



 DREW & NAPIER

Prudential Treatment of Cryptoassets on Permissionless Blockchains

28 April 2026

LEGAL
UPDATE

In this Guide

In April 2026, the Monetary Authority of Singapore (“MAS”) published a Consultation Paper on the Prudential Treatment of Cryptoassets on Permissionless Blockchains, setting out the applicable Classification Conditions for cryptoassets, as well as introducing a new principle-based framework.

This regulatory development also introduces deeming conditions that provide greater certainty, while also allowing for the preservation of flexibility for alternative safeguards. Banks and other market participants should assess the potential impact of these proposed Classification Conditions and review their existing arrangements for compliance with these proposed updated requirements.

03
INTRODUCTION

03
BACKGROUND: CLASSIFICATION OF CRYPTOASSETS

05
REQUIREMENTS FOR PERMISSIONLESS CRYPTOASSETS TO BE CLASSIFIED AS GROUP 1 CRYPTOASSETS

06
DEEMING PROVISIONS OF PRINCIPLE-BASED REQUIREMENTS

07
EXPOSURE AND ISSUANCE CAPS

09
PROPOSED INTERIM TREATMENT TILL THE CRYPTOASSET RULES ARE IMPLEMENTED

09
CONCLUSION

Introduction

In April 2026, the Monetary Authority of Singapore (“MAS”) published a Consultation Paper on the Prudential Treatment of Cryptoassets on Permissionless Blockchains (“**Permissionless Cryptoassets Consultation Paper**”). Cryptoassets on a permissionless blockchains are generally considered to be inherently higher risk and thus subject to more conservative prudential treatment (“**Group 2 cryptoassets**”). The Permissionless Cryptoassets Consultation Paper proposes to allow banks to classify and treat a permissionless cryptoasset as cryptoassets that bear similar risks to traditional assets (“**Group 1 cryptoassets**”) subject to certain requirements being fulfilled such that the risks arising from the use of permissionless blockchains are sufficiently mitigated.

For banks, the Permissionless Cryptoassets Consultation Paper offers certainty, expressly setting out the applicable classification conditions and enabling such banks to accurately assess their compliance against specific criteria. The presence of deeming conditions supplements this, while simultaneously preserving the flexibility for alternative safeguards to be recognised where such deeming provisions are not met.

The Permissionless Cryptoassets Consultation Paper also evinces that the MAS is willing to accommodate innovation in the blockchain and cryptoasset space, as long as the underlying risks are demonstrably mitigated. Further, as the framework adopts principle-based requirements as opposed to prescriptive rules, the framework is also well positioned to evolve alongside technological developments in the blockchain and Cryptoasset space. These principle-based requirements may also be indicative of the broader regulator expectations that may be relevant to other financial institutions in this space; any individual or entity that engages with permissionless cryptoassets would benefit from considering the risk management standards and safeguards outlined in this Permissionless Cryptoassets Consultation Paper, even where such expectations may not be directly applicable to them.

Background: Classification of Cryptoassets

- (a) Under the MAS consultation paper issued on 27 March 2025 (“**March 2025 Consultation**”) MAS had proposed that in order for a cryptoasset to qualify as a Group 1 cryptoasset, it must satisfy the following conditions:
- i. The nature and stabilisation mechanism of the asset (“**Classification Condition 1**”).
 - ii. The validity or enforceability of rights arising from the cryptoasset management (“**Classification Condition 2**”).

- iii. The transferability, settlement finality, redeemability or traceability of the cryptoasset (“**Classification Condition 3**”).
- iv. The governance and regulatory oversight of key service providers involved in cryptoasset management (“**Classification Condition 4**”).

(each a “**Classification Condition**” and collectively the “**Four Classification Conditions**”)

- (b) The MAS had identified concerns in relation to permissionless cryptoassets, including but not limited to the transferability, redeemability and traceability of such permissionless cryptoassets. Under the above proposed classification conditions, all permissionless cryptoassets would be treated as Group 2 cryptoassets and thus subject to more conservative prudential treatment applicable to Group 2 cryptoassets.
- (c) Having received feedback to the March 2025 Consultation that such a preclusion may be overly restrictive, the MAS deliberated further and agrees that permissionless cryptoassets should not be precluded from being treated as Group 1 cryptoassets should the relevant risks have been addressed. The MAS in the Permissionless Cryptoassets Consultation Paper identified the following risks when the bank takes a position in or issues a permissionless cryptoasset.
 - i. Governance Risk: Overconcentration of governance authority, reducing clear accountability.
 - ii. Technology Risk: Vulnerability to blockchain-specific attacks (e.g., 51% attacks).
 - iii. Settlement Finality Risk: Probabilistic settlement, leading to subsequent reversal.
 - iv. Anti-Money Laundering (“AML”)/Countering the Financing of Terrorism (“CFT”) risk: Pseudonymisation of permissionless assets, facilitating illicit finance that brings reputational and operational risks.
- (d) The MAS has also specified a list of deeming provisions for each of the principle-based requirements. Should the deeming provisions not be met, the bank must demonstrate, to the MAS’ satisfaction, that the permissionless cryptoasset meets the principle-based requirements specified via other forms of safeguards, before the permissionless cryptoasset can be classified as a Group 1 cryptoasset.

Requirements for permissionless cryptoassets to be classified as Group 1 cryptoassets

- (a) The MAS specifies that the bank may classify and treat permissionless cryptoassets as Group 1 cryptoassets if the bank ensures that the permissionless cryptoasset meets the Four Classification Conditions, except for the following:
- i. In relation to Classification Condition 3, the requirement that the network of the cryptoasset does not pose any material risk that could affect transferability, settlement finality or, where applicable, redeemability of the cryptoasset, and the requirement for compliance of node validators with risk governance policies and well-defined key network elements.
 - ii. In relation to Classification Condition 4, the requirement that node validators must be regulated and supervised, or subject to appropriate risk management standards, and must have in place a publicly disclosed, comprehensive risk governance framework.
- (b) To address governance risks arising from taking a position in or issuing a cryptoasset on a permissionless blockchain, banks must ensure that:
- i. The permissionless blockchain has a sufficiently diversified set of validators.
 - ii. The permissionless blockchain operates with comprehensive governance arrangements, which are clearly documented and accessible to users of the blockchain.
- (c) To address the technology risk and settlement finality risk arising from taking a position in or issuing a cryptoasset on a permissionless blockchain, banks must ensure that:
- i. The cryptoasset issuer has in place systems to ensure the accuracy and integrity of the transaction records.
 - ii. The cryptoasset issuer must have an effective business continuity plan (“**BCP**”) in place to ensure the operational resilience of the cryptoasset even if the permissionless blockchain fails.
- (d) To address the AML/CFT risk arising from the use of permissionless blockchains, banks must ensure that:

- i. The cryptoasset issuer is regulated for AML/CFT risks and maintains adequate policies for customer on-boarding, issuance and redemption of the cryptoasset.
- ii. The cryptoasset issuer must have in place mechanisms to verify the identity of each cryptoasset holder or when full verification is not possible, appropriate measures demonstrated to be effective in mitigating AML/CFT risks.

Deeming Provisions of Principle-based Requirements

- (a) The bank is deemed to mitigate governance risk, where the blockchain possesses following safeguards, including:
 - i. A sufficiently distributed validator network consisting of a significantly large number of validator nodes or no single entity controlling a significant share of validator nodes or voting power.
 - ii. The blockchain has:
 - a. Monitoring mechanisms to assess validator node performance and governance mechanisms to detect and penalise malicious behaviour or performance failures of validator nodes.
 - b. Dispute resolution mechanisms and consensus mechanisms to address any disagreements between validator nodes to allow for consensus to be reached on decisions relating to the blockchain protocol.
 - iii. Governance arrangements are clearly documented and available to users.
- (b) The bank is deemed to mitigate the technology and settlement risk, where the following safeguards are in place, including:
 - i. The cryptoasset issuer retaining control functions to correct or freeze transactions on the blockchain where necessary, and governance controls to ensure legal rights of issuers and prevent unilateral amendments.
 - ii. A defined point of finality for the underlying blockchain of the cryptoasset, documented and made available to users, referring to a level of confirmation where any transaction reversal would be impractical.
 - iii. The bank must:

- a. Establish a surveillance process, possibly conducted by reliable third-party vendors, to monitor the health of the underlying blockchain of the cryptoasset and detect anomalies, erroneous behaviours and events indicating potential cyber incidents, on the underlying blockchain.
 - b. Assess the results from the surveillance process on an ongoing basis.
 - iv. Independent third-party audits of any smart contracts used.
 - v. Regular review and test a BCP that contains at least the following to ensure that it remains fit for purpose, comprehensive and appropriate:
 - a. Documented policies on the golden source of transactions in the event of blockchain incidents.
 - b. Identification of, and well-documented backup and disaster recovery procedures for, critical business functions and systems.
- (c) The bank is deemed to satisfy the AML/CFT risk requirements, where the cryptoasset issuer has in place:
- i. Permissioning controls, possibly conducted by reliable third-party service providers, ensuring only verified white-listed entities can hold or perform transactions with the cryptoasset.
 - ii. Independent audits of smart contracts, should they be used to implement permission controls.

Exposure and Issuance Caps

- (a) The MAS introduced the following exposure and issuance caps for both locally incorporated banks and bank branches in Singapore, to contain the risks arising from permissionless cryptoassets classified as Group 1 cryptoassets, during the interim period till the rules are finalised.
- i. The MAS clarifies that the proposed exposure and issuance caps are not intended to limit banks' holdings and issuances of permissionless cryptoassets, but are instead intended to limit the amount of permissionless cryptoassets that are eligible to be treated as Group 1 cryptoassets.
 - ii. The MAS mandates that, should the caps be exceeded, banks classify the excess exposures or issuances as Group 2

cryptoassets, subject to the prudential treatment applicable to Group 2 cryptoassets, even if the permissionless cryptoasset meets the principle-based requirements, making it eligible for classification as a Group 1 cryptoasset.

- (b) The proposed exposure and issuance caps for a locally-incorporated bank are as follows:
- i. Exposure cap:
The bank must subject its exposures to permissionless cryptoassets that are classified as Group 1 cryptoassets to an exposure cap equivalent to 2% of the bank's Tier 1 capital.
 - ii. Issuance cap for liabilities:
The bank must subject its issuances of permissionless cryptoassets that result in liabilities for the bank and are classified as Group 1 cryptoassets to an issuance cap equivalent to 5% of the bank's Tier 1 capital.
- (c) The proposed exposure and issuance caps for a bank branch in Singapore ("**Singapore Branch**") are as follows:
- i. Exposure cap:
The bank must subject its exposures to permissionless cryptoassets booked in the Singapore Branch that are classified as Group 1 cryptoassets to an exposure cap equivalent to 0.2% of the total assets in the Singapore Branch.
 - ii. Issuance cap for liabilities:
The bank must subject its issuances of permissionless cryptoassets booked in the Singapore Branch that result in liabilities for the bank and are classified as Group 1 cryptoassets to an issuance cap equivalent to 1% of the total assets in the Singapore Branch.
- (d) The bank must measure each cryptoasset exposure as follows:
- i. For a direct or indirect holding of a cryptoasset, the market value of the cryptoasset.
 - ii. For a derivative referencing a cryptoasset, the delta-weighted position calculated as follows:

$$\text{Delta-weighted position} = \text{Market value of the underlying cryptoasset} \times \text{delta}$$
- (e) The bank may net long and short exposures, if the exposures are to the same cryptoasset.

- (f) The bank must not consider issuances of cryptoassets as short exposures for the purposes of calculating the exposures.

Proposed interim treatment till the cryptoasset rules are implemented

- (a) During the interim period, the bank is allowed to classify and treat a permissionless cryptoasset as a Group 1 cryptoasset if the following conditions are met:
 - i. The bank must notify MAS, with a supporting written confirmation from their executive officer that the asset and its underlying blockchain meets all principle-based requirements and deeming provisions, at least one (1) month prior to the date the bank intends to treat the permissionless cryptoasset as a Group 1 cryptoasset.
 - ii. In cases where the deeming provisions are not met, the bank must seek approval from MAS, by demonstrating that the permissionless cryptoasset meets the principle-based requirements via other safeguards.
- (b) The bank must ensure that:
 - i. Its exposures to permissionless cryptoassets, that apply to this treatment, do not exceed the specified exposure cap in the case of locally-incorporated banks or in the case of bank branches in Singapore.
 - ii. Its issuances of permissionless cryptoassets, that apply to this treatment, do not exceed the specified issuance cap for locally-incorporated banks and/or bank branches in Singapore as may be applicable.
- (c) In the case where the bank has existing exposures or issuances of a permissionless cryptoasset, classified as a Group 2 cryptoasset, the bank is allowed to reclassify the permissionless cryptoasset as a Group 1 cryptoasset if the bank ensures that the conditions specified above are met, by submitting a single notification for each permissionless cryptoasset. The bank must submit a new notification to MAS if there are any changes to the design of the permissionless cryptoasset or its underlying blockchain.

Conclusion

The Permissionless Cryptoassets Consultation Paper contains a key development in Singapore's approach to digital assets, with the MAS adopting a more risk sensitive prudential framework, recognising that

permissionless cryptoassets need not be deemed to always be “high risk” should there be necessary safeguards implemented. Banks and other market participants should assess the potential impact of the proposed Classification Conditions and review their existing arrangements for compliance with these updated requirements.

How Drew & Napier LLC can assist

Drew & Napier’s Financial Regulatory practice is well positioned to support clients in navigating the evolving regulatory landscape and in interpreting supervisory expectations with respect to the deployment and use of emerging technologies. This includes advising on the design and implementation of robust policies and procedures across a spectrum of use cases, whether in relation to traditional systems, generative AI, agentic AI or other advanced technological frameworks. The team combines deep regulatory expertise with a practical understanding of financial services operations, enabling it to deliver tailored, commercially grounded advice that aligns with applicable MAS requirements and broader governance, risk management and compliance expectations.

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval.

Special thanks to Kyra Tan, Legal Intern, for her diligent assistance with this publication.

Please feel free to reach out to us if you have any query in this area:



Grace Chong

Head, Financial Services Regulation
Director, Corporate & Finance

T: +65 8869 0445

E: grace.chong@drewnapier.com



Bryan Ong

Senior Associate, Corporate & Finance

T: +65 8058 8905


E: bryan.ong@drewnapier.com

Drew & Napier LLC

10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T: +65 6535 0733
T: +65 9726 0573 (After Hours)
E: mail@drewnapier.com

 **DREW & NAPIER**