HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C

16 April 2024

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Risk management considerations related to the use of distributed ledger technology

I am writing to share with the industry the key risk management considerations that the HKMA has regard to when it reviews proposals of authorized institutions (AIs) involving the use of distributed ledger technology (DLT).

Since the Government published its *"Policy Statement on Development of Virtual Assets (VAs) in Hong Kong"* in 2022, the HKMA has noted growing interest from AIs to explore how they can apply the DLT that underlies the VA ecosystem to traditional financial market operations. As these explorations have gathered pace, an increasing number of AIs have - consistent with the HKMA's supervisory expectations set out in its circular letter of 28 January 2022 - reached out to seek the HKMA's views on their planned initiatives.

The HKMA is supportive of AIs adopting DLT-based solutions so long as they can adequately manage the associated risks. Specifically, it has been encouraging banks to study the potential of taking "tokenised" deposits. To lend further support to these explorations, the HKMA considers it useful to provide more clarity on the key risk management considerations that it has regard to when reviewing the DLT-related proposals of AIs.

In line with its risk-based and technology-neutral approach to supervision, the HKMA's focus when reviewing these proposals is on ascertaining whether an AI has put in place adequate systems and controls to manage those additional risks that may arise due to DLT adoption. Although the HKMA's exact considerations will vary based on the specific solution under review, there are some common risk

areas that are generally relevant to DLT adoption. Noting AIs may wish to take these into account when designing and developing their DLT solutions, the HKMA has prepared a note setting out these key supervisory considerations **(Annex)**. AIs are encouraged to take into account these considerations when preparing their DLT-related submissions.

In leveraging the guidance, AIs should note that the considerations are non-binding, non-exhaustive and will continue to evolve as the market and related technologies develop. For instance, the considerations currently focus more on those products and activities that are receiving the greatest market attention and interest at present (e.g. tokenisation of traditional assets and liabilities, and the provision of supporting services for these tokenised products) to increase their utility and relevance to AIs today.

Should you have any questions about this circular, please email dlt_supervision@hkma.gov.hk.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)

Annex

Risk management considerations related to the use of DLT

Introduction

- Since the Government published its *"Policy Statement on Development of Virtual Assets (VAs) in Hong Kong"* in 2022, the HKMA has noted growing interest from AIs to explore how they can apply the DLT that underlies the VA ecosystem to traditional financial market operations. As these explorations have gathered pace, an increasing number of AIs have - consistent with the HKMA's supervisory expectations set out in its circular letter of 28 January 2022 - reached out to seek the HKMA's views on their planned initiatives.

- The HKMA is supportive of AIs adopting DLT-based solutions so long as they can adequately manage the associated risks. In line with its risk-based and technology-neutral approach to supervision, the HKMA's focus when reviewing AIs' DLT-related proposals is on ascertaining whether an AI has put in place adequate systems and controls to manage those additional risks that may arise due to DLT adoption.

- Although the HKMA's exact considerations will vary based on the specific solution under review, there are some common risk areas that are generally relevant to DLT adoption. To facilitate AIs' adoption of DLT solutions, the HKMA has set out in this note: (i) the key issues that it will typically consider when evaluating an AI's DLT-related proposals; and (ii) the competencies and conditions that it would generally expect an AI to demonstrate and/or fulfil under each area.

- These considerations are non-binding, non-exhaustive and will continue to evolve as the market and related technologies develop. Accordingly, while AIs may refer to them as reference when designing and developing their DLT-related solutions, the HKMA's detailed supervisory expectations will continue to be discussed with AIs on a bilateral basis, to ensure that they are suitable for the specific case at hand.

Key considerations

Governance

1. Board and senior management assume full responsibility for an AI's adoption of DLT and for adequately managing related risks - Given its focus on decentralisation, DLT adoption involves not only the novel application of technology but also untraditional governance philosophies. When implementing DLT solutions, AIs may encounter a range of new DLT-specific risks, including those related to governance[1]. Accordingly, the HKMA would expect an AI's board and senior management to put in place adequate systems and controls to mitigate these risks. As part of this, an AI should review and update its relevant policies and frameworks to reflect DLT-specific factors as needed. These policies and frameworks include amongst others, technology risk management (e.g. change management, access control, network security), business continuity planning (BCP), and outsourcing. With regard to internal capacity, it should be apparent that an AI has sufficient staff with expertise in DLT available to support the implementation process, and that its management is equipped with adequate knowledge to review and assess the AI's strategy and approach to DLT adoption. 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 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.

Application design and development

2. Right DLT network selected for a given application – The way that a DLT network is structured and governed (e.g. permissionless, private-permissioned or public-permissioned) has a direct bearing on the security, stability, scalability and resilience of the network. The HKMA would therefore expect an AI to fully understand the different types of DLT networks available and make an appropriate choice based on the nature and risks of the application in question, and with consideration for its own legal and regulatory responsibilities. If an AI decides to pursue design choices that may involve higher risks, the HKMA would expect it to have critically evaluated and ensured the availability of compensating risk management controls. For instance, given its open membership and generally greater

[1] For instance, these include the possibility of having to share solution ownership responsibility with other stakeholders, which may potentially affect the AI's autonomy over changes.

susceptibility to malicious actors, permissionless networks may not be a natural first choice for applications involving the transfer of sensitive data. However, assuming an AI can find appropriate measures to manage the associated risks (e.g. cryptographic solutions like zero-knowledge proof or a mix of on and off-chain solutions), these networks need not be ruled out by default for such applications.

3. Smart contracts are "fit for purpose" – While smart contracts can offer efficiency benefits through automation, they may not be appropriate for all business scenarios or should only be deployed with customised controls. For instance, unchecked automation may not be preferred in situations that usually involve some degree of human judgement (e.g. complex loan assessments), and a smart contract may only be appropriate if manual intervention options can be built in. Where an AI deems it appropriate to use smart contracts, the HKMA would expect it to effectively manage the vulnerabilities commonly associated with smart contracts. These include operational risk (e.g. non-malicious coding errors and cyberattacks), third-party risk (e.g. the reliability of "oracles" used to source external data) and legal risks (e.g. whether the legal foundation of the smart contract is established). To this end, AIs are advised to put in place a rigorous governance framework for introducing and updating smart contracts. An effective framework would, amongst others, assess the suitability of adopting smart contracts for a given scenario, require due diligence reviews of the smart contracts that will be deployed from operational, technological and legal perspectives, ensure the necessary risk management controls are incorporated in the final designs of the smart contracts, and cover procedures/considerations for upgrading the smart contracts[2]. Where necessary, AIs should consider engaging professional advice, including suitable third parties, to conduct audits on the smart contracts before they are deployed.

4. Understand and mitigate potential legal risks – The legal basis for applying DLT to traditional financial market activities is still evolving. For example, with respect to the issuing and trading of tokenised products, while "settlement finality" under traditional financial systems is a clear and well-defined point in time that is underpinned by a strong legal foundation, the point at which settlement finality is reached under DLT arrangements may be less clear-cut given the use of consensus-based validation mechanisms. Subject to how a traditional product is "tokenised", there may also be changes

[2] With respect to upgrading smart contracts, AIs may wish to pay particular attention to issues surrounding the deployment process, backward compatibility and data migration. For instance, an AI should, as appropriate, assess whether the upgrade will have any impact on existing users and applications, and implement a strategy for migrating data from the old contract to the upgraded version to preserve data integrity and continuity.

to its legal standing and subsequent regulatory treatment. AIs should be aware of these possible legal grey areas, seek professional advice where necessary and put in place measures during the design process to mitigate the ensuing legal risks.

5. Effectively manage third party-related risks – The HKMA would expect an AI, in the process of evaluating whether to adopt a DLT solution, to have reviewed and satisfied itself that it can manage the risks that third parties involved in the DLT arrangement may present. In particular, given DLT networks operate on consensus-based mechanisms and therefore rely on node operators to validate and confirm changes to the ledger, an AI should, with regard to the application at hand, duly consider whether the node operators are sufficiently trustworthy, reliable and diverse. Where deficiencies are noted, AIs should put in place adequate risk compensating measures. An AI would also be expected to duly consider the impact that the design of the DLT network may have on its ability to adequately manage third party-related risks. For instance, permissionless networks, by design, have open membership and allow any participants, including pseudonymous ones, to become validators. In these cases, AIs would have less control over the involved third parties and it would likely be inappropriate for AIs to adopt this type of DLT solution for highly critical or sensitive functions unless they are able to adopt adequate compensating risk management controls.

6. Safely enable interoperability and connectivity – The HKMA would expect AIs to, as far as practicable, design their DLT-based systems to be compatible and able to "communicate" with both traditional and other DLT-based solutions. This may help limit market fragmentation, support operational efficiencies and ensure the longer-term relevance of the DLT solution. For instance, the HKMA has been encouraging banks to explore the potential of deploying DLT to take deposits (i.e. "tokenised" deposits), as such deposit-taking activity is permissible under the Banking Ordinance. During the process, it has noted views from banks that a tokenised deposit that can only be used within an AI's own proprietary network may bring relatively less additional value to clients, compared to one that can be used for interbank transfers and to settle a variety of tokenised assets stored on different DLT networks. With this in mind, AIs are advised to consider adopting technical standards that are more widely accepted by industry to support compatibility. As with any interbank initiatives, AIs should ensure that these connections are made in safe and secure ways, including to protect them from cyberattacks, security vulnerabilities and risks of data leakage.

On-going maintenance and monitoring

7. Establish level of cybersecurity commensurate with traditional technology applications - DLT-based applications should enjoy commensurate levels of cybersecurity as those with traditional underlying technology. The HKMA would expect AIs to have effective mechanisms in place for countering both DLT-specific cyber risks (e.g. 51% attacks) as well as other common cybersecurity threats (e.g. distributed denial of service (DDoS) attacks). They should also stay vigilant to the emerging modus operandi of threat actors and developments in novel technologies that may affect the security of DLT applications (e.g. quantum computing), and regularly update their response capabilities.

8. Securely manage private keys – An AI's access to and responsibility for safeguarding private keys will vary based on the purposes for which it adopts DLT applications and whether it offers certain services. Given the varied possibilities, the HKMA would, as a general rule, expect AIs to demonstrate that robust policies and procedures are in place to provide a level of security to any private keys held or under their management that are appropriate for the nature and risks of the application, the underlying assets associated with the keys, as well as the duties assumed by the AI. For instance, an AI that serves as a custodian for its client's digital assets would generally be expected to put in place more rigorous security procedures to ensure that the associated private keys (and seeds as applicable) are securely generated, stored and backed up at all times. This may involve amongst others, implementing controls to strictly limit access to the keys to authorized personnel, utilising cold storage and developing offsite backups and other contingency arrangements[3].

9. Ensure compliance with data privacy and protection requirements – Prevailing data privacy and protection requirements continue to apply regardless of whether the data is stored on centralised or DLT-based ledgers. AIs should therefore demonstrate that they have adequate systems and controls in place to ensure their continued compliance with the requirements. Where needed, mitigating measures should be introduced to manage complications that may arise due to the unique nature of DLT arrangements. These may include, amongst others, difficulties complying with requirements related to data retention (e.g. given the immutability of data on a DLT network), guaranteeing personal data confidentiality (e.g. in light of the transparent nature of certain DLT networks) and data localisation (e.g. in the event that a DLT network is spread out across multiple jurisdictions).

[3] AIs may wish to refer to the HKMA's separate guidance on the *"Provision of Custodial Services for Digital Assets"* issued on 20 February 2024.

10. Tailor contingency planning and testing arrangements – Where an AI adopts DLT for critical functions, the HKMA would expect it to include testing scenarios (e.g. common DLT cyberattacks, loss/theft of private keys, and possibility of "forking") and contingency arrangements that are specific to DLT in its BCP. In particular, AIs would be expected to be aware of and take into account the unique operating dynamics of DLT networks, and especially those that may affect system and capacity management (e.g. the possibility for validation congestion and a need to pay higher fees to expedite urgent transactions) when conducting the planning and testing[4]. In contemplating more extreme scenarios, AIs should also consider the need for backup options to cater for situations where the DLT solution may become temporarily or permanently unavailable.

[4] For instance, an AI may wish to consider volume testing to verify that the system capacity of the DLT network remains adequate even under stress conditions.