discounts and other benefits when certain conditions are met, such as spending at a specific store. This eliminates the need for customers to manually select or remember which vouchers to use while removing the need for merchants to verify expiry dates and conditions (see Figure 10).

Figure 10: Hypothetical e-HKD Use Case by Hang Seng Bank



Source: Hang Seng Bank, Interview findings, Quinlan & Associates analysis

A report published by Hang Seng Bank indicates that 81% of users were satisfied, and 83% believed that the programmability feature surpassed their expectations.⁷ Additionally, merchants are not required to verify the authenticity of the vouchers or check compliance with usage conditions; the redemption and verification process are both fully automated through the hypothetical e-HKD's smart contracts.

Upon payment initiation, the funds are immediately settled in the merchant's account using hypothetical e-HKD's DLT payment rails with atomic settlement capabilities. This allows merchants to receive their payments within minutes, if not seconds, instead of waiting for a bank or Point-of-Sale system operator to process their transactions. All transactions are automatically reconciled and recorded in merchants' accounts through smart contracts.

Rationale for Adopting DLT

Hang Seng Bank adopted DLT for its hypothetical e-HKD solution due to the benefits brought about by programmability, atomic settlement, enhanced security, and immutability.

In its pilot programme, Hang Seng Bank wanted to capture the programmability trait of DLT networks in its conditional payments. This trait allowed merchants to embed conditions through smart contracts within the hypothetical e-HKD and minimise the framework and operational procedures needed for a successful reward programme. Rather than creating additional processes to distribute and validate voucher usage, merchants can simply design and program the reward programme features.

The pilot programme also took advantage of DLT networks' atomic settlement capabilities. By enabling instant settlements for merchants, smart contracts significantly reduce the time for merchants to receive their capital. The smart contracts also automatically reconcile transactions, eliminating previously manual processes.

In addition to these traits, Hang Seng Bank cited the security and immutability of DLT networks as critical for merchants and the retail ecosystem. The tamper-proof nature of DLT networks prevents external factors from interrupting past and current transactions, instilling trust within the payment system.

In its hypothetical e-HKD merchant solution, Hang Seng Bank utilised a private-permissioned DLT on R3 Corda developed by FORMS HK, citing higher accountability, stricter governance, and superior performance versus permissionless DLTs.

Hang Seng Bank stated that the centrally operated nature of permissioned DLTs ensures the accountability of each validating party. Additionally, as access levels differ for each participant, permissioned networks offer strict governance, with each party having clearly defined roles and responsibilities. This explicit definition of roles imbues greater accountability to the service providers and better supports compliance obligations with regulatory bodies.

Due to their streamlined consensus mechanism, permissioned networks typically can process a higher number of transactions within a specific timeframe than permissionless DLT networks. This trait allowed Hang Seng Bank to quickly scale its pilot and encompass multiple concurrent merchant transactions.



We enhanced the user experience and eliminated manual processes within the reward lifecycle, from distribution to payment settlement, for merchants, users, and financial institutions via conditional payments, instantaneous settlements, and automatic reconciliation.



⁷ Hang Seng Bank. 2023. *Envisioning Programmable Payments in Hong Kong: How could an e-HKD further improve payments in Hong Kong?* (https://www.hangseng.com/content/dam/hase/pdf/envisioning_programmable_payments_in_hong_kong.pdf).

3.2 Experimental Tokenised Deposit Solution by HSBC for Efficient Cross-Border Fund Transfers

In recent years, HSBC has been exploring a range of payments and settlement solutions that leverage the advantages of DLT-based digital currencies while maintaining the fractional backing of traditional deposits. This approach helps to prevent liquidity lockups often associated with central bank digital currencies (CBDCs) and stablecoins.

Although the bank remains in the exploratory phase of tokenised deposits, it recognises the potential to utilise DLT-specific features, such as atomic settlements, in areas like payments, cross-border transactions, foreign exchange settlement, and digital asset settlements. Notably, HSBC has been developing a tokenised deposit based cross-border

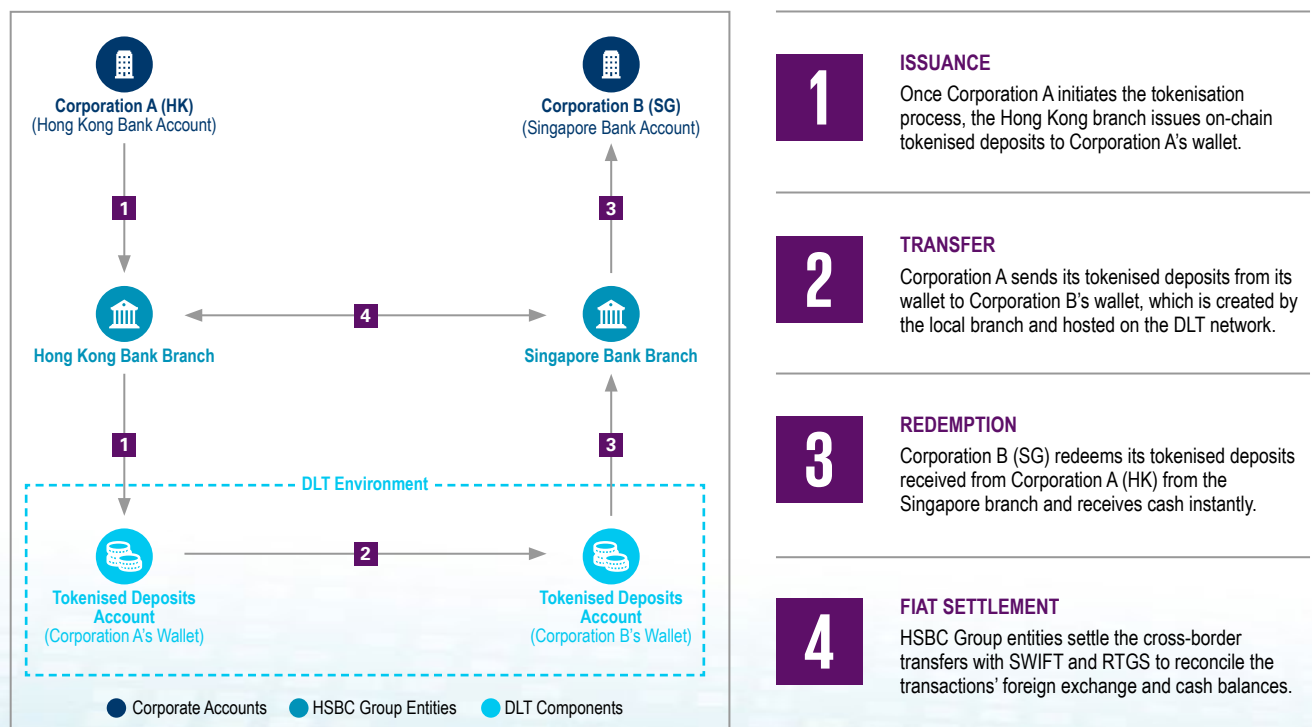
fund transfer solution, which facilitates faster and more flexible real-time fund movements for corporate accounts internationally.

Solution Mechanism

In traditional cross-border fund transfers, businesses often encounter lengthy processing times due to restrictions imposed by payment rails. However, HSBC's proposed tokenised deposit solution, utilising a DLT-based platform, would enable around-the-clock fund movements, bypassing local real-time gross settlement (RTGS) working hours. This innovation offers an always-on channel for cross-border transfers between HSBC locations, improving access to funds for businesses. Moreover, programmable rules can be implemented on their tokens for autonomous execution.

To initiate a cross-border transfer, corporate clients of HSBC request the bank to tokenise their deposits. The bank then mints tokens into an on-chain wallet for the corporate while locking the corresponding amount from the client's deposit account (see Figure 11).

Figure 11: Tokenised Deposit Solution by HSBC



Source: HSBC, Interview findings, Quinlan & Associates analysis



The solution aims to enable 24/7 fund transfers for customers through tokenised deposits, enhancing clearing capabilities and addressing the limitations of traditional clearing systems.



When a corporate client wishes to transfer tokenised deposits to another entity, the tokenised deposits are sent via DLT rails to the recipient's wallet, enabling instantaneous settlement and 24/7 access. Once the recipient wants to redeem the funds to their deposit account, the tokens are destroyed, making the fiat funds available in the client's deposit account. The branches then utilise Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging and local RTGS systems to settle the cross-border transfers and reconcile the underlying fiat currency balances between the two HSBC entities.

As part of Phase 1 of the e-HKD Pilot Programme, HSBC partnered with Hang Seng Bank and Visa to explore the atomicity and interoperability of on-us⁸ and cross-chain payments across two key interbank B2B payment flows using tokenised deposits settled by CBDC.

In a notable test case within the HKMA Fintech Supervisory Sandbox, HSBC tested a prototype of the tokenised deposit solution with Ant International exploring the use of deposit solution as part of its intragroup treasury operations. In the test, HSBC issued tokens on a proprietary network based on deposits held in the banking infrastructure, allowing seamless movement of treasury funds across different group entities and achieved instant and round-the-clock settlement via the token transfer.

Looking ahead in HKMA's Project Ensemble, HSBC aims to expand its tokenised deposit solution to interbank applications. By leveraging the HKMA's interoperability layer, this experimental financial market infrastructure will enable the interbank settlement of tokenised deposits. While the HKMA's current focus in Project Ensemble is primarily on domestic applications, the concept may also expand to enable cross-border payments in future.

Rationale for Adopting DLT

HSBC recognises significant potentials in leveraging DLT networks for its business operations. The programmability of tokens allows for the implementation of business rules and autonomous execution based on predefined conditions, eliminating the need for manual intervention. This capability enables various use cases, such as automatic escrows and conditional payments. Moreover, DLT networks enhance accessibility by providing services 24/7 and circumventing the operating time restrictions of local RTGS systems. They also facilitate atomic settlements, enabling tokenised deposits to support faster and more efficient transactions across various asset classes, including real-world assets (e.g., property), digital assets, and cross-border settlements.

DLT also adds a layer of visibility to fund transfers, transforming a typically opaque process into one that is more transparent. Cross-border transactions often involve multiple parties with disparate systems; however, in HSBC's test case with Ant International, the bank and its customers gained clearer insights into payments information and statuses.

The solution developed for this test case was built for integrating onto a third-party private-permissioned DLT network, given that regulators are more familiar with permissioned networks. In terms of DLT network design, HSBC supports risk-based and technology-neutral approaches, which allow the bank to adapt to evolving needs, including customer demands and regulatory requirements. For example, the bank highlighted that tokenised deposits can also service DvP settlement on HSBC's proprietary tokenised asset network, HSBC Orion, which utilises private and public blockchains, with legal holdings on the private chain and transaction metadata on the public chain.

⁸ On-us refers to a payment where the initiating and receiving financial institution are the same and there is no interbank movement of funds. This is also referred to as a book transfer.

3.3 Digital Trade Token by Linklogis for Enhanced Supply-Chain Financing

In partnership with Standard Chartered Bank, Linklogis introduced conditional payments through digital tokens. Through the adoption of a DLT-based trade finance solution, anchor buyers can strengthen the resilience of their supply chain. This initiative creates a new pathway for small-and-medium-sized enterprise suppliers to fulfil their working capital needs while providing investors with access to an alternative asset class for financing downstream obligations.

Solution Mechanism

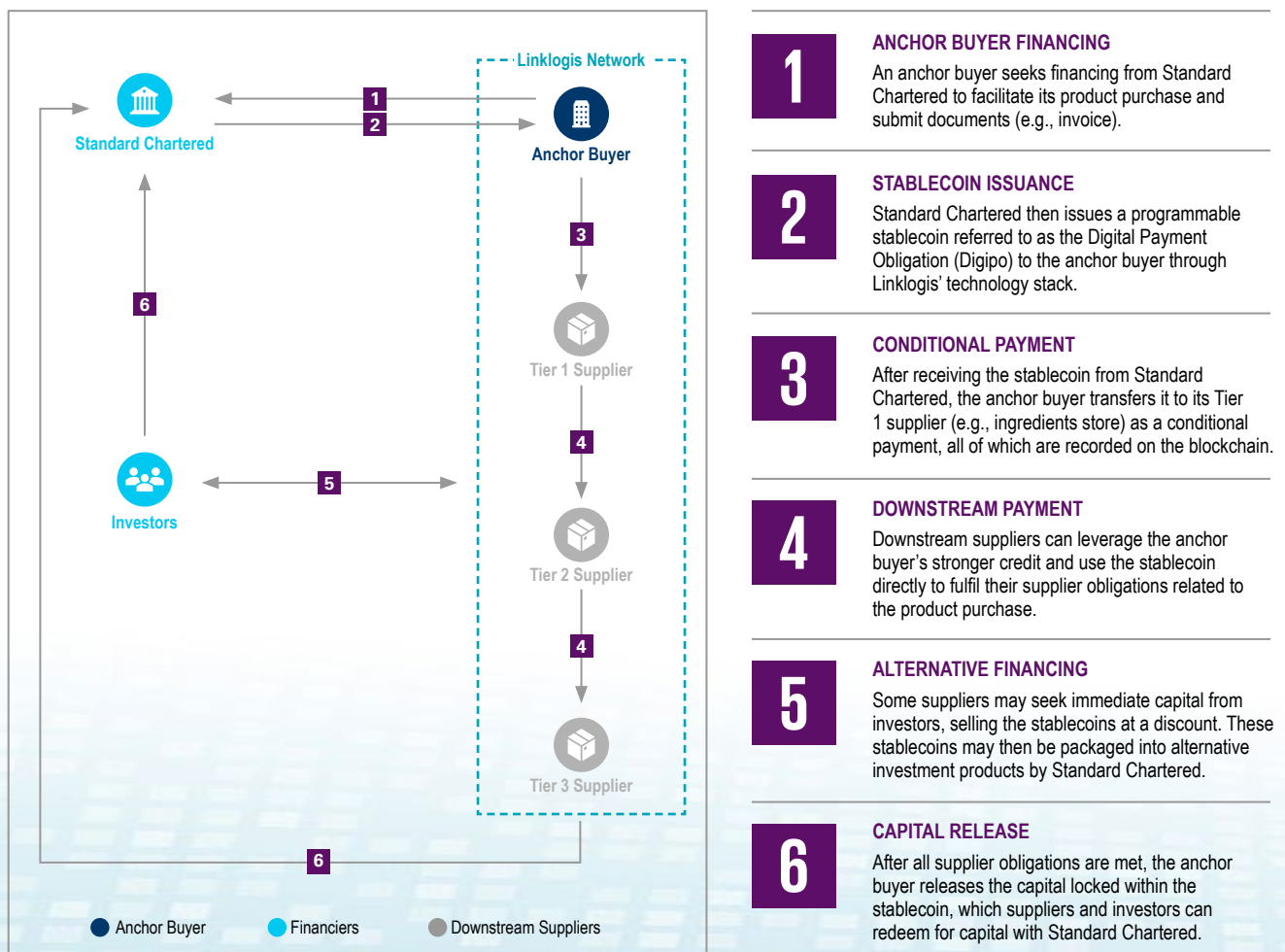
An anchor buyer kickstarts the financing process with a banking institution, drawing a line of credit. Like traditional credit applications, the anchor buyer submits documents to secure financing for the

purchase. With this credit line, the banking institution issues the corresponding amount of tokens, namely the programmable stablecoin, to the anchor buyer (see Figure 12).

The anchor buyer can use this stablecoin to pay the downstream suppliers (i.e., Tier 1 suppliers). Once the obligations of the downstream supplier are met, the anchor buyer can then release the cash payment from the bank. Anchor buyers can set these conditions and transfer the tokens through a website interface.

Tokens can be used by downstream suppliers in three ways, including: (1) as payment to fulfil further downstream payments to upstream suppliers (i.e., Tier 2 and 3 suppliers); (2) liquidating them at a discount to investors for working capital management; or (3) waiting until the anchor buyer releases the capital by holding onto them. Once the downstream supplier has met its obligations, the token holders can redeem the tokens with the bank for cash.

Figure 12: Digital Trade Token by Linklogis



Source: Linklogis, Interview findings, Quinlan & Associates analysis



We provide deep-tier supply chain financing through stablecoin-based conditional payments, allowing anchor buyers to manage their whole supply chain ecosystem and banks to gain more visibility into the downstream payments of their financed space.



Rationale for Adopting DLT

Linklogis chose to adopt DLT for its supply-chain financing solution as it provides enhanced traceability of money flow and accelerated peer-to-peer transactions. The technology also enables unique characteristics to be embedded at the token level, facilitating the separation of digital monies within the same account (i.e., stablecoins coded for different payment purposes). Such separation provides visibility into the use of funds by the financed party, providing financial institutions with a deeper understanding of their clients' financial positions. Traceability permanently records a stablecoin's origin and circulation history, which equips participants with the information to evaluate an entire supply chain.

In addition, DLT networks allow the platform to quickly establish trust with supply chain financing participants. The programmable nature of the stablecoin also removes the need to trust a single entity, as payments are automatically executed. While traditional escrow solutions may deliver the same effect, DLT's programmability and low fees outperform their tedious and costly processes.

Due to the closed-loop nature of private-permissioned networks, which can restrict the size and scope of the served ecosystem, Linklogis opted to use Ethereum's permissionless network to develop its solution. The low barrier of entry and easy accessibility of the public-permissionless network enables more supply chain stakeholders to be seamlessly onboarded, despite divergence in their digitalisation efforts, such as variations in Enterprise Resource Planning systems for accounting and bookkeeping.

3.4 Wecan Comply by Wecan Group for Secure and Efficient Data Exchange

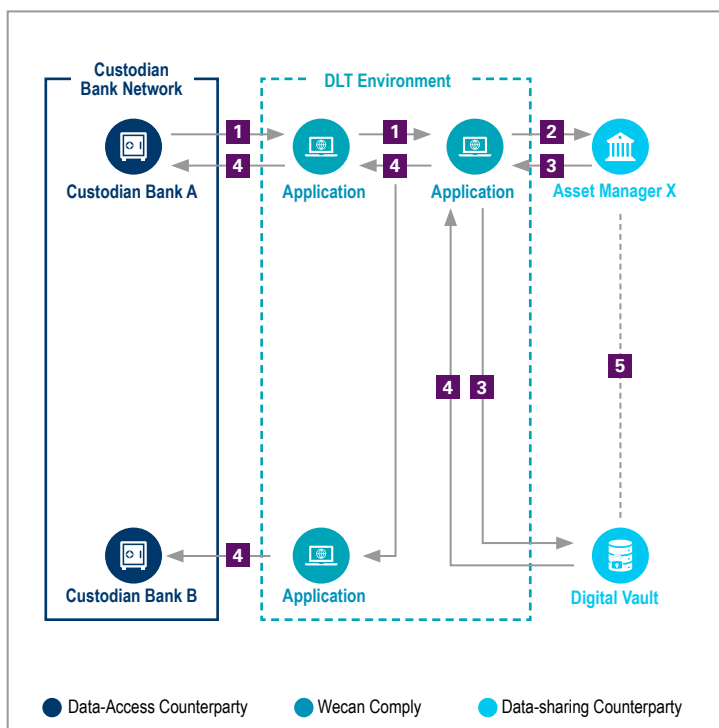
Financial institutions must navigate the data-sharing process for KYC and Know Your Business (KYB) purposes with various counterparties. The process often involves duplicative efforts, as the same information is repeatedly shared, leading to time-consuming form-filling and inefficiencies for institutions and their end users. Additionally, the data's sensitive nature requires institutions to manage it with utmost security during storage and transfer. To address these challenges, Wecan Group in Switzerland has introduced a private DLT network designed to facilitate the secure and efficient exchange of data. In this network, Wecan Group cannot access sensitive data shared amongst financial institutions.

Solution Mechanism

Wecan Comply is an application for various types of counterparties, including banks and wealth managers, to exchange compliance-related data for KYC and KYB purposes in a one-to-many format. Users can access the solution through a straightforward web-based interface or achieve full integration with broader systems, like customer relationship management, via application programming interfaces (APIs).

Custodian banks can utilise standard KYC / KYB forms or upload their own KYC / KYB forms to collect time stamped data from asset managers digitally (see Figure 13). This solution ensures that valid, accurate, immutable, and up-to-date data can be securely shared with multiple parties simultaneously.

Figure 13: Wecan Comply by Wecan Group



1

REQUEST

Custodian Bank A requests Asset Manager X to provide relevant data for due diligence purposes.

2

NOTIFICATION

Through Wecan Comply, a notification is sent to Asset Manager X indicating that Custodian Bank A is requesting a data submission.

3

SUBMISSION

Asset Manager X fills in requested data for due diligence requirements (e.g., onboarding), which is encrypted and stored in a digital vault.

4

SHARING

Asset Manager X controls access and shares the data with multiple custodian banks without duplicative efforts.

5

MAINTENANCE

Reminders are sent for documents with imminent expiry and notifications are sent for any changes made to the stakeholders.

Source: Wecan Group, Interview findings, Quinlan & Associates analysis

To initiate the KYC / KYB data sharing process, an external asset manager selects one or several custodian banks, fills in data as required by the corresponding institutions' KYC / KYB forms, and shares the said forms. The application then notifies the bank(s) to validate the received data. Sensitive information is securely stored in a private digital vault created by Wecan Group, with access restricted solely to the concerned parties. Before sharing any information, the asset manager internally validates the data to ensure accuracy. Manual confirmation is required to minimise the risk of errors.

When the asset manager decides to disclose the information to the custodian bank, the underlying DLT network synchronises the information across all authorised parties. Custodian banks can set expiration dates for request forms to ensure the validity of the shared data. As the expiration date approaches, the application automatically reminds the asset manager to confirm or update the information to keep it current. Both parties can also track status and edit history throughout the data-sharing process via an application dashboard.



Wecan Comply allows one party to share and update compliance-related data simultaneously with a network of permissioned counterparties.



Overall, the solution supports an efficient and compliant data-sharing process between custodian banks and asset managers by reducing redundant data-sharing efforts.

Rationale for Adopting DLT

The solution is built on an institutional blockchain, whose network nodes are managed by a consortium of reputable Swiss institutions, strengthening trust and operational resilience. By leveraging distributed solutions, Wecan Comply enables financial institutions to maintain full control, ownership, and auditability of their sensitive data throughout the exchange process. All data encryption occurs directly within the user's browser, with users retaining sole ownership of the encryption keys. This approach limits data access and management to authorised parties only, enhancing security while reducing dependence on the solution provider.

3.5 Digital Identity in Project DAMA 1 PoC by Deutsche Bank, in partnership with Memento Blockchain, for Seamless KYC Documentation and Identity Authentication

To address key challenges associated with the launch, distribution and servicing of digital funds, Deutsche Bank, in collaboration with Memento Blockchain Pte Ltd, conducted Project DAMA 1 (Digital Assets Management Access) Proof-of-Concept (PoC). The digital asset project featured fund tokenisation, distribution, valuation, investor KYC / Anti-money laundering (AML) filtering, fund administration, reporting, recording, and custody capabilities.

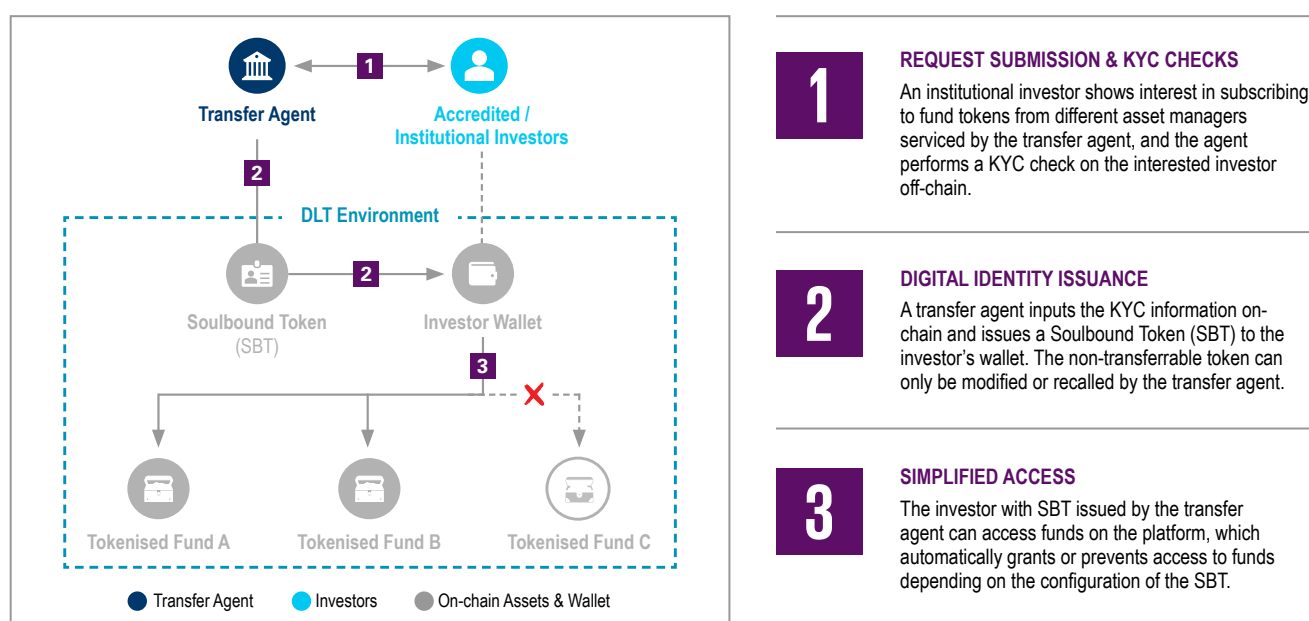


Solution Mechanism

One of the most notable features of Project DAMA 1 PoC (2023)⁹ is its digital identity solution, which can enable investors to reduce unnecessary time and

effort spent on on-chain KYC-type documentation and make identity authentication more seamless. It can enable new scenarios like the one illustrated below (see Figure 14).

Figure 14: Digital Identity in Project DAMA 1 PoC



Source: Deutsche Bank, Interview findings, Quinlan & Associates analysis

In traditional processes, an investor subscribing to different funds under the same transfer agent typically must submit requests for multiple KYC checks – one for every asset manager subscribed. Project DAMA envisages the transfer agent to conduct the required KYC checks, such as investor KYC profiles and sources of wealth. After successful checks, the transfer agent then issues a non-transferable Soulbound Token (SBT) containing metadata to the investor's wallet as proof of the KYC check. The token can potentially allow the investor to access multiple funds from different asset managers without further checks. It can also automatically block investors from subscribing to unsuitable products.

The smart contract programmability ensures that the token cannot be easily transferred to other entities, preventing impersonation. The team had also assessed that the SBT token can be executed in trusted environments for mobile devices, ensuring that the SBT is not replicated to the cloud and is instead tied directly to the device. They envisaged two-factor authentication as a method to further prevent identity fraud. It also ensures that investors are not exposed to public / private key management. These traits would become back-end processes to maximise accessibility and streamline the user experience.

⁹ Deutsche Bank. 2023. *Simplifying digital fund management and investment servicing – Corporates and Institutions*. (<https://corporates.db.com/publications/White-papers-guides/simplifying-digital-fund-management-and-investment-servicing>)

In the case of changing investor profiles (e.g., risk profile changes), the transfer agency may recall or modify the SBT token, adding another layer of flexibility. Additionally, the transfer agency can easily apply additional filters to change investor access to funds depending on regulations (e.g., sanctions). The conditions are automatically updated for all similar investors.

Aside from digital identity management, the project also tested out digital fund creation, management, and distribution capabilities for fund managers. Fund managers can directly create funds by listing their fund strategy, asset weighting, risk rating, and management fees on Project DAMA's platform. Fund managers can manage their active and passive funds on the platform, such as rebalancing their portfolios composed of digital and tokenised assets.

Investors can access those funds through on-ramp solutions, fund subscriptions, and redemption services. On-ramp gateway solutions proved they can seamlessly convert fiat currencies, such as the United States Dollar (USD), to digitally native assets, like stablecoins in USD, for on-chain usage. Investors can use these digitally native assets to subscribe to funds. When investors redeem these funds, digital proceeds can be deposited into their whitelisted wallet. Regulations permitting, investors can also sell digital fund tokens in the secondary market to gain more access to liquidity.

Rationale for Adopting DLT

Project DAMA 1 PoC saw programmability, automation, and traceability as the primary drivers of benefits in utilising a DLT-based network. The PoC also tested mass customisation feasibility. Using Ethereum's infrastructure, transfer agents could easily grant and enforce investors' access to digital funds via SBTs. This programmed access can reduce the manual processes needed for repeated KYC processes and would facilitate compliance with the corresponding laws. With information represented on-chain, transfer agents and asset managers have greater control and governance in distribution.

Automation on DLT networks allowed Project DAMA 1 PoC to collapse certain post-trade processes into a single smart contract, reducing the workflow needed for funds and asset servicing.

The Ethereum network allowed investors to leave clear audit trails of their transactions, allowing fund and on-chain custody service providers to easily reflect the information on their internal databases. On the fund administration front, on-chain expenses are transparent to the public and are reliably recorded by smart contracts. This transparency supports the automation of information flow to facilitate net asset valuation calculations.

Project DAMA 1 PoC leveraged the Ethereum blockchain network to lower adoption barriers and allow accessibility for digital assets compatible with "Ethereum Virtual Machine". The bank cites that if the underlying DLT network is not easily adoptable by asset managers, distributors, investors, and service providers, it could lead to isolation and fragmentation.



Project DAMA 1 has the potential to be a one-stop digital fund investment servicing platform to reduce the effort for asset managers, transfer agents, fund administrators, and custodians to launch and service digital funds.



3.6 Synapse by HKEX, powered by Digital Asset, for Real-Time Settlement Status Updates

Mainland China's A-Share market requires T+0 settlement within a 4-hour window, introducing layers of complexity due to time zone differences for international buy-side participants.

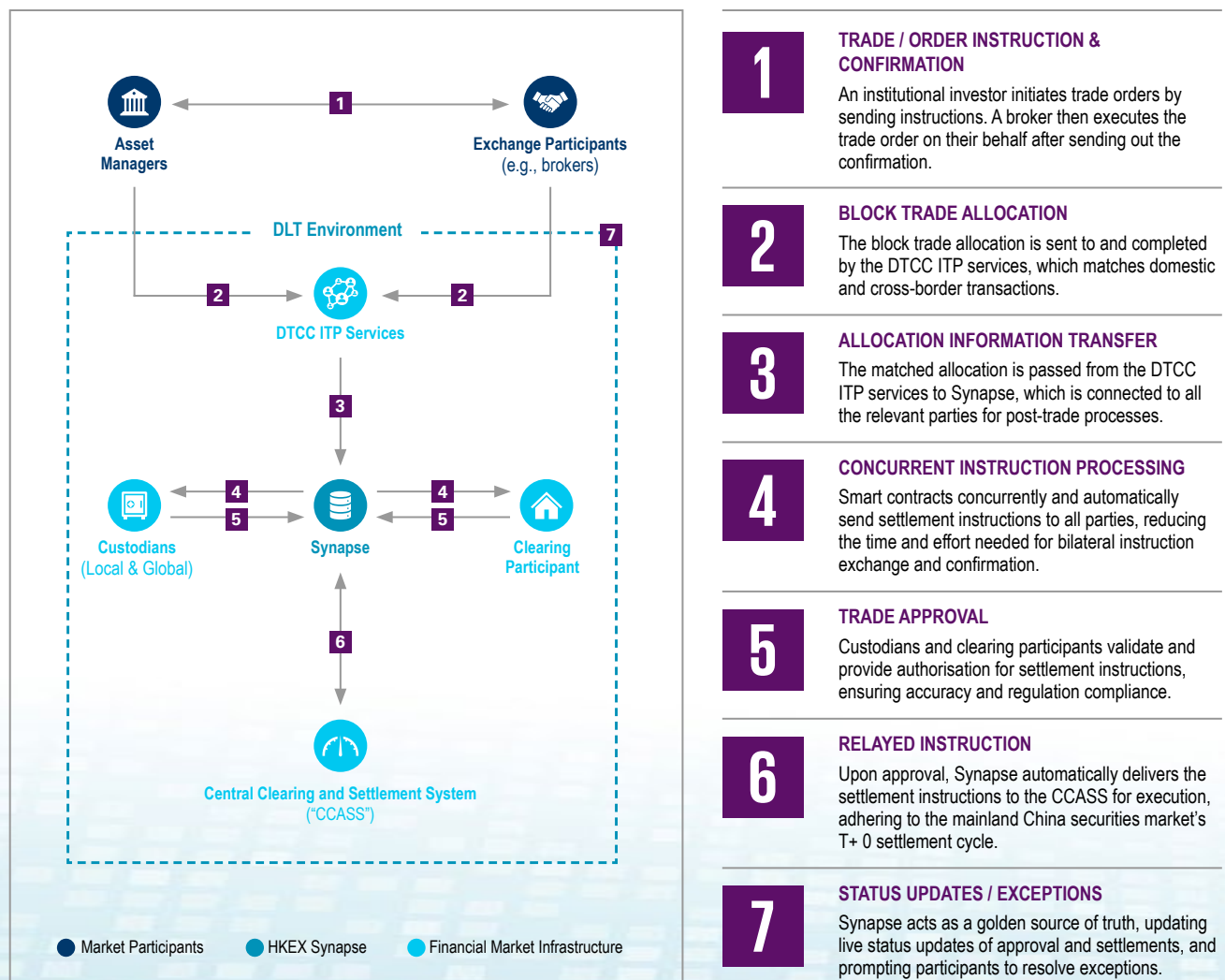
As traditional sequential workflows for settlement introduce delays and compress the available time for necessary adjustments, Hong Kong Exchange and Clearing Limited (HKEX) launched Synapse, powered by Digital Asset's smart contract language - Daml, to bring market and settlement participants together for seamless trade settlement for Northbound Stock Connect.

Solution Mechanism

Synapse acts as a central information hub for exchange participants (i.e., sell-side and buy-side financial institutions), clearing participants (i.e., local / global custodians and clearing participants), and financial market infrastructure (i.e., the Central Clearing and Settlement System (CCASS) and the Depository Trust & Clearing Corporation Institutional Trade Processing (DTCC ITP) Services for HKEX's Northbound Stock Connect (see Figure 15).

After receiving trade instructions – including block trade allocations – from exchange participants, the DTCC ITP processes the trades, which are matched with domestic and other cross-border trades via a Central Trade Matching mechanism.

Figure 15: Synapse by HKEX



After matching the trades, the DTCC ITP services transfer the matched allocation and participant information to Synapse, which is connected to all relevant stakeholders in the transaction. Daml Smart contracts power the operating workflow, updating all parties with the instructions and actions of others in real-time, transforming a previously sequential process into a simultaneous one. Overseas asset managers, in particular, can adjust to different time zones by sending specific conditional trade instructions to their global and local custodians, allowing their trades to be better allocated according to their detailed preferences.

The platform collates validations from each party and updates the information in real-time, giving market participants visibility on pending actions. After all parties authorise the transaction, Synapse communicates the settlement instructions to CCASS, completing the intraday settlement process.

For asset managers, Synapse provides an unprecedented level of transparency and adaptability. Previously, asset managers were not directly involved in the settlement process, which prevented them from adjusting their market orders. By being connected to – and having a real-time view of – the entire settlement process, asset managers can directly mitigate or identify issues.

Global and local custodians also receive similar benefits. Being connected to a real-time information flow allows custodians to act, adjust, and settle when needed, rather than reactively waiting for information within a reduced and intense timeframe. As trades unfold, custodians can view and interact with settlement information before and as it happens.

This increased connectivity and transparency brings greater settlement efficiency to other exchange and clearing participants. Moving away from a sequential workflow allows all participants to start their processes independently, rather than waiting for other parties. Combined with greater transparency, each party can immediately identify errors and adjust trade settlement conditions without derailing prior progress.

Rationale for Adopting Daml

HKEX's adoption of Daml was a heavily evaluated process. Before launching Synapse as a commercialised product, HKEX created a prototype, collected feedback from its stakeholders, documented requirements for the product launch, drafted an RFP on the requirements, and then built the product.

HKEX sought to have Synapse connect traditional sell-side clients and new buy-side clients in a multi-party workflow. Smart contracts could power these dynamic and iterative processes and give transparency to all parties.

To complement these capabilities, HKEX needed to preserve the privacy of the relevant parties and ensure that each stakeholder could not inappropriately expose their data to other parties serviced by HKEX. The permissioned nature of Daml smart contracts allowed HKEX to succinctly limit data access of clearing and exchange parties.

In addition to this, HKEX needed to streamline compliance and preserve market rules due to the exchange's systemically important nature. With Daml and its underlying platform Canton, HKEX retains the ability to automatically comply with market rules while retaining a full and cryptographically signed audit trail.



Synapse is a unique program that enables global investors to more efficiently manage time zone constraints in Mainland China's A-shares market through Northbound Stock Connect by replacing traditional sequential settlements with simultaneous conditional approvals and incorporating buy-side and custodians into the process.



3.7 Digital Financing Application on J.P. Morgan's Kinexys Digital Assets Platform for Precise, Automated, and Controlled Repo Transactions

Kinexys by J.P. Morgan, the firm's blockchain business unit, offers solutions in key areas: (1) exchanging payments-related information (Kinexys Liink), (2) transferring money (Kinexys Digital Payments), (3) settling transactions that involve assets (Kinexys Digital Assets), and (4) incubating new applications using blockchain technology, developing use cases for digital identity, etc. (Kinexys Labs).

The Kinexys Digital Assets platform drives innovation through asset tokenisation. A notable application is Digital Financing, jointly developed with J.P. Morgan's Markets business on the Kinexys Digital Assets infrastructure. This solution enables secured borrowing and lending via repurchase agreements (repo) by facilitating the near-instantaneous settlement of tokenised assets and cash. Since its inception, the application has processed over USD 1.6 trillion in volume.

Solution Mechanism

By tokenising traditional fixed income collateral and utilising on-chain cash, Digital Financing enables repo transactions to be executed and settled via smart contracts. This unique integration of execution and settlement enables the enforcement of a pre-trade funding requirement and the implementation of precise settlement times. Repo sellers can obtain faster, more cost-effective intraday funding without

the need to tap into their balance sheets, while repo buyers can optimise capital deployment and reduce operational costs. Both counterparties can obtain greater control over the repo process by programming the exact settlement and maturity times (see Figure 16).

The legal and regulatory nature of transactions are comparable to traditional repos conducted under the remit of Master Repurchase Agreements or Global Master Repurchase Agreements. However, on account of using blockchain as an alternative recordkeeping system, repos on blockchain have a unique operational flow integrating execution and settlement.

The trade begins with collateral tokenisation. The seller transfers collateral to a designated securities account at a triparty agent. The platform subsequently uses a collateral token to record ownership over the securities on the Kinexys Digital Assets blockchain ledger. Separately, the buyer transfers funds held in a J.P. Morgan demand deposit account (DDA) to a J.P. Morgan blockchain-based deposit account.

The seller can then electronically propose a trade, comprised of the typical terms: buyer, seller, dollar value, collateral type, and interest rate. While traditional repo negotiations also include a settlement date and maturity date, Digital Financing provides for more flexible and precise settlement by allowing for settlement and maturity times to be agreed upon. At the agreed settlement and maturity times, the exchange of collateral and cash is settled on an atomic DvP basis. The repo seller can transfer the funds received into its DDA to be used to fulfil intraday liquidity needs.

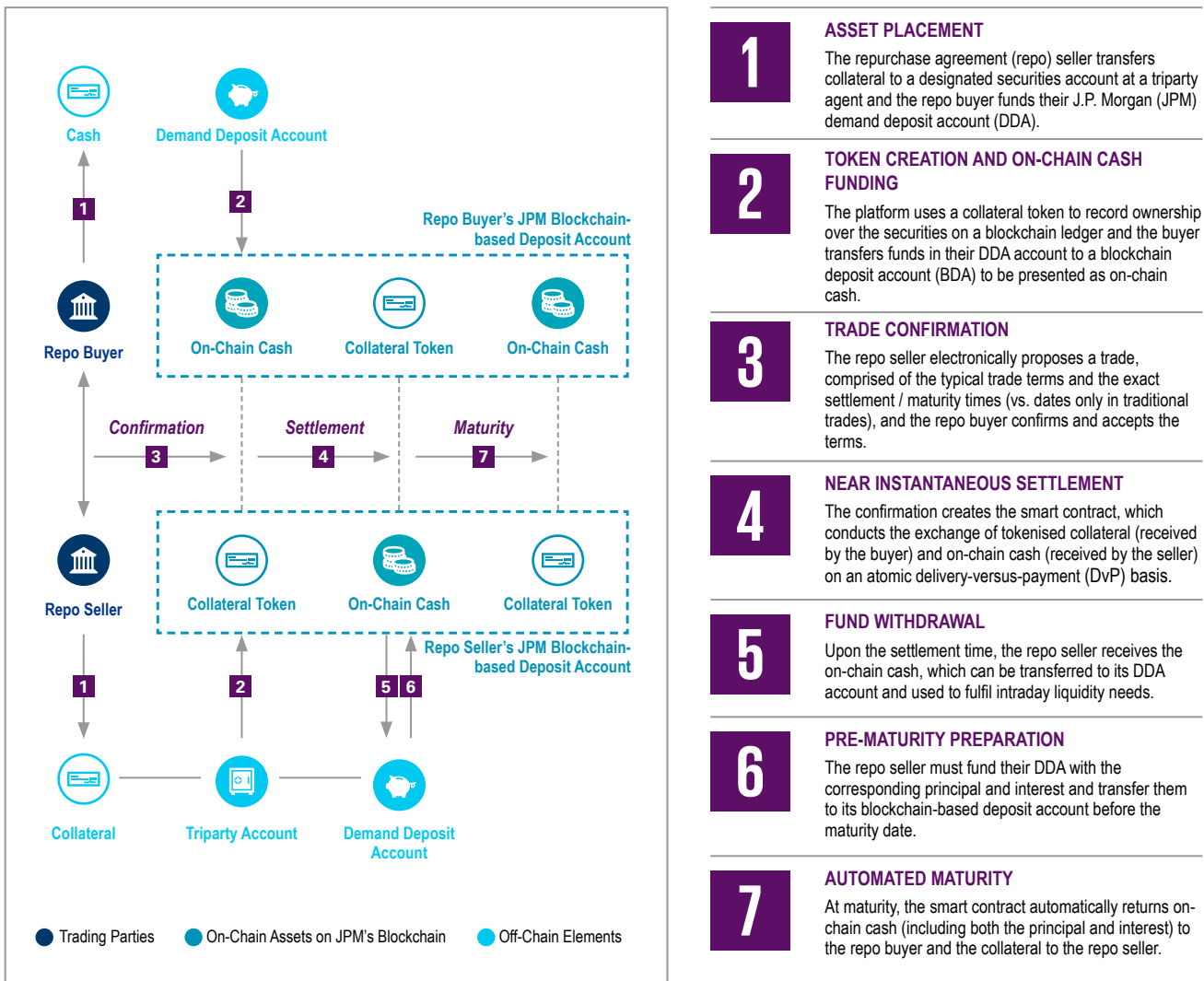
Before maturity, the repo seller must fund its DDA with the corresponding principal and interest. The DvP exchange at maturity can then be automatically completed.



Digital Financing provides secured financing against tokenised collateral on an intraday, overnight or term basis. Integrating the execution and settlement, it adds precision, automation, and control in repos.



Figure 16: Digital Financing Application on Kinexys Digital Assets



Source: J.P. Morgan, Interview findings, Quinlan & Associates analysis

Rationale for Adopting DLT

J.P. Morgan identified four benefits of adopting DLT: control, automation, precision, and transparency. The bank highlighted that programmability embedded at the asset level allows financial institutions to have stronger control over transaction activities, such as being able to set detailed conditions to a 'time-level' in repo transactions. Programmability also facilitates condition-based automated transactions, which removes unnecessary human intervention. Furthermore, assets traditionally recorded in separate ledgers are now being integrated into a single ledger, which enables atomic DvP settlement of different assets and automated maturity with a high degree of

precision. Finally, with transactions taking place on a single ledger, repo buyers and sellers have access to a consolidated and transparent record.

Kinexys Digital Assets is an Ethereum-based proprietary private-permissioned blockchain-based platform. This configuration retains the benefits of Ethereum, such as smart contract functionality, while allowing the bank to capitalise on the advantages of a private-permissioned platform, such as enhanced privacy and permissioning. Protecting information from any unauthorised access and maintaining accountability of the underlying platform operator responsible for facilitating financial transactions are the key reasons the bank chose this type of DLT network.

3.8 UBS Tokenize for Facilitation of Greater Issuers and Investors Accessibility

UBS operates a DLT-based tokenisation service called 'UBS Tokenize' that covers services ranging from the tokenisation, issuance, distribution, and custody of digital assets.¹⁰ UBS Tokenize has longstanding experience in issuing and distributing a wide range of products, including tokenised fix-rate notes, structured notes, bonds, and Variable Capital Company funds. UBS's tokenisation of a warrant in Hong Kong serves as one of the notable examples of natively issued warrants on a public blockchain.¹¹ The main benefits of DLT-based tokenisation on a public blockchain are easier access for issuers and investors, quicker, and more flexible issuances and increased automation across the lifecycle.

Solution Mechanism

UBS Tokenize is a service that enables the issuance, custody, and distribution of securities on public and private blockchains. UBS Tokenize combines

an innovative product framework and blockchain technology capabilities with its global capital market expertise to bring the benefits of DLT to the whole securities lifecycle.

Compared to traditional processes, which may take several days due to the engagement of multiple parties, such as a Central Securities Depository, UBS's security tokens are issued within minutes and enable more flexibility in terms of maturity and trade sizes. As a secondary benefit, assets can settle instantly, and the lifecycle can be fully automated by programming these into the smart contract. The service is built on an open architecture, allowing seamless and flexible connections across different participants.

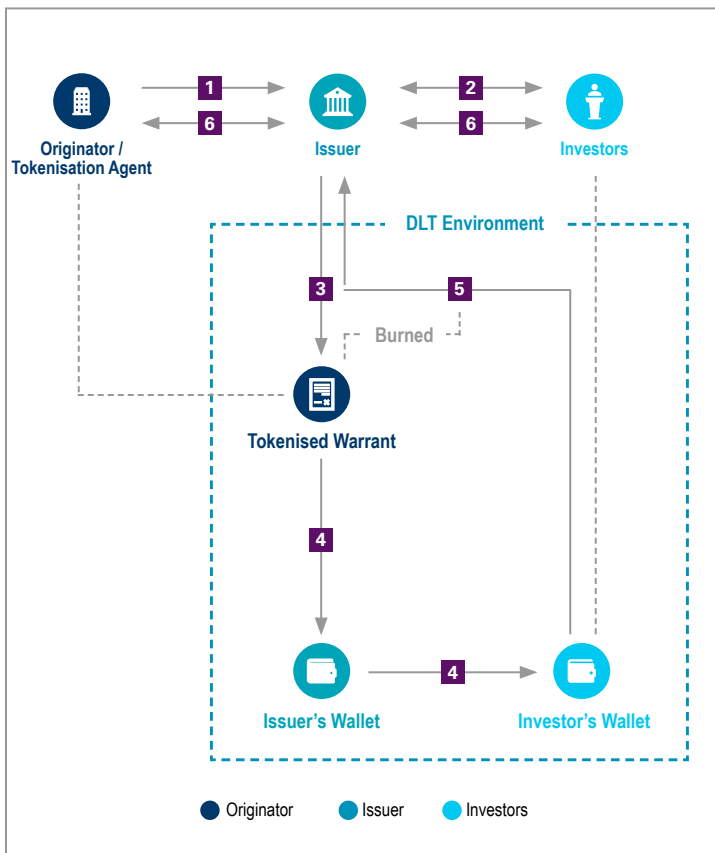
In the case of the warrant tokenisation, the originator first approaches the issuer (in this case UBS) regarding the issuance of the derivative instrument. The two parties discuss and specify the warrant details and finalise the product design. During the offering and sale, the issuer secures investors (in this case OSL Digital Securities) and receives capital to purchase the security. While the payment is executed through traditional payment mechanisms, settling the whole transaction on the DLT may lead to significant efficiency gains and flexibility (see Figure 17).



¹⁰ UBS. 2024. *UBS Tokenize*. (<https://www.ubs.com/global/en/investment-bank/tokenize.html>).

¹¹ UBS. 2024. *UBS expands its digital asset capabilities by launching Hong Kong's first-ever tokenized warrant on the Ethereum network*. (<https://www.ubs.com/global/en/media/display-page-ndp/en-20240207-tokenized-warrant.html>).

Figure 17: UBS Tokenize



Note: All historical transactions are kept visible to all participants
 Source: UBS, Interview findings, Quinlan & Associates analysis

The issuer then tokenises the warrant instrument through the UBS Tokenize service, registering the security natively on the Ethereum public blockchain through a dedicated smart contract. Using a shared common ledger between the issuer, distributor, and investor makes transactions faster and more flexible, reducing the number of parties involved. The newly minted warrant instrument token is then transferred to the investor's wallet. Upon the maturity date, the investor may exercise the option by contacting the issuer. Upon exercise verification, this token is expired and burnt to prevent duplicate usage. Meanwhile, the investor transfers the funds to the issuer to purchase the originator shares at the strike price, while the originator transfers the shares to the

issuer. The subsequent delivery of the funds and shares is completed via traditional DvP settlement rails.

UBS Tokenize allows greater accessibility for issuers to tap into new and more flexible funding pools and issuance. Investors have greater access to new issuers, smaller ticket sizes and more flexible product characteristics. Furthermore, the automation possibilities promise to automate many administrative processes via smart contracts, greatly increasing efficiency and offering new product structuring possibilities. The model is built on open-source standards ensuring smooth interoperability across all participants and the possibility for 24/7 instant settlement.



UBS Tokenize allows greater accessibility for issuers to tap into new and flexible funding pools.



Rationale for Adopting DLT

UBS embraced DLT for the tokenisation and issuance of securities due to its programmability, efficiency across market participants, and transparency features. The programmability of DLT networks enhances the speed and flexibility of security issuance, allowing issuers to bypass time and cost restrictions from long intermediary chains and issue securities of smaller denominations across a broader product range. A shared and programmable ledger across market participants promises to significantly improve timeliness and reduce reconciliation and integration efforts. Additionally, in the midterm, increasing scale and programmable features promise to significantly reduce transaction costs, automate the lifecycle management and enable new composable features for financial products and services.

The immutability and transparency of DLT networks bring a layer of risk management to UBS's security tokenisation. As all issuance and transaction records are immutably recorded, any transactions and issuance leave clear audit trails, preventing double-counting issues of tokens for the same underlying asset.

UBS's decision to use an Ethereum network for their UBS Tokenize solution is driven by the advantages of participating in an existing and thriving ecosystem of financial services, technology firms and a large developer community. This provides an existing ecosystem of market participants mitigating often-cited challenges with fragmented liquidity and interoperability. Furthermore, Ethereum has showcased longstanding reliability and security through its established infrastructure and diverse participations. Ethereum secures and transacts billions of USD daily and has millions of daily active addresses. Public blockchain-enhanced compatibility, open-source standards and wide connectivity among various market participants support UBS Tokenize's objective of facilitating easy access to its products. However, public blockchains are still emerging technology, especially for regulated financial services, and must be closely monitored for "fit-for-purpose" per use case regarding emerging technology risks and scalability.

Tokenisation can already deliver tangible benefits under existing legal frameworks. UBS has been exploring DLT for capital markets and has developed a risk framework to manage new technology risks while enabling key benefits. To realise key benefits of tokenisation, the industry needs to agree on appropriate standards.

3.9 Cross-Border Claims Settlement Solution by Allianz for Streamlined Cross-Country Motor Claims

The European Union (EU), consisting of 27 member states, features the Schengen Area, which allows for free travel among its countries. An important document for travellers is the Green Card, which serves as an international insurance certificate that verifies a motor vehicle is covered for compulsory motor third-party liability in the country being visited. Within the Green Card Free Circulation Area, which encompasses all EU countries, drivers are not required to present a Green Card when travelling between member states. While these measures enhance convenience for travellers, they pose challenges for insurers in settling cross-border motor claims. To address these challenges, Allianz has developed a blockchain platform for its operating entities in 23 countries.

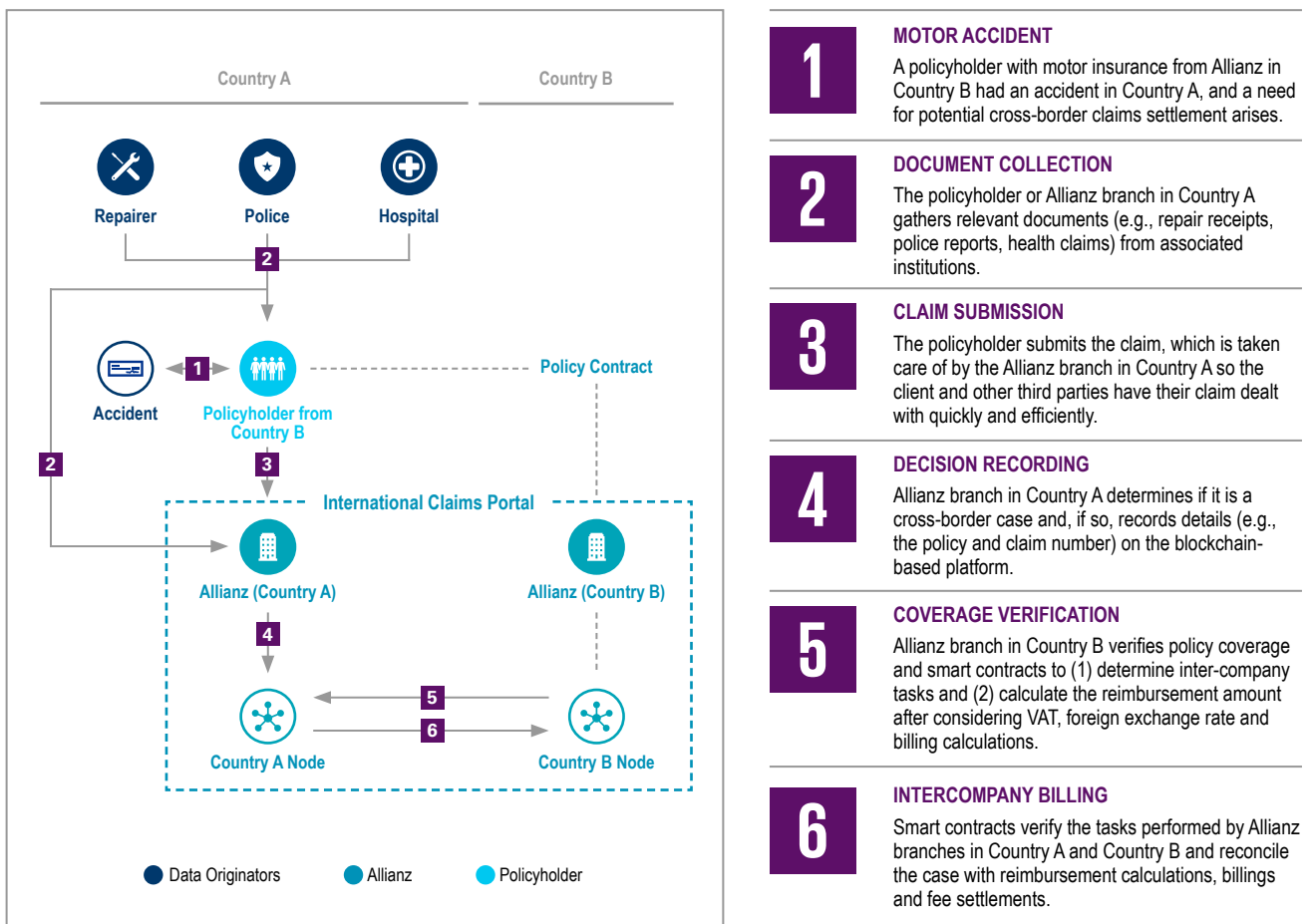
Solution Mechanism

Allianz's innovative solution streamlines the claims settlement process, facilitating efficient management of insurance claims for policyholders involved in accidents abroad. The process begins when a policyholder from Country B, insured through Allianz's branch there, experiences an accident in Country A. The policyholder can either gather the necessary documents from the auto repair shop, police, and healthcare providers or have Allianz's branch in Country A collect them. Once the required documentation is gathered, the policyholder submits a claim for the accident.

Allianz's branch in Country A takes charge of managing the case, ensuring an efficient claims and complaints settlement process for the policyholder and any third parties involved. Once the Allianz branch in Country A processes the claim, it conducts an internal settlement review. If the case requires cross-border settlement, the branch logs relevant transaction data – such as the policy number, local

claim number, involved countries, involved parties, and other claim details – onto the International Claims Portal that operates on Allianz's blockchain (see Figure 18). Most importantly, this process does not include any personally identifiable information, instead, personal data is securely stored in local country relational databases.

Figure 18: Cross-Border Claims Settlement Solution by Allianz



Source: Allianz, Interview findings, Quinlan & Associates analysis

Each country's branch is represented as a node on the blockchain, with smart contracts overseeing end-to-end cross-border business processes with full audit, validation, verification, and reconciliation built-in. This setup guarantees that transaction data is recorded on the blockchain, establishing an immutable source of truth.

One significant challenge addressed by this solution is the currency exchange rate used in calculations. While most EU countries use the Euro, some jurisdictions adopt their own currencies. In the

past, smaller branches relied on online exchange rate data for their calculations, which often led to inconsistencies as different branches may see different exchange rates. To mitigate these issues, the solution centralises the exchange rate by embedding it directly within the smart contracts used for calculations, using authoritative exchange rate data purchased by the larger branches that possess the financial resources to acquire such data. Additionally, it standardises the calculation basis date across all branches, reducing ambiguity in the handling process.



The solution streamlines the end-to-end European cross-country motor claim business while improving the governance in a frictionless way.



Aside from information recording and sharing, smart contracts also verify the tasks performed by each country branch and reconcile the case with reimbursement calculations, billing, and fee settlements. Allianz's branches in Country A and Country B manage their own profit and loss. When the branch in Country A collects documents and performs checks on various items such as policy validity and coverage, the branch in Country B must validate the information provided by Country A and pay a handling fee. By leveraging this solution, all tasks are bundled in a service level agreement, ensuring that teams in both Country A and Country B complete their responsibilities within specified timeframes. The handling fee is also encoded into the smart contracts, streamlining the settlement process.

Rationale for Adopting DLT

Allianz's solution connects 25 organisational silos through a streamlined communication process.

For the international handling team, each entity previously relied on its own methods of communication, such as isolated emails and phone calls, which demanded considerable manual effort. However, the programmability of DLT helps automate much of this process, significantly reducing costs and time spent during the settlement process while enhancing the overall policyholder experience and the liquidity of the Allianz operating entity. Between

the initial launch in 2021 and 2024, hundreds of Allianz employees facilitated approximately 5.7 million transactions, successfully managing all EU Green Card claims for Allianz operating entities onboarded to the solution. This solution also bolstered fraud prevention efforts by enhancing transparency in records and communications, a crucial development since detecting fraud in international claims is far more challenging than in domestic cases.

For the group-level debt management team, settling inter-entity debts to zero has historically been a challenge due to the limited visibility created by information silos. The increased transparency in handling processes and calculation of inter-entities bills now equips the group with stronger oversight, allowing for more accurate financial settlement.

With this unified solution, Allianz Group can also adapt more easily to regulatory requirements. The EU has introduced several new regulations in recent years, including the Digital Operational Resilience Act and Network and Information Systems Directive 2. This solution enables Allianz to fulfil many aspects of the new regulations and effectively communicate its compliance to regulators.

Allianz chose to develop its solution on the Linux Foundation Hyperledger Fabric, a private-permissioned blockchain. From the initiative's inception in late 2018 to its official launch in 2021,



the industry lacked sufficient regulatory clarity and technological maturity, particularly regarding the use of public blockchains. As such, many industry players were hesitant to adopt public blockchains. Since the solution's value proposition could be achieved without relying on a public blockchain, a private blockchain was a logical choice. At that time, Hyperledger Fabric was the most commonly used blockchain among banks and insurers. Allianz opted for Hyperledger Fabric to ensure that its solution could achieve seamless interoperability across various systems.

3.10 MIDAS by HKFI, in partnership with CryptoBLK, for Reliable and Real-Time Motor Insurance Authentication

A large-scale motor insurance fraud case shocked Hong Kong in 2016, involving over 1,000 forged motor cover notes that victimised more than 700 people, which triggered significant alarm among all

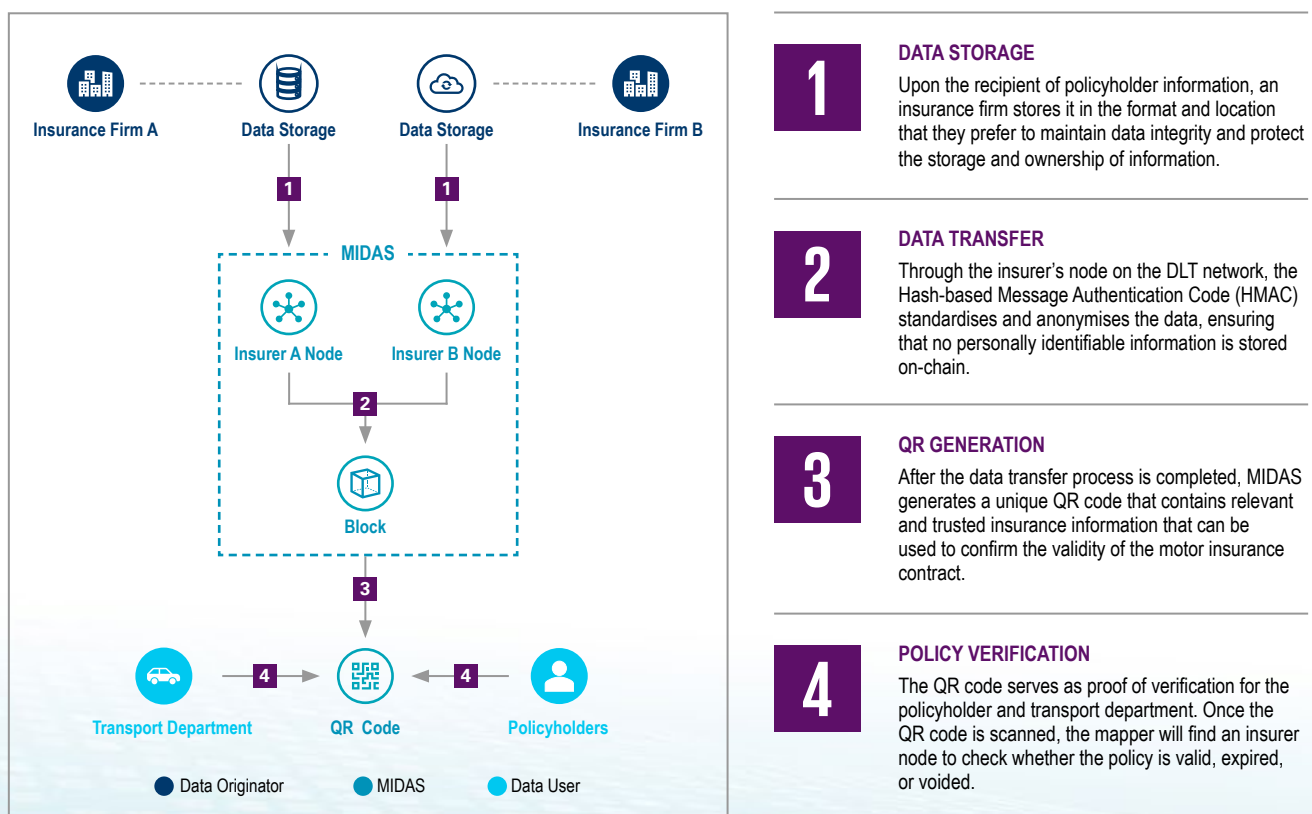
parties concerned. After rounds of discussions with the Transport Department, the IA, and the Hong Kong Police Force, the Hong Kong Federation of Insurers (HKFI) decided to deploy blockchain to address this problem. In 2018, the HKFI partnered with CryptoBLK to introduce the Motor Insurance DLT-based Authentication System (MIDAS), a reliable and real-time insurance validation platform.

Solution Mechanism

Upon receiving policyholder information, an insurance firm stores it in the format and location they prefer, in the cloud or on-premises. This guarantees data integrity, as the storage and ownership of information are strictly at the insurer's discretion.

Through the insurer's node in the DLT network, CryptoBLK offers a middle layer to convert the data into a standardised format. The Hash-based Message Authentication Code (HMAC) anonymises the data and stores the hash in the distributed ledger. This ensures that personally identifiable information remains secure under the insurer's watch (see Figure 19).

Figure 19: MIDAS by HKFI and CryptoBLK



Source: HKFI, CryptoBLK, Interview findings, Quinlan & Associates analysis

Once the anonymised data is recorded on the blockchain, MIDAS generates a unique QR code that contains relevant and trusted insurance information. Data users, including policyholders and relevant government bodies, can use the QR code as proof of verification to confirm the validity of the motor insurance contract. Once the QR code is scanned, the mapper will find an insurer node to check whether the policy is valid, expired, or voided.

With MIDAS, insurance firms face less reputational risk while maintaining data integrity, supported by flexible data storage methods at their discretion. Car owners benefit from the assurance of having legitimate coverage, as well as a fully digitalised experience without the need to visit and line up at the Transportation Department. Government bodies can verify the authenticity of motor insurance policies in real-time to curb any forged policies, allowing for more citizen-friendly services and efficient enforcement. MIDAS is an example of promoting the city as an insurance and technology hub, providing policyholders with proper insurance coverage and reducing fraud incidents.

MIDAS has advanced to Phase 2, which integrates the MIDAS platform with insurers' systems via API. Following the enforcement of the Motor Vehicles Insurance (Third Party Risks) (Amendment) Regulation 2024 on 30 December 2024, MIDAS has

officially been integrated into the e-Licensing Portal by the Transport Department. Verification of third-party insurance records will be seamlessly handled through MIDAS for online vehicle licence applications, streamlining administrative processes and saving hassle for Hong Kong residents.

Rationale for Adopting DLT

MIDAS adopted DLT for its motor insurance authentication because it provides an immutable record of the relevant documents and contracts. For its solution, each new entry in the ledger includes an HMAC, a cryptographic process that acts as a digital seal linking the current entry to its predecessor. This mechanism allows tampering attempts immediately noticeable and creates a clear audit trail to ensure the data remains accurate and trustworthy.

MIDAS is built on the Kentro Network, a public-permissioned DLT operated by CryptoBLK. Through the permissioned DLT characteristics of the Kentro Network, MIDAS has control over the prospective node participants (e.g., insurance companies) to meet the necessary due diligence requirements given the sensitive information being handled on the platform. However, since the solution needs to be accessible to a broader audience, such as the Transport Department and the policyholders, it also requires public DLT characteristics so that the information stored on DLT is easily accessible.



MIDAS is the first industry-wide DLT application in Asia for insurance that allows parties to authenticate motor insurance without disclosing personal information.



4. Practical Guidance for DLT Adoption

The previous section highlighted ten notable cases of DLT adoption across the banking, securities, and insurance sectors worldwide, showcasing applications ranging from digital identity to international claims settlement. These notable examples represent only a fraction of the global exploration and implementation of DLT, as financial institutions recognise its potential and are already making steady progress by experimenting and refining their approaches to integrate the technology into their operations.

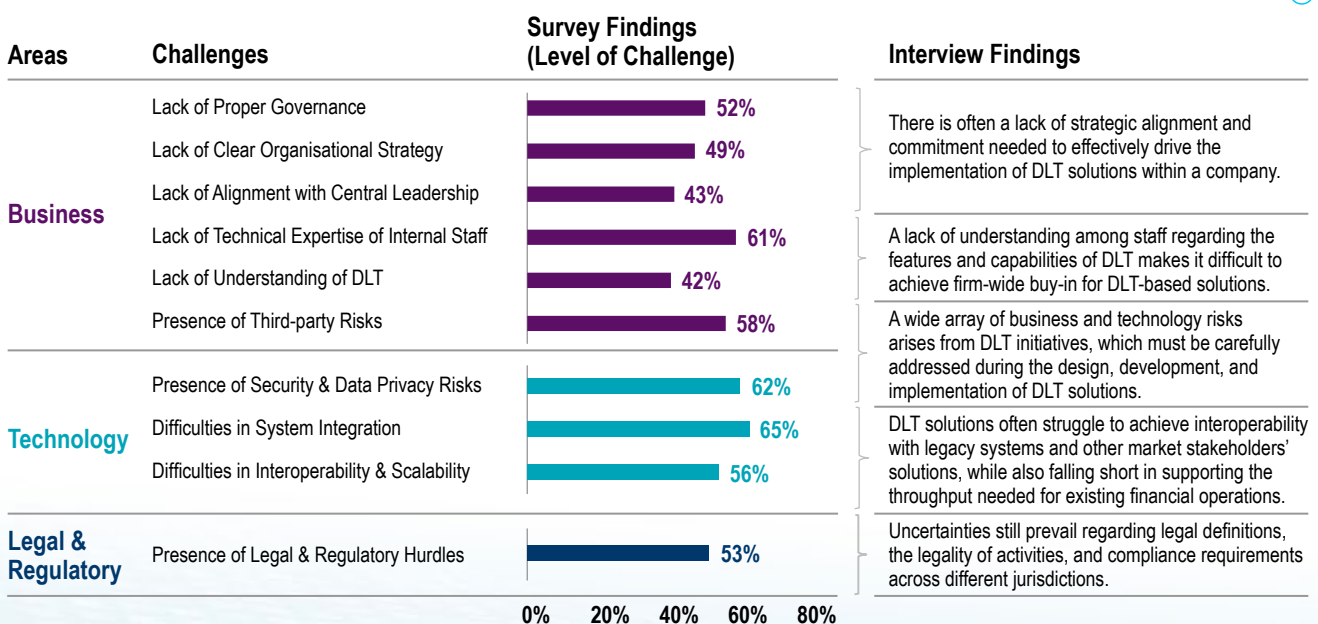
The DLT space is characterised by rapid technological advancements and evolving regulatory frameworks, which present a range of uncertainties, risks, and challenges for adoption. Building on the foundation of

the HKMA's recent circular, titled *“Risk Management Considerations Related to the Use of Distributed Ledger Technology”* (hereinafter “previous HKMA circular”),¹² this section highlights key adoption challenges identified through surveys and interviews and provides practical guidance for financial institutions to consider as they continue their ongoing DLT adoption efforts.

4.1 Adoption Challenges

Based on our interview and survey findings, we have identified several key adoption challenges related to DLT initiatives across business, technology, as well as legal and regulatory perspectives (see Figure 20).

Figure 20: Adoption Challenges



Note: The survey findings indicate the proportion of respondents who identified the corresponding issues as moderate-to-major challenges

Source: HKMA Fintech Adoption Study (2023), Interview findings, Quinlan & Associates analysis

¹² Hong Kong Monetary Authority. 2024. *Risk Management Considerations Related to the Use of Distributed Ledger Technology*. (<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2024/20240416e1.pdf>).

Business Challenges

Despite the widely acknowledged potential of DLT to transform financial operations, many financial institutions face a lack of organisational and operational readiness for its adoption. Approximately half of the survey respondents identified the lack of proper governance, clear organisational strategy, and alignment with the central leadership team as key barriers to adoption. These challenges create broader issues of strategic and operational misalignment, which can lead to delays or failures in adoption efforts. One of the interview participants shared that leadership backing often determines the pace and scale of adoption within large institutions and, without such support, DLT initiatives may face resistance or stall during the rollout phase.

A significant challenge also lies in the expertise gap among middle- and execution-level employees. According to 61% of survey respondents, this gap is most pronounced in technical expertise, while 42% cited a general lack of understanding of DLT. A global bank noted that this knowledge gap extends beyond internal teams to external clients, many of whom remain unaware of the full capabilities and potential of DLT. Many interview participants echoed the concern that this knowledge gap could prevent institutions from fully realising the value of their DLT investments.

Furthermore, the involvement of third parties (e.g., technology vendors) poses an operational challenge for financial institutions. This challenge, shared by 58% of survey respondents and multiple interview participants, reflects the complexities associated with maintaining oversight and control over third-party engagements, whether it be for infrastructure, technical support, or network validation. Institutions not only face concerns about the security associated with these engagements but also about the consistency and quality of the support provided over time, raising the importance of having adequate risk management measures and service-level guarantees to safeguard the DLT solution's trustworthiness and continuity over the long term.

Technology Challenges

Financial institutions encounter various DLT-specific technological challenges, including concerns around unauthorised access, integration, scalability, and interoperability. These challenges can heighten

security risks and limit operational efficiencies, presenting barriers to adoption at both the organisational and industry-wide levels.

Although DLT networks are designed to be tamper-proof, malicious actors can still gain unauthorised access and introduce unwanted transactions to the ledger, a concern raised by 62% of survey respondents. Several interview participants also highlighted the challenges in maintaining control over confidential information on public, permissionless networks. With these concerns in mind, many emphasised the need for stronger security measures and governance protocols. Without these measures in place, the risk of data leakage increases, which could have financial and reputational implications.

Beyond security vulnerabilities, the integration of DLT solutions with existing infrastructures stands out as one of the most widespread challenges among financial institutions. According to 65% of survey respondents, a primary obstacle lies in aligning disparate systems and technology stacks that were not originally designed to interface with DLT networks. Traditional, centralised architecture typically relies on fixed protocols and data structures, limiting their compatibility with DLT solutions. As a result, integration is a complex and resource-intensive task, with two interview participants emphasising the need for customisations and dedicated resources to ensure seamless communication between DLT solutions and their existing systems.

Challenges related to interoperability and scalability of DLT solutions continue to be pressing issues for 56% of survey respondents. Interoperability remains a critical challenge, particularly for global banks managing cross-border operations. One global institution we interviewed, for instance, faced notable frictions in aligning data standards and protocols across jurisdictions when managing global corporate accounts. Without seamless interoperability, DLT systems risk operating in isolation, limiting their ability to communicate across platforms and restricting their potential to support a broad range of use cases. With regards to scalability, a major bank we spoke to highlighted that the current throughput might not be sufficient to support the full rollout of its solution across the entire ecosystem. This raises important questions about the technology's ability to handle increasing transaction volumes as adoption grows, particularly in scenarios where speed and efficiency are crucial.

Legal & Regulatory Challenges

Regulatory uncertainty emerges as a key barrier to DLT adoption, with 53% of survey respondents highlighting it as a major challenge – a view shared by most financial institutions during our interviews. Without a clear regulatory environment, institutions face difficulties in navigating the complexities of legal definitions, enforceability, and compliance requirements, all of which are crucial for the successful integration of DLT into financial operations.

As the technology is still in its nascent stages, there are no universally accepted legal definitions for various digital assets, and the legality of activities and transactions within DLT environments remains ambiguous. For example, a global bank is actively seeking regulatory clarity on the legality of tokenised deposits and transaction settlements conducted on-chain, highlighting the need for formal legal recognition of these practices. Similarly, another banking institution has called for guidance on the use of smart contracts, particularly regarding their enforceability and the legal scope of these agreements, which remain unclear in some jurisdictions.

With the growing demand for DLT adoption, the need for legally binding standards has become more pressing. One interview participant has advocated for compliance requirements tailored to financial institutions. Two banking institutions further echoed

this sentiment, specifically seeking clarity on AML / CTF requirements, as well as on-chain and cross-border identity credentials. Meanwhile, one bank expressed the importance of having clear guidance on preferred DLT network types to better navigate the diverse market solutions available. Without such frameworks, institutions find themselves navigating uncertainties, hindering their ability to adopt DLT solutions with confidence.

For institutions with regional and global operations, the challenge extends beyond local regulatory clarity to the need for cross-jurisdictional regulatory harmonisation. Discrepancies in regulatory approaches across borders complicate the implementation of DLT solutions at scale, particularly in applications such as international payments and claims settlements. This fragmentation risks limiting DLT’s potential for widespread, global adoption.

4.2 Practical Guidance

Recognising the challenges faced by industry participants, this paper outlines a set of practical guidance in the form of guiding principles (see Figure 21). Each principle is informed by insights gathered from our survey findings and in-depth interviews, ensuring they are grounded in the realities faced by industry participants. These principles serve as a framework for financial institutions to facilitate smoother implementation, mitigate risks, and ultimately foster a more conducive environment for DLT adoption.

Figure 21: Practical Guidance

Areas	Challenges	Interview Findings	Practical Guidance
Business	Lack of Proper Governance	There is often a lack of strategic alignment and commitment needed to effectively drive the implementation of DLT solutions within a company.	<ol style="list-style-type: none"> 1. Develop a firm-wide DLT strategy 2. Centralise efforts with a dedicated DLT team
	Lack of Clear Organisational Strategy		
	Lack of Alignment with Central Leadership		
	Lack of Technical Expertise of Internal Staff	A lack of understanding among staff regarding the features and capabilities of DLT makes it difficult to achieve firm-wide buy-in for DLT-based solutions.	<ol style="list-style-type: none"> 3. Deliver fit-for-purpose DLT training programmes for solution activation
	Lack of Understanding of DLT	A wide array of business and technology risks arises from DLT initiatives, which must be carefully addressed during the design, development, and implementation of DLT solutions.	<ol style="list-style-type: none"> 4. Develop mitigation plans for identified risks and challenges
Presence of Third-party Risks			
Technology	Presence of Security & Data Privacy Risks	DLT solutions often struggle to achieve interoperability with legacy systems and other market stakeholders’ solutions, while also falling short in supporting the throughput needed for existing financial operations.	
	Difficulties in System Integration		
Legal & Regulatory	Difficulties in Interoperability & Scalability	Uncertainties still prevail regarding legal definitions, the legality of activities, and compliance requirements across different jurisdictions.	<ol style="list-style-type: none"> 5. Continue with adoption efforts under the existing regulatory principles 6. Proactively communicate needs and collectively develop regulations
	Presence of Legal & Regulatory Hurdles		

Source: HKMA Fintech Adoption Study (2023), Interview findings, Quinlan & Associates analysis

4.2.1 Develop a Firm-Wide DLT Strategy

Regardless of the technology being utilised, financial institutions understand that genuine innovation faces many challenges, which stem from deficient structured innovation processes, a weak innovation culture, and broader financial constraints. Market leaders typically address these challenges by setting up and empowering centralised innovation teams; however, the advent of new technology pillars like DLT necessitates a more nuanced approach.

The premise of a successful DLT adoption lies in a well-defined strategy. However, many institutions face challenges where innovation initiatives are mandated from the top without being integrated into the organic part of everyday business culture. This often leads to board mandates that are ambiguous and lack actionable direction. When these mandates fail to generate commercial friction, boards typically pull the plug.

To develop an effective DLT strategy, the board must collaborate with business units to clearly define specific business problems that DLT can address. Rather than merely seeking generic solutions to broad internal issues identified by senior management, business units should identify clear DLT value propositions that enhance services, improve efficiency, or create competitive advantages.

Achieving this proposition requires a thorough understanding of the current operational landscape, gained through comprehensive analyses of both the institution and the broader market. This understanding is crucial to avoid unrealistic digital innovation aspirations and to setting fit-for-purpose objectives.

Simultaneously, the board and senior management are expected to establish sufficient systems and controls to address risks specific to DLT, particularly those concerning governance. As noted in the previous HKMA circular, organisations should assess and revise their relevant policies and frameworks to reflect the DLT-specific factors as needed. This review should encompass factors such as technology risk (including change management, access control, and network security), business continuity planning, and outsourcing. Where a DLT solution has customer

facing elements, attention should also be paid to the need for additional safeguards and arrangements related to consumer education and dispute handling or redress, amongst others. Such mechanisms can be complemented by a compensation framework to address instances of user loss, demonstrating financial institutions' accountability for errors.

Once the ambitions and risk management controls are clearly defined, business units can assess the potential of DLT solutions and shortlist solutions that are feasible within the available resources and capabilities. To ensure the framework remains effective over time, banks should adopt a dynamic approach to risk management, regularly reviewing and refining their controls to address emerging risks and changing circumstances. This iterative process helps maintain alignment with regulatory expectations and the institution's evolving risk appetite. Once the plans are developed, they should be presented to the board for approval, accompanied by robust business cases supplemented by preliminary budgets and key milestones. This approach directly addresses key concerns of limited leadership commitment, as raised by survey respondents, enhancing alignment and prioritisation across financial institutions.

In building these DLT business cases, business units should carry out adoption strategies to move the financial institution's top and bottom lines and incorporate tracking metrics to track the solutions' deployment effectiveness, areas for improvement, and benchmarks for success. These indicators should also be tailored to a financial institution's profitability, so business units can readily demonstrate the impact of their DLT solutions to the board.

Financial institutions will typically need to track a wide range of metrics to measure the benefits of their DLT solution(s). Metrics related to a solution's effectiveness generally include improvements in task completion times, employee productivity, and cost savings, all of which evaluate its impact on operational efficiency. Additional metrics, such as time spent using the solution, support requests, and user satisfaction surveys, can reveal underlying issues and areas for improvement. Finally, institutions must consider all impacted revenue streams and cost factors when measuring the financial impact and success of their DLT solutions. For example, in addition to direct costs, it is essential to account for ancillary expenses, such as training programmes,

to accurately calculate a solution's return on investments. This comprehensive approach ensures an accurate picture of profitability and helps prevent unexpected expenses that may derail management support.

4.2.2 Centralise Efforts with a Dedicated DLT Team

Financial institutions may consider establishing a dedicated DLT team to steer and oversee the implementation of the firm-wide strategy, a practice suggested by nearly half of the interview participants. This aligns with the previous HKMA circular's suggestion that an AI should ensure that it has sufficient staff with expertise in DLT to support the implementation of DLT solutions. One model to consider is a centralised team, such as a Centre of Excellence or a hub-and-spoke model, where the central team coordinates efforts across various departments.

A centralised DLT team is often more effective than a decentralised one because it consolidates expertise, streamlines decision-making, and ensures consistency in strategy implementation. To be effective, the team should be staffed with a mix of technology experts and business professionals. Technology experts within the central team can concentrate knowledge, keep pace with industry advancements, and manage training programmes, which is particularly important since DLT is a new concept for many employees. Meanwhile, business professionals with deep industry knowledge would help align DLT initiatives with core business objectives, ensuring that resource allocation is optimised for return on investment. Aside from that, business professionals can manage the change process, minimising disruptions and ensuring that the institution can smoothly integrate DLT solutions with its existing processes.

By centralising DLT efforts within this team, financial institutions can also reduce redundancies and inefficiencies that often arise when different departments handle similar initiatives independently. This centralisation promotes more efficient use of resources, including budget allocation, personnel, and risk management.

Last but not least, a member of the organisation's senior management team should ideally serve as the executive-level sponsor for the DLT team. This leadership role helps secure organisation-wide buy-in, elevate DLT initiatives to a strategic priority, and ensure that the team receives the necessary support and resources for long-term success.

4.2.3 Deliver Fit-for-Purpose DLT Training Programmes for Solution Activation

The deployment of DLT solutions without effective activation efforts among end users, whether internal staff or external clients, can severely undermine their potential. While subject matter experts often possess deep technical expertise, many industry practitioners lack a foundational understanding of DLT concepts.

Without adequate knowledge, employees may struggle to leverage DLT solutions effectively or resist adoption due to perceived complexity or lack of relevance. Similarly, external clients of a financial institution may experience friction when using DLT-enabled solutions if they do not fully grasp the solution's value proposition or operational mechanism.

To address this, financial institutions should provide fit-for-purpose training programmes, either through internal corporate trainers or in partnership with vendors, to equip end users with a well-rounded understanding of DLT solutions and their applications.

Effective training programmes must be tailored to the unique needs and requirements of the intended end users, following a structured process to ensure the successful activation of DLT solutions (see Figure 22). This process involves assessing the current state of DLT adoption, setting clear objectives, designing and delivering targeted training programmes, and continuously evaluating programme outcomes for future optimisation. At each stage, institutions should look to address critical questions, such as how to define their training objectives and which methods are best suited for tracking metrics associated with the effectiveness of the training programme.

Figure 22: Suggested Approach

	SET	ASSESS	TAILOR	DELIVER	EVALUATE & OPTIMISE
<i>Description</i>	Understand the adoption status quo and define an overarching goal for using DLT solutions	Evaluate capability gaps, training needs, and available internal and external resources	Develop training programme(s) that aligns with end users' needs based on the gaps identified	Implement the training session to the end users to encourage the intended usage of DLT solutions	Track metrics and collect feedback for refinement of training programmes and activation approaches
<i>Key Questions to Address</i>	<p><i>What is the current adoption status of the DLT solution?</i></p> <p><i>What is the objective for designing and delivering the training programme(s)?</i></p>	<p><i>What are the required capabilities for the end users to fully capitalise on the DLT solution?</i></p> <p><i>What are the common challenges for usage and what kinds of support are end users looking for?</i></p>	<p><i>What are relevant contents and tools that the training programme should include?</i></p> <p><i>How can the institution collaborate with its vendors to develop and deliver the training programme?</i></p>	<p><i>What is the ideal design for each training module in terms of channels, coverage, frequency, and format?</i></p>	<p><i>What are the KPIs and the best approach for tracking the usage and adoption of DLT?</i></p> <p><i>What are the success thresholds for each module and what enhancements can be made to improve effectiveness?</i></p>

Source: Quinlan & Associates analysis

Training initiatives should begin with assessing the current state of adoption to establish a clear objective for how the programme will facilitate user uptake. The objective should be:

1. **Specific** – Clearly defining what needs to be achieved;
2. **Measurable** – Enabling quantifiable progress tracking;
3. **Actionable** – Ensuring feasibility with available resources;
4. **Relevant** – Aligning with end user adoption goals; and
5. **Timebound** – Setting a defined timeline for completion.

Once objectives are established, financial institutions should prioritise understanding the specific needs and challenges of end users, which are often overlooked or inadequately addressed. Failing to address these needs can hinder the wider adoption of DLT solutions.

To identify these needs, institutions can use tools such as focus groups, surveys, or support tickets to gain insights into the end users' needs and challenges related to DLT adoption. For example, such analysis may reveal gaps in end users' technical skills or a lack of motivation to use the DLT solution, stemming from limited awareness regarding its benefits. Identifying these gaps can enable institutions to tailor training programmes that effectively address adoption barriers and better align with end user needs.

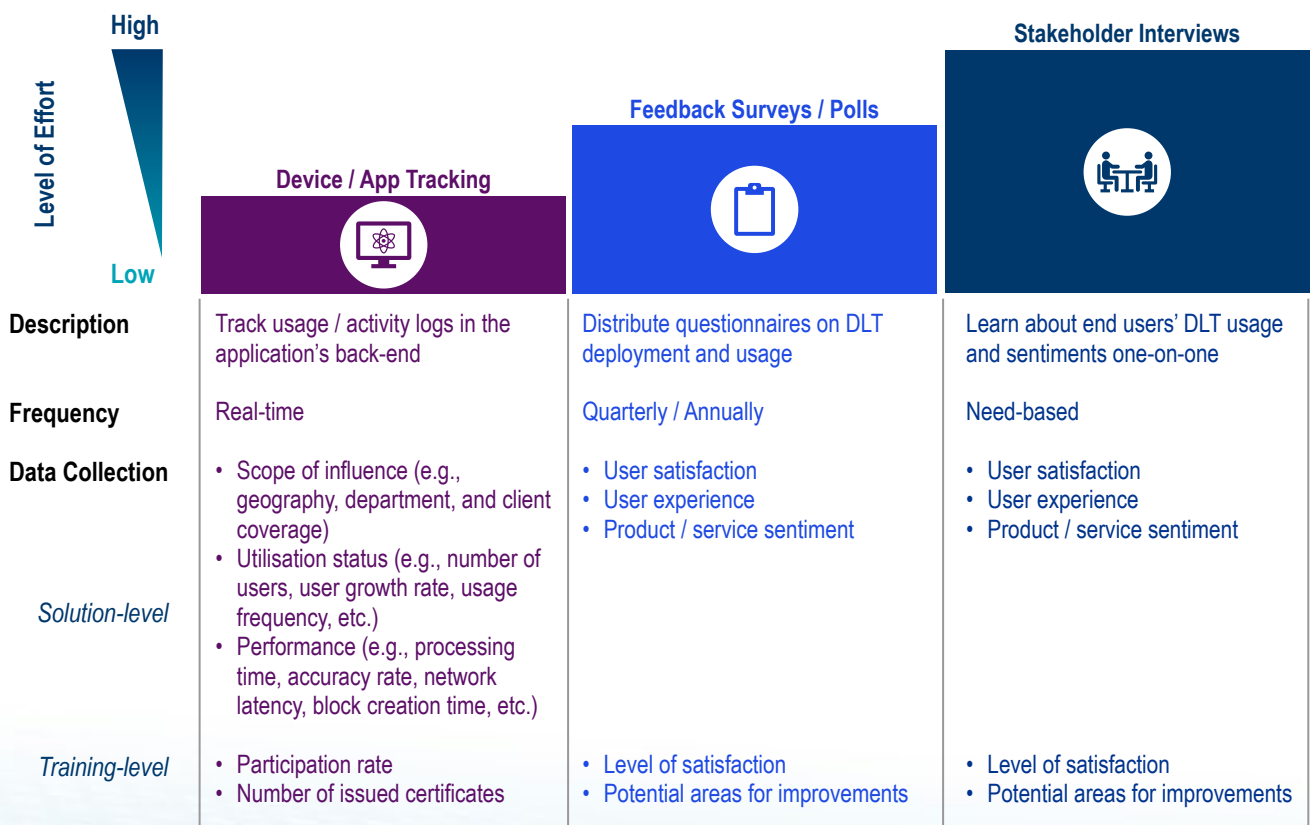
When designing training programmes, financial institutions may engage technology service providers to develop customised training sessions. Service providers bring specialised expertise and can offer innovative training methods, such as interactive simulations and e-learning modules, which can enhance learning outcomes. Aside from choosing the delivery owner or partner, financial institutions must carefully consider other key factors when designing fit-for-purpose training programmes, including (1) channels, (2) coverage, (3) format, and (4) frequency.

Training can be delivered through various channels. Online channels, such as webinars and e-learning modules, offer flexibility, scalability, and structured learning. Alternatively, offline workshops can provide more interactive, hands-on sessions that are difficult to replicate in a virtual setting. Financial institutions should choose delivery channels based on their training objectives and the target audience.

The training structure can vary from standalone modules to integrated series, depending on the target audience and whether the training is intended for individuals, teams, departments, or the organisation. The selected format and structure should inform the frequency of training, ensuring programmes remain relevant and impactful over time. For instance, regular refresher sessions can be held to keep pace with evolving technology and user needs. Above all, financial institutions should prioritise actionable guidance and practical tools that can be showcased during the training sessions that participants can apply in their daily workflows.

Once training programmes are implemented, financial institutions should look to continuously evaluate their effectiveness, including tracking their impacts on DLT solution adoption. This can be achieved by setting clear KPIs, collecting feedback, and incorporating insights to improve future training initiatives (see Figure 23).

Figure 23: Monitoring & Data Collection



Source: Quinlan & Associates analysis

For example, institutions can track DLT adoption rates through usage and activity logs within the application's back end, alongside monitoring participation rates in e-learning modules or other training programmes. To supplement the quantitative data, surveys, interviews, and focus groups can be conducted to provide deeper qualitative insights. These approaches can help financial institutions to better understand user experience, identify lingering challenges, and optimise training programmes to accommodate educational needs that continue to evolve alongside the latest developments in DLT.

4.2.4 Develop Mitigation Plans for Identified Risks and Challenges

DLT-specific technology challenges stem from the unique vulnerabilities inherent in its characteristics and the limitations it poses on commercial adoption. Given that these vulnerabilities are likely to persist, financial institutions must thoroughly understand these risks and challenges, identify them in their DLT initiatives, and develop a robust corresponding mitigation plan.

Effective mitigation plans should include comprehensive testing scenarios that take into account DLT-specific operating dynamics and include contingency arrangements as part of the institution's overall business continuity planning, as highlighted in the previous HKMA circular. When DLT is adopted for critical functions, testing scenarios should be tailored to identified risks, such as common DLT cyberattacks, loss/theft of private keys, and the possibility of forking. As part of developing the testing scenarios, institutions must remain cognisant of the unique operating dynamics of DLT networks, especially those that may affect system and capacity management, such as potential validation congestion and the possible need to pay higher fees to expedite urgent transactions. In addition to testing, financial institutions could set up contingency arrangements such as backup options to address instances where DLT solutions become temporary or permanently unavailable.

To address limitations for commercial adoption and develop corresponding mitigation strategies, financial institutions are encouraged to stay updated on new solutions introduced to the market that are designed to augment DLT's business and functional

requirements. As the choice of blockchain type has a direct influence on security, stability, and resilience, financial institutions should understand the nuances between each type to identify applicable risks and develop corresponding mitigation and business continuity plans when implementing their DLT solutions. Furthermore, financial institutions should carefully evaluate the legal and regulatory responsibilities that come with adopting DLT solutions.

Regardless of the blockchain type being considered (i.e., private-permissioned, public-permissioned, or permissionless networks), financial institutions should be aware of and address DLT-specific technology risks and challenges.

Based on insights gathered from interviews and surveys, the following are some of the more commonly cited risks and challenges associated with DLT adoption. While not exhaustive, these risks highlight key areas that financial institutions should consider when implementing DLT solutions.

1. Third-Party Risks

DLT initiatives driven by financial institutions often involve partnerships with external technology vendors, which can introduce business and operational risks. These risks arise from reliance on third parties for key components, such as platform development, network infrastructure, and ongoing technical support. To address these challenges, financial institutions should conduct a comprehensive risk assessment and implement robust frameworks for managing third-party risks.

Key measures should include a thorough evaluation of vendor reliability, security protocols, and regulatory compliance at every stage of the DLT adoption lifecycle. This encompasses initial network assessments, architectural design, pilot testing, and full-scale deployment, as well as ongoing operational maintenance. Furthermore, institutions should establish clear contractual agreements outlining performance expectations, data security obligations, and service-level guarantees. To mitigate potential disruptions, contingency arrangements, such as backup vendors, failover mechanisms, and incident response plans, should be predefined and regularly reviewed. These proactive steps will help ensure the resilience and integrity of DLT initiatives while minimising exposure to third-party risks.

2. Node Concentration Risk

One of the more prominent risks of DLT is node concentration risk. Malicious parties can compromise a ledger's integrity if they gain control of over 50% of the total nodes, computational power, or staked tokens of a DLT network.

For all types of networks, shared vulnerabilities among nodes make the network more susceptible to attacks. For example, if many nodes are hosted by the same service provider or in the same geography, the network becomes more prone to damage from coordinated attacks or natural disasters due to shared risks. Other similar risks include software vulnerabilities in network nodes, which often rely on software implementations provided by different developers and organisations. If a specific software implementation has vulnerabilities or weaknesses, attackers can target it to gain control over a significant portion of the network. These shared vulnerabilities may lead to forking possibilities, where different ledgers are created due to the divergence of node validation.

In the case of permissionless networks, their open nature makes them vulnerable to outside sources taking control, as no restrictions prevent parties from becoming network validators. If a party gains enough resources in a 51% attack, it may be able to quietly control the network without the financial institution's knowledge.

Both private- and public-permissioned networks, on the other hand, already have gated access to network validation. However, compared to permissionless networks, the nodes of permissioned DLT networks face elevated concentration risks, as the network is already controlled by a defined number of parties who share the same operator vulnerabilities. Malicious parties can also rely on traditional security breaching avenues, such as through employee laptops, to take advantage of network vulnerabilities. In addition, the high degree of control is especially vulnerable to the administrator's actions. As control is concentrated in the hands of the administrator, employee sabotage and a lack of risk-control procedures may result in adverse actions from a single individual.

To mitigate node concentration risks, financial institutions should explore diversifying their node operation services and integrating robust software

review procedures. Diversifying node operations, such as by utilising different service providers for nodes, decreases the number of shared vulnerabilities between nodes and ensures that the network nodes are not compromised altogether. Similarly, instilling robust software review and testing procedures will minimise the number of common vulnerabilities that nodes share across a network. Stress testing the network may allow financial institutions to identify hidden software vulnerabilities and soft spots.¹³ Financial institutions should also formulate tailored contingency planning to ensure continued operations, such as non-DLT-based alternatives, in case nodes are compromised.

Financial institutions using permissionless networks should adopt robust consensus mechanisms that prevent easy centralisation (e.g., PoS) and continuously monitor the presence of validator nodes to track and prevent early signs of network centralisation. The adoption of robust consensus mechanisms serves to raise attack barriers for malicious actors. Regular reviews of node activity enhance transparency on financial institutions' network state, allowing them to take steps to identify potential attackers.

External risks from permissioned network usage may be mitigated by strengthening network security, such as implementing firewalls, intrusion detection systems, and advanced network monitoring tools to detect and mitigate external threats. Regular security assessments and penetration testing can help identify on- and off-chain vulnerabilities to ensure that appropriate security measures are in place.

Financial institutions should control internal risks by enforcing strict access controls and monitoring employee activities to prevent potential sabotage. Implementing role-based access controls, and regularly reviewing and updating user privileges, are all examples that may help financial institutions limit internal risks. Additionally, adopting robust identity and access management solutions can limit the downside of internal malicious activities.

3. Smart Contract Risk

Smart contracts, a crucial component of many DLT networks, pose significant risks, including inherent coding vulnerabilities and oracle concentration risks. As smart contracts execute automatically on

¹³ Trail of Bits. 2024. *Security Engineering*. (<https://www.trailofbits.com/services/security-engineering/>).

DLT networks, existing bugs and loopholes can be exploited by malicious actors, which can greatly deteriorate a DLT network's operations. The precision and speed of smart contract execution exacerbate the scale and impact of such attacks. Furthermore, as many smart contracts rely on external information, oracles may reintroduce concentration risks, as their single point of failure or corruption may impede the accurate functioning of smart contracts.

In the context of permissionless DLT networks, financial institutions face security and trust risks. The openness of these networks allows anyone to participate, increasing the potential for malicious parties to create bogus or harmful smart contracts. Moreover, the lack of formal governance structures in permissionless networks makes it difficult to address smart contract vulnerabilities or enforce compliance with regulations.

For both private- and public-permissioned DLT networks, limited network trust and governance challenges remain prominent risks. While these networks offer enhanced privacy and control, trust in participating nodes and network administrators is crucial. Breaches in trust can result in unauthorised access or manipulation of smart contracts. The effectiveness and fairness of smart contract execution can also be manipulated by the governance structure within the consortium or organisation operating the network.

Therefore, as per the previous HKMA circular, financial institutions are recommended to carefully consider use cases for smart contracts, as they may not be feasible for all business scenarios. Automation applications should allow for manual intervention where necessary to incorporate human

judgement and the usage of smart contracts should be paired with effective management of associated vulnerabilities, including operational risks, third-party risks, and legal risks.

As such, financial institutions will need a rigorous governance framework for introducing, assessing, and updating smart contracts. To mitigate these risks, financial institutions should use this framework to systematically identify software vulnerabilities and organisational harms, assess smart contract suitability, and ensure necessary controls are in place. The framework should also cover rigorous testing to identify vulnerabilities before smart contracts are published, processes for seamless data migration during updates to preserve data integrity and ensure operational continuity, and contingency plans that account for cases where operations are disrupted due to smart contracts.

Market solutions are available to address these identified exposures. For instance, during smart contract development, the use of community-reviewed smart contract libraries and frameworks significantly reduces smart vulnerabilities. Before product launches, financial institutions may leverage third-party code audits to examine solutions for potential weaknesses, thereby minimising risks. Throughout implementation, decentralised oracles help mitigate the threat of input tampering. By adopting security measures from market solutions, financial institutions can strengthen their defences against attacks on smart contracts and their inputs.

For permissionless networks, a structured code approval process from major validators, coupled with regular reviews, may help decrease the influence of malignant participants. When necessary, financial



institutions may need to engage in professional advice for third-party audits and reviews. Similarly, careful due diligence of consortium partners and organisation employees establishes safeguards for permissioned networks. By addressing these risks proactively, financial institutions can leverage the benefits of smart contracts while protecting their operations and stakeholders.

4. Immutability Risk

While immutability may be a desired property of DLT networks, the immutability of some data and transactions on DLT networks poses risks for financial institutions. Once information is recorded on the ledger, it becomes extremely difficult to reverse or modify. This can be problematic in cases of errors, fraudulent activities, or disputed transactions, as the ability to rectify or address such issues may be limited. The irreversible nature of transactions increases the importance of accurate data input and thorough validation processes.

This effect is particularly amplified in permissionless DLT networks. These networks' open and decentralised nature means that anyone can participate and contribute to the ledger. While this fosters transparency, it also exposes financial institutions to potentially malicious activities or fraudulent transactions that can be virtually permanently recorded on the immutable ledger. These risks expose financial institutions' lack of full control over the network, which limits their ability to reverse immutability. Unlike traditional centralised systems where a central authority can intervene and reverse transactions, a permissionless network's decentralised and trustless nature makes it difficult for any single entity to unilaterally alter or reverse transactions once they are recorded on the immutable ledger. Financial institutions must rely on the consensus mechanisms and governance processes inherent in permissionless networks to address these issues. This often involves engaging with the broader network participants, presenting evidence, and convincing the network validators to agree on a course of action, which can be time-consuming and complex.

While private- and public-permissioned DLT networks have a more centralised structure and can reintroduce mutability a lot easier, rectifying fraudulent transactions or errors still requires consensus among the participating entities. Without a clear governance

structure and mechanisms for dispute resolution in place, financial institutions may face delays and potential losses in addressing immutability-related risks.

To navigate immutability-related risks, financial institutions should focus on prevention, accuracy, and thorough validation processes. They should prioritise robust security measures and conduct regular audits to prevent unauthorised transactions on their DLT networks. Financial institutions should establish clear governance frameworks, update existing dispute-handling procedures, and set up immediate resolution processes to liaise with external and internal parties to reverse transactions. By proactively addressing immutability-related risks, financial institutions can leverage the benefits of DLT networks while ensuring the integrity and reliability of their financial operations.

5. Private Key Risk

While DLT networks are secure against tampering, the theft and unauthorised use of private keys may still affect operations. As such, financial institutions should be aware of potential vulnerabilities associated with the management and storage of private keys, which are crucial for accessing and controlling digital assets on DLT networks. These risks include unauthorised access, where malicious actors may exploit weak security measures to gain control over private keys; loss or destruction, which can occur due to hardware failures, human error, or inadequate backup systems; and phishing attacks, where individuals may be deceived into revealing their private keys through fraudulent communications. The improper handling of private keys can lead to security breaches, resulting in operational disruptions and possibly, financial losses.

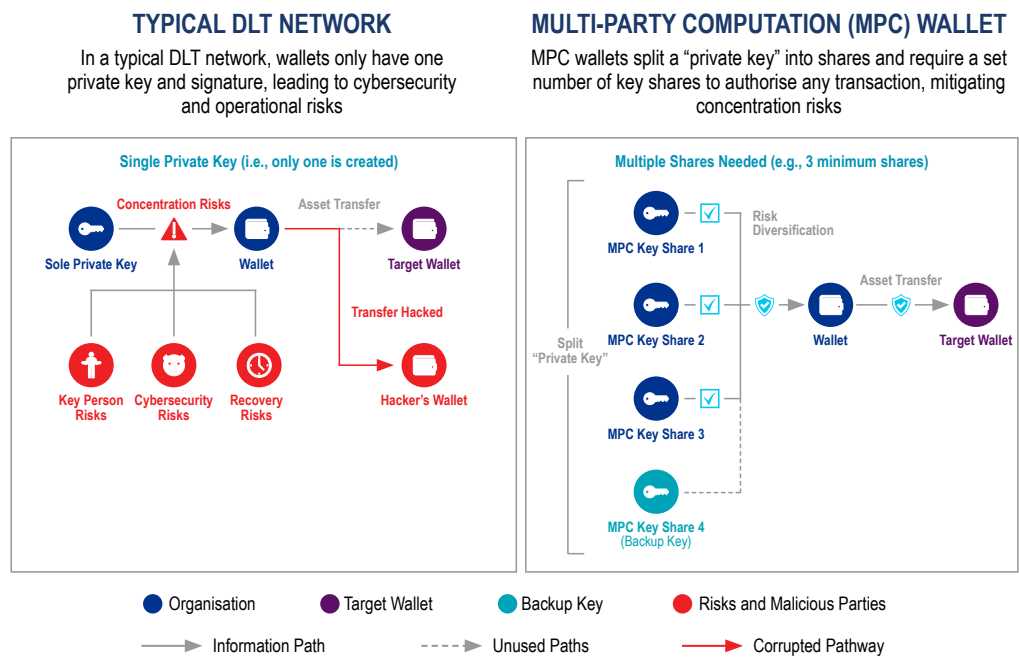
As such, the management of private keys is an important factor for financial institutions to consider, irrespective of the type of blockchain employed. However, the level of access and responsibility for safeguarding these keys will differ depending on the extent of the DLT application and the specific services offered. Considering these variations, the previous HKMA circular advises financial institutions to establish robust policies and procedures that ensure adequate security and contingency plans for any private keys in their possession, tailored to the nature and risks associated with the application and the underlying assets.

For example, a financial institution acting as a custodian for clients' digital assets is typically expected to implement stringent security measures to protect associated private keys and recovery keys, where applicable. These measures should include secure generation processes to avoid potential compromise during creation, stringent access controls to limit key management privileges to authorised personnel, the use of proprietary cold storage, and reliable backup mechanisms to safeguard against accidental loss, among others. To further mitigate risks, financial institutions can establish contingency arrangements. This includes implementing a detailed incident response plan, which could incorporate a rapid alerting system and regular simulations to ensure that staff are prepared to handle key security incidents efficiently.

Financial institutions may explore a range of market solutions, including but not limited to: hardware security modules, which facilitate secure transaction signing and ensure regulatory compliance across different DLT platforms; key management platforms, which provide secure access to DLT nodes and smart contracts; and multi-party computation (MPC) wallets, which enhance security by distributing private keys across multiple locations.^{14, 15, 16}

One of the notable measures that financial institutions could consider mitigating private-key concentration risks is MPC (see Figure 24).

Figure 24: DLT Security Solution



Key Features

Key Person Risk Mitigation	✗	✓
Cybersecurity Risk Mitigation	✗	✓
Recovery Risk Mitigation	✗	✓
Operational Simplicity	✓	✗

✓ Favourable ✗ Unfavourable

Source: S&P Global, Oxford Academic, The Law Commission, Quinlan & Associates analysis

¹⁴ Thales. 2024. *Luna Network Hardware Security Modules*. (<https://cpl.thalesgroup.com/encryption/hardware-security-modules/network-hsms>).
¹⁵ Microsoft Azure. 2024. *Key Vault*. (<https://azure.microsoft.com/en-us/products/key-vault>).
¹⁶ Fireblocks. 2024. *Fireblocks Direct Custody Principles*. (<https://www.fireblocks.com/principles/>).

Rather than using a single private key, MPC wallets split the functionalities of a private key into multiple shares and distribute them among multiple parties. MPC wallets require a subset of these key shares to collaboratively generate a signature (or cryptographic result) to authenticate (sign) the movement of wallet assets. Financial institutions can assign these MPC key shares to different parts of their organisation, ensuring layers of checkpoints to distribute control of the wallet. Additional MPC key shares can also be created to accommodate organisational changes. Even if internal or external bad actors gain access to one key share, the other key shareholders can easily prevent unauthorised access to assets. These additional private keys can also act as a backup in case of the loss of another key. To protect their assets and solution integrity, financial institutions can leverage on-the-market MPC custody solutions to enhance DLT system security through diversification while maintaining operational flexibility.

6. Common Cybersecurity Risks

DLT networks are not completely immune to traditional cybersecurity risks. For example, end-point attacks, including phishing attempts on employees and DDoS (distributed denial of service) attacks, still threaten network integrity and can disrupt day-to-day operations. While existing information on DLT networks remains tamper-proof, malicious actors can still gain unauthorised access through various means and add unwanted transactions to the ledger.

As per the previous HKMA circular, financial institutions are encouraged to establish commensurate levels of cybersecurity protection as traditional infrastructure, with effective mechanisms in place for countering both DLT-specific and common cybersecurity threats. Implementing measures against common cybersecurity risks can bolster financial institutions' resilience against malicious attempts. Implementing multi-factor authentication solutions can significantly increase the complexity for malicious actors to gain control of key DLT network access points. Due to their immutability, DLT networks may require more attention to common cybersecurity measures to prevent unwanted information from being written on them.

Financial institutions should also continuously monitor developments in novel technologies that may disrupt their solution's security, such as quantum computing. In response to these developments, financial institutions should regularly evaluate and adapt their mechanisms, response capabilities, and business continuity plans correspondingly to preserve trust and resilience in their DLT networks.

7. Data Privacy Risk

While beneficial in sharing information, DLT networks' transparency causes confidentiality issues for some organisations. Details regarding the transacting parties and the underlying transaction may need to remain hidden from others in both permissioned and permissionless networks. Revealing the identities of the transacting parties may leak sensitive information such as trade partners, activity, and frequency. In addressing data privacy and protection requirements, financial institutions need adequate systems and controls to ensure their ongoing compliance with regulatory requirements. For example, to adequately protect data confidentiality, financial institutions can adopt technologies in their DLT networks to shield different parts of their transactions, such as proxy and stealth addresses for recipients, ring signatures for senders, and zero-knowledge proofs for transaction details. Whether developed in-house or with third-party vendors, these solutions enable financial institutions to adhere to data privacy confidentiality clauses while adopting DLT networks involving multiple organisations or individuals.¹⁷

Financial institutions may also face data retention issues when adopting DLT, such as scenarios where participants would like to exit the network and remove their pre-existing data from it. Financial institutions should similarly implement contingency plans and controls to address these issues. For example, storage techniques, such as storing sensitive data in off-chain databases or permanently destroying encryption keys for on-chain data, can lend flexibility to financial institutions to stay compliant with data retention regulations. These same techniques can be used to comply with data localisation regulations, where sensitive data can be stored off-chain locally. While some on-chain data are impossible to remove, financial institutions can "delete" such data by rendering access virtually impossible for data retention purposes.

¹⁷ Stanford University. 2024 *Bulletproofs*. (<https://crypto.stanford.edu/bulletproofs/>).

8. Interoperability Challenges

Establishing a unified perspective on technological initiatives across the industry can be challenging, with each organisation having its own strategic priorities, operating procedures, risk tolerance levels, and various other factors. In the case of running DLT initiatives, for instance, there is still no consolidated view on which blockchain type (i.e., private-permissioned, public-permissioned, or permissionless) is most suitable for financial operations. According to research conducted by the BIS, 48% of financial institutions are exploring initiatives on private- or public-permissioned networks, 24% on permissionless networks, and 28% on more than one type of DLT.¹⁸

Consequently, siloed development and experimentation, with different messaging formats, communication protocols, payment processing rules, and access regimes, remain widespread across financial institutions exploring DLT adoption. These differences create barriers to the flow of information and transactions between initiatives, inhibiting DLT adoption at scale across the wider industry. Even within a single organisation, legacy infrastructure and DLT networks lack messaging interoperability, increasing integration costs of adoption. Moreover, when two or more parties need to communicate and share data between DLT networks, they are often forced to resort to off-chain channels due to the high costs of standardisation, introducing a layer of inefficiency and undermining the full benefits of DLT.

To address this challenge, interoperability solutions have been developed to connect independent workstreams managed by different institutions across diverse network types. These solutions deliver added value by enabling interbank transfers and settlement of various assets, extending their utility beyond proprietary networks. The BIS has outlined three interoperability models for payment systems: the pre-compatible model, the interlinked model, and the single-system model.¹⁹

The pre-compatible model refers to individual DLT systems that adhere to common standards, including messaging formats (e.g., International Organization for Standardization (ISO) guidelines), cryptographic techniques, and data requirements. Many interoperability solutions that use the pre-compatible

model use messaging to ensure consistency in communication across different platforms and DLT and non-DLT networks. For example, many institutions have adopted or are currently migrating their messaging standards to ISO 20022, a global standard for the electronic exchange of financial information, due to its advantages of interoperability and standardisation among on- and off-chain infrastructure.²⁰

Compared to the pre-compatible model, the interlinked model establishes connections among various DLT systems through technical and contractual agreements. There are three types of interconnected models: bilateral link, single access point, and hub-and-spoke solutions. The bilateral link model creates a direct connection between two distinct DLT systems, allowing participants to engage in transactions directly with those in the foreign system. Solutions that require greater scalability may adopt the single access point model, which allows participants within a designated system to access another system through a single gateway. The hub-and-spoke model utilises a central hub to serve as a connecting point for two or more separate DLT systems. The hub assumes responsibility for accounting and clearing functions, while settlement can occur either on the hub's own ledger or through the services of a designated settlement agent.

Finally, the single-system model establishes a common platform for participants, while allowing different standards within various systems and jurisdictions to exist. One of the examples of this model aims to allow interoperability between all regulated liabilities (e.g., central bank money, commercial bank money, and electronic money) via tokenisation on a shared ledger.

Given recent developments in interoperability, a broader spectrum of applications within the blockchain ecosystem is being unlocked. By enabling seamless communication and data exchange between networks and platforms, interoperability facilitates the development of multi-party solutions that were previously hindered by isolated systems.

To prevent market fragmentation and maintain the long-term viability of their solutions, financial institutions are encouraged to develop or adopt DLT

¹⁸ Bank of International Settlements. 2023. *Project Dynamo CBDCs, Stablecoins, and Deposit Tokens: Wholesale Adoption Explorations and Challenges*. (https://www.bis.org/innovation_hub/dynamo_study.pdf).

¹⁹ Bank of International Settlements. 2022. *Options for access to and interoperability of CBDCs for cross-border payments*. (<https://www.bis.org/publ/othp52.pdf>).

²⁰ World Bank Group. 2021. *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*. (https://fastpayments.worldbank.org/sites/default/files/2021-11/Fast%20Payment%20Flagship_Final_Nov%201.pdf).

systems that are compatible with both traditional and DLT-based solutions. In their previous circular, the HKMA recommends utilising widely accepted technical standards to facilitate compatibility, while ensuring that any potential connections are established securely to safeguard against cyberattacks, security vulnerabilities, and risks of data leakage.

When adopting interoperability solutions, financial institutions should also have rigorous layers of testing and contingency scenario planning. This multifaceted approach is essential for ensuring that systems can communicate effectively across various platforms, minimising the risk of errors or failures. Thorough testing allows institutions to identify and address potential issues before they impact operations, while contingency planning prepares them for unforeseen disruptions, such as unexpected system outages. By prioritising these layers of planning, financial institutions not only safeguard their operations but also enhance their overall resilience, fostering greater confidence among clients and stakeholders in their adoption of DLT solutions.

9. Scalability Challenges

Despite the versatility of DLT, network scalability has been another major challenge for adoption. Currently, there is a cap on a blockchain's throughput (i.e., processing speed) measured by transactions per second (TPS). On average, Ethereum processes around 12-15 TPS, while Bitcoin can only handle

around 6-8 TPS.²¹ This low throughput poses a significant barrier for financial applications that require high transaction volumes. In comparison, SWIFT facilitates international money transfers through its network, processing an average of 523.14 TPS as of 2022, a significantly higher rate than many blockchains can support.²²

Delays and inefficiencies may arise when the transaction volume exceeds the chain's processing capacity. Network congestion can become particularly severe during peak periods, hindering overall performance. Without scalable solutions, financial institutions may find their DLT-based applications struggling to meet the demands of the financial industry, limiting their adoption and usability.

To enhance the throughput of DLT networks, Layer 1 (L1) and Layer 2 (L2) scaling solutions have been introduced. L1 solutions involve changing the underlying blockchain protocol itself, such as increasing block size, modifying consensus mechanisms, or partitioning the database (i.e., sharding). For example, in March 2024, Ethereum announced its Dencun upgrade through proto-danksharding,²³ which promises a vastly more efficient data management system.²⁴ While these solutions offer scalability improvements to both permissioned and permissionless networks, they may involve complex technical challenges and require extensive network upgrades.



²¹ Chainspect. 2024. *What is Transactions Per Second (TPS)?* (<https://chainspect.app/blog/transactions-per-second-tps>).

²² Chainspect. 2023. *Blockchains vs. SWIFT: Ease of Use, Speed, and Throughput Comparison.* (https://medium.com/@chainspect_app/blockchains-vs-swift-ease-of-use-speed-and-throughput-comparison-c9c085087252).

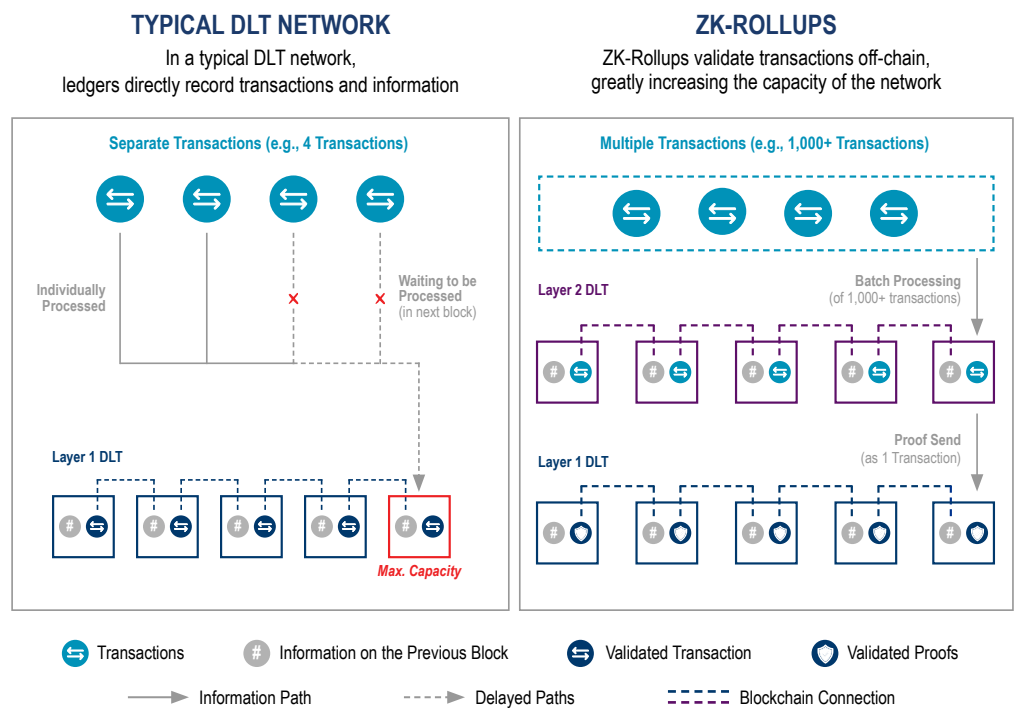
²³ Proto-danksharding (EIP-4844) is a proposed change to the Ethereum network that would allow for the inclusion of additional "blobs" of data with transactions to enhance the network's scalability. These blobs would be temporarily stored on Ethereum's servers, without adding significant overhead. EIP-4844. 2022. *EIP-4844: Shard Blob Transactions Proto-Danksharding.* (<https://www.eip4844.com/>).

²⁴ CoinDesk. 2024. *Ethereum Blockchain Counts Down to 'Dencun' Upgrade, Set to Reduce Fees.* (<https://www.coindesk.com/tech/2024/03/12/ethereum-blockchain-counts-down-to-dencun-upgrade-set-to-reduce-fees/>).

On the other hand, L2 solutions may be quicker to implement and are generally less disruptive to the network and hence are preferred for financial institutions to address scalability challenges. Measures financial institutions may consider include rollups (i.e., bundling of transactions), side chains (i.e., parallel blockchains), and state channels (i.e., off-chain handling of transactions). In particular, the use of zero-knowledge rollups (ZK-Rollups) may

allow financial institutions to process thousands of TPS and reduce the main blockchain’s computational load while ensuring the security and privacy of the network.²⁵ ZK-Rollups achieve this by aggregating transactions into a single proof. As a result, all transactions on the L2 protocol do not require approval from all the nodes, significantly accelerating transaction processing (see Figure 25).

Figure 25: DLT Scalability Solution



Key Features

Security	✓	✓
Computation Efficiency (Per Transaction)	✗	✓
Cost Efficiency (Per Transaction)	✗	✓
Transactions per Second	✗	✓

✓ Favourable ✗ Unfavourable

Source: Chainlink Labs, Polygon, Quinlan & Associates analysis

²⁵ zkSync. 2022. *Technology: Maximum throughput*. (<https://docs.lite.zksync.io/userdocs/tech/#zk-rollup-architecture>).

With enhanced scalability through technologies like zero-knowledge proofs, both permissioned and permissionless DLT platforms have the potential to be better equipped to handle the high-volume transactions of the financial industry. Overall, adopting scalability solutions will give DLT networks a significant boost in transaction throughput, empowering financial institutions to process payments and transactions quicker and more effectively.

When adopting these scalability solutions, financial institutions should employ systematic frameworks to test their impact. This process involves evaluating how these DLT solutions affect existing systems and workflows, allowing institutions to identify any potential bottlenecks or inefficiencies before full implementation. Rigorous testing helps to assess not only the technical aspects but also the operational implications, ensuring that the solutions can handle increased demand without compromising service and usage quality. These thorough evaluations enable financial institutions to make informed decisions, optimise their resources, and ultimately minimise risks associated with scaling, fostering a more robust and agile organisational framework.

4.2.5 Continue with Adoption Efforts under the Existing Regulatory Principles

The lack of regulatory clarity has been consistently raised as the overarching adoption hurdle by financial institutions and DLT solution providers engaged in the HKMA's research. The regulators recognise that clear and principle-based regulatory guidance may provide an additional layer of confidence for embracing DLT adoption.

As regulators continue to monitor various market and technological developments to form concrete views and introduce policy-level measures that may be legally binding and enforceable, financial institutions are encouraged to proceed with DLT adoption efforts under the existing regulatory principles guiding current financial market operations. Regulators also understand that specific nuances may arise from the new operational paradigm introduced by DLT. In such cases, financial institutions are encouraged to collectively steer relevant policy developments by participating in consultation papers and maintaining open communication through the channels provided

by regulators. During implementation, financial institutions may need to seek professional advice when necessary and place measures during the design process to mitigate legal risks.

The nature of financial assets and their purchase implications on financial (e.g., financial return, risk exposure, etc.) and legal (e.g., statutory rights, investor protection, issuer obligations, etc.) perspectives will likely remain unchanged – “same activity, same risk, same regulation”. In other words, regardless of how and where financial assets are recorded and traded, new regulations, where applicable, will likely adhere to existing principles while incorporating details specific to the DLT environment. Such regulatory development approaches are common in different jurisdictions.

As stated in the previous HKMA circular, financial institutions should still be aware of possible legal grey areas and regulatory developments, especially in the legal definitions of factors like settlement finality and the treatment of tokenised assets. That said, progress is being made on this front. Specifically, it has been observed that while variations exist in the legal definitions and requirements for smart contracts, there are emerging views that activities in the DLT environment leveraging smart contract functionalities can be legally binding if they satisfy the necessary principles for contract formation within their respective legal frameworks.

1. Hong Kong Special Administrative Region

Smart contracts lack a specific legal definition, but their potential as legally binding agreements hinges upon the context. Forming such agreements necessitates fulfilling several requirements, including agreement, consideration, certainty and completeness, intention to create legal relations, and compliance with formalities.

2. Singapore

The principles of common law govern contractual arrangements. Contracts must encompass elements of an offer, acceptance, and consideration. Should smart contracts meet these legal requirements, they can be enforced in Singapore. However, explicit written confirmation or precedent-setting cases from local courts are currently lacking. The Electronic Transactions (Amendment) Act of 2021 supports the legal framework for smart contracts in Singapore.²⁶

²⁶ Singapore Statutes Online. 2021. *The Electronic Transactions (Amendment) Act 2021*. (<https://sso.agc.gov.sg/Acts-Supp/5-2021/Published/20210312?DocDate=20210312>).

3. United States

Smart contracts are regarded as computer code and may represent all, part, or none of a valid legal contract. While smart contracts facilitate the execution of legal agreements, traditional contracts remain indispensable for legal effectiveness in smart transactions. Common law principles dictate that a smart contract should incorporate the three elements of an offer, acceptance, and consideration. State-level legislation, such as Arizona's HB2417, enacted in 2017, and the Enacted E-sign Act of 2000, reinforce this legal perspective.²⁷

4. United Kingdom

Smart contracts possess the potential to fulfil the conditions requisite for contract formation, including agreement, consideration, certainty, and an intention to create legal relations. In November 2021, the Law Commission expressed confidence in the UK's common law system's ability to handle smart contracts. The Legal Statement on Crypto Assets and Smart Contracts by the Law Commission in 2019 further bolsters this viewpoint.²⁸

4.2.6 Proactively Communicate Needs and Collectively Develop Regulations

The regulators also understand that a new operational paradigm may be introduced by DLT, potentially requiring a new regulation capturing specific nuance and policy-level support. In such cases, financial institutions are encouraged to collectively steer relevant policy developments. For example, financial institutions are encouraged to closely monitor the release of consultation and discussion papers that allow the private sector to provide their suggestions in advance to shape regulations to better reflect needs and demands. In addition, financial institutions are encouraged to leverage the various supervisory arrangements introduced that allow them to gradually refine and enhance their risk management controls under an iterative and guided approach (see Figure 26).

Figure 26: Supervisory Arrangements for Fostering DLT-related Initiatives

Regulatory Body	 The Hong Kong Monetary Authority	 The Securities and Futures Commission	 The Insurance Authority
Supervisory Arrangement	Supervisory Incubator for Distributed Ledger Technology	SFC Regulatory Sandbox	Insurtech Sandbox
Objective	To support Authorized Institutions to productionise DLT-based banking products and services in a risk-controlled manner through bank-level and industry-level initiatives	To provide a confined regulatory environment for qualified firms to operate regulated activities under the SFO before Fintech is used on a fuller scale	To facilitate a pilot run of innovative Insurtech applications by authorized insurers to be applied in their business operations
Environment	Under the one-stop supervisory platform, supervisory flexibility can be provided to facilitate the testing and reaffirmation of risk management controls, on the condition that adequate risk management controls are in place	Enable qualified firms, through close dialogue with and supervision by the SFC under the licensing regime, to readily identify and address any risks or concerns relevant to their regulated activities	Allow a new Insurtech initiative to collect sufficient data to demonstrate that it can broadly meet relevant supervisory requirements arising from IA's codes and guidelines and other regulatory practices
Participants	Authorized Institutions (including in partnership with fintech firms)	Licensed corporations and start-up firms	Authorized insurers and licensed insurance broker companies
Contact Point	Supervisory Incubator for Distributed Ledger Technology Team supervisory_incubator_DLT@hkma.gov.hk	Fintech Contact Point fintech@sfc.hk	Insurtech Facilitation Team Insurtech@ia.org.hk

Source: HKMA, SFC, IA

²⁷ Federal Deposit Insurance Corporation (FDIC). 2014. *FDIC Consumer Compliance Examination Manual – January 2014*. (<https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/10/x-3-1.pdf>).

²⁸ The Law Commission. 2021. *Smart Contracts*. (<https://lawcom.gov.uk/project/smart-contracts/>).

1. HKMA: Supervisory Incubator for Distributed Ledger Technology

Launched in January 2025, the Supervisory Incubator for DLT (hereinafter “the Incubator”) is a new supervisory arrangement designed to help banks maximise the potential benefits of DLT adoption by effectively managing the associated risks. It will augment risk management capabilities at both the individual bank and industry levels, with a particular focus on addressing those risks that may arise as banks move to productionise relevant services that cut across DLT-based and legacy banking infrastructures.

At the individual bank level, the Incubator offers a one-stop supervisory platform that enables banks to reaffirm the adequacy of their risk management controls prior to the full launch of a DLT-based initiative. By leveraging this platform, banks have access to a dedicated team from the HKMA for obtaining supervisory feedback and may opt to conduct live trials to validate and refine specific aspects of their risk management implementation under a hands-on and iterative approach, as needed.

The Incubator will also promote industry awareness and understanding of best practices in DLT risk management through a range of targeted initiatives, such as supervisory guidance, industry sharing sessions, and forward-looking research projects. Collectively, these initiatives will enhance the overall industry’s ability and readiness to deploy DLT-based solutions in the long run.

2. SFC: Regulatory Sandbox

Recognising the use of innovative technologies, the SFC launched the SFC Regulatory Sandbox in 2017 for qualified firms. Through close dialogue with and supervision by the SFC under the licensing regime, qualified firms can readily identify and address any risks or concerns regarding their regulated activities before providing the services to Hong Kong’s wider public.²⁹ To qualify for this sandbox, a firm must be either a licensed corporation or a start-up firm that intends to carry on an activity regulated by the SFC.

Regulation of virtual asset (VA) activities is a salient example of the importance of the SFC Regulatory Sandbox in the SFC’s regime development. Since 2018, the SFC has put in place holistic and

comprehensive frameworks for regulating VA activities from an investor protection perspective, covering key investor protection concerns. VA activities regulated by the SFC have increased over the years and now include operation of centralised VA trading platforms and VA-related activities conducted by SFC-licensed intermediaries. Another example is the SFC’s joint effort with the HKMA, titled ‘Project Ensemble’, to facilitate the Hong Kong asset management industry’s adoption of tokenisation.³⁰

Building on its commitment towards fostering a resilient and well-regulated VA ecosystem, the SFC recently introduced the *ASPIRe* roadmap in February 2025.³¹ This roadmap outlines 12 major initiatives under five pillars (i.e., Access, Safeguards, Products, Infrastructure, and Relationships). The initiatives will streamline access for global liquidity, enable adaptive compliance and product frameworks focusing on security, and drive infrastructure upgrades for traditional finance to tap into blockchain efficiency. The roadmap represents the SFC’s forward-looking commitment to addressing the VA market’s most pressing challenges. The roadmap is not a final destination but a living blueprint, one that invites collective efforts to advance Hong Kong’s vision as a global hub where innovation thrives within guardrails. By embracing this mindset, the market can forge a resilient path forward, ensuring that growth and integrity coexist in an ever-evolving financial landscape.

3. IA: Insurtech Sandbox

The IA launched an Insurtech Sandbox in 2017 to facilitate a pilot run of innovative Insurtech applications by Authorized insurers if they are uncertain about the compliance of initiatives that apply innovative technologies.³²

To promote technology development for Hong Kong’s insurance industry, the IA allowed flexibility in the supervisory requirements in the Insurtech Sandbox. Participants gain real market data and information on user experience in a controlled environment before the market launch. Meanwhile, considering the latest technological applications, the IA could obtain valuable inputs for refining supervisory requirements. The IA expanded the participant scope to include licensed insurance broker companies in 2021.³³

²⁹ Securities and Futures Commission. 2023. *SFC Regulatory Sandbox*. (<https://www.sfc.hk/en/Welcome-to-the-Fintech-Contact-Point/SFC-Regulatory-Sandbox>).

³⁰ Securities and Futures Commission. 2024. *SFC welcomes launch of Project Ensemble Sandbox as key step in Hong Kong’s tokenisation development*. (<https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=24PR140>).

³¹ Securities and Futures Commission. 2025. *“A-S-P-I-Re” for a brighter future: SFC’s regulatory roadmap for Hong Kong’s virtual asset market*. (<https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/A-S-P-I-Re-for-a-brighter-future-SFCs-regulatory-roadmap-for-Hong-Kongs-virtual-asset-market>).

³² Insurance Authority. 2024. *Insurtech Sandbox*. (https://www.ia.org.hk/en/aboutus/insurtech_corner.html#1).

³³ Insurance Authority. 2021. *Embracing the New Normal Annual Report 2020-21*. (https://www.ia.org.hk/en/infocenter/files/IA_Annual_Report_2020_21_Eng.pdf).

5. The Way Forward

The HKMA recognises the interest in and benefits of DLT adoption in the financial services industry, as highlighted in section 3. To facilitate a more conducive environment for DLT integration, the HKMA is committed to helping financial institutions overcome the barriers to DLT adoption by fostering a collaborative approach with industry stakeholders.

5.1 Regulatory Coordination

The HKMA acknowledges that proactive regulatory guidance plays a crucial role in facilitating DLT adoption. To this end, the HKMA will continue to engage in active dialogue and consultation with other regulatory bodies, industry stakeholders, and international organisations.

Regulatory coordination across the banking, securities, and insurance sectors can help unlock the full potential of DLT by providing clarity and consistency in policy approaches. Maintaining open communication between financial regulators, legislators, and industry participants will support the development of a regulatory framework that effectively addresses common industry needs.

In addition to fostering collaboration among regulators, ongoing industry consultation will be essential. Gathering input from both financial institutions and DLT solution providers through supervisory arrangements will help identify areas where regulatory clarity is needed, ensuring that policies evolve in line with market developments.

As many financial institutions in Hong Kong operate on a regional or global scale, aligning regulatory principles with international best practices could facilitate more seamless and scalable DLT adoption.

As such, monitoring regulatory developments in other jurisdictions and engaging in international forums may provide valuable insights into emerging standards. Encouraging dialogue at bilateral and multilateral levels could further support efforts to establish common regulatory principles and share best practices.

5.2 DLT Ecosystem Facilitation

Several support programmes and initiatives, ranging from the Supervisory Incubator for Distributed Ledger Technology, flagship DLT seminar, annual Hong Kong Fintech Week, and industry-led incubator / accelerator programmes, are crucial in facilitating financial institutions and service providers to harness the full potential of DLT. The HKMA will continue to foster the collaborative and sustainable ecosystem needed for DLT adoption in Hong Kong.

1. Consolidate Support Initiatives

The HKMA recognises that information surrounding DLT support initiatives remains fragmented, each with its own structure and form, given that they are driven by different public entities. This makes it challenging for financial institutions to easily locate, access, and leverage relevant supporting information. Meanwhile, various programmes and events, particularly those with limited promotions, may go unnoticed.

Recognising the need for a more unified and streamlined approach, the HKMA will seek to consolidate support initiatives with the aim of enhancing their accessibility and visibility. By offering a single point of access where these initiatives can

be located, financial institutions can more proactively check for updates, receive notifications, and register for events that are of interest, as opposed to constantly pushing information to the community.

For instance, the aforementioned Supervisory Incubator for Distributed Ledger Technology consolidates support for both individual banks and the industry within one initiative. Specifically, besides offering a one-stop supervisory platform for banks to conduct live trials of their DLT-related initiatives, it will also leverage potential learnings from these pilots to initiate work (e.g., issuance of supervisory guidance, arrangement of sharing sessions, conducting of research, etc.) that aims to enhance the overall industry's awareness and understanding of best practices in DLT risk management. Some of this work will also support the initiatives or items that follow below.

2. Provide Avenues for Success

Hong Kong provides avenues for Fintech stakeholders to connect, share insights, and foster partnerships for DLT adoption. These avenues include Hong Kong Fintech Week, FiNETech by the HKMA, and private-led events such as the Web3 Festival by Wanxiang Blockchain Labs and HashKey Group. Moreover, Hong Kong has become a regional and global hub for hosting large-scale, influential events from overseas.

The HKMA will look to organise more DLT-focused events, ranging from expert-focused conferences to expand networks, regular meetups for industry professionals, and hackathons targeting aspiring developers and entrepreneurs to facilitate knowledge exchange and collaboration.

3. Nurture DLT Talents

Nurturing a strong DLT ecosystem requires cultivating local talent from an early stage, fostering interest, appreciation, and an understanding of DLT. This effort extends beyond professionals to include students, who are the future innovators in this field.

As such, the HKMA will encourage collaboration among financial institutions, DLT solution providers, and academic institutions to drive educational initiatives across various groups. These institutions can offer courses designed to strengthen practical DLT competencies, followed by boot camps that

allow students to apply their knowledge and develop relevant skill sets. Such initiatives can inspire students to consider careers in the DLT space. For industry professionals, the HKMA will explore opportunities to expand flexible, self-paced online learning resources, direct shadowing, and training led by industry experts.

4. Encourage Research Collaboration

Hong Kong has made significant strides in establishing regular research collaborations. Academic institutions, such as the Hong Kong Polytechnic University, have established dedicated centres like the Centre for Blockchain Technology. Public research institutions, such as the Hong Kong Applied Science and Technology Research Institute, have also set up innovation and research labs in collaboration with both academic and financial institutions.

To keep the financial industry abreast of the latest developments in DLT and foster innovative adoption, the HKMA aims to strengthen private-public research collaborations with the objective of developing practical suggestions and solutions for overcoming DLT-specific challenges in Hong Kong. This effort will involve providing research theses based on DLT-specific challenges identified through the HKMA's research efforts, inviting institutions that are leading DLT innovation in areas such as interoperability and scalability, connecting these organisations with the public research institutions, and providing the necessary support to ensure the success of these collaborative research efforts.

5.3 Financial Support

1. Implementation Support

Recognising the high costs of deploying and integrating DLT solutions as a major business challenge for financial institutions to deploy DLT solutions, the HKMA and other public bodies in Hong Kong have introduced various funding and grant schemes to encourage broader adoption.

As announced in the 2024 Policy Address, the HKMA's recent Digital Bond Grant Scheme by the HKMA aims to promote the digital securities market's development and encourage broader adoption of tokenisation initiatives.³⁴ Applications are required

³⁴ Hong Kong Monetary Authority. 2024. *HKMA launches Digital Bond Grant Scheme*. (<https://www.hkma.gov.hk/eng/news-and-media/press-releases/2024/11/20241128-3/>).

to either have a DLT development and/or operations team for the digital bond issuance with a substantial Hong Kong presence or issue the digital bond on a DLT platform by the Central Moneymarkets Unit. Upon meeting additional requirements, the applicant can qualify for the Full Grant up to Hong Kong Dollar (HKD) 2.5 million.

2. Talent Attraction and Upskilling

The successful implementation of DLT solutions heavily depends on having qualified professionals to utilise DLT solutions to their fullest. To nurture the local talent pool, Hong Kong has provided subsidies to attract foreign talents with DLT expertise and upskill local professionals with specialised DLT training.

To promote the professional development of Fintech talents in Hong Kong, the Training Subsidy for Fintech Practitioners scheme was introduced for banking practitioners, with a focus on specialised areas including DLT.³⁵ HKMA-licensed Authorised Institutions must first sponsor their employees to undergo the required training and submit applications to the Hong Kong Institute of Bankers within 3 months after these employees attain relevant professional qualifications. For each eligible professional qualification, the scheme will reimburse 80% of the training costs, subject to a cap of HKD 25,000.

5.4 Conclusion

The HKMA remains committed to fostering a dynamic and supportive environment for DLT adoption in Hong Kong's financial services industry. Recognising both the opportunities and challenges associated with DLT adoption, the HKMA will proactively monitor the landscape to identify and bridge regulatory and structural gaps that may hinder adoption.

Looking ahead, the HKMA will maintain a close working relationship with industry stakeholders, policymakers, and academia, to refine its approach in responding to evolving market needs and technological advancements. By nurturing a conducive ecosystem for DLT innovation, the HKMA aims to strengthen Hong Kong's position as a leading global financial hub, leveraging DLT to drive efficiency, security, and financial inclusion in the years to come.

³⁵ Hong Kong Monetary Authority. 2022. *Pilot Scheme on Training Subsidy for Fintech Practitioners*. (<https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/soft-infrastructure/pilot-fintech/>).

6. Appendix

6.1 List of Abbreviations

- **AML:** Anti-money laundering
- **API:** Application programming interface
- **BIS:** Bank for International Settlements
- **CBDCs:** Central bank digital currencies
- **CCASS:** Central Clearing and Settlement System
- **DDA:** Demand deposit account
- **DLT:** Distributed Ledger Technology
- **DTCC ITP:** Depository Trust & Clearing Corporation Institutional Trade Processing
- **DvP:** Delivery versus payment
- **EU:** The European Union
- **FDIC:** Federal Deposit Insurance Corporation
- **FSS:** Fintech Supervisory Sandbox
- **HKD:** Hong Kong Dollar
- **HKEX:** Hong Kong Exchanges and Clearing Limited
- **HKFI:** The Hong Kong Federation of Insurers
- **HKMA:** The Hong Kong Monetary Authority
- **HKSAR:** The Hong Kong Special Administrative Region
- **HMAC:** Hash-based Message Authentication Code
- **IA:** The Insurance Authority
- **ISO:** International Organization for Standardization
- **JPM:** J.P. Morgan
- **KYB:** Know Your Business
- **KYC:** Know Your Customer
- **L1:** Layer 1
- **L2:** Layer 2
- **MIDAS:** Motor Insurance DLT-based Authentication System
- **MPC:** Multi-party computation
- **MPFA:** The Mandatory Provident Fund Schemes Authority

- **PoC:** Proof-of-Concept
- **PoS:** Proof-of-Stake
- **PoW:** Proof-of-Work
- **Repo:** Repurchase agreements
- **RTGS:** Real-time gross settlement
- **SBT:** Soulbound Token
- **SFC:** The Securities and Futures Commission
- **SWIFT:** Society for Worldwide Interbank Financial Telecommunication
- **TPS:** Transactions per second
- **USD:** United States Dollar
- **VA:** Virtual Asset

6.2 Glossary of Key Terms

- **Bilateral Link Model:** An interoperability model that creates a direct connection between two distinct DLT systems, allowing participants to engage in transactions directly with those in the foreign system
- **Blockchain:** A category of DLT networks that consists of a linear chain of information blocks that store transaction records
- **Blocks:** Organised data on a DLT network that contains batches of previously validated information agreed upon by network participants
- **Burn:** The irrevocable destruction of a token to exclude it from circulation
- **Central Bank Digital Currencies:** M0 digital currencies issued by central banks
- **Consensus Mechanisms:** Algorithms governing how participating nodes interact to validate, agree upon, and record transactions on the distributed ledger to ensure entry consistency
- **Cryptography:** The practice of securing communication and information by converting it into a coded format, ensuring that only authorised parties can access and understand the data

- **Distributed Denial of Service (DDoS) Attacks:** Attacks involve overwhelming a target server or network with traffic from multiple compromised sources, rendering it unavailable to legitimate users
- **Delivery versus Payment (DvP):** A financial settlement mechanism where the transfer of securities occurs simultaneously with the payment, ensuring that neither party is at risk of default
- **Distributed Ledger Technology (DLT):** A method of proposing and validating records on a synchronised ledger system based on pre-agreed protocols between multiple entities from different locations
- **Ethereum:** An open-source DLT network platform that enables developers to build and deploy decentralised applications using smart contracts
- **Encryption Keys:** Strings of data used in cryptographic algorithms to encode and decode information, ensuring that only authorised users can access the original data
- **Endpoint Attacks:** Cyberattacks targeting end user devices, such as computers or mobile phones, to gain unauthorised access or steal data
- **Forking:** The process of creating a new version of a DLT network by diverging from its original protocol, which can lead to a split into two separate networks
- **Fungible Token:** A type of digital asset that is interchangeable with others of the same type, meaning each token holds the same value and can be exchanged on a one-to-one basis
- **Hash:** A fixed-size string of characters generated by a cryptographic algorithm, representing data in a unique format, commonly used in DLT networks for data integrity
- **Hub-and-Spoke Model:** An interoperability model that utilises a central hub to serve as a connecting point for two or more separate DLT systems
- **Interoperability:** The ability of different DLT systems and networks to communicate and interact with each other seamlessly
- **Layer 1:** The base layer of a DLT architecture, responsible for the main protocol and security of the network
- **Layer 2:** A secondary framework built on top of a Layer 1 DLT network to improve scalability and transaction speed, often facilitating off-chain transactions
- **Mint:** The process of creating new tokens and adding them to a DLT network
- **Multi-Party Computation Wallets:** Wallets that split the functionalities of a private key into multiple shares and distribute them among multiple parties
- **Network:** Nodes managed by network participants
- **Nodes:** Individual computers connected to a functioning DLT, each maintaining an updated copy of the ledger
- **Non-Fungible Token:** A unique digital asset representing ownership of a specific item or piece of content on a DLT network, distinguished by its non-interchangeable nature
- **Off-chain:** Refers to transactions or processes that occur outside the DLT network
- **Oracles:** Intermediary protocols that bridge DLT networks to off-chain data sources, such as queries to internal databases
- **On-chain:** Refers to transactions or activities that occur directly on a DLT network
- **Permissioned Networks:** DLT networks that are controlled by approved entities
- **Permissionless Networks:** DLT networks that offer an open environment where participation is open to anyone who can connect to the network
- **Public:** Refers to DLT networks that are open and accessible to anyone
- **Private:** Refers to DLT networks that restrict access and participation to a specific group of users
- **Proof-of-Concept:** A demonstration or prototype that is created to validate an idea, concept, or theory, helping organisations make informed decisions about moving forward with a project
- **Proof-of-Stake:** A consensus mechanism where a node's likelihood of validating transactions correlates with its stake (i.e., the number of tokens held in the network)
- **Proof-of-Work:** A consensus mechanism where nodes compete to solve complex mathematical puzzles to validate transactions
- **Protocol:** Guiding principles and relevant tools for participation in a DLT network
- **Seed Phrase:** A sequence of random words that stores the data required to access or recover cryptocurrency
- **Service-Level Guarantees:** Agreements that define the expected level of service performance, including availability, reliability, and response times, often used in contractual contexts

- **Settlement Finality:** The assurance that a transaction, once completed, cannot be reversed or altered, providing certainty to the parties involved
- **Sharding:** A scaling technique that divides a DLT network into smaller, more manageable pieces (shards) to improve transaction speed and efficiency
- **Smart Contracts:** Transaction instructions with predefined conditions, executed automatically and settled instantly, typically on a DLT network
- **Stablecoin:** A type of token designed to maintain a stable value, often pegged to a fiat currency or a basket of assets, to reduce volatility
- **Token:** A digital unit of value created on a DLT network, representing assets or utilities
- **Tokenisation:** The process of converting ownership rights of an asset into a digital token
- **Tokenised Assets:** Physical or digital assets that have been converted into tokens on a DLT network
- **Tokenised Deposit:** A digital representation of a deposit, often issued by a financial institution on a DLT network
- **Zero-Knowledge Proofs:** Cryptographic methods that allow one party to prove to another that a statement is true without revealing any specific information about the statement itself
- **Fireblocks:** Fireblocks Direct Custody Principles (2024)
- **Global Financial Innovation Network:** Cross-border Testing (2021)
- **Google:** Patent search results for “DLT”, “Distributed Ledger Technology” and “Blockchain” (2024)
- **Hang Seng Bank:** Envisioning Programmable Payments in Hong Kong: How could an e-HKD further improve payments in Hong Kong? (2023)
- **Hong Kong Monetary Authority:** Pilot Scheme on Training Subsidy for Fintech Practitioners (2022), Risk Management Considerations Related to the Use of Distributed Ledger Technology (2024), Fintech Supervisory Sandbox (FSS) (2024), Stablecoin Issuer Sandbox (2024), HKMA establishes the Project Ensemble Architecture Community (2024), HKMA launches Digital Bond Grant Scheme (2024)
- **Insurance Authority:** Embracing the New Normal Annual Report 2020-21 (2021), Insurtech Sandbox (2024)
- **Microsoft Azure:** Key Vault (2024)
- **Securities and Futures Commission:** SFC Regulatory Sandbox (2023), SFC welcomes launch of Project Ensemble Sandbox as key step in Hong Kong’s tokenisation development (2024), “A-S-P-I-Re” for a brighter future: SFC’s regulatory roadmap for Hong Kong’s virtual asset market (2025)
- **Singapore Statues Online:** The Electronic Transactions (Amendment) Act 2010 (2021)
- **Stanford University:** Bulletproofs (2024)
- **Tatum:** Smart Contracts (2022)
- **Thales:** Luna Network Hardware Security Modules (2024)
- **The Law Commission:** Smart Contracts (2021)
- **Trail of Bits:** Security Engineering (2024)
- **UBS:** UBS expands its digital asset capabilities by launching Hong Kong’s first-ever tokenized warrant on the Ethereum network (2024)
- **World Bank Group:** Considerations and Lessons for the Development and Implementation of Fast Payment Systems (2021)
- **zkSync:** Technology: Maximum throughput (2022)

6.3 List of References

- **Bank of International Settlements:** What is distributed ledger technology? (2017), Options for access to and interoperability of CBDCs for cross-border payments (2022), Project Dynamo CBDCs, Stablecoins, and Deposit Tokens: Wholesale Adoption Explorations and Challenges (2023)
- **Chainspect:** Blockchains vs. SWIFT: Ease of Use, Speed, and Throughput Comparison (2023), What is Transactions Per Second (TPS)? (2024)
- **Coindesk:** Ethereum Blockchain Counts Down to ‘Dencun’ Upgrade, Set to Reduce Fees (2024)
- **Federal Deposit Insurance Corporation:** FDIC Consumer Compliance Examination Manual – January 2014 (2014)
- **Financial Services and Treasury Bureau:** Policy Statement on Development of Virtual Assets in Hong Kong (2024)

6.4 Acknowledgements

This paper has greatly benefitted from the contributions of various external collaborators. We would like to thank the Securities and Futures Commission, the Insurance Authority, the Mandatory Provident Fund Schemes Authority, and various divisions of the Hong Kong Monetary Authority, including the Communications Division, the External Division, the Fintech Facilitation Office, and the Banking Supervision Division, for their comments and suggestions.

We are also grateful for the collaboration of Quinlan & Associates and KPMG in designing and conducting interviews with various market participants, including technology providers, banks, securities, and insurance firms.

We wish to extend our gratitude to Allianz Technology SE, CryptoBLK Limited, Deutsche Bank Aktiengesellschaft, Digital Asset Holdings, LLC, Hang Seng Bank, Limited, Hong Kong Exchanges and Clearing Limited, The Hong Kong Federation of Insurers, Hongkong and Shanghai Banking Corporation Limited (The), JPMorgan Chase Bank, National Association, Linklogis Inc., Memento Blockchain Pte. Ltd, UBS AG, and WeCanGroup SA for their valued contributions.