Consultation paper | CP 24.01

February 2024

Cryptoasset Exposures

HONG KONG MONETARY AUTHORITY
香港金融管理局

Contents

I INTRODUCTION

1 Purpose

1 This consultation paper sets out the Hong Kong Monetary Authority's (HKMA) proposal for implementing new regulations on the prudential treatment of cryptoasset exposures.

2 The HKMA invites comments on the proposal of this paper by 6 May 2024. Please submit your comments to your industry associations or directly to the mailbox at cp24.01@hkma.gov.hk.

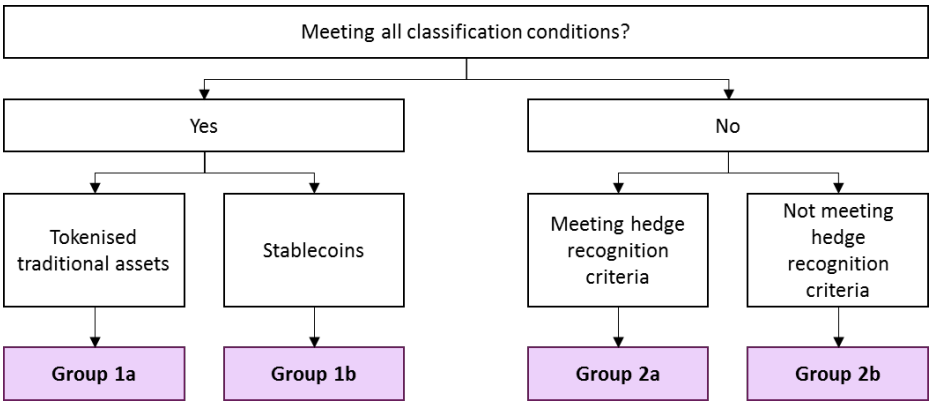
3 Following the close of this consultation, the HKMA will further refine its proposed revisions taking into account the feedback received.

2 Background

4 In December 2022, the Basel Committee on Banking Supervision (BCBS) issued its new standard *"Prudential treatment of cryptoasset exposures"*.[1] It aims at providing a robust and prudent global regulatory framework for internationally active banks' exposures to cryptoassets that promotes responsible innovation while preserving financial stability. Subsequently, the BCBS published two consultative documents "*Disclosure of cryptoasset exposures*"[2] and "*Cryptoasset standard amendments*"[3] in October 2023 and December 2023, respectively. So far, not all of the additional requirements proposed in the two consultative documents have been incorporated in this consultation paper. The HKMA will further update the local implementation proposal after the conclusion of the BCBS' consultation process.

5 Under the new standard, cryptoassets will be categorised into two broad groups. Group 1 cryptoassets consist of qualifying tokenised assets and stablecoins. They will generally be subject to the risk-based capital requirements of the existing Basel capital framework. Group 2 cryptoassets are cryptoassets that fail to meet all of the Group 1 classification conditions. These cryptoassets will be subject to a more conservative capital treatment.

[1] http://www.bis.org/bcbs/publ/d545.htm
[2] http://www.bis.org/bcbs/publ/d556.htm
[3] http://www.bis.org/bcbs/publ/d567.htm



3 Scope of Application

6 For the purpose of the prudential treatment of cryptoasset exposures, cryptoassets will be defined as private digital assets that depend on cryptography and distributed ledger technologies (DLT) or similar technologies. Digital assets are a digital representation of value, which can be used for payment or investment purposes or to access a good or service.

7 Dematerialised securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through DLT or similar technologies are considered to be within the scope of the prudential treatment and are referred to as tokenised traditional assets, whereas those dematerialised securities that use electronic versions of traditional registers and databases which are centrally administered are not within scope.

8 The prudential treatment of central bank digital currencies (CBDCs) is not covered by this new standard.

9 For the purposes of this consultation paper–

- the term “exposure” includes on- and off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks;
- although most parts of the new standard set out the capital and liquidity requirements in respect of Authorized Institutions’ (AIs’) direct exposures to cryptoassets, certain parts of the standard, such as the operational risk requirements in section 16 and the risk management and supervisory review in section 21, are also applicable to AIs’ cryptoasset activities, such as custodial services involving the safekeeping or administration of client cryptoassets on a segregated basis, that do not generally give rise to credit, market or liquidity requirements.

10 The references to the Banking (Capital) Rules (BCR) in this document are based on the version which takes into account the proposed amendments to the BCR for the implementation of the Basel III final reform package.

4 Implementation Timeline

11 The HKMA plans to work on the local implementation based on the following schedule and intends to put the new standards into effect no earlier than 1 July 2025.

	Legislative changes	Regulatory reporting
H2 2024	Preliminary consultation on the proposed amendments to the rules	
Q1 2025	Consultation on draft amendments to the rules	Industry consultation on draft revised banking return and completion instructions
Q2 2025	• Finalisation of revised rules taking into account industry comments • Gazetting of revised rules and tabling the rules at the Legislative Council for negative vetting	
No earlier than 1 July 2025	Revised rules coming into effect	

Table 1

12 As the prudential treatment of cryptoasset exposures interacts with various elements of the capital framework, it is likely to have impacts on, among other things, the capital charges, systems, data and resources of AIs. Those with plans to conduct cryptoasset-related business activities are therefore strongly recommended to consider the implications of implementation for their institutions and to start preparing a plan for the local implementation of the prudential treatment in due course.

5 Implementation Arrangements

13 The BCBS presents the prudential treatment of cryptoasset exposures as a comprehensive document while its various components will likely be integrated into

relevant sections of the Basel framework at a later stage. In terms of the local implementation, the HKMA will check the need for potential legislative amendments to various sets of rules, including the Banking (Capital) Rules, Banking (Disclosure) Rules, Banking (Liquidity) Rules and Banking (Exposures Limits) Rules. Where appropriate, technical provisions and supervisory guidance will also be set out in Code of Practices, Supervisory Policy Manuals, etc.

14 AIs, on an ongoing basis, are responsible for assessing whether the cryptoassets to which they are exposed are compliant with the classification conditions set out in section II and the hedging recognition criteria set out in paragraph 69. These assessments will determine whether the cryptoassets are classified as Group 1a, Group 1b, Group 2a or Group 2b. To this end, AIs must have in place the appropriate risk management policies, procedures, governance, human and IT capacities to evaluate the risks of engaging in cryptoassets and implement these accordingly on an ongoing basis and in accordance with established standards. AIs must fully document the information used in determining compliance with the classification conditions and make this available to the HKMA on request. In advance of any acquisition of a new type of cryptoassets, an AI must inform the HKMA of its classification assessment of the cryptoassets.

15 In case the HKMA does not agree with the assessments undertaken by AIs, the HKMA will have the power to override AIs' classification decisions.

16 To ensure consistent application across jurisdictions, the HKMA will routinely compare and share its supervisory information on AIs' assessments of cryptoassets against the classification conditions with regulators or supervisors in other jurisdictions.

II CLASSIFICATION CONDITIONS

17 The prudential treatment of an AI's cryptoasset exposures varies according to the regulatory classification of the cryptoassets. To determine the regulatory classification, an AI must screen the cryptoassets on an ongoing basis and classify them into two broad groups:

- Group 1 cryptoassets are cryptoassets that meet all the classification conditions in this section. It consists of:
  - Group 1a: tokenised traditional assets; and
  - Group 1b: cryptoassets with effective stabilisation mechanism.
- Group 2 cryptoassets are cryptoassets that fail to meet any of the classification conditions in this section. It consists of:
  - Group 2a: cryptoassets (including tokenised traditional assets, stablecoins and unbacked cryptoassets) that pass the Group 2a hedging recognition; and
  - Group 2b: all other cryptoassets (including tokenised traditional assets, stablecoins and unbacked cryptoassets) that fail the Group 2a hedging recognition criteria.

18 To be classified as Group 1a or Group 1b, cryptoassets must meet on an ongoing basis all four classification conditions mentioned in sections 6 to 9.

6 Classification Condition 1

19 The cryptoasset is either: (i) a tokenised traditional asset; or (ii) has a stabilisation mechanism that is effective at all times in linking its value to a traditional asset or a pool of traditional assets (i.e. reference assets).

20 Tokenised traditional assets can only meet classification condition 1 if they satisfy all of the following requirements:

- They are digital representations of traditional assets using cryptography, DLT or similar technology to record ownership.
- They pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset. In practice, this means the following for tokenised traditional assets.
  - Bonds, loans, claims on banks (including in the form of deposits),[4] equities and derivatives: the cryptoasset must confer the same level of legal rights as

[4] In certain jurisdictions bank-issued tokenised payment assets that are backed by the general assets of the bank and not by a pool of reserve assets may be referred to as "stablecoins". Notwithstanding

ownership of these traditional forms of financing (e.g. rights to cash flows, claims in insolvency, etc.). In addition, there must not be any features of the cryptoasset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenised) version of the asset.

– Commodities: the cryptoasset must confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.
– Cash held in custody: the cryptoasset must confer the same level of legal rights as cash held in custody.

21 Cryptoassets do not meet the condition set out in paragraph 20 if they:

- need to be redeemed or converted into traditional assets first before they receive the same legal rights as direct ownership of traditional assets; or
- involve additional counterparty credit risks relative to traditional assets through their specific construction.

22 Cryptoassets that have a stabilisation mechanism will only meet classification condition 1 if they satisfy all of the following requirements.

- The cryptoasset is designed to be redeemable for a predefined amount of one or more reference assets (e.g. HKD 1 or 1 ounce of gold) or cash equivalent to the current market value of the reference assets. The value of the reference assets to which one unit of the cryptoasset is designed to be redeemable is referred to as the "peg value".
- The stabilisation mechanism aims to minimise fluctuations in the market value of the cryptoassets relative to the peg value. In order to satisfy the "effective at all times" condition, AIs must have a monitoring framework in place to verify that the stabilisation mechanism is functioning as intended.
- The stabilisation mechanism enables risk management similar to the risk management of traditional assets, based on sufficient data or experience. For newly established cryptoassets, there may be insufficient data and/or practical experience to perform a detailed assessment of the stabilisation mechanism. AIs should document and make available to the HKMA on request the assessment they conducted and the evidence used to determine the effectiveness of the stabilisation mechanism, including the composition, valuation and frequency of valuation of the reserve assets and the quality of available data.

how they may generally be referred to within the jurisdiction, these assets may be included in Group 1a provided they meet all the requisite conditions and would not be assigned to Group 1b based solely on their commonly used local name.

- There exists sufficient information that AIs use to verify the ownership rights of the reserve assets upon which the stable value of the cryptoasset is dependent. In the case of underlying physical assets, AIs must verify that these assets are stored and managed appropriately. This monitoring framework must function regardless of the cryptoasset issuer. AIs may use the assessments of independent third parties for verification of ownership rights only if they are satisfied that the assessments are reliable.
- The cryptoasset passes the redemption risk test set out in paragraph 23 and the issuer is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements to the issuer.[5]

23 This paragraph sets out the redemption risk test for Group 1b cryptoasset. The objective of this test is to ensure that the reserve assets are sufficient to enable the cryptoassets to be redeemable at all times for the peg value, including during periods of extreme stress. To pass the redemption risk test, the AI must ensure that the cryptoasset arrangement meets the following conditions.

- Value and composition of reserve assets: the value of the reserve assets (net all non-cryptoasset claims on these assets) must at all times, including during periods of extreme stress, equal or exceed the aggregate peg value of all outstanding cryptoassets. If the reserve assets expose the holder to risk in addition to the risks arising from the reference assets,[6] the value of the reserve assets must sufficiently overcollateralise the redemption rights of all outstanding cryptoassets. The level of overcollateralisation must be sufficient to ensure that even after stressed losses are incurred on the reserve assets, their value exceeds the aggregate value of the peg of all outstanding cryptoassets.
- Asset quality criteria for reserve assets: for cryptoassets that are pegged to one or more currencies, the reserve assets must be comprised of assets with minimal market and credit risk. The assets shall be capable of being liquidated rapidly with minimal adverse price effect. Further, reserve assets must be denominated in the same currency or currencies in the same ratios as the currencies used for the peg value (unless explicitly otherwise allowed by the HKMA). A de-minimis portion of the reserve assets may be held in a currency other than the currencies used for the peg value, provided that the holding of such currency is necessary for the

[5] In its consultative document "*Cryptoasset standard amendments*", the BCBS has proposed to require banks to perform due diligence to ensure that they have an adequate understanding, at acquisition and thereafter on a regular basis, of the stabilisation mechanism of the cryptoasset and of its effectiveness.

[6] For example, consider a cryptoasset that is redeemable for a given currency amount (i.e. the currency amount is the reference asset) but is backed by bonds denominated in the same currency (i.e. the bonds are the reserve asset). The reserve assets will give rise to credit, market and liquidity risks that may result in losses relative to the value of the reference asset.

operation of the cryptoasset arrangement and all currency mismatch risk between the reserve assets and peg value has been appropriately hedged.[7]

- Management of reserve assets: the governance arrangements relating to the management of reserve assets must be comprehensive and transparent. They must ensure that the following requirements are met:
  - The reserve assets are managed and invested with an explicit and legally enforceable objective of ensuring that all cryptoassets can be redeemed promptly at the peg value, including under periods of extreme stress.
  - A robust operational risk and resilience framework exists to ensure the availability and safe custody of the reserve assets.
  - A mandate that describes the types of assets that may be included in the reserve must be publicly disclosed and kept up to date.
  - The composition and value of the reserve assets are publicly disclosed on a regular basis. The value must be disclosed at least daily and the composition must be disclosed at least weekly.
  - The reserve assets are subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

24 Stabilisation mechanisms that: (i) reference other cryptoassets as underlying assets (including those that reference other cryptoassets that have traditional assets as underlying); or (ii) use protocols to increase or decrease the supply of the cryptoasset[8] do not meet classification condition 1.

7 Classification Condition 2

25 All rights, obligations and interests arising from the cryptoasset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed. In addition, the applicable legal frameworks must ensure settlement finality in both primary and secondary markets. AIs are required to conduct a legal review of the cryptoasset arrangement to ensure this condition is met, and make the review available to the HKMA upon request.

[7] In its consultative document "*Cryptoasset standard amendments*", the BCBS has proposed additional specifications on the asset quality criteria for reserve assets.

[8] Cryptoassets that use protocols to maintain their value are in some cases referred to as "algorithm-based stablecoins".

26 To meet classification condition 2, the following requirements must be met:

- At all times, the cryptoasset arrangements must ensure full transferability and settlement finality. In addition, cryptoassets with stabilisation mechanisms must provide a robust legal claim against the issuer and/or underlying reserve assets and must ensure full redeemability (i.e. the ability to exchange cryptoassets for amounts of pre-defined assets such as cash, bonds, commodities, equities or other traditional assets) at all times and at their peg value. In order for a cryptoasset arrangement to be considered as having full redeemability, it must allow for the redemption to be completed within five calendar days of the redemption request at all times.
- At all times, the cryptoasset arrangements are properly documented. For cryptoassets with stabilisation mechanisms, cryptoasset arrangements must clearly define which parties have the right to redeem; the obligation of the redeemer to fulfil the arrangement; the timeframe for this redemption to take place; the traditional assets in the exchange; and how the redemption value is determined. These arrangements must also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the cryptoasset is issued and redeemed. At all times, settlement finality in cryptoasset arrangements must be properly documented such that it is clear when the cryptoasset has become irrevocably and unconditionally transferred, transferring key financial risks from one party to another. The documentation described in this paragraph must be publicly disclosed by the cryptoasset issuer. If the offering of the cryptoasset to the public has been approved by the relevant regulator on the basis of this public disclosure, the condition in this sub-paragraph will be considered fulfilled. Otherwise, an independent legal opinion would be needed to confirm the requirements mentioned in this bullet point are met.

8 Classification Condition 3

27 The functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks.

28 To meet classification condition 3, the following requirements must be met:

- The functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets, and the network on which it runs, do not pose any material risks that could impair the transferability, settlement finality or, where applicable, redeemability of the cryptoasset. To this end, entities performing

activities associated with these functions[9] must follow robust risk governance and risk control policies and practices to address risks including, but not limited to: credit, market and liquidity risks; operational risk (including outsourcing, fraud and cyber risk) and risk of loss of data; various non-financial risks, such as data integrity; operational resilience (i.e. operational reliability and capacity); third-party risk management; and anti-money laundering / countering the financing of terrorism (AML/CFT).

- All key elements of the network must be well-defined such that all transactions and participants are traceable. Key elements include: (i) the operational structure (i.e. whether there is one or multiple entities that perform core functions of the network); (ii) degree of access (i.e. whether the network is restricted or unrestricted); (iii) technical roles of the nodes (including whether there is a differential role and responsibility among nodes); and (iv) the validation and consensus mechanism of the network (i.e. whether validation of a transaction is conducted with single or multiple entities).

9 Classification Condition 4

29 All entities that execute redemptions, transfers, storage or settlement of the cryptoasset, or manage or invest reserve assets, must: (i) be regulated and supervised, or subject to appropriate risk management standards; and (ii) have in place and disclose a comprehensive governance framework.

30 Entities subject to condition 4 include operators of the transfer and settlement systems for the cryptoasset, wallet providers and, for cryptoassets with stabilisation mechanisms, administrators of the stabilisation mechanism and custodians of the reserve assets. Node validators may be subject to appropriate risk management standards as an alternative to being regulated and supervised.

[9] Examples of these entities include but are not limited to: issuers, operators of the transfer and settlement systems for the cryptoasset, administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism.

III CAPITAL REQUIREMENTS FOR CRYPTOASSETS

10 Boundary Between Books

31 AIs should follow sections 281A to 281D of the BCR to determine the allocation of cryptoassets between the banking book and trading book, subject to the following specifications and exceptions:

- Group 1a cryptoassets must be assigned to the banking book or trading book based on the application of the boundary criteria to the non-tokenised equivalent traditional assets.
- Group 1b cryptoassets must be assigned to the banking book or trading book based on the application of the boundary criteria to the reference assets.
- Group 2a cryptoassets must be treated according to the proposed market risk rules, independent of whether they stem from trading or banking book instruments (i.e. similar to FX and commodities risk).
- Group 2b cryptoassets must be treated according to the standardised conservative prudential treatment outlined in paragraphs 97 to 100.

11 Use of Internal Models and Accounting Classification

32 AIs should follow the relevant sections in the BCR to determine whether Group 1 cryptoasset exposures can be treated according to standardised or model-based approaches to credit and market risk. Models-based approaches must not be applied to Group 2 cryptoassets.

33 Cryptoasset exposures are not subject to the deduction requirement that applies to intangible assets set out in section 43 of the BCR, even in cases where the cryptoasset is classified as an intangible asset under the applicable accounting standard.

12 Credit Risk

34 This section describes how Parts 4, 5, 6, 6B and 7 of the BCR are to be applied to cryptoasset exposures.

12.1 Treatment of Group 1a Cryptoassets

Calculation of credit risk

35 Group 1a cryptoassets (tokenised traditional assets) held in the banking book will generally be subject to the same rules to determine risk-weighted amounts for credit risk as non-tokenised traditional assets (i.e. the rules set out in Parts 4, 6, 6B and 7 of the BCR), except for AIs adopting the basic approach. For example, a tokenised corporate bond held in the banking book will be subject to the same risk weight as the non-tokenised corporate bond held in the banking book.

36 For AIs adopting the basic approach, only Group 1a cryptoassets issued by the HKSAR Government and domestic public sector entities (DPSEs, e.g. HKMC) held in the banking book will be subject to the same rules to determine risk-weighted amounts for credit risk as non-tokenised traditional assets. Other Group 1a cryptoassets held in the banking book must be risk-weighted at 1,250% and will not be eligible to be used as collateral for credit risk migration. As such, under the basic approach, paragraphs 37 to 39 will only apply to Group 1a cryptoassets issued by the HKSAR Government and DPSEs.

37 The treatment outlined in paragraph 35 above is based on the assumption that if two exposures confer the same level of legal rights (to cash flows, claims in insolvency, ownership of assets, etc.) and the same likelihood of paying the owner all amounts due on time (including amounts due in case of default), they will likely have very similar values and pose a similar risk of credit losses. However, there are areas of the credit risk standards that aim to capture risks that are not directly related to the legal rights of an asset held by an AI or likelihood of timely payment. AIs must separately assess the tokenised traditional asset against these rules, and not assume qualification for a given treatment simply because the traditional (non-tokenised) asset qualifies. For example, when considering the eligibility of being recognised as collateral, it should be noted that a tokenised asset may have different market liquidity characteristics than the traditional (non-tokenised) asset. This could arise because the pool of potential investors that are able to hold tokenised assets might be different to non-tokenised assets.

Credit risk mitigation

38 Sections 79 and 80 of the BCR set out the list of eligible forms of financial collateral that may be recognised for the purpose of calculating the RWA of an exposure under the standardised (credit risk) approach. The list is also the basis of recognised financial collateral under the foundation IRB approach. Only Group 1a cryptoassets that are

tokenised versions of the instruments included on the list of eligible financial collateral set out in sections 79 and 80 of the BCR may qualify as recognised collateral (subject to meeting the eligibility criteria as set out in Part 4, 6 or 7 (e.g. section 77 of the BCR), as the case requires, as well as the requirements described below).

39 The potential for market liquidity characteristics and market values of tokenised assets to differ from non-tokenised assets is important in considering whether Group 1a cryptoassets meet the requirements for the purposes of credit risk mitigation within the credit risk standards. Also, the speed with which a secured creditor could take possession of cryptoasset collateral may be different from that for a traditional asset. Therefore, before such assets are recognised as collateral for the purposes of credit risk mitigation, AIs must separately assess whether they comply with the relevant eligibility requirements for collateral recognition, such as whether the collateral can be liquidated promptly and legal certainty requirements (see section 77(2)(a) of the BCR). In addition to assessing whether tokenised assets held as collateral are eligible to be recognised as credit risk mitigation, AIs must analyse the period of time over which they can be liquidated and the depth of market liquidity during a period of downturn. Cryptoassets shall only be recognised as collateral where volatility in values and holding periods under distressed market conditions can be confirmed to not be materially increased compared with the traditional asset or pool of traditional assets. This may not be applicable to the IRB approach, since an AI can reflect any material increase in relevant parameters as part of own LGD estimates. Having said that, an AI adopting the IRB approach must receive the approval from the HKMA to recognise the credit risk mitigation effect of using any cryptoassets as collateral in its LGD estimates as if the AI intended to make a significant model change (or to adopt a new model where appropriate).

12.2 Treatment of Group 1b Cryptoassets

Calculation of credit risk

40 As a result of the classification conditions, Group 1b cryptoassets must be designed to be redeemable for a predefined amount of a reference asset or assets, or cash equal to the value of the reference assets. In addition, the cryptoasset arrangement must include a sufficient pool of reserve assets to ensure the redemption claims of cryptoasset holders can be met. Aside from these common elements, Group 1b cryptoassets may be structured in a variety of different ways. AIs that have banking book exposures to Group 1b cryptoassets must analyse their specific structures and identify all risks that could result in a loss. Each credit risk must be separately

capitalised by AIs following one or more of Parts 4, 6, 6B and 7 of the BCR.[10] Paragraphs 41 to 48 below describe various ways in which credit risks may arise from AIs' exposures to Group 1b cryptoassets and the capital requirements that would apply in each case. The list is not exhaustive, and it is the responsibility of AIs to comprehensively assess and document the full range of risks arising from each of its exposures to Group 1b cryptoassets.

41 *Risk from reference asset*. If the reference asset for a Group 1b cryptoasset gives rise to credit risk (e.g. a bond), AIs may suffer a loss from the default of the reference asset's issuer. AIs must therefore calculate a risk-weighted amount (RWA) for the credit risk of the reference asset under Part 4, 6 or 7 of the BCR as if the AIs had a direct holding of the reference asset. If the reference asset gives rise to FX or commodities risk (e.g. financial assets denominated in a foreign currency or physical commodities), AIs must calculate market risk RWA for the exposure equal to the market risk RWA that would apply to a direct holding of the underlying traditional asset.

42 For Group 1b cryptoassets that reference a pool of traditional assets, AIs must apply the requirements applicable to equity investments in funds[11] (see Part 6B of the BCR) to determine the RWA applicable as if the AIs had a direct holding of the referenced pool of traditional assets, as required in paragraph 41. The look-through approach, the third-party approach and the mandate-based approach set out in Part 6B of the BCR are available for cryptoassets that fulfil all requirements for using these approaches. Otherwise, the fall-back approach (i.e. a 1,250% risk weight) must be applied.

43 *Risk of default of the redeemer*. Group 1b cryptoassets must be redeemable and if the entity that performs the redemption function (the "redeemer") fails, the cryptoassets may become worthless. The capital treatment[12] of AIs' credit exposures to the redeemer depends on the nature of the exposures:

- If the AI holding the cryptoasset has an unsecured claim on the redeemer in case of default, the AI must calculate a credit risk RWA for its exposure to the redeemer equal to the RWA that would apply under Part 4 or 6 of the BCR to a

[10] For an AI adopting the basic approach, all Group 1b cryptoassets held in the banking book must be risk-weighted at 1,250% and will not be eligible to be used as collateral for credit risk migration.

[11] In this paper, the term "equity investments in funds" has the same meaning of "CIS exposures" as defined in section 2(1) of the BCR.

[12] As mentioned in section 13 relating to market risk RWA, credit risk RWA must be calculated for instruments in the trading book that give rise to credit risk as a result of potential default of the redeemer. Such credit risk RWA must be calculated in the manner outlined in this subsection and included in the AI's risk-weighted amount for credit risk as defined in section 2(1) of the BCR.

direct unsecured loan to the redeemer. For this purpose, the loan amount should equal the redemption claim (i.e. peg value) of the cryptoasset.

- If the AI holding the cryptoasset has a secured claim on the redeemer in case of default, the AI must calculate a credit risk RWA for its exposure to the redeemer equal to the RWA that would apply under Part 4 or 6 of the BCR to a direct secured loan to the redeemer. For this purpose, the loan amount, before any recognition of credit risk mitigation, should equal the redemption claim (i.e. peg value) of the cryptoasset. All conditions on the eligibility of collateral for the purposes of recognising credit risk mitigation set out in Part 4 or 6 of the BCR apply.

44 Certain Group 1b cryptoassets may be structured to avoid the cryptoasset holders being exposed to the credit risk (either directly or indirectly) of the redeemer. AIs are not required to calculate any credit risk RWA in respect of the risk outlined in paragraph 43 if the two following conditions are met:

- The underlying reserve assets are held in a bankruptcy-remote special purpose vehicle (SPV) on behalf of the holders of cryptoassets who have direct claims on the underlying reserve assets.
- The AI has obtained an independent legal opinion for all laws relevant to involved parties, including the redeemer, the SPV and custodian, affirming that relevant courts would recognise underlying reserve assets held in a bankruptcy-remote manner as those of the cryptoasset holder.

45 *Risks arising when intermediaries perform the redemption function*. Group 1b cryptoassets may be structured such that only a subset of holders ("members") are allowed to transact directly with the redeemer to redeem the cryptoasset. Holders that cannot transact directly with the redeemer ("non-member holders") are therefore reliant on the members for the cryptoassets to maintain their value relative to the reference assets. This type of structure itself may include variants, for example:

- The members may issue a legally binding commitment to buy cryptoassets from non-member holders at a price equal to that of the reference assets.
- The members may not make a commitment, but may be incentivised to purchase the cryptoassets from non-member holders because the members know they can exchange the cryptoassets with the redeemer for cash/assets (as long as the redeemer does not fail).

46 AIs that are members of cryptoasset arrangements as described in paragraph 45 above ("member AIs"), must calculate RWA for their own cryptoasset holdings in the same way as required for holders in cryptoassets arrangements in which all holders can deal directly with the redeemer (i.e. as set out in paragraphs 43 to 44). In addition,

member AIs may be exposed to the risk that the redeemer fails and they are committed to purchase cryptoassets from non-member holders. In such cases, a member AI must also calculate a credit risk RWA for such a commitment as if the member AI held all of the cryptoassets that it could be obliged to purchase (i.e. as set out in the first bullet of paragraph 45). Even if there is no legal obligation for a member AI to purchase cryptoassets from non-member holders, the member AI must consider whether in practice it would be obliged to step-in and purchase the cryptoassets in order to satisfy the expectations of non-member holders and protect the its reputation. Where such step-in risk exists, the member AI must calculate a credit risk RWA for such risk as if a legally binding commitment had been made by the member AI. Exceptions would only be made if the AI can demonstrate to the HKMA that such step-in risk does not exist.

47 The risks to AIs as holders of cryptoassets that cannot deal directly with the redeemer (i.e. non-member holders) depend on whether the members have committed to purchase cryptoassets from all non-member holders in unlimited amounts (i.e. they have made a standing and irrevocable offer to purchase all outstanding cryptoassets from non-member holders):

- If members have committed to buy cryptoassets in unlimited amounts, the non-member holders are exposed to: (i) the risk arising from the changing value or potential default of the reference asset; and (ii) the risk that all members default, leaving non-member holders with no way to redeem their cryptoassets. When AIs are non-member holders they must sum the RWAs calculated for the two risks. The first risk must be calculated as the RWA that would be calculated as if the AI had a direct exposure to the reference asset (see paragraphs 41 and 42). The calculation of the RWA for the default of the members is more complex given that there may potentially be multiple members that have made commitments to purchase the cryptoassets (i.e. the holder can choose whether to sell the cryptoasset to any one of a number of members). If there is just one member, the RWA must be calculated as the cryptoasset holding multiplied by the risk weight applicable to an unsecured loan to the member. If there are multiple members, the risk weight to be used must be the risk weight that would be applicable to an unsecured loan to the member with the lowest risk weight.[13]

[13] For example, consider the situation in which there is only one member and it has a low risk weight. Its low risk weight should be used to determine the credit risk of non-member holders. Now consider an additional member is added that has a high risk weight. The addition of this new member does not increase the risk to non-member holders (in fact it decreases it by giving them more options for redeeming their assets). Thus, the low risk weight of the first member can continue to be used to determine the credit risk to non-member holders.

- If members have not committed to purchase cryptoassets in unlimited amounts from all non-member holders, the latter are exposed to: (i) the risk arising from the changing value or potential default of the reference asset; (ii) the risk that all the members default, leaving non-member holders with no way to redeem their cryptoassets assets; and (iii) the risk that the redeemer defaults (because if it failed, the members would no longer have the incentive to purchase the cryptoassets from the non-member holders). In such cases, the AI as a non-member holder must calculate an RWA for each of the three separate exposures. The RWA for the first two risks must be calculated in the same way as described in the first bullet point above. The RWA for the third risk must be calculated as the RWA that would be calculated for a direct unsecured loan to the redeemer.

Credit risk mitigation

48 Group 1b cryptoassets, including those that can be redeemed for traditional instruments that are on the list of eligible financial collateral set out in section 79 or 80 of the BCR, are not recognised collateral in themselves for the purposes of the BCR. This is because, as outlined above, the process of redemption may add counterparty risk that is not present in a direct exposure to a traditional asset.

12.3 Counterparty Credit Risk

49 This subsection describes how the capital requirements for counterparty credit risk (CCR) are to be applied to derivatives referencing cryptoassets and securities financing transactions (SFTs) whose underlying assets are cryptoassets.

50 AIs must calculate the default risk exposures of the SFTs in accordance with section 226MJ or 226MK of the BCR, as the case requires, and calculate the RWAs of the default risk exposures in accordance with one or more of Parts 4, 5 and 6 of the BCR. As noted in paragraph 38, only Group 1a cryptoassets that are tokenised versions of the instruments included on the list of eligible financial collateral set out in section 79 and 80 of the BCR may qualify as recognised collateral.[14] Group 1b, Group 2a and Group 2b cryptoassets are not recognised collateral for the purposes of the BCR and therefore when AIs receive them as collateral under SFTs, they will not be taken into account when calculating the default risk exposures and the RWAs of the SFTs. As with all non-eligible collateral, AIs that lend Group 1b, Group 2a or Group 2b cryptoassets as part of an SFT, when applying the comprehensive approach under Part 4 or section

[14] For an AI adopting the basic approach, the RWAs of the SFTs would be calculated without considering any cryptoasset received by the AI as collateral under the SFTs (except Group 1a cryptoassets issued by the HKSAR Government and DPSEs). The risk weight applicable to the default risk exposure is that of the counterparty determined by using the basic approach.

226MK of the BCR, use the same haircut that is used for equities that are not traded on a recognised exchange (i.e. a haircut of 30%).

Group 1a (tokenised traditional assets)

51 Derivatives on Group 1a cryptoassets will generally be subject to the same rules to determine CCR as non-tokenised traditional assets (i.e. the rules set out in Part 6A of the BCR), which includes the internal models (counterparty credit risk) approach (IMM(CCR) approach), where the same requirements apply for tokenised assets as for traditional assets.

52 For the cases described in paragraph 105 for credit valuation adjustment (CVA) risk, especially in presence of significant valuation differences between the traditional and the tokenised asset and in presence of significant basis risk, there could be limitations to apply the IMM(CCR) approach in case of missing data or too short history or in presence of data quality problems, which then requires to apply the SA-CCR approach as described below for derivatives on Group 2a cryptoassets.

Group 1b cryptoassets (cryptoassets with stabilisation mechanisms)

53 Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CCR as non-tokenised traditional assets (i.e. the rules set out in Part 6A of the BCR).

Group 2a cryptoassets

54 Derivatives on Group 2a cryptoassets will be subject to the SA-CCR approach (i.e. the rules set out in Division 1A of Part 6A of the BCR), amended by the following:

- The replacement cost (RC), which takes into account derivative contracts that are covered by a valid bilateral netting agreement as defined in section 2(1) of the BCR, may include derivatives on Group 2a cryptoassets.
- In order to calculate the potential future exposure (PFE) of a netting set that contains derivatives on Group 2a cryptoassets, a new asset class “crypto” will be created in the SA-CCR approach.
  - The mathematical structure for calculating the add-on for this asset class will be in line with the structure used in the asset class of exchange rate contracts, but with different parameters.
  - There are separate hedging sets for each cryptoasset priced in applicable fiat currencies or in another Group 2a cryptoasset.
  - The supervisory factor will be 32% for all cryptoasset / fiat currency and cryptoasset/cryptoasset pairs, and the supervisory volatility for options will equal 120%.

- The adjusted notional of the derivative is the notional amount of the underlying cryptoasset expressed in HKD. For the case of a cryptoasset priced in another cryptoasset, the adjusted notional amount of the derivative will be the larger of the two adjusted notionals.[15]
- The supervisory delta adjustment and the maturity factor applicable to the derivative will be determined in the same ways as for derivatives falling within the other asset classes.
- The add-ons of the hedging sets of the "crypto" asset class will be aggregated in the same way as for the asset class of exchange rate contracts.

Group 2b cryptoassets

55 For derivatives that have Group 2b cryptoassets as the underlying exposures or that are priced in units of a Group 2b cryptoasset, the default risk exposure will be calculated as the replacement cost (RC)[16] plus the potential future exposure (PFE), both multiplied by the alpha factor specified in section 226BC of the BCR, where the PFE is to be calculated as 50% of the gross notional amount. The RC is to be calculated using the existing requirements specified in the SA-CCR approach set out in Part 6A of the BCR, with the exception that, if the derivatives are covered by a valid bilateral netting agreement, netting of the derivatives within a netting set is permitted only between derivatives referencing to the same Group 2b cryptoasset. If a netting set contains both derivatives related to Group 2b cryptoasset and other assets that are not Group 2b cryptoassets, the netting set must be split into two sub-netting sets: one containing the derivatives related to Group 2b cryptoassets; and one containing derivatives related to the assets other than Group 2b cryptoassets. When calculating the PFE for derivatives on Group 2b cryptoassets, the 50% of the gross notional amount must be applied per contract– derivatives on Group 2b cryptoassets must not form part of any hedging set.

[15] If pairs to HKD are not liquidly traded, the most liquid fiat currency needs to be taken with FX spot rates against the HKD.

[16] The replacement cost is subject to a floor of zero.

13 Market Risk

13.1 Treatment of Group 1 Cryptoassets

56 This section describes how the capital requirements for market risk are to be applied to Group 1 cryptoasset exposures under the simplified standardised approach, the standardised (market risk) approach, and the internal models approach.[17]

Simplified standardised approach

57 An AI must apply the following specifications when calculating the market risk capital charge under the simplified standardised approach for Group 1 cryptoassets.

- All instruments, including derivatives and off-balance sheet positions that are affected by changes in Group 1 cryptoassets prices, must be included.
- The AI must first express each Group 1 cryptoasset position in terms of its quantity, then convert it at the current spot price into HKD.
- The AI must consider for Group 1 cryptoassets the same risk categories as the one used for traditional assets they digitally represent (i.e. interest rate risk, equity risk, FX risk and commodities risk), as defined in Part 8 of the BCR.
- The AI must consider for Group 1 cryptoassets the same treatment for options as the one defined for traditional assets they digitally represent (see Division 7 of Part 8 of the BCR).
- Netting and hedging are recognised between Group 1a cryptoassets and the traditional assets they digitally represent, and both must be mapped to the same risk category.
- Netting and hedging are recognised between Group 1b cryptoassets and the traditional assets that the cryptoasset references, and both must be mapped to the same risk category.
- If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the capital requirements for credit risk.

Standardised (market risk) approach

58 An AI must apply the following specifications when calculating the market risk capital charge under the standardised (market risk) approach for Group 1 cryptoassets.

[17] An AI with cryptoasset exposures will not be qualified for the de-minimis exemption for market risk.

59 An AI must map Group 1 cryptoassets to the current risk classes set out in the sensitivities-based method. Specifically:

- Each tokenised instrument in Group 1a should be decomposed into the same risk factors as the traditional asset it digitally represents. For the tokenised asset, its sensitivities to the traditional risk factors should be identical to those of the traditional asset it digitally represents within the respective current risk classes.
- Each stablecoin instrument in Group 1b should be decomposed into the same risk factors as the traditional assets that it references. Its sensitivities to the traditional risk factors should be identical to those of the traditional assets that it references within the current risk classes.

60 For the standardised default risk charge (SA-DRC), a Group 1 cryptoasset should have its gross jump-to-default (JTD) risk amount considered as equivalent to those from the traditional asset it digitally represents or references.

61 If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the capital requirements for credit risk.

Internal models approach

62 When calculating the market risk capital charge for Group 1 cryptoassets under the internal models approach (IMA), AIs must apply the specifications set out in paragraphs 63 to 67.

63 To determine the aggregate capital charge under the IMA, an AI must calculate the default risk charge (DRC) and an aggregate non-DRC capital charge as set out in section 322D(2) of the BCR. For the latter, the AI will need to determine an aggregate stressed expected shortfall (SES) capital measure according to section 322D(4) of the BCR for the non-modellable risk factors and an aggregate capital charge for modellable risk factors (IMCC) according to section 322D(3) of the BCR.

64 The use of the IMA for instruments referencing Group 2 cryptoassets is not permitted.

65 The market risk capital charge for modellable and non-modellable risk factors allows mapping of exposures to risk factors as follows:

- Each tokenised instrument in Group 1 must be decomposed into the same risk factors as the traditional asset it digitally represents within the respective current risk classes.

- Each stablecoin instrument in Group 1 must be decomposed into the same risk factors as the traditional assets that they reference within the respective current risk classes.

66 For the DRC, tokenised asset and non-tokenised asset are regarded as different instruments to the same obligor. Similarly, traditional assets referenced by a stablecoin and the stablecoin itself are regarded as different instruments to the same obligor. The AI must take into account the different losses in different instruments in accordance with section 2(1)(i) of Schedule 3 of the BCR. Differences in instruments should be reflected in LGD estimates. Maturity mismatches between tokenised and non-tokenised assets, and between stablecoins and the traditional assets they reference, should be captured in accordance with section 2(1)(k) of Schedule 3 of the BCR.

67 If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function must be treated in line with the capital requirements for credit risk.

13.2 Treatment of Group 2 Cryptoassets

68 Group 2 cryptoassets are divided into:

- Group 2a: cryptoassets that meet the hedging recognition criteria set out in paragraph 69 below. Group 2a cryptoassets are subject to modified versions of the simplified standardised approach or the standardised (market risk) approach set out in paragraphs 71 to 96 below. The treatment permits some recognition of hedging. The IMA is not applicable to Group 2a cryptoassets.
- Group 2b: cryptoassets that do not meet the hedging recognition criteria. Group 2b cryptoassets are subject to a new conservative treatment set out in paragraphs 97 to 100 below, which does not permit AIs to recognise hedging. A Group 2 cryptoasset must be classified as Group 2b unless an AI demonstrates to the satisfaction of the HKMA that the cryptoasset meets hedging recognition criteria.

Group 2a hedging recognition criteria

69 Group 2 cryptoassets that are assessed to meet all three of the following hedging recognition criteria[18], will be classified as Group 2a cryptoassets:

- The AI's cryptoasset exposure is one of the following:
  - A direct holding of a spot Group 2 cryptoasset where there exists a derivative or exchange-traded fund (ETF) / exchange-traded note (ETN) that solely references the cryptoasset and that is traded on a regulated exchange that clears these trades through a qualifying central counterparty (QCCP).
  - A derivative or ETF/ETN that references a Group 2 cryptoasset, where the derivative or ETF/ETN has been explicitly approved by a jurisdiction's markets regulators for trading or the derivative is cleared by a QCCP.
  - A derivative or ETF/ETN that references a derivative or ETF/ETN that meets the criterion of the second indent above.
  - A derivative or ETF/ETN that references a cryptoasset-related reference rate published by a regulated exchange that clears these trades through a QCCP.

- The AI's cryptoasset exposure, or the cryptoasset referenced by the derivative or ETF/ETN, is highly liquid. Specifically, both of the following must apply:
  - The average market capitalisation was at least HKD 78bn over the previous year.
  - The 10% trimmed mean of daily trading volume with major fiat currencies is at least HKD 390m over the previous year.

- Sufficient data is available over the previous year. Specifically, both of the following must apply:
  - There are at least 100 real price observations over the previous year. The "real price observation" is defined in section 281 of the BCR.
  - There are sufficient data on trading volumes and market capitalisation.

70 An AI should calculate the market risk capital charge for Group 2a cryptoassets according to:

- a modified version of the simplified standardised approach set out in paragraphs 71 to 79; or

[18] The BCBS intends to monitor closely the specification of the various thresholds in the criteria and the degree of hedge recognition that the Group 2a classification permits. As such, the HKMA will impose the BCBS' potential updates.

- a modified version of the standardised (market risk) approach set out in paragraphs 80 to 96.

Simplified standardised approach for Group 2a cryptoassets

71 For Group 2a cryptoassets, the simplified standardised approach will include a separate risk category with its capital requirement determined based on the specifications set out in paragraphs 72 to 79.

72 All instruments, including derivatives and off-balance sheet positions that are affected by changes in Group 2a cryptoasset prices must be included.

73 An AI must first express each Group 2a cryptoasset position in terms of its quantity, and then convert it at the current spot price into the AI's reporting currency.

74 When consolidated, an AI must not offset positions for each Group 2a cryptoasset in different markets or exchanges, meaning that the AI must determine separate long and short gross consolidated positions. In addition, only the products listed in paragraph 69 may be used for the purposes of offsetting and for the purposes of calculating the net position set out in paragraph 75 below. Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

75 For each Group 2a cryptoasset *k*, an AI must determine a net position based on the following formula:

$$Net\ \ position_k = max(long\ \ position_k, |short\ \ position_k|) - 0.65 \cdot min(long\ \ position_k, |short\ \ position_k|)$$

76 The capital requirement for position risk of a Group 2a cryptoasset will be 100% of its respective net position.

77 The total capital requirement for position risk consists of the simple sum of all Group 2a cryptoasset capital requirements.

78 For options with a Group 2a cryptoasset as underlying asset, an AI must calculate the market risk capital charge under the scenario approach.[19] The simplified approach and the delta-plus approach are not allowed. In particular, the AI must:

[19] An AI should use the scenario approach without the prior consent of the HKMA only for options with a Group 2a cryptoasset as underlying asset. For option exposures to debt securities, interest rates, equities, foreign exchange (including gold) and commodities, the use of the scenario approach requires the prior consent of the MA set out in section 299(c) of the BCR.

- revalue the options using matrices for simultaneous changes in (i) the underlying price and (ii) the volatility of that price;
- set up a different matrix for each Group 2a cryptoasset;
- for each matrix:
  - use ±100% for the underlying price change and divide the ±100% range by at least seven observations into equally-spaced intervals (including the current observation);
  - use ±100% for the relative volatility change, and at the request of the HKMA, use additional intermediate points between the ±100% range; and
- calculate the net profit or loss of options in each cell of the matrix.

The market risk capital charge for each Group 2a cryptoasset is equal to the largest loss contained in the matrix.

79 The Group 2a risk class total capital charge must be aggregated in a manner consistent with section 284(1) of the BCR. Instead of the scaling factors in section 284(1) of the BCR, a scaling factor of 1 shall apply for the Group 2a cryptoassets.

Standardised (market risk) approach for Group 2a cryptoassets

80 An AI should include Group 2a cryptoassets in the standardised (market risk) approach as a separate risk class and determine its capital requirement based on the specifications set out in paragraphs 81 to 96.

81 All risk factors, including those related to derivatives and off-balance sheet positions that are affected by changes in Group 2a cryptoasset prices must be included.

82 An AI must first express each Group 2a cryptoasset position in terms of its quantity, and then convert it at its current spot price into HKD.

83 When consolidated, an AI must not offset sensitivities for each Group 2a cryptoasset in different markets or exchanges, meaning the AI must calculate those sensitivities as separate long and short gross consolidated sensitivities. In addition, only the products listed in paragraph 69 may be used for the purposes of offsetting and for the purposes of calculating the capital charge set out in paragraphs 85 to 96 below. Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

84 The computation of the sensitivities-based method for Group 2a cryptoassets includes new specifications of delta, vega and curvature risk factors. The sensitivity definitions are also extended to include those of Group 2a cryptoassets. Finally, a new bucket

structure is introduced, composed of multiple buckets, one for each Group 2a cryptoasset, containing only its respective sensitivities.

85 *Group 2a cryptoasset delta spot specification*: the sensitivity is measured by changing the Group 2a cryptoasset spot price by 1 percentage point (i.e. 0.01 in relative terms) and dividing the resulting change in the market value of the instrument V_i by 0.01 (i.e. 1%) as follows:

$$s_k = \frac{V_i(1.01 \cdot CRYPTO(G2a)_k) - V_i(CRYPTO(G2a)_k)}{0.01}$$

where:

- *k* is a given Group 2a cryptoasset;
- $CRYPTO(G2a)_k$ is the market value of the Group 2a cryptoasset *k*; and
- V_i is the market value of instrument *i* as a function of the price of the Group 2a cryptoasset *k*.

86 *Group 2a cryptoasset vega specification*: the option-level vega risk sensitivity to a given Group 2a cryptoasset is the mathematical product of the vega and the implied volatility of the option as follows:

$$s_k = vega \times implied\ \ volatility$$

where:

- *vega,* $\frac{\partial V_i}{\partial \sigma_i}$, is defined as the change in the market value of the option V_i as a result of a small amount of change to the implied volatility σ_i; and
- the instrument's vega and implied volatility should be sourced from pricing models used by the independent risk control function of the AI.

87 *Bucket structure*: the new risk class will comprise "*n*" buckets, where each bucket corresponds to the aggregate positions in a specific Group 2a cryptoasset; this is reflected in the following tables.

Delta cryptoasset buckets and risk weights		
Bucket number	*Group 2a cryptoasset*	*Risk weight*
1	Cryptoasset X_1	100%
...	...	...
n	Cryptoasset X_n	100%

Table 2

Vega cryptoasset buckets and risk weights		
Bucket number	*Group 2a cryptoasset*	*Risk weight*
1	Cryptoasset X_1	100%
...	...	...
n	Cryptoasset X_n	100%

Table 3

88 *Delta (vega) capital requirements*: Delta sensitivities must be determined based on a risk factor structure considering two dimensions[20]:

- exchange; and
- time to maturity, at the following tenors: 0 years, 0.25 years, 0.5 years, 1 year, 2 years, 3 years, 5 years, 10 years, 15 years, 20 years and 30 years.

89 For vega sensitivities, no differentiation by exchange or underlying maturity is considered. Group 2a cryptoasset vega risk factors are defined along the maturity of the option. The implied volatility of the option is mapped to one or more of the following tenors: 0.5 years, 1 year, 3 years, 5 years and 10 years.

90 In order to calculate the delta (or vega) capital requirements for a single bucket *b* $\rho_{kl} = 94\%$.

91 The delta (or vega) capital requirement, K_b, for a single bucket *b* is calculated as follows:

$$K_b = \sqrt{\max(0, \sum_k WS_k^2 + \sum_k \sum_{l \neq k} \rho_{kl} WS_k WS_l)}$$

92 The delta (or vega) capital requirement for the Group 2a cryptoasset risk class is $\sum_b K_b$, taking into account that there is no recognition of diversification between different Group 2a cryptoassets.

93 *Curvature capital requirements*: for the curvature risk capital requirement, the delta buckets specified above must be used. The curvature sensitivities must be calculated by shifting all tenors in parallel (i.e. no term structure decomposition is required). For calculating the net curvature risk capital requirement CVR_k for the risk factor *k* for the

[20] That is, distinct risk factors need to be considered for identical contracts traded on different exchanges or at different tenors, so that no perfect offsetting is permitted between risk factors arising from different exchanges or different tenors.

Group 2a cryptoasset, the curvature risk weight, which is the size of a shock to the given risk factor, is a relative shift equal to the delta risk weight.

94 For aggregating curvature risk positions within a bucket, the following formula must be used:

$$K_b = \max(K_b^+, K_b^-)$$

where:

$$K_b^+ = \sum_k max(0, CVR_k^+)$$

$$K_b^- = \sum_k max(0, CVR_k^-)$$

95 Curvature risk cannot be diversified across buckets. The total curvature risk capital charge across the entire portfolio is $\sum_b K_b$.

96 Group 2a cryptoassets are not subject to the SA-DRC. In case of a stablecoin included in Group 2a, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function must be treated in line with the capital requirements for the credit risk.

Capital requirements for Group 2b cryptoassets

97 There is no separate trading book and banking book treatment for Group 2b cryptoassets. The conservative treatment is intended to capture both credit and market risk, including CVA risk. For consistency, the RWA calculated under this approach must all be reported as part of the AI's risk-weighted amount for credit risk. In addition to direct exposures, the conservative prudential treatment set out in paragraphs 98 to 100 also applies to:

- Funds of Group 2b cryptoassets (e.g. Group 2b cryptoasset ETFs) and other entities, the material value of which is primarily derived from the value of Group 2b cryptoassets.
- Equity investments, derivatives or short positions in the above funds or entities.

98 For each separate Group 2b cryptoasset to which an AI is exposed, it must apply a risk weight of 1,250% to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoasset. That is, the

RWA of each separate Group 2b cryptoasset to which the AI is exposed is calculated as follows:

$$RWA = 1{,}250\% \cdot max(|long\ \ exposure|, |short\ \ exposure|)$$

99 For each cryptoasset derivative (i.e. a derivative with a Group 2b cryptoasset as the underlying asset), the exposure value used in the above formula is the value of its underlying cryptoassets. For leveraged derivatives (i.e. a derivative that returns a multiple of the value of the underlying), the exposure value of the underlying position must be adjusted upward to take account of the leverage. The exposure value calculated according to this paragraph can be capped at the maximum possible loss on the cryptoasset derivative.

100 The application of the 1,250% risk weight set out in paragraph 98 will ensure that AIs are required to hold capital at least being equal to the value of their Group 2b cryptoasset exposures. For simplicity, the formula also applies the 1,250% risk weight to short positions. Theoretically, short positions and certain other types of exposures could lead to unlimited losses. Thus, in some circumstances, the formula could require capital that is insufficient to cover potential future losses. AIs are responsible for demonstrating the materiality of these risks under the supervisory review of cryptoassets and whether risks are materially underestimated. The HKMA will then consider imposing an additional capital charge in the form of a Pillar 1 add-on in cases where AIs have material exposures to short positions in cryptoassets or to cryptoasset derivatives that could give rise to losses that exceed the capital required by the 1,250% risk weight. In those cases, the capital add-on will be calibrated by requiring AIs to calculate aggregate capital requirements under the market risk capital charge (i.e. applying a 100% risk weight for delta, vega, and curvature in the sensitivity-based method) and basic CVA approach and to use this amount if the result is higher than the requirement based on a 1,250% risk weight.

14 Infrastructure Risk Add-on for Group 1 Cryptoassets

101 The technological infrastructure that underlies all cryptoassets, such as the DLT, is still relatively new and may pose various additional risks even in cases where the cryptoassets comply with the Group 1 classification conditions. Therefore, the HKMA may apply an add-on to the capital requirement for exposures to Group 1 cryptoassets.

102 The add-on for infrastructure risk described above will initially be set as zero but will be increased by the HKMA based on any potentially observed weaknesses in the infrastructure used by Group 1 cryptoassets.

15 CVA Risk

103 This section describes how the capital requirements for CVA risk are to be applied to cryptoasset derivatives exposures and material and fair-valued SFTs referencing cryptoassets, as described in Part 8A of the BCR.

15.1 CVA Risk for Group 1 Cryptoassets

Group 1a cryptoassets

104 Derivatives and SFTs on Group 1a cryptoassets will generally be subject to the same rules to determine the CVA risk capital charge as non-tokenised traditional assets (i.e. the rules set out in Part 8A of the BCR). In other words, if an AI holds a derivative or an SFT on a tokenised asset having a price close to the traditional asset and being subject to CVA risk as set out in Part 8A of the BCR, it will be reflected in the CVA risk capital charge in the same way as a derivative or SFT on the non-tokenised traditional asset.

105 AIs must assess the tokenised traditional asset itself against the rules set out in Part 8A of the BCR. Qualification for a given treatment cannot be derived from the respective traditional (non-tokenised) asset. This requirement of individual assessment includes, but is not limited to, the liquidity characteristics. Different liquidity characteristics between the traditional (non-tokenised) asset and the tokenised asset could result in a higher basis risk between the two. In case of insufficient data availability to model the impact of these different liquidity characteristics on their market values, especially of the exposure underlying CVA, the standardised CVA approach cannot be applied for calculating CVA risk, i.e. such tokenised assets are subject to the basic CVA approach.

Group 1b cryptoassets

106 Derivatives on Group 1b cryptoassets will be subject to the same rules to determine CVA risk capital charge as non-tokenised traditional assets (i.e. the rules set out in Part 8A of the BCR).

15.2 CVA Risk for Group 2 Cryptoassets

Group 2a cryptoassets

107 Group 2a cryptoassets will be only subject to the rules set out in Part 8A of the BCR, except that the use of standardised CVA approach is not permitted for derivatives and SFTs referencing Group 2a cryptoassets.

Group 2b cryptoassets

108 The treatment of CVA risk for Group 2b cryptoassets is covered in paragraphs 97 to 100.

16 Operational Risk

109 The operational risk resulting from cryptoasset activities should generally be captured by the standardised (operational risk) approach (see Division 3 of Part 9 of the BCR) through the Business Indicator – which should include income and expenses resulting from activities relating to cryptoassets – and through the Internal Loss Multiplier – which should include the operational losses resulting from cryptoasset activities. To the extent that operational risks relating to cryptoassets are insufficiently captured by the minimum capital requirements for operational risk and by the internal risk management process of the AIs, AIs should take appropriate steps to ensure capital adequacy and sufficient resilience. The HKMA would also take appropriate measures in the context of the supervisory review process (SRP). Some key dimensions of this issue are elaborated in subsection 21.

IV OTHER REQUIREMENTS

17 Liquidity Risk

110 This section outlines the HKMA's intended approach to treating cryptoasset exposures (including assets, liabilities and contingent exposures) within the Hong Kong liquidity regime. This approach closely aligns with the relevant requirements for cryptoasset exposures set by the BCBS.

111 Generally, cryptoasset exposures should be treated consistently with the existing liquidity requirements for traditional exposures that carry economically equivalent risks. However, cryptoassets may entail additional risks compared to traditional assets, and there is relative lack of historical data on cryptoassets in the market. Therefore, this section provides further clarification and elaboration to address these additional risks associated with cryptoasset exposures.

17.1 Treatments under the LCR and NSFR

High-quality liquid assets

112 A cryptoasset cannot be recognised by a category 1 institution as high-quality liquid assets (HQLA) unless the following conditions are met:

- It is a Group 1a cryptoasset, which is a tokenised version of a traditional asset falling within a class of assets specified in Schedule 2 to the Banking (Liquidity) Rules (BLR);
- Both the underlying asset in its traditional form and the tokenised form of the asset satisfy all the applicable characteristics and operational requirements specified in Schedules 3 and 4 to the BLR[21]; and
- The category 1 institution complies with all the relevant operational requirements specified in Schedule 4 to the BLR.

[21] An example of such a Group 1a cryptoasset could be a tokenised form of a corporate bond that satisfies the relevant HQLA eligibility criteria (e.g. having a qualifying credit rating, being denominated in a currency that is freely convertible into HKD, etc.). The tokenised bond should also reside on a well-established distributed ledger and have an active and sizable market, ensuring the holding category 1 institution can easily and immediately monetise the tokenised bond at any time within the LCR period, with minimal or no loss of value.

Cash flow and stable funding requirements

113 The appropriate classification and calibration of liquidity coverage ratio (LCR) outflow and inflow rates, as well as net stable funding ratio (NSFR) available stable funding (ASF) and required stable funding (RSF) factors for cryptoassets and cryptoliabilities, depend on factors such as the structure of the cryptoasset or cryptoliability, its practical commercial function, and the nature of a category 1 institution's exposure to the cryptoasset or cryptoliability.

114 In general, the LCR and NSFR treatments of cryptoasset exposures vary based on whether they are:

- tokenised claims on a regulated and supervised bank;
- stablecoins; or
- other cryptoassets.

115 *Tokenised claims on a regulated and supervised bank*. If a category 1 institution has issued Group 1a cryptoassets that (i) represent a legally binding claim on the institution; (ii) are redeemable in fiat currency at par value; and (iii) have a stable value supported by the issuing category 1 institution's creditworthiness and asset-liability profile (rather than a segregated pool of assets), the institution may treat the cryptoliabilities as unsecured funding, subject to the following considerations:

- The maturity of the claim on a bank must be determined based upon the contractual redemption rights available to the holder.
- To the extent that the issuing institution can identify the holders of the cryptoassets at all times, it may apply the applicable LCR outflow rates and NSFR ASF factors for the cryptoliabilities (based on the earliest date upon which the liabilities could be redeemed by the holders and the counterparty types of the holders), by following the treatments for retail deposits, small business funding and unsecured wholesale funding under the LCR and NSFR. However, the treatments of stable deposits do not apply to these cryptoliabilities.
- If the issuing institution cannot identify, at all times, the holders of the cryptoassets, it must treat the cryptoliabilities as unsecured wholesale funding provided by other legal entities.
- If the cryptoassets are used primarily as a means of payment and created as part of an operational relationship between the issuing institution and its wholesale customers, the relevant treatments and categorisation methodology for operational deposits under the LCR and NSFR should be followed. However, the lower outflow rate provided under clause 7(1)(a) of the Banking (Liquidity Coverage Ratio – Calculation of Total Net Cash Outflows) Code does not apply.

116 On the asset side, if a category 1 institution holds such Group 1a cryptoassets (issued by a regulated and supervised bank), inflows should not be recognised under the LCR if the cryptoassets are not redeemable within 30 days. If the cryptoassets are held for operational purposes, the category 1 institution should treat them as operational deposits and follow the relevant inflow and RSF treatments under the LCR and NSFR.

117 *Stablecoins*. Group 1b cryptoassets, and certain Group 2 cryptoassets[22] that are fully collateralised by a segregated pool of underlying assets that do not count toward the category 1 institution's stock of HQLA, must be treated similarly to securities, subject to the following considerations:

- When a category 1 institution is the issuer of such a stablecoin, and the stablecoin issuance represents a legally binding claim on the institution:
  - The issuing institution must recognise 100% outflows under the LCR if the stablecoin is redeemable within 30 days. An appropriate ASF factor should be assigned to the stablecoin based on the earliest possible redemption date of the stablecoin under the NSFR.
  - The issuing institution may recognise reduced outflows under the LCR if the stablecoin is backed by HQLA that is not included in the institution's eligible HQLA amount, but would be unencumbered and freely available for liquidation upon redemption of the stablecoin. The reduction in outflows must consider the required haircut applied to the HQLA under the LCR and must not result in net inflows.
  - The assets segregated to support the stablecoin's value must be assigned an appropriate RSF factor for encumbered assets, as required under the NSFR. The factor should be based on the earliest date upon which the stablecoin could be redeemed.

- When a category 1 institution holds such a stablecoin on its balance sheet:
  - Generally, the stablecoin should be treated the same as non-HQLA, subject to at least an RSF factor of 85% under the NSFR and not resulting in inflows under the LCR.
  - However, if the stablecoin exposure has a final contractual maturity that would result in cash inflow within the 30-day LCR period or 1-year time horizon, the holding institution may recognise the inflow under the LCR or apply an appropriate RSF factor to the stablecoin based on its residual

[22] Stablecoins that do not qualify as Group 1b cryptoassets due to redemption restrictions (i.e. minimum notice periods) will be included in Group 2. They will, however, be eligible for the treatment outlined in this paragraph, provided they satisfy all criteria for classification under Group 1b except for the requirement of being redeemable at all times, as specified in paragraph 23.

contractual maturity under the NSFR. To avoid confusion, if the stablecoin includes an embedded option allowing holders to redeem it before its final contractual maturity, the holding institution must assume that the option will not be exercised.

118 *Other cryptoassets*. The treatment of Group 2 cryptoassets that do not qualify for the treatments outlined in paragraph 117 (hereafter referred to as "other Group 2 cryptoassets") must be aligned with the treatment of other non-HQLA applicable in the LCR and NSFR standards, subject to the following considerations:

- A category 1 institution that holds other Group 2 cryptoassets or loans denominated in these cryptoassets on its balance sheet must assign an RSF factor of 100% to them under the NSFR, and must not recognise any inflows associated with the liquidation, redemption or maturity of these cryptoassets under the LCR.
- A category 1 institution that has borrowed other Group 2 cryptoassets on an unsecured basis and has an obligation to return these cryptoassets within 30 days must apply a 100% outflow rate against the market value of the assets that must be returned to the institution's customer or counterparty under the LCR, unless the obligation can be settled with certainty from the institution's own unencumbered inventory of the same Group 2 cryptoassets. Similarly, borrowings denominated in other Group 2 cryptoassets must be assigned a 0% ASF factor under the NSFR.

119 Notwithstanding the clarifications above, where necessary, the HKMA may apply more stringent LCR and NSFR treatments if, after considering the features and liquidity risk profiles of a cryptoasset, the HKMA determines that there may be additional liquidity risk inherent in the cryptoasset[23] or contingent risks due to a category 1 institution's role in issuing or transacting in cryptoassets.[24] This conclusion may be based on factors including, but not limited to, the technical design of the cryptoassets, the role of category 1 institutions and the market circumstances.

120 To avoid doubt, other types of transactions involving cryptoasset exposures, which are not explicitly mentioned above, should be treated in alignment with the existing treatments for similar transactions under the LCR and NSFR frameworks. These types of transactions include, for example, the following:

[23] For example, certain characteristics of a cryptoasset may increase the likelihood of a holder seeking redemption from an issuing category 1 institution during a period of stress. Alternatively, these characteristics may restrict a holding category 1 institution from redeeming its funds.

[24] For example, a category 1 institution may need to provide non-contractual liquidity support for the redemption of certain stablecoins, where it is the issuer or a material service provider, to protect its franchise or otherwise avoid negative signalling effects.

- derivatives where the reference asset is a cryptoasset;
- secured funding and lending with cryptoassets as collateral;
- collateral swaps involving cryptoassets; and
- commitments to lend cryptoassets.

17.2 Treatments under the LMR and CFR

121 To ensure a level playing field, the treatments for cryptoassets under the liquidity maintenance ratio (LMR) and core funding ratio (CFR) are generally consistent with those under the LCR and NSFR, incorporating any necessary modifications.

Liquefiable assets

122 Category 2 institutions must not recognise a cryptoasset as liquefiable assets unless the following conditions are met:

- The cryptoasset is a Group 1a cryptoasset that is a tokenised version of an asset falling within a class of assets specified in Table A in section 2 of Schedule 5 to the BLR; and
- Both the underlying asset in its traditional form and the tokenised form of the asset satisfy the relevant qualifying criteria and requirements specified in rule 49 of the BLR.

Cash flow and core funding requirements

123 Group 1a cryptoassets representing tokenised forms of traditional assets or liabilities should adhere to the treatments applicable to the corresponding types of traditional assets or liabilities with equivalent risks under the LMR and CFR. Additionally, Group 1a cryptoassets, which are tokenised claims on a category 2A institution and meet the requirements specified in paragraph 115, may be treated as "deposits" under the CFR if the holders of these cryptoassets are non-bank customers.

124 The stablecoins referred to in paragraph 117 should be subject to similar treatments currently applied to securities under the LMR and CFR. If these stablecoins are redeemable within a month, the issuing category 2 institutions must recognise them as qualifying liabilities under the LMR. In the context of the CFR, appropriate available core funding (ACF) factors should be assigned based on the earliest possible redemption date for the stablecoins. If a category 2A institution holds such stablecoins, the institution should assign a required core funding (RCF) factor to the stablecoins based on their contractual maturity, if applicable. An RCF factor of 100% should be assigned if the stablecoins have no specified term to maturity.

125 Regarding the other Group 2 cryptoassets mentioned in paragraph 118, they should be subject to the most stringent requirements under the LMR (i.e. 0% inflow / 100% outflow) and CFR (0% ACF factor / 100% RCF factor), aligning with the requirements for LCR and NSFR purposes.

126 Where necessary, the consideration set out in paragraph 119 will also apply for the purpose of the LMR and CFR.

18 Leverage Ratio

127 Consistent with the leverage ratio standard, cryptoassets are included in the leverage ratio exposure measure according to their value for financial reporting purposes, based on applicable accounting treatment for exposures that have similar characteristics. For the cases where the cryptoasset exposure is an off-balance sheet item, the relevant credit conversion factor set out in the leverage ratio framework will apply in calculating the exposure measure. Exposures for cryptoasset derivatives must follow the treatment of the risk-based capital framework.

128 For Group 1b cryptoassets, if the AI is involved in the cryptoasset network as a member who is able to deal directly with the redeemer and has promised to purchase cryptoassets from non-member holders, the member also needs to include the total current value of all the off-balance sheet cryptoassets that the AI could be obliged to purchase from holders (as set out in paragraph 46).

19 Large Exposures

129 For large exposures purposes, the treatment for cryptoassets will follow the same principles as for other exposures as set out in the Banking (Exposures Limits) Rules (BELR). Consistent with the requirements set out in BELR, cryptoasset exposures that give rise to a credit risk exposure are included in the large exposure measure according to their accounting value as set out in LEX30.3. The AI must identify and apply the large exposure limits to each specific counterparty or group of linked counterparties to which it is exposed under the risk-based capital framework. Where the cryptoasset exposes the AI to the risk of default of more than one counterparty, the AI must compute for each counterparty the respective amount to which it is exposed to default risk for large exposure purposes. When the cryptoasset also entails a default risk of reference assets, these will be considered for the purpose of the large exposures framework and the AI must follow the existing large exposures rules applicable to transactions with underlying assets (see LEX30.41 to LEX30.53). Cryptoassets that do not expose AIs to default risk (such as physical exposures of gold,

other commodities or currencies, and exposures of some forms of cryptoassets with no issuer) do not give rise to a large exposures requirement; however, the counterparty credit risk exposures arising from derivative contracts that reference cryptoassets with no issuer will fall in the scope of the large exposure requirement.

20 Group 2 Exposure Limit

130 The group 2 exposure limit only applies to systemically important AIs (SIBs). This includes global systemically important AIs (G-SIBs) and domestic systemically important AIs (D-SIBs) as designated under sections 3S and 3U of the BCR.

131 SIBs must apply the exposure limit to their aggregate exposures to Group 2 cryptoassets, including both direct holdings (cash and derivatives) and indirect holdings (e.g. those via investment funds, ETF/ETN, or any legal arrangements designed to provide exposures to cryptoassets).

132 A SIB's total exposure to Group 2 cryptoassets should not generally be higher than 1% of its Tier 1 capital and must not exceed 2% of its Tier 1 capital.

133 Breaches of the Group 2 exposure limit threshold of 1% should not generally occur and SIBs must have arrangements in place to ensure compliance with the limit. For any breach that does occur, the SIB must notify the HKMA as soon as practicable and the breach must be rapidly rectified. Until compliance with the 1% limit is restored, the SIB's exposures that are in excess of the threshold will be subject to the capital requirements that apply to Group 2b cryptoasset exposures [25] (as set out in paragraphs 97 to 99). A SIB's exposures must not exceed 2% of its Tier 1 capital. If a breach of the 2% limit occurs under exceptional circumstances, all Group 2 cryptoasset exposures will be subject to the capital requirements that apply to Group 2b cryptoasset exposures. Exposures are expected to be reduced below the 1% limit.

134 For the purposes of assessing compliance with the Group 2 exposure limit threshold:

- Exposures must be measured using the same methodology that applies for determining the Group 2b capital treatment outlined in paragraphs 97 to 99. That is, exposures to all Group 2 cryptoassets (Group 2a and Group 2b) must be measured using the higher of the absolute value of the long and short exposures in each separate cryptoasset to which the AI is exposed. Derivative exposures must be measured using a delta-equivalent methodology.

[25] In its consultative document "*Cryptoasset standard amendments*", the BCBS has proposed an approach to calculating the capital impact.

- Tier 1 capital is defined in section 37 of the BCR.

21 Risk Management Systems and Supervisory Review

135 This section describes how the supervisory review process (SRP) is to be applied in the case of AIs' exposures to cryptoassets. It sets out potential supervisory actions in cases where risks are not sufficiently covered by minimum capital requirements or AIs' risk management systems are insufficient.

Risk management systems

136 Cryptoasset activities introduce new kinds of risk and increase certain traditional risks. AIs with direct or indirect exposures or that provide related services to any form of cryptoasset must establish policies and procedures to identify, assess and mitigate the risks (including operational risks, credit risks, liquidity risks (including funding concentration risk) and market risks) related to cryptoassets or related activities on an ongoing basis. The policies and procedures followed by AIs for cryptoasset activities must be informed by the SPM modules OR-1 "Operational Risk Management" and OR-2 "Operational Resilience" on operational risk management generally as well as Statement on Cryptoassets published by the BCBS on cryptoassets in particular. In accordance with these requirements, AIs' operational risk management practices must include, but are not limited to, conducting assessments of these risks (i.e. how material these risks are, and how they are managed) and taking relevant mitigation measures to improve their operational resilience capabilities (specifically regarding information, communication, and technology (ICT) and cyber risks). The decision to hold cryptoassets (either under trading or banking book) and provide services to cryptoasset operators must be fully consistent with the AI's risk appetite and strategic objectives as set down and approved by the board, as well as with senior management's assessment of the AI's risk management capabilities, in particular for market and counterparty risk (including CVA), liquidity risk (including funding concentration risk) and operational risk.

137 Considering the particular features of cryptoassets and their markets as well as the potential difficulties in adopting standard arrangements for managing related market risk and counterparty risk, including CVA risk, AIs must conduct ex ante a prudent assessment of any cryptoasset exposures they intend to take on and verify the adequateness of existing processes and procedures. The AI must have a sound risk management approach for managing the risks of cryptoassets, including limits and hedging strategies, together with clearly assigned responsibilities for the management

of these risks. Particular attention must be paid to the assessment of the effectiveness of any hedging techniques AIs may adopt.

138 AIs must also inform the HKMA of their policies and procedures, assessment results, as well as their actual and planned cryptoasset exposures or activities in a timely manner and to demonstrate that they have fully assessed the permissibility of such activities, the associated risks and how they have mitigated such risks.

139 The mapping of risks relating to cryptoasset activities to risk categories (credit risk, market risk, and operational risk in particular) depends on how these risks manifest. Many of the risks introduced or increased by cryptoasset activities are covered by the operational risk framework (e.g. ICT and cyber risks, legal risks, money laundering and financing of terrorism). A mapping of the technological risks of cryptoassets to Basel risk categories would depend on the circumstances. If the triggering event leading to a loss is due to processes or systems outside of the AI's control and the loss to the AI manifests through the value of a held cryptoasset position, such losses would be covered by the rules related to credit risk (for banking book positions) or market risk (for trading book positions). When losses result from inadequate or failed processes, people or systems of the AI (e.g. loss of a private cryptographic key by the AI), such losses would be operational losses.

140 Risks that AIs need to consider in their risk management of cryptoassets activities include, but are not limited to, the following:

- *Cryptoasset technology risk:* AIs must closely monitor the risks inherent to the supporting technology, whether cryptoasset activities are conducted directly or through third parties, including but not limited to:
  - *Stability of the DLT or similar technology network:* the reliability of the source code, governance around protocols and integrity of the technology are among key factors related to stability of the network. Key considerations include capacity constraints, whether self-imposed or due to insufficient computing resources; digital storage considerations; scalability of the underlying ledger technology; whether the underlying technology has been tested and had time to mature in a market environment; and robust governance around changes to the terms and conditions of the distributed ledger or cryptoassets (e.g. so-called "forks" that change the underlying "rules" of a protocol). In addition, the type of consensus mechanism (i.e. for a transaction to be processed and validated) is an important consideration as it relates to the security of the network and whether it is safe to accept a transaction as "final".

- *Validating design of the DLT, permissionless or permissioned:* cryptoassets may rely on a public ("permissionless") ledger, whereby the validation of transactions can be done by any participating agent, or distributed among several agents or intermediaries, which could be unknown to the users. In contrast, a private ("permissioned") ledger restricts and pre-defines the scope of validators, with the validating entities known to the users. On a permissionless ledger, there may be less control of technology and on a permissioned ledger there may be a small group of validators with greater control. Risks related to the validating design of the DLT include the accuracy of the transaction records, settlement failure, security vulnerabilities, privacy/confidentiality, and the speed and cost of transaction processing.
- *Service accessibility:* one of the distinguishing features of cryptoassets is its accessibility to holders of these assets. A holder of cryptoassets is assigned a set of unique cryptographic keys, which allow that party to transfer the cryptoassets to another party. If those keys are lost, a holder will generally be unable to access the cryptoassets. This increases the possibility of fraudulent activities such as a third-party gaining access to cryptographic keys and using the keys to transfer the cryptoasset to themselves or another unauthorised entity. Furthermore, the risk of a large-scale cyberattack could leave AIs' customers unable to access or recover cryptoasset funds.
- *Trustworthiness of node operators and operator diversity:* since the underlying technology and node operators facilitate the transfer of cryptoassets and keep records of transactions that take place across the network, their role is essential in designating and sizing the amounts that are held by the holder. Whether nodes are run by a single operator or are distributed among many operators and whether the operators are trustworthy (e.g. whether the nodes are run by public/private institutions or individuals) are relevant considerations in third-party risk management.

- *General ICT and cyber risks:* an AI holding cryptoassets may be exposed to additional ICT and cyber risks that include, but are not limited to, cryptographic key theft, compromise of login credentials, and distributed denial-of-service (DDoS) attacks. The results of ICT failure and cyberthreats may lead to consequences such as unrecoverable loss or unauthorised transfers of cryptoassets.

- *Legal risks:* cryptoasset activities are still relatively new and quickly evolving. Thus, their legal framework remains uncertain and untested in many areas, and AIs' legal exposure is heightened, especially in the following dimensions:

- *Accounting:* there may be legal risk arising from a lack of accounting standards for cryptoassets, which could result in fines due to the underpayment of taxes or failure to comply with tax reporting obligations.
- *Taking control/ownership:* there is substantial legal uncertainty around cryptoassets, which could raise questions as to whether AIs that take cryptoassets as collateral can take possession in the event of default/margin call.
- *Disclosure and consumer protection*: AIs that issue/redeem or provide dealer or advisor services for cryptoassets can face legal risk around the disclosures they provide for the cryptoassets (including cryptoassets that are considered to be securities), particularly as regulations and laws continue to evolve (e.g. those around data privacy and data retention).
- *Uncertain legal status*: jurisdictions can decide (and have decided) to ban cryptoasset mining for a variety of reasons, including its environmental impact. Such developments could reduce the amount of computing power available to secure a network.

- *Money laundering and financing of terrorism:* AIs in their role of providing banking services to Virtual Asset Service Providers (VASP) or to customers involved in virtual asset activities, or through engaging in VASP activities themselves need to apply the risk-based approach as set out by the Financial Action Task Force (FATF) for the purposes of AML and CFT. In addition to regulatory consequences, inadequate compliance with AML or CFT laws (including sanctions) and best practices could result in operational losses and reputational damages for AIs.

- *Valuation:* Many cryptoassets pose valuation challenges, due (among other things) to their volatility and variable pricing on different exchanges, particularly given that most of the cryptoassets are currently traded on unregulated marketplaces. These challenges can result in losses for AIs in a variety of contexts tied to mispricing due to inadequate operational processes.

Supervisory review

141 *Risk identification and assessment:* under Pillar 2, the HKMA evaluates how well AIs assess their capital needs relative to their risks and take measures, where appropriate. As cryptoasset activities are something relatively new and evolving, their related risks are also evolving. Supervisory evaluation is therefore particularly relevant regarding these activities. Thus, the appropriateness of AIs' policies and procedures for identifying and assessing those risks and the adequacy of their assessment results will be subject to supervisory review. AIs will be required to address any deficiencies in

their identification or assessment process of cryptoasset risks. In addition, the HKMA may require AIs to undertake stress testing or scenario analysis to assess risks resulting from cryptoasset exposures. Such analyses can inform assessments of the AI's capital adequacy.

142 Upon the identification of capital inadequacy or shortcomings in an AI's risk management system, the specific supervisory action may vary according to the circumstances. Supervisory action may include the following:

- *Additional capital charges*: the HKMA may impose additional capital charges to individual AIs for risks not sufficiently captured under the minimum capital requirements for operational risk, credit risk, or market risk. Also, add-ons may be needed in cases where the AI's risk management of cryptoassets is considered inadequate.
- *Provisioning*: the HKMA may request AIs to provision for losses related to cryptoassets where such losses are foreseeable and estimable.
- *Supervisory limit or other mitigation measures*: the HKMA may impose mitigation measures on AIs, such as requiring an AI to establish an internal limit to contain the risks not adequately identified or assessed in the AI's risk management framework.

22 Disclosure Requirements

143 The disclosure requirements for AIs' exposures to cryptoassets or related activities must follow the five general guiding principles for AIs' disclosures set out in section 8 of the SPM CA-D-1 "Guideline on the Application of the Banking (Disclosure) Rules".[26] As such, in addition to the quantitative information, AIs must provide qualitative information that sets out an overview of the AI's activities related to cryptoassets and main risks related to their cryptoasset exposures, including descriptions of:

- business activities related to cryptoassets, and how these business activities translate into components of the AI's risk profile;
- risk management policies of the AI related to cryptoasset exposures;
- scope and main content of the AI's reporting related to cryptoassets; and
- most significant current and emerging risks relating to cryptoassets and how those risks are managed.

[26] The HKMA will consult the industry in due course the standard disclosure tables and templates for disclosure requirements.

144 In accordance with the general guiding principles, AIs must disclose information regarding any material Group 1a, Group 1b, Group 2a and Group 2b cryptoasset exposures on a regular basis, including for each specific type of cryptoasset exposure information on:

- the direct and indirect exposure amounts (including the gross long and short components of net exposures);
- the capital requirements; and
- the accounting classification.

145 In addition to the separate disclosure requirements set out above that apply to all Group 1a, Group 1b, Group 2a and Group 2b cryptoassets, AIs must include exposures to Group 1 cryptoassets in the relevant existing disclosure templates that apply to traditional assets (e.g. for credit risk and market risk).