BNP PARIBAS

September 2021

PRUDENTIAL TREATMENT OF CRYPTOASSET EXPOSURES

Basel Committee on Banking Supervision Consultative Document

Q1. What are your views on the Committee's general principles ?

We agree with the general principles laid down by the Committee. However, we do have some comments on how they are applied in the consultative document. We also think that they could be supplemented.

Cryptoassets are a new kind of assets. Their very existence depends on IT infrastructures and on the governance of protocols. If the infrastructure is not properly set up or if the governance is not sound, the assets can be stolen or just vanish. Therefore the risk on cryptoassets depends first on the soundness of the infrastructure and the governance. Actually, Group 1 cryptoassets could be more risky than Group 2 if the infrastructure and governance are not secure. The general principles laid down by the Committee do not take into account this specificity of cryptoassets. In our opinion, an independent rating of the infrastructure and the governance is needed. A central list of approved Group 1 cryptoassets could also be a useful tool to promote a consistent treatment in this global market. At a minimum, an international guidance will be necessary to help ensure assessments of IT infrastructure and governance are made in a consistent manner across jurisdictions.

Same risk, same activity, same treatment

As regards the first principle, "same risk, same activity, same treatment", which we strongly support, we regret that it is not fully applied here.

Given the proposed classification in two groups only, it appears that cryptoassets of a very different nature would be likely to classify as Group 2 assets and then be subject to the same capital treatment, i.e. the application by default of a 1250% risk weight, whereas they may represent very different risks. With a narrow Group 1 and a large Group 2 submitted to the conservative capital proposed, the classification set out in the consultative document would create an unjustified cliff effect.

More importantly, given the mandate of the BCBS, only some actors exposed to these cryptoassets, i.e. the banks, would be subject to the rules proposed by the Committee, while non-bank financial intermediaries (NBFIs) would be able to conduct identical activities, being thus exposed to the same risks without being subject to an equivalent treatment.

This asymmetry of treatment would raise questions of fair competition between banks and NBFIs and even worse would create a risk of shifting systemic financial risk to the latter. Failures of non-banks related to cryptoassets could eventually destabilize the whole financial system, including banks. This destabilization could occur even in a situation where banks would not be directly exposed to cryptoassets. From that perspective, i.e. systemic risk and financial stability, we believe that it would

be a wrong approach to consider that risks associated with cryptoassets activities could be tackled via banking prudential requirements only. All actors exposed to cryptoassets should be subject to equivalent rules and supervision, a principle which raises in fact the question of the licensing, authorisation and registration procedures for cryptoasset service providers (CSPs) and issuers. In this respect, the works underway within the various international standard-setting bodies (BCBS, CPMI, IOSCO, FATF, OECD, FSB…) and in some jurisdictions (e.g. MiCA proposal in the EU) to cover the different issues arising from cryptoassets are of tremendous importance. One can mention the paper published in early June by the Financial Stability Institute about how non-bank payment service providers (NBPSPs) are regulated so far[1]. According to the paper, "application of some regulatory requirements for payment services varies widely. Requirements related to AML/CFT, risk management and cybersecurity, data protection and consumer protection are, in general, uniformly applied across payment services. However, this is not the case for requirements related to authorisation, minimum capital, safeguarding of funds and interoperability. The objectives of these requirements may be the same, but how they are applied across payment services can be quite different. Moreover, the practices of implementation of these requirements vary significantly across jurisdictions even with the same payment service." A clear statement of the inequalities of treatment between NBPSPs, including in the field of cryptoassets.

Simplicity

We also agree with the principle of simplicity, in particular as it would help to ensure a consistent application across jurisdictions. However, the simplicity sought should not lead to a simplistic understanding of a subject that is inherently complex. For example, an excessively simplifying approach could lead to the classification in Group 2 of cryptoassets that do not fulfil the conditions for belonging to Group 1 without presenting genuinely significant risks. The less precise the different categories are, the more likely cryptoassets may be captured in wrong categories and therefore submitted to inadequate prudential treatment. In the following questions, we explain in more detail our views on the classification methodology proposed by the Committee.

Minimum standards

When it comes to the "minimum standards" principle, it should be specified that in conjunction with the "same risk, same activity, same treatment" principle, if a jurisdiction prohibits its banks from having exposures to cryptoassets, it has to do the same with non-bank financial intermediaries entities for similar exposures.

Also, while BNPP is supporting this initiative to define minimum global prudential standards for cryptoasset exposure, it would also like to highlight that some jurisdictions are or are planning to set up sandboxes or pilot regimes for market infrastructures based on distributed ledger technology (DLT). These jurisdictions have a policy interest in developing and promoting the uptake of technologies such as DLT in the financial sector which is particularly relevant for cryptoassets in Group 1a. Some of these sandboxes and pilot regimes have, or will have, pre-defined mechanisms (ie: limit thresholds, exemption requests, exit strategy…) to limit systemic risks for the industry within these specific frameworks while encouraging technological innovation. In order to encourage innovation, it might be interesting to consider to provide a regulatory support by relaxing some of the prudential requirements considered for Group 1, cryptoassets as long as they are issued within a sandbox or a pilot regime that is offering sufficient guarantee of protection against systemic risks.

[1] "Fintech and payments: regulating digital payment services and e-money", July 2021, FSI Insights on policy implementation N° 33

Accounting treatment

Finally, an additional general principle should be considered: as accounting and prudential treatments are mutually linked, we think that the prudential treatment and its development timeline need to be coherent with the ones of the accounting rules. As a matter of fact, the Basel Committee states in its consultation document that the proposed capital treatment would only apply to those cryptoassets that do not qualify for capital deduction, i.e. that are not classified as intangibles from an accounting point of view. But as things stand currently, since the accounting treatment of cryptoassets has not been fully clarified by accounting standard-setters, there is a high level of uncertainty. In this respect, it is worth noting the need for consistency between approaches to be adopted within the different accounting frameworks. Indeed, it would be an anomalous outcome if banks subject for example to IFRS or local country GAAP became subject to inconsistent capital requirements for the same activities.

Q2. What are your views on the Committee's approach to classify cryptoassets through a set of classification conditions ? Do you think these conditions and the resulting categories of cryptoassets (Group 1a, 1b and 2) are appropriate ? Which existing cryptoassets would likely meet the Group 1 classification conditions ?

If appropriate in its general principle, the proposed methodology needs to be supplemented and refined in some respects, in order to result in a more precise and risk sensitive classification.

With regard to Group 1a assets, the understanding is that they are cryptoassets confering the same level of legal rights as traditional assets but using "an alternative way of recording ownership through the use of cryptography, Distributed Ledger Technology (DLT) or similar technologies, rather than recording ownership through the account of a central securities depository (CSD)/custodian". There is a need however to define what are these "traditional assets" in question. Are those mentioned in paragraph 2.1 - i.e. (i) bonds, (ii) loans, (iii) deposits, (iv) equities, (v) commodities, (vi) cash held in custody - merely examples or is it a limitative list defining the scope of the assets concerned ? Would a Non-Fungible Token (NFT) of art, video or music meeting the definition of cryptoassets be considered as a tokenized traditional asset ? In addition, differentiation between categories 1a and 1b is unclear for stablecoins which are legally structured as liabilities of a SPV which holds monetary assets. Should such cryptoassets be classified as 1b (because they are stablecoins) or 1a (because they are a representation of a traditional financial asset) ? The classification of the "utility tokens" seems also uncertain. Would they fall into the first Group or in the second one ? Also, what about tokens which provide voting rights with no commercial purpose and no trading on a secondary market, ie tokens with community, justice or social goals ? Would they be classified in Group 2 and then be submitted to the conservative treatment envisaged, whatever the real risks associated with them ?

To avoid such uncertainties, the following elements could be taken into consideration:

1. Group 1a, which scope needs to be specified, should include cryptoassets:

   - that qualify as securities or financial instruments under the law of the relevant jurisdiction (e.g. MiFID in Europe) ;
   - which are a representation on a DLT of (i) ownership on assets that do not qualify as securities or financial instruments : real estate, precious metals, loans…, or (ii) rights in these assets, e.g. interests of a loan.

2. Group 1b, given the fact that stablecoins are very heterogeneous, should be broken down into subgroups based on their various characteristics and risk profile (e.g. tokenized form of commercial bank money, token backed by one specific asset Vs by a pool of assets, full or partial collateralization, nature of backing assets, governance of the management of the pool of backing assets, auditability of

the backing assets…), in order to devise specific conditions for each sub-groups. The classification of the stablecoins should be established by regulators.

3. Group 2 should be divided at least into three sub-groups, the first one being dedicated to the riskier cryptoassets, ie those with no intrinsic value (that includes algorithm-based stablecoins), the second one gathering some tokenised traditional assets not fulfilling all the conditions set out for Group 1 and the last one consisting of the utility tokens.

Lastly, we believe that an exception could be provided for Group 2 cryptoassets used for transactions fees payments (or "gas" payments). These fees are transaction costs that are paid automatically at the time of registration or transfer of data on a DLT. We consider that classifying such transaction fee-related cryptoassets as prepaid expenses would be an appropriate treatment from a prudential perspective.

Q3. What are your views on the classification conditions ? Are there any elements of these conditions that should be added, clarified or removed in order to: − ensure full transferability, settlement finality, and/or redeemability; − limit regulatory arbitrage, cliff effects and market fragmentation; and − take account of new and emerging cryptoassets ?

The cumulative nature of the conditions listed by the Committee, combined with the fact that there are only two groups in the proposed classification and that assets necessarily fall into Group 2 if they do not meet all these conditions, is problematic. Indeed, it means that cryptoassets with limited risks would be subject to the conservative treatment proposed (i.e. the application of a 1250% risk weight).

As explained previously, we believe that there should be more categories, based on additional conditions related to infrastructure and governance to ensure that the level of actual risks to which the banks are exposed is taken into account in an accurate way. Indeed, it seems to us that the proposed method, in addition to the nature of the cryptoassets considered, should take into account the nature of the distributed ledger technologies (DLT), between "permissioned" and "permissionless" ones, so that the real risks are properly understood. Indeed, as the consultative document states, "cryptoassets are defined as private digital assets that depend primarily on cryptography and distributed ledger or similar technology (FSB (2020)", which means that the existence of the assets depends on the infrastructure where they are stored and on the governance of this infrastructure. Very often, not only the ledger is decentralized (i.e. the asset is stored in many places at the same time), but also the governance is decentralized (i.e. there is no centralized legal entity which owns and governs the decentralized ledger and the coding is also decentralized). Those decentralized structures are very difficult to regulate or to pursue. They operate worldwide without any legal presence in a jurisdiction. Therefore, the focus cannot be only on the asset, as it exists only together with the infrastructure and the governance. For example, there is the possibility of hostile DLT takeovers by miners who can then alter its content without any limit or even delete it. When looking at a cryptoasset on a standalone basis, it could for example qualify as eligible high-quality liquid assets (HQLA), while the same asset would be classified in Group 2 if combined with the knowledge of the infrastructure and the governance.

Q4. For the first classification condition, is there an alternative methodology to assess the effectiveness of the stabilisation mechanism of Group 1b cryptoassets ? Would this proposed methodology be consistent with ensuring the effectiveness of the stabilisation mechanism while also being practical ?

It should first be noted that the focus on price fluctuation can produce false conclusions: when the operator of a stablecoin works very efficiently, he can ensure a limited price fluctuation even with a low level of collateral. In practice, there are several stabilisation mechanisms:

- full collateralisation with underlying (for each coin, there is one unit of Fiat) ;
- partial collateralisation with underlying (outstanding coins > Fiat collateral) ;
- collateralized with different assets than underlying (e.g collateralized with HQLA of pegged currency, collateralized with all other kinds of assets, even crypto…) ;
- algorithmic (supply demand control) without collateral.

Additionally the governance can be very different from one stablecoin to another. Stablecoins backed by fiat currency or bonds need a legal entity to manage the pool of assets, whereas other stabilisation mechanisms can be governed by fully decentralized autonomous protocols. Those using legal entities need sound principles of limitations on assets and maturities. USDC for example switched only recently to a cash and ST bond backed asset pool, before it used also corporate debt and CD's.

It means that the stabilisation mechanism should be analysed not strictly in terms of price fluctuation but also in terms of level of collateralisation, nature of collateralisation and solidity of the infrastructure and governance. Taking into account these different elements, the classification of the stabilisation mechanism and its governance should result in prudential treatment ranging from HQLA assets to Group 2 assets.

Given this diversity of possible approaches and their potential consequences in terms of stability, we believe that a regulation and a classification are needed to qualify the stabilisation mechanisms and the soundness of the governance and sorts the assets then in adequate sub-groups associated with an appropriate prudential treatment.

Combined with this need for regulation and classification, we also believe that for those issued by third parties, it should not be the responsibility of banks to check if the collateral is available and stored properly, as banks have little control over the underlying reserve pool and stabilization mechanism and cannot take over the tasks of auditors and supervisors.

Quantitative criteria

The Basel proposal includes a quantitative criteria for a cryptoasset to be designated as Group 1: the value of the cryptoasset shall not differ from that of the underlying traditional asset by more than 10bp more than three times over a 1 year period.

This criteria is very strict as 10bp in value is a very low threshold. It guarantees a near identical value at all time and hence hardly any added risk for the cryptoasset when compared to the underlying traditional asset. As a result of this strict criteria, few cryptoassets may end up being classified as Group 1. Besides, there will be a cliff effect when a cryptoasset stop meeting the criteria resulting in variability in risk weighted assets.

We believe that the proposed requirement could be loosened to no value differences in excess of [25bp] more than [10] times a year, adding hardly any credit risk when in the banking book and adding only limited basis risk when within the trading book. Indeed:

- the banking book capitalises primarily issuer risk over a 1 year horizon. The prospect to risk up to [0.25] for an investment worth 100 is hardly relevant in a banking book perspective ;
- in the trading book, which capitalises value risk over shorter horizons, it may add some basis risk but no primary delta risk.

We therefore propose a two-steps approach:

- Up to a tight limit (ex.: value difference not exceeding [10bp] more than [3] times a year), a cryptoasset would be considered as Group 1b and treated as an exposure to the underlying traditional asset.
- Up to a wider limit (e.g.: value difference not exceeding [25bp] more than [10] times a year), a cryptoasset would still be considered as Group 1b:
  - for banking book exposures, the risk weight could remain the one applicable to the underlying traditional asset given that [25bp] over a 1 year horizon is not really significant (25bp/8% ≈ 3% RW). Alternatively, the applicable risk weight could be that of the underlying trading asset plus a few percentage points, for example [+5%] ;
  - for trading book exposures, under the FRTB SA sensitivity based method, a basis correlation of [99.9%] may be introduced with exposures to the underlying traditional asset or other Group 1 cryptoassets of same underling traditional asset.
- Above this latter limit, a crypto would be considered as Group 2.

Q5. For the third classification condition, (i) would risk governance and risk control practices for Group 1 and Group 2 cryptoassets differ; and (ii) are there alternatives to the required risk governance and risk control practices that would ensure that material risks of the network are sufficiently mitigated and managed ?

The proposal set out in the Basel consultation document, in the "Box 1" section lays out the fundamental requirements for a good governance. We support the risk management framework for cryptoassets should be fully integrated into the overall risk management processes taking into account AML. We also agree that banks should implement risk management processes that are consistent with the high degree of risk of cryptoassets.

Whilst the Group 1 and Group 2 assets are different in nature, they remain cryptoassets. As such, there should be a set of requirements that will set out the minimum governance for all cryptoassets.

Generic risk governance framework is certainly a good start. However, we recommend that a governance scheme like the PCI-DSS, that is currently used for the payment card industry, is set out for the "cryptoasset industry". This is particularly important for cryptoasset custodian and web aspect of crypto-exchanges. Any such scheme should be designed to address various risks to a manageable level. Cryptoasset is a growing field, fairly recent and new to most people. In order to avoid any early big disappointment from a security stance, the directives to manage the risks should fairly prescriptive whilst allowing flexibility in the final implementation of controls. Whilst there will be various challenges to mandate these directives given the decentralised nature of the cryptocurrency landscape, these should at the very least set clear guidelines to support the security of cryptoasset operations especially for custodian of cryptoassets. Adherence to such guidance could set

The following are suggestions of what the guidelines should consider :

- Operational environment security and monitoring :
  - physical access control to networks handling cryptoassets (key/seed generation; key compromise; wallet creation; key storage ;
  - data & network controls (audit logs) ;

- security and resilience testing.

- Maintain an information security policy (security lifecycle management of assets/keys/wallets) :
- Build and maintain secure networks (trading platform resilience; incident response; access management including 3rd party management):
- Protection of identity of cryptoasset holders (whilst EU laws are underway to mandate that transactions are not anonymous, it might not be in the public interest or safe for the public to know who is behind each transaction. The identity of clients and their transactions should still benefit a fairly strong security. Assuming that by default all transactions will be processed securely, we therefore suggest:
    - data protection ;
    - anonymity protection when appropriate.
- Maintain vulnerability management program:
    - anti-virus ;
    - system & application security ;
    - cryptoasset specific vulnerabilities. Whilst the bank do not control or own cryptoassets, there should be provision made at the bank level to react to vulnerabilities impacting cryptoasset. As for example, there a recent vulnerability discovered in Monero impacted transaction privacy.
- Implement strong access control measure:
    - personal access control ;
    - physical access control.

Given the nature of cryptoassets we also would like to suggest (as set out in our draft response question2) that technology specific requirements at set out. Whilst this suggestion may not align with the same risk, same activity, same treatment, there should be further analysis to assess the impact of different technologies.

Q6. For the fourth classification condition, (i) to what extent would the regulation and supervision of entities that execute redemptions, transfers, or settlement finality of the cryptoasset reduce risk in cryptoasset exposures held by banks; (ii) which entities should/ should not be in scope of regulation or supervision ? For instance, are there entities involved in the transfer and settlement systems of cryptoassets (such as nodes, operators and/or validators) that should be excluded from the condition of required regulation and supervision ?

The regulation and supervision of entities that execute redemptions, transfers or settlement finality of cryptoassets would reduce the counterparty risk the bank takes on the exchange. It would also help to prohibit illicit activities AML/CFT, if the exchange has to trace back the operations. The regulation and supervision of the administrators of private keys would also contribute to protect the property rights of the owners.

Overall, in line with the “same risk, same activity, same treatment” principle, all cryptoasset service providers - custodians (i.e. wallet providers), trading platforms, exchange services fiat-to-crypto and crypto-to-crypto, execution, placing, reception and transmission of orders, advice… - should ideally be regulated and supervised, as soon as they provide one or more cryptoasset services to third parties on a professional basis, especially if these services are critical in the chain. Optimally, even professional/corporate miners should be regulated and supervised, because of the possibility of hostile blockchain takeovers by miners. It may seem unrealistic to consider being able to regulate all the participants in decentralized protocols, as they can be very numerous, small and localized across the globe. However, given the risks at stake, the issue of regulation and supervision of professional cryptoasset service providers should be carefully assessed. In any case, a strong international coordination between supervisors/jurisdictions is necessary for cryptoassets based on decentralized protocols.

Q7. Do you consider the responsibilities of banks and supervisors to be clear and appropriate ? Are there any other responsibilities for banks or supervisors that the Committee should consider ?

A case-by-case approach would be excessively costly and would create issues of legal uncertainty for banks. It would lead to different treatments from one bank to another and would create an unlevel playing field. Also, it could encourage banks to give up such activities, which would then be conducted only by non-banks, less regulated, less supervised and less able to manage the associated risks.

To avoid these problems, a centralized approach, based on guidelines and on a taxonomy to be developed by the regulator, is needed to ensure a consistent treatment across banks and jurisdictions and to prevent banks from being evicted from these activities.

Q8. Are there ways in which the increased operational risk relating to cryptoassets (relative to traditional assets) can be measured ? How should a pillar 1 add-on be designed to capture additional operational risks arising from exposures to cryptoassets ?

The Committee states that "given that cryptoassets, and the technologies on which they are based, are new and rapidly evolving, there is potentially an increased likelihood that they pose unanticipated operational risks" and that therefore these "risks could be addressed via the application of a Pillar 1 add-on operational risk charge for all Group 1 cryptoassets to which a bank is exposed."

It should be noted first that under the Basel III framework, for the banks that use the advanced measurement approach, these risks are already taken into account.

It should be borne in mind also that certain cryptoassets, in particular from Group 1, may contribute to the reduction of operational risks, notably by:

- increasing data accuracy and transparency ;
- reducing the risk of external fraud ;
- eliminating the risk of errors and the need for manual reconciliations ;
- minimizing the risk of disputes ;
- improving the identification of investors and hence better monitoring vs. AML-FT risks.

Concerning possible criteria for assessing the operational risks, the following could be taken into consideration :

- concentration of power at miners ;
- countries where miners operate ;
- intransparency of HR ressouces (programmers, design of the protocol) ;
- transparency on decision taking within the protocols / amendments of the protocol ;
- number of soft forks/hard forks, reasons for the forks ;
- successful attacks from hackers;
- cyber security risks applied to cryptoassets (with a focus on confidentiality, availability, integrity and traceability);
- increase in discussions on mistakes/incidents on social networks ;
- publications of exchanges like Coinbase/Binance ;
- delisting of cryptocurrencies by service providers (example Ripple when Ripple was pursued by the SEC);
- actions of other regulators or jurisdictions (example China against miners).

Q9. Are there further aspects of the credit risk and market risk requirements that could benefit from additional guidance on how they should apply to Group 1a cryptoassets ?

Credit risk mitigation

We agree with the Basel proposal that Group 1a cryptoassets shall be eligible collateral assets if the underlying reference is an eligible financial collateral under Chapter CRE22 subject to meeting the additional requirements set by the consultative document in Section 2.1.

On the other hand, we do believe that Group 1b cryptoassets may be eligible collateral as well despite the added counterparty risk to the redeemer that those cryptoassets may entail. It is our view that, if the underlying reference of a Group 1b cryptoasset is an eligible financial collateral under Chapter CRE22 and that the additional requirements of the consultative document Section 2.1 are met, then the exposure to the client may be mitigated as if the collateral provided was the underlying reference itself. However, to account for the added counterparty credit risk on the redeemer, the reduction of exposure to the initial counterparty should be capitalised as an exposure to the redeemer in the same way as an unfunded credit protection would be in the substitution approach.

For instance, let consider the following:

- a bank extend a loan to a Client for an amount of 100M ;
- the client provides a cryptoasset belonging to Group 1b for a value of 100M as collateral ;
- the underlying reference of the cryptoasset is an eligible collateral under Chapter CRE22 ;
- all additional requirements of Section 2.1 are met and in particular the cryptoasset liquidity is sufficient and similar to that of the underlying reference asset ;
- the applicable haircut to the underlying reference asset is HC.

In such case, the RWA for the risk mitigated loan is:

$$RWA = \left(100\text{M} - 100\text{M} \cdot (1 - HC)\right) \cdot RW_{Client} + 100\text{M} \cdot (1 - HC) \cdot RW_{Redeemer}$$

This approach is conservative since the counterparty credit risk on the redeemer only appears following the default of the client, i.e. losses (other than those related to the collateral value slippage captured in the haircut) only materialise when there is a joint default of the client and the redeemer. However, this approach has the merit to be simple and consistent with the substitution approach of the Basel framework.

Note that:

- in the instance where the Group 1b cryptoassets have no redeemer, there would be no added RWA than when using a Group 1a cryptoasset collateral ;
- this proposal may not apply to Group 2b cryptoassets as defined in our response to Q12.

Q10. Do you have any views on the Committee's current thinking on the capital requirements for Group 1b cryptoassets ?

Regarding stablecoins, the proposed Basel approach makes no distinction between fully collateralised, partially collateralised and uncollateralised stablecoins: in all circumstances the exposure to the redeemer is risk weighted as senior unsecure. The pool of collateral provides additional protection that should be recognised as risk reducing under some conditions. The applicable conditions or requirements would involve (but are not limited to):

- sound governance of the management of the assets in the pool ;

- sufficient equipment and staffing of the entity managing the asset pool ;
- accounting for the quality of the assets within the pool of collateral: the assets should be eligible collateral and their value haircut according to the prudential Basel framework rules ;
- there should be restrictions to the redeemer's use of collateral that will guarantee the size of the pool ;
- the collateral will be made available to the cryptoassets members in the event of the redeemer default in a timely manner ;
- limits on liquidity and interest rate transformation ;
- limits on credit risk in the collateral pool.

The risk reduction provided by the pool of collateral should be reflected in the applicable risk weight to the exposure to the redeemer in agreement with the Basel prudential rules.

In case of heavy outflows, the stablecoin manager has to liquidate the collateral pool. The assets in the collateral pool have to be sufficiently liquid. Liquidity, market and credit risk within the collateral pool should be limited and closely monitored. In fact, collateral pools of stablecoins could be compared to monetary funds and should be regulated in a similar way.

When the bank is a member providing access and redemption services in the cryptoassets to non-members holders, the bank is indeed at risk to purchase the cryptoassets from non-members if it has the legal obligation to do so or even, in some cases, if, without a legal obligation, it would be obliged to step-in. In which circumstances it make sense to capitalise the additional risk of having to buy the cryptoassets from the non-members as exposure to the redeemer since the risk materialise in the event of the redeemer's default. However, the proposed Basel approach fails to recognise that the risk may be mitigated in some instances, for example:

- if the legal commitments to purchase of all members exceed the outstanding amount of cryptoassets held by non-member holders, we may assume that the amount purchased from non-member holders following the default of the redeemer will be lower than the legal commitment amount ;
- in the event of the redeemer default, the cryptoasset value is bound to drop significantly so that the current value of the cryptoassets that the bank is legally committed to purchase largely overstate the actual amount the bank will have to pay to the non-member holders in the event of the redeemer default.

Hence, a credit conversion factor of 100% appears way too high in most cases. We would recommend that such legal commitment (or step-in exposure) CCF be reviewed downward.

In the instance where the bank is a non-member holder of cryptoassets relying on members to redeem, the bank is at risk of all members defaulting, leaving the bank with no option to redeem its cryptoassets. The Basel proposal consists in adding risk weighted assets to the exposure to the members using the risk weight of the member of lower risk weight. However, this approach fails to recognise that the risk is only materialising if all members default, resulting in a very rare occurrence of such event. In effect, the risk weight should be adjusted downward to reflect the low probability of a joint default of all members. Besides, in such event, the redeemer would likely look for solutions, for instance giving member status to new entities, such as the risk would not be on the full value of the cryptoassets but rather a slippage risk for not being able to redeem for a period of time. If we were to draw a parallel with client clearing, the client risk weight to the clearing member is zero when the clearing member is pass-through, omitting the very remote risk of all clearing members defaulting simultaneously. Hence, for stablecoins with a sufficiently resilient framework, the applicable risk weight to the members should be low, lower than that of any of the member applicable risk weight, as such reflecting the low probably occurrence of a joint default of all members. It could even be set to zero when enough safeguards exist and some requirements are met, considering the very remote risk entailed.

Q11. What further aspects of the credit risk and market risk requirements could benefit from additional guidance on how they should apply to Group 1b cryptoassets ?

As stated in our answer to Q10, we think that a limitation of credit risk and market risk in the collateral pool is necessary to protect holders of stablecoins.

Collateral pools are exposed to defaults of issuers of bonds. They are also exposed to widening credit spreads and to increases in interest rates when the collateral is composed of fixed rate bonds. As well, as some stablecoins have become very important in size, a run on such stablecoins could trigger massive liquiditation of collateral and a deterioration of prices on assets held in the pool.

Therefore the regulator should apply additional rules similar to those applicable to monetary funds.

Q12. Do you think the proposed capital treatment of Group 2 cryptoassets, including the application of a 1250% risk weight instead of deducting the asset from capital (for the reasons explained above), appropriately reflects the unique risks inherent in these assets ?

Group 2 cryptoassets, as currently defined, are a very large group that encompasses a very broad range of assets, with multiple embedded risks, ranking from utility tokens to physical bitcoin, including as well cryptoassets that behave like Group 1 assets from a credit/market risk point of view but that have failed a single condition required to be categorized as Group 1. Not only this Group 2 captures a very large group of assets, but the proposed capital treatment should be extended to funds of Group 2 cryptoassets, and also to "other entities, the material value of which is primarily derived from Group 2 cryptoassets". This latter definition is not sufficiently precise and could potentially capture a lot of corporates that are linked to the value of Group 2 cryptoassets (as an example, would Microstrategy or Tesla shares be treated as Group 2 cryptoassets on the back of Tesla holdings a significant amount of Bitcoins for its treasury management ?).

The proposed capital treatment is not risk sensitive at all, to say the least since :

- it does not make any distinction between very different Group 2 cryptoassets ;
- as a result, is much too conservative for some of the Group 2 cryptoasset exposures ;
- it does not recognise any netting benefit between long and short positions in the same underlying cryptoasset ;
- it fails to properly capitalise some complex derivatives (unless a more risk sensitive approach is used such as the FRTB sensitivity based method as suggested on page 15 of the Basel consultative document).

In this context, we believe that the Committee should consider a more granular categorisation for Group 2 cryptoassets. If the intention is not to propose here a precise and definitive taxonomy, we present a simple proposal to divide the Group 2 in three sub-groups :

- Sub-Group 2a would bring together high-risk cryptoassets, i.e. the ones with no intrinsic value because not explicitly and directly linked to, or backed by, assets with intrinsic values.

  A proper risk sensitive framework should be defined for those cryptoassets while retaining some specific elements of conservatism until when sufficient hindsight in Group 2a cryptoassets is reached. Failing to devise an alternative framework to the one proposed for Group 2 cryptoassets, a framework that would have added risk sensitivity and in particular that would recognise netting

benefits between long and short positions in the same underlying cryptoassets, would prevent banks to participate in his market and serve their clients.

Typically, banks are bound to develop some businesses in the future to meet the increasing client's demand as per their core function of intermediary to execute, clear, settle, custody, finance (or even acting as a market maker). Those core strategies of a banking activity generally use listed cash-settled derivatives (i.e. not physically settled), with no direct access to the blockchain.

- Sub-Group 2b would relate to tokenised traditional assets and cryptoassets with stabilisation mechanism that do not meet all the conditions required to qualify as Group 1 cryptoassets but do meet those conditions ensuring that credit and/or market risks are not much different to that of the underlying traditional assets.

Such a distinction would allow a prudential treatment for credit and market risk similar to that of Group 1b cryptoassets. Additional risks resulting from not meeting all conditions for a Group 1 classification should result in add-on capital charges, for instance in the form of added operational risks.

- Sub-Group 2c would relate to utility tokens, i.e. tokens that may enable access to a specific product or service (loyalty programs, gift card rewards, cloud…).

Further analysis should be conducted to devise a capital treatment that reflect adequately the true risk on exposures to utility tokens.

In any case, in accordance with the iterative approach supported by the Committee, as the environment around cryptoassets is moving very fast with a variety of initiatives across the world, there is bound to be a need to have an improved granularity compared to the 3 classes proposed here as a first step toward a comprehensive prudential framework.

Q13. Are there alternative approaches that the Committee should consider that are simple, conservative and easy to implement ? For exposures in the trading book, would it be appropriate to permit recognition of hedging via the application of a modified version of the standardised approach to market risk ?

As per our answer to Q12 and our proposed categorization into 3 sub-groups, we believe that distinct approaches should apply depending on the classification to the Group 2 sub-groups. Besides, we may distinguish between banking book exposures and trading book exposures.

Credit risk of Banking Book exposures

Banking book exposures consist primarily in assets' holdings, in this instance cash position in cryptoassets. For those banking book exposures that are risk weighted 1250%, banks should have the option to deduct from own funds their investments in lieu of risk weighting them at 1250%.

The risk weight applicable to Group-2 cryptoassets banking book holdings should depend on the riskiness of the cryptoassets which, in turn, depends on the Sub-Group they belong to.

- Sub-Group 2a cryptoassets have no issuer risk, only value risk. It therefore make sense to capitalise banking book Sub-Group 2a cryptoasset exposures in the market risk framework, similarly to foreign exchange risk in the banking book.
However, for as long as in the trading book Sub-Group 2a cryptoasset are weighted at 100% in the FRTB Sensitivity Based Method (pending further review of the prudential treatment of

cryptoassets), we may choose to alternatively risk weight separately Sub-Group 2a banking book exposures at 1250% or deduct them from own funds.
- Since Sub-Group 2b cryptoassets are no different to cryptoassets of Group 1 when it comes to credit risk, the applicable risk weight shall be identical to that of the Group 1 cryptoassets.
- Finally, Sub-Group 2c cryptoassets deserve further thoughts and analysis.

Derivatives referencing cryptoassets (at the exception of hedges to banking book exposures) and any short positions in cryptoassets should generally be part of the trading book where an adequate capital framework could be devised.

Market and credit risks of Trading Book exposures

The effective framework for capitalising market and credit risk in the trading book is the FRTB. We see no reason why trading book positions in cryptoassets should be subject to a specific prudential framework. However, we recognise that adaptations to the framework are needed in places to cope for the uniqueness of crypto exposures when compared to the asset classes covered by the FRTB. Besides, we may introduce, initially, some elements of conservatism which should be reviewed in due time when more experiences are gathered on cryptoassets.

In the section (b) of annex 2 of the consultative document, it is stated that using market risk rules will have two drawbacks: being more complex and forcing a separate approach for credit risk and market risk. We do not understand those concerns. Surely a bank having cryptoasset exposures in its trading book also holds exposures to traditional assets for which it is able to calculate the FRTB capital charge. There is no added complexity in capitalising exposures to cryptoassets in the market risk framework. Besides, distinguishing between trading book and banking book is a general feature of the prudential framework. Why should we not do so when it comes to cryptoasset positions ? The trading book holds exposures with trading intent characterised by long and short positions that diversifies or offsets and that are held over a much shorter period of time. Those features should be reflected in the capital charge framework.

Our proposed alternative approach consists in the below, where Sub-Groups are distinguished:

- Sub-Group 2a cryptoassets should be capitalised with conservatism to begin with. For this reason it may be prudent, as suggested in the consultative document:

    - to only allow the FRTB standardised approach ;

    - to apply the conservative weight of 100% for all of Delta, Vega and Curvature capital charges (equivalent to a 1250% risk weight in the banking book) ;

    - to not allow any offsetting and diversification across Sub-Group 2 cryptoassets.

  At the same time, we believe that the exposures on the same underlying cryptoasset should be allowed to net. As a result, our proposal would be to capitalise cryptoassets in the same way as equities in the “Other sector” bucket [MAR21.79], simply using a weight of 100% instead of 70%. A time to maturity dimension may be added to the delta risk factors. For instance, the same approach as for the Commodity asset class may be used [MAR21.13(1)], defining a correlation ρ_{tenor} between weighted sensitivities mapped to different tenors [MAR21.83(2)].

  Finally, the framework should be reviewed periodically as experience in cryptoassets increases and the history of data lengthened, in line with the iterative process proposed in the Introduction of the consultative document. It may ultimately lead to, depending on the outcome of the reviews, lower FRTB SBM weights, diversification benefit across Sub-Group 2a cryptoasset exposures and eligibility to the internal model approach.

- Sub-Group 2b cryptoassets consist in cryptoassets that are not unlike Group 1 cryptoassets in term of market and credit risks. As a result, it would make sense to capitalise their market and credit risk in the same way as Group 1 cryptoassets.

For market risk, that would mean using the FRTB approach applied to the traditional asset underlying reference either in the standardised approach or the internal model approach if the bank has received approval for its internal model on the reference traditional asset and have successfully passed the eligibility tests (back-testing, P&L attribution test). However, depending on the characteristics of the cryptoasset, full netting between the cryptoasset and its underling traditional asset may be disallowed. In the standardised approach, this basis is materialised by a correlation (ρ_{basis}) between exposures to the traditional asset and exposures to the cryptoasset. Mechanically, this would translate in the internal model approach, in the requirement to model the basis risk factor [MAR31.3]. A default risk charge may also apply if the referenced traditional asset bears issuer risk.

- Sub-Group 2c cryptoassets, given their specificities, should be subject to a specific prudential treatment to be determined.

Counterparty credit risk: collateral recognition

Collateral eligibility, collateral haircutting and margin period of risk (MPoR) length (collateralised netting sets) of Sub-Group 1a, 1b cryptoassets should follow the rules applicable to the referenced traditional assets. The same apply to Sub-Group 2b cryptoassets if the failed condition required to qualify as Group 1 cryptoassets does not entail additional uncertainty in the Sub-Group 2b crypo asset value.

However, the cryptoassets liquidity, when lower than that of the referenced traditional assets, should be taken into account in the determination of collateral eligibility, collateral haircutting and MPoR. Determining the cryptoassets liquidity should not rely solely on the time needed to liquidate but as well on the ability to hedge with the referenced traditional asset or another Sub-Group 1a, 1b or 2b cryptoasset referencing the same traditional asset.

Sub-Group 2a cryptoassets may not be eligible collateral at this point of time, however, in the longer run, the eligibility of Sub-Group 2a cryptoassets may be reviewed.

Counterparty credit risk: derivatives exposure

The Basel proposal for Group 2 (which in our approach relates only to Sub-Group 2a) cryptoassets is overly conservative.

We agree that, initially, only the standardised approach for counterparty credit risk of derivatives (SA-CCR) may be used for netting sets including derivatives with Sub-Group 2a cryptoasset underlyings. Alternatively, a netting set could be split into two synthetic netting sets, one with no derivatives referencing Sub-Group 2a cryptoassets, the other one including derivatives referencing Sub-Group 2a cryptoassets. The exposure on the former synthetic netting set will be calculated with whichever method the bank usually use while the exposure of the latter synthetic netting set will use mandatorily SA-CCR.

Under SA-CCR, the approach may be made more risk sensitive, closer to the general SA-CCR framework while still remaining conservative. Our proposal would consist in:

- not mandatorily isolating in hypothetical netting sets Sub-Group 2a cryptoassets ;
- a replacement cost calculated in the usual way, allowing netting between all transactions ;
- a distinct add-on for each Sub-Group 2a cryptoassets underlying ;
- for a Sub-Group 2a cryptoasset, netting should be recognised in the calculation of the add-on ;

- the cryptoasset add-ons of all cryptoasset underlyings are added (simple sum) with the usual asset classes add-ons [CRE52.25] in the potential future exposure (PFE) calculation [CRE52.23].

Hence, our approach to counterparty credit risk is consistent with our market risk approach, relying largely on existing methodologies with added conservatism (no diversification and offsetting between different Sub-Group 2a cryptoassets). As for market risk, the process shall be iterative with periodic revision leading progressively to a more risk sensitive approach.

Q14. Do you have any views on the Committee's current thinking regarding the leverage ratio, large exposures framework and liquidity ratio requirements ? Are there further aspects of these requirements that could benefit from additional guidance ?

The Committee explains that it is of the view that cryptoassets would not qualify as eligible HQLA. It points out however that it "will continue to investigate the prospect of recognising as HQLA those cryptoassets that […] are deemed to be equivalent to traditional assets that themselves qualify for inclusion in HQLA". At the same time, in its introductory remarks on the general principles guiding its paper, the BCBS states about the "same risk, same activity, same treatment" principle that "a cryptoasset that provides equivalent economic functions and poses the same risks compared with a "traditional asset" should be subject to the same capital, liquidity and other requirements as the traditional asset." In our view, the lack of recognition of Group 1a tokenised traditional assets as high-quality liquid assets (HQLA) would be inconsistent with their capital treatment and with the "same risk, same activity, same treatment" principle. To be consistent, where the traditional assets, e.g. government bonds, qualify as HQLA, then the equivalent tokenised assets should also be eligible, provided of course that they present similar characteristics to those of the HQLA-eligible assets. We even consider that some cryptoassets with stabilisation mechanisms should be able to be recognized as HQLA if they meet the relevant qualifying criteria established by the Committee.

Q15. Do you have any views on the responsibilities of banks ? Are there any other responsibilities or aspects that should be covered by banks for the purposes of the supervisory review ?

A first remark concerns the statement that "Banks with direct or indirect exposures to any form of cryptoasset should ensure that risks not captured under the Basel framework are assessed, managed and appropriately mitigated on an ongoing basis". The wording ("risks not captured under the Basel framework") is surprising since the risks in question are in principle already taken into account under operational risk.

Operational and cyber risk

The cyber-threats mentioned in the consultative document (cryptographic key theft; compromise of login credentials; and distributed denial-of-service (DDoS) attacks…) are good examples of actual risks. In view of these risks, we support the idea that the surveillance, in terms of Information, Communication and Technology (ICT) risk, should encompass at least, as suggested by the Committee:

- governance requirements and risk management requirements on ICT risk ;
- ICT related incidents ;
- requirements on testing of ICT tools and systems ;
- requirements on ICT third-party risk management.

An approach in this respect could be to use market standards in terms of cyber risk by referring to the CIA triad (Confidentiality, Integrity, Availability).

Underlying technologies

As proposed, banks or any third party in charge shall be limited to the monitoring of the applied technologies and shall not be required to remediate (unless the cryptoasset is on a private DLT, under the responsibility of a dedicated public consortium / entity). In terms of risk management, when a risk cannot be mitigated (which is the case when there is no control over the underlying technology), you can accept it or stop the activity or make a transfer (take insurance, for example).

About the issue of stability of the distributed ledger technology (or similar technology network), one has to note that it can be extremely complex in the case of the public DLT.

Concerning the service accessibility, if private keys are retained by the client, mechanisms exist (key constrict) but they are organizationally complex. Indeed, key management shall be using key escrow mechanism in order to provide recovery mechanisms, which can be provided only by a third party and not by the bank.

Money laundering and financing of terrorism

As regards anti-money laundering and countering the financing of terrorism, we do support that the banks, in all their activities related directly or indirectly to cryptoassets, should apply the risk-based approach as set out by the Financial Action Task Force (FATF), in line with the BCBS' proposal.

Q16. Do you have any views on the responsibilities of supervisors ? Are there any other responses that could be considered by supervisors when conducting supervisory review ?

Supervisors should assume a greater and specific responsibility for crypotassets based on decentralized protocols. The decentralisation even implies in fact the development of a dedicated cooperation between supervisors. Also, as stated in the reply to question 1, a central list of approved Group 1 cryptoassets would be extremely useful to avoid a divergent treatment among supervisors, particularly in the case of decentralized protocols.

Q17. Do you have any views on the adjustments to minimum Pillar 1 capital requirements to capture additional credit and/or market risk ? Are there any other potential modifications that supervisors may need to consider ?

-

Q18. Do you have any views on the potential design of disclosure requirements ?

We share the view that disclosure requirements for banks' exposures to cryptoassets or related activities should follow the general guiding principles for banks' Pillar 3 disclosures in the Basel Framework.

Contact

Hubert d'Etigny - hubert.detigny@bnpparibas.com

BNP Paribas - Group Public Affairs
3, rue d'Antin
75002 Paris - France