Appendix

Part A: List of non-exhaustive factors for intermediaries' consideration

(a) the experience and track record of the third-party vendor(s)/service provider(s) used in the tokenisation arrangement of the Tokenised Securities (eg, tokenisation technology developers, tokenisation platform providers, wallet service providers/custodians and anti-money laundering solutions);

(b) the technical aspects of the Tokenised Securities, in particular:

(i) smart contract deployed (if any);

Note: For example, an intermediary should consider whether appropriate technology audits have been conducted in respect of the technical aspects of the Tokenised Securities[1]. In particular, if a smart contract is deployed in the Tokenised Securities' operation, the intermediary may need to ensure a smart contract audit has been conducted on the smart contract. If the intermediary relies on a smart contract audit conducted by a third party, it should be able to demonstrate that it is reasonable to rely on such smart contract audit. The smart contract audit should focus on reviewing whether the smart contract is not subject to any contract vulnerabilities or security flaws with a high level of confidence.

(ii) robustness of the DLT network (eg, the security infrastructure of its blockchain protocol, the size of the blockchain and network, and especially how resistant it is to common attacks, including a 51% attack or similar attacks which would have an impact on transaction finality, the type of consensus algorithm, and the risks relating to code defects, breaches, exploits and other threats relating to the Tokenised Securities and its supporting blockchain, the international/industry best practices and protocols that apply to them, and any adverse incidents relating to the DLT used and whether they have been resolved);

(iii) inter-operability issues between DLT networks and the back-end systems of the product issuer and other parties throughout the security lifecycle (such as custodians/wallet service providers);

(iv) robust and properly maintained policies and procedures, systems and controls underpinning the operation of the Tokenised Securities to manage eg, the private key and risks of theft, fraud, errors and omissions, and cybersecurity risks, etc.;

Note: For example, adequate administrative controls in the form of transfer restrictions, mint-and-burn mechanism, transaction reversals or redemption

[1] Where the blockchain is merely used as a secondary record in certain tokenisation models, a proper application of the underlying technology may still require appropriate technology audits.

procedures should be implemented to protect investors' ownership interest, which is of particular importance for Tokenised Securities deployed on public-permissionless networks.

(c) the legal and regulatory status associated with the Tokenised Securities, in particular:

(i) legal position on "settlement finality" (which generally means the point where a transaction is considered as finally settled, regardless of whether the sending participant has become insolvent or transfer orders have been revoked);

(ii) enforceability of the Tokenised Security and any security interest attached to the Tokenised Securities (as applicable);

(iii) enforceability of any rights extrinsic to the Tokenised Securities and the potential impact of the Tokenised Securities' trading activity on the underlying markets;

Note: For example, whether the ownership interest of the underlying assets of the Tokenised Securities are legally valid under the applicable governing laws, whether there are regular reconciliations between the records for the extrinsic rights and the records for the distributed ledger tokens, or whether any encumbrance affects the extrinsic rights.

(iv) regulatory status of a Tokenised Security in Hong Kong and whether regulatory approval under the relevant laws is required;

(d) business continuity planning (eg, redeployment plans to migrate DLT-related records to a different blockchain) for DLT-related events which are not adequately addressed with other measures;

(e) appropriate measures to address data privacy risks (eg, as public blockchains store transaction data publicly, this may expose sensitive information of token holders if their identities are revealed); and

(f) money laundering and terrorist financing risks associated with the Tokenised Security (eg, whether there are administrative controls over the Tokenised Securities being transferred to parties which have not undergone know-your-client and anti-money laundering procedures).

Part B: Additional considerations on the custodial arrangement for bearer form Tokenised Securities using permissionless tokens on public-permissionless networks

Intermediaries should consider the following non-exhaustive factors in ascertaining whether the custodial arrangements are appropriate and robust enough to effectively mitigate risks associated with Tokenised Securities in bearer form using permissionless tokens on public-permissionless networks:

(a) the immobilisation[2] of the Tokenised Securities with central custody;

(b) the time required to transfer the Tokenised Securities;

(c) the security of the custodial facility, ie, whether there are adequate safeguards in place to protect the facility from external threats, including cyberattacks or the ability of the custodian to compensate for any loss of Tokenised Securities;

(d) the experience and track record of the custodian in providing custodial services for Tokenised Securities;

(e) the custodian's internal policies and procedures, systems and controls including those governing private key management to ensure the secure storage of the private keys;

(f) whether the custodian has appropriate segregation arrangements in place such that the Tokenised Securities are, throughout the custody chain, segregated from:

  (i) the assets of the custodian/sub-custodian; and

  (ii) the assets of other customers of the custodian (unless the Tokenised Securities are held in an omnibus client account);

(g) the financial resources of the custodian (ie, the custodian's ability to compensate its customers in the event of any loss of customers' Tokenised Securities);

(h) the custodian's management of actual and potential conflicts of interest;

(i) the custodian's operational capabilities and arrangements, for example, the "wallet" arrangements and cybersecurity risk management measures; and

(j) where the appointment of sub-custodians is allowed, the custodian would use due skill, care and diligence in the selection, appointment and monitoring of its sub-custodians.

[2] Generally, financial instruments are "immobilised" by being safekept with a custodian in such way that it is not possible for them to enter into circulation and by having the entitlement to them recorded with account-entry records and transferred with book entries.