CRAVATH, SWAINE & MOORE LLP

David L. Portilla
+1-212-474-1410
dportilla@cravath.com

Will C. Giles
+1-212-474-1828
wgiles@cravath.com

Basel Committee Issues Second Consultation on Prudential Framework for Cryptoasset Exposures

July 11, 2022

The Basel Committee on Banking Supervision ("BCBS") recently published a [second consultative document](#) on the prudential treatment of cryptoasset exposures (the "Consultation") to address issues raised in comments in its initial consultative document published in June 2021 (see our prior analysis [here](#)). In the Consultation, the BCBS outlined classifications of different cryptoassets and minimum capital requirements based on various risks. The Consultation also outlined how regulators should supervise banks with cryptoasset activities and how banks should disclose those activities. Comments are due by September 30, 2022.

KEY TAKEAWAYS

- The addition of formal standards text and the expectation of finalizing the rule by the end of 2022 suggest that the BCBS is prioritizing cryptoassets and believes its policy process on the appropriate prudential treatment is advanced.

- The final standards could shape aspects of the cryptoasset ecosystem. For example, stablecoins may be designed to qualify for a less punitive capital treatment provided in the Consultation, in order to encourage banks to hold or otherwise interact with such stablecoins.

- The Consultation responded to many comments on BCBS's initial consultative document. The BCBS continues to take a conservative approach to banks' involvement in cryptoasset activities. For example, banks would appear to be required to receive supervisory approval to apply anything other than a 1250% risk weight to a cryptoasset. Therefore, although it may not prevent banks from engaging in cryptoasset activities, it is unclear whether the Consultation would allow banks to engage in such activities at scale or calibrate the prudential treatment so that cryptoasset activities may come within the prudential regulatory perimeter.

- The Consultation applies to both "on- and off-balance sheet amounts that give rise to credit, market operational and liquidity risks". Although the Consultation notes that it applies to "non-fiduciary custodial services[] that may only give risk to operational risk", it is unclear whether or how the regulators expect the Consultation to address on-balance sheet assets created by the Securities and Exchange Commission's Staff Accounting Bulletin 121, which could require certain banks to create new on–balance sheet exposures due to banks' non–fiduciary custodial and other activities related to cryptoassets.

CHANGES FROM THE FIRST CONSULTATIVE DOCUMENT

The Consultation responds to many of the comments the BCBS received from the initial consultative document. The BCBS's changes include:

- Establishing a new cryptoasset classification (*i.e.*, "Group 2a") and updating the classification conditions to provide further details and new qualification tests.

- Including a new infrastructure risk "add-on" to cover the risk of infrastructure for Group 1 cryptoassets.

- Recognizing to some degree hedging for the new Group 2a cryptoassets.

- Providing that cryptoasset exposures are not subject to the deduction requirement that applies to intangible assets, even in cases where the cryptoasset is classified as an intangible under the applicable accounting standard.

- Providing clarification on operational risks and more details on the application of the liquidity coverage ratio ("LCR") and net stable funding ratio ("NSFR").

- Adding a Group 2 exposure limit as a percentage of tier 1 capital.

- Providing additional details through a standards text—*SCO60: Cryptoasset Exposures*—for inclusion in the Basel Framework.

CATEGORIES OF CRYPTOASSETS

The Consultation applies to "cryptoassets", which are "private digital assets that depend primarily on cryptography and distributed ledger or similar technology". A digital asset is "a digital representation in value which can be used for payment or investment purposes or to access a good or service". Central bank digital currencies are "digital representations of fiat currencies" and are excluded from the scope of the Consultation.

The Consultation categorizes cryptoassets into two groups, each with two subgroups. Group 1 consists of cryptoassets that pass the Group 1 classification conditions. This group is subdivided into:

- Group 1a: Tokenized traditional assets (*i.e.*, tokenized versions of assets that are captured within the Basel Framework and not within the Consultation) that meet the Group 1 classification conditions.

- Group 1b: Cryptoassets with stabilization mechanisms (aka "stablecoins") that is effective at all times that meet the Group 1 classification conditions.

Group 2 consists of cryptoassets that do not meet the classification conditions. This group is subdivided into:

- Group 2a: Cryptoassets that pass Group 2a hedging recognition criteria.

- Group 2b: All other cryptoassets.

Supervisory approval would be necessary to classify a cryptoasset as anything other than Group 2b, which is the category associated with the most conservative capital treatment. In addition, banks generally would be required to screen cryptoassets on an ongoing basis to determine classification.

GROUP 1 CLASSIFICATION CONDITIONS

The Consultation outlines four classification conditions to be considered a Group 1 cryptoasset.

Condition 1

The first condition would require the cryptoasset to be either a tokenized traditional asset or have an effective stabilization mechanism. For a tokenized traditional asset to meet the this classification condition, it must:

- Be a digital representation of a traditional asset using cryptography, distributed ledger technology ("DLT") or similar technology.

- Pose the same level of credit and market risk as the traditional form of the asset. This means that the cryptoasset would need to confer the same level of legal rights as the traditional form of the asset.[1]

To meet the first classification condition, a cryptoasset with an effective stabilization mechanism must:

- Be designed to be redeemable for a predefined amount of reference assets (the "peg value").

- Have a stabilization mechanism designed to minimize fluctuations in value relative to the peg value.

- Have a stabilization mechanism that allows for risk management similar to that of traditional assets.

- Have significant information for banks to verify the ownership rights of the reserve assets behind the cryptoasset. (Evidence would need to be provided to satisfy supervisors of the effectiveness of the stabilization mechanism, including composition, valuation and frequency of valuation of the reserve assets and the quality of available data.)

- Meet the "redemption risk" test. To help ensure that the reserve assets are sufficient at all times to ensure redemption for the peg value, the Consultation includes a two-part test for the value and composition or reserve assets, as well as the management of reserve assets.

  - The value of reserve assets at all times (including during extreme stress) must equal or exceed the aggregate peg value. If the reserve assets expose the holder to risks other than those arising from the reference assets, the reserve assets would need to be sufficiently overcollateralized to ensure that their value would exceed the aggregate peg value after stress losses.

  - The governance and management of reserve assets would be comprehensive and transparent and would ensure, among other things, that a robust operational resilience framework exists, the value of the reserve assets are disclosed at least daily and their composition disclosed at least weekly. In addition, there should be an explicit legally enforceable objective of ensuring that all cryptoassets can be redeemed promptly at the peg value, including under periods of extreme stress, and the reserve assets should be subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

- Meet the "basis risk" test. A holder of a cryptoasset must be able to sell the asset in the market for an amount close to the peg value. If the peg value exceeds the market value by 10bp no more than three times (based on number of days in which the breach is observed) over the past 12 months, the cryptoasset has "fully passed".[2] If peg value exceeds the market value more than 20bp more than 10 times over the past 12 months, the cryptoasset has failed. If it has neither "fully passed" nor failed, it has "narrowly passed".

- RWA Adjustment for "Narrowly Passed" Cryptoassets: Cryptoassets that narrowly pass are still considered to have met the classification conditions for Group 1b, but are subject to a risk-weighted asset ("RWA") adjustment. For exposures in the banking book, the credit RWA would be increased by 100% of the exposure value. For exposures in the trading book, the market RWA would be increased by 100% of the exposure value.

- Be issued by an institution that is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements. Importantly, the Consultation states that the BCBS is considering this test as an *alternative* to the redemption risk and basis risk tests above.

- Not be an algorithmic stablecoin or reference other cryptoassets as underlying assets.

Condition 2

The second classification condition would require that all rights, obligations and interests arising from the cryptoasset are clearly defined and legally enforceable in the jurisdiction in which it is issued and redeemed. In addition, the legal framework should ensure settlement finality. This classification condition requires that:

- Cryptoasset arrangements would need to include full transferability and settlement finality. Cryptoassets that have stabilization mechanisms would be required to be redeemable within five calendar days of a request.

- Unless the offering of the cryptoasset has been approved by the relevant regulator, banks would be required to receive an independent legal opinion confirming that arrangements (*e.g.*, redemption obligations for stablecoins) are properly documented.

Condition 3

The third classification condition focuses on ensuring that the network on which the cryptoassets operate is designed to mitigate and manage material risks. This condition would be satisfied when functions of the cryptoasset network, such as issuance, redemption, validation and transfer, and the network itself do not pose any material risks to implementation of those functions. Companies should have governance and risk management policies in place to address credit, market, operational, liquidity, data security and anti–money laundering risks. Networks that fulfill this condition have well–defined key aspects. These include: operational structure, degree of access, technical role of nodes and validation mechanisms.

Condition 4

The fourth classification condition would require that entities that execute redemptions, transfers, storage or settlement, or entities that would manage and invest in reserve assets, are regulated and supervised or subject to appropriate risk management standards. Entities subject to this condition include operators of transfer and settlement systems, wallet providers, administrators of stabilization mechanisms and custodians of reserve assets.

MINIMUM CAPITAL REQUIREMENTS FOR CREDIT RISK FOR GROUP 1 CRYPTOASSETS

For Group 1a cryptoassets:

- Generally, tokenized assets would be subject to the same credit RWA as the non-tokenized, traditional form of the asset (assuming the former confers the same level of legal rights and likelihood of on-time payment as the latter).

- The Consultation notes, however, that there are areas of credit standards that try to capture risk that are not associated with legal rights. Banks should assess those risks too and not simply assume a given course of treatment because of the treatment of the traditional asset.

For Group 1b cryptoassets:

Banks with banking book exposures to Group 1b cryptoassets would be required to analyze their structure and identify all risks that could result in a loss. Each credit risk should then be separately capitalized. Risks for 1b cryptoassets can arise from the following (though the Consultation notes that the list is not exhaustive):

- <u>Risk from reference asset</u>:
  - Banks should apply the credit RWA that would apply to the underlying asset. If the asset gives rise to a foreign exchange or commodity risk, banks should apply the market RWA that would apply to a direct holding of such an asset.
  - If the underlying asset is a pool of assets, banks should apply the requirements applicable to equity investments in funds.

- <u>Risk of default of the redeemer</u>:
  - If the bank has an unsecured claim on the redeemer, the bank would be required to calculate a credit RWA equal to the credit RWA that would apply for a direct unsecured loan (with the amount equaling the amount of the redemption claim) to the redeemer. If the claim is instead secured, the RWA would be equal to the credit RWA that would apply for a direct, secured loan.
  - Banks would not be required to calculate this credit RWA if (1) the underlying, reserve assets are held in a bankruptcy remote special purpose vehicle on behalf of the cryptoasset holders, who have direct claims to the underlying reserve assets and (2) the bank has received an independent legal opinion affirming that relevant courts would recognize such an arrangement.

- <u>Risks arising when intermediaries perform the redemption function</u>:
  - o The Consultation provides additional requirements for stablecoin arrangements in which only a subset of holders ("members") are permitted to redeem cryptoassets directly from the redeemer.
  - o Where a bank is a member and has committed to buy cryptoassets from non-member holders, the bank would need to include the RWAs of the cryptoassets (1) it is legally obligated to purchase and (2) it would nonetheless be obliged to purchase in order to satisfy expectations and protect the bank's reputation (if the bank or its supervisor determines such step-in risk exists).
  - o When members have committed to buy cryptoassets in unlimited amounts and a bank is a non-member holder, the bank would be required to sum the risk of the changing value or potential default of the reserve asset and the risk that all members default. When members have not committed to buy in unlimited amounts, the non-member bank would be required to sum such risks and the risk that the redeemer defaults.

MINIMUM CAPITAL REQUIREMENTS FOR MARKET RISK FOR GROUP 1 CRYPTOASSETS

The Consultation provides additional detail regarding how banks should apply the simplified standardized approach (the "SSA"), the standardized approach (the "SA") and the internal models approach (the "IMA") for calculating minimum risk-based capital requirements for market risk. Examples of this additional detail include:

- For the SSA, all instruments including derivatives and off-balance sheet positions that are affected by changes in Group 1 cryptoassets should be included, and netting and hedging are recognized between Group 1a/b cryptoassets and the traditional assets they represent/reference.

- For the SA, the Consultation would require that the cryptoassets be mapped to the current risk classes under the sensitivities-based approach wherein the cryptoasset is decomposed into the traditional asset(s) the cryptoasset represents/references. The default risk capital ("DRC") requirements should be equivalent to those of the traditional asset, and banks should use the same approach for redeemer default risk as they did in the credit risk section.

- For the IMA, the non-DRC allows mapping of exposures similar to that for the SA (discussed above). Banks would not be permitted to use IMA for instruments referencing Group 2 assets.

INFRASTRUCTURE RISK ADD-ON FOR GROUP 1 CRYPTOASSETS

Although the BCBS expects to review whether the additional amount continues to be necessary in the future, banks would be required to include an add-on for infrastructure risk since many of the technologies, such as DLT, that underly the cryptoassets are new. For both banking and credit book exposures, the total credit/market risk RWA would be increased by 2.5%.

However, the add-on does not apply to Group 1a assets that are backed by the full faith and credit of a central bank or sovereign entity.

GROUP 2a HEDGING RECOGNITION CRITERIA

A Group 2a cryptoasset can be a:

- Direct holding of a spot Group 2 cryptoasset where there exists a derivative or exchange-traded fund ("ETF") or exchange-traded note ("ETN") that is traded on a regulated exchange that solely references the cryptoasset.

- Cash-settled derivative or ETF/ETN that references a Group 2 cryptoasset, where the derivative or ETF/ETN has been explicitly approved by a jurisdiction's markets regulators for trading or the derivative is cleared by a qualifying central counterparty.

- Cash–settled derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion in the bullet immediately above.

- Cash–settled derivative or ETF/ETN that references a cryptoasset-related reference rate published by a regulated exchange.

A Group 2a cryptoasset would be required to:

- Be highly liquid (meaning that, over the previous year, the average market capitalization was at least USD $10 billion and the 10% trimmed mean of daily trading volume with major fiat currencies was at least USD $50M million); and

- Have sufficient data associated with it (meaning at least 100 price observations over the previous year and sufficient data on trading volumes and market capitalization).

A Group 2 cryptoasset would be required to be classified as a Group 2b cryptoasset unless the bank demonstrates to the supervisor that the cryptoasset meets the criteria above.

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

For Group 2a cryptoassets (*i.e.*, cryptoassets that pass the Group 2a hedging recognition criteria described above), the capital requirements should be calculated by a modified version of the SSA or the SA. This treatment permits some recognition of hedging.[3]

For cryptoassets in Group 2b, there is not a separate trading book and banking book treatment. The more conservative approach is designed to capture both credit and market risk. For each Group 2b asset, banks would be required to apply an RWA of 1250% to the greater of the absolute value of the aggregate long and short positions.

CAPITAL REQUIREMENTS FOR CREDIT VALUATION ADJUSTMENT ("CVA")

Group 1a cryptoassets would generally be subject to the same treatment for CVA as the non-tokenized version of the assets. Banks would still need to assess the tokenized asset since qualification for a given treatment does not always follow that of the non-tokenized asset. For example, the Consultation states that the standardized approach ("SA-CVA") may not be applied to Group 1a cryptoassets in certain cases where sufficient data is not available.

Group 1b cryptoassets would be subject to the same capital requirements for CVA as the non-tokenized assets.

Group 2a cryptoassets would only be subject to the basic approach ("BA-CVA"). The SA-CVA is not available for derivatives and securities financing transactions referencing Group 2a cryptoassets.

See above for capital treatment of Group 2b cryptoassets.

MINIMUM CAPITAL REQUIREMENTS FOR COUNTERPARTY CREDIT RISK ("CCR")

Groups 1a and 1b generally would be subject to the same CCR rules as the non-tokenized asset; this includes the internal models method ("IMM"). However, for Group 1a, problems with data availability may require application of the standardized approach ("SA-CCR").

Group 2a cryptoassets would follow a modified SA-CCR, which includes a new asset class "crypto". There would be separate hedging sets for each "crypto currency" priced in applicable fiat currencies or in another Group 2a "crypto currency".

Group 2b cryptoassets calculate the exposure for CCR as the sum of the replacement cost and the potential future exposure ("PFE") multiplied by an alpha factor, where the PFE is calculated as 50% of the gross notional amount.

Netting sets containing derivatives related to Group 2b assets and other assets would be split into two (separating Group 2b assets from other assets).

MINIMUM CAPITAL REQUIREMENTS FOR OPERATIONAL RISK

The operational risk resulting from cryptoasset activities should generally be captured in the operational risk standardized approach through the business indicator (which should include income and expenses resulting from activities relating to cryptoassets and through the internal loss multiplier (which should include operational losses resulting from cryptoasset activities). To the extent that operational risks are not sufficiently captured in minimum capital requirements, banks and supervisors also should take appropriate steps to ensure capital adequacy and sufficient resilience in the context of the supervisory review process.

MINIMUM LIQUIDITY RISK REQUIREMENTS

Generally, the calculation of the LCR and the NSFR would follow treatments when calculating exposures of similar risks.

Group 1a cryptoassets that are tokenized versions of high-quality liquid assets ("HQLA") can be considered HQLA, but only if they separately satisfy the characteristics of HQLA. In contrast, Group 1b and Group 2 cryptoassets may not be considered HQLA.

Specific parameters for LCR and NSFR treatment are outlined below, depending on the scenario.

- Tokenized claims on a bank: Group 1a tokenized claims on banks would be treated as unsecured funding instruments when they are issued by a regulated and supervised bank, represent a legally binding claim on a bank, are redeemable at par value in fiat currency and have a stable value. The Consultation provides a number of additional considerations, including:

  o The maturity is based upon contractual redemption rights available to the holder.

  o For liabilities from own–issued tokenized claims on a bank, the LCR outflow rates and NSFR available stable funding factors would be based on the earliest date the liability could be redeemed, and the associated liabilities would not be treated as stable retail deposits.

  o If a bank holds another bank's tokenized liability, the holder would not recognize inflows in the LCR if the liability is not redeemable in 30 days or if it is held for operational purposes.

- Stablecoins: Group 1b assets (as well as certain Group 2 stablecoins[4]) would be treated similar to securities, subject to a number of considerations, including:

  o If the bank is the issuer and stablecoin represents legally binding claims on the bank, the bank should recognize 100% outflows in the LCR if the stablecoin is redeemable within 30 days.

  o If the bank holds a stablecoin on its balance sheet, it would generally be subject to an 85% required stable funding ("RSF") factor in the NSFR and not result in LCR inflows. Exceptions exist to the extent that the stablecoin has a final contractual maturity and the maturity would result in an inflow of fiat currency within the relevant time horizon.

- Other cryptoassets: These should generally follow the treatment of other non–HQLA, subject to a number of considerations, including:

  o A bank that holds other cryptoassets or loans denominated in these assets on its balance sheet would assign 100% RSF to the carrying value of these assets in the NSFR and would not recognize any inflows associated with the liquidation, redemption or maturity of these assets.

  o A bank that has borrowed other cryptoassets on an unsecured basis and has an obligation to return these assets within 30 days would apply a 100% outflow rate against the market value of the asset that would be returned

to the bank's customer or counterparty (unless the obligation can be settled with certainty from the bank's own unencumbered inventory of the same asset).

LARGE EXPOSURE REQUIREMENTS

Cryptoassets will be subject to the BCBS's large exposure rule and will follow the same principles as other exposures. Cryptoasset exposures that give rise to a credit risk exposure would be included in the large exposure measure according to their accounting value, as set out in the large exposure standards.

GROUP 2 EXPOSURE LIMIT

In addition, the Consultation would establish a new limit on a bank's exposure to Group 2 cryptoassets. A bank's aggregate exposure from direct and indirect holdings of Group 2 assets would be limited at all times to 1% of the bank's tier 1 capital. Exposures include direct (cash and derivatives) and indirect holdings (*i.e.*, those via investment funds, ETFs/ETNs, special purpose vehicles). Moreover, the limit would apply to all Group 2 cryptoassets on a gross exposure basis.

The Consultation states that the BCBS intends to review the limit in the future and may increase or eliminate it.

BANK RISK MANAGEMENT AND SUPERVISORY REVIEW

Banks should develop policies to identify, assess and mitigate risks associated with cryptoassets. The policies should be informed by existing Basel committee statements on operational risk management generally and cryptoassets in particular.

Banks would be expected to inform their supervising agency of their:

- Risk management plans for cryptoassets.

- Actual and planned cryptoasset exposures and activities in a timely manner and to demonstrate that they have fully assessed the permissibility of such activities, the associated risks and how they have mitigated those risks.

The Consultation provides a non-exclusive list of risks associated with cryptoassets that banks should consider:

- Cryptoasset Technology Risk: Banks should consider the stability of the network and DLT, the design of the DLT, service accessibility and the trustworthiness of node operators.

- IT and cybersecurity risks: Banks should be aware that cryptoassets bring new IT and cybersecurity risks. These include cryptographic key theft, distributed denial of service attacks and compromised login credentials.

- Legal risks: The novelty and fast evolution of cryptoassets bring unique legal risks. Banks should be aware of accounting procedures, control and ownership rules, disclosure requirements and bans associated with cryptoassets.

- Money laundering and financing terrorism risks: Banks should continue to apply risk-based anti-money laundering and countering financing terrorism practices for cryptoassets.

- Valuation risks: Cryptoassets are volatile and have variable prices on different exchanges. This can cause banks to face losses due to mispricing from operational deficiencies.

The Consultation states that supervisory evaluation of cryptoasset activities is "particularly relevant" because the activities and related risks are new and evolving. Supervisors would be expected to exercise their authority to require banks to address any deficiencies identified and may recommend that banks perform stress testing or scenario analysis to assess cryptoasset-related risks. Supervisory actions also could include additional capital charges, provisioning for losses related to cryptoassets or mitigations measures such as internal limits.

DISCLOSURE REQUIREMENTS

Banks should disclose their business activities related to cryptoassets and how those activities impact the risk profile of the bank, risk management policies for cryptoasset exposures, scope of the bank's reporting for cryptoassets, significant and emerging risks for cryptoassets and how they would be managed. Banks should disclose any material exposure to Group 1a, 1b, 2a and 2b cryptoassets on a regular basis. This disclosure should include direct and indirect exposure amounts, capital requirements and accounting procedures.

This publication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It should not be relied upon as legal advice as facts and circumstances may vary. The sharing of this information will not establish a client relationship with the recipient unless Cravath is or has been formally engaged to provide legal services.

New York
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

London
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com

---

[1] For bonds, loans, claims on banks, equities and derivatives, this also means that there must not be any feature of the cryptoasset that could prevent obligations to the bank being paid in full when due as compared with the traditional version of the asset.

[2] No breach is deemed occur if the market value exceeds the peg value.

[3] This treatment is not further described herein because its complexity is not consistent with the summary nature of this document.

[4] Specifically, stablecoins that do not meet the Group 1 classification only due to failure to meet minimum notice periods or the basis risk test and that are fully backed by a segregated pool of underlying assets that do not count towards the bank's stock of HQLA.