FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

FB-0100/2024 São Paulo, January 31, 2024.

Basel Committee on Banking Supervision
Bank for International Settlements
Centralbahnplatz 2, CH-4002 Basel, Switzerland

Ref: *"Disclosure of Cryptoasset Exposures* - consultative document"

The Brazilian Banks Federation (FEBRABAN) is grateful for the opportunity to comment on the Basel Committee's public consultation on the "Disclosure of Cryptoasset Exposures".

We welcome the consultation on the disclosure of cryptoassets exposures. We believe that the disclosure framework is an essential part of the regulatory architecture and that a correct disclosure of cryptoasset exposures can provide relevant information to stakeholders. Nevertheless, an excessively detailed disclosure on very technical and complex issues can also have a detrimental effect on transparency.

In this sense, FEBRABAN understands that some adjustments to the current proposal must be taken into consideration to preserve the intended purpose and suggests that the Committee consider the following points in the review.

Initially, it is important to mention that the cryptocurrency market is a developing segment in the world and presents extremely different stages of maturity and depth between jurisdictions. It is also worth mentioning that these assets are still insignificant in the total assets of most of the banks, especially in the segment of the systemic important institutions among the localities, and the cryptoassets market is still concentrated mainly in companies and funds that are outside of the banking sector.

It is also important to mention that these assets will be subject to the same treatments observed for other assets of the institutions and subject to the entire current prudential framework, like credit, market, and operational risks. As well these

Av. Brigadeiro Faria Lima / 4300, 4º andar
04538-132 / São Paulo SP / Brasil

55 11 32449800
febraban.org.br

assets will also be subject to the same treatment of the other assets on the leverage ratio and liquidity indicators of the banks.

We support the relevance of defining the appropriate prudential treatment for the cryptoassets, as addressed by the BIS in the standard published at the end of 2022. However, we consider that will be necessary to take in account the materiality of this market for the banking sector, when defining the relevance of detailed and technical information required to market agents and given the implicit operational effort.

In this sense, we believe that the need to report on the topic must comply with minimum criteria of materiality and representativeness in the assets, as is observed in other aspects of international prudential regulation and applied in local jurisdictions.

We would like to mention that Brazil is experiencing a preliminary process to that of other jurisdictions. Brazilian authorities are still building the entire legal framework relating to cryptoassets. In December 2023, the Central Bank of Brazil (BCB) published one consultative document which deals with the construction of an appropriate regulatory framework for service providers to operate with these assets. As part of this work, the BCB is asking participants to answer a set of questions with the aim of obtaining contributions and information for drafting the market function and the regulation on the topic.

Despite some comments on specific points in the document, our main concerns lie in two general aspects in relation to the topics mentioned, which are the timing of the implementation and the materiality to require the disclosure of this information, given the perceived costs and benefits.

1) Implementation Deadline: The proposition of implementation by 2025 for certain jurisdictions seems out of market development reality or relevance. The legislative / rulemaking agenda in various jurisdictions is currently under unusual amounts of stress, which is likely to lead to delayed implementation of the cryptoasset prudential framework in some major jurisdictions. This would result in misaligned implementation dates and a lack of consistency in applicable standards which would have a disproportionate impact on entities operating on a global basis.
Brazil, as mentioned, is an earlier stage in the discussions and the market is very

incipient in terms of the total assets of the banking sector. In this sense, we consider that the BIS could postpone and give the local regulators the flexibility to define the adequate implementation schedule for the layouts suggested by the BIS consultation.

As such, we propose extending the effective date from January 1, 2025 to January 1, 2027, allowing member jurisdictions sufficient time to implement the Committee's standards within a globally consistent timeframe.

2) Materiality: The role of materiality in the proposed disclosure requirements does not align with existing principles of appropriate disclosure. Parts of the proposed templates requires the disclosure of all cryptoasset exposures, even if they are immaterial for a particular bank. Such extensive disclosure requirements for potentially immaterial aggregate exposures could discourage the testing and adoption of innovative technologies. It is critical that the final disclosure requirements align carefully with the Committee's longstanding policy objectives for banks' disclosures.

Further, the proposed introduction of a specific disclosure threshold for "material" cryptoasset exposures is inconsistent with existing disclosure regimes and Basel Framework principles. Typically, materiality tests are instead based around a subjective user test. If a specific threshold were to be included in order to determine when a bank's overall exposure to cryptoassets is considered material and therefore subject to any disclosure requirements, it would need careful consideration in relation to a bank's total risk-weighted assets.

A second-stage test would then be required to determine whether an individual cryptoasset exposure is material and subject to applicable individual disclosures. We would suggest that this is based on a quantitative test, for example 10% of a bank's total exposures to cryptoassets. The threshold contemplated in the Consultation (i.e., a cryptoasset exposure is material if it exceeds 5% of total cryptoasset exposures) inappropriately conflates these two separate assessments.

A materiality calculation on this basis would likely include immaterial exposures while potentially excluding subjectively material ones.

We therefore suggest the disclosure templates are amended to provide that a bank should decide which disclosures are relevant for it based on the materiality concept

in accordance with the Basel Framework and as originally contemplated by SCO60.129. This would include maintaining the use of qualitative judgment towards the definition of material, ensuring that this is consistent with the definition of material according to relevant established and recognized accounting standards such as GAAP or under the International Accounting Standards, as set out in IAS 1.

In addition, we have comments about the proposed templates and the specific issues raised by the Basel Committee:

1) Avoiding window dressing: we share the concerns on the need to have an accurate view of a bank's cryptoasset exposures and to avoid any potential window dressing. Nevertheless, we think that there are some issues to consider in this regard.

We do not agree that disclosing the amounts in Template CAE1 using daily average values would be an appropriate addition to the proposed disclosure requirements. Such data averaging is unlikely to achieve the stated aim of giving a more accurate picture of risk and presents significant operational complexity and costs that are not justified.

On the one hand, we think that we need to assess the added value that daily average data can provide. We certainly think that for RWA purposes, it would not be significant. For us, the avoidance of window dressing makes special sense in requirements that come in the form of a limit (here for example for the group 2 limit), but not for capital requirements. For entities with minor exposures in cryptoassets, having so much operational burden can effectively prevent entities from entering in cryptoassets markets.

On the second hand, using daily average values is nearly impossible or has a big operational burden for entities. Currently, it is very difficult to have information more granular than monthly. This is even more difficult in decentralized banks with presence in third countries, as we would be obliged to require this information from all the subsidiaries. However, we share the concerns on the need to have an accurate view of a bank's cryptoasset exposures and to avoid any potential window dressing.

We recommend alignment with existing Pillar 3 disclosure requirements for market risk. For Group 2 cryptoassets, disclosure consistent with existing market risk disclosures would avoid the challenges mentioned above. Group 1 cryptoassets would already be included in existing disclosures. However, if a separate additional disclosure is required, then trading book Group 1 cryptoasset reporting frequency would align with the above. Group 1 banking book disclosures should only be required for the period-end date on a point-in-time basis.

2) Classification condition assessment detail: Although we consider it very useful that stakeholders have information about how the bank assesses the compliance with classification conditions, we are of the view that the feasibility and utility of providing the requested information should be assessed with a long-term view. Additionally, considering all the information required for the prospectus, it should be analyzed the potential overlapping to reduce the reporting burden.

Nevertheless, we need to consider that very complex or detailed information may have a counterproductive effect. Therefore, we should avoid entering in a level of detail that prevents regular stakeholders from getting an overview of the bank's activities related to cryptoassets. In this sense, we find that the proposed additional information includes very technical information that may be difficult to understand. For example, information on the functioning of the stabilization mechanisms, some legal requirements, technical information on the design and the functioning of the network etc. That's why we would propose to keep the level of detail proposed in the template CAEA without including the information on the annex.

In addition, we consider there is a need to differentiate between information that is going to be provided by group 1a and the information to be provided for the rest of the groups. When the traditional tokenized assets will have issued as business as usual, it would be impossible to provide all the suggested info. For a traditional bond so much detail is not required, to a tokenized traditional assets additional information should not be required either.

The Group 1 classification condition assessment details, as reflected in row (f) of Table CAEA, require banks to disclose the approach they have used to assess compliance with each of the four Group 1 classification conditions (as noted in SCO60.8-60.19) for each cryptoasset. This would include any public information

used but exclude any confidential and proprietary information. We propose instead that a more streamlined disclosure approach is taken which requires more general background on banks' assessment approach to be provided. This would allow market participants to understand how a bank screens cryptoassets in accordance with the Committee's prudential standard, while minimizing the operational complexity introduced by any final disclosure framework.

For the same reason, we suggest the Committee not to incorporate the additional elements contemplated in Annex 2 in respect of each classification condition in any final disclosure framework. In addition to generating undue operational complexity for reporting banks, overly complex or detailed information may have the unintended effect of preventing a variety of stakeholders from receiving an overview of a bank's cryptoasset-related activities, risks, and approaches. Additionally, public documents published by issuers of Group 1 assets, and the networks they operate on, would, in most cases, contain the information in Annex 2, rendering such disclosure here duplicative.

3) Operational risk losses: The Table CAE1 requires banks to disclose the amount of their operational risk losses related to cryptoassets, which are defined as "total amount of operational losses related to cryptoassets net of recoveries and net of excluded losses within the 10-year window or fewer years in accordance with OPE25.10 that is relevant for the Loss Component calculation."

We do not support the public disclosure of losses linked to cryptoassets for the following reasons:

- According to the Basel Standards, banks need to disclose their aggregate operational risk loss and we think this should be the right level of disclosure, and therefore, we would like to ask for the removal of this requirement.
- The main argument is Operational security reasons. Should a bank have to deal with problems in the operations with cryptoassets, it would not be wise to publicly disclose these losses from an operational security perspective, since this would mean identifying potential weaknesses could produce a call effect for potential hackers and lead to further trouble. While we think that this information could be subject to reporting to the supervisor on a confidential basis, when it meets the current supervisory reporting requirements, it should not be disclosed to the public in general.

- The fact that banks may be required to disclose their operational risk losses related to cryptoassets, while this is not the case for non-banks, which are in fact the main actors, may lead the general public to think that banks are less safe institutions because they have losses linked to cryptos, when the fact is that the majority of the activity is carried out by non-banks, particularly in the case of the riskier ones.
- The scope of what is an operational loss linked to a cryptoasset is not clearly defined. This could lead to different interpretations by the different jurisdictions.

4) Risk of unintended consequences: The cryptoasset market is evolving quickly. If disclosure requirements are not calibrated correctly, and result in a required level of detail that is not operationally feasible or commercially viable for reporting banks, it will likely be more difficult for such institutions to engage in cryptoasset-related activity that they could otherwise conduct in a safe and sound manner with positive ultimate impacts for customers and market function.

There is also a risk that extensive granular disclosures by banks could result in market participants making inferences that banks are riskier than non-bank competitors, which are not required to disclose the same level of information about their cryptoasset exposures.

5) Custody: We think the disclosure requirements for the custody of cryptoassets should be consistent with the disclosure requirements that apply under Pillar 3 in relation to the custody of traditional assets.

The disclosure templates contemplate the disclosure of cryptoassets under custody in several places, including in column (g) in Template CAE1 and row (a) under Table CAEA. However, cryptoassets under custody do not belong to the custodian and therefore do not give rise to credit, market, or liquidity risk for the custodian. Before the finalization of any disclosure framework for banks' cryptoasset exposures, the proposed requirements should be revised so that banks would not be required to provide quantitative or qualitative disclosures related to the cryptoassets they hold in custody for clients. If such requirements remain, there is a risk that such disclosures of assets held in custody may be misconstrued as reflecting the cryptoasset

exposures of the bank, which would not accurately represent the risk profile of the bank and its financial activities.

Once again, we appreciate the opportunity to comment on revisions to the ““Disclosure of Cryptoasset Exposures””. Should you have any questions on the issues raised in this letter, please contact the undersigned com.gestao.riscos@febraban.org.br.

Very truly yours,

Rubens Sardenberg
Prudential Regulation,
Risk and Economic Affairs Direction

Tatiana Grecco
Director of the Risk Management
Committee

Oficio FB 0100-2024 pdf

Código do documento bd7927ae-9e74-4141-8295-b6effb7966ef

Assinaturas

Rubens Sardenberg
rubens.sardenberg@febraban.org.br
Assinou

Tatiana Grecco
tatiana.grecco@itau-unibanco.com.br
Assinou

Eventos do documento

31 Jan 2024, 18:07:57
Documento bd7927ae-9e74-4141-8295-b6effb7966ef **criado** por GISELE PAES MOREIRA SENA (e6c332a5-e2e1-47f1-9890-d5e3be078278). Email:gisele.paes@febraban.org.br. - DATE_ATOM: 2024-01-31T18:07:57-03:00

31 Jan 2024, 18:08:42
Assinaturas **iniciadas** por GISELE PAES MOREIRA SENA (e6c332a5-e2e1-47f1-9890-d5e3be078278). Email: gisele.paes@febraban.org.br. - DATE_ATOM: 2024-01-31T18:08:42-03:00

31 Jan 2024, 18:09:45
RUBENS SARDENBERG **Assinou** (84e81abf-69b6-4878-a68d-559697c4decc) - Email: rubens.sardenberg@febraban.org.br - IP: 18.228.6.126 (ec2-18-228-6-126.sa-east-1.compute.amazonaws.com porta: 5946) - Documento de identificação informado: 023.297.238-90 - DATE_ATOM: 2024-01-31T18:09:45-03:00

31 Jan 2024, 18:18:06
TATIANA GRECCO **Assinou** - Email: tatiana.grecco@itau-unibanco.com.br - IP: 200.196.153.154 (200.196.153.154 porta: 48846) - Documento de identificação informado: 167.629.258-63 - DATE_ATOM: 2024-01-31T18:18:06-03:00

Hash do documento original
(SHA256):f7ba444394d2269dff3d8ec55b241ea178cad1c9ee70f55a35c3666a1a452cc5
(SHA512):7bb3eaa6b5798f1f39d5c703d0da7036b0c93feda4d589bda5980955eb43533a702ed57a81f4c696657ed3a28772a2cd06401d5a52119a1baf7181b88f46071a

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign