Risk management considerations related to the use of distributed ledger technology (DLT)

April 2024

Since the Government published its "Policy Statement on Development of Virtual Assets in Hong Kong" in 2022, the banking sector has shown a growing interest in exploring how to apply the DLT that underlies the virtual assets ecosystem to traditional financial market operations.

The Hong Kong Monetary Authority (HKMA) is supportive of Authorised Institutions (AIs) adopting DLT-based solutions so long as they can adequately manage the associated risks. Specifically, HKMA has been encouraging banks to study the potential of taking “tokenised” deposits. HKMA provided more clarity on the key risk management considerations that it considers when reviewing the DLT-related proposals of banks in the recent circular Risk management considerations related to the use of distributed ledger technology (hkma.gov.hk).

It is worth noting that the HKMA will review the bank’s proposal on the use of DLT on a case-by-case basis. The considerations listed in the circular are non-binding, non-exhaustive and will continue to evolve as the market and related technologies develop.

In this brief, KPMG outlines the key considerations described by HKMA in the circular together with some industry practices and our insights.

When developing a business initiative with DLT, a bank should consider the following:

Governance

- Board and senior management assume full responsibility for an AI’s adoption of DLT and for adequately managing related risks

Application Design and Development

- Correct DLT network selected for a given application
- Smart contracts are “fit for purpose”
- Understand and mitigate potential legal risks
- Effectively manage third party-related risks
- Safely enable interoperability and connectivity

On-going maintenance and monitoring

- Establish level of cybersecurity commensurate with traditional technology applications
- Securely manage private keys
- Ensure compliance with data privacy and protection requirements
- Tailor contingency planning and testing arrangements

The release of these risk management considerations by the HKMA gives the industry a clear indication of regulators' expectations which will give banks the confidence to move ahead with DLT-related projects. Adoption of DLT will be critical for all financial institutions and we expect at some point it will become mandatory as regulators look to ensure that banks are 'future proof' and able to interact with financial markets in the future. All banks in Hong Kong should therefore have a DLT strategy.

Risk management considerations related to the use of DLT

Governance

Board and Senior Management's Responsibility

AIs should have sufficient staff with expertise in DLT available to support the implementation process, and management should be equipped with adequate knowledge to review and assess the AI's strategy and approach to DLT adoption when proposing DLT initiatives.

Given the rapid pace of technological advancements, AIs should keep in view the need to offer regular training to staff, and re-configure work processes to keep current with the latest developments.

Where a DLT solution has customer-facing elements, an AI should review the need to make DLT-specific consumer education efforts and/or update existing dispute-handling procedures, as well as redress and compensation mechanisms.

The HKMA expects an AI's board and senior management to put in place adequate systems and controls to mitigate the risks from DLT adoption including risks related to governance. An AI should review and update its relevant policies and frameworks to reflect DLT-specific factors as needed. These policies and frameworks include:

- Technology risk management (eg change management, access control, network security)
- Business continuity planning (BCP)
- Outsourcing

KPMG Insights

An appropriate governance framework is essential to the safe and effective implementation of the new technology. Although DLT technology may still be in its infancy, AIs should not overlook the need to upskill and develop DLT capabilities and frameworks today. Capabilities and frameworks are developed over time, AIs should recognise the time it may take to sufficiently be ready for a future transition to a DLT-based system.

At this initial stage of introducing DLT into the business, we recommend AIs to have a dedicated committee to oversee and support DLT initiatives.

AIs should prepare now by undertaking small DLT-linked projects and ensuring their people receive appropriate training to develop the necessary skills and experience. This will ensure that sufficient staff with DLT expertise will be ready and will help future-proof the organisation.

In addition to the policies and frameworks suggested by HKMA, AIs also need to ensure they have designed and implemented appropriate internal controls including in relation to technology risk management and capacity monitoring.

Risk management considerations related to the use of DLT

Application design and development

KPMG has summarised the key aspects below:

1. Appropriate selection of DLT Network for given application

- AIs must comprehend various DLT networks (permissionless, private-permissioned or public-permissioned) and select the suitable option based on the application's nature and risks. If higher-risk choices are made, compensating risk management controls should be implemented.

2. "Fit for purpose" Smart Contracts

- AIs must adeptly manage smart contract vulnerabilities, including operational, third-party, and legal risks. It is crucial to establish a strong governance framework for the introduction and updating of smart contracts, incorporating due diligence reviews and risk management controls.

3. Understanding and Mitigation of Legal Risks

- AIs should understand and mitigate potential legal risks arising from the evolving legal basis for applying DLT to traditional financial activities, such as issues related to settlement finality and the legal standing of tokenised products.

4. Effective Management of Third Party-related Risks

- AIs must assess and handle risks associated with third parties engaged in the DLT arrangement, such as the trustworthiness and reliability of node operators. Appropriate risk mitigating measures should be implemented when deficiencies are identified.

5. Safe Enablement of Interoperability and Connectivity

- AIs should design their DLT-based systems to be compatible and able to communicate with both traditional and other DLT-based solutions, while ensuring secure connections to protect against cyberattacks, vulnerabilities and data leakage.

KPMG Insights

Recognising the rapid innovation within DLT infrastructure, AIs should consider the latest developments on a risk-by-risk basis and evaluate how risks can be addressed holistically through the combination of technologies at the AI's disposal. First and foremost, AIs should consider interoperability with current banking infrastructure including the application of validiums in the Ethereum Virtual Machine (EVM) compatible environment.

AIs should not simply choose between the different types of DLT - public vs private, permissioned vs permissionless - but rather should conduct a risk assessment, and identify the mechanisms and controls that can mitigate such risks. For example, a public DLT infrastructure may not necessarily be inappropriate to protect the security and privacy of certain data if a Zero Knowledge architecture is adopted, and there are already innovations in this space such as the Ethereum layer 2 rollup zkSync.

Adding to the above, AIs should ensure that there is a process in place to keep the organisation up to date on developments in smart contract standards. Leveraging the industry's research and experience could be a key driver towards standardisation and interoperability. In addition, if AIs look beyond the infrastructure, there have been a number of recent developments in Smart Contract Standards such as ERC3643, which provides a frame for anonymous yet verifiable user credentials. These should be explored and assessed to determine how they can contribute to the future of banking infrastructure.

We believe interoperability and common standards are key to the successful adoption of any new technology. As such we encourage the industry to work together on such topics. In exploring these topics, all stakeholders should be involved, including public infrastructure developers, private infrastructure developers, financial institutions, academics, regulators among other ecosystem participants.

Innovation in DLT is progressing rapidly, and the traditional financial services sector can leverage developments in interoperability standards, smart contract standards, and DLT-related privacy and security standards by the public and research sector to arrive at a holistic view for future road mapping.

Risk management considerations related to the use of DLT

On-going maintenance and monitoring. AIs should:

Cybersecurity

Have effective mechanisms to counter both DLT-specific cyber risks (eg 51% attacks) and common cybersecurity threats (eg DDoS attacks). AIs should stay vigilant **against** emerging threats and update their response capabilities accordingly.

Private Key Management

Manage private keys with robust policies and procedures in place outlining the nature and risks of the application, the underlying assets and the duties assumed by the AI.

Data Privacy and Management

Ensure compliance with data privacy and protection requirements of DLT-based ledgers.

Introduce mitigating measures to manage complications arising from the unique nature of DLT arrangements.

Contingency planning and testing arrangements

Tailor testing scenarios and contingency arrangements specific to DLT in business continuity planning, taking into account the unique operating dynamics of DLT networks.

KPMG Insights

AIs should form working groups to leverage developments and innovation by the academic and public community on topics of security, key management, infrastructure and standards that will facilitate compliance, and continuity planning and testing as they relate to a DLT-enabled environment. The selection of infrastructure (eg private DLT, public DLT, validiums, rollups etc) could dictate how the AI should approach such topics.

AIs should have robust policies and procedures in place to securely manage private keys, with a level of security appropriate for the nature and risks of the application, and the duties assumed by the AI. Custodians of digital assets should implement strict access controls, cold storage and offsite backups, and further mechanisms of controls should be in place for the traditional asset represented by any on-chain tokens.

AIs should ensure compliance with data privacy and protection requirements, even when data is stored on DLT-based ledgers. Mitigating measures should be introduced to manage complications arising from the unique nature of DLT arrangements, such as difficulties with data retention, confidentiality and localisation.

As DLT adoption expands, the need for robust cybersecurity increases. Decentralisation is a unique advantage of blockchain, where data is stored across multiple nodes without central authority control. While this makes it challenging for attackers to compromise the network, it also poses major security concerns.

Another key area for cybersecurity is interoperability. Cyber attacks in the crypto sector have focused on the connectivity points. The growing number of platforms creates a demand for interoperability, resulting in higher risk, particularly with open-source DLTs where there is a possibility of different versions or forks of the technology being created. This can lead to fragmentation of security standards, creating potential vulnerable points of attacks, particularly around connectivity points.

Key challenges related to the adoption of new technologies

Roadblocks:

With reference to *HKMA Fintech Adoption Study (2023)*, KPMG has summarised the major roadblocks hindering the adoption of fintech solutions (such as DLT) suggested by fintech users and providers respectively:

Fintech user

1. Lack of overall awareness of the solution

- Employees are not aware of the fintech solution that is available within the financial institution

2. Integration difficulties

- The process of integrating new fintech solutions into existing systems and workflows can be complex and time-consuming

3. Insufficient resources to offer technical support and assistance

- There are insufficient resources to fully integrate new fintech solutions, as coordination and compatibility with legacy infrastructure within the financial institution are needed

Fintech provider

1. Lack of user understanding

- There is a limited understanding of how to incorporate the fintech solution into existing daily practices

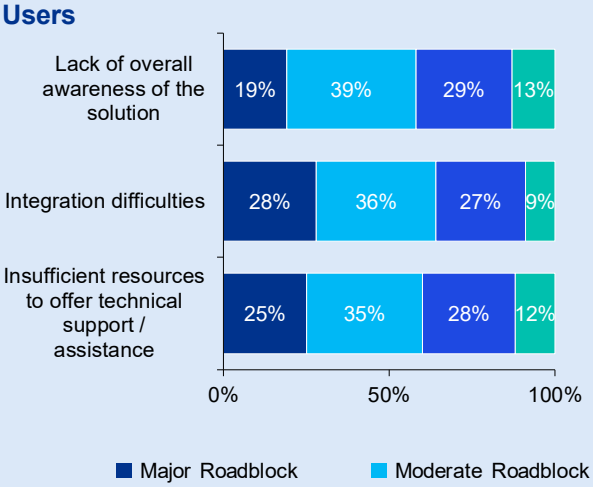
2. Organisational inertia

- Organisations can be reluctant to change due to familiarity with existing tools and processes

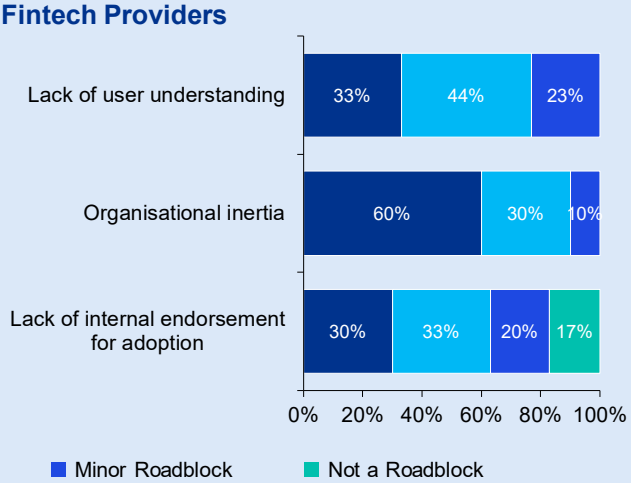
3. Lack of internal endorsement for adoption

- Post-implementation endorsement may be insufficient due to the required time, budget and resources for IT departments

Major Activation Roadblocks from Fintech Users



Major Activation Roadblocks from Fintech Providers



Major Roadblock | Moderate Roadblock | Minor Roadblock | Not a Roadblock

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

Risks related to the use of DLT

Key Emerging Risks

Data Integrity Risk

Risk:

- Risk to the accuracy and validity of the data stored on DLT
- Manipulation of data, fraudulent transactions, compromised audit trails

Potential Mitigation:

- Implement stringent data validations and verification mechanisms such as cryptographic techniques and digital signatures

Scalability Issues

Risk:

- Limitations in the scalability of the DLT network with the banks business model
- Slow transaction processing, congestion, bottlenecks in the bank operations

Potential Mitigation:

- Advancement in DLT technology is currently addressing this issue (for example, certain L2 rollups can theoretically accommodate thousands of transactions per second). Further design and operating enhancement should be studied

Smart Contract Vulnerabilities

Risk:

- Flaws in blockchain-based smart contracts such as vulnerable codes or bugs
- Exploitation of vulnerabilities, unauthorised manipulation of transactions, financial losses, contract disputes

Potential Mitigation:

- Conducting extensive code reviews and security audits of smart contracts may identify potential vulnerabilities
- Using accepted and verified smart contract standards
- Thoroughly testing smart contracts using various techniques helps identify potential cases and assess contract behaviours, including stress testing

Privacy Challenges

Risk:

- Difficulties in ensuring user privacy
- Exposing transaction details. Compromising investor confidentiality, regulatory non-compliance

Potential Mitigation:

- Robust encryption safeguards data from unauthorised access, eg homomorphic encryption enables computations on encrypted data without decryption
- Implementing permissions and privacy-enabled DLT networks or smart contract standards may help ensure sensitive information is only shared with trusted entities

Lack of Interoperability

Risk:

- Difficulties in integrating diverse platforms
- Incompatibility, data fragmentation, hindrance of cross-platform transactions

Potential Mitigation:

- Implementing well-defined communication protocols will enable seamless communication and data exchange between different DLT platforms
- Adoption of common standards and protocols across different DLT platforms to develop interoperability

How KPMG can help

KPMG is a market leader in providing virtual asset advisory in Hong Kong. We have a team of seasoned experts with deep knowledge of the virtual assets space ready to support you in your adoption of DLT-based solutions with management strategies of the associated risks

Implementation Assessment

- Review and assess your current strategy and recommend an efficient approach for adopting DLT into the current business models
- Perform gap analysis of policies and frameworks to ensure DLT-specific factors are governed and recommend appropriate controls for the corresponding risk types
- Review the technology design and development and provide advice on interoperability and connectivity

Implementation Support

- Planning and managing the technical and functional implementation of DLT into your current practice
- Support the implementation of appropriate DLT-specific frameworks, policies, controls and processes
- Tailor contingency planning and testing based on your chosen DLT to your business model

Business Support

- Decompose risks arising from DLT applications, i.e. tokenized products, and provide recommendations and implementation support
- Ensure effective mechanisms for IT and cybersecurity are in place to counter both DLT-specific cyber risks and common threats.
- Perform regular assessments and health checks to ensure continued compliance with HKMA expectations.

Contact us

Tom Jenkins
Head of Governance, Risk and Compliance
KPMG China
T: +852 2143 8570
E: tom.jenkins@kpmg.com

Stanley Sum
Head of Digital Enablement
KPMG China
T: +852 2143 8808
E: stanley.sum@kpmg.com

Robert Zhan
Director,
Virtual Assets and DLT
KPMG China
T: +852 3927 5731
E: robert.zhan@kpmg.com

Lanis Lam
Partner, Technology Consulting
KPMG China
T: +852 2143 8803
E: lanis.lam@kpmg.com

Angel Mok
Partner,
Technology Consulting
KPMG China
T: +852 3927 5804
E: angel.mok@kpmg.com

Lancer Hui
Manager,
Financial Risk Management
KPMG China
T: +852 2826 7104
E: lancer.hui@kpmg.com

kpmg.com/cn/socialmedia