A response by the Federation of Latin American Banks – FELABAN to the Basel Committee on Banking Supervision's consultative document on:

Prudential treatment of cryptoassets exposures (second consultation)

Dear Basel Committee on Banking Supervision members:

The Federation of Latin American Banks - FELABAN acknowledges the Basel Committee on Banking Supervision (hereinafter *the Committee)* for the opportunity to discuss the proposals included in the consultative document "*Prudential treatment of cryptoassets exposures – Second consultation*", published on June 2022.

Even though the regulated financial sector (both worldwide and across Latin America) has shown interest both on cryptoassets and their underlying technology, its adoption and use still lag behind. Particularly, an absence of a regulatory framework is a deterrent that has prevented financial intermediaries from getting into this market and this ecosystem – beyond regulatory sandboxes and supervisor-controlled tests. Thus, a coordinated, international regulatory framework in this regard is welcome.

FELABAN analyzed and discussed its content with the Banking Associations we represent, as well as with our Latin American Committee on Risks, and the outcome is this document, which highlights our comments and views on this initiative. We believe it will be a useful point of reference when considering a prudential treatment for cryptoasset exposures, from the point of view of the Latin American banking sector.

***

Overall comments

In this regard, we believe that banks' involvement in the crypto-environment is essential to ensure a secure development of the market, and is beneficial both for the general public and regulators. This is because, while cryptoassets might be new, the potential harms to the financial sector that they might bring are not, and banks have a longstanding experience in dealing with different types of risks. In fact, banks are already subject to comprehensive and robust risk management, supervision and examination processes, and have long standing expertise in complying with consumer protection and anti-money laundering laws and regulations.

1. We consider the proposed framework still includes restrictive deterrents in terms of capital requirements that may ultimately discourage the participation of financial market intermediaries, at the expense of the current framework's objective of fostering a global, coordinated standard across jurisdictions aiming to achieve greater transparency, less fragmentation and better risk management approach, as well as developing sound, efficient and competitive markets. This is key, keeping in mind the evolution and development of the cryptoasset market and the participation of unregulated players who may never be subject to any of the proposed regulatory treatments. We briefly address some of them below:
    a. We consider that some of Group 1 classification critera are restrictive and do not recognize the decentralized character of the underlying technology, assigning financial entities regulatory responsibilities out of their control. It is unlikely such requirements can be fully complied in practice, which may lead to increments of assets classified under Group 2, thus limiting banks' participation on cryptoasset markets due to higher capital requirements. Instead, we suggest to ensure that classification criteria are able to strengthen mechanisms, structures and measures allowing banks to react should any risk outside its control ensues.
    b. The document states that supervisors are responsible for approving banks criteria on if and whether a cryptoasset meets Group 1 criteria. We consider this is against the fundamentals of a risk-based supervision such as the one prevailing in most Latin American countries and, therefore, financial

intermediaries should be granted the capacity of approving them – of course, with the supervisor's support and guidance.

c. The Committee proposes to establish a risk add-on in order to account for unforeseen risks (related to the implementation of a new technology) derived from cryptoasset activities. This add-on may over-estimate the real exposure, ignore banks' risk management procedures and, indirectly, claiming that there are no differences in terms of risk management experience or maturity across entities. We suggest this add-ons should not be established *a priori* – instead, they should reflect the needs and reality of a given jurisdiction in order not to unduly penalize banks.

d. We do not deem as appropriate to have a single weight (1250%) for all cryptoassets classified into Group 2, given that the nature of bank exposures may vary depending on their risk profile and risk appetite. By establishing a single category, there is no possibility of acknowledging the associated capital requirements, for example, in terms of liquidity (market depth), market risk (hedging), collateralization (especially high-quality collaterals) or legal rights (compensation agreements).

2. Volatility: it is important to take into account their volatility, given it is an intrinsic attribute of these assets. Banks have the responsibility of properly identify their clients according to their risk profile and investment time horizon.
3. Basis risk test. We consider the proposed threshold is restrictive, and may lead to straight Group 2 classifications. For example, quarterly volatility estimates for Tether/USD and USDC/USD on 2020 vary between 12 and 18 basis points. Therefore, we suggest the Committee to consider broadening the threshold (at least 20 basis points) or, alternatively, to consider some sort of graduality (i.e., additional requirements in case the base threshold is exceeded).
4. Credit risk: The proposed treatment to collateralized and non-collateralized cryptoassets in terms of capital requirements is not fully clear. Specifically, there is not any differentiation that acknowledges the effect after credit risk mitigation, nor there are any differences in the risk weight that take into account the effect of collaterals, liquidity facilities or additional credit risk mitigation mechanisms.

5. Liquidity risk: the document proposes that Gorup1b and Group 2 cryptoassets cannot be considered as HQLA. We deem this criterion restrictive, as a cryptoassets that already complies with eligibility criteria defined by the Committee should not be excluded. Similarly, we suggest to enable Group 2 cryptoassets as level II HQLAs, for example, as long as liquidity coverage ratios are fulfilled.
6. We suggest to include more definitions and recommendations regarding the Travel Rule on the following aspects: prompt enforcement in the cryptoassets industry; references on private wallets (unhosted wallets); address the various transactional flows between centralized and private wallets; and mechanisms allowing market participants within the ecosystem to share information across them.
7. Address the jurisdiction risk specifically applied to the digital asset ecosystem, so that financial entities are able to perform and undertake controls (such as due diligence) when establishing business relationships with Virtual Asset Services Providers.
8. Provide more depth on the way financial entities should develop a proper risk framework, as well as the associated controls to be implemented, so that they can manage and mitigate the inherent risks related to cryptoassets.
9. Regarding the proposal of a 1250% risk weight for all Group 2 cryptoassets, rather than a capital deduction, the Committee and states that this would (in practice) ensure that banks are required to hold risk-based capital equal in value to their Group 2 cryptoasset exposures. However, we flag out that in practice, this capital treatment could be even more conservative/penalizing than the deduction. This is because many banking organizations are effectively subject to capital requirements in excess of the 8% minimum risk-based capital requirement (as a result of buffer requirements, Pillar 2 requirements and additional buffers held as a prudential management buffer). Therefore, the 1250% risk weight would in practice mean that banks need to hold risk-based capital in excess of the exposure to the cryptoasset.
    a. Example: for a bank managing a 12% total risk-based capital ratio, a 1250% risk weight would translate to a $150 total capital requirement for a $100 gross exposure to Group 2 cryptoassets.
10. Classification of Cryptoassets in a group other than Group 2b Cryptoassets: Entities should be allowed to classify Group 1 Cryptoassets following certain pre-defined criteria. Otherwise, the process could be too burdensome and there may be a problem

of coordination between supervisors. (We understand we should also include Group 2a under this point) (This point was made in the previous consultation).

11. Classification Conditions for Group 1 Cryptoassets seem very exhaustive. There is the risk they are not well understood by the industry, especially by medium-sized and small banks and financial intermediaries.
12. Regarding Redemption risk test, it is not clear how often banks would be expected to assess compliance with this test. 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 Committee should confirm, either through modifications to proposed SCO60.13(1) or through other guidance, that banks may comply with this requirement by analyzing a stablecoin issuer's public disclosures of the value of reserve assets backing the stablecoins and the aggregate peg value of the stablecoins, and individual banks should not expected to make their own assumptions in real time in order to continuously assess this requirement.
13. Regarding Basis risk test, we consider these "tests" are not against "cliff effects", but volatility (variance). They do not provide proof that the peg-to-market value difference will not collapse (cliff effect). Suppressing variability (which is not the same as suppressing risk) might have unintended consequences. Perhaps, initially, as the nature and risks of cryptoassets is not fully understood, it could be desirable to not have a "fully passed" category. Only after reaching certain maturity, a cryptoasset in group 1b should be able to "graduate" (i.e., move into) towards Group 1a.
14. *One area of the proposals on which the Committee would particularly welcome feedback is the treatment of cryptoassets that are based on permissionless blockchains*.
    a. At this moment in time, we do not envision alternative approaches that could be easier to implement.
    b. Cryptoassets that are based on permissionless blockchains should be eligible to be included in Group 1, subject to the existence of certain controls. We 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 protocols for the governance, tracking, and control of cryptoasset movement.

c. Permissioned apps built on Permissionless DLT networks should be eligible to be considered as a Group 1 Cryptoassets.

15. Regarding infrastructure risk add-on, it is not clear what risk regulators want to cover with the infrastructure add-on. It assumes that the DLT and the issuer (debtor) are the same thing, and they clearly are not. In our view, the risk to be covered would be the following: The DLT is the technology used to record the ownership of the Cryptoassets (just as it could be an Excel file or an email). If the DLT fails, it is as if somebody deleted an excel or an email. In case of failure of the DLT, it is necessary to safeguard the ownership of the assets. Therefore, the way to cover this risk should not be the infrastructure add-on but a sound Business Continuity Plan, which could be a clause stating what would happen in the case of a catastrophe. Such clause could include an external data recording system (e.g., back-up system stored in the cloud). An example of this BCP can be found in the French (DLT Decree of Dec 24, 2018), German and Luxembourgish Laws. In the case of the French Law, there is a registrar, who acts on behalf of the issuer of the instrument. The register oversees this BCP to guard against the event of a DLT outage.
16. Similarly, it is not clear to us why Government or Central Bank backed tokenized assets should be excluded from this treatment if the add-on is about technology.
17. An infrastructure add-on would kill the development of the digital markets, investors will always prefer the cheaper instruments due to their lower capital requirements: in the case of bonds, investors will prefer to buy a traditional bond vs. a digital bond.
18. Regarding the recognition of hedging of certain Group 2 cryptoassets: in accordance with the principle of simplicity and to ensure a better reflection of the positions, a more direct approach is suggested, which shows a real net position.

    BCBS formula: RWA= RW x max [abs(long exposure),abs (short exposure)]

    Proposed: RWA= RW x max [abs((long exposure)- (short exposure))]
19. Regarding Operational risk clarifications, With regards to the banks' risk management and supervisory review process, we have made several comments in the next section.

As a general comment, the supervisory review process should rely on the currently existing structure, it should avoid setting up new structures. The standards should distinguish:

a. If we are in control of a DLT network, then we should be responsible for it.
b. If the DLT is external, we should have a contingency plan (BCP) for outages. We may be required to assess the risk of the DLT but not to be constantly monitoring it or be responsible for its failure.

20. Also, the standards should distinguish what requirements are critical and which ones are not. Finally, we are also including comments on operational risk: need to make some clarifications in the delineation vs. credit and market risk and also in the definitions.
21. Regarding liquidity rules, we suggest the Committee to consider the possibility of including Group 1b cryptoassets as eligible for HQLA, as the rule requires that these types of assets pass both the Redemption risk test and the Basis risk test. The latter is very much in line with what is required by the Liquidity Provisions in Mexico to classify level II liquid assets:
    a. Level IIA: Assets may be classified in this Group provided that, from January 3rd, 2005 to date, they have not presented an accumulated decrease in their market price greater than 10% during a period of thirty days.
    b. Level IIB: Assets may be classified in this Group, provided that, from January 3rd, 2005 to date, during a period of thirty days they have not presented an accumulated decrease in their market price greater than 20% during a period of 30 days.
22. Finally, regarding Group 2 exposure limits, we agree with the general principles of large exposures, and agree on the need to measure them properly, however the limit of 1% on Tier 1 capital seems extremely restrictive, especially considering the other existing limits for large exposures, so a limit aligned to the threshold of 5% of the capital base is suggested, such as the one applied in cases of individual concentration.
    a. The definition of the exposure amount lacks any recognition of hedging long and short positions, which means that banks would receive no credit for managing their exposures to Group 2 cryptoassets in a prudent manner and they have no control over the exposure amount in the event they exceed the exposure limit. By introducing a risk mitigant for an exposure based on the

proposed calculation the bank would further exceed the exposure limit. This is inconsistent with long-standing risk management and hedging practices.

b. The calibration of the limit especially as per the proposed 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 drive or keep those services and products away from the regulated banking sector. It is important to notice that banks manage exposures at lower levels to the regulatory exposure limits which translates to even lower capacity for the banks to make markets and meet their clients' demands.
c. The scope of exposures subject to the limit, which would otherwise double-count certain exposures already subject to the large exposure rules or include exposures that do not expose banks to market risk; and
d. The excessively punitive penalty for exceeding the limit and associated "cliff effect".

Specific comments

- 60.2 → It would not be appropriate for assets that rely on DLT for recordkeeping purposes but are not issued in tokenised form on DLT to automatically be included in Group 2 / to be subject to the cryptoasset exposure framework. In such cases, the use of DLT results in no change in the risk or liquidity profile of the underlying assets, but only in the mechanism by which the ownership title is transferred. 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 the classification requirements / additional risk weightings or capital charges, solely as a result of the use of DLT for transfers of ownership. The current proposed treatment would discourage banks from participating in securities markets that adopt DLT. As a result, we request clarification of where DLT is used, in order to facilitate the recording of transfers of ownership without the creation of a distinct tokenised asset.
- 60.6 → How often is “on an ongoing basis”? More clarity regarding the intended frequency would be desirable.

- 60.8 → We suggest to clarify whether the condition refers to the stabilization mechanism itself or the market value of the cryptoasset.
- 60.9 → 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)), would disqualify many tokenised arrangements that we believe should be Group 1a assets.
- In addition to the later, 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)) fails to take into account the unique characteristics of tokenisation arrangements, such as special AML requirements and controls.
- 60.10 → Proposed SCO60.10(1) provides that cryptoassets would fail to meet the 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." This requirement will hinder banks' ability to create highly conservative tokenisation arrangements and should be not be incorporated in a subsequent version.
- 60.12 → "Redeemable at all times" = "Absolutely redeemable"? (Absolutely redeemable understood as "everyone can redeem the assets at all times" vs "Actuarially redeemable" (i.e., everyone who desires at any given time to redeem the assets, will be able to do so).
- 60.13 → 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 Committee should clarify (1) what risks banks are expected to measure for purposes of this requirement, (2) what constitutes sufficient overcollateralisation, and (3) whether the degree of overcollateralisation is at the banks' discretion.

- Additionally, 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)). It is unclear what would qualify as a "robust" operational risk and resilience framework for this purpose, and how a bank can "ensure" that such a framework exists when the stablecoin issuer, not the bank, is responsible for developing or maintaining the framework.
- 60.14 → What happens if the breach is momentary (i.e. lasts less than a day)? Or repeatedly momentary? How does this "breached time" add up?
- Additionally, this test depends on how the day is defined, which could be different from one geography to another, given the continuous frequency of cryptoasset trading, and the different time zones. These should be better defined to have consistent treatment among jurisdictions.
- 60.17 → We support the alternative to the 2 tests that the BCBS is considering (being a regulated and supervised entity).
- It would be useful to specify the criteria to be classified as regulated.
- 60.18 → We should ensure that these restrictions and classifications do not inhibit financial innovation in banks and foster an increase in shadow banking entities.
- 60.21 → 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 cannot uniformly attest to the operation of aspects of a distributed and decentralized 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.

- Using existing risk management expectations to manage risks of cryptoassets and networks upon which they operate should be sufficient to support safety and soundness and would be consistent with the technology neutral principle of the First Consultation.
- 60.33 → We believe this assumption does not hold in reality. The nature of cryptoassets adds an additional "layer" of rights and thus correlated (but not equal) likelihood of paying the owner all amounts due.
- 60.40 → We recommend that the Committee recognizes that Non-Redemption Risk Group 1b cryptoassets qualify for recognition as collateral for credit risk mitigation purposes to the same extent as their underlying traditional assets.
- 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, we believe that there is no basis for disqualifying such a cryptoasset from recognition as collateral for credit risk mitigation purposes to the extent the underlying traditional asset(s) qualify as collateral.
- 60.47 → The bank would already hold capital against the risk of default of the redeemer under SCO60.50 (standardised approach for market risk) or SCO60.56 (internal models approach for market risk), as applicable. Increasing the amount of market risk RWAs a bank would recognize in this case would be to require a bank to hold capital against a risk it does not need to bear if it can redeem the cryptoassets directly with the issuer, namely, the risk of being unable to sell the cryptoasset itself in the market.
- 60.60 → We 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.
- This criterion results in an overly narrow category of products and should be revised. These product categories should be designed to be as inclusive as possible, with the subsequent requirements relating to liquidity and data availability further

constrained by the existence of recognized hedges. To that end, we recommend that proposed SCO60.60(1) be revised to read as follows:

- (a): A direct holding of a spot Group 2 cryptoasset where there exists either a derivative that is cleared by a qualifying central counterparty (QCCP) or an exchange-traded fund(ETF)/exchange-traded note (ETN) that is traded on a regulated exchange that references the cryptoasset.
- (b): An ETF/ETN that is traded on a regulated exchange or a regulated mutual fund that references a Group 2 cryptoasset that meets criterion (a) above.
- (c): A derivative that is cash-settled or that is physically-settled into digital assets (including tokenised traditional assets, commercial bank deposit coins, stablecoins, and Group 2 cryptoassets) on a regulated exchange.

- It is not clear whether the requirement that "the average market capitalization is at least USD10 billion over the previous year" should be measured on a rolling 12-month basis or once annually on a static basis. We suggest that such market capitalization be measured on a rolling 12-month basis to minimize cliff effects that would result from a single yearly measurement.
- 60.74 → The sensitivities do not consider netting for exposures that sit in different exchanges and/or different time to maturity buckets but have legally binding provisions. Exposures that are in different risk factor buckets should be allowed to net to the following extent:
  - 100% hedge recognition where one instrument can be delivered against the other (for example, a future on a crypto ETN and a position in that ETN);
  - 100% hedge recognition where the legal agreement provides for "execution pricing" to link the price of a derivative to the price on the hedge and includes provisions to deal with hedge disruption; and
  - 90% hedge recognition for instruments defined in SCO60.60 referencing the same cryptoasset, provided the instruments demonstrate greater than 90% correlation over a period of at least the last 12 months, including where the instruments are listed on different markets or exchanges.
- 60.126 → It states that: "Cryptoassets activities introduce new kinds of risks and increase certain traditional risks". We would like to make the following correction:

"Cryptoassets activities introduce new kinds of risk and increase or reduce certain traditional risks". Cryptoassets activities do not always increase traditional risks, they may also reduce them, for instance in the case of digital securities.

- 60.129 → Regarding paragraph 60.129, that delineates operational risk vs. credit and market risk:
    - As a general comment, the supervisory review process should rely on the currently existing structure, it should avoid setting up new structures.
    - A mapping of the technological risks of Cryptoassets to Basel risk categories would depend on the circumstances:
    - If the triggering event leading to a loss is due to processes or systems outside of the bank's control and the loss of the bank manifests through the value of a bank position in Cryptoassets, such losses would be covered by the credit risk framework (for banking book positions) or the market risk (for trading book positions).
    - When losses result from inadequate or failed processes, people or systems of the bank (e.g., loss of a cryptographic key by the bank), such losses would be operational losses.
- 60.130 → Regarding the Bank risk management requirements (paragraph 60.130) and the ones that refer to “Cryptoasset technology risk” it is important to assess what part is critical and what part is not. Stability of the DLT is fine but, for instance, nobody is asking us (banks) to guarantee the stability of the telephone service. It would also be necessary for the standards to distinguish between:
    - If we are in control of a DLT network, then we should be responsible for it.
    - If the DLT is external, we should have a contingency plan (BCP) for outages. We may be required to assess the risk of the DLT but not to be constantly monitoring it or be responsible for its failure.
- It is our view that Permissioned applications built on Permissionless Blockchain should be eligible to fall under Group 1 Cryptoassets.
- In the case of a failure of the DLT, it would be necessary to safeguard the ownership of the Cryptoassets.
- The way to mitigate the risk of losing the recording of the ownership of the assets would be requiring a Business Continuity Plan (BCP), which would contain a clause

stating what would happen in the case of a catastrophe. Such a clause could include an external data recording system (e.g., back-up system stored in the cloud). The BCP should not cover all the network functions but just the recording of the ownership of the assets.

- An example of this BCP can be found in the French (DLT Decree of Dec 24, 2018), German and Luxembourgish Laws. In the case of the French Law, there is a registrar, who acts on behalf of the issuer of the instruments, who must oversee this BCP to guard against the event of a DLT outage.
- Paragraph 60.130: "General information, communication and technology (ICT) and cyber risks". From an operational risk perspective, this category does not currently exist in the Basel framework. It would be necessary to clarify how it would fit with the Basel categories for operational risk: Level 1 and Level 2 Loss Event type Classification.
- Paragraph 60.130: "Legal risks". We think that the proposed definition would not be fully consistent with the Basel categories for operational risk:
    - (b) Taking Ownership and (d) Uncertain Legal Status should be Legal risk.
    - (a) Accounting should be Financial, reporting and tax risk.
    - (c) Disclosure and consumer protection should fall under Business Practices (conduct risk).
- 60.134 → Precision on how often should this information be disclosed would be appreciated.

***

FELABAN wishes to thank the Committee for considering the above comments, and hope they enrich the development of a potential cryptoasset prudential and regulatory framework. Should any clarification arise regarding our comments to this consultative document, we look forward to discussing them further.

Sincerely,

GIORGIO TRETTENERO CASTRO

Secretary General

FELABAN – FEDERATION OF LATIN AMERICAN BANKS