HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref: B1/15C
G16/1C

20 February 2024

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Sale and distribution of tokenised products

I am writing to set out the supervisory standards expected of authorized institutions ("AIs") in the sale and distribution of tokenised products to their customers.

Coverage

This circular covers tokenised products which, for the purpose of this circular, refer to digital representation of real-world assets[1] using distributed ledger or similar technology, but does not apply to those regulated under the Securities and Futures Ordinance ("SFO") and governed by the relevant requirements[2] issued by the Securities and Futures Commission ("SFC") and the Hong Kong Monetary Authority ("HKMA") from time to time.

General principle

The HKMA is supportive of AIs' initiatives on tokenisation, and is encouraged by the progress the industry has made so far. The HKMA considers it timely to provide guidance on activities related to tokenised products, thereby providing

[1] For example, tokenised non-SFO-regulated structured investment products and tokenised spot precious metal. For the avoidance of doubt, this circular does not apply to stablecoins. In respect of placing of tokenised deposits by customers, AIs should also comply with the standards set out in this circular.

[2] For example, the "Circular on intermediaries engaging in tokenised securities-related activities" issued by the Securities and Futures Commission on 2 November 2023.

the banking industry with regulatory clarity to support continued innovation and realisation of benefits that may be brought by tokenisation, with appropriate safeguards from consumer/investor protection perspective.

As a general principle, the prevailing supervisory requirements and consumer/investor protection measures for the sale and distribution of a product are also applicable to its tokenised form as it has terms, features and risks (other than any risks arising from tokenisation itself) similar to those of the underlying product.

As illustrations of the above general principle:

(i) AIs distributing a tokenised non-SFO-regulated structured investment product are expected to adopt the prevailing supervisory requirements and investor protection measures applicable to the selling of that non-SFO-regulated structured investment product set forth by the HKMA; and

(ii) AIs distributing tokenised gold are expected to follow the same requirements as those governing the selling of gold, which include the Code of Banking Practice, the Treat Customers Fairly Charter as well as any other applicable requirements issued by the HKMA.

While some tokenised products are basically traditional products with a tokenisation wrapper, there could be situations where the nature, features and risks of a tokenised product are altered by how the product is structured and arranged in the tokenisation process. For example, the arrangement for tokenisation of fractionalised interests in an asset may amount to a collective investment scheme. Hence, AIs should ensure that they evaluate and understand the terms, features and risks of each tokenised product, and should exercise professional judgment to ascertain the applicable legal and regulatory requirements. In addition to the expected standards set out in this circular, AIs are reminded to also comply with all the applicable legal and regulatory requirements when selling and distributing tokenised products. Before selling and distributing a tokenised product to customers, AIs should put in place adequate systems and controls to ensure that all the applicable requirements are complied with, and implement appropriate additional internal controls to

address the specific risks and unique nature of the tokenised product. If in doubt, AIs should seek professional advice.

Along with the above general principle, AIs are expected to implement the consumer/investor protection measures in respect of due diligence, disclosure and risk management for tokenised products as set out in the following sections.

(A) Due diligence

In line with the requirements for the underlying products, AIs should conduct adequate due diligence and fully understand the tokenised products before offering them to customers and on a continuous basis at appropriate intervals, having regard to the nature, features and risks of the products.

AIs should act with due skill, care and diligence, and perform due diligence based on all the available information to identify and ensure that they have thorough understanding of the terms, features and risks of the tokenised products (including those relating to the underlying product and those relating to the technology aspects of tokenisation).

AIs should conduct due diligence on the issuers of the tokenised products and their third-party vendors/service providers (e.g. tokenisation platform providers) involved in the tokenisation arrangement, including their experience and track record, as well as the features and risks arising from the tokenisation arrangement. AIs should understand and be satisfied with the systems and controls put in place by the issuers and their third-party vendors/service providers, including whether and how the new risks relating to ownership[3] and the underlying technology of the tokenised products are managed. There should be appropriate arrangements for technology audits (in particular, smart contract audits[4]), proper policies, procedures, systems and controls (including adequate administrative controls[5]) in regard to the operation of the tokenised products, such as private key management and safeguards against theft, fraud, errors and omissions, hacking and other cybersecurity risks. There should also be effective contingency plans in the event of, for example, distributed ledger technology

---

[3] For example, how ownership right is transferred and recorded.

[4] Where smart contract is used in the operation of the tokenised products.

[5] For example, restriction on transfer, minting and burning functions, transaction reversals or redemption procedures, as applicable.

("DLT") network failure, cyber-attacks, unauthorised transfer and loss of private keys for access to tokenised products. The interoperability between DLT networks and the systems of the issuer and other parties such as custodians; the robustness of the DLT network adopted for the tokenised products, including the potential impact of such DLT network in terms of, for example, security, privacy, vulnerability, and scalability; and legal and regulatory status of the tokenised product should also be considered. AIs should assure themselves of the existence of the asset which backs the digital token as well as the rights attached thereto.

It is noted that AIs may also issue tokenised products themselves. If an AI issues or is substantially involved in the issuance of a tokenised product, it should take into account the considerations stated in the paragraphs above regarding due diligence on the issuers and third-party vendors/service providers involved in the tokenisation arrangement. In addition, the AI should consider the most appropriate custodial arrangement for the tokenised product taking into account the features and risks of the tokenised products, including but not limited to the relevant considerations where permissionless tokens on public-permissionless DLT network are used.

(B) Product and risk disclosure

AIs are expected to act in the best interests of their customers and make adequate disclosure of the relevant material information about a tokenised product, including key terms, features and risks, to enable the customer to make an informed decision. When offering a tokenised product, AIs should disclose material information on the tokenisation arrangement according to the circumstances of the tokenised product, for example:

- Risks posed by the DLT network utilised (including potential uncertainty about operational and security issues arising from the evolving technology) as well as possible lack of interoperability of the DLT network with other networks or infrastructures

- Vulnerability to cybersecurity threat, such as hacks and security breaches

- Any limitations imposed on transfers of the tokenised product

- Where applicable, risks related to the use of smart contracts (including the risk of vulnerabilities or security flaws in smart contracts) as well as whether smart contract audit has been conducted before the deployment of the smart contract

- Potential legal uncertainty around areas such as ownership rights and settlement finality on a DLT network

- Whether off-chain or on-chain settlement is final

- Key administrative controls, and contingency and backup plans in the events of system malfunction, DLT network failure and other unforeseen circumstances

- Where applicable, custodial arrangement and risks associated with the custody of the tokenised product

- Where applicable, risks associated with reliance on third-party vendors/service providers and technologies

All the information given to customers should be accurate, fair and not misleading, and presented in a clear, concise and user-friendly manner that is easily accessible by customers. This includes information contained in advertising messages and marketing materials, whether online, in paper form, or through social media platforms. AIs should use plain language and avoid highly technical terms or jargon in their disclosures to customers.

(C) Risk management

Proper policies, procedures, systems and controls should be put in place to identify and mitigate the risks arising from tokenised product-related activities. AIs should ensure that appropriate risk management frameworks for the selling activities in respect of tokenised products are in place, which should include policies and procedures for risk management, internal control, complaint handling, compliance, internal audit and business contingency planning.

AIs should allocate resources to ensure that their management and relevant staff have the necessary expertise to perform their duties in conducting activities relating to tokenised products, including their capability to explain the tokenised products to customers and to manage the risks arising from tokenisation.

(D) Custodial services

AIs that are also providing custodial services of tokenised products should meet the expected standards on digital asset custody as issued by the HKMA from time to time.

Implementation

Before engaging in tokenised product-related activities, AIs are reminded to implement adequate policies, procedures, systems and controls to ensure compliance with the requirements set out in this circular and other applicable requirements, and discuss with the HKMA in advance. The HKMA will continue to keep in view the regulatory landscape and global developments in the tokenised markets, and provide further guidance to AIs as appropriate.

If there is any question on this circular, please contact Ms Karin Lee at 2878-1604 or Ms Katy Chan at 2878-1210.

Yours faithfully,

Alan Au
Executive Director (Banking Conduct)

c.c. SFC (Attn: Keith Choy, Interim Head, Intermediaries)