



Re: Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures

The Global Financial Markets Association,¹ the Futures Industry Association, the Institute of International Finance, the International Swaps and Derivatives Association, the International Securities Lending Association, the Bank Policy Institute, the International Capital Markets Association, and the Financial Services Forum (collectively, the “Associations”) appreciate the opportunity to respond to the Basel Committee on Banking Supervision’s (the “Basel Committee”) second consultative document on the “Prudential treatment of cryptoasset exposures” (the “Second Consultation”).² The Associations welcome the Basel Committee’s continued focus on designing a prudential framework for cryptoassets that is risk sensitive as demonstrated by the Second Consultation, including the creation of a Group 2a cryptoasset category, and the partial recognition of hedging for and the use of modified versions of the standardised capital approaches for that category.³ Furthermore, we look forward to ongoing collaboration as these markets evolve.

The Associations support the design of a cryptoasset exposure framework that facilitates bringing these financial activities within the prudential framework where associated risks will be subject to robust capital and liquidity regulation, sound risk management and ongoing supervisory oversight. To that end, we encourage a suitably conservative but appropriately structured and designed regulatory framework and we believe our goal is very closely aligned with the objectives of the Basel Committee.

¹ GFMA brings together three financial trade associations, including the Association for Financial Markets in Europe (“AFME”), the Asia Securities Industry & Financial Markets Association (“ASIFMA”), and the Securities Industry and Financial Markets Association (“SIFMA”).

² See Appendix 5 for information regarding each of the Associations.

³ The Second Consultation defines cryptoassets as private digital assets that depend primarily on cryptography and distributed ledger or similar technology. To determine the prudential classification, cryptoassets must be screened on an ongoing basis and classified into two broad groups: Group 1a cryptoassets consisting of tokenised traditional assets; Group 1b: Cryptoassets with effective stabilisation mechanisms; and Group 2a cryptoassets (unbacked cryptoasset, including tokenised traditional assets and stablecoins that fail to meet Group 1 conditions) that pass the Group 2a hedging recognition criteria, and Group 2b: all other cryptoassets that do not satisfy Group 1 or Group 2a conditions.

With these principles in mind, the Associations' comprehensive review of the Second Consultation has identified some features and calibrations that individually and collectively would meaningfully reduce banks' ability to—and in some cases effectively preclude banks from—utilising the benefits of distributed ledger technology (“DLT”) to perform certain traditional banking, financial intermediation and other financial functions more efficiently. As a result, banks would be limited in their ability to respond to their customers' demand for access to cryptoasset products and services. That outcome is not in the best interests of customers, investors or the financial system more broadly. Indeed, the role of banks in the financial system and the scope of the financial sector within the purview of prudential regulators could be affected.⁴

Thus, our comments aim to improve the mutual understanding of current and emerging risks, the role of existing processes and frameworks for regulated entities to manage such risks, and to identify balanced solutions to help in the design of a capital framework that supports enhancing financial stability while avoiding overly restrictive limits to innovation. Getting this right is critical to meet customer demand and harness the benefits of DLT and similar technologies. For example, the speed by and transparency with which transactions can be recorded using DLT, combined with the ability to swap and record assets and cash simultaneously, (1) would help mitigate counterparty, liquidity and settlement risk, (2) allow transactions to settle, and funds and assets to reach their intended recipient, faster and (3) allow for efficiencies in collateral management.

Recent heightened volatility in cryptoasset markets has underscored the risks that emerge when a significant financial market develops outside a prudential risk management framework where excess leverage, inadequate liquidity, and lack of capital can materialise, regardless of the benefits of technology. Allowing appropriately risk-managed cryptoasset banking and other financial activities to take place within the regulatory perimeter should be a central goal of the final Basel Committee standards. A prudential framework that permits banks to support the growth of cryptoassets benefits supervisors by providing better insight into the evolution and growth of these activities (e.g., by requiring the reporting of cryptoasset exposures). At the same time, customers and investors will benefit from more transparent trusted alternatives and the protections of fully regulated institutions providing services.

Otherwise, un- and -lesser-regulated entities are likely to be predominant providers of cryptoasset-related services. The result would be an unlevel playing field and a lack of transparency in the buildup of leverage and risk in the financial system outside the regulatory perimeter. In that case, the absence of regulated financial institutions engaging in cryptoasset-related activities would be net worse than if banks were providing these

⁴ See, e.g., Caitlin Long, *Banks Are About To Face The Same Tsunami That Hit Telecom Twenty Years Ago*, FORBES (Sep. 23, 2022), available at <https://www.forbes.com/sites/caitlinlong/2022/09/23/banks-are-about-to-face-the-same-tsunami-that-hit-telecom-twenty-years-ago/?sh=3e1d483b7a7a> (stating “I fear global bank regulators are about to make a decision that will unintentionally ‘obsolete’ the banks, by prohibiting a coming tech pivot. Making this mistake would guarantee that the tech industry continues going around the banks, right as internet-native payment technologies are starting to scale.”).

services subject to an appropriately calibrated framework. Therefore, the Associations welcome the ongoing work by the Basel Committee and other global standard setters to align with “same risk, same activity, same treatment: a cryptoasset that provides equivalent economic functions and poses the same risks as a “traditional asset” should be subject to the same capital, liquidity and other requirements as the traditional asset.”⁵ As the Associations highlighted above, financial institutions can offer valuable expertise in setting market standards consistent with prudent risk management. In addition to the points noted above, bringing cryptoasset-related activities into the prudential regulatory perimeter would (1) garner the benefits of the operational risk management and operational resiliency of banks and (2) enhance customer protection due to the existing frameworks for claims against banks and their regulated affiliates, in the unlikely event of bankruptcy or insolvency.

The Associations stressed in our response (the “First Consultation Comments”) to the First Consultation that banks have a long history of integrating new technologies into their product offerings and activities and working with supervisors to ensure the regulatory framework remains fit for purpose to support safety and soundness and financial stability. As reference, in Appendix 1, we provide relevant case studies that exemplify how the banking industry is effectively collaborating with supervisors while integrating cryptography and distributed ledger or similar technology into products and services to meet client demand and to deliver market efficiencies.

At this critical juncture in the development of cryptoasset markets, there are a range of issues we ask the Basel Committee to address. Among them, two could have a gating effect: (1) the design and calibration of the Group 2 exposure limit and (2) the proposed infrastructure risk add-on for Group 1 cryptoassets. If these issues are not addressed in whole, it may not be economically viable and rational to make the investments necessary to facilitate clients’ needs on cryptoasset-related activities, which likely would result in a shift of activity in this space to the nonbank sector. The infrastructure risk add-on is particularly pronounced given the breadth of cryptoassets that the Second Consultation covers. That is, a wide range of tokenisation activities, including prudentially- and market-regulated traditional financial activities and assets, could be subject to the add-on, impacting cost structure of firms leveraging the benefits of DLT or similar technology. While a 2.5% risk-weighted asset (“RWA”) increase may not sound material, the overall position of banks trying to lessen RWA constraints combined with significant build expense would make the decision to engage in DLT infrastructure unattractive. This result also could derail the market and associated regulatory innovation via the introduction of regulatory sandboxes in a few jurisdictions starting in Q1 2023, whereby banks would need to justify additional capital requirements that would result from participation. Therefore, to avoid an effective preclusion on banks participating and developing in these markets, we underscore our view that the Basel Committee should address these two issues.

⁵ BASEL COMMITTEE ON BANKING SUPERVISION; *Prudential treatment of cryptoasset exposures* (June 2021), available at <https://www.bis.org/bcbs/publ/d519.pdf> (hereinafter the “First Consultation”) at 2.

To sum up, our overarching goal is to help in the design of a prudential framework that supports enhanced financial stability and avoids overly restrictive limits to innovation. Accordingly, the Associations have identified features of the Second Consultation that would impede banks from engaging in such activities. Specifically:

- **The Group 2 Cryptoassets Exposure Limit Is Prohibitive and Should Be Recalibrated and Calculated on a Net, Rather than Double-Gross, Basis (pp. 10-22):** The Second Consultation proposes to limit banks' exposures to Group 2 cryptoassets to 1% of the bank's Tier 1 capital, calculated on a "double-gross" basis by adding the long and short positions without any hedging recognition. The Associations believe the exposure limit construct components: (a) gross calculation methodology; (b) the extremely restrictive quantitative limit calibration; (c) the scope of cryptoasset exposures subject to the exposure limit and (d) the cliff-effect penalty resulting from an exposure limit breach, individually and collectively would effectively bar banks from participating in Group 2 cryptoassets. Importantly, the proposed methodology does not allow banks to manage limit utilisation to cryptoassets as the addition of a hedge instrument or a price increase of the underlying cryptoasset could make breaching the limit more likely by increasing the total exposure. Instead, the Associations propose that a modified exposure limit—calculated on a net basis, calibrated to 5% of Tier 1 capital and accompanied with disclosure to supervisors of gross positions, as well as a supervisory approach to any breach of the limit—would ensure adequate capitalisation and transparency while not undermining the economic viability for banks to serve clients' risk management needs with the digital and cryptoasset markets.
- **The Infrastructure Risk Add-On Is Unnecessary and Seeks to Address Risks that Are Already Addressed by the Existing Prudential Framework and Risk Management Systems (pp. 29-37):** The Second Consultation proposes an infrastructure risk add-on for all Group 1 cryptoasset exposures as well as a classification that goes beyond focusing on a bank's third-party risk management and operational resilience controls. This capital penalty and the current scope of the associated classification condition appear to be inconsistent with a technology risk-neutral approach in that the add-on penalises a particular technology and these measures are not necessary to protect the safety and soundness of banks; these risks are already addressed through existing operational risk and third-party risk management frameworks and programs⁶. Supervisory tools and controls are also available to address any such identified risks. Finally, this capital charge would act as a disincentive to banks given the significant—but necessary—investment in these technologies and systems required to appropriately service clients in these markets and could encourage the movement of cryptoasset activity outside the regulatory perimeter. The Associations recommend removing the infrastructure

⁶ BANK OF ENGLAND; *Existing or planned exposure to cryptoassets* (Mar. 24, 2022), available at <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2022/march/existing-or-planned-exposure-to-cryptoassets.pdf?la=en&hash=9C23154F16580082C3DD6437B4C3352591A0F946>.

risk add-on to reflect a more nuanced picture of how technology infrastructure can be used.

- **Group 2a Cryptoassets Hedging Recognition Should Be Further Adjusted (pp. 22-29):** While the Associations appreciate that the Second Consultation recognises partial hedging for Group 2a cryptoassets, the Associations believe that it would be appropriate to make certain further adjustments to the risk factor structure and correlation parameter calibration for Group 2a cryptoassets to more accurately reflect the actual risk characteristics of such assets and give appropriate recognition to established risk management practices.
- **The Group 1 Asset Supervisory Classification Process Is Not Workable (pp. 37-38):** The Second Consultation envisions supervisors reviewing and pre-approving a bank’s determination whether a cryptoasset qualifies as a Group 1 cryptoasset to avoid prudential treatment as Group 2. The Associations affirm the need for sustained, iterative dialogue between supervisors and banks on integrating DLT and related technologies into their activities and offerings. However, the Associations maintain that a more practical and less burdensome model for supervisory engagement would be for banks, rather than supervisors, to be responsible for making these determinations, subject to satisfying the specified, clear classification criteria. The Associations’ suggested approach would, on the one hand, be more responsive to the potentially vast universe of cryptoassets than pre-approvals for each individual cryptoasset while, on the other hand, supporting global consistency in cryptoasset treatment.
- **The Scope of the Cryptoasset Exposure Framework Should Be Clarified to Ensure that It Does Not Have Unintended Consequences (pp. 38-40, 61-63):** The Basel Committee should clarify the scope as follows:
 - *Assets under Custody:* Because assets under custody only give rise to operational risk, only the operational risk requirements of the cryptoasset exposure framework should be applicable to assets under custody both in fiduciary and non-fiduciary arrangements, similar to the treatment for traditional assets under custody.
 - *Settlement and Recordkeeping Functions:* The use of DLT for settlement or recordkeeping purposes—for example, including internally developed, private, permissioned blockchain systems— should not by itself subject the related asset to the cryptoasset exposure framework because such activities generally do not create a new asset that is distinct from the underlying asset or increase the risk or liquidity profile of the underlying assets.
 - *Scope of Exposures Subject to Group 2b:* The Associations seek confirmation that the reference to “other entities” in the scope definition of Group 2b only relates to fund vehicles and not to corporations, such as equity investments in crypto exchanges.

- **The Scope of Classification Condition 1 Should Be Revised (pp. 41-48):** Digitally native cryptoassets should be eligible for treatment as Group 1 cryptoassets. Certain requirements for Group 1a cryptoassets are overly restrictive and should be revised to better accommodate innovation in tokenised arrangements. For Group 1 cryptoassets, classification condition 1 requires minor modifications to allow digital representations of traditional assets (such as bank-issued tokens) using cryptography, DLT or similar technology to record ownership and that pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset to qualify. The Associations also welcome that the Second Consultation recognises that a stablecoin that is issued by a supervised and regulated entity should be deemed to meet classification condition 1 in lieu of the redemption risk and basis risk tests.
- **Permissionless Blockchains and Public Permissioned Blockchains Should Be Eligible for Group 1 Treatment (pp. 51-53):** Cryptoassets that are based on permissionless blockchains should be eligible to be included in Group 1, subject to the existence of certain controls. We believe that, given the risk mitigants available to banks in their engagement with this technology, permissionless blockchain should be eligible for Group 1 treatment to allow stablecoins to be used for payment. If cryptoassets based on permissionless blockchains are not eligible to be included in Group 1, those based on permissioned public blockchains should be eligible to be included in Group 1.

In addition to the main body of the letter, this letter also includes the following appendices:

- Appendix 1: Cryptoasset Case Studies and Use Cases
- Appendix 2: Proposed Rule Text for Interim Approach
- Appendix 3: Correlation Across Tenors for Bitcoin and Ether
- Appendix 4: Supporting Analysis for Exposure Limit Calibration
- Appendix 5: Background Information on the Associations
- Appendix 6: Index of Defined Terms

* * *

Table of Contents

	<u>Page</u>
I. The Group 2 Cryptoassets Limit Is Prohibitive and Should Be Recalibrated and Calculated on a Net, Rather than Double-Gross, Basis	10
A. The “double-gross” definition of exposure amount is flawed and inconsistent with prudent risk management.....	12
1. Total exposure should be calculated based on a net exposure approach to avoid prohibiting banks from providing client services for Group 2 cryptoassets	12
2. The Basel Committee could consider an Interim Approach which at least moderates the cliff effects of price increases by allowing the recognition of reduced hedging benefits	16
B. The exposure limit is calibrated so low as to effectively prohibit banks from providing client services for Group 2 cryptoassets.....	17
C. The scope of exposures subject to the Group 2 cryptoasset exposure Limit should be clarified as well as modified.....	20
D. The effect of breaching exposure limit is excessively punitive.....	21
II. Standardised Approach (“SA”) for Market Risk for Group 2a Cryptoassets	22
A. The Group 2a cryptoasset risk factor structure should be modified	22
1. The maturity dimension should be removed.....	22
2. The exchange dimension should be modified to reflect a more appropriate set of risk factors applicable to Group 2a cryptoassets	23
B. The correlation parameter for the “exchange” dimension should be recalibrated.....	23
C. Exposures to non-redeemable trusts should map to standalone buckets rather than netting with other Group 2a cryptoassets	25
D. The current 100% risk weight for each Group 2a cryptoasset bucket should be reduced	26
1. Liquidity comparison with Large Cap Equities	26
2. Liquidity comparison with FX currency pairs	27
E. Group 2a cryptoassets should not be subject to the residual risk add-on charge	28
III. The Infrastructure Risk Add-on for Group 1 Cryptoassets Is Unnecessary and Creates Negative Incentives.....	29
IV. Responsibility for Classification Determinations Should Reside with Banks.....	37
A. Banks should be responsible for determining whether a cryptoasset qualifies as a Group 1 cryptoasset, subject to satisfying specified, clear classification criteria	37

B.	Banks should also be responsible for determining whether a cryptoasset qualifies as a Group 2a cryptoasset.....	37
C.	The Basel Committee’s Supervisory Cooperation Group should maintain a list of Group 1 and 2a classification determinations for reference as cryptoasset markets develop	38
D.	Unless otherwise specified, banks should be required to assess whether a cryptoasset meets a particular classification condition on an annual basis	38
V.	The Scope of the Cryptoasset Exposure Framework Should be Clarified to Ensure that It Does Not Have Unintended Consequences.....	38
A.	The Basel Committee should clarify that assets under custody are only subject to the operational risk requirements of the cryptoasset exposure framework.....	38
B.	The Basel Committee should confirm that the use of DLT for certain settlement or recordkeeping purposes does not by itself subject the related asset to the cryptoasset exposure framework.....	39
VI.	Additional Areas for Consideration	40
A.	Classification of Group 1 Cryptoassets.....	41
1.	Classification Condition 1.....	41
2.	Classification Condition 2.....	48
3.	Classification Condition 3.....	48
4.	Classification Condition 4.....	50
5.	Permissionless Blockchains and Public Permissioned Blockchains.....	51
B.	Minimum Capital Requirements for Group 1 Cryptoassets	53
1.	Credit Risk for Group 1 Cryptoassets.....	53
2.	Market Risk, Counterparty Credit Risk and CVA Risk for Group 1 Cryptoassets.....	56
C.	Classification of Group 2 Cryptoassets.....	57
1.	Group 2a Hedging Recognition Criteria.....	57
D.	Other Issues Relating to Minimum Capital Requirements for Group 2 Cryptoassets	59
1.	Non-native Group 2a Cryptoassets (i.e., Group 1 cryptoassets that become Group 2) should be subject to Group 2a treatment for market risk.....	59
2.	Group 2a Cryptoasset ETFs should be recognised as eligible financial collateral.....	60

3.	The potential applicability of the internal models approach (“IMA”) for Group 2a cryptoassets should be revisited when more data is available.....	61
4.	Minimum Capital Requirements for Group 2b Cryptoassets	61
5.	Minimum Capital Requirements for Credit Valuation Adjustment (“CVA”) Risk.....	63
6.	Minimum Capital Requirements for Counterparty Credit Risk (“CCR”)	63
7.	Minimum capital requirements for operational risk arising from cryptoasset activities are covered by existing approaches	64
E.	Trading Book / Banking Book Boundary	65
1.	The trading book / banking book boundary for Group 1b cryptoassets should be based on the application of the boundary criteria to the stablecoin instrument itself and not the underlying reference asset(s)	65
F.	Leverage Ratio Requirements.....	66
G.	Minimum Liquidity Risk Requirements	66
1.	The Basel Committee should clarify that operational requirements for Group 1a cryptoassets to be considered as HQLA-eligible should include settlement and monetisation both on-chain and off-chain	66
2.	Certain Group 1b stablecoins backed by reserve assets that are solely HQLA should be considered as HQLA-eligible	66
H.	Technical Corrections and Questions	67
VII.	Conclusion	67

I. The Group 2 Cryptoassets Limit Is Prohibitive and Should Be Recalibrated and Calculated on a Net, Rather than Double-Gross, Basis

The Basel Committee proposes to establish a limit on banks' exposures to Group 2 cryptoassets on the basis that the large exposure rules do not impose limits on asset classes, and certain cryptoassets, such as Bitcoin, have "no counterparty." See Second Consultation page 6. The exposure limit would be 1% of a bank's Tier 1 capital "at all times" calculated on a "double-gross" basis by adding the long and short positions without any hedging recognition, and any breach of the limit would result in all Group 2a cryptoassets becoming subject to the capital requirements that apply to Group 2b cryptoassets (i.e., disallowing any offsetting or netting). See SCO60.121-124.

The Associations have four major concerns with the proposed exposure limit:

- defining the total exposure based on the addition of both the gross long and gross short exposures affirmatively penalises hedging, because hedges would contribute to the total exposure. Not only would banks be unable to manage the exposure limit by putting on more hedges, but such activity would in fact make a potential limit breach more likely by increasing the total exposure. This means that banks are unable to effectively manage their compliance with the limit and could make limit breaches inevitable merely because of price increases in the underlying cryptoassets. In the event of such a breach, the only recourse banks would have is to unwind positions. Forced selling caused by banks trying to manage their exposure limits could lead to unwanted and unnecessary market instability, especially during any period where stressed conditions prevail in the market. This design of the limit is inconsistent with long-standing risk management and hedging practices, especially since a market event that causes a fall in Group 2 cryptoasset prices would have the paradoxical effect of creating more room under the limit;
- the calibration of the limit, especially because of the proposed "double-gross" calculation methodology, at 1% of a bank's Tier 1 capital, is prohibitive for banks to offer services and products related to Group 2 cryptoassets for the benefit of their clients and will drive those services and products away from the regulated banking sector. Banks generally manage exposures at lower levels compared to regulatory exposure limits and—given the volatility in these underlying markets—the "buffer" to avoid a breach of such a low limit would need to be significant. This effect translates to even lower capacity for the banks to make markets and meet their clients' demands and could result in banks carefully considering whether it is worth the build and implementation costs for such a low exposure amount;
- the potential wide scope of exposures subject to the limit, which could result in double-counting of certain exposures already subject to the large exposure rules, include exposures that do not expose banks to direct price

risk, or cover exposures the risks of which are already fully captured by other provisions of the Basel capital framework; and

- the excessively punitive penalty for exceeding the limit and associated “cliff effect” whereby any hedging recognition is removed from the entire asset class subject to the exposure limit.

These concerns are mutually interlinked and the Associations’ recommendations with respect to them should be viewed as complimentary rather than mutually exclusive.

In addition, the specification of the Group 2 exposure limit is inconsistent with any existing limit frameworks within the capital rules with respect to the limit size, exposure calculation and the consequences of any breach. The table below lists a range of existing exposure limits that are relevant data points. Across the limit categories, the calibrations of the limits are significantly higher than the proposed 1% in the Second Consultation even though the limits have similar goals in ensuring that exposures remain manageable relative to a bank’s loss-absorbing capacity. None of these limits are based on a double-gross basis. In fact, all of them allow either long and short positions or against certain liabilities. Finally, the penalty of breaching any of the limits below is less punitive than what is proposed in the Second Consultation. With respect to the threshold deductions, the penalty only applies to the excess exposures, not all exposures; and with respect to the large exposure framework, the consequence of a breach is a notification to the supervisor with a requirement to take corrective actions.

Threshold	Limit	Netting	Citation
Threshold Deduction for Non-Significant (<10%) Unconsolidated Financial Institutions	■ 10% of CET1	■ Net long position	■ CAP 30.22, 30.23, 30.26
Threshold Deduction for Significant (>=10%) Unconsolidated Financial Institutions	■ 10% of CET1	■ Net long position	■ CAP 30.29, 30.32(1)
Threshold Deduction for Mortgage Servicing Assets	■ 10% of CET1	■ Net of associated DTLs	■ CAP 30.7, 30.32(2)
Threshold Deduction for Temporary Difference Deferred Tax Assets	■ 10% of CET1	■ Net of associated DTLs	■ CAP 30.9, 30.32(3)
Combined Threshold Deduction	■ 15% of CET1	■ Same netting as for individual deductions	■ CAP 30.33
Large Exposure Limits	■ 25% of T1 (15% of T1 for G-SIB/G-SIB)	■ Net of credit risk mitigation (banking book) ■ Net long position (trading book)	■ LEX 20.1, 30.13, 30.07-30.13, 30.23-30.31

Given the significant enhancements to micro- and macro-prudential regulation and supervision that have taken place since the global financial crisis, including extensive

supervisory review and stress testing, the minimum standards should be designed and calibrated to facilitate participation in digital and cryptoasset markets, and not to limit participation to uneconomic levels for banks.

A. The “double-gross” definition of exposure amount is flawed and inconsistent with prudent risk management

As part of prudent risk management practices, banks proactively engage in risk mitigation activities such as hedging. The proposed definition of the exposure amount within the Group 2 cryptoasset exposure limit not only fails to recognise prudent risk management by hedging, but also treats *both sides* of a risk position and its hedged position (the long *and* the short) as separate exposures that should be aggregated for purposes of applying the exposure limit.

The Associations believe that this is a flawed approach and, by failing to distinguish between risk-taking positions and risk-mitigating positions it creates a perverse incentive that is contrary to what prudent risk management would dictate. It is an approach that is internally inconsistent within the Second Consultation itself – i.e., the recognition of hedging in calculating market risk capital requirements for Group 2a cryptoassets – and is also inconsistent with the recognition of hedging in numerous other parts of the Basel framework, such as the calculation of net long and short positions for threshold deductions from CET1 capital and the use of net credit exposures for purposes of the large exposure limits, as demonstrated in Section I above.⁷ In fact, the Associations are unaware of any part of the Basel framework in which a gross limit is based on the sum of long and short positions.

To remedy this flaw, the Associations strongly recommend that the proposed definition of the exposure amount for purposes of the exposure limit be modified to be calculated on a net basis by cryptocurrency for Group 2 exposures.

1. Total exposure should be calculated based on a net exposure approach to avoid prohibiting banks from providing client services for Group 2 cryptoassets⁸

Under this approach, all instrument-level exposures to a given unique Group 2 cryptoasset (e.g., the exposure from a long Bitcoin exchange traded fund (“ETF”) and from a short Bitcoin Chicago Mercantile Exchange (“CME”) future would be part of the same Group 2a cryptoasset, namely Bitcoin) are allowed to net to arrive at that Group 2a cryptoasset-level net exposure. The total exposure to all Group 2a cryptoassets for purposes of this

⁷ The Associations note that the Basel Committee invoked the large exposure rules in explaining the need for the proposed Group 2 cryptoasset limit. The Associations see no reason why the large exposures rules’ recognition of net exposures should not apply to this limit as well.

⁸ The Associations acknowledge that Group 2b cryptoassets would be included in the exposure limit as proposed in the Second Consultation. However, the Associations suggest to exclude Group 2b from the exposure limit as per Section I.C and therefore, the proposal is limited to Group 2a cryptoassets.

limit is equal to the sum of the absolute values of all Group 2a cryptoasset-level net exposures:

$$Total\ Exposure = \sum_c^C \left| \sum_i^I Instrument\ Exposure_i \right|$$

where C denotes the number of distinct Group 2 cryptoassets (e.g., all instruments referencing Bitcoin are considered as exposures to Bitcoin), c denotes a given cryptoasset, i denotes the i th instrument belonging to cryptoasset c and I denotes the number of instruments relating to specific cryptoasset c .

As of the date of this letter, the Associations believe that only Bitcoin and Ether would qualify as Group 2a cryptoassets based on application of the relevant hedging recognition criteria.

- (a) The net exposure approach is supported by the highly effective hedging of Group 2a exposures (i.e., spot Bitcoin and Ether with their respective futures or ETFs).

A common method to demonstrate the strength of the relationship between two independent variables is regression analysis.⁹ The regression involves determining the correlation between the two variables by looking at the slope and the coefficient of correlation of the best fit line between changes in the hedged item and hedging instrument. A pair consisting of a hedged item and a hedging instrument is deemed to be effective if the regression intercept ($|\hat{\beta}|$) and coefficient of determination (R -squared) satisfy the following conditions: $0.80 \leq |\hat{\beta}| \leq 1.25$ and $R\text{-squared} \geq 0.80$.

⁹ FINCAD; *Basics of Hedge Effectiveness Testing and Measurement*, available at <https://www.cmegroup.com/education/files/basics-of-hedge-effectiveness.pdf>.

The table below shows the hedge effectiveness test results for spot Bitcoin and Ether positions and their respective candidate hedging instruments as of July 15, 2022:

Hedged Item	Hedging Instrument	5d returns			10d returns			30d returns		
		$\hat{\beta}$	R-squared	effective	$\hat{\beta}$	R-squared	effective	$\hat{\beta}$	R-squared	effective
Bitcoin	CME BTC Futures	0.97	0.94	TRUE	0.97	0.98	TRUE	1.02	0.99	TRUE
Bitcoin	CME BTC micro Futures	0.98	0.95	TRUE	0.94	0.96	TRUE	0.96	0.99	TRUE
Bitcoin	ICE Bakkt Bitcoin Futures	1.01	0.98	TRUE	1.02	0.99	TRUE	1.01	1.00	TRUE
Bitcoin	ProShares Bitcoin Strategy ETF	0.99	0.99	TRUE	0.99	0.99	TRUE	0.98	1.00	TRUE
Bitcoin	VanEck Bitcoin Strategy ETF	0.99	0.99	TRUE	1.00	0.99	TRUE	0.90	0.99	TRUE
Bitcoin	BetaPro Inverse Bitcoin ETF	(1.02)	0.96	TRUE	(1.02)	0.97	TRUE	(1.04)	0.98	TRUE
Bitcoin	Bitcoin ETF CAD	0.95	0.97	TRUE	0.96	0.99	TRUE	0.96	0.99	TRUE
Bitcoin	Eurex future on BTCetc	0.90	0.88	TRUE	0.91	0.95	TRUE	1.06	0.97	TRUE
Bitcoin	BTCetc	0.94	0.96	TRUE	0.98	0.97	TRUE	0.97	0.99	TRUE
Ether	CME ETH Futures	1.01	0.95	TRUE	0.96	0.97	TRUE	0.99	0.99	TRUE
S&P 500 Index	SPDR S&P 500 ETF TRUST	1.00	1.00	TRUE	1.00	1.00	TRUE	1.00	1.00	TRUE
Russel 2000 Index	CME E-mini Russell 2000 Index Futures	1.01	0.99	TRUE	1.01	1.00	TRUE	0.99	1.00	TRUE
NASDAQ 100 Index	Generic 1st NASDAQ 100 E-mini	1.00	0.99	TRUE	1.00	1.00	TRUE	1.01	1.00	TRUE

Hedged Item	Hedging Instrument	5d returns			10d returns			30d returns		
		$\hat{\beta}$	R-squared	effective	$\hat{\beta}$	R-squared	effective	$\hat{\beta}$	R-squared	effective
Bitcoin	Grayscale Bitcoin Trust	1.01	0.69	FALSE	1.11	0.80	FALSE	1.07	0.86	TRUE
Ether	Grayscale Ethereum Trust	0.95	0.39	FALSE	1.08	0.46	FALSE	1.18	0.43	FALSE

The first table shows that the hedging instruments for spot Bitcoin and Ether are highly effective and are comparable to the hedging relationships between large equity indices such as the S&P 500, the Russell 2000, the NASDAQ 100, and their respective futures and ETFs.

In contrast, the second table shows a low correlation for Bitcoin and Ether Grayscale trust funds (GBTC and ETHE, respectively), which are neither futures nor ETFs. The Associations believe that the poor hedge effectiveness of GBTC and ETHE is driven by the non-redeemable structure of trusts (as opposed to ETFs), which leads to a relatively low correlation parameter. As described in Section II.C below, in order to include fund exposures with other Group 2a cryptoasset exposures referencing the same cryptoasset, a mechanism needs to exist where shares can be created and redeemed at will. Because Grayscale would not satisfy this criterion, the Associations believe that its use in generalising the effectiveness of hedging is unwarranted.

To further support this analysis, a hedge effectiveness stability test was conducted over six series of stability tests with different types of sub-periods (90 days using five-day log returns, 180 days using five-day log returns, 180 days using 10-day log returns, 360 days using five-day log returns, 360 days using 10-day log returns, and 360 days using 30-day log returns) to ensure the presence of sufficient regression data points in each sub-period for the results to be meaningful.

For each scenario, the table below shows the proportion of sub-periods where hedging is effective. For example, if there were 10 consecutive sub-periods of 90 days, and nine sub-periods showed effective hedging, the stability tests would return a score of 90%, indicating that hedging would be consistently effective over the period. A high percentage value close to 100% indicates a consistently effective hedging relationship, while a low percentage

indicates a consistently ineffective hedging relationship. The range of sub-periods used tends to show that hedging is either consistently effective, or consistently ineffective.

Hedged Item	Hedging Instrument	90d period, 5d returns	180d period, 5d returns	180d period, 10d returns	360d period, 5d returns	360d period, 10d returns	360d period, 30d returns
Bitcoin	CME BTC Futures	95%	100%	100%	100%	100%	100%
Bitcoin	CME BTC micro Futures	100%	100%	100%	100%	100%	100%
Bitcoin	ICE Bakkt Bitcoin Futures	100%	100%	100%	100%	100%	100%
Bitcoin	ProShares Bitcoin Strategy ETF	100%	100%	100%	100%	100%	100%
Bitcoin	VanEck Bitcoin Strategy ETF	100%	100%	100%	100%	100%	100%
Bitcoin	BetaPro Inverse Bitcoin ETF	100%	100%	100%	100%	100%	100%
Bitcoin	Bitcoin ETF CAD	100%	100%	100%	100%	100%	100%
Bitcoin	Eurex future on BTCetc	100%	100%	100%	100%	100%	100%
Bitcoin	BTCetc	100%	75%	100%	100%	100%	100%
Ether	CME ETH Futures	100%	100%	100%	100%	100%	100%
S&P 500 Index	SPDR S&P 500 ETF TRUST	100%	100%	100%	100%	100%	100%
Russel 2000 Index	CME E-mini Russell 2000 Index Futures	100%	100%	100%	100%	100%	100%
NASDAQ 100 Index	Generic 1st NASDAQ 100 E-mini	91%	100%	100%	100%	83%	100%

Hedged Item	Hedging Instrument	90d period, 5d returns	180d period, 5d returns	180d period, 10d returns	360d period, 5d returns	360d period, 10d returns	360d period, 30d returns
Bitcoin	Grayscale Bitcoin Trust	57%	42%	50%	50%	67%	50%
Ether	Grayscale Ethereum Trust	31%	43%	29%	33%	33%	33%

As described previously and in more detail in Section II.C below, the Associations believe the use of GBTC and ETHE in determining the effectiveness of hedging is unwarranted.

- (b) The net exposure approach would be limited to calculation of the total exposure for the exposure limit

The net exposure approach is simple and transparent. It recognises the full benefit of hedging within each Group 2a cryptoasset and properly incentivises – instead of working at cross-purposes with — prudent risk management. It would still be consistent in principle with the capital requirements for Group 2a cryptoassets because the full hedging benefits under this option are recognised solely for purposes of the exposure limit. The hedging benefits under the capital requirements for Group 2a cryptoassets would continue to be only partially recognised through, for example, the correlation parameter under the standardised approach for market risk. The Associations believe that using this net exposure approach for the Group 2a cryptoasset exposure limit strikes the right balance between responsible financial innovation and prudent risk management practices by banks. It also gives banks the tools necessary to manage their exposures against this limit without becoming forced sellers, which could result in liquidity spirals and market instability.

The Associations recognise that the Basel Committee may wish to have more insight into the gross long exposures and the gross short exposures that banks net against one another, on the basis that there may be a difference in risk profile between a bank that reports a net exposure of \$10 million based on netting a gross long position of \$10 billion and a gross short position of \$9.99 billion, and a bank that reports a net exposure of \$10 million based on netting a gross long position of \$20 million and a gross short position of \$10 million. To address this issue, the Associations believe that the Basel Committee should require that banks disclose, for Group 2a cryptoassets, their gross long and short positions and their net exposure amount to their supervisor. Such an approach would give banking supervisors the transparency they need to address any concerns about any outsized gross positions

without sacrificing long-standing principles of prudent risk management and without disincentivising hedging activities for Group 2a cryptoassets.

2. *The Basel Committee could consider an Interim Approach which at least moderates the cliff effects of price increases by allowing the recognition of reduced hedging benefits*

If the Basel Committee is unwilling to adopt the net exposure approach described above given the nascence of this asset class, the Associations would propose an approach that at least provides some reduced recognition of hedging benefits (the “Interim Approach”) until this market is more established. The Associations recommend that the Interim Approach be reviewed by the Basel Committee every two years to ensure the calibration and calculation methodology are still appropriate given this rapidly evolving market.

This Interim Approach would introduce a hedging disallowance parameter (R) that would ensure a minimum exposure amount for fully hedged positions. If this approach were to be adopted, the Associations would propose setting R at 20% which over time could be reduced to zero as the market matures.

The exposure per Group 2a cryptoasset would consist of the net exposure, i.e., the unhedged component and a percentage equal to R of the hedged exposure:

$$\textit{Total Exposure} = \textit{Unhedged Exposure} + R \times \textit{Hedged Exposure}$$

- *Unhedged Exposure* is equal to the absolute difference between the long positions and short positions for a particular Group 2a cryptoasset. Derivative exposures must be measured using a delta-equivalent methodology.
- *Hedged Exposure* is the lower of the absolute value of the gross long positions and gross short positions for a particular Group 2a cryptoasset. Derivative exposures must be measured using a delta-equivalent methodology.
- R is the hedging disallowance parameter.

The example below illustrates how this approach would be calculated for a sample portfolio:

Sample Portfolio:

Cryptoasset	Product	Maturity	Exchange	Exposure
BTC	Spot	0	Exchange 1	30,000
BTC	Futures	0.5	Exchange 1	(60,000)
BTC	Option	1	Exchange 1	20,000
BTC	Spot	0	Exchange 2	15,000
ETH	Spot	0	Exchange 2	15,000
ETH	Futures	0.25	Exchange 2	(20,000)

Delta-Adjusted Exposure to Bitcoin and Ether Using the Interim Approach:¹⁰

BTC	Exposure	Interim Approach	Interim Approach	Interim Approach	Net Approach	Double Gross
Total Long (1 + 3 + 4)	65,000					
Total Short (2)	(60,000)					
Total Hedged Amount	60,000	Hedged Exposure * R	= 60,000 * 20% =	12,000		
Total Unhedged Amount	5,000	Unhedged Exposure	= 5000 * 100% =	5,000		
Total BTC Exposure				17,000	5,000	125,000
ETH	Exposure	Interim Approach	Interim Approach	Interim Approach	Net Approach	Double Gross
Total Long (5)	15,000					
Total Short (6)	(20,000)					
Hedged	15,000	Hedged Exposure * R	= 15,000 * 20% =	3,000		
Unhedged	5,000	Unhedged Exposure	= 5000 * 100% =	5,000		
Total ETH Exposure				8,000	5,000	35,000
TOTAL EXPOSURE				25,000	10,000	160,000

The Interim Approach would not recognise the full benefits of hedging and its degree of misalignment with prudent risk management practices compared to the net exposure approach depends on the size of the hedging disallowance parameter. While this approach would be an improvement compared to the “double-gross” exposure calculation as currently defined, it still would not allow a bank to fully control and manage the utilisation of its exposure limit. An increase in the price of the underlying cryptoasset could still lead to a limit breach and there is nothing the bank could do within its control to avoid such a breach beyond promptly liquidating its position, which could result in value-destroying fire sales. See Appendix 2 for proposed rule text reflecting the Interim Approach.

B. The exposure limit is calibrated so low as to effectively prohibit banks from providing client services for Group 2 cryptoassets

As shown above, the proposed 1% limit is much lower than comparable limits within the capital framework that also aim at minimising the impact of systematic risks on banks

¹⁰ Note in this example R is set to 20%.

relative to their loss-absorbing capacity. Consequently, in addition to the need to revise the definition of the total exposure amount as described above, the Associations believe that the calibration of the limit itself – 1% of a bank’s Tier 1 capital – is too restrictive and not proportional to the potential risks in relation to comparable limit frameworks. In addition, the limit is so restrictive that it effectively shuts banks out of being able to provide an appropriate level of products and services for Group 2 cryptoassets to their clients. Banks typically manage their exposures at a lower level than any applicable regulatory limits, thereby reducing even more their capacity to make markets and meet client demand. In addition, given the volatility of these Group 2 assets which would likely lead to a larger buffer below the actual limit, it is unlikely that banks would invest in the build costs associated with this very limited amount of permitted activity.

To put the proposed 1% of Tier 1 capital total exposure limit in context, the Associations looked to other asset classes to assess the footprint necessary for banks to facilitate client demand. Based on availability of data, the Associations looked at banks’ equity investments in financial institutions (“FI”), which banks report including gross long and short positions at least annually (e.g., on the G-SIB disclosure interconnectedness indicator schedule).

FI Footprint		Cryptoasset Footprint	
Category	Value	Category	Value
FTSE All World Index market cap	\$73.8tn		
FI Stocks in the index market cap	\$10.5tn	Cryptoasset market cap	\$2.2tn
FI Investment (Double Gross Long / Short)	\$664bn	Comparable Cryptoasset Footprint (Double Gross Long / Short)	\$138bn
FI Footprint (Double Gross Long / Short)	6.3%	Comparable Cryptoasset Footprint (Interim Approach)	\$98bn
FI Investment (Interim Approach)	\$469bn		
FI Footprint (Interim Approach)	4.5%		
GSIB Cryptoasset Capacity			
Tier 1 capital of 21 GSIB			\$2.1tn
1% capacity			\$21bn
5% capacity			\$104bn

Comparable Footprint
Vs
Capacity

As shown in the table above, the Associations reviewed data for 21 (out of 30) G-SIBs as of year-end 2021, again based on disclosure data.¹¹ The total financial sector securities gross exposure for these 21 G-SIBs was \$664 billion on a “double-gross” basis or \$469 billion based on the Interim Approach as described in Section I.A.2, including R set to 20%. To calculate a relative measure of the banks’ footprint, the Associations approximated the universe of FI stocks by looking at their share of the FTSE All World Index as of year-end 2021, which was \$10.5 trillion out of \$73.8 trillion total market capitalisation. The G-SIB footprint is then 6.3% (\$664 billion out of \$10.5 trillion) on a “double-gross” basis or 4.5% (\$469 billion out of \$10.5 trillion) based on the Interim Approach.

¹¹ See [Appendix 4](#) for additional supporting information and limitations of this analysis.

The cryptoasset market capitalisation across all coins was approximately \$2.2 trillion as of year-end 2021 according to CoinMarketCap. A comparable client footprint to the one G-SIBs have in equity investments in FIs would result in a “double-gross” exposure of \$138 billion (i.e., 6.3% of \$2.2 trillion) or in an exposure of \$98 billion (i.e., 4.5% of \$2.2 trillion) based on the Interim Approach. To relate this comparable footprint to the maximum capacity afforded by the proposed Group 2 cryptoasset limit, the Associations collected the aggregated Tier 1 capital of the analysed 21 G-SIBs, which was \$2.1 trillion. The proposed 1% limit would correspond to \$21 billion of aggregate exposure for the G-SIBs, falling far short of \$138 billion or \$98 billion. Even an increase of the limit to 5% would result in a capacity of \$104 billion, which is still significantly below the comparable footprint based on the “double-gross” approach and is only approximately equal to the comparable footprint under the Interim Approach. In short, the G-SIBs simply could not provide a comparable level of client facilitation and intermediation services in respect of Group 2 cryptoassets as they can provide for the financial sector based on the proposed limit exposure specification for Group 2 cryptoassets.

While this analysis already shows the constraints of the proposed limit, it likely understates the issue because investments in other FIs are discouraged and therefore the footprint for FI investments is most likely lower than that for other investments. Furthermore, for purposes of this analysis, the Associations did not match long and short positions; however, for cryptoasset exposures, banks are most likely to closely hedge their exposures and therefore the proposed gross limit would be even more constraining.

The proposed calibration of the exposure limit would (i) stifle banks from offering innovative financial products or services related to Group 2 cryptoassets, and (ii) drive or keep that activity (and the clients needing their banks to offer products and services for Group 2 cryptoassets related to that activity) away from the regulated financial sector that is subject to the Basel capital framework into under-regulated or completely unregulated sectors. From a systemic risk perspective, the Associations do not understand how keeping Group 2 cryptoassets out of the perimeter of highly regulated and prudentially supervised financial institutions would contribute to the financial stability of the jurisdictions that have adopted the framework. In particular, banks are best positioned to apply disciplined risk management in the cryptoasset sector, including robust risk governance and controls in areas such as know-your-customer, anti-money laundering, counterterrorism financing and operational risk. By pushing Group 2 cryptoassets out of the regulated banking perimeter, regulators everywhere will have less visibility in the evolution of cryptoasset ecosystem, its various market participants, and the complexity of emerging cryptoasset products and services.

To strike the right balance between the benefits of bringing Group 2 cryptoassets within the perimeter of highly regulated and prudentially supervised banks and the Basel Committee’s concerns about a potential gap in the large exposure rules for exposures to Group 2 cryptoassets as an asset class, the Associations recommend increasing the exposure limit to 5% of a bank’s Tier 1 capital. This limit, when coupled with the adoption of the net exposure approach described above, would provide clients of banks with the benefit of a more appropriate level of products and services relating to this asset class

instead of forcing them to use products and services offered by less regulated or unregulated market players.

As demonstrated in Section I above, a limit of 5% of a bank's Tier 1 capital would be substantially lower than the 25% of Tier 1 capital limit (for banks that are not G-SIBs) and the 15% of Tier 1 capital limit (for banks that are G-SIBs) under the large exposure rules of the Basel framework, especially taking into account the fact that the large exposure rules permit the exposures to be calculated on a net basis. It would also be generally lower than the 10% of CET 1 capital limits under the threshold deduction approach for certain exposures under the Basel capital framework such as significant investments in unconsolidated financial institutions, which are also calculated on the basis of net long positions. These other capital limits are relevant because they represent the tolerance levels set by regulators for banks' financial sector exposures relative to their loss-absorbing capacity in other contexts. The Associations therefore believe that the modified limit would still be conservative, in line with the Basel Committee's evident concerns about banks' exposures to Group 2 cryptoassets.

C. The scope of exposures subject to the Group 2 cryptoasset exposure Limit should be clarified as well as modified

The Group 2 cryptoasset exposure limit applies to banks' aggregate exposures, including both direct holdings (cash and derivatives) and indirect holdings (through, for example, investment funds, ETFs and SPVs). *See* SCO60.121. Furthermore, SCO60.124(2) refers to "individual gross long and short exposures." The Associations seek clarification that only positions with direct price risk to Group 2 cryptoassets, i.e., where the bank is long or short, are included and not exposures where there is no direct price risk. Under this approach, a securities financing transaction ("SFT") referencing Group 2 cryptoassets, margin loans or client-cleared exposures where the bank acts as clearing member to clear trades for clients would not be in scope for the exposure limit. With respect to SFTs with collateral consisting of Group 2 cryptoassets, a bank is exposed to counterparty credit risk, which is already subject to the large exposure framework, and there is no direct price risk to Group 2 cryptoassets. In addition, any Group 2 collateral that is recognised on a bank's balance sheet would already be included in this limit as an on-balance sheet exposure and therefore, if SFTs were included, there would be a double count. With respect to client-cleared exposures referencing Group 2 cryptoassets where banks clear trades for clients in their capacity as clearing members banks are only exposed to counterparty credit risk. Hence, there is no direct price risk to underlying Group 2 cryptoassets and the counterparty credit risk component to the client is already fully covered by the large exposure framework.

The Associations urge the Basel Committee not to penalize client-clearing by including client-cleared exposures, where the bank acts as clearing member to clear trades for clients, in the Group 2 cryptoasset exposure limit. If these exposures are included, the framework would undermine consensus reforms and discourage banks from facilitating the central clearing of cryptoasset linked derivatives, thereby limiting the risk-reducing effect on

cryptoasset markets that central clearing has on other derivative markets and limiting hedging opportunities for market participants.¹²

In addition, consistent with the principle that only exposures to direct price risk should count against the exposure limit, the Associations request confirmation that assets held under custody would not count towards the exposure limit. Assets under custody generally do not expose banks to credit or market risk, only to operational risk, and any operational risk arising from Group 2 cryptoassets would be addressed by the existing operational risk provisions of the capital rules. Moreover, any limit calibrated at 1% or even 5% of Tier 1 capital, if applied to any amount of assets under custody, would prevent any bank from acting as custodian for Group 2 cryptoassets.

The Associations also believe that Group 1 cryptoassets that fail the classification conditions applicable to Group 1 cryptoassets should be excluded from the Group 2 cryptoasset exposure limit to the extent that the underlying traditional assets would be subject to the large exposure rules. This exclusion would avoid the double-counting problem already described above. In addition, it would avoid a potential limit breach arising from a mere reclassification of a Group 1 instrument as Group 2.

The Associations believe that the scope of Group 2 cryptoasset exposures that are subject to the exposure limit should also exclude Group 2b cryptoassets because this category of cryptoassets is already subject to a punitive capital treatment, namely, a 1250% risk weight applied to the max gross long or short position. As a 1250% risk weight effectively requires a bank to deduct the exposure amount from its regulatory capital by holding at least as much capital against the exposure as the amount of the exposure itself, the Associations believe that applying the Group 2 exposure limit to Group 2b cryptoassets would be redundant and unnecessary. The 1250% risk weight would already act as an effective deterrent to banks' engagement with Group 2b cryptoassets.

D. The effect of breaching exposure limit is excessively punitive

The penalty for exceeding the Group 2 exposure limit is to lose all hedging recognition that was previously recognised for all Group 2a cryptoassets and to subject all Group 2a cryptoassets to the same capital treatment as for Group 2b cryptoassets, namely, a 1250% risk weight applied on a maximum of gross long and gross short exposures basis. *See* SCO60.123, SCO60.89. The Associations believe that this approach is excessively punitive and could create the cliff effect of a sudden increase in a bank's RWAs and a sudden decrease in the bank's CET 1 and Tier 1 risk-based capital ratios. There is no precedent or risk management basis for this draconian impact, as previously explained in Section I above.

¹² The Futures Industry Association ("FIA") is filing a supplemental response to the Second Consultation providing more detail about aspects of the Second Consultation related to client clearing, and specifically why the Group 2 cryptoasset exposure limit should clarify that client clearing is out of scope as clearing member banks do not have direct exposure to the changes in value of the client's underlying position.

To avoid this cliff effect and the unprecedented effect of penalising an entire asset class when limits are breached, the Associations recommend modifying the exposure limit provisions of the Second Consultation by requiring a bank to immediately notify its primary regulator of any breach of the exposure limit and to promptly provide a plan to come back into compliance with the exposure limit. This is similar to the approach applied in the event of a breach of the Liquidity Coverage Ratio or the large exposure framework. The large exposure limit framework specifies that when “breaches of the limit [occur], which must remain the exception, [it] must be communicated immediately to the supervisor and must be rapidly rectified.” *See* LEX20.3.

Accordingly, the Basel Committee should not prescribe a specific consequence or capital penalty of a breach of the exposure limit but should leave that to the discretion of national supervisors based on the individual facts and circumstances that gave rise to the breach. If a national supervisor decides to impose a capital penalty for a limit breach, the Associations also believe that, absent special circumstances, any penalty for a Group 2 cryptoasset exposure limit breach should be applied only to the exposure amount in excess of the limit rather than to all Group 2 cryptoassets in order to prevent the cliff effect described above.

The existing capital rules where limits are specified require the breached excess to be penalised and not the entire asset class. For example, under CAP30.226, if the total holding of capital instruments and other TLAC liabilities in aggregate exceed 10% of the bank’s CET1, then “the amount above 10% is required to be deducted.” In addition, the 15% limit threshold on significant investments in unconsolidated FIs, mortgage service rights, and DTAs when breached will apply a capital deduction only to the excess above the threshold. *See* CAP30.33 FAQ1.

II. Standardised Approach (“SA”) for Market Risk for Group 2a Cryptoassets

A. The Group 2a cryptoasset risk factor structure should be modified

Under the SA for market risk for Group 2a cryptoassets, the Second Consultation contemplates using delta sensitivities based on a risk factor structure that considers two dimensions: (1) the exchange and (2) time to maturity, at certain prescribed tenors. *See* SCO60.79. The Second Consultation explicitly cites the risk factor provision for commodities, MAR21.13, and in fact the prescribed risk factor structure for Group 2a cryptoassets is like that of commodities. As explained in MAR21.13(1), “[F]or some commodities such as electricity . . . the relevant risk factor can either be the spot or the forward price, as transactions relating to commodities such as electricity are more frequent on the forward price than transactions on the spot price.” Commodity delta risk factors are thus determined along two dimensions: (1) the delivery location, and (2) time to maturity of the traded instrument.

1. The maturity dimension should be removed

The Associations note, however, that the valuation of transactions relating to Group 2a cryptoassets are based on spot prices rather than forward prices. Storage costs and the

associated convenience yields that may drive forward prices for commodities are not relevant to cryptoassets. CME Bitcoin futures are based on the CME Crypto Facilities Bitcoin Reference Rate, which reflects the USD price of one Bitcoin on major Bitcoin spot exchanges. Like the delta risk factors for foreign exchange (“FX”) and equity, cryptoasset spot prices do not have a tenor dimension. Any funding-related risk factors as a result of buying or selling the cryptoasset forward would be captured as general interest rate risk factors as defined in MAR21.8. This funding risk is not inherent in the cryptoasset price, unlike commodities where—as mentioned above—storage costs and convenience yields can influence forward prices. As a result, the Associations recommend the removal of the maturity dimension from the delta risk factor structure under SCO60.79(2).¹³

2. *The exchange dimension should be modified to reflect a more appropriate set of risk factors applicable to Group 2a cryptoassets*

The Associations recommend modifying the exchange dimension in SCO60.79(1) to reflect a more appropriate set of risk factors applicable to Group 2a cryptoassets. The reference to “exchange” in SCO60.79 should be modified to read: “(i) exchange or market, or (ii) reference rate or instrument,” and should explicitly state that the following types of trades or positions would be treated as having the same delta risk factor:

- Any derivatives referencing the same cryptocurrency benchmark rate (e.g., the CME Bitcoin Reference Rate) should be assigned to the same risk factor. This includes both uncleared and cleared derivatives, e.g., NDFs and futures (listed on any regulated exchange), provided they all reference the same rate.
- Any derivative (e.g., an uncleared swap, a listed option, or a cleared Future) referencing the price of the same crypto ETF/ exchange traded note (“ETN”) (e.g., BITO or BTC, etc.) and any trading book position in that ETF/ETN should be assigned to the same delta risk factor.
- All direct holdings of a cryptoasset for which execution is not tied to a specific exchange or market, and for which execution services are available that meet the criteria in that jurisdiction for best execution should be assigned to the same delta risk factor. This ensures a more appropriate netting logic based on the underlying price risk. For example, ETFs might be listed on different exchanges, but ultimately the price risk is the same and banks should be allowed to apply netting to the exposures. Similarly, if the underlying reference rate is the same, netting should be possible across an OTC derivative and a listed derivative such as the CME future.

B. The correlation parameter for the “exchange” dimension should be recalibrated

The correlation parameter for the intra-bucket correlation parameter ρ_{kl} is set to 94%. See SCO60.81. The calibration of this parameter is inconsistent with observed correlations.

¹³ If the Basel Committee were to retain the maturity factor it should be calibrated to at least 99%. See [Appendix 3](#) for supporting analysis.

The Associations analyzed the correlation along the exchange dimension for spot and futures. The tables below show the pairwise correlations of spot Bitcoin and Ether between the various exchanges, based on 10-day overlapping returns, and supports a correlation parameter along the exchange dimension of at least 99%:

Spot Bitcoin Correlation Across Exchanges (data sourced from TradingView for period May 2021 to August 2022)

10d Returns								
	Binance	Binance US	Bitfinex	Bitstamp	Coinbase	FTX	Gemini	Kraken
Binance	100.00%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%
Binance US		100.00%	100.00%	100.00%	100.00%	100.00%	99.99%	100.00%
Bitfinex			100.00%	100.00%	100.00%	100.00%	99.99%	100.00%
Bitstamp				100.00%	100.00%	100.00%	100.00%	100.00%
Coinbase					100.00%	100.00%	99.99%	100.00%
FTX						100.00%	99.99%	100.00%
Gemini							100.00%	99.99%
Kraken								100.00%

Spot Ether Correlation Across Exchanges (data sourced from TradingView for period October 2021 to August 2022)

10d Returns								
	Binance	Binance US	Bitfinex	Bitstamp	Coinbase	FTX	Gemini	Kraken
Binance	100.00%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%	99.98%
Binance US		100.00%	100.00%	100.00%	100.00%	100.00%	99.99%	100.00%
Bitfinex			100.00%	100.00%	100.00%	100.00%	99.99%	100.00%
Bitstamp				100.00%	100.00%	100.00%	100.00%	100.00%
Coinbase					100.00%	100.00%	99.99%	100.00%
FTX						100.00%	99.99%	100.00%
Gemini							100.00%	99.99%
Kraken								100.00%

The below table shows Bitcoin futures correlation across exchanges (data sourced from Bloomberg for period January 1, 2017 to July 15, 2022):

10d Returns				
	Bitcoin spot	CME BTC Futures	CME BTC micro Futures	ICE Bakkt Bitcoin Futures
Bitcoin spot	100.00%	99.01%	99.36%	99.70%
CME BTC Futures		100.00%	100.00%	99.18%
CME BTC micro Futures			100.00%	99.43%
ICE Bakkt Bitcoin Futures				100.00%

The “Generic 1st” Bitcoin futures time series between CME and ICE have a correlation of 99% using 10-day returns. The strength of the spot and generic futures correlation suggests that a correlation parameter along the exchange dimension would be appropriately set at 99%.

In light of these results,¹⁴ the Associations believe that the Second Consultation’s proposed correlation parameter of 94% for a single bucket is far too conservative and should be recalibrated to 98%, which reflects the empirical data plus a small buffer for conservatism.

An illustration of the capital and RWA impact with different correlation parameters is provided below using a long Bitcoin ETF hedged by short Bitcoin futures at notional. The simple portfolio contains long Bitcoin ETF CAD (with exposure +\$100) and short CME Bitcoin Futures (with exposure -\$100).

	Transaction	Risk Exposure	FRTB Exposure	Risk Weight	Implied RWA	Required Capital ¹
Long ETF / Short CME (different exchange, $\rho = 94\%$)	■ Long: \$100	■ \$0	■ \$34.6	■ 1250%	■ 433	■ \$34.6
	■ Short: \$100					
Long ETF / Short CME (different exchange, $\rho = 98\%$)	■ Long: \$100	■ \$0	■ \$20	■ 1250%	■ 250	■ \$20
	■ Short: \$100					

Based on the Associations’ revised risk factor dimension of “(i) exchange or market, or (ii) reference rate or instrument,” these two instruments would not map to the same risk factor and their exposures would not net, but a correlation parameter would be applied due to the difference in the “exchange dimension” for the two instruments. In this context, the CME future would be assigned to the CME Bitcoin Reference Rate risk factor, while the ETF would be assigned to the ETF Bitcoin risk factor.

However, the capital requirement for the portfolio would be \$34.6 using the Second Consultation correlation parameter of 94%. Using a more appropriate correlation parameter of 98%, the capital requirement would be \$20. This calculation is based on the pairwise correlation for delta sensitivities within a bucket (given that this is a standalone asset class) without considering adjustments for high, medium, and low correlation scenarios at an aggregated level (across risk classes), which could result in a higher capital charge.

C. Exposures to non-redeemable trusts should map to standalone buckets rather than netting with other Group 2a cryptoassets

As shown in Section I.A.1(a) above, the Associations understand that the proposed correlation parameter may have been set based on the poor hedge effectiveness of non-redeemable trusts (e.g., GBTC and ETHE) driven by the structure of trusts (as opposed to ETFs). However, the Associations believe that the inclusion of non-redeemable trusts data in calibrating the correlation parameter for Group 2a cryptoassets is unwarranted as this type of instrument would not meet the criteria for Group 2a cryptoasset designation. Instead, the Associations propose to introduce a further criterion for closed-end funds to

¹⁴ See [Appendix 3](#) for more correlation analysis across different products consistent with the high correlation parameters shown above.

be assigned to the same bucket as the Group 2a cryptoasset they reference. For a closed-end fund to be assigned to the same bucket as the underlying Group 2a cryptoasset, a mechanism for the closed-end fund needs to exist where shares can be created and redeemed at will in order to balance demand and supply of the shares. This added criterion would further exclude non-redeemable trusts from the Bitcoin Group 2a cryptoasset bucket, thus creating a standalone bucket.

D. The current 100% risk weight for each Group 2a cryptoasset bucket should be reduced

The Associations also recommend reducing the current 100% risk weight for each Group 2a cryptoasset as proposed in SCO60.78.

Implied RWs based on 10-day price returns from 1-Oct-2017 to 15-Jul-2022:

Liquidity Horizon	Group 2a*		Group 2b**	
	99% VaR	97.5% ES	99% VaR	97.5% ES
10 days	64	64	94	107
20 days	90	90	132	151
60 days	156	156	229	261
120 days	221	221	324	369

* Group 2a sample includes Bitcoin cash, Bitcoin, Bitcoin futures, and Ether

** Group 2b sample includes Litecoin, BAT, Neo, XRP, Dogecoin

The Associations believe that a lower risk weight of 64% is supported by the fact that Group 2a cryptoassets are more liquid than single-name large cap equities and have comparable liquidity to certain FX currency pairs, both of which are assigned a 10-day liquidity horizon (see MAR33.12, table 2). Accordingly, Group 2a cryptoassets should also have a liquidity horizon of 10 days.

In the comments to the First Consultation, the Associations acknowledge that they advocated for a 20-day liquidity horizon. However, the Associations believe that a change to 10-day liquidity horizon is now justified because the Second Consultation has introduced strict criteria relating to trading volumes and the qualifications for Group 2a cryptoassets that were not part of the First Consultation.

1. Liquidity comparison with Large Cap Equities

In order to compare the liquidity profile of large cap equities that receive a 10-day liquidity horizon, the Associations looked at the trading volume for EQ FTSE All-World Index as of July 15, 2022, selecting 3,774 constituents that met the definition for large cap (\$2 billion USD) pursuant to MAR 21.74.¹⁵ The 1-year average daily trading volume was

¹⁵ The FTSE All-World Index covers 90-95% of the world's investable market capitalization. The index includes over 40 countries in developed and emerging markets and approximately 4,000 constituents. Due to data availability the actual index used excludes Greece or approximately 12 constituents representing approximately 3bps of total market capitalization.

approximately **\$129 million**, with a median of **\$35 million**, for data spanning one year up to July 15, 2022. Comparing the large cap equity trading volume over the same period to the 1-year average daily trading volume of BTC/USD and ETH/USD, which were **\$1.9 billion** and **\$1.5 billion**, respectively, demonstrates that BTC/USD and ETH/USD trading pairs are significantly more liquid than large cap equities. Similarly, Euro trading pairs with BTC and ETH 1-year average daily trading volume of **\$344 million** and **\$231 million**, respectively, exceeded large cap equity trading volume.

2. Liquidity comparison with FX currency pairs

In addition to large cap equity trading volumes, the Associations compared the trading volume of FX specified currency pairs that receive a 10-day liquidity horizon with BTC and ETH spot trading pair volume. FX specified currency pairs are defined in MAR 33.12 to include, but not limited to, USD/EUR, EUR/JPY, USD/ZAR, USD/TRY, USD/NOK, USD/BRL and JPY/AUD. Furthermore, MAR33.12 Footnote 1 states that currency pairs forming first-order crosses across the specified currency pairs are also subject to the same 10-day liquidity horizon. This would include, but is not limited to, EUR/CAD and JPY/NZD.

The Associations reviewed a sample of FX currency pair trading volumes published by the Bank for International Settlements (“BIS”) Triennial Central Bank Survey of Foreign Exchange and Over-the-Counter Derivatives Markets 2019. The sampled currency pairs are presented in the table below.¹⁶

FX Currency Pair	Spot volume from BIS Survey (bn USD)	LH 10-days in MAR 33.12
USD/EUR	416.3	Specified Currency Pair
EUR/JPY	44.3	Specified Currency Pair
USD/ZAR	24.8	Specified Currency Pair
USD/TRY	22.2	Specified Currency Pair
USD/NOK	18.7	Specified Currency Pair
JPY/AUD	17.8	Specified Currency Pair
USD/BRL	13.4	Specified Currency Pair
EUR/SEK	18.7	First-Order Cross
EUR/NOK	17.5	First-Order Cross
EUR/AUD	8.2	First-Order Cross
EUR/CAD	5.7	First-Order Cross
JPY/CAD	3.1	First-Order Cross
JPY/NZD	2.7	First-Order Cross
JPY/TRY	1.0	First-Order Cross
JPY/ZAR	0.8	First-Order Cross
EUR/TRY	0.7	First-Order Cross
JPY/BRL	0.1	First-Order Cross

The Associations analyzed the trading volume for a variety of BTC and ETH trading pairs, including stablecoin pairs (see table below), to determine whether the volume was

¹⁶ This statistical release concerns the Spot FX turnover part of the 2019 Triennial Survey, which reports the daily average currency pair volumes for April 2019. The values reported are from the detailed Annex tables, available at https://www.bis.org/statistics/rpfx19_fx_annex.pdf.

consistent with the currency pairs receiving a 10-day liquidity horizon. The Associations believe that the liquidity horizon test should also include stablecoin pairs because when traders rebalance or reduce their cryptoasset exposures, they sell into stablecoins, which reduces friction costs and tax impacts. The traders then sell out of stablecoins when they buy back into the cryptoasset market. Therefore, the expectation is trading volume for cryptoassets will generally tend to be paired more with stablecoins than with fiat currencies.

According to the trading volume results, BTC/USDT and ETH/USDT 1-year average daily trading volumes were **\$10.8 billion** and **\$6.3 billion**, respectively. These volumes are consistent with, and exceed, many of the sampled first-order cross currency pairs. BTC/USDT volume is also consistent with USD/BRL specified currency pair volume of **\$13.4 billion**. Furthermore, BTC/USD and ETH/USD 1-year average daily trading volumes of **\$1.9 billion** and **\$1.5 billion** are also consistent with and exceed some of the sampled first-order cross currency pairs that receive a 10-day liquidity horizon.

Estimated 1-year average volumes for selected crypto trading pairs across a significant sample of the main exchanges (stablecoins highlighted)¹⁷

BTC pair	1-year avg volume (bn USD)	ETH pair	1-year avg volume (bn USD)
BTC_USDT	10.78	ETH_USDT	6.26
BTC_USD	1.95	ETH_USD	1.50
BTC_BUSD	0.67	ETH_BUSD	0.51
BTC_EUR	0.34	ETH_EUR	0.23
BTC_USDC	0.26	ETH_USDC	0.12
BTC_KRW	0.13	ETH_KRW	0.08
BTC_GBP	0.06	ETH_GBP	0.04
BTC_TRY	0.03	ETH_TRY	0.03
BTC_JPY	0.01	ETH_JPY	0.00
BTC_DAI	0.01	ETH_DAI	0.02

The Associations therefore believe that a 10-day liquidity horizon for Group 2a cryptoassets can be supported because BTC and ETH volumes are generally more liquid than single-name large cap equities and have comparable liquidity to FX currency pairs.

E. Group 2a cryptoassets should not be subject to the residual risk add-on charge

The Associations believe that Group 2a cryptoassets should not be subject to any residual risk add-on (“RRAO”) for market risk. If the Basel Committee does not reduce the risk

¹⁷ The trading pair volume was sourced by CCTX and represents over 80% of the global volume for each specified crypto trading pair. BANK FOR INTERNATIONAL SETTLEMENTS; *Triennial Central Bank Survey: Global foreign exchange market turnover in 2019* (Dec. 8, 2019), available at https://www.bis.org/statistics/rpfx19_fx_annex.pdf.

weight below 100% as recommended above, the application of an RRAO could have the effect of increasing a Group 2a cryptoasset's risk weight above 100%, which would effectively mean that a bank would need to hold more capital against the exposure than the market risk to which it is exposed on that exposure.

III. The Infrastructure Risk Add-on for Group 1 Cryptoassets Is Unnecessary and Creates Negative Incentives

While we acknowledge and support the Basel Committee's decision not to proceed with the operational risk add-on that was proposed in the First Consultation, the Associations do not support the proposed application of an infrastructure risk add-on for all Group 1 cryptoasset exposures.

The proposed infrastructure risk add-on represents a divergence from the recognition in the Second Consultation that Group 1a and Group 1b assets pose similar risks to their underlying traditional assets, and thus effectively departs from a technology risk-neutral approach in that it appears to single out a particular technology.¹⁸ The Second Consultation properly recognises that, compared to traditional assets, there may be additional exposures resulting from the structural arrangements of Group 1 cryptoassets (e.g., exposures to redeemers or other intermediaries), and that capital should be held against those exposures. Those additional capital requirements arise from additional risks related to the legal and operational structures of the cryptoassets. The Second Consultation affirmatively singles out the DLT infrastructure on which cryptoassets are based as being "new and evolving" and, notwithstanding substantial work to date by central banks and private sector participants to validate the effective functioning of DLT as a reliable tool that can be utilised to reduce (rather than increase) risks, affirmatively concludes that it "may pose various unforeseen risks" that should then be subject to a specific additional charge.

The infrastructure risk add-on is thus a capital penalty applied to all assets that *may* use DLT against the currently unforeseen risks that the infrastructure *may* produce. It would be applied regardless of whether the technology may actually *reduce* certain risks (such as the risks arising from extended settlement periods for transactions) and costs (such as those associated with the use of decentralised and paperless recordkeeping and tracking assets).

In that regard, the use of DLT can be fully consistent with existing BIS guidance relating to legal certainty and finality of settlement. For example, the BIS CPMI Consultative Report *Facilitating increased adoption of payment versus payment*¹⁹ contains repeated examples of how DLT can reduce settlement risk by means of enabling payment-versus-payment arrangements that build on a foundation of processes that entail appropriate legal

¹⁸ See First Consultation at 2.

¹⁹ BANK FOR INTERNATIONAL SETTLEMENTS; COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES; *Consultative report: Facilitating increased adoption of payment versus payment (PvP)* (July 2022), available at <https://www.bis.org/cpmi/publ/d207.pdf> (the "CPMI July 2022 Consultative Report").

certainty and finality and can reduce risk. Similar examples are found in other use case studies sponsored by the BIS and that involved the BIS Innovation Hub, including Project Helvetia (which utilised a DLT-based platform to demonstrate the reduction of securities settlement risk)²⁰ and Project Dunbar (which utilised DLT to align settlements of different currencies on a cross-border basis).²¹ Other central banks have similarly applied DLT to accomplish risk reduction for cross-border payments (Project Jasper-Ubin, which involved the Bank of Canada and the Monetary Authority of Singapore)²² and to ensure that risks of incorrect payments could be effectively controlled within a DLT-based network (such as Project Stella, which involved the Bank of Japan and the European Central Bank).²³ Application of a monolithic add-on, regardless of legal certainty and finality, cannot be reconciled with existing BIS guidance.

The infrastructure risk add-on also does not recognise the benefits of existing regulatory and industry-wide frameworks to mitigate infrastructure risk in DLTs and other digital technologies. **Banking organisations are already required to actively manage third-party relationships, including with respect to information security, operational resilience, and safe market and trading practices, among other factors.**²⁴ As such, **existing frameworks require firms adopting these new technologies to proactively identify and manage infrastructure risk, overall contributing to the soundness and safety of these platforms as they are adopted.**

Appendix 1 includes a series of case studies and use cases which demonstrate the risk management approaches, systems, procedures and protocols being applied by banks in arranging and facilitating cryptoasset transactions and services. These cases showcase the adoption, adaptation and expansion of bank risk management frameworks for this new asset class and demonstrate the rigorous system and risk management controls being undertaken in order to mitigate and manage operational and infrastructure risk. These cases also demonstrate the benefits this innovative technology is bringing to financial services. These cases include:

- *Digital Bond Issuance by European Investment Bank (“EIB”): Permissioned tokenised traditional assets in a permissionless blockchain.* This case study showcases the risk management protocols and critical processes in identification, validation and

²⁰ BANK FOR INTERNATIONAL SETTLEMENTS; *Project Helvetia: A multi-phase investigation on the settlement of tokenised assets in central bank money*, available at <https://www.bis.org/about/bisih/topics/cbdc/helvetia.htm>.

²¹ BANK FOR INTERNATIONAL SETTLEMENTS; *Project Dunbar: international settlements using multi-CBDCs*, available at <https://www.bis.org/about/bisih/topics/cbdc/dunbar.htm>.

²² BANK OF CANADA AND MONETARY AUTHORITY OF SINGAPORE; *Jasper-Ubin Design Paper*, available at <https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf>.

²³ BANK OF JAPAN AND EUROPEAN CENTRAL BANK; *STELLA – joint research project of the European Central Bank and the Bank of Japan* (Feb. 2020), available at https://www.boj.or.jp/en/announcements/release_2020/data/re1200212a1.pdf.

²⁴ See, e.g., BASEL COMMITTEE ON BANKING SUPERVISION; *Outsourcing in Financial Services* (Feb. 2005), available at <https://www.bis.org/publ/joint12.pdf>.

verification, data retention, monitoring, registration, settlement and business continuity planning for this groundbreaking digital bond transaction. It also demonstrates the risk management and compliance framework adopted for the successful issuance in a permissionless blockchain of the bonds as permissioned tokens.

- *Intraday Repo: Permissioned tokenised traditional assets in a private blockchain which enables secured and rapid intraday repo transactions.* Utilising DLT as a key enabler, this use case demonstrates the speed and efficiency and risk reduction for such transactions in a way not achievable on traditional platforms and elaborates on the steps taken in risk mitigation and management.
- *The JPM Coin: a permissioned blockchain system for recording deposit account balances and making instant payments.* This case study illustrates the successful integration and interaction of a DLT-based system with existing systems for a product which facilitates instantaneous payments, addresses challenges of cross-border payments, simplifies liquidity funding requirements of clients and delivers enhanced corporate treasury solutions.
- *Third-Party Vendor Engagement and Management: Identification, Selection and Onboarding of Digital Custodians:* This case study demonstrates the comprehensive review, qualification and risk-assessment procedures undertaken by banks in selecting suitably qualified third-party vendors in the digital arena. The case study elaborates upon the adaptation and extension of the bank's third-party risk management framework to digital service providers, including review and approval procedures by extended and dedicated risk committees. The stringent risk management procedures required by the banks of third-party vendors are helping to cultivate a virtuous cycle of more effective control environments as regulated entities increase engagement with digital third parties.

More fundamentally in prudential capital terms, the add-on sets a precedent for applying a capital penalty to the introduction of any new technology, notwithstanding that new technology infrastructure developments, such as new software, new communications systems and new technology platforms (such as e-mail, the Internet, smartphones, mobile applications, artificial intelligence and the cloud) have been introduced in the banking system over the past several decades without needing the attention of a special infrastructure risk add-on in the Basel capital framework. The infrastructure risk add-on represents a blunt instrument for seeking to capture unknown and unidentified risks of a certain technology, and as such could be categorised as a tax on innovation, which is in contravention of regulators' oft-stated desire to support innovation in financial services.

The cost of capital (especially regulatory capital) is a factor that can affect whether a bank offers a product or service, as well as the pricing, volume of business and the contractual and other terms on which a product or service is offered by a bank. It is the Associations' understanding that one of the purposes of the infrastructure risk add-on is to address potential basis risks between tokenised and traditional forms of an asset. However, the higher cost of capital associated with DLT-related activities could cause pricing dislocation (i.e., basis) between the tokenised and traditional forms of an asset, which is seemingly counter to this purpose as these pricing effects could give rise to the basis risk that the

infrastructure add-on itself seeks to address. **All other things being equal, if the cost of regulatory capital between tokenised products or stablecoins and their underlying traditional assets are higher for the cryptoassets than for the traditional assets (due to the impact of the capital penalty), the infrastructure risk add-on, combined with the significant build and management cost associated with this activity, will act as a strong disincentive for banks to offer clients private digital assets, products, or services that depend on cryptography and DLT or similar technology.**

In turn, this would very likely have two consequences; first, it will inappropriately restrict banks from offering innovative financial products or services merely because they are in the form of digital assets based on a new technology infrastructure; and secondly, it will drive that activity (and the clients needing their banks to offer products and services for the asset classes related to that activity) away from the regulated financial sector into less comprehensively regulated markets, with the consequent loss of transparency and supervisory oversight. The Associations do not believe that either of those consequences would contribute to a more accessible, competitive, inclusive, and innovative banking sector or to the financial stability across jurisdictions. DLT already has extensive applications in banking and finance, including (i) payments and cross-border remittance, (ii) anti-money laundering (“AML”), know your customer (“KYC”), and client onboarding, (iii) trade finance, (iv) asset tokenisation, (v) exchanges and platforms, (vi) fund and distribution transactions, (vii) trade execution, (viii) supply chain management, (ix) clearing and settlement of securities, and (x) corporate actions, shareholders’ rights and proxy voting. The imposition of a capital penalty based on whether an asset has underlying DLT would represent a tax on innovation and risk undermining progress in all these areas.

The Associations also believe that the infrastructure risk add-on is unnecessary and duplicative of existing requirements under the Basel capital framework and other provisions of the Second Consultation itself, especially after taking into account the CPMI July 2022 Consultative Report (as discussed above) and multiple use case studies by the BIS and central banks.

First, Group 1 cryptoassets are subject to four classification conditions, one of which, classification condition 3, explicitly requires “[t]he 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.” See SCO60.21 (emphasis added). Among the requirements that must be met to satisfy classification condition 3 are:

- The functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets, and the network on which the cryptoasset runs, do not pose any material risks that could impair the transferability, settlement finality or redeemability of the cryptoasset; and
- A network that satisfies this condition would have well-defined key aspects such that all transactions are traceable, with the key aspects being (i) operational structure, (ii) degree of access, (iii) technical roles of the nodes, and (iv) validation and consensus mechanism.

See SCO60.22. As discussed in Section VI.A.3 below, the Associations have recommended narrowing classification condition 3 to focus on banks' operational resilience and third-party risk management controls and capabilities with respect to cryptoasset and DLT networks. Even if modified in accordance with these recommendations, classification condition 3 would still require that, before a bank can classify a cryptoasset as a Group 1 cryptoasset, it should satisfy itself that it can manage the very types of risks that the infrastructure risk add-on is presumably intended to cover, including its understanding of the legal certainty and finality required elsewhere in the Second Consultation and covered in existing Basel Committee guidance.

Secondly, banks are required to calculate operational risk RWAs for their exposures, including cryptoasset exposures, as specifically contemplated by the Second Consultation. *See* SCO60.105. Cryptoasset exposures are currently extremely limited in the context of operational risk capital that firms are already holding against tail risks in traditional assets. Existing capital processes will capture digital assets exposure as it becomes a higher concentration of banks' overall portfolios.

Banks must currently calculate operational risk RWAs for:

- external fraud (which cover systems security);
- business and system disruption (which cover losses arising from hardware, software, telecommunications and utility failures);
- clients, products and business practices (which cover legal settlements and fines); and
- execution, delivery and process management (which cover losses from failed transaction processing or process management, including with respect to vendors).

Banks will also be required to do so under the new Standardised Approach for Operational Risk that becomes effective in January 2023. *See* OPE 25 (Calculation of RWA for Operational Risk – Standardised Approach), 25.17 and Table 2.

Applying this new standardised operational risk framework generally results in a significant increase to a bank's operational risk RWAs. Again, these include the very types of risks that the infrastructure risk add-on is presumably intended to cover. These risks are assessed according to the prevailing risks that are applied to applicable facts and circumstances, rather than the monolithic add-on proposed in the Second Consultation, which may add capital charges where the facts and circumstances underlying loss events and operational risk RWA calculations would not require such a result.²⁵

²⁵ In this context, the Associations seek confirmation that the Group 1 infrastructure risk add-on would not apply to exposures, such as Group 1 cryptoassets held under custody by a bank, that do not generate any credit risk or market risk for the bank. The Second Consultation is clear that the infrastructure risk add-on would increase total credit risk RWAs and total market risk RWAs. *See* SCO60.57(1) – (2). The Second

Third, the Basel capital framework contemplates, and the Second Consultation itself specifically refers to, the supervisory review process that can result in pillar 2 requirements above and beyond the capital requirements for operational risk and a bank's own internal risk management framework. *See* SCO60.105. As described in the Second Consultation's section on a bank's risk management framework and the supervisory review process, a bank's internal risk management framework should address, with respect to its activities in cryptoassets:

- Cryptoasset technology risk, including (a) the stability of the DLT or similar technology network, (b) validating the design of the DLT, (c) service accessibility, and (d) the trustworthiness of node operators and operator diversity;
- Information, communication and technology (“ICT”) and cyber risks;
- Legal risk;
- Money laundering and financing of terrorism risk; and
- Valuation issues.

See SCO60.130. The pillar 2 supervisory review process includes an evaluation of how well a bank assesses its capital adequacy relative to its risks. *See* SCO60.131. This assessment appropriately adapts capital requirements to applicable facts and circumstances, rather than imposing a monolithic add-on as proposed in the Second Consultation. In the United States, prior to engaging in new cryptoasset activities, a bank must notify its supervisor and demonstrate that it has adequately considered and addressed the risks associated with the activity.²⁶

In light of the foregoing three levels of requirements or controls – the classification conditions, operational risk requirements, and (where applicable) the pillar 2 supervisory review process – the Associations believe that the types of risks that the proposed infrastructure risk add-on is presumably designed to address would in fact already be more than adequately covered. This is consistent with the findings of the BIS's own Financial Stability Institute, which found that among supervisory authorities with a holistic operational resilience policy, the definition of important operations and services takes a macroprudential view but setting standards of resilience for these operations and services and testing against these standards are left to individual firms.²⁷

Consultation does not contemplate any increase in operational risk RWAs. In light of the broad reference to exposures that only give rise to operational risk in SCO60.4, the Associations seek confirmation that the infrastructure risk add-on would not apply to increase operational risk RWAs, which instead would be calculated under the applicable operational risk provisions of the Second Consultation.

²⁶ *See* the Board of Governors of the Federal Reserve System's (“FRB”) SR 22-6, the Office of the Comptroller of the Currency's (“OCC”) Interpretive Letter #1179 and the Federal Deposit Insurance Corporation's (“FDIC”) FIL-16-2022.

²⁷ BANK FOR INTERNATIONAL SETTLEMENTS; FINANCIAL STABILITY INSTITUTE; *FSI Brief No 17: Safeguarding operational resilience: the macroprudential perspective* (August 2022), available at <https://www.bis.org/fsi/fsibriefs17.pdf>.

Accordingly, while it is appropriate for the Basel Committee to identify DLT infrastructure as a potential source of operational risk, the Associations believe that it would not be appropriate to prescribe a specific standard infrastructure risk add-on charge to deal with this risk when individual firms are better suited to quantify and mitigate their specific idiosyncratic DLT risks.

For example, to address the risk of an unforeseen outage of the DLT infrastructure on which a Group 1 cryptoasset may be based, which may create a temporary unavailability of transaction processing capabilities and the record of the relevant cryptoassets' completed transactions, the Associations believe that it would be consistent with classification condition 3 and the supervisory requirements for a bank's vendor risk management framework to ensure that there is an appropriate business continuity plan ("BCP") for the technology network's operator. The BCP could include an external data recording system (e.g., a back-up system stored on the cloud) under which a registrar acting on behalf of the issuer of the instrument must adopt such a BCP in the event of a DLT outage.²⁸ Banks already currently use BCPs to address risks associated with traditional assets. The Associations believe that would be a more appropriate way of addressing these types of technology infrastructure risks than an add-on capital requirement.

When considering a bank's exposure resulting from a DLT outage, the most important considerations are (1) the bank's financial exposure to the DLT, (2) the time period of the outage and (3) the availability of alternate mechanisms to execute the activity. None of these considerations are unique to DLT and the DLT-specific unknowns that are of potential concern (e.g., the potential failure modes of the DLT) are of a secondary importance compared to these primary considerations.

If the Basel Committee aims to mitigate an operational failure, in this case specifically a technology failure, cyber or otherwise, it appears to be conflating the concepts of operational and financial resilience by putting financial resilience measures in place to mitigate an operational resilience issue. This is unlikely to work as in the event of a catastrophic technology failure, because capital does not help and will not "recover" the technology or corrupted data. This is the reason the Basel Committee separately released *Principles for Operational Resilience*.²⁹

An important consideration is that DLT may actually reduce infrastructure risk compared to the current centralised financial market utilities ("FMUs"), where an outage of the FMU would make it impossible to process transactions, building up settlement risk and creating single points of failure. In a DLT environment, where the unavailability of a processing node can be compensated by other nodes assuming that activity, that risk is actually

²⁸ See, e.g., French Decree No. 2018-1226 of Dec. 24, 2018 related to the use of a shared electronic recording system for the purpose of representing and transferring securities and issuing and selling minibons.

²⁹ BASEL COMMITTEE ON BANKING SUPERVISION; *Principles for Operational Resilience* (Mar. 2021), available at <https://www.bis.org/bcbs/publ/d516.pdf>.

reduced. It is therefore inappropriate to add a fixed surcharge to DLT infrastructures where they could actually reduce systemic risk.

Moreover, to the extent that the infrastructure risk add-on is intended to address concerns about differences between the risk weights applicable to the underlying traditional assets and an issuer of the Group 1 cryptoassets, the Associations believe this risk is already captured by existing capital requirements or in the Second Consultation itself. If there is a difference in risk weight between an underlying traditional asset (e.g., 0% for U.S. Treasuries) and an issuer of a Group 1b stablecoin based on that underlying traditional asset (e.g., a bank with a 20% risk weight), that difference is already captured by the requirement to recognise a credit risk on the stablecoin's redeemer. *See* SCO60.39.

The Associations do not believe that the potentially temporary nature of the proposed infrastructure risk add-on mitigates the Associations' concerns, especially given that any sunset period must first be agreed to by the Basel Committee and then considered and adopted by national regulators, meaning that it will in practice be several years longer than any decision by the Basel Committee. *See* SCO60.58.³⁰ The cryptoasset market is not a mature market and will likely react and respond rapidly even to short-term differences in capital costs between cryptoassets and traditional assets. Nor will it be possible, given the inherent discretion that banking supervisors can be expected to retain over the applicability, conditions and duration of the infrastructure risk add-on, for banks or the cryptoasset markets to have sufficient certainty of when the infrastructure add-on would cease to apply. Furthermore, since the risks that the risk add-on is intended to address are not specified or identified, it is extremely difficult if not impossible for banks to determine or demonstrate if these 'unknown' risks have been sufficiently diminished or eliminated. The combination of these factors means that, in effect, the difference in capital requirements between Group 1 cryptoassets and their underlying traditional assets will be assumed to be permanent or in any event long-term.

In short, the Associations are concerned that the infrastructure risk add-on, when combined with the build cost for developing or investing in new technology and the related risk management controls, will act as a significant disincentive to banks to appropriately invest in and participate in these markets and to develop their business of supporting clients' activities in Group 1 cryptoassets. As the Associations have previously stated, regulated banks deliver significant benefits in terms of sophisticated risk management capabilities, liquidity, reporting and client protections for these markets, making them safer, more efficient and more transparent.

The infrastructure risk add-on represents a capital add-on which inappropriately penalises the involvement of regulated banks in core banking and client activities as the market evolves and embraces DLT to bring financial products in a more streamlined and efficient

³⁰ The Associations also note that the proposed infrastructure risk add-on would not apply to Group 1a cryptoassets that are backed by the full faith and credit of a central bank or sovereign entity. *See* SCO60.58. Because the infrastructure risk add-on is supposed to cover the risks of the technology infrastructure itself, the Associations do not understand the relevance of whether the issuer of the cryptoasset is or is not a sovereign.

way to the market. This inhibition for the regulated sector to innovate would pose risks on its own beyond just core cryptoasset market activity.

IV. Responsibility for Classification Determinations Should Reside with Banks

A. Banks should be responsible for determining whether a cryptoasset qualifies as a Group 1 cryptoasset, subject to satisfying specified, clear classification criteria

The Second Consultation contemplates supervisors reviewing and approving banks' demonstrations of whether a cryptoasset qualifies as a Group 1 cryptoasset (SCO60.26). The statement that "[a] cryptoasset must be classified as a Group 2 cryptoasset, unless a bank demonstrates to the supervisor that the cryptoasset meets all the classification conditions" (SCO60.26) could be read to impose a requirement for affirmative prior regulatory approval for every classification of a Group 1 cryptoasset.

In the First Consultation Comments, the Associations suggested that banks, rather than supervisors, should be responsible for determining whether a cryptoasset qualifies as a Group 1 cryptoasset, subject to satisfying specified, clear classification criteria. The Associations continue to believe this should be the case. Under the Basel Framework, banks make other determinations of capital treatment, such as whether an exposure is subject to the general credit risk framework or the securitisation framework, applying the relevant definitions for what constitutes a securitisation exposure. As we noted in the First Consultation Comments and in other engagements, our suggested approach would help to ease administrative and operational burdens for both supervisors and banks and support global consistency in cryptoasset treatment. For example, if the Basel Committee adopts its suggestion that digital assets issued by a supervised and regulated institutions could qualify for Group 1a treatment, a bank should be able to make that determination without needing to seek supervisory approval. A requirement for banks to obtain pre-authorisation for Group 1 treatment will be impractical for both national authorities and banks given the potentially vast universe of these type of assets. DLT could become the main conduit for transacting in all sorts of financial instruments if expected efficiency gains materialise. Requiring banks to treat all cryptoassets as Group 2 unless and until they obtain supervisory approval would effectively preclude banks from continuing to participate in core banking functions, such as trading, underwriting, and origination.

B. Banks should also be responsible for determining whether a cryptoasset qualifies as a Group 2a cryptoasset

The Second Consultation does not specify whether banks or supervisors should be responsible for determining whether a Group 2 cryptoasset meets the hedging recognition criteria for inclusion in Group 2a or instead defaults to Group 2b. The Associations believe that banks should be responsible for such determinations. This is consistent with banks' responsibility for making other determinations of capital treatment, as described above.

C. The Basel Committee’s Supervisory Cooperation Group should maintain a list of Group 1 and 2a classification determinations for reference as cryptoasset markets develop

Banks’ determinations of the treatment of cryptoassets would and should be subject to review in the ordinary course of the supervisory process. Recognising the dynamic nature of the development of these cryptoassets, banks’ determinations will benefit from the ongoing supervisory engagement with relevant authorities that regulated firms already have throughout the year. To foster global regulatory alignment and consistency on Group 1 determinations as cryptoasset markets develop, the Associations encourage the Basel Committee’s Supervisory Cooperation Group (“SCG”) to maintain a public list of DLT platforms and cryptoassets that satisfy the relevant Group 1 conditions. The SCG should likewise maintain a list of cryptoassets that in their view satisfy the hedging recognition criteria for treatment as Group 2a cryptoassets. These lists would effectively be safe harbours for bank treatment of cryptoassets, but would not exclude the ability of banks to determine that other cryptoassets are Group 1 or Group 2a cryptoassets. The proposed SCG list could be based on an annual survey of authorities and thereby facilitate needed transparency within the regulatory community by fostering global coordination as banks aim to serve clients in the jurisdictions where they want to do business.

D. Unless otherwise specified, banks should be required to assess whether a cryptoasset meets a particular classification condition on an annual basis

The Second Consultation states that banks are responsible “on an ongoing basis” for “assessing whether a cryptoasset is compliant with the classification conditions” for treatment as Group 1. The Basel Committee should provide that unless otherwise specified (such as in the basis risk test, which is measured continuously on a rolling 12-month basis), after making an initial determination that a cryptoasset meets the requirements for Group 1a, 1b, or 2a treatment, a bank would satisfy this “ongoing basis” expectation by conducting an annual assessment to identify any material changes affecting the conditions. If a bank became aware of a change in a cryptoasset between those annual assessments that affected the classification of the cryptoasset, the bank would be required to adjust the classification accordingly. The Associations believe that this is a reasonable and appropriate approach to the assessment of qualitative criteria given that it will not be operationally feasible for banks to conduct daily or even monthly assessments of the classification of cryptoassets as the number and variety of cryptoassets increases over time.

V. The Scope of the Cryptoasset Exposure Framework Should be Clarified to Ensure that It Does Not Have Unintended Consequences

A. The Basel Committee should clarify that assets under custody are only subject to the operational risk requirements of the cryptoasset exposure framework

The Second Consultation states that “the term ‘exposure’ includes on- or off-balance sheet amounts that give rise to credit, market, operational and liquidity risks. It includes activities, such as nonfiduciary custodial services, that may only give rise to operational

risk.” See SCO60.4. The Associations understand the Second Consultation to be stating that to the extent a cryptoasset gives rise to a particular category of risk (e.g., operational risk) under the capital rules, it would be subject to the provisions of the Second Consultation that relate to that risk category. Accordingly, the Associations also understand, and request that the Basel Committee confirm, that under the Second Consultation custodians that merely hold the cryptoassets under custody for their clients would only be subject to recognising operational risk RWAs with respect to that activity.³¹ A contrary reading of the Second Consultation, through this single reference in SCO60.4, would create unintended consequences and be inconsistent with the current treatment of assets under custody under the Basel framework. Assets held in custody are neither on- nor off-balance sheet exposures of a custodian, and they do not attract credit or market risk under the risk-based capital requirements, a liquidity outflow under the liquidity coverage ratio requirement, or a stable funding factor under the net stable funding ratio requirement. Reading SCO60.4’s proposed definition in a manner contrary to the Association’s understanding risks the creation of an untenable framework for custody of cryptoassets by banks, thereby preventing banks that currently engage in custody activities for traditional assets from extending their custody services to cryptoassets.

The Basel Committee should clarify that exposures are treated under the parts of the capital rules and cryptoasset exposure framework that are applicable to those exposures. Specifically, the Associations seek confirmation that because assets under custody only give rise to operational risk, only the operational risk requirements of the cryptoasset exposure framework are applicable to assets under custody both in fiduciary and non-fiduciary arrangements, similar to the treatment for traditional assets under custody.

B. The Basel Committee should confirm that the use of DLT for certain settlement or recordkeeping purposes does not by itself subject the related asset to the cryptoasset exposure framework

The Basel Committee should confirm that the use of DLT for settlement or recordkeeping purposes does not by itself subject the related asset to the cryptoasset exposure framework. Banks may, for example, use DLT, including but not limited to internally developed, private, permissioned blockchain systems, to facilitate the execution or recording of transfers of ownership interests in an underlying traditional asset without ever “tokenising” or creating a programmable asset that is distinct from the underlying asset. Instead, the official registry and record of title for the underlying dematerialised traditional assets may remain in traditional custody networks at all times. DLT migrations of clearing services have also been announced across the globe. For example, the Australian Securities Exchange (“ASX”) is migrating its current CHESS equities clearing, settlement system, and post-trade settlement services to a permissioned, private blockchain based on Digital

³¹ To the extent that a custodian extends credit to custody clients or enters into FX transactions with custody clients, the Associations recognise that such activities may result in credit risk or market risk RWAs as applicable. But merely holding assets under custody should not be treated as resulting in credit risk or market risk.

Asset's DLT.³² ASX will not be issuing tokenised securities. Similar DLT migrations have been announced by Hong Kong Exchanges and Clearing Limited (“HKEX”),³³ Deutsche Börse,³⁴ and DTCC.³⁵ DLT is also being used in securities financing transactions.³⁶

SCO60.2 introduces some uncertainty as to how such projects would be categorised under the cryptoasset prudential framework. In part, SCO60.2 states that “[d]ematerialised securities ... that are issued through [DLT] or similar technologies are considered to be within the scope of this chapter 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.” In many cases where DLT is used for settlement or recordkeeping, no asset is *issued* through DLT. No distinct digital asset is created at all. However, the execution or recording of transfers of ownership occurs through DLT, rather than using “electronic versions of traditional registers and databases which are centrally administered.”

In addition, reliance on DLT for recordkeeping or settlement purposes does not increase the risk or liquidity profile of the underlying assets. Where the underlying traditional assets can still be accessed through the traditional custodian network that is holding the assets, it would not be appropriate to apply conservative risk weightings or capital charges solely because of the use of DLT for evidencing transfers of ownership.

The markets would greatly benefit from clarity that such uses of DLT would not lead to the underlying dematerialised assets being treated as “cryptoassets.” Otherwise, banks will be disincentivised from participating in innovative solutions that are implemented to improve market efficiencies by using DLT infrastructure.

VI. Additional Areas for Consideration

The Associations also request that the Basel Committee consider the following recommendations. The following areas for consideration are generally presented in the same order in which they are addressed in the Second Consultation and do not represent an order of prioritisation among the Associations.

³² See ASX; *CHESS Replacement*, available at <https://www2.asx.com.au/markets/clearing-and-settlement-services/chess-replacement>.

³³ See HKEX; *Synax*, available at https://www.hkex.com.hk/synapse?sc_lang=en.

³⁴ See DEUTSCHE BÖRSE; *7 Market Technology: D7 Digitising Financial Instruments*, available at <https://www.deutsche-boerse.com/d7/>.

³⁵ See DTCC; *DTCC's Project Ion Now Live in Parallel Production Environment, Processing Over 100,000 Transactions Per Day on DLT*, available at <https://www.dtcc.com/news/2022/august/22/project-ion>.

³⁶ See, e.g., JPMORGAN; *Onyx Digital Assets*, available at <https://www.jpmorgan.com/onyx/onyx-digital-assets.htm>; HQLA^x; available at <https://www.hqla-x.com/>.

A. Classification of Group 1 Cryptoassets

The consultation outlines that only those assets that “meet in full a set of classification conditions” will be eligible for recognition as Group 1 cryptoassets. As outlined in Section IV, the Associations believe banks should be responsible for classification determinations and therefore for assessing whether the classification conditions have been met. In order to carry out such assessments, the Associations have detailed where further refinements are necessary to better reflect the features of cryptoasset markets and be more practicable.

1. Classification Condition 1

- (a) Digitally native cryptoassets such as digital equity securities or bonds should be eligible for treatment as Group 1 cryptoassets

Classification condition 1 currently limits the scope of Group 1 cryptoassets to tokenised traditional assets and stablecoins. Digitally native assets other than cryptocurrencies, such as digital equity securities or bonds, are not tokenised traditional assets because no traditional, off-chain version of the assets exists, and they are also not stablecoins. Classification condition 1 should be revised so that a digitally native cryptoasset that has the same risk profile as a traditional asset is eligible as for treatment as a Group 1 cryptoasset.

- (b) Certain requirements for Group 1a cryptoassets are overly restrictive and should be revised to better accommodate innovation in tokenised arrangements

The requirement that tokenised traditional assets qualify as Group 1a cryptoassets only to the extent that they “pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset,” including by conferring the same level of legal rights as the corresponding traditional assets (SCO60.9(2)), could disqualify many tokenised arrangements that the Associations believe should be Group 1a cryptoassets. The Associations believe that such a requirement is unnecessary and extends beyond the principle of “same risk, same activity, same treatment” set forth by the Basel Committee in this consultation process. To the extent legal rights differ, any additional risks posed would be separately accounted for by the existing capital rules. The capital rules already expressly recognise certain legal rights when they relate directly to risk. As an example, the capital rules generally require a bank to have a valid qualified master netting agreement in place in order to recognise a net exposure for capital purposes. Such a requirement is sensible because the absence of a valid qualified master netting agreement would result in a bank having a gross rather than net exposure in the event of the counterparty’s insolvency. This example is instructive because it relates to a specific legal arrangement regarding a specific risk that can be directly related to a capital-relevant outcome (i.e., insolvency and resulting losses). Absent a specific, capital-relevant motivation, the framework should not require equality between the legal rights applying to tokenised traditional assets and traditional assets because such differences may be driven by legal and technical factors unrelated to risk. Treating such assets as Group 2 cryptoassets solely

as a result of differences in legal rights, and thereby subjecting them to more conservative capital treatment, is not justified in light of the existing capital rules.

In addition, the requirement that tokenised bonds, loans, claims on banks (including deposits), equities and derivatives can only qualify as Group 1a cryptoassets if there is “no feature 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” (SCO60.9(2)(a)) should be modified so that it does not unintentionally restrict the ability of issuers to program a token to comply with applicable law such as AML and sanctions requirements. For example, as noted in Section VI.A.5(a), a cryptoasset may be programmed to provide for freezing on the blockchain or “burning” (i.e., destroying) if needed for AML or sanctions compliance reasons. For instance, USD Coin allows for the freezing of tokens such that transfers can no longer take place after the order is given and the blacklisting of suspicious addresses. The Basel Committee should make clear that such technological controls would not disqualify a tokenised traditional asset from treatment as a Group 1a cryptoasset by carving out legal, compliance, and risk-related requirements from being included as “a feature that could prevent obligations to the bank being paid in full when due as compared with a traditional version of the asset.” Subjecting cryptoassets to more conservative Group 2 capital treatment as a result of such risk-reducing features would be inappropriate.

We suggest the following drafting for SCO60.9 instead:

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

- (1) They are digital representations of traditional assets using cryptography, DLT or similar technology to record ownership.*
- (2) They pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset. In practice, this means:*
 - Other than for legal, compliance, and risk-related requirements, there must be no feature of the cryptoasset that could prevent obligations being received in full when compared with a traditional (non-tokenised) version of the asset.*
 - In relation to commodities or cash held in custody, legal ownership of the cryptoasset can be evidenced.*

Proposed SCO60.10(1) provides that cryptoassets would fail to meet the same legal rights requirement in proposed SCO60.9(2) if they “first need to be redeemed or converted into traditional assets before they receive the same legal rights as direct ownership of traditional assets.” The Associations believe that this requirement is unnecessary. It is not clear what

additional risk is introduced by redemption or conversion such that these cryptoassets should be subject to higher capital requirements, particularly if the process for redeeming or converting a cryptoasset into a traditional asset is instantaneous and ensures legal certainty and settlement finality.³⁷ Furthermore, conversions to achieve the same legal rights already exist in the funds markets like ETFs. Equity ETF investors historically have not had voting rights power as they would if they directly owned the underlying equity holdings. Instead, the fund managers have historically held and exercised the legal voting rights.³⁸ From a risk management and economic perspective, there is no meaningful difference in how a bank manages its risk when investing in ETFs or the specific underlyings due to this difference in particular legal rights. Therefore, the Associations believe that this requirement is unnecessary and unclear as to the risk being addressed and recommend removing SCO60.10(1).

- (c) A stablecoin that is issued by an entity that is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements should be deemed to meet classification condition 1 without regard to the redemption risk and basis risk tests

In proposed SCO60.17, the Basel Committee indicated that it is considering creating an alternative to the redemption risk and basis risk tests whereby a stablecoin would meet classification condition 1 without regard to the redemption risk and basis risk tests if its issuer is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements. The Associations support the creation of such an alternative test for stablecoins issued by prudentially regulated entities. For the avoidance of doubt, the Associations also agree that, as suggested by SCO60.9 footnote 2,³⁹ tokenised deposits issued by banks as commercial bank money should be analysed as Group 1a cryptoassets, not Group 1b cryptoassets. Such an approach would appropriately recognise that “banks’ exposures to stablecoins issued by regulated entities will generally be lower risk than those issued by unregulated entities.”⁴⁰ This approach would also reduce the burden associated with tracking compliance with the redemption risk and basis risk tests for stablecoins that are issued by prudentially regulated entities.

The Basel Committee should make clear the scope of stablecoin issuers that would be subject to this alternative treatment would include not only banks, but also regulated

³⁷ See CPMI July 2022 Consultative Report.

³⁸ Recently, BlackRock has begun to offer certain institutional ETF investors the ability to exercise voting rights.

³⁹ “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 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 placed in Group 1b based solely on their commonly used local name.” Second Consultation, SCO 60.9 footnote 2.

⁴⁰ Second Consultation at 4.

nonbank issuers that are subject to prudential capital and liquidity requirements as part of their specific legal frameworks (e.g., e-money institutions in the EU).

For the avoidance of doubt, any test related to issuance by a prudentially regulated entity should be an alternative to, and not a replacement for, the redemption risk and basis risk tests. Stablecoins issued by nonbanks that are not prudentially regulated should be eligible for treatment as Group 1b assets, subject to meeting these other requirements.

- (d) The Associations support the proposed redemption risk test for Group 1b cryptoassets, but recommend refinements to certain details of that test

The Associations support the inclusion of a redemption risk test that focuses on the value, composition and management of reserve assets backing stablecoins. However, several aspects of the redemption risk test should be refined to tailor the test more appropriately to stablecoins.

The redemption risk test requires that “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” (SCO60.13(1)). “At all times” could be read to imply that banks must assess their compliance with this test on a continuous basis, but such an expectation is not practicable. Since only the issuers of stablecoins, not the banks holding those stablecoins, have access to real-time information on the value of reserve assets backing the stablecoins, banks are not in a position to assess compliance with this test on a continuous basis. Thus, the Basel Committee should confirm, either through modifications to proposed SCO60.13(1) or through other guidance, that banks may comply with this requirement by analysing a stablecoin issuer’s public disclosures of the value of reserve assets backing the stablecoins and the aggregate peg value of the stablecoins, and that individual banks are not expected to make their own assumptions in order to continuously assess this requirement. In addition, banks should be able to rely on a quarterly attestation from a third party, e.g., audit firm, to determine whether this provision of the redemption risk test is met.

The redemption risk test also requires that “if the reserve assets expose the holder to risk in addition to the risks arising from the reference assets, 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” (SCO60.13(1)). The nature of the “risks” giving rise to an overcollateralisation requirement is unclear, as is the standard for identifying “sufficient” overcollateralisation. The Basel Committee should clarify what risks banks are expected to measure for purposes of this requirement and that what constitutes sufficient overcollateralisation based on those risks is in a bank’s discretion. As part of that discretion, banks should be permitted to rely on third-party analyses of the level of overcollateralisation of a particular stablecoin, rather than be required to conduct their own analysis.

In addition, the redemption risk test requires that the governance arrangements relating to the management of reserve assets “ensure that a robust operational risk and resilience framework exists to ensure the availability and safe custody of the reserve assets” (SCO60.13(2)(b)). While the Associations support this requirement in principle, it is unclear what would qualify as a “robust” operational risk and resilience framework for this purpose. The Basel Committee should clarify in SCO60.13(2)(b) that a framework that complies with its *Principles for Operational Resilience*⁴¹ and *Principles for the Sound Management of Operational Risk*,⁴² or any similar principles adopted in the future with respect to stablecoin issuers, would qualify as a “robust” framework. Similarly, third-party audit attestations should be able to be relied upon for determining operational resiliency. In addition, given that the stablecoin issuer, not the bank, is responsible for developing or maintaining its own operational risk and resilience framework, the Basel Committee should clarify that a bank’s obligation to “ensure” that such a framework exists is simply an obligation to conduct appropriate due diligence, which may include reliance on an annual audit attestation from the issuer.

Finally, the redemption risk test should only apply to a bank where that bank is serving as the manager of the reserve assets backing the stablecoins, not where it is custodial on behalf of clients. In a traditional custody arrangement, the bank is responsible for maintaining the control account and is not obligated to determine whether the reserve is sufficient, monitor the underlying transaction, or make margin calls.

- (e) The Associations support the proposed basis risk test for Group 1b cryptoassets but recommend some adjustments to its specific calibrations

The Associations support the revised structure of the basis risk test to include a “narrowly passed” category (SCO60.14), which reduces the risk of a “cliff effect” as compared to the First Consultation, but recommend some further adjustments to the specific calibrations in that test. The Second Consultation retains the 10-basis-point threshold that was in the First Consultation, but introduces a second threshold to reduce cliff effects. Specifically, if the peg-to-market value difference does not exceed 10 bp more than three times over the prior 12 months, the cryptoasset has “fully passed” the basis risk test. If the peg-to-market value difference exceeds 20 bp more than 10 times over the prior 12 months, the cryptoasset has “failed” the basis risk test. If the cryptoasset has neither “fully passed” nor “failed” the basis risk test, it is considered to have “narrowly passed” the basis risk test. Cryptoassets that meet all the requirements for inclusion in Group 1b, but only narrowly pass the basis risk test, will be subject to an add-on to risk weighted assets.

⁴¹ BASEL COMMITTEE ON BANKING SUPERVISION; *Principles for Operational Resilience* (Mar. 2021), available at <https://www.bis.org/bcbs/publ/d516.pdf>.

⁴² BASEL COMMITTEE ON BANKING SUPERVISION; *Principles for the Sound Management of Operational Risk* (June 2011), available at <https://www.bis.org/publ/bcbs195.pdf>; BASEL COMMITTEE ON BANKING SUPERVISION; *Revisions to the Principles for the Sound Management of Operational Risk* (Mar. 2021), available at <https://www.bis.org/bcbs/publ/d515.pdf>.

Our First Consultation Comments provided an analysis of the number of 10 bps threshold breaches each year for certain large stablecoins and equity, commodity and bond exchange traded funds (“ETFs”). Some ETFs are similar to stablecoins in that they are a tradable asset whose market value should closely track the value of the reference asset or index. In the case of an ETF this might be an index such as the S&P 500, while in the case of stablecoins this is normally fiat currency, such as the U.S. dollar. Our analysis, as described in the First Consultation Comments, found that even the largest and most liquid ETFs would fail to meet the 10 bps threshold for fully passing the basis risk test.

The Associations have refreshed that analysis, taking account of the revised structure of the basis risk test. We analysed:

- SPDR S&P 500 Trust (“SPY”);
- Invesco QQQ Trust Series 1 (“QQQ”);
- iShares MSCI EAFE ETF (“EFA”);
- iShares Core U.S. Aggregate Bond ETF (“AGG”);
- Vanguard Total Bond Market Index Fund ETF (“BND”);
- SPDR Gold Shares (“GLD”); and
- United States Oil Fund, LP (“USO”).

Breaches were counted when the difference between the price of an ETF share and its net asset value per share was greater than 10 bps or 20 bps at market close. Only downside breaches were counted given that the redemption risk test requires the value of the reserve assets to *equal or exceed* the aggregate peg value of all outstanding cryptoassets (SCO60.13(1)).

The table below shows the total number of threshold breaches under the Second Consultation for a given ETF from August 2020 to August 2022.

Number of ETF Basis Risk Test Threshold Breaches (August 2020 to August 2022)

	Equity			Fixed Income		Real Assets	
	SPY	QQQ	EFA	AGG	BND	GLD	USO
# >10 bps	5	14	175	33	77	226	156
# >20 bps	0	2	90	4	6	179	110

The table below shows the highest 12-month rolling breach count from August 2021 to August 2022.

Highest 12-Month Rolling Breach Count (August 2021 to August 2022)

	Equity			Fixed Income		Real Assets	
	SPY	QQQ	EFA	AGG	BND	GLD	USO
# >10 bps	1	9	120	4	3	97	117
# >20 bps	0	2	81	0	0	76	87

As indicated by the tables above, only SPY and BND would fully pass under the current proposed calibration of the basis risk test. The fact that highly liquid ETFs such as QQQ and AGG would not fully pass the basis risk test strongly suggests that the current calibration of the fully passing threshold is too restrictive. The Associations therefore believe that the 10 bps threshold for fully passing the basis risk test should be increased to 15 bps and the 20 bps threshold for narrowly passing the basis risk test should be increased to 25 bps. Increasing the fully passing threshold from 10 bps to 15 bps would allow both QQQ and AGG to fully pass the test, as illustrated by the table below. We note that this is still a relatively conservative threshold—not all of the ETFs would fully pass or even narrowly pass.

**Highest 12-Month Rolling Breach Count – Impact of Adjusted Thresholds
(August 2021 to August 2022)**

	Equity			Fixed Income		Real Assets	
	SPY	QQQ	EFA	AGG	BND	GLD	USO
# >10 bps	1	9	120	4	3	97	117
# >15 bps	0	3	99	3	1	85	104
# >20 bps	0	2	81	0	0	76	87
# >25 bps	0	2	64	0	0	68	71

- (f) Where banks can redeem directly without market risk, the basis risk test should not apply

In addition, where a bank is able to redeem a cryptoasset directly with the issuer of the cryptoasset at its peg value and the cryptoasset meets all other criteria for treatment as a Group 1b cryptoasset, the basis risk test should not apply. The stated purpose of the basis risk test is “to ensure that the holder of a cryptoasset can sell it in the market for an amount that closely tracks the peg value.” This consideration is relevant if a holder is unable to redeem a stablecoin directly with the issuer of the stablecoin at its peg value and instead must sell the stablecoin at a loss, either to the issuer or on an exchange. In such circumstances, the bank would incur losses on the sale of the stablecoin and therefore has basis risk. But if a bank is able to redeem a stablecoin directly with the issuer at its peg value, only the counterparty risk to the issuer is relevant, and banks are already capitalised for counterparty risk.

2. Classification Condition 2

- (a) The Basel Committee should clarify the requirement for a legal analysis of a cryptoasset’s redemption jurisdiction in classification condition 2

Classification condition 2 requires that “[a]ll rights, obligations and interests arising from the cryptoasset arrangement [be] clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed” (SCO60.19). The intended scope of “jurisdictions where the asset is . . . redeemed” is unclear. The Basel Committee should change the word “redeemed” to “redeemable.” Doing so would clarify that (1) where a cryptoasset is redeemable only with the issuer, then the redemption jurisdiction is the same as the issuance jurisdiction, and (2) where a cryptoasset is redeemable with one or more intermediaries other than the issuer, then the redemption jurisdiction(s) is the home jurisdiction(s) of such intermediaries.

- (b) The Basel Committee should confirm that redemption in kind of stablecoins is permitted under classification condition 2

SCO60.20(1) states that for classification condition 2 to be satisfied by a stablecoin, the cryptoasset “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.” The Associations seek confirmation that in-kind redemptions would be allowed and would satisfy this condition.

3. Classification Condition 3

- (a) Classification condition 3 is overly broad and should be narrowed to focus on banks’ management or risks relating to cryptoassets and DLT networks

In the First Consultation Comments, the Associations identified that classification condition 3 was overly broad, would impose unworkable requirements and is not necessary

for safety and soundness purposes. The Associations believe that classification condition 3 should be narrowed to focus on the banks' operational resilience and vendor risk management controls and capabilities with respect to cryptoassets, DLT networks, and key service providers interfacing with the networks.

The Associations' members are committed to effective ongoing risk management to mitigate material risks posed by the cryptoassets they hold and the DLT networks in which they participate. Doing so supports bank safety and soundness, while also creating appropriate conditions for clients and counterparties to hold and trade Group 1 cryptoassets with confidence.

As currently proposed, classification condition 3 would require the functions of the cryptoasset and the network on which it operates to be designed and operated to sufficiently mitigate any material risks (SCO60.21). Banks would face major impediments to concluding that cryptoassets based on permissionless blockchains meet this condition. Although banks can manage and mitigate risks related to their engagement with the network, banks cannot uniformly attest to the operation of aspects of a distributed and decentralised network that they do not own or otherwise maintain any contractual or other rights to operate and administer. Banks can be expected to dynamically assess the design of such networks through existing operational resilience and operational risk principles, including the design of their operation. However, the global and disaggregated nature of these networks would make full oversight of all aspects of their operation wholly infeasible.

Instead, the scope of classification condition 3 should be narrowed to the risks that banks face when engaging with the network or the cryptoasset, focusing on their key service providers and third-party risk management. Banks will, of course, maintain robust operational resilience and risk management procedures to understand and monitor all material risks associated with Group 1 cryptoassets and the networks upon which they operate, consistent with existing supervisory expectations for third-party risk management.⁴³ For example, the U.S. federal banking agencies proposed guidance outlining how banks should manage third-party relationships based on their level of risk and complexity, such as engaging in robust due diligence when selecting third parties, negotiating for relevant risk controls and legal protections in contracts, promoting oversight and accountability and conducting ongoing monitoring of the third-party relationship.⁴⁴ With respect to cryptoassets in particular, the Bank of England has discussed

⁴³ See, e.g., BASEL COMMITTEE ON BANKING SUPERVISION; *Outsourcing in Financial Services* (Feb. 2005), available at www.bis.org/publ/joint12.pdf. The Associations support ongoing work by international bodies to identify principles for the oversight of critical third parties.

⁴⁴ FRB, FDIC, OCC, Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 318182 (July 19, 2021).

the importance for firms to assess operational risk in their crypto-related activities, including with respect to third-party risk.⁴⁵

In addition, focusing on key service providers would align with the European Union’s Markets in Crypto-Assets (“MiCA”) Regulation of cryptoasset service providers (“CASPs”) and the Financial Action Task Force (“FATF”) guidelines on virtual asset service providers (“VASPs”).⁴⁶ MiCA and FATF service providers include exchanges, custodians, operators of trading platforms, and wallet providers. The CASPs and VASPs will be subject to a host of operational resilience and risk management standards such as consumer protection, market integrity, transparency, supervision, and AML/CFT requirements. Therefore, in light of existing third-party risk management practices, focusing the classification condition 3 on these key service providers who interface with the underlying blockchain and assess the operational risk, governance, and risk management of the underlying blockchain would be more appropriate and more practical to implement.

Banks also should seek to ensure that the network’s structures are designed to mitigate, and that their participation in the operation of such networks is conducted in a manner that mitigates, all material risks relating to their engagement with the network (e.g., by creating a permissioned, closed layer on the permissionless blockchain such as a permissioned trading platform). These processes should suffice to ensure that any risks associated with the bank’s engagement with the DLT are appropriately mitigated. Finally, banks will also monitor these structures and put mitigation measures in place to respond to any material risks that arise and are outside of their control. These steps are consistent with the approach to the risk management of other FMUs in which banks participate but do not have full operational control, such as exchanges, central counterparties and central securities depositories. Accordingly, using existing risk management expectations to manage risks of cryptoassets and networks upon which they operate should be sufficient to support safety and soundness.

4. *Classification Condition 4*

- (a) Classification condition 4 should not refer to storage providers or node validators

Under classification condition 4, to qualify as a Group 1 cryptoasset, “[e]ntities that execute redemptions, transfers, storage or settlement finality of the cryptoasset, or manage or invest reserve assets, [must be] regulated and supervised, or subject to appropriate risk management standards” (SCO60.23). The Second Consultation states that in-scope entities for this requirement “include operators of the transfer and settlement systems for the

⁴⁵ BANK OF ENGLAND; *Existing or planned exposure to cryptoassets* (Mar. 24, 2022), available at <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2022/march/existing-or-planned-exposure-to-cryptoassets.pdf>.

⁴⁶ FATF; *Virtual Assets and Virtual Asset Service Providers* (Oct. 2021), available at <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>.

cryptoasset, wallet providers, administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism,” and specifically calls out node validators as subject to this condition (SCO60.24).

Classification condition 4 should not refer to storage providers. Prudentially regulated bank custodians would, of course, meet the requirement of being regulated and supervised or subject to appropriate risk management standards. But other storage providers, such as wallet providers, are less certain to meet that requirement. For cryptoassets based on a decentralised and permissionless network such as Ethereum, it might not be possible for a bank to identify, let alone assess the risk management standards of, all of the entities that are capable of storing cryptoassets apart from the storage providers the bank uses. Thus, while a bank should ensure that its own storage providers are regulated and supervised or subject to appropriate risk management standards consistent with existing third-party risk management standards, it may not be able to do so with respect to all storage providers providing such services to the permissionless network. In practice, this would make it impossible for a bank to conclude that classification condition 4 has been met by a cryptoasset based on a permissionless network.

A similar reasoning applies to node validators. Decentralised and permissionless networks have many node validators. For cryptoassets based on such networks, it is not possible for a bank to ensure that all node validators are regulated and supervised or subject to appropriate risk management standards. This requirement would likewise render classification condition 4 unworkable for a cryptoasset based on a permissionless network or a permissioned network with a non-trivial amount of validators.⁴⁷ An unintended outcome of this requirement might be to require banks to assess the risk management standards of their regulators because supervisors may become node participants to obtain market data for surveillance and supervisory-related activities.

5. Permissionless Blockchains and Public Permissioned Blockchains

- (a) Cryptoassets that are based on permissionless blockchains should be eligible to be included in Group 1, subject to the existence of certain controls

Classification conditions 3 and 4 should be modified so that cryptoassets that are based on permissionless blockchains are eligible to be included in Group 1, subject to the existence of appropriate controls. The Associations acknowledge the additional governance, security and AML risks associated with cryptoassets that use permissionless blockchains, as compared to permissioned blockchains. Those risks are mitigated, however, where permissionless blockchains have adopted or programmed protocols for the governance, tracking, and control of cryptoasset movement. In particular, the risks of using a permissionless blockchain as a base layer for the creation of (regulated) tokenised traditional assets can be very effectively controlled. In such cases, the tokenisation agent

⁴⁷ For example, Figure Technologies’ \$150 million tokenised securitization of home equity lines of credit in March 2020 on its public permissioned blockchain has 12 node participants but they may increase over time.

may remain (for the entire lifetime of the token) in control over the token through embedded functions like seize, freeze and burn. As a final fallback, the terms and conditions of the tokenised traditional assets can also entail the right of the tokenisation agent to take the tokenised traditional asset off-chain by, as one example, burning or otherwise removing from circulation the ledger-based tokenised traditional asset and subsequently issuing the asset in a traditional way.

To use Ethereum as a specific example, there are varying levels of token contracts that can be placed on the Ethereum blockchain that allow for graduating levels of controls, such as blacklists, whitelists and transfer restrictions. ERC20, the most common token standard, allows for basic security functions encoded directly into the token contract (e.g., grants of permission to certain entities to move tokens at a pre-specified volume). ERC1400, on the other hand, includes an encoded mechanism to restrict the usage of tokens based on identity and jurisdiction, stipulate the holding period of a token in a given wallet, approve only certain buyers and sellers, KYC certain wallets and require the approval to be updated at a specified frequency, as well as place limits on transactions sizes. ERC3643 provides the foregoing functionality as well as a validation mechanism for on-chain transfers and a token recovery process, in addition to other enhanced features that mitigate some of the security concerns historically associated with permissionless blockchains. In sum, though the superficial features of permissionless blockchains (e.g., broad access, less centralised control, etc.) may raise supervisory concerns, these can be largely mitigated, and validated by banks through longstanding risk management practices, through token contracts themselves. A tangible example of this is USD Coin, which leverages the ERC20 standard, and allows for the freezing of tokens such that transfers can no longer take place after the order is given, the blacklisting of suspicious addresses and the granting of access to third-party providers to render security services such as fraud detection, risk assessment and identity management.⁴⁸

It is therefore appropriate for a cryptoasset that uses a permissionless blockchain to be eligible as a Group 1 cryptoasset where the blockchain has inherent tools to mitigate material risks in line with classification condition 3, such as: the ability to whitelist and blacklist addresses, the ability to freeze transfers, the ability to grant permissions to an entity to transact, and mechanisms to restrict usage based on identity, jurisdiction, and asset category.

- (b) If cryptoassets based on permissionless blockchains are not eligible to be included in Group 1, the Basel Committee should at a minimum confirm that cryptoassets that are based on public permissioned blockchains are eligible to be included in Group 1

Cryptoassets issued on public permissioned blockchains should not be excluded from Group 1. The Associations believe that public permissioned blockchains (i.e., where permissionless blockchains are adapted or programmed to function with an overarching permissioned system that enables adequate governance, tracking and controls of

⁴⁸ See CIRCLE; *USDC Risk Factors* (July 29, 2021), available at <https://www.circle.com/en/legal/usdc-risk-factors>.

cryptoasset ownership and transfers) are sufficiently similar to private permissioned blockchains in their design, level of control, and risk mitigation capabilities. Public permissioned blockchains are inherently highly customisable. They offer the ability to limit access to the network to identified participants and set different access levels for each participant. The network operators can easily alter consensus rules. Security risks can be mitigated through immutability techniques such as cryptographic security measures and validation through consensus mechanisms. Access is permissioned and can be revoked.

An example of a highly secure permissioned usage of smart contracts on a public blockchain is the EIB's bond issuance on the Ethereum blockchain in April 2021. Though a public blockchain was used, underwriting banks were still able to limit placement of the bonds to vetted market participants. These restrictions on the investor base exist even during secondary trading, which demonstrates that a public blockchain can include a token with permissioned features. For more information, please see Section III above and Appendix 1.

The inclusion of cryptoassets based on public permissioned blockchains in Group 1, subject to meeting the classification criteria, will offer important benefits for banks and their customers. It will allow for collaboration between multiple banks and market participants in the issuance and tokenisation of traditional assets. It will also increase the usability and transferability of Group 1 assets and provide more value to customers transacting in them. Given the manageable level of risks that public permissioned blockchains pose, excluding cryptoassets based on such blockchains from the definition of Group 1 will unjustifiably hinder banks' ability to experiment with highly beneficial use cases.

B. Minimum Capital Requirements for Group 1 Cryptoassets

1. Credit Risk for Group 1 Cryptoassets

(a) Group 1a Cryptoassets

Subject to our comments in Section VI.A above relating to the classification conditions for Group 1 assets, including that certain requirements for Group 1a cryptoassets are overly restrictive and should be revised to better accommodate innovation in tokenised arrangements, the Associations generally support the Basel Committee's proposed treatment of Group 1a cryptoassets for credit risk, including the recognition in the Second Consultation that it is the responsibility of the banks themselves to assess the legal rights with respect to tokenised assets, and whether the tokenised assets comply with the relevant eligibility requirements for recognition as collateral for credit risk mitigation purposes.

(b) Group 1b Cryptoassets

Subject to our comments in Section IV.A above relating to the classification conditions for Group 1 assets, the Associations generally support the Basel Committee's proposed treatment of Group 1b cryptoassets for credit risk, with three important modifications. First, the Associations recommend that the Basel Committee recognise the Group 1b cryptoassets as eligible financial collateral to the extent that any security interest in, or legal title to, such collateral meets the legal certainty and finality standards otherwise applicable

under existing BIS guidance and there is no redemption risk or the stablecoin issuer is prudentially regulated. Secondly, if the Basel Committee is unwilling to remove the basis risk test altogether for banks or other prudentially supervised institutions, the Associations do not believe that there should be any increase in credit risk RWAs for Group 1b cryptoassets that “narrowly pass” the basis risk test if the bank can redeem the relevant Group 1b cryptoassets directly with the issuer. Third, the credit risk RWA amount of Group 1b cryptoassets should be based on the value of the Group 1b cryptoasset exposure amount, not the amount of underlying assets to ensure that overcollateralisation is not penalised.

- (1) The Basel Committee should recognise Group 1b cryptoassets as eligible financial collateral

The Associations believe that the logical consequence of the Second Consultation’s distinction between Group 1b cryptoassets that expose banks to the risk of default of the redeemer and those that do not (the latter category, “Non-Redemption Risk Group 1b”) should be that Non-Redemption Risk Group 1b cryptoassets are recognised as eligible financial collateral for credit risk mitigation purposes.

The Second Consultation explicitly and correctly recognises that Group 1b cryptoassets may be structured so that the holder is not exposed, either directly or indirectly, to the risk of default by the redeemer of the cryptoasset, i.e., where the underlying reserve assets are held in a bankruptcy remote SPV on behalf of the holders of the cryptoassets, with the holders having direct claims on the underlying reserve assets. *See* SCO60.40. But the Second Consultation continues to state – similarly to the First Consultation – that Group 1b cryptoassets, even if they can be redeemed for traditional assets that are themselves eligible collateral for credit risk mitigation purposes, are not recognised as collateral because “the process of redemption *may* add counterparty risk that is not present in a direct exposure to a traditional asset.” *See* SCO60.44 (emphasis added).

The Associations believe that SCO60.44 is logically inconsistent with SCO60.40. If a Group 1b cryptoasset does not expose the holder to the default risk of the redeemer, then such a Non-Redemption Risk Group 1b cryptoasset does *not* add counterparty risk. Because the Non-Redemption Risk Group 1b cryptoasset does not add counterparty risk to the redeemer, the Associations believe that there is no basis for disqualifying such a cryptoasset from recognition as eligible financial collateral for credit risk mitigation purposes to the extent the underlying traditional asset(s) qualifies as eligible financial collateral.

Just as with Group 1a cryptoassets, for which the credit risk on the tokenised cryptoasset is treated in the same way as that on the underlying traditional asset, the credit risk on a Non-Redemption Risk Group 1b cryptoasset is treated in the same way as that on the underlying traditional asset(s). The same parallel treatment should extend to recognition of Non-Redemption Risk Group 1b cryptoassets as eligible financial collateral. The Associations therefore recommend that the Basel Committee recognise—consistently with SCO60.40—that Non-Redemption Risk Group 1b cryptoassets qualify for recognition as eligible financial collateral for credit risk mitigation purposes to the same extent as their underlying traditional assets. Under the comprehensive method, the Associations also

recommend that the standard haircut applied under CRE22.44 to a stablecoin should be determined in a way consistent with the look-through approach for investment funds such as UCITs and mutual funds.

In the same vein, if the requirement in SCO60.17 of the Second Consultation that the issuer of a Group 1b cryptoasset must be an institution subject to prudential capital and liquidity requirements (such an institution, a “Prudentially Regulated Issuer”) provides an alternative to meeting certain Group 1 conditions, the Associations believe that any Group 1b cryptoasset issued by a Prudentially Regulated Issuer should be recognised as eligible financial collateral for credit risk mitigation purposes. This would be justified by the lower level of default and redemption risk associated with a Prudentially Regulated Issuer.

- (2) There should be no increase in credit risk RWAs for the “narrowly passed” basis risk test if the bank can directly redeem with the issuer at the peg value

As noted in Section VI.A.1(c) above, the Associations recommend that the basis risk test for Group 1b cryptoassets should not apply to banks or other prudentially supervised institutions. If, however, the Basel Committee is unwilling to remove the basis risk test as recommended and it continues to apply to banks, the Associations recommend that the credit risk RWA treatment for cryptoassets that “narrowly pass” the basis risk test should be modified as described below.

The Associations do not believe that, for Group 1b cryptoassets where the holder has a direct right against the issuer to redeem the cryptoasset at the peg value, there is any justification for increasing the amount of credit risk RWAs that a bank holding the cryptoassets would be required to recognise if the cryptoasset only “narrowly passes” the basis risk test under SCO60.14. According to the Second Consultation, the objective of the basis risk test is “to ensure that the holder of a cryptoasset can sell it in the market for an amount that closely targets the peg value.” See SCO60.12(2). If, however, the bank holding the Group 1b cryptoasset has the right to redeem the cryptoasset directly with the issuer at the peg value, this in turn means that there is no need for the bank to sell the cryptoasset itself on an exchange in order to monetise it, and therefore the basis risk test should not be relevant to the calculation of the bank’s credit exposure.

The credit exposure the bank would have to the issuer of the Group 1b cryptoasset is the aggregate amount of the cryptoassets held by the bank at the balance sheet value. The bank would already hold capital against the risk of default of the redeemer under SCO60.39. Increasing the amount of credit risk RWAs a bank would recognise in this case would require a bank to hold capital against a risk it does not bear when able to redeem the cryptoassets directly with the issuer, namely, the risk of being unable to sell the cryptoasset itself in the market.

- (3) The credit risk RWA amount of Group 1b cryptoassets should be based on the value of the Group 1b cryptoasset exposure amount, not the amount of underlying assets

The Second Consultation states that, for Group 1b cryptoassets that reference a pool of traditional assets, banks must apply the requirements applicable to equity exposures to investment funds, and that the look-through approach and mandate approach are available to the extent the requirements for those approaches are satisfied. *See* SCO60.38. The Associations request confirmation from the Basel Committee that, consistent with the current requirements for calculating RWAs for equity investments in funds (CRE60) and the calculation guidance provided in CRE99.127,⁴⁹ the RWA amount of an exposure to Group 1b cryptoassets that reference a pool of traditional assets is calculated based on the value of the Group 1b cryptoasset held by the bank (e.g., \$10 million), and not on the total amount of the pool of traditional assets underlying the Group 1b cryptoasset (e.g., \$100 million). Otherwise the banks would be penalised for investing in Group 1b cryptoassets with underlying traditional assets that exceed the value of the Group 1b cryptoasset itself, which would be inconsistent with the requirements for equity exposures to investment funds and would disincentivise investments in Group 1b cryptoassets that are backed by a higher reserve amount. The Associations assume that this is not what the Basel Committee intends in SCO60.38.

2. Market Risk, Counterparty Credit Risk and CVA Risk for Group 1 Cryptoassets

The Associations generally support the Basel Committee’s proposed treatment of Group 1a and 1b cryptoassets for market risk, subject to two exceptions regarding Group 1a cryptoassets. First, the Associations do not believe that, for purposes of calculating RWA for market risk, a Group 1a tokenised asset should generally be treated as a different instrument from the traditional asset the tokenised asset represents. Secondly, the Associations understand that “in [the] presence of significant valuation differences between the traditional and the tokenised asset and in [the] presence of significant basis risk,”⁵⁰ there are limitations to which a bank can apply the internal models method (“**IMM**”) to these exposures. However, these factors do not change the Group 1 vs Group 2 classification. In other words, a Group 1 cryptoasset where there are valuation concerns still remains in principle a Group 1 cryptoasset. As such, the consequence of these modelling issues should not be that such cryptoassets are subject to Group 2a treatment as SCO60.100 indicates (“which then requires to apply SA-CCR as described for Group 2a cryptoassets”). The consequence of such data-related issues should be that SA-CCR must be used instead of IMM. Accordingly, the Associations propose to change the text under 60.100 to “. . . which then requires a bank to apply SA-CCR as applicable to Group 1 cryptoassets.”

(a) Group 1a Cryptoassets under IMA Default Risk Charge

⁴⁹ CRE99.127 provides, in relevant part: “The bank’s total RWA associated with its equity investment is calculated as the product of the average risk weight of the fund, the fund’s maximum leverage and **the size of the bank’s equity investment**” (emphasis added).

⁵⁰ *See* SCO60.100.

The Second Consultation requires that, for the default risk charge applicable under the IMA to Group 1a cryptoassets, tokenised assets and the underlying traditional assets should be regarded as different instruments to the same obligor. *See* SCO60.55. The Associations believe they should be treated as the same instruments to the same obligor as the tokenised asset does not introduce higher jump-to-default risk relative to traditional assets of same seniority and maturity with respect to the same obligor.

(b) CCR and CVA Risks of Derivatives on Group 1a Cryptoassets

SCO60.100 requires that “there could be limitations to apply the IMM in case of missing data or too short history or in presence of data quality problems, which then requires to apply the SA-CCR as described below for Group 2a cryptoassets.” The Associations believe that “in presence of significant valuation differences between the traditional and the tokenised asset and in presence of significant basis risk,” SA-CCR for the traditional assets should be used instead of SA-CCR for Group 2a cryptoassets. SA-CCR for the traditional assets is calibrated significantly more conservatively than IMM. Any basis risk between Group 1a cryptoassets and the traditional assets would have been adequately captured by the inherent conservatism of SA-CCR relative to the IMM. Such a treatment would maintain consistency of capitalisation approaches for Group 1 cryptoassets.

C. Classification of Group 2 Cryptoassets

1. Group 2a Hedging Recognition Criteria

- (a) Dividing Group 2 cryptoassets into those that meet hedge recognition criteria and those that do not is appropriate

The division of Group 2 cryptoassets into those that meet hedge recognition criteria and those that do not, as reflected in proposed SCO60.59, is appropriate and was one of the key industry recommendations from the First Consultation. A fundamental tenet of the Basel Framework is that when a bank mitigates risk by hedging an exposure, that risk mitigation should be recognised through a decreased capital requirement applied to the exposure. From a trading book perspective, the ability to offset risk is fundamental to ensure appropriate risk representation of the underlying exposures. The Second Consultation recognises this fundamental tenet by bifurcating Group 2 cryptoassets into those that meet the hedging recognition criteria (Group 2a) and those that do not (Group 2b) and providing for different capital treatments appropriate to the different risks posed by Group 2a and Group 2b cryptoassets. The Associations believe that this division is appropriate in reflecting the ability of banks to mitigate their risk by hedging exposures arising from Group 2a cryptoassets and their derivatives.

- (b) The product-based hedging recognition criterion results in an overly narrow category of Group 2a cryptoassets and should be revised

The first proposed Group 2a hedging recognition criterion in paragraph SCO60.60(1) is that the bank’s cryptoasset exposure falls into one of four categories. The Associations

believe that, as drafted, this criterion results in an overly narrow category of products with some ambiguities and overlap in the definitions between paragraphs (a) and (b).

Furthermore, under the current proposal, while direct holdings of a spot Group 2 cryptoasset are clearly eligible for Group 2a treatment, physically-settled derivatives referencing these Group 2 cryptoassets do not appear to be. This would exclude, for example, the Eurex Bitcoin ETN, which is physically-settled. It is not clear why a physically-settled derivative exposure should be treated differently from an exposure to the underlying cryptoasset. As physically-settled derivatives referencing Group 2 cryptoassets can result, at the time of physical settlement, in either no exposure or in direct holdings of the spot Group 2 cryptoasset (or a derivative thereon), the capital treatment of a physically-settled derivative on a Group 2 cryptoasset should be eligible to be categorised in Group 2a to the same extent as its underlying cryptoasset.

These criteria should be refined to be as clear and as inclusive as possible. To that end, the Associations recommend that proposed SCO60.60(1) be revised as follows:

- | |
|---|
| <p>(a) A direct holding of a spot Group 2 cryptoasset where there exists a derivative or exchange-traded fund (ETF)/exchange-traded note (ETN) that: <u>(i) has been explicitly approved by a jurisdiction's markets regulators for trading and/or is traded on a regulated exchange that and/or is cleared by a qualifying central counterparty (QCCP); and (ii) solely references the Group 2 cryptoasset.</u></p> <p>(b) A cash-settled 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 qualifying central counterparty (QCCP)<u>(s) that meets criterion (a)(i) above.</u></p> <p>(c) A cash-settled derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion (b) above.</p> <p>(d) A cash-settled derivative or ETF/ETN that references a cryptoasset-related reference rate published by a regulated exchange.</p> |
|---|

- (c) To avoid cliff effects, the hedging recognition criteria should include a supervisory mechanism that could temporarily suspend the quantitative requirements in case of broad market dislocations

The proposed hedging recognition criteria do not provide for a gradual transition should a quantitative criterion, e.g., the trading volume requirement, that was previously satisfied become no longer satisfied. This leads to the possibility of cliff effects where the bank's exposure would suddenly change from Group 2a to Group 2b, imposing a 1250% risk weight and other conservative capital treatments.

The concern is that such a cliff effect could be procyclical and exacerbate broad market dislocations. The Associations recognise that regulators have acknowledged these effects previously in different contexts and have provided relief, e.g., the impact of heightened volatility on market risk capital requirements.⁵¹ The Associations note that the Basel Committee included language in the context of the modellability test under the fundamental review of the trading book (“**FRTB**”) that, in the event of systematic market disruptions, a supervisor could allow banks to deem risk factors that fail the quantitative modellability tests to be modellable (see MAR31.24). The Associations believe that similar supervisory discretion is warranted with respect to the quantitative test for Group 2a cryptoassets and encourage the Basel Committee to adopt a similar mechanism in this context.

- (d) The market capitalisation requirement in proposed SCO60.60(2)(a) should be measured on a rolling 12-month basis

It is not clear whether the requirement that “the average market capitalisation is at least USD10 billion over the previous year” (SCO60.60(2)(a)) should be measured on a rolling 12-month basis or once annually on a static basis. The Associations suggest that the market capitalisation be measured on a rolling 12-month basis to ensure continuous monitoring of the relevant conditions.

D. Other Issues Relating to Minimum Capital Requirements for Group 2 Cryptoassets

1. Non-native Group 2a Cryptoassets (i.e., Group 1 cryptoassets that become Group 2) should be subject to Group 2a treatment for market risk

Failed Group 1 cryptoassets that are trading book-eligible based on the trading book / banking book boundary as defined under RBC25 should be subject to the Group 2a treatment for market risk on the basis that this is the relevant framework for market risk exposures. Otherwise, the criteria as defined under SCO60.60 would in most cases not be met as they are designed for native cryptocurrencies and not tokenised assets where the individual market values would generally be smaller than the \$10 billion threshold for Group 2a hedging recognition criteria. For example, for an entity that has issued only equity in tokenised form, a \$10 billion threshold would be much higher than the \$2 billion threshold for large cap equities under the FRTB market risk rules. If condition 1 in the Group 1 classification conditions is met, and the asset meets the trading book criteria as defined in RBC25, the Associations believe the tokenised asset should be considered part of Group 2a. Netting of these failed Group 1a instruments should be allowed if the underlying issuer(s) or underlying asset(s) is the same. Consistent with the Group 2a treatment, any failed Group 1a assets should not be subject to the default risk charge even if the underlying asset would be in order to avoid a situation where the capital charge applied to the exposure would exceed the charge for Group 2b. Failed Group 1a tokenised cryptoassets in the banking book would be subject to Group 2b capital treatment.

⁵¹ See, e.g., FRB; *COVID-19 Supervisory and Regulatory FAQs* (Apr. 8, 2021), available at <https://www.federalreserve.gov/covid-19-supervisory-regulatory-faqs.htm>.

Furthermore, there is a link between the hedging recognition criteria and the market risk capital requirements for Group 2a cryptoassets in SCO60.74: “. . . only the products listed in [SCO60.60](1) may be used for the purposes of offsetting and for the purposes of calculating the net capital set out in [SCO60.76] to [SCO60.87].” For failed Group 1 cryptoassets that are classified as Group 2a, we propose the following revised language to SCO60.74:

When consolidated, sensitivities for each Group 2a cryptoasset in different markets or exchanges must not be offset, meaning those sensitivities will be calculated as separate long and short gross consolidated sensitivities. In addition, only the products listed in [SCO60.60](1), and failed Group 1 assets that meet condition 1 as set out in [SCO60.8] to [SCO.18] and trading book criteria as defined in RBC25, may be used for the purposes of offsetting and for the purposes of calculating the net capital set out in [SCO60.76] to [SCO60.87] below.⁵² Other products that reference Group 2a cryptoassets are subject to the capital requirements that apply to Group 2b cryptoassets.

2. Group 2a Cryptoasset ETFs should be recognised as eligible financial collateral

In addition to the comments made in Section VI.B.1(b)(1) above for the recognition of Group 1b cryptoassets as eligible collateral, the Associations believe that Group 2a ETFs would currently qualify as eligible collateral because they satisfy the existing criteria for publicly traded investment funds. Similarly, failed Group 1 cryptoassets that meet classification condition 1 should be eligible financial collateral under existing collateral eligibility criteria. In addition, a bank extending credit through repo-style transactions and margin loans involving Group 2a cryptoassets should be permitted to calculate capital charges using the comprehensive approach in place for these types of exposures with any other form of eligible collateral.

The Second Consultation summarises the current framework for identifying eligible financial collateral, the preconditions for which are “whether the collateral can be liquidated promptly and legal certainty requirements.” As this eligibility framework has been used to determine the current list of eligible financial collateral, it should also be used when evaluating cryptoassets.

The principles for financial collateral recognition emphasise that any asset classified as eligible financial collateral must be or have:

- Subject to legally enforceable documentation that gives a bank the right to liquidate or take legal possession of the collateral in a timely manner;

⁵² Debt, equity, and similar Group 1 instruments may be netted based on the same CUSIP, ISIN, or other issue identifier. Offsetting may be permitted across the prescribed netting parameter for the same issuer.

- Subject to legal arrangements in which a bank has a perfected, first-priority security interest; and
- Sufficient levels of liquidity and price transparency.

See generally CRE 22, *Standardised approach: credit risk mitigation*, CRE 22.26-27.

The Associations recognise that the Basel Committee is not currently prepared to permit Group 2a cryptoassets to qualify as financial collateral. However, the Associations believe that the Basel Committee should periodically revisit the issue of recognition of direct Group 2a cryptoassets over time as more clarity develops with respect to their legal treatment in cases of bankruptcy or insolvency.

3. *The potential applicability of the internal models approach (“IMA”) for Group 2a cryptoassets should be revisited when more data is available*

The Second Consultation explicitly states that the market risk IMA is not available for instruments referencing Group 2 cryptoassets, and only allows for the Simplified Standardised Approach (“SSA”) and SA for market risk for Group 2a cryptoassets. *See* SCO60.53, 60.61. The Associations believe that Group 2a cryptoassets are highly liquid by definition and would have a high degree of price transparency under the classification and hedging recognition criteria discussed above, making them good candidates for applicability of the IMA. However, the Associations recognise that the Basel Committee does not currently have sufficient confidence that enough high-quality historical data for Group 2a cryptoassets exists to permit banks to apply the IMA as it relates to a stressed period calibration. The Associations therefore recommend revisiting the potential applicability of the IMA when banks have had more time to obtain and assess the quality and reliability of the data relating to this class of cryptoassets.

4. *Minimum Capital Requirements for Group 2b Cryptoassets*

- (a) The Basel Committee should clarify the scope of exposures subject to the Group 2b cryptoasset capital requirements

The Second Consultation states that the capital treatment applicable to Group 2b cryptoassets applies not only to “direct exposures,” but also to (1) funds of Group 2 cryptoassets, such as Group 2b cryptoasset ETFs, and “other entities, the material value of which is primarily derived from the value of Group 2b cryptoassets,” and (2) equity investments, derivatives or short positions in “the above funds or entities.” *See* SCO60.88. The Associations are concerned that the reference to such “other entities” could, if read broadly, include equity investments in crypto exchanges, wallet providers, blockchain miners, blockchain application developers, crypto/blockchain infrastructure providers and derivatives referencing such entities. The Associations are also concerned

about the need to potentially account for indirect secondary exposures through investments in broad indices, ETFs⁵³ or baskets that include exposures to such entities.

In light of the punitive capital treatment of Group 2b cryptoassets – i.e., not just a 1250% risk weight, but applied to the maximum of gross long and gross short exposures, thus eliminating the benefit of any hedging whatsoever – and the Group 2 cryptoasset exposure limit, the Associations are concerned that any expansion of the scope of Group 2b cryptoassets beyond direct exposures could effectively prohibit banks from investing in, or entering into derivatives and other intermediation and client facilitation transactions typical for banks with, certain service providers in the cryptoasset sector. This prohibition would have the knock-on effect of further driving cryptoasset products and services out of the regulatory perimeter, with all the consequential implications that entail for financial stability oversight. The Associations therefore request confirmation that SCO60.88 is not intended to capture exposures to such cryptoasset service providers (whether directly or by way of derivatives, indices, ETFs or baskets), based on the following considerations:

First, such an expansion of Group 2b cryptoassets would be at odds with the Second Consultation’s own definition of cryptoassets as “private digital assets that depend primarily on cryptography and distributed ledger of similar technology.” *See* SCO60.1. Equity investments in or derivative exposures to companies that provide services in relation to cryptoassets are not the same as investments in, or exposures to, Group 2b cryptoassets themselves.

Secondly, such an expansion of Group 2b cryptoassets would be at odds with the treatment of similar exposures to other companies that are engaged in activities relating to an underlying class of assets that are treated differently under the Basel capital framework. For example, equity investments in, or derivative exposures to, oil and gas or other energy companies are not treated as exposures to the underlying commodities that those companies may produce or in respect of which they may provide services. A derivative referencing the equity of an oil and gas company would be allocated to a credit risk hedging set under SA-CCR, not a commodity risk hedging set.

Third, the earnings of companies that are service providers in the cryptoassets sector are not derived directly from the value of the cryptoassets themselves, but from trading revenues, transaction validation volumes, service fees, and revenues generated from such activities as payment services and cold wallet storage, the fees from which can be independent of the value of the underlying cryptoassets.

The Associations therefore seek confirmation that the scope of SCO60.88 refers only to direct exposures to cryptoassets as defined by SCO60.1 and SCO60.2, as well as direct exposures to funds, SPVs, trusts, collective investment schemes and similar entities that own investments in, have short positions in, or have derivatives exposures referencing such Group 2b cryptoassets.

⁵³ Crypto Thematic Indices referencing such entities include Schwab Crypto Thematic Index, iShares Blockchain and Tech ETF, and Fidelity Crypto Industry and Digital Payments ETF.

5. *Minimum Capital Requirements for Credit Valuation Adjustment (“CVA”) Risk*

The Second Consultation states that Group 2a cryptoassets are subject to the basic approach for CVA risk (“BA-CVA”) as set forth in MAR50.1 through MAR50.26, and that the use of the standardised approach for CVA risk (“SA-CVA”) is not permitted for derivatives and SFTs that reference Group 2a cryptoassets. The Associations believe that, because of the liquidity requirements and corresponding price observability and FRTB-SA framework that can be applied to Group 2a cryptoassets, in principle, Group 2a cryptoassets should be allowed to be modelled under SA-CVA. SA-CVA is in any event subject to supervisory approval, and as a result regulators will review a bank’s implementation and always can require Group 2a cryptoasset exposures to be excluded from SA-CVA to the extent necessary.

6. *Minimum Capital Requirements for Counterparty Credit Risk (“CCR”)*

The Associations generally support the approach taken by the Basel Committee in the Second Consultation with respect to how minimum risk-based capital requirements for counterparty credit risk are to be applied to derivatives referencing cryptoassets, including the availability of the IMM for Group 1a cryptoassets. There are, however, four points on which the Associations seek clarification from the Basel Committee:

First, the Second Consultation states that, where there is a significant valuation difference or basis risk between a Group 1a tokenised asset and the underlying traditional asset, and there are limitations in applying the IMM because of missing data, too short a history or data quality problems, instead of the IMM, banks are obligated to apply a modified form of SA-CCR for Group 2a cryptoassets. *See* SCO60.100. As already explained in Section VI.B.2(b) above, the Associations do not understand why the inability to apply the IMM to any Group 1a cryptoassets should be treated any differently from the inability to apply the IMM to any other type of asset. If the requirements for use of the IMM are not satisfied, the default should be to use the applicable standardised approach for Group 1a cryptoassets, not the modified SA-CCR for Group 2a cryptoassets.

Second, the Second Consultation states that, for SFTs, banks should apply the comprehensive approach formula used in the standardised approach to credit risk. *See* SCO60.98. The Associations seek confirmation from the Basel Committee that an SFT or margin loan relating solely to traditional assets, even if the SFT is executed on a platform that uses the blockchain, would be eligible for the comprehensive approach to the same extent as any other SFT or margin loan involving traditional assets, including the recognition of eligible collateral. An SFT or margin loan that relates partially or wholly to Group 1a, Group 1b, and Group 2a cryptoassets would similarly qualify for the comprehensive approach to the same extent as any other SFT or margin loan involving traditional assets, subject of course to any limitations on the recognition of the relevant cryptoassets as eligible collateral.

Third, in the context of counterparty credit risk exposures for Group 2b derivatives (*see* SCO60.103), the Associations seek confirmation that banks are allowed to apply collateral,

subject to the standard haircuts under CRE22, if a bank has an enforceable netting agreement. This relates to the Replacement Cost component.

Fourth, similar to the comments made above with respect to SFTs and margin loans, the Associations seek confirmation that derivatives executed on a platform that uses the blockchain would be subject to the same rule requirements as outlined in CRE51 if they do not reference cryptoassets and that SCO60.98-60.104 would apply only if cryptoassets are referenced.

7. Minimum capital requirements for operational risk arising from cryptoasset activities are covered by existing approaches

The Second Consultation articulates two main principles relating to the treatment of operational risk for cryptoassets: first, pillar 1 operational risk RWAs would be determined by the two main components of the standardised approach for operational risk, the business indicator component and the internal loss multiplier, as set forth in OPE25; and second, to the extent that operational risks arising from cryptoassets were insufficiently captured by the minimum capital requirements for banks and a bank's internal risk management process, capital adequacy and sufficient resilience would be addressed as part of the pillar 2 supervisory review process. *See* SCO60.105.

With respect to banks' risk management processes, the Second Consultation notes that many of the risks arising from cryptoasset activities are already covered by the operational risk framework, such as ICT (general information, communication and technology) risks, cyber risks, legal risks, and money laundering and financing of terrorism risks. *See* SCO60.129. Other risks that the Second Consultation recommends that banks should consider in their risk management processes include cryptoasset technology risk, such as the stability and design of the DLT or similar technology network, the accessibility of cryptoassets to their holders (e.g., through cryptographic keys), the trustworthiness node operators and operator diversity, and valuation challenges arising from their volatility and variable pricing. *See* SCO60.130 (1) and (5).

The Associations agree that the minimum capital requirements for operational risk arising from cryptoasset activities are covered by the existing approaches to calculating operational risk RWAs, including the standardised approach that is effective from January 2023. The Associations also believe that the types of risks identified by the Second Consultation are addressed by the existing operational risk framework and by banks' risk management processes, although of course those processes must address the specific types of cryptoassets for which a bank offers products or services.

For example, many of the types of cryptoasset technology risks identified by the Second Consultation are variants of existing risks relating to vendor management and use of or reliance on a technology platform or communication system. To the extent a bank offers online banking services, it is dependent on the reliability of its internet services provider and on the reliability of any technology application or platform that it uses to provide such services, which may be provided by and/or outsourced to multiple vendors. Vendor management is an integral part of any bank's risk management processes, including the

development of a bank's own business continuity plans for technology outages and, where appropriate, the assessment of a vendor's business continuity plans.

Similarly, while different types of cryptoassets may present their own unique service accessibility issues, such as cryptographic keys, the potential loss, theft or forgery of means of accessing services is not a new type of risk. It exists currently for safety deposit keys, passwords and other means of authentication, and indeed for documents and data relating to a customer's identity, such as social security and tax identification numbers.

The same is true for valuation. The risk of limited available data for the valuation of assets, including because there are limited sources of price information or because transactions occur away from regulated exchanges, exists today for various categories of assets, including ownership interests in privately held companies or other legal entities. Accounting principles have long recognised different levels, classifications or acceptable valuation methods for assets based on the availability of underlying price data, and banks already have controls, policies and procedures related to valuation limitations in their financial disclosure, accounting policy, and risk management processes.

In short, while the Associations agree that it is necessary for banks' risk management processes and operational risk framework to take into account the specific features of the different types of cryptoassets, the Associations do not believe that these are entirely new categories of risk that banks are not equipped to address and manage. It is for this very reason that, as already discussed above in Section III, the Associations do not support the infrastructure risk add-on for Group 1 cryptoassets.

E. Trading Book / Banking Book Boundary

1. The trading book / banking book boundary for Group 1b cryptoassets should be based on the application of the boundary criteria to the stablecoin instrument itself and not the underlying reference asset(s)

While the Associations generally agree with the trading book / banking book boundary as defined under SCO60.28, there is a concern around the specification for Group 1b cryptoassets. As per SCO60.28, "Group 1b cryptoassets should be assigned to the banking book or trading book based on the application of the boundary criteria to the reference assets." It is unclear how this requirement should be applied in practice given that the trading book / banking book boundary is not just based on the properties of the underlying assets, e.g., listed / unlisted equity, but also on how an asset is accounted for or what the intent of holding the asset is. For this, the relevant instrument is the stablecoin that the bank holds and accounts for on the balance sheet, and not the underlying reference assets. In addition, the Associations do not believe that a given stablecoin position should be split between the trading and banking book based on the underlying assets. This would also be inconsistent with the treatment of funds in the capital rules where the fund is either completely in the trading book or banking book irrespective of whether look-through is applied to capitalise the fund. Therefore, the trading book / banking book boundary should be based on the stablecoin instrument and not the underlying reference assets and the Associations recommend modifying SCO60.28 to state: "Group 1b cryptoassets should be

assigned to the banking book or trading book based on the application of the boundary criteria to the stablecoin.” The Associations do not believe any stablecoin-specific trading book / banking book conditions are necessary beyond those generally applicable to bank’s exposures under RBC25.

F. Leverage Ratio Requirements

Proposed SCO60.118 states that “exposures for cryptoasset derivatives must follow the treatment of the risk-based capital framework.” The Associations seek confirmation of their understanding that cryptoasset derivatives exposures would follow the counterparty risk calculations pursuant to SCO60.98-60.104 and otherwise follow existing leverage exposure practices.

G. Minimum Liquidity Risk Requirements

1. The Basel Committee should clarify that operational requirements for Group 1a cryptoassets to be considered as HQLA-eligible should include settlement and monetisation both on-chain and off-chain

Proposed SCO60.107 states in the footnote that “[Group 1a cryptoassets] must also satisfy the operational requirements in [LCR30.13] to [LCR30.28]” in addition to both the underlying asset and the token satisfying the characteristics of HQLA in order to be considered as HQLA. Under [LCR30.17], “monetization of [an HQLA] asset must be executable, from an operational perspective, in the standard settlement period for the asset class in the relevant jurisdiction.” In the early stages of new cryptoasset offerings, on-chain liquidity may be thin and standard settlement periods for on-chain transactions may not exist; as such, monetisation of the tokenised asset may only be available via the redemption for the physical underlying asset, and subsequently monetised via traditional means (e.g., sale and/or repo). The off-chain monetisation process may therefore be longer versus the standard settlement period of the traditional physical asset alone. The Basel Committee should clarify that such monetisation and settlement periods are still within the guidelines under the operational requirements for HQLA in [LCR30.17], despite the potential increase in settlement period.

2. Certain Group 1b stablecoins backed by reserve assets that are solely HQLA should be considered as HQLA-eligible

Proposed SCO60.108 does not allow consideration of Group 1b stablecoins as HQLA. However, a subsection of Group 1b stablecoins are wholly backed by HQLA-eligible reserve assets and have established on-chain market depth. Given that these cryptoassets would already fulfil the basis risk and redemption test to be classified as Group 1b stablecoins, the Associations believe that a bank holding such stablecoins should be allowed to consider such holdings as part of its stock of HQLA (provided that the stablecoin satisfies other operational requirements of HQLA) as these stablecoins can be demonstrably monetised with little or no loss of value. As a corollary, any holdings of such Group 1b stablecoins should not be assigned an 85% RSF risk factor for purposes of the NSFR.

H. Technical Corrections and Questions

The Associations would also like to make the following observations relating to technical corrections and questions in connection with the Second Consultation.

- Regarding SCO60.60, “major fiat currency” is undefined. We recommend the most liquid currencies specified in MAR 33.12(3) meet this definition, specifically the 10-day liquidity horizon currencies for “interest rate: specified currencies and Foreign Exchange (FX) rate: specified currency pairs.”
- Regarding SCO60.88(2), derivatives in this line reference cryptoasset ETFs, and other entities. The Associations presume the intention was to also include derivatives referencing direct cryptoasset exposures.
- Regarding SCO60.98 & 60.104, the reference cited should begin at CRE22.40 not CRE22.45
- Regarding SCO60.104, beginning January 1, 2023 haircuts applied to other equities that are traded on a recognised exchange will be 30% pursuant to CRE22.49. The Associations seek clarification whether the Committee intends to apply a 25% haircut or the 30% haircut.

VII. Conclusion

The Associations support the Basel Committee’s development of a framework for the prudential treatment of cryptoassets. The Associations believe that the Second Consultation contains several improvements to the First Consultation’s cryptoasset exposure framework, including the creation of a Group 2a cryptoasset category and the partial recognition of hedging for that category. At the same time, the Associations believe that the Second Consultation includes features and calibrations that could meaningfully reduce the ability of banks to – and in some cases effectively preclude banks from – offering their customers cryptoasset products and services and utilising DLT to perform traditional functions more efficiently.

Interest in cryptoassets from consumers and institutional investors has increased rapidly in recent years. In addition, DLT and similar technologies underlying cryptoassets hold significant promise for making the financial sector safer, more efficient, and more inclusive. The Associations’ recommendations contained in this letter seek to ensure that the design of the cryptoasset exposure framework is appropriately calibrated and facilitates bringing these activities within the regulatory perimeter where they will be subject to appropriate regulation, risk management and supervisory oversight.

The Associations’ comments aim to improve the mutual understanding of current and emerging risks, the role of existing processes and frameworks for regulated entities to manage such risks, and to identify balanced solutions to help in the design of a capital framework that supports enhancing financial stability while avoiding overly restrictive limits to innovation.

In sum, bringing cryptoasset activities into the regulatory perimeter where institutions are subject to comprehensive regulation and supervision and have significant experience managing financial and operational risks would be beneficial for the stability of the financial system. Enabling banks to utilise cryptography and DLT or similar technology would also allow bank customers and the broader financial sector to benefit from the advances in efficiency, transparency and speed that these innovations offer.

* * *

The Associations appreciate your consideration of our comments and proposals and remain at your disposal to discuss any of these views in greater detail.

Respectfully submitted,



Allison Parent
Executive Director
Global Financial Markets
Association



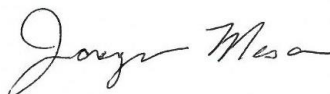
Panayiotis Dionysopoulos
Head of Capital
International Swaps and
Derivatives Association



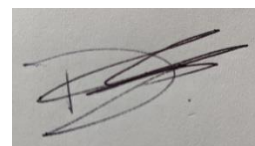
Richard Gray
Director, Regulatory Affairs
Institute of International
Finance



Sean D. Campbell
Chief Economist and
Head of Policy Research
Financial Services Forum



Jacqueline Mesa
COO and SVP Global Policy
Futures Industry Association



David Shone
Director – Market
Infrastructure & Technology
The International Securities
Lending Association



Kathryn Collard
Senior Vice President and
Associate General Counsel
Bank Policy Institute



Gabriel Callsen
Director,
FinTech and Digitalization
International Capital Market
Association

cc: François Villeroy de Galhau, Chair, Bank for International Settlements
Sir Jon Cunliffe, Chair, Committee on Payments and Market Infrastructures
Klaas Knot, Chair, Financial Stability Board
Ashley Ian Alder, Chair, International Organization of Securities Commissions

Appendix 1 Cryptoasset Case Studies and Use Cases

Digital Bond Issuance by European Investment Bank (EIB): Permissioned tokenised traditional assets in a permissionless blockchain.

Summary:

In April 2021, the European Investment Bank (EIB) issued the 1st multi dealer led, primary issuance of digital bonds (EUR 100M) using the Ethereum permissionless blockchain technology, rated Aaa/AAA/AAA, in collaboration with Banco Santander, Goldman Sachs and Societe Generale as joint lead managers. The settlement of such issuance has been realised in a digital representation of euro (wholesale central bank digital currency (“CBDC”)) issued by the French central bank (Banque de France). EIB digital bonds have been clearly defined in the issuance documentation as bonds in dematerialised form, issued in fully registered form (*‘nominatif pur’*) in a permissionless blockchain under French law, conferring the same legal rights of ownership as bonds issued in book-entry form. While the underlying blockchain technology is permissionless, the EIB bonds are permissioned tokens: in accordance with the Compliant Architecture for Security Tokens (“CAST”) security tokens framework, the identity of the issuer’s agent (registrar and settlement agent) has been directly whitelisted within the EIB bonds’ smart contract and a validation process has been put in place within the smart contract to authorise *ex ante* any potential transfer of property realised on the blockchain. Therefore, no peer-to-peer transfer of EIB bonds is possible without the prior approval of the issuer and/or its agent. Besides, for risk management and regulatory purposes, Societe Generale-Forge, the regulated subsidiary of Societe Generale mandated by the EIB as registrar and settlement agent under the issuance documentation to validate EIB bonds’ transactions on the blockchain, has put in place a business continuity plan, including notably an external data retention system, to keep at all times an ‘off-chain’ monitoring of the EIB bonds holders’ positions and mitigate any potential technological issue.

Background:

The European Investment Bank (EIB) is the lending arm of the European Union. The EIB is one of the largest multilateral financial institutions and has delivered a total of EUR 95 billion in financing in 2021 alone. The EIB works with other EU institutions to foster European integration, promote development in the European Union and support EU policies.

Fostering market developments in the digitalisation of capital markets and paving the way for market participants to adopt blockchain technology for the issuance and trade of financial instruments, the EIB issued in April 2021 its first ever digital bond on a public blockchain. Made in collaboration with Goldman Sachs, Santander and Societe Generale, the € 100 million 2-year bond issuance, placed with key market investors, represented the first multi-dealer led, primary issuance of digitally native tokens using the public blockchain technology Ethereum. The project has been selected by Banque de France as part of its Central Bank Digital Currency (CBDC) experimental projects.

This debt issuance (ISIN FR0014003521) has generated more than 15 transactions among top-tier investors to date.

How did the issuance work?

On 28 April 2021, the EIB issued a digital bond, governed by French Law, on a blockchain platform. The full issuance and registration of these digital bonds were made on the Ethereum permissionless blockchain. This EIB issuance was rated Aaa/AAA/AAA by credit agencies, which did not discount it for any additional risk when compared to “traditional” EIB bonds.

In a partnership with Banque de France, the proceeds from the issuance of the tokenised bond provided to the EIB have been represented on the blockchain in the form of a wholesale CBDC, i.e., a digital representation of the Euro on the Ethereum permissionless blockchain.

The EIB mandated Banco Santander, Goldman Sachs and Societe Generale as joint lead managers for the securities’ placing. Societe Generale-FORGE, a regulated subsidiary of Societe Generale, has been mandated as joint structuring manager, registrar and settlement agent, and as such validated *ex ante* the compliance controls (KYC, AML, sanctions and embargoes) for all securities transactions on the blockchain before their effective technological registration on the permissionless blockchain.

How was the issuance made legally and technologically secure?

The booking was performed exactly like a traditional bond, with the notable exception that no central security depository (“CSD”) was needed for this issuance: the EIB bonds were issued directly on a public blockchain (Ethereum) as a “native token,” and were legally characterised under French Law as MiFID2 financial instruments, and more specifically as bonds issued in fully registered form (*‘nominatif pur’*) in a permissionless blockchain, conferring the same legal rights to bondholders as bonds issued in book-entry, and with the transfer of ownership of the EIB bonds performed by the transfer of the tokens within the blockchain.

With the objective of facilitating risk management and compliance in line with traditional securities market practices, the EIB bond issuance was structured according to the CAST framework. In addition to the whitelisting of the issuer’s agents (registrar and settlement agent), preventing non-identified actors to intervene on the transactions, the smart contract of the bonds included a function requiring that any transfer of financial securities between the issuer and investors and between two investors (strictly identified within legal documentation as well as by their two own addresses, known by the issuer and/or its agents) be validated by one or several agents acting on behalf of the issuer, i.e., the registrar and the settlement agent, based on banking-grade KYC, AML and sanctions and embargoes controls. Transactions on the EIB digital bonds are therefore based on permissioned services by regulated entities enabled on DLT-based permissionless securities. This *ex ante* validation of any transaction on the permissionless blockchain makes it possible, independently of the underlying technology, to verify that the future owner of the

tokenised traditional securities is duly identified and checked (KYC/AML, sanctions-embargoes, etc.) before the effective completion of the transaction.

Due diligence in terms of regulatory obligations, and notably financial crime (KYC-AML, freezing of assets, embargoes and sanctions, etc.), has been realised while using a permissionless technology as golden source for the registration of property transfer.

Finally, the settlement was successfully carried out using a wholesale version of Central Bank Digital Currency (CBDC) on a blockchain, under the Banque de France experimental ecosystem. From a technological standpoint, the issuance required the development and deployment of smart contracts under secured conditions, ensuring that CBDC tokens were safely issued and controlled, and that CBDC transfers occurred simultaneously with the delivery of securities tokens to the investors' portfolio, in a Delivery versus Payment, without requesting the intermediation of neither a CSD nor Target-2 Securities.

What are the benefits for the issuer?

According to the EIB press release on such issuance, “the digitalisation of capital markets may bring benefits to market participants in the coming years, including a reduction of intermediaries and fixed costs, better market transparency through an increased capacity to see trading flows and identity asset owners, as well as a much faster settlement speed.” Added value for both issuers and investors has consisted in fewer intermediaries, a much faster settlement speed (T0), and the possibility for investors to read their positions directly on the blockchain on a 24/7 basis without intermediation.

The role of issuer's agent for the registration of the bonds in a smart contract (i.e., registrar), based on Societe Generale-FORGE capabilities, enabled the issuer and dealers to transfer EIB bonds in a safe manner and to be informed of the events related to the EIB bonds during their lifecycle. As an example, noteholders were recently informed of the occurrence of a significant technical upgrade on the Ethereum blockchain (“[The Merge](#)”), on which the EIB bonds were issued, realised on 15 September 2022, as announced by the Ethereum Foundation. Besides, for risk management and regulatory purposes, Societe Generale-FORGE has, according to French Law, put in place a business continuity plan, including notably an external data retention system, to keep at all times an ‘off-chain’ monitoring of the EIB bonds holders' positions and mitigate any potential technological issues.

On the secondary market, liquidity is limited to OTC transactions as only a few counterparties are technically equipped to perform transactions. Nevertheless, a cross-border collateral upgrade repo transaction involving this bond had been booked using the DLT with a German asset manager. This was the first time a digital bond was borrowed on a blockchain, collateralised through a triparty agent and backed by a traditional contractual setup.

The EIB tokenised bond issuance is still outstanding, with ongoing OTC transactions on the secondary market. Transactions can be visualised by all bondholders directly on the Ethereum blockchain (via Etherscan, a node, etc.). These capabilities of public blockchains

bring a central registry ‘on-chain’, accessible by everywhere, whilst remaining anonymous, which reduces massively reconciliations between capital market participants.

What conclusions can be drawn from this pioneering transaction?

The EIB digital bond issuance on a permissionless blockchain represents a significant step taken by financial institutions to facilitate blockchain based bond issuances. Since 2018, an equivalency of rights between a registration of securities in a book-entry form and a registration on a blockchain is recognised in France, and since then in Luxembourg, Germany and soon in the EU through the “DLT Pilot Regime.” After the substantial move from paper-based securities to dematerialised securities since the 1980s in France, and more recently in Germany, the use of DLTs could be the next step of securities digitisation and processing automation. It is crucial that regulated financial institutions will remain a major part of innovation in this area to facilitate such core banking services.

Intraday repo: Permissioned tokenised traditional assets in a private blockchain

The intraday repo product is designed to reduce risk in the wholesale cash clearing markets. This happens by shifting risk from unsecured, uncommitted credit facilities provided by the cash clearing bank, to secured financing transactions. The risk profile changes from one that can cause further friction during a market stress, due to the reduced appetite to offer unsecured credit, to one where the cash clearing market - which underpins the funding for securities settlement venues (DTC progress payments, etc.), continues to be available to the banks and dealers who rely on it to meet their intraday liquidity obligations.

The product enables this by enhancing the speed and control of settlement of repo transactions using a private, permissioned distributed ledger. By using this ledger, in concert with existing market platforms, underpinned by existing legal and regulatory frameworks, clients can execute repo transactions in minutes, that last minutes or hours. The process for settlement front-loads the operational steps, preventing fails, partials or other incomplete settlements. The means of executing this trade and reducing risk in this way is not achievable using existing platforms in their current construct; distributed ledger technology is the key enabler.

From a tech controls point of view, private permissioned DLT platforms will follow standard and rigorous processes for app development by necessity; these are already mandated in operational risk requirements. This includes the identification and remediation of software vulnerabilities, including in open source software, code scanning to identify common anti-patterns, code review and software-development-lifecycle processes, segregation of duties regarding the production environment, hardware resiliency standards and testing, and cyber and wider technology control protections. The overall stack of software associated with private permissioned DLT networks should be considered as a complimentary set of technologies, with the same level of testing, resilience, protection and control as all other software used by regulated institutions – as required by existing regulatory requirements and practices.

JPM Coin System: A permissioned blockchain system for recording deposit account balances and making instant payments.

In 2020, JPMorgan Chase Bank, N.A. (“JPMCB”), a wholly-owned subsidiary of JPMorgan Chase & Co. (“JPM”), launched the JPM Coin System, JPM’s first production based implementation of blockchain technology for value recordation and value bearing transactions.

The JPM Coin System allows participating clients of JPMCB to record demand deposit balances and make instant payment transfers using a blockchain ledger. The system helps to address the challenges of cross border payments, simplifies clients’ liquidity funding needs and provides better treasury solutions to corporate clients.

The JPM Coin System consists of the blockchain ledger, the deposit accounts recorded on the blockchain ledger (“Blockchain Deposit Accounts”), and certain technical components that allow for clients to send instructions to JPMCB regarding their accounts, which are similar to those used with other payments services. The JPM Coin System operates in coordination with JPMCB’s existing non-blockchain demand deposit recordkeeping systems (as balances can move between accounts on the different systems) and other systems and applications used by the Firm to support payments activity.

Using blockchain technology, the JPM Coin System is fundamentally just an alternate way of representing and recording how many U.S. dollars—recorded as the balances in Blockchain Deposit Accounts on the JPM Coin System—each participating client has on deposit at JPMCB and how many such U.S. dollars are being or have been transferred among users of the JPM Coin System. The Blockchain Deposit Accounts on the JPM Coin System are the official record and evidence of the deposit balance that JPMCB owed to each participating client under current applicable U.S. banking laws and regulations.

Additionally, the blockchain ledger used in the JPM Coin System is private and permissioned, which means that JPMCB is the single entity which is the central authority that determines who can participate and/or transact on the blockchain ledger. Also, the consensus mechanism for the JPM Coin System is set up such that JPMCB is the sole party allowed to make changes to the ledger.

Blockchain Deposit Accounts are subject to existing bank capital and liquidity requirements as well as other bank risk management, resolution planning and related requirements that are intended to control systemic and other risks associated with deposit-taking activities.

Third Party Vendor Engagement and Management – Identification, Selection and Onboarding of Digital Custodians (H1 2021)

In 2021 a systemically important bank undertook an effort to identify, select and onboard digital asset custodians as part of a multi-custodian strategy to support the firm’s objectives of engage in issuance, trading and management of digital assets. Although use cases are varied, the custodians have capability to custody both Group 1 and Group 2 assets. In the pre-qualification phase, the firm conducted a structured Request for Information (“RFI”)

and ranked six custodians utilising objective criteria related to pricing, security/insurance, legal/compliance, brand/reputational risk, track record and scale, product, financial stability and trade execution. The firm contracted a big four consulting firm to review and improve the RFI and provide their view of firm's rankings. Since the RFI, the firm has onboarded two digital assets custodians in accordance with the third party risk management framework, and fourth party due diligence process. In addition, Operational Risk conducted a second line review utilising key vendor onboarding artifacts (e.g., RFI results, vendor information security reviews, SOC reports, vendor interviews). The results of this review were presented at the bank's operational risk and resilience committee. Further, new activities that utilise digital custodians are required to be reviewed and approved at the firm's new activity committees and any automated trading capabilities directly accessed by the firm will be governed under the firm's automated trading control governance.

By utilising the firm's governance bodies and risk management frameworks, as required by policy, the firm was able to bring its expertise to bear on this new vendor class, and identify potential risks and control weaknesses leading to improvements prior to onboarding. Examples of resulting improvements include (1) improvements to patch management policy, (2) technical controls to restrict capability to write to external drives, (3) improvements to encryption key lifecycle management, (4) implementation of hard blocking message rate controls for Smart Order Routers ("SOR"), and (5) implementation of SOR related 'cancel on disconnect' controls.

Overall, the firm has found this class of third parties highly receptive to suggested control improvements resulting in a virtuous cycle of more effective control environments as regulated entities increase engagement with digital third parties.

Appendix 2 Proposed Rule Text for Interim Approach

If the Interim Approach is adopted, the Associations propose to replace paragraph SCO60.124 with the following:

Definition of total exposure value

60.124 The total exposure to Group 2a cryptoassets that will be subject to the 5% limit will be defined using the formula below, where:

- (1) c is the reference to a distinct Group 2a cryptoasset.
- (2) *Instrument Exposure_i* is an individual gross long or short Group 2a cryptoasset exposure or individual derivative referencing a Group 2a cryptoasset. Derivative exposures must be measured using a delta-equivalent methodology
- (3) *Longs_i* is an individual gross long Group 2a cryptoasset exposure or individual derivative referencing a Group 2a cryptoasset. Derivative exposures must be measured using a delta-equivalent methodology
- (4) *Shorts_i* is an individual gross short Group 2a cryptoasset exposure or individual derivative referencing a Group 2a cryptoasset. Derivative exposures must be measured using a delta-equivalent methodology
- (5) R denotes the hedging disallowance parameter, set to 20%

Total Exposure

$$= \sum_c \left[\left| \sum_i^I \text{Instrument Exposure}_i \right| + R \left(\min \left[\sum_i^I \text{Longs}_i, \left| \sum_i^I \text{Shorts}_i \right| \right] \right) \right]$$

The calibration of the hedging disallowance parameter R is subject to a review by the Basel Committee at least every two years.

The text incorporates two other recommendations from the Associations, specifically, the higher exposure limit of 5% as described in Section I.B and the exclusion of Group 2b cryptoassets from the limit as per Section I.C.

The formula above is consistent with the framework presented in Section II as the term above can be split into an unhedged and hedged exposure as per below:

$$\text{Unhedged Exposure} = \left| \sum_i^I \text{Instrument Exposure}_i \right|$$

$$\text{Hedged Exposure} = \left(\min \left[\sum_i^I \text{Longs}_i, \left| \sum_i^I \text{Shorts}_i \right| \right] \right)$$

Appendix 3 Correlation Across Tenors for Bitcoin and Ether

The correlation across tenors for Bitcoin and Ether (using CME futures) shown below suggests that a correlation parameter along the maturity dimension would be appropriately set to 99% given all pairs are well above that threshold. The data spans from spot to 5-month futures. For longer tenors, given lower liquidity, the data are sporadic and are excluded from the analysis:

10 day returns for Bitcoin across tenors (data sourced from Bloomberg for period 1/1/2017 to 7/15/2022):

10d returns						
	Bitcoin spot	Bitcoin 1M	Bitcoin 2M	Bitcoin 3M	Bitcoin 4M	Bitcoin 5M
Bitcoin spot	100.00%	99.36%	99.35%	99.33%	99.24%	99.23%
Bitcoin 1M		100.00%	99.99%	99.96%	99.90%	99.81%
Bitcoin 2M			100.00%	99.98%	99.93%	99.84%
Bitcoin 3M				100.00%	99.95%	99.86%
Bitcoin 4M					100.00%	99.86%
Bitcoin 5M						100.00%

10 day returns for Ether across tenors (data sourced from Bloomberg for period 1/1/2017 to 7/15/2022):

10d returns						
	Ether spot	Ether 1M	Ether 2M	Ether 3M	Ether 4M	Ether 5M
Ether spot	100.00%	99.42%	99.39%	99.37%	99.32%	99.32%
Ether 1M		100.00%	99.98%	99.95%	99.92%	99.84%
Ether 2M			100.00%	99.98%	99.95%	99.87%
Ether 3M				100.00%	99.98%	99.91%
Ether 4M					100.00%	99.93%
Ether 5M						100.00%

Appendix 4 Supporting Analysis for Exposure Limit Calibration

The following tables support the derivation of the potential crypto footprint borrowing data from client facilitation of financial institutions from G-SIB disclosures:

The GSIB Assets & Tier 1 Capital are as of YE 2021. Intra-financial assets do not include derivatives referencing FIs.				
(in MM of USD)	Client Demand			Tier 1 Capital
	Intra-Financial System Assets: Equity Securities (gross longs)	Intra-Financial System Assets: Offsetting Short Positions (gross shorts)	Gross (L + S)	
Bank of America	15,763	3,947	19,710	196,465
JP Morgan	18,266	16,724	34,990	246,162
Citigroup	28,991	15,187	44,178	169,568
Wells Fargo Company	8,177	560	8,737	159,671
Morgan Stanley	24,239	11,226	35,465	83,348
Goldman Sachs	15,658	10,903	26,561	106,766
BNP Paribas	171,928	2,836	174,765	114,068
HSBC	66,506	11,957	78,463	156,300
Barclays	29,863	0	29,863	81,591
Deutsche Bank	3,521	71	3,591	62,976
Bank of New York Mellon	401	0	401	23,485
Group BPCE	11,425	2,926	14,351	79,340
Group Credit Agricole	17,878	0	17,878	122,312
ING Bank	6,285	2,795	9,080	64,390
Royal Bank of Canada	18,010	841	18,851	65,083
Santander	10,031	1,947	11,978	90,912
Societe Generale	72,835	10,673	83,508	65,856
Standard Chartered	2,597	29	2,626	45,153
State Street	1,414	0	1,414	17,923
Toronto Dominion	25,213	15,755	40,967	59,916
UniCredit	6,817	230	7,046	65,711
Total	555,818	108,606	664,423	2,076,998

The limitations of this analysis include the fact that G-SIB intra-financial assets include funds. Hence, the investments might be overstated relative to pure direct investments in financial institutions.

The reporting date used for Canadian banks follows the Canadian fiscal calendar. Hence, October 31, 2021 was used as the as-of date for Canadian banks instead of December 31, 2021.

Appendix 5

Overview of the Associations

The **Financial Services Forum** (“FSF”) is an economic policy and advocacy organisation whose members are the chief executive officers of the eight largest and most diversified financial institutions headquartered in the United States. Forum member institutions are a leading source of lending and investment in the United States and serve millions of consumers, businesses, investors and communities throughout the country. The Forum promotes policies that support savings and investment, deep and liquid capital markets, a competitive global marketplace and a sound financial system.

The **Futures Industry Association** is the leading global trade organisation for the futures, options and centrally cleared derivatives markets, with offices in London, Brussels, Singapore and Washington, DC. FIA’s mission is to support open, transparent and competitive markets; protect and enhance the integrity of the financial system; and promote high standards of professional conduct. FIA’s membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from more than 48 countries, as well as technology vendors, lawyers and other professionals serving the industry.

The **International Securities Lending Association** (“ISLA”) is a leading non-profit industry association, representing the common interests of securities lending and financing market participants across Europe, Middle East and Africa. Its geographically diverse membership of over 180 firms includes institutional investors, asset managers, custodial banks, prime brokers and service providers. ISLA advocates for, amongst other things, the importance of securities lending to the broader financial services industry. It supports the Global Master Securities Lending Agreement (“GMSLA”) legal framework, including the Title Transfer and Securities Interest over Collateral variants, as well as the periodical enforceability and security enforcement across global jurisdictions.

The **Bank Policy Institute** is a nonpartisan public policy, research and advocacy group, representing the nation’s leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation’s small business loans and are an engine for financial innovation and economic growth.

The **International Capital Market Association** (“ICMA”) promotes well-functioning cross-border capital markets, which are essential to fund sustainable economic growth. It is a not-for-profit membership association with offices in Zurich, London, Paris, Brussels, and Hong Kong, serving around 600 members in 65 jurisdictions globally. Its members include private and public sector issuers, banks and securities dealers, asset and fund managers, insurance companies, law firms, capital market infrastructure providers and central banks. ICMA provides industry-driven standards and recommendations, prioritising three core fixed income market areas: primary, secondary and repo and collateral, overlaid by the transformational cross-cutting themes of sustainable finance and Fintech and digitalisation. ICMA works with regulatory and governmental authorities,

helping to ensure that financial regulation supports stable and efficient capital markets.
www.icmagroup.org

The **Global Financial Markets Association** (“[GFMA](#)”) represents the common interests of the world’s leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. [GFMA](#) brings together three of the world’s leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (“[AFME](#)”) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (“[ASIFMA](#)”) in Hong Kong and the Securities Industry and Financial Markets Association (“[SIFMA](#)”) in New York and Washington are, respectively, the European, Asian and North American members of GFMA.

The **Institute of International Finance** (“[IIF](#)”) is the global association of the financial industry, with more than 400 members from more than 70 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks.

Since 1985, the **International Swaps and Derivatives Association** (“[ISDA](#)”) has worked to make the global derivatives markets safer and more efficient. Today, ISDA has over 990 member institutions from 78 countries. These members comprise a broad range of derivatives market participants, including corporations, investment managers, government and supranational entities, insurance companies, energy and commodities firms and international and regional banks. In addition to market participants, members also include key components of the derivatives market infrastructure, such as exchanges, intermediaries, clearing houses and repositories, as well as law firms, accounting firms and other service providers. Information about ISDA and its activities is available on the Association’s website: www.isda.org. Follow us on [Twitter](#), [LinkedIn](#), [Facebook](#) and [YouTube](#).

**Appendix 6
Defined Terms**

Defined Terms	Page No. for Definition
AFME: Associations for Financial Markets in Europe	1
AGG: iShares Core U.S. Aggregate Bond ETF	46
AML: Anti-money laundering	32
ASIFMA: Asia Securities Industry & Financial Markets Association	1
Associations: The Global Financial Markets Association, the Futures Industry Association, the Institute of International Finance, the International Swaps and Derivatives Association, the International Securities Lending Association, the Bank Policy Institute, the International Capital Markets Association and the Financial Services Forum	1
ASX: Australian Securities Exchange	39
BA-CVA: Basic approach for CVA risk	63
Basel Committee: Basel Committee on Banking Supervision	1
BCP: Business continuity plan	35
Blockchain Deposit Accounts: Deposit accounts recorded on the blockchain ledger	74
BND: Vanguard Total Bond Market Index Fund ETF	46
CASP: Cryptoasset service provider	50
CAST: Compliance Architecture for Security Tokens	70
CBDC: Central Bank Digital Currency	70
CCR: Counterparty credit risk	63
CME: Chicago Mercantile Exchange	12

CSD: Central security deposit	71
CVA: Credit valuation adjustment	63
DLT: Distributed ledger technology	2
EFA: iShares MSCI EAFE ETF	46
EIB: European Investment Bank	30
ETF: Exchange traded fund	12
ETN: Exchange traded note	23
FATF: Financial Action Task Force	50
FDIC: Federal Deposit Insurance Corporation	34
FI: Financial institutions	18
FIA: Futures Industry Association	21
First Consultation Comments: The Associations' response to the First Consultation	3
First Consultation: Basel Committee's first consultative document on the "Prudential treatment of cryptoasset exposures"	3
FMU: Financial market utility	35
FRB: Board of Governors of the Federal Reserve System	34
FRTB: Fundamental review of the trading book	59
FSF: Financial Services Forum	79
FX: Foreign exchange	23
GFMA: Global Financial Markets Association	80
GLD: SPDR Gold Shares	46
GMSLA: Global Master Securities Lending Agreement	79
HKEX: Hong Kong Exchanges and Clearing Limited	40
ICMA: International Capital Market Association	79

ICT: Information, communication and technology	34
IIF: Institute of International Finance	80
IMA: Internal models approach	61
IMM: Internal models method	56
Interim Approach: Proposal by the Associations for an approach that provides some reduced recognition of hedging benefits in the event the Basel Committee does not adopt the net exposure approach	16
ISDA: International Swaps and Derivatives Association	80
ISLA: International Securities Lending Association	79
JPM: JPMorgan Chase & Co.	74
JPMCB: JPMorgan Chase Bank, N.A.	74
KYC: Know your customer	32
MiCA: Markets in Crypto-Assets	50
Non-Redemption Risk Group 1b: Group 1b cryptoassets that do not expose banks to the risk of default of the redeemer	54
OCC: Office of the Comptroller of the Currency	34
Prudentially Regulated Issuer: Institution subject to prudential capital and liquidity requirements	55
QQQ: Invesco QQQ Trust Series 1	46
RFI: Request for Information	74
RRAO: Residual risk add-on	28
RWA: Risk-weighted asset	3
SA: Standardised Approach	22
SCG: Basel Committee's Supervisory Cooperation Group	38

Second Consultation: Basel Committee's second consultative document on the "Prudential treatment of cryptoasset exposures"	1
SFT: Securities financing transaction	20
SIFMA: Securities Industry and Financial Markets Association	1
SOR: Smart Order Routers	75
SPY: SPDR S&P 500 Trust	46
SSA: Simplified Standardised Approach	61
The Merge: A significant technical upgrade on the Ethereum blockchain on which EIB bonds were issued	72
USO: United States Oil Fund, LP	46
VASP: Virtual Asset Service Provider	50