EBF_045802
30 September 2022

EBF RESPONSE TO THE SECOND BCBS CONSULTATION ON THE PRUDENTIAL TREATMENT OF CRYPTOASSET EXPOSURES

EXECUTIVE SUMMARY

- Coordinated action in the prudential treatment of cryptoassets is key: We welcome this second consultation as we consider that a global framework for the prudential treatment of these exposures is of utmost importance in order to ensure a global level playing field across multiple jurisdictions. In the meanwhile, it is essential that jurisdictions which develop their own requirements on these activities should aim to an alignment with the global discussion, since they could give rise to potential extraterritorial effects or undermine the level playing field having very detrimental effects on the development of cryptoasset markets. While this topic cannot necessarily be addressed by the Basel Committee, we would like to draw your attention to this point as it can be quite significant.
- We welcome the number of developments in this second consultative document whereby the Basel Committee has taken into account some of the European banking industry comments made on the first consultation dealing with the same topic. These positive developments include, for instance, the increased granularity within group 2 cryptoassets related to some partial recognition of hedging, the increased granularity for the basis risk test, the introduction of an alternative to the basis risk and redemption risk tests for regulated and supervised issuers, the recognition of some cryptoassets as HQLAs, the removal of the link between the prudential treatment and the accounting classification, the removal of the Pillar 1 operational risk add-on and the more favourable liquidity treatment of crypto-liabilities. Generally, the second BCBS consultation on the prudential treatment of cryptoassets, although presenting some advances compared to the first consultation last summer, tends to disadvantage banking players in the cryptoasset markets, due to the discrepancies in requirements imposed to banking institutions compared to non-regulated players. We think that the regulators should also take this opportunity to establish the means that would allow banking supervisors and regulators to conduct a rigorous and iterative review of activities related to cryptoassets.
- The current applicable BCBS framework is being also transformed to impose a more stringent prudential treatment compared to traditional assets, in terms of both capital and liquidity, that we consider it as differential from the "same risk, same activity, same treatment" principle.
- The prudential treatment of cryptoassets should ensure consistency with the regulatory regime of existing traditional assets. From our point of view, it would be necessary the approach *vis-à-vis* the regulation of cryptoassets should follow the same spirit as the regulation of traditional assets, where justified. One of such examples would be the exposure limit for group 2 cryptoassets, which does not exist in the same way for other asset classes. Also, the BCBS should clarify thatcustody services are only subject to operational risk requirements, in line with the current treatment of any traditional assets under custody.

European Banking Federation aisbl
Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

Group 1 cryptoassets and the infrastructure add-on: Prudential requirements related to Group 1a cryptoassets should be based on legal characterization of an asset and the feasibility to comply with regulatory requirements, and not on technological grounds. Technological neutrality is a cornerstone of securities regulation in the EU and banks are experimenting in an iterative way the potential use of permissionless and permissioned technologies for the issuance and trade of dematerialised securities. In the case of group 1b cryptoassets, prudential requirements should also be technological neutral and not be more stringent than those that refer to similar traditional assets that are not penalised with an infrastructure add-on. Furthermore, the Basel framework already has strong safeguards ensuring a clear and consistent approach to the prudential treatment of financial assets. In coherence with the Basel framework, technology should not be the ground for additional safeguards imposed on regulated institutions only, which will dilute, delay and/or preclude their involvement in such assets. This comes at the risk of preventing crypto-assets markets from being safer and better controlled, with a risk for the financial stability and the safeguard of retail customers investing in such markets.

SCOPE OF THE STANDARD

The BCBS proposal includes in its scope "non fiduciary custodial services that may only give rise to operational risk". We believe it is important the Committee make clear that custody services only give rise to operational risk, as currently happens with custody services of any other asset. The way it is phrased in the consultation, it might provoke confusion as to whether these activities could also be subject to credit or market risk, when this is clearly not the intention.

CLASSIFICATION CONDITIONS

Generally, the BCBS should clarify whether the framework applies only to fully digitalized financial assets or even to partially digitalized assets. Moreover, clients assets' custody for digital assets should be treated in the same way, as the one for traditional assets. Please also refer to our remarks regarding the group 2 exposure limit.

Eligibility of cryptoassets that are based on permissionless DLT

- It is our view that permissioned applications, assets and services built on permissionless Blockchain networks should be eligible for group 1, subject to the existence of certain controls. Indeed:
  - We believe that the prudential framework should not exclude the banks and their clients from the benefits of the innovations taking place on public blockchains;
  - The fact that issuances are made on permissionless blockchains does not prevent the risks from being carefully taken care of and to intermediate every trade realised on such assets. Examples of this include protocols for the governance, tracking and control of cryptoassets movement, tokens and smart contracts. In some cases, for instance, the tokenisation agent might remain (for the entire lifetime of the token) in control over the token through embedded functions, like seize, freeze and burn. As a final fallback, the terms and conditions of the tokenized traditional assets can even entail the right of the tokenisation agent to take the tokenised traditional assets off.
  - In many OECD countries, such as France, Germany or Luxembourg, the securities laws have adopted a legal framework authorizing the issuance and the trading of unlisted securities on either permissionless or permissioned blockchain technology. More recently, the EU has adopted the EU Regulation 2022/858 of 30 May 2022 which provides the possibility, under stringent

conditions and strong supervision, for market infrastructures to experiment the use of permissionless and permissioned blockchain technology for the issuance and trading of listed DLT financial instruments on trading venues. These regulations rely on a deep dialogue between regulators and regulated entities to assess the potential of decentralised technologies, and such experimentations should not be prohibited for prudential reasons. Various experiments of issuances of dematerialised securities (bonds, structured products, etc.) have been performed and processed since 2019 on permissionless blockchains in Europe under applicable law, including by the supranational European Investment Bank, Société Générale and BNP Paribas. These gradual experimentations of securities digitisation on permissionless DLT under applicable EU regulations will continue in close dialogue with EU and national regulators and with processes put in place which allow the intermediation of every transaction on these securities.

- Finally, in case of failure of a DLT, it is possible to safeguard the ownership of the Cryptoassets. The way to mitigate the risk of losing the recording of the ownership of the assets, whatever the underlying technology chosen (permissionless or permissioned), would be to require from the issuer and/or a third party (issuer's agent or market infrastructure) in charge of registry to put in place and maintain a Business Continuity Plan, which could be a clause stating what would happen in the case of a catastrophe. As part of this BCP, a node that is connected to the blockchain could be used to ensure that the lost data can be recovered and the records about the ownership of the assets can be retrieved. Please see also our comments on Business Continuity Plan under the infrastructure risk add-on section.

Given these elements, we believe that classification conditions 3 and 4 need to be adapted to permit the inclusion in group 1 of cryptoassets based on permissionless blockchains. The modifications we propose in this respect are described below.

Classification condition 1

- Claims on banks (group 1a): it should be made more explicit that all tokenized traditional bank assets and liabilities belong to group 1a, i.e. not only tokenized bank deposits but also for instance tokenized commercial bank money issued by banks. In this respect, we recommend clarifying some definitions, notably to avoid any confusion between tokenized commercial bank money and asset backed stablecoins. The term "stablecoin" should not be used for commercial bank money tokens or tokenized deposits.
- On this basis, we strongly support the idea (raised by the BCBS in article 60.17 of the proposal) that issuance by a prudentially regulated and supervised entity is considered as an alternative requirement to the basis risk and redemption risk tests. Considering that it would be difficult to define the adequate level of regulation and supervision to be required, we believe that the scope of this requirement should be limited to banks. It would recognize that exposures to stablecoins issued by banks are lower risk than those issued by non-banks, given the level of prudential requirements applicable to banks.
- Moreover, there is some uncertainty as to which assets meet the classification of group 1b cryptoassets (either under the stabilisation mechanism criteria or the governance/regulatory criteria that apply to non-banking players, on which banks will have no influence to verify conditions set at all times – e.g., node validators).

Basis risk test:

- The new basis risk test proposed by the Committee is in our view a positive step forward compared to the first consultation document with regard to the cliff effect issue. We would however suggest three alternative proposals to make it more flexible:
  - "If the peg-to-market value difference does not exceed 10bp more than 3 times over the prior 12 months, the cryptoasset has "fully passed" the basis risk test." We believe that also a minimum number of consecutive days for which the peg has fallen below a given threshold should be considered (indicating some persistence of the de-peg).
  - As an alternative solution we would suggest that the 10 bps threshold for fully passing the basis risk test should be increased to 15 bp and the 20 bps threshold for narrowly passing the basis risk test should be increased to 25 bps.
  - The third proposal aims at further increasing progressivity using on a linear risk-weight add-on function:

    In Credit risk

$$basis_{avg} = \frac{1}{1Y}\sum_{i \le 1Y} Max\{0; Diff_{bp}\}$$

$$RW_{addon} = Max\{0; basis_{avg} - [2bp]\} \cdot [100\%]$$

    The total risk weight (of the pegged instrument and the add-on) shall be cap at 1250%, as a result the cap is reached for:

$$basis_{avg}^{max} = [2bp] + \frac{1}{[100\%]}(1250\% - RW_{peg})$$

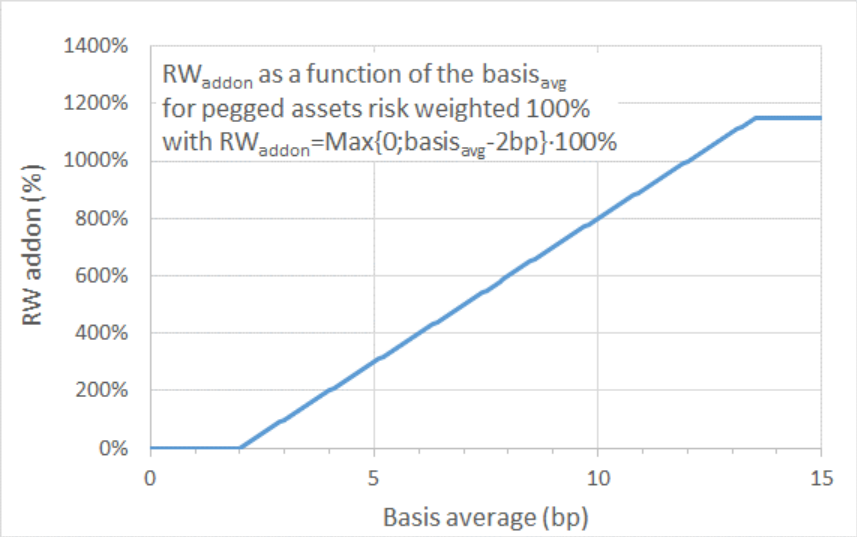
    Above that threshold the stable coin is risk weighted at 1250%, i.e. we are reaching the level at which as group 2b crypto-asset is capitalised [SCO60.89].

    In Market risk

    We suggest that the stable coin may remain in the market risk framework as if an exposure to the pegged instrument consistently with SCO60.48(2) and SCO60.54(2). To account for the difference between the peg and the stablecoin value risk, an additional capital charge applies. This capital add-on is equal to the credit risk weight add-on as calculated for Credit risk (see above) multiplied by 8% times the net exposure in the stablecoin. The credit risk weight add-on is capped to 1250% minus 12.5 times the applicable FRTB-SA supervisory risk weight.

    Examples

Example of USD pegged stablecoin		$Basis_{Avg}$	No Diff>10bp	No Diff>20bp	RW_{addon}
True USD	**TUSD-USD**	1,24	7	0	0%
USD coin	**USDC-USD**	1,37	4	0	0%
Tether	**USDT-USD**	1,93	26	2	0%
Binance USD	**BUSD-USD**	2,32	25	0	32%
DAI	**DAI-USD**	3,63	26	13	163%
Pax dollar USD	**USDP-USD**	5,91	78	34	391%
USDD	**USDD-USD**	42,96	156	137	1150%
Neutrino USD	**USDN-USD**	184,22	362	362	1150%



Stablecoins that reach the average basis leading to a total 1250% risk weight will be consider as of Group 2b for other purposes (collateral eligibility, etc…).

- This would also allow to smoothen the cliff-effect inherent to the basis risk test, which could potentially trigger a negative feedback loop (if a stablecoin becomes no longer eligible to group 1, market players would sell theirs, thus, worsening the problem)
- The consultation states that the reserve behind each stablecoin should be sufficiently overcollateralized in order to exceed at all times, including under stresses conditions, the value of the peg. The expected level of collateralization of the reserve of assets should be made clearer and be included in the Basel text, to avoid a different application in each jurisdiction.

Classification condition 3

As currently drafted, classification condition 3, which is very broad, implies that banks bear all the responsibility to assure the functioning of the infrastructure, no matter if they are the operator or not.

When legal entities are the operators of the infrastructure – which is the case when operating private blockchains – the rule makes sense. Banks are committed to effective ongoing risk management to mitigate risks posed by cryptoassets they issue and by the private DLT networks they operate or in which they participate.

On the contrary, when the infrastructure of a public blockchain is used, entities cannot bear the responsibility. Public blockchains are not operated by legal entities, are fully decentralized and maintained by a large number of players, which means that there is no single counterparty identified. It is the set-up of the protocol that determines the solidity of the infrastructure, as well as the resilience against fraud and cyber risks.

In the case of permissioned applications, which are built on top of the permissionless blockchains, banks can make sure that they provide the necessary controls (Access, KYC, governance and security requirements…). As mentioned above, banks cannot attest the correct functioning of the DLT in the case of permissionless DLTs, since there is no legal entity being responsible therefor. In case of a DLT outage, what is relevant is that the

issuer or its agent has a proper Business Continuity Plan in place that will safeguard the ownership of the assets.

In this respect, the resilience of public blockchains is not the same from one to another, as blockchains can have very different characteristics and exposures to risks. Banks cannot attest the correct functioning of such infrastructures in all circumstances.

Although these protocols provide financial markets infrastructures (FMIs), they operate today in an unregulated space. We believe therefore that protocols providing FMIs should be rated or regulated similarly to existing FMIs in the traditional world. It seems not realistic that banks could fulfil this task. Different banks might also come to different conclusions. Neobanks might be less conservative as traditional banks. In our opinion, the regulator should not leave open the possibility of such a vast range of different judgements.

Classification condition 4

An alternative to condition 4 could be to introduce an independent rating of such public infrastructures based on the solidity and the governance of the protocol behind the blockchain (for example its capacity to maintain a reliable, immutable ledger, its way to deal with upgrades (forks), the solidity of the consensus mechanism, the number of miners (51% risk), its way to deal with attacks from hackers).

The Second Consultation states that in-scope entities for this requirement "include operators of the transfer and settlement systems for the cryptoasset, wallet providers, administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism," and specifically names node validators as subject to this condition (SCO60.24).

When a public blockchain is used, it is neither possible for a bank to control the entities who store the cryptoassets nor to admit or reject new entities. A public blockchain has a huge number of nodes running worldwide. Those nodes store a copy of the ledger. It is impossible to verify and to request that all node operators are regulated. The same would be applicable to storage providers. We believe that Condition 4 should be amended to remove this requirement related to node operators and storage providers.

However, when token issuers use a public blockchain, depending on the programmability of the token, the token can be permissioned thanks to a smart contract (example ERC1400 token on Etherium). Such standards allow the role of a "Controller" – an actor that can control access, freeze, reverse or destroy a cryptoasset or block a transaction - allowing for example KYC/AML/CTF checks. Public blockchains meeting those requirements are highly customizable. They offer the ability to limit access to the token to identified participants and set different access levels for each participant. An adaptation of the classification condition 3 to take that into account could be to write at 60.22(2)(ii) "degree of access of the digital asset (i.e. whether the digital asset is restricted or un-restricted)" instead of "; (ii) degree of access (i.e. whether the network is restricted or un-restricted)".

ADD-ON FOR INFRASTRUCTURE RISK FOR GROUP 1 CRYPTOASSETS

- It appears to be unclear what risk regulators want to cover with the infrastructure add-on. It seems to be the case that the infrastructure add-on implies that the DLT and the issuer (debtor) are the same thing, while they are different things. From our perspective, 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 or an email). If the DLT goes away, it is like 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.
- Against this background, we would like the Basel Committee to consider the following considerations:
    - Although we agree with the statement made in the consultation paper that the technology is new and evolving, we do not think that an infrastructure add-on is justified, while it would duplicate existing requirements, such as operational risk. It is useful to recall that when other new technologies were introduced, i.e. cloud technology, institutions have never been subject to an infrastructure risk add-on. In our opinion, there are better ways to manage any risk arising from the technology than applying a flat 2.5% capital add-on. Especially given that the classification conditions for group 1 assets are already very strict.
    - In any case, the way to cover for the risk of failure of a DLT should not be the infrastructure add-on but a Business Continuity Plan from the issuer and/or a third party in charge of registry, which could be a clause stating what would happen in the case of a catastrophe. In the case of private as well as public blockchains, nodes connected to the blockchain can be used to recover the data at the time of a failure as it also includes the latest transactions. This would not be the case with external registries.
- In addition, it is argued that the technological infrastructure that underlies all cryptoassets, such as the DLT, is still relatively new and may pose various additional risks even in cases where the cryptoassets comply with the group 1 conditions. At the same time, it is decided that this add-on for infrastructure does not apply to Group 1a assets that are backed by the full faith and credit of a central bank or sovereign entity (e.g. a tokenised asset issued by a sovereign entity). Given that this add-on refers to a technology, we do not see the reason that there should be such a difference between types of issuers that will be using the same technology. Also, this will create and unlevel playing field between public and private issuers, where digital assets backed by central banks and sovereign entities will not be penalised versus their traditional assets and will be able to fully develop, while assets issued by private issuers will be unable to compete with their traditional versions. We are clearly **not** in favor of this add-on, which is segregating the type of issuer or guarantor.
- Ultimately, an infrastructure add-on would inhibit the development of the digital markets, as investors will always prefer the cheaper instruments due to having lower capital requirements: in the case of bonds, investors will prefer to buy the traditional bond vs. the digital bond. Even though the DLT technology can provide significant efficiency benefits and simplify current solutions, those would be outweighed by the additional costs that the regulation would entail. Therefore, this would be a significant obstacle to the adoption and application of DLT technology in the banking sector.

- In the EU, specific regulations have been developed, such as the pilot regime, which fosters the development of new marketplaces for crypto-assets that qualify as financial instruments, and the MiCA Regulation, which allows for other crypto-assets that do not qualify as financial instruments (such as stablecoins, e-money tokens and utility tokens) to be issued, stored and transferred on a distributed ledger. These regulations are expected to open up opportunities for efficiency improvements in trading and post-trading processes, while at the same time ensuring consumer protection and financial stability. It is of the upmost importance that European banks be allowed to take part in these new regulations to take them at scale, to secure them and launch new experiments, with a similar framework as non-bank intermediaries.

GROUP 2 EXPOSURE LIMIT

- The group 2 exposure limit as currently defined is overly punitive for banks. When a hard exposure limit is established, banks have to operate way below it, in order to allow for a certain buffer that prevents breaches of that limit. This effectively means that the 1% Tier 1 limit will be much lower when operationalised by entities.
- Regarding the group 2 exposure limit, it is worth mentioning that the similar financial sector entity exposure limit of the Basel III regulation has much higher limit value (10%) and allows for netting in the exposure calculation. Similarly, in the EBA Guidelines on shadow banking exposures and hedge funds, for example, which could be considered as equally risky and speculative investments as cryptos, do not impose such a strict limit, instead they have a limit of net exposures equal to 25% of the Tier 1. Therefore, we consider that this limitation to 1% of Tier 1 capital, does not reflect current supervisory practices.
- The scope of the limit should be clarified. Group 2b cryptoassets should be exempted from the limit, given that they are already under the subject to the 1.250% RW. Moreover, it should be clarified that off-balance sheet exposures (e.g. those from custody services) only generate operational risk and are not covered by this limit.
- Although we are not in favor of such an exposure limit, we would ask the Basel Committee to at least raise the limit up to, for example, 5 %, and to allow for netting. With regard to netting, it is critical to mention that the calculation of the total exposure to Group 2 cryptoassets does not take into account netting rules similar to those netting rules for the calculation of market risks. Without such nettings rules and with a limit of just 1% of the bank`s Tier 1 capital, banks will be hardly able to offer services or products on Group 2 cryptoassets. For instance, a bank with a Tier 1 capital of EUR 10 bn which yields a Group 2 crypto asset exposure limit of EUR 100 million. If the bank sells derivatives on Ether or on the CME Ether future with a delta-equivalent of EUR 50 million to its clients and hedges the market risk with a corresponding matching CME Ether future also with a delta-equivalent of EUR 50 million, the bank would have already reached the Group 2 exposure limit despite the fact that the market risk of the position might be close to zero. It is clear that no profitable business case covering all infrastructure and administration costs can be developed based on such a tight exposure limit together with no netting rules with the consequence that such services and products would only be offered outside the banking sector.
- The very strict conditions behind the classification as group1, that must be met at all times, increases the risk of reclassification of Group 1 crypto assets to Group 2, making the 1% Tier One limit very difficult to monitor and its breaches difficult to anticipate, also making it more probable the punitive 1250% treatment in case of breach.

MINIMUM CAPITAL REQUIREMENTS FOR CREDIT AND MARKET RISK FOR GROUP 2 CRYPTOASSETS

Capital requirements Group 2a cryptoassets: standardised approach (SA)

- A risk weight has been chosen to be 100% for all Group 2a crypto assets in the standardized approach (60.71-60.78) which means a simulation of a +100% increase and a decrease to 0 value needs to be carried out for the calculation of the curvature risk. Such extremely prudent market risk scenarios for all Group 2a crypto assets including the most liquid ones seem to be unjustified and would have the consequence that banks would not be in the position to offer any products with non-linearity (e.g. call options or put options) on group 2a crypto assets to their clients due to uneconomically high capital costs. We would propose to introduce different risk buckets with different risk weights within the Group 2a crypto assets similar to the different risk buckets for equities or FX within the FRTB standard approach framework.

Netting between exchanges and markets

- Section 60.65 of the proposal states that: "When consolidated, positions for each Group 2a cryptoasset in different markets or exchanges must not be offset". We understand this the way that it is not possible to net between the same product traded on different exchanges or in different markets. For example, it can be a group 2a asset with reference to Ether traded on two different exchanges. As a starting point, we do not see any reason why it should not be possible to net in this case. On the contrary, it may limit the possibilities of hedging and otherwise increase concentration risks if institutions only trade certain products on certain exchanges or markets. Netting between exchanges and markets should therefore be allowed for both group 2a and 2b assets.

Scope of group 2b Cryptoassets

- The second consultation states that the capital treatment for group 2b cryptoassets applies not only to direct exposures but also to funds of group 2b cryptoassets such as group 2b cryptoassets ETFs and "other entities, the material value of which is primarily derived from the value of group 2b cryptoassets. This reference is quite concerning and we would ask for clarification that group 2b capital treatment does not cover crypto exchanges, wallet providers, blockchain miners and other entities which if constrained by this capital requirement, would drive cryptoasset products outside the regulated banking system.

Use of the 1250% risk weight

- A risk weight of 1250% is to be applied to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the separate Group 2b crypto assets to which an institution is exposed. The 1250% risk weight is calibrated so that the effect will simulate a deduction in own funds of the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the separate Group 2b crypto assets to which the bank is exposed, assuming that the bank is subject to the 8% minimum regulatory capital requirement. However, banks are subject to pillar 2 capital requirements and buffer requirements on top of the 8% minimum regulatory capital requirement. If management buffers on top on the regulatory requirements are also accounted for, the 1250% risk weight would, for most banks, result in additional capital of at least twice the amount of the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short

positions. Such capital requirements seem excessive and unjustified considering the original intention with applying the 1250% risk weight. We suggest that banks as an alternative to applying a 1250% risk weight should be permitted to deduct from own funds an amount equivalent to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the separate Group 2b crypto assets to which they are exposed.

LIQUIDITY

Treatment as high-quality liquid assets (HQLA)

- We welcome the positive development with the recognition as HQLA assets of group 1a cryptoassets. However, we are surprised by the absence of recognition of group 1b cryptoassets where the reference asset is HQLA. If the reference assets of a group 1b crypto asset are HQLAs, compliance with the redemption risk test (whose "*objective […] is to ensure that the reserve assets are sufficient to enable the cryptoassets to be redeemable at all times, including during periods of extreme stress, for the peg value*") should make it possible to ensure an easy and almost immediate sale (as defined for LCR [LCR30.2] where "*Assets are considered to be HQLA if they can be easily and immediately converted into cash at little or no loss of value*") and at the value of the reference assets.
- This point is all the more valid as the basis risk test should make it possible to ensure that the value does not deviate from the value of the reference asset.

Application of the LCR and NSFR frameworks

- Although it is stated in SCO60.106 and 60.110 that liquidity treatment of "cryptoasset exposures, including assets, liabilities and contingent exposures, should generally follow a treatment that is consistent with existing approaches for traditional exposures with economically equivalent risks", 60.112 (2) b does not allow the same LCR treatment for tokenized retail deposits. We believe that all tokenized traditional bank assets and liabilities, included in group 1a, should obtain LCR/NSFR treatment equivalent to corresponding traditional balance sheet items (for example tokenized claims on banks), especially as banks are regulated and supervised entities and will only use infrastructures that pass first regulatory requirements and second their own risk management requirements.

The liquidity treatment, in particular the one described in 60.113, should also recognize liquidity inflows in the form of CBDC, rather than fiat currencies only.

BANK RISK MANAGEMENT AND SUPERVISORY REVIEW

- As a general comment, the supervisory review process should rely on the currently existing structure, it should avoid setting up new structures
- Paragraph 60.126 says that: "Cryptoassets activities introduce new kinds of risk 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 not always increase traditional risks, they may also reduce them, for instance in the case of digital securities.
- 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 would be Legal risk
    - (a) Accounting would be Financial, reporting and tax risk
    - (c) Disclosure and consumer protection should fall under Business Practices (conduct risk)

DEFINITIONS

To foster a common understanding of the cryptoassets and contribute with the allocation of various cryptoassets as regards the responsibilities of banks and supervisors *vis-à-vis* the classification of cryptoassets, the EBF is in favour of defining a set of common criteria for the classification of widely used and accepted cryptoassets. This would deter banks and supervisors from carrying an additional burden and it would eventually guarantee consistency across multiple jurisdictions. At the same time, sufficient flexibility to this classification should be left to allow for new use cases to be included into the framework.

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.

www.ebf.eu @EBFeu

For more information contact:

Lukas BORNEMANN
Vasileia TSIRIGKAKI
Policy Advisers - Prudential Policy & Supervision

Email:

l.bornemann@ebf.eu
v.tsirigkaki@ebf.eu