Consultation response

Basel Committee on Banking Supervision – Cryptoasset standard amendments, December 2023

The Global Financial Markets Association,[1] the Futures Industry Association, the Institute of International Finance, the International Swaps and Derivatives Association, and the Financial Services Forum (collectively, the "Associations") appreciate the opportunity to respond to the Basel Committee on Banking Supervision's (the "BCBS") consultative document "Cryptoasset standard amendments" dated December 2023 (the "Consultation").[2]

The Associations welcome the BCBS's continued focus on designing and improving the prudential framework for cryptoassets. We look forward to ongoing collaboration as these markets continue to evolve.

Executive Summary

Public permissionless blockchains – We note the BCBS's conclusion that the use of permissionless blockchains gives rise to a number of unique risks, some of which cannot be sufficiently mitigated at present. We respectfully disagree with that conclusion. We acknowledge that there are risks with the use of permissionless blockchains but are of the firm view that industry has all necessary expertise and robust compliance frameworks to fully identify, manage and mitigate these risks. Hence, we recommend permitting banks to conduct a Group 1 assessment for permissionless blockchains.

As the uses of distributed ledger technology ("DLT") are evolving it is imperative not to disincentivise or prevent industry participants from investing in, exploring and innovating in all forms of technology including public blockchains. If banks are prevented from using public blockchains this may encourage the market to focus on the non-bank financial institutions / shadow banking space, which may result in systemic risks outside of the regulatory perimeter.

[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 2 for information regarding each of the Associations.

There have been several successful pilot tests which relied on permissionless technologies which have allowed many of the resulting risks to be understood and controlled.

The BCBS's stance is contrary to the prudential principles of technological neutrality and "same asset, same risk" and may impact on the wider development of liquid tokenisation markets, not least due to the potential lack of interoperability between private blockchains. While we acknowledge that risk mitigation techniques are evolving for permissionless cryptoassets to be assessed for Group 1 cryptoassets, we are confident that solutions already exist in respect of specific use cases. Therefore, as long as banks can satisfy themselves that relevant risks have been addressed, the use of permissionless blockchains should remain possible. We request the BCBS to continue engaging with the industry and share its assessment of permissionless blockchains.

Classification Condition 2 and Settlement Finality – Legal frameworks are in the process of being developed globally to help address settlement finality and private or commercial law considerations for tokenised securities and payments settlement in both primary and secondary markets. We therefore request that the classification condition for a Group 1 cryptoasset related to settlement finality for both primary and secondary markets be made non-prescriptive. In practice, the settlement finality requirement should be deemed satisfied where: (1) the processes as to how and when settlement of the transaction is achieved (whether pursuant to a bilateral contract or pursuant to the rules or technical processes or conventions of the relevant market, exchange or other venue) is reasonably clear to the bank; and (2) the bank has conducted a review of the settlement process and has concluded to its satisfaction that settlement finality is achieved, or is likely to be achieved in practice. This approach would be consistent with the fact that the use of DLT can assist in mitigating settlement risk in many use cases as recognised by the BIS and the BIS Innovation Hub.[3]

Group 1b Eligibility – The BCBS's proposed amendments at SCO 60.12(2)(b)(iv)[4] and SCO 60.12(2)(c)(iii)[5] would appear not to allow a bank serving as custodian for reserve assets to hold any of the stablecoin's cash on deposit, whether actual cash reserves or frictional cash that results from the provision of day-to-day safekeeping and asset administration services. Hence, we suggest that while segregation away from the insolvency risk of the custodian can be achieved and should be the objective for securities or other non-cash assets, there should be an exemption for cash (reserve assets) placed or deposited with (1) any prudentially regulated bank or (2) other arrangements which are remote from the insolvency of stablecoin *issuers*.

In respect of the BCBS proposal that authorities must have the power to apply an infrastructure risk add-on to the capital requirement for exposures to Group 1 cryptoassets, we would like to reiterate that this is unnecessary, given that it seeks to address risks that are already addressed by the existing prudential framework and risk management systems such as operational risk and third-party risk management frameworks, supervisory tools and controls. We urge BCBS

---

[3] See for example, the BIS CPMI Consultative Report Facilitating increased adoption of payment versus payment, and BIS Innovation Hub Project Helvetia or Project Dunbar.

[4] "[The] reserve assets are placed in structures that are bankruptcy remote from any party that issues, manages or involved in the stablecoin operation, or custodies the reserve assets".

[5] Eligible reserve assets include "deposits at high credit quality banks with safeguards, such as: a concentration limit applied at group level that include entities with close links; bankruptcy remoteness of the deposits from any party that issues, manages or is involved in the stablecoin operation; and the banks apply the Basel Framework (including the liquidity coverage ratio)."

to remove the infrastructure risk add-on in its entirety, or otherwise recommend a consistent cross-jurisdictional approach where the use of the infrastructure risk add-on is a last resort.

Finally, as the BCBS kindly stated that it welcomes comments on all aspects of the proposed amendments to the cryptoasset standards, we have suggested certain changes to the regime applicable to Group 2 cryptoassets.

Consultation Response

1. Public permissionless blockchains

Introduction and background

We note that the BCBS in the Consultation states that it "has completed this review and concluded that the use of permissionless blockchains gives rise to a number of unique risks, some of which cannot be sufficiently mitigated at present".[6]

As a starting point, we think that is important that we define exactly what is meant by permissionless blockchains in order that there is a clear consensus on what we understand your analysis to be based on. To that end, we have included a suggested definition at *Appendix 1* to this Consultation Response.

The BCBS position regarding the perceived risks inherent in public permissionless blockchains would disincentivise, and ultimately is likely to prevent, banks from investing in and exploring the public blockchain. The statement that permissionless blockchains give rise to a number of unique risks, some of which cannot be sufficiently mitigated at present, is not conducive to innovation and does not allow participants to understand and propose adequate solutions for managing such risks. In fact, where SCO 60 bans the use of a particular type of technology, this could cause relevant risks to cluster outside of the regulatory perimeter (encouraging, for example, participants to look to the non-bank financial institutions / shadow banking space).

Although we acknowledge the BCBS's reservations, we consider that cryptoassets that use permissionless blockchains should be capable of being assessed to be fully recognised within Group 1. As we explain below, permissionless technologies have been tested with other open networks and the risks can be understood and controlled.

In the Association's response to the BCBS's second consultation on cryptoassets, we acknowledged that there are risks with permissionless blockchains but suggested that banks have the expertise and robust compliance frameworks to mitigate the risks of new technology as banks know the downsides of private blockchains, including fragmentation, lack of interoperability and insufficient liquidity. [7] Although we continue to recognise the risks, we note that there are already four strict classification criteria that function as mitigation, and that the current version of SCO 60 would require banks to fully document the information used in determining compliance with such classification conditions and to make such documentation available to supervisory authorities on request. The exclusion of permissionless public networks may impact on the wider development of liquid tokenisation markets not least due to the potential lack of interoperability between private blockchains.

It should also be stressed that the current exposure to risks in this area by banks would and will be proportionate to the availability of the appropriate mitigation and risk management tools (technological, legal, or compliance). Over time, technological advancements and evolution of

---

[6] While not specifically related to this consultation, we would request that the BCBS kindly publish – perhaps in summary or redacted form – its analysis regarding such risks and why it believes they cannot be mitigated. With this information, the industry might be in a better position to suggest or develop solutions to the BCBS's concerns.

[7] https://www.icmagroup.org/assets/Joint-TA-response-to-BCBS-2nd-consultation-crypto-assets-30092022.pdf, at page 51- 53.

risk management capabilities will allow an increase in the engagement by retaining the same level of residual risk. The principle should be that, where risks can be managed, the use of public permissionless blockchains to develop tokenised assets should be allowed in order to improve efficiency.

By way of example, in our view, the risks of using a permissionless blockchain as a base layer for the creation of (regulated) tokenised traditional assets can be effectively controlled. In specific cases, the tokenisation agent may (for the entire lifetime of the token) remain 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.

As a more general comment, we are of the view that the BCBS's standards at SCO 60 are at odds with two cornerstone principles of prudential regulation: technological neutrality (because banks' exposures to cryptoassets using private blockchains are afforded a radically different treatment to exposures to cryptoassets using public blockchains) and the notion of "same asset, same risk" (and same prudential treatment), for much the same reason.

Precedents for permissionless networks; no binary distinction

Permissionless technologies are long-standing, familiar and well tested in one guise or another. Consider the internet and email. Internet and email are both permissionless (*i.e.*, open) networks that were designed to be maximally resilient in times of extreme duress. The resulting packet switched architecture led to these global open networks being built around simple technical protocols (TCP/IP, HTTP and SMTP), where anyone can read the protocol specification and build the required software (*i.e.*, a web server or an email server) to connect to either of these networks in a completely permissionless manner. It is this openness and permissionlessness that has accelerated the digital economy of the entire world for the past 30 years. The internet and email are single global networks of information built to common technical standards where massive numbers of different applications and websites run side-by-side from all over the world simultaneously. But even though the internet and email are permissionless *at the network layer*, there are many forms of permissioning that have been implemented *at the application layer*. Simple examples are Gmail (username, password), AWS (username, password, 2FA, subscription fee), online banking (KYC, username, password, 2FA, etc.) and other services, all of which run over the public internet with tight permissioning and encryption. In other words, very sophisticated permissioning and other forms of access control can be built on top of an underlying permissionless network. And in terms of regulation, both the internet and email are unregulated at the network layer as those technical standards are determined by the open-source community of engineers, but regulations can most certainly apply at the application layer.

Within the context of public blockchains, the concepts are closely analogous. The network layer is permissionless where anyone can download the protocol specification and build software to connect to the network. But the application layer can be as tightly permissioned as required and be appropriately regulated. Open applications can readily be built on public blockchains and completely closed institutional-facing applications that are only available to KYC'd participants can also be built on the same public blockchains thereby realising the same benefits from having a single global network as with the internet and email.

In technical terms, the design of suitable permissioning for the various users and administrators of applications is called Role-Based Access Control ("RBAC") and has been well understood for many years and has allowed the panoply of applications available via the internet to flourish with high degrees of confidence and security.[8] General considerations of who has read access, write access, code deployment and update rights are all covered by RBAC policies. Precisely the same concepts that apply to permissioning on the internet also apply to public blockchains with some nuances around implementation.

An example would be the cross-border transaction tested as part of MAS-sponsored Project Guardian, where three participating banks (UBS, SBI, DBS) performed a repurchase agreement of a debt instruments paid with a Japanese-issued stablecoin.[9] The whitelisting mechanism and asset-level governance input in the smart contract permitted to fully control the participants in the transaction, while retaining the efficiency of a public network.

In addition to RBAC for permissioning and security, the other key failsafe is disaster recovery, which in most firms is covered via an appropriate Business Continuity Plan ("BCP") and can be specifically included in certain regulations. A BCP, of course, involves having various redundant backups of data and applications in secure locations in case of natural disasters, hacks, power outages, wars or other unpredictable random events. In the case of blockchains specifically, the BCP is straightforward in that all nodes connected to the network generally store the complete history of the relevant data and running redundant nodes as backups is trivial as part of an organisation's overall BCP and disaster recovery plan.

It is also important to recognise that the question of permissioned or permissionless is not binary and that there are many options between the extremes. In particular, public blockchain architecture is tending towards having multiple layers (*e.g.*, layer 1, layer 2, layer 3, etc.) with the different layers having various characteristics driven by different business requirements. These different layers can all follow common technical specifications that lead to a high degree of interoperability. For example, it is perfectly possible to imagine a "layer 2" that has been built specifically for the financial industry with various forms of permissioning that is anchored to a public "layer 1" blockchain. The best analogy to think of is how many companies today have internal websites and applications that follow the general standards of the internet and use the public internet to communicate with other websites and applications.

An example of a permissioned bond on a permissionless network is the EIB's April 2021 digital bond issuance[10] which runs on public Ethereum DLT network. While the network was permissionless, the application for the issuance was tightly permissioned. This meant that all tokens had whitelisting in place to restrict holders to eligible counterparties and investors. Furthermore, smart contracts were put in place that conducted KYC/AML/CFT and sanctions

---

[8] Role-Based Access Control ("RBAC") restricts network access based on a person's role within an organisation and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network. Effectively employees' or users' access rights can be set so that they are only allowed to access the information necessary to effectively perform their functions. Access can be based on several factors, such as authority, responsibility, and job competency. In addition, access to computer resources can be limited to specific tasks such as the ability to view, create, or modify a file.

[9] https://www.mas.gov.sg/schemes-and-initiatives/project-guardian.

[10] *EIB issues its first ever digital bond on a public blockchain*, European Investment Bank (Apr. 28, 2021), https://www.eib.org/en/press/all/2021-141-european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain.

checks to verify counterparty identities before the relevant transaction could take place. A monitoring system was also put in place outside of a distributed ledger, to track any potential operational risk issues.

The upshot is that the concept of a permissionless system is neither as unfamiliar nor as untested as it may seem, and the associated risks are not as unmanageable as the BCBS might conceive. Nor is the division between permissioned and permissionless technologies and cryptoassets quite so absolute as they may seem.[11]

Other considerations voiced by regulators

Regulators have expressed concerns that permissionless blockchains may facilitate the unknowing payment of gas fees to undesirable parties. This is, of course, a legitimate concern, but we do not consider it to be an unsolvable problem and it should not preclude the use of permissionless blockchains altogether; for example, the trend towards multiple layers (discussed in the previous paragraph above) may prove the key – potentially, a second layer above the public layer could be designed to track the payment of gas fees (although other technical solutions may also be found).

We acknowledge that randomly allocated transaction fees may create uncertainty as to the extent that there is a contractual arrangement between users who may not know with whom they are interacting and that this might give pause from a wider compliance perspective in respect of users' ability to meet AML and/or sanctions requirements. There are, however, several ways to mitigate this problem:

1) Contract with a large, known operator of validators (*e.g.*, Coinbase, Blockdaemon) to process a financial institution's transactions via the operator's validator network.
2) Utilise a "layer 2" sub network that uses a set of KYC'd validators. This approach has many of the characteristics of a private/permissioned or public/permissioned network while using the underling "layer 1" permissionless network as a kind of ultimate BCP.
3) In the case of Ethereum specifically, the transaction fees are calculated according to the EIP 1559 specification.[12] The transaction fee is made up of two components: the "base fee" which is burnt (or destroyed) during a transaction and the "priority fee" that can easily be set to zero. A zero-priority fee approach guarantees that none of the user's transaction fees goes to a specific validator thereby avoiding the problem entirely.

Conclusions and recommendations

We respectfully disagree with the BCBS's conclusion. We acknowledge that there are risks with the use of permissionless blockchains but are of the firm view that industry has all necessary expertise and robust compliance frameworks to fully identify, manage and mitigate these risks. Hence, we recommend permitting banks to conduct a Group 1 assessment for

---

[11] See also *Types of Blockchains Explained- Public Vs. Private Vs. Consortium*, Blockchain Council (Nov. 14, 2023), https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/.

[12] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md.

permissionless blockchains. As long as banks can satisfy themselves that relevant risks have been addressed, the use of permissionless blockchains should remain possible. We request the BCBS to continue engaging with the industry and share its assessment of permissionless blockchains.

The BCBS's stance is contrary to the prudential principles of technological neutrality and "same asset, same risk" and, as mentioned above, may impact on the wider development of liquid tokenisation markets not least due to the potential lack of interoperability between private blockchains. Registered, KYC'd cryptoassets under full AML control have been recorded and issued on permissionless networks since at least 2019 (*e.g.*, Santander, Société Générale digital bonds and others), and have been recorded on banks' balances sheets as traditional securities using standard BCP and technical risk mitigation methods in case of any technical issues. We consider it inappropriate that the BCBS should disregard the possibility of recognising these assets as Group 1 cryptoassets. By sharing its present concerns and understandings of the risks, the BCBS could put the industry in a better position to help the BCBS understand, manage and eventually regulate for such products.

Furthermore, there are views amongst some of our members that a network's level of permissioning should not be included as a classification condition at all; rather the classification conditions should focus on the asset and the risk it presents to a bank as holder. On that logic, the level and nature of permissioning may be relevant to the analysis supporting a bank's conclusion that a cryptoasset satisfies such conditions, but not a determining factor in and of itself.

2. <u>Classification Condition 2 and Settlement Finality (General)</u>

Background

SCO 60.14 outlines classification condition 2, which a cryptoasset must satisfy if it is to be classified as a Group 1 cryptoassets. There are two limbs to classification condition 2: a legal enforceability limb, and a settlement finality limb. Our comment relates to the settlement finality limb only.

The BCBS proposes, at SCO 60.14, that to satisfy classification condition 2, the legal system pertaining to a cryptoasset must ensure settlement finality for both primary and secondary markets.

The challenge

From a technological perspective, settlement finality applies to tokenised assets, stablecoins and, cryptoassets generally. Legal frameworks are being developed globally to help address settlement finality and private or commercial law considerations relating to tokenised securities and payments settlement in both primary and secondary markets. For example, in the US and other jurisdictions such as the UK, legal changes are in progress or under consideration to enable clarity around the private or commercial law aspects of transferring cryptoassets (*e.g.*, via the 2022 amendments to state UCC laws or through UK Law Commission recommendations). The UK's FCA/Bank of England's proposals (which do envisage the use of stablecoins in payment systems) apply to systemically important stablecoins. Therefore, while such frameworks are being developed for this condition to operate effectively, we make the following proposal.

Our proposal

In the longer term, demonstrable settlement finality, in both the primary and secondary markets can become a classification condition, but in the meantime any such requirement should be non-prescriptive.

We would recommend the settlement finality limb of classification condition 2 under SCO 60.14 should be considered satisfied where the following two conditions are met:

> 1) the processes as to how and when settlement of the transaction is achieved (whether pursuant to a bilateral contract or pursuant to the rules or technical processes or conventions of the relevant market, exchange or other venue) is reasonably clear to the bank; and
>
> 2) the bank has conducted a legal review of the settlement process and has concluded to its satisfaction that settlement finality is achieved or is likely to be achieved in practice.

For the purposes of conditions 1) and 2) above, settlement finality should be construed by reference to the rights and obligations of the transferor and transferee (in the case of a secondary transaction/transfer) or issuer and subscriber (in the case of a primary transaction/issuance) as between themselves only, and need not consider the rights and obligations of any third party, such as a platform operator, creditor or insolvency officer of either party.

Permitting banks to conduct the settlement finality assessment would be consistent with prior BCBS guidance. In prior guidance on the subject of settlement finality for foreign exchanges, the BCBS noted that "[a] bank should obtain legal advice that addresses settlement finality with respect to its settlement payments and deliveries. The legal advice should identify material legal uncertainties regarding settlement finality so that the bank may assess when key financial risks are transferred" and that "[a] bank needs to know with a high degree of certainty when settlement finality occurs as a matter of law."[13] This is similar (but not identical) to the guidance in respect of FMIs at paragraph 3.8.4 of the CPMI/IOSCO *Principles for financial market infrastructures*.[14]

More generally, our proposed approach is in line with the position recognised by, among others, the BIS Innovation Hub, that the use of DLT can be fully consistent with existing BIS guidance relating to legal certainty and finality of settlement.[15]

---

[13] https://www.bis.org/publ/bcbs241.pdf para 3.6.5.

[14] https://www.bis.org/cpmi/publ/d101a.pdf

[15] See, for example, BIS CPMI Consultative Report Facilitating increased adoption of payment versus payment (which contains repeated examples of how DLT can reduce settlement risk by means of enabling payment-versus-payment arrangements) as well as 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) and Project Dunbar (which utilised DLT to align settlements of different currencies on a cross-border basis).

3. Eligibility of Group 1b Cryptoassets as Collateral

The BCBS has proposed additional requirements that stablecoin reserves need to meet in order for the stablecoin to be included in Group 1b; many of them will ensure the reserves are highly liquid, have high credit quality, and have low volatility.

However, the current prudential framework holds that Group 1b cryptoassets are also not eligible as collateral in themselves for purposes of credit risk mitigation (SCO 60.39). The consultation would not alter these restrictions, even if Group 1b cryptoassets meet the additional requirements that it introduces.

We propose that stablecoins that meet the new additional requirements as well as the existing classification conditions for Group 1b should be eligible as collateral (funded credit protection) for the purposes of CRE22.

4. General Comments in respect of Group 1b Eligibility

As a general comment, the classification conditions that the BCBS proposes (in terms of maturity, credit quality, bankruptcy remoteness etc.) may be more stringent that policy proposals for stablecoin frameworks published in certain jurisdictions with sophisticated financial markets including the UK, EU, Singapore, Dubai and Hong Kong.

For example, the framework for the regulation of e-money tokens under the EU's markets in crypto-assets regulation 2023/1114 ("MiCA"), as well as the framework proposed in the UK for stablecoins generally are less stringent than the BCBS's proposals. This is also the case in equivalent regimes found in Hong Kong, Dubai and Singapore. There are some similar features when considering the UK regime proposed by the Bank of England for systemic stablecoins.

This results in odd outcomes, for example, in the UK and EU today banks are allowed to issue e-money without having to meet the combined maturity, credit quality and bankruptcy remoteness requirements proposed in the amended classicisation conditions. The classification conditions would effectively act as a barrier, preventing banks from issuing e-money in token form on the same terms. More generally, existing widely-traded stablecoins operate differently to how the BCBS envisages them to.

In other words, existing regulations recently enacted or being proposed in UK, EU and other jurisdictions may not comply with the BCBS proposed classification conditions. The goal of the BCBS should be to create a prudential framework that aligns and complements existing regulatory outcomes imposing minimum requirements that enhance financial prudence, safety and soundness. There are potential unintended consequences if the BCBS's amendments are not outcome based so that banks can comply with applicable regulatory regimes, as well as investor and client expectations across geographies. Similarly, the BCBS's amendments should not have the effect of preventing banks from exercising rights that have already been enshrined in existing regulatory and legal framework.

5. Insolvency Remoteness of Reserve Assets Custodians/Deposit-takers

Background

The BCBS's proposed amendments at SCO 60.12(2)(b)(iv)[16] and SCO 60.12(2)(c)(iii)[17] would appear to not allow a bank serving as custodian for reserve assets to hold on deposit any of the stablecoin's cash, whether cash reserves or frictional cash that results from the provision of day-to-day safekeeping and asset administration services. This is a major problem that would essentially prohibit banks from acting as custodians for stablecoin assets.

While segregation away from the custodian's insolvency risk can be achieved and should be the objective for securities or other non-cash assets, we believe there should be an exemption for cash (reserve assets) held with financial institutions. If cash is deposited with a bank, the deposit is, ordinarily, a liability of the bank to the unsecured creditor (depositor). While non-cash assets should be insolvency remote, cash should be treated as a liability to the deposit-holders in line with its existing treatment in other contexts. Cash segregation would introduce undue operational complexities, prevent financial institutions from using that cash (thus generating interest and income from it) for general purposes and disincentivise the engagement of established banks as custodians.

In this regard, we also note the recent U.S. Office of the Comptroller of the Currency ("OCC") and Federal Reserve letters sent to the Securities and Exchange Commission ("SEC") regarding the SEC's safeguarding of client assets proposed rule. In response to the SEC's request for custodians to make cash bankruptcy remote, the OCC and Federal Reserve sent robustly worded letters arguing that this would overturn centuries of custody practice.[18]

Our suggestions

We would suggest that the BCBS removes the proposed requirements more generally, or otherwise amends the proposed texts so either to permit reserve assets to be placed or deposited with (1) any prudentially regulated bank or (2) other entities which are remote from the insolvency of stablecoin *issuers* (rather entities involved in the operation/management or custodying thereof).

If the BCBS's proposed requirements are removed, we would support the implementation of conditions to this exemption for cash, such as a requirement for adequate disclosure of the risks involves, or the appointment of qualified (adequately capitalised and supervised) financial institutions.

---

[16] The "reserve assets are placed in structures that are bankruptcy remote from any party that issues, manages or involved in the stablecoin operation, or custodies the reserve assets".

[17] Eligible reserve assets include "deposits at high credit quality banks with safeguards, such as: a concentration limit applied at group level that include entities with close links; bankruptcy remoteness of the deposits from any party that issues, manages or is involved in the stablecoin operation; and the banks apply the Basel Framework (including the liquidity coverage ratio)."

[18] Letters available here (https://www.politico.com/f/?id=0000018d-671a-d4fe-addf-6f5f9fa20000, Federal Reserve) and here (https://www.politico.com/f/?id=0000018d-671b-da7a-abcd-67ffa82c0000, OCC).

6. **SCO 60.12 Reserve Asset Quality and HQLA**

We propose that it is clearly stated that Level 1 HQLA will always satisfy the asset quality criteria for reserve assets for Group 1 cryptoassets.

In other words, so long as a bank is satisfied that the relevant reserve assets meet the requirements for Level 1 HQLA (for the purposes of LCR 30), it may be satisfied that the assets satisfy the asset quality criteria for reserve assets at SCO 60.12, without further enquiry.

7. **SCO 60.12(2) Reserve Assets Relationship between Reserve Assets and HQLA**

For cryptoassets that are pegged to one or more currencies, the reserve assets must comprise assets that are capable of being liquidated rapidly with minimal adverse price effect. These include Level 1 HQLA as stipulated in SCO 30.41. However, we suggest that the category of eligible reserve assets be broadened to include reverse repurchase agreements backed by other eligible reserve assets. This should be conditional on Group 1b cryptoasset issuers putting in place appropriate capital buffers and risk mitigants to ensure that Group 1b assets remain at least fully capitalised and are redeemable at par in a timely manner.

Repurchase agreements pose different types of risks than HQLA, and those risk should be accounted for in a Group 1b cryptoassets issuer's mandated capital buffers. However, those risks are not necessarily materially greater, but are different from what HQLA presents, and those risks may still be easily mitigated. Limiting available reserve assets only to a subset of HQLA reserve assets may also have the unintended effect of concentrating risks in issuers that could, over time, cause an accumulation in the stablecoin sector.

We therefore propose that the BCBS explicitly include reverse repurchase agreements backed by eligible reserve assets in SCO 60.12(2)(c). This inclusion would allow issuers to reduce market risk by shifting assets to reverse repurchase agreements. We note that in traditional markets, the use of reverse repurchase agreements in this way has at least one precedent – for example, in the context of periods of sovereign debt concerns relating to U.S. debt limits when cash funds shifted assets away from Treasury markets to reverse repurchase agreements during the summer 2023 U.S. debt ceiling negotiations.

8. **Monitoring of Reserve Assets**

We note that the BCBS proposes to introduce certain risk management and due diligence requirements that aim to ensure banks adequately assess and monitor the risks of reserve assets. The BCBS should make clearer whether it is effectively asking banks to do a full look-through for the underlying reserves for such purposes.

SCO 60.20(3) also requires routine testing of the stabilisation mechanism for Group 1b cryptoassets. We note that effective stabilisation mechanisms for asset-referenced cryptoassets depend solely on the ability for Group 1b assets to maintain full redemption at par with the underlying reference assets. Secondary market price does not have any bearing or influence over the issuers ability to redeem holder funds, even in times of stress or heavy redemption. Group 2 cryptoassets, on the other hand, do rely on secondary markets for stability, a distinction that should be noted.

As a result, for Group 1b assets, the requirement in SCO60.12(4)(d) on risk management framework – whether explicitly or de facto a full look-through for the underlying reserves –

effectively captures the risks to the reserve asset and efficacy of the stabilisation mechanism. As such, SCO 60.20(3) and SCO 60.12(4)(d) should be interchangeable and not impose additional duplicative due diligence requirements for banks.

9. SCO 60.52: Add-on for Infrastructure Risk for Group 1 Cryptoassets

To account for the fact that DLT is a relatively new technology, the BCBS proposes that authorities must have the power to apply an infrastructure risk add-on to the capital requirement for exposures to Group 1 cryptoassets. This risk add-on will initially be set at zero but can be increased by authorities based on any observed weaknesses in the infrastructure used by such cryptoassets.

We believe that the infrastructure risk add-on is unnecessary given that it seeks to address risks that are already addressed by the existing prudential framework and risk management systems such as operational risk and third-party risk management frameworks, supervisory tools and controls. The proposal would also appear to be at odds with a technology risk-neutral approach because it would penalise this particular technology above others.

Overall, we would recommend removing the infrastructure risk add-on in its entirety. However, if the BCBS is insistent on its inclusion, we would recommend a consistent approach across all jurisdictions where the use of the infrastructure risk add-on is a last resort.

In this scenario, we would support the approach recently proposed by the Hong Kong Monetary Authority ("HKMA"). The HKMA proposal begins with a risk add-on of zero. To the extent that additional risks in the underlying technology are identified, the authorities would then look at each institution on an individual basis and assess whether it should add an additional risk weighting based on the robustness of its internal infrastructure. Only then, if the institution's infrastructure is insufficient, should the authority resort to imposing an infrastructure risk add-on.

10. SCO 60.55(1): QCCPs

The BCBS has proposed certain amendments to the Group 2a hedging recognition criteria in SCO 60.55(1) subparagraphs (a) and (d). While we are in largely in agreement with the proposed changes, we would recommend clarifying the phrasing of subparagraph (a) to more clearly reflect the reality that ETFs/ETNs are traded on regulated exchanges but rarely cleared through QCCPs. We propose the following alternative wording:

"(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 solely references the cryptoasset and that is traded on a regulated exchange and, in the case of a derivative, is cleared through a QCCP."

11. SCO 60.74: Delta Risk Factor Calculation

To compute the market risk for Group 2a cryptoassets, the BCBS consultation contemplates using delta sensitivities based on a risk factor structure that considers two dimensions: (1) the exchange; and (2) the time to maturity, at certain prescribed tenors.

We recommend simplifying the dimensions of the delta risk factor in certain cases by proposing the following clarification in a new footnote, [X] after footnote [9] at SCO 60.74:

[X] "*In the case of an ETF or ETN that is backed by cryptoassets, and derivatives referencing the same ETF or ETN, the spot price of the ETF or ETN may be used as the delta risk factor provided any positions treated as such are placed into a separate bucket for each risk factor.*"

This proposal is aligned with the risk arising from such exposures because the exchange and maturity dimensions are not relevant for delta risk when all of the exposures in a bucket reference an identical listed instrument.

12. Group 2 Exposure Limit (SCO 60.116 ff)

Exposures with no direct price risk to Group 2 assets

We would suggest that the BCBS clarifies that only direct exposures to Group 2 assets are included within the Group 2 exposure measure, for the purposes of the Group 2 Exposure Limit (and not exposures where there is no direct price risk to Group 2 assets). For further details, we refer the BCBS to section I.C. (page 20) of our response to the Second Consultation.[19]

Client-cleared exposures

We suggest that BCBS not penalise client-clearing by including client-cleared exposures, where the bank acts as clearing member to clear trades for clients, in the Group 2 cryptoassets exposure limit. If these exposures are included, the framework would undermine consensus reforms and discourage banks from facilitating the central clearing of cryptoassets 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.

For centrally-cleared derivatives, the risk posed is already capitalised for the banks for clearing of derivatives with crypto assets in form of SA-CCR to cover the client counterparty credit risk, in addition to the mitigating benefits of central clearing. Introducing punitive requirements on banks centrally clearing crypto derivatives for clients will continue to push activity to the non-bank space, who are already the most active providers in this asset class.

Group 1 assets and the Group 2 exposure limit

We suggest 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.

Group 2b cryptoassets and the Group 2 exposure limit

We suggest that Group 2b cryptoassets should be excluded from the scope of the Group 2 exposure limit. If not, we would suggest that Group 2b assets should not be considered for the purposes of the additional RWA requirements imposed by SCO 60.118 in the case of breaches of the 1% limit.

This is 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.

---

[19] https://www.bis.org/bcbs/publ/comments/d533/jta.pdf.

Formula at SCO 60.118

Why is the denominator in the **formula at SCO 60.118** expressed as "2% of Tier 1 capital – 1% of Tier 1 capital", rather than "1% of Tier 1 capital"?

Furthermore, a main issue still with the formula at SCO 60.118 is that Group 2a cryptoassets are measured gross for the threshold test. So once a bank runs up against the limit, putting on effective hedges of Group 2a cryptoassets that would otherwise be recognised as a benefit in RWA calculations results in an increase in RWA; this would, inappropriately, disincentivise hedging. For further details, we refer the BCBS to our proposals at sections I.A.1. and I.A.2. (pages 12-17) of our response to the Second Consultation.[20]

13. **Other Suggested Amendments:**

Group 2b

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 SCO 60.88. 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 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.

SCO 60.12(2)(a) "The reserve assets must be comprised of assets with minimal market and credit risk *where*:"

"Where" is ambiguous; are the following limbs (i) and (ii) *indicators* of minimal market and credit risk or must the reserve assets comprise assets with minimal market and credit risk *if* limbs (i) and (ii) are satisfied? Presumably the former, in which case replace "*where*" with *". The reserve assets shall be considered to have a sufficiently minimal market and credit risk where all of the requirements at subparagraphs [(i) and (ii)] are satisfied:"*

SCO 60.12(2)(b) "The reserve assets must be capable of being liquidated rapidly with minimal adverse price effect where:"

As for SCO 60.12(2)(a), "where" is ambiguous. Replace "*where*" with ". *The reserve assets shall be considered be sufficiently capable of being liquidated rapidly with minimal adverse price effect where all of the requirements at subparagraphs (i) to (iv) are satisfied:*"

SCO 60.12(2)(c) "Eligible types of reserve assets include, but not limited to"

Add the word "*are*" between "*but*" and "*not*".

[20] https://www.bis.org/bcbs/publ/comments/d533/jta.pdf.

It is unclear whether SCO 60.12(2)(c) should be construed to mean that the assets listed at limbs (i) to (iii) should be deemed automatically to satisfy the requirements at SCO 60.12(2)(a) and SCO 60.12(2)(b). If so, specify so. If not, what is the purpose in including the list at SCO 60.12(2)(c) at all?

Moreover, SCO 60.12(2)(c) should exist as a standalone rule (SCO 60.12(3)) (specifying that this provision only applies to reserve assets for cryptoassets pegged to currencies) with the following renumbered, and not as a sub-paragraph of SCO 6012(2). This is because grammatically, current SCO 60.12(2)(c) does not follow on from/integrate into "the following requirements must be met" (end of SCO 60.12(2), second line).

SCO 60.12(2)(c)(i) "central bank reserves to the extent that the stablecoin issuer is eligible and the central bank policies allow them to be drawn down in times of stress;"

The meaning of "eligible" is unclear: "eligible" for what? What if the issuer is not eligible? Does that mean that the stablecoins cannot fall within the category at (c)(i), or that a different test/standard applies (in which case what?). Is the reference to "eligible" necessary at all?

SCO 60.12(3) "That means, the reserve assets should only include the reference assets, except for a de minimis portion of the reserve assets may be held in cash or bank deposit, provided that the holding is necessary for the operation of the cryptoasset arrangement."

Replace "*reasonably necessary for the operation*" with "*reasonably considered necessary or advantageous for the efficient and/or prudent operation*"; otherwise "necessary" appears an impossibly high or difficult-to-prove standard.

Same comment at (already existing) SCO 60.12(2)(d).

SCO 60.12 FN[5] "… so that the cryptoassets remains redeemable at all times for the peg value, even on stress period and volatile markets."

Replace "even on stress period and volatile markets" with ", including during stressed periods and periods of volatile markets."

SCO 60.12 FN[7] "…as well as securities representing claims on or guaranteed by sovereign or central bank …"

Insert "*a*" before "sovereign."

SCO 60.12 FN[8] "**…collateral used in credit support annex agreements should be encumbered and be subtracted…**"

Delete "*be encumbered and*" – the phrase is confusing/misleading (presumably it is meant to read "should be deemed to be encumbered for certain unspecified purposes", although it reads like a requirement that collateral can only be posted where the relevant assets are encumbered).

SCO 60.20(3): "<u>For cryptoassets that are classified as Group 1b, a bank must perform due diligence to ensure that they have an adequate understanding, at acquisition and thereafter on a regular basis (at least semi-annually), of the stabilisation mechanism of the cryptoasset and of its effectiveness.</u>"

We suggest that this diligence should take place semi-annually. Given that category 1b cryptoassets should be stable, the likelihood is that they will not require monitoring as frequently.

14. <u>Observations relating to the Second Consultation (30 June 2022)</u>

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

- Regarding SCO 60.55,[21] "major fiat currency" is undefined. We recommend the most liquid currencies specified in MAR 33.12(3) (and associated footnotes) meet this definition, specifically the 10-day liquidity horizon currencies for "interest rate: specified currencies and Foreign Exchange (FX) rate: specified currency pairs."

- Regarding SCO 60.83(2),[22] 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 SCO 60.94[23] and 60.104, the reference cited should begin at CRE 22.40 not CRE 22.45.

- Regarding SCO 60.104, as referenced in the second consultation,[24] beginning 1 January 2023 haircuts applied to other equities that are traded on a recognised exchange will be 30% pursuant to CRE 22.49. The Associations seek clarification whether the Committee intends to apply a 25% haircut or the 30% haircut (if this proposal is still live).

---

[21] The second consultation numbered this SCO 60.60. This is SCO 60.55 in the current framework text.

[22] The second consultation numbered this SCO 60.88(2). This is SCO 60.83(2) in the current framework text.

[23] The second consultation numbered this SCO 60.98. This is SCO 60.94 in the current framework text. The second consultation made the same reference to CRE 22.45 in SCO 60.104, which is not included in the present framework. That reference should also read CRE 22.40.

[24] Although, this does not appear in the current framework and so may have been dismissed.

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

Jacqueline Mesa
Senior Vice President, Global Policy
Futures Industry Association

Richard Gray
Director, Regulatory Affairs
Institute of International Finance

Panayiotis Dionysopoulos
Head of Capital
International Swaps and Derivatives Association

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

Appendix 1

DLT Definitions

(i) "**DLT Network**": a database construct that brings together existing approaches around distributed computing networks and data encryption. Separate participants in different locations, known as nodes, each maintain a copy of a common ledger. The verification of transactions requires the consensus of participating nodes accomplished through the applicable governance mechanism of the underlying infrastructure. Verified transactions form a record that is protected by cryptography so historical transactions cannot be altered, known as immutability. There are various configurations of DLT Networks, each with varying levels of decentralisation, privacy, governance, and control – thereby driving different risk and legal considerations.

(ii) "**Private-permissioned**": Private-permissioned networks are characterised by a centralised authority that can control access to the network (private) and actors that can perform actions on the network (permissioned). Private networks are typically governed by a formal rulebook and enable a comparable model to existing infrastructure in use by capital markets today, with control over all network layers, and their defining characteristics.

(iii) "**Public-permissioned**"**:** Public-permissioned networks are characterised by allowing public access to the network and a centralised authority to control actors that can perform actions on the network (permissioned). Though public-permissioned distributed networks mark a step away from the tight central control of private networks, they also operate as closed networks with centralisation retained over key network attributes.

(iv) "**Public-permissionless**": Public-permissionless networks allow unrestricted access to the network and to perform actions on the network by default. These publicly available distributed ledger networks have defining characteristics, such as decentralisation of access and control, pseudonymity of participants, and governance of the network by majority consensus that may require validation of transfers with unknown third parties, and large-scale user bases, that are significantly different to private-permissioned and public-permissioned networks. Anyone can access and connect to the network, often anonymously and in a censorship-proof way. Where applicable, a governing body of the network may blacklist identities that broke network rules, but enforcement of blacklists is conducted by network participants.

Appendix 2

Overview of the Associations

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 Singapore, 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 **Futures Industry Association** ("FIA") 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 **Institute of International Finance** ("IIF") is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. 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, professional services firms, exchanges, 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 1,000 member institutions from 77 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.

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.