Basel Committee
on Banking Supervision

# Consultative Document

## Prudential treatment of cryptoasset exposures

Issued for comment by 10 September 2021

June 2021

BIS

This publication is available on the BIS website (www.bis.org).



ISBN 978-92-9259-480-0 (online)

## Contents

# Prudential treatment of cryptoasset exposures

## Introduction

The past few years have seen rapid growth in cryptoassets and the estimated market capitalisation of some of these assets have recently reached new all-time highs. While the cryptoasset market remains small relative to the size of the global financial system, and banks' exposures to cryptoassets are currently limited, its absolute size is meaningful and there continues to be rapid developments, with increased attention from a broad range of stakeholders. Cryptoassets have given rise to a range of concerns including consumer protection, money laundering and terrorist financing, and their carbon footprint.

The Committee is of the view that the growth of cryptoassets and related services has the potential to raise financial stability concerns and increase risks faced by banks. Certain cryptoassets have exhibited a high degree of volatility, and could present risks for banks as exposures increase, including liquidity risk; credit risk; market risk; operational risk (including fraud and cyber risks); money laundering / terrorist financing risk; and legal and reputation risks.

To that end, the Committee has taken steps to address these risks.[1] In March 2019, the Committee published a newsletter on the risks associated with cryptoassets, outlining a set of minimum supervisory expectations for banks that are authorised, and decide, to acquire cryptoassets and/or provide related services.[2] In December 2019, the Committee published a discussion paper seeking views of stakeholders on a range of issues related to the prudential treatment of cryptoassets.[3]

Building on the discussion paper and responses received from a broad range of stakeholders, as well as ongoing initiatives undertaken by the international community, the Committee is publishing this consultation paper to seek the views of stakeholders on a preliminary proposal of the prudential treatment for cryptoassets. Given the rapidly evolving nature of this asset class, the Committee is of the view that policy development for cryptoasset exposures is likely to be an iterative process, involving more than one consultation. The Committee has decided to proceed with the public consultation to enable further work to continue with the additional benefit of incorporating feedback from external stakeholders. The Committee will also continue to coordinate with other international organisations that are developing their approaches to cryptoassets.

Cryptoassets are defined as private digital assets that depend primarily on cryptography and distributed ledger or similar technology (FSB (2020)).[4] Digital assets are a digital representation of value,

[1] Initiatives by the Committee form part of a broader work plan, consisting of: (i) vigilant monitoring of market and regulatory developments related to cryptoassets and an assessment of the impact of such developments on the banking system; (ii) the quantification of banks' direct and indirect exposures to cryptoassets through periodic data-collection exercises; and (iii) an assessment of the appropriate prudential treatment for banks' exposures to cryptoassets.

[2] See www.bis.org/publ/bcbs_nl21.htm.

[3] See www.bis.org/bcbs/publ/d490.htm.

[4] See https://www.fsb.org/wp-content/uploads/P131020-3.pdf.

which can be used for payment or investment purposes or to access a good or service.[5] The prudential treatment of central bank digital currencies (CBDCs) is not within the scope of this paper.

The prudential treatment of cryptoassets set out in this paper has been guided by the following general principles:

- **Same risk, same activity, same treatment:** a cryptoasset that provides equivalent economic functions and poses the same risks compared with a "traditional asset"[6] should be subject to the same capital, liquidity and other requirements as the traditional asset. As a starting point, the prudential framework should apply the concept of "technology neutrality" and not be designed in a way to explicitly advocate or discourage the use of specific technologies related to cryptoassets. The prudential treatment should, however, account for any additional risks arising from cryptoasset exposures relative to traditional assets.
- **Simplicity:** The design of the prudential treatment of cryptoassets should be simple. Cryptoassets are currently a relatively small asset class for banks. As the market, technologies and related services of cryptoassets are still evolving, there is merit in starting with a simple and cautious treatment that could, in principle, be revisited in the future depending on the evolution of cryptoassets.
- **Minimum standards:** Any Committee-specified prudential treatment of cryptoassets would constitute a minimum standard for internationally active banks. Jurisdictions would be free to apply additional and/or more conservative measures if warranted. As such, jurisdictions that prohibit their banks from having any exposures to cryptoassets would be deemed compliant with a global prudential standard.

[5] Dematerialised securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through distributed ledger or similar technologies are considered to be within the scope of this framework, whereas those dematerialised securities that use electronic versions of traditional registers and databases are not within the scope. Decentralised Finance (DeFi) instruments or Non-Fungible Tokens (NFTs) meeting the definition of cryptoassets are considered to be within the scope of this paper.

[6] Traditional assets are those assets that are captured within the current Basel Framework.

The general structure of the proposal set out in this consultation document is summarised below:

An overview of the prudential treatment of cryptoasset exposures — Table 1

| Prudential requirements | Group 1 cryptoassets (fulfilling classification conditions) | | Group 2 cryptoassets (not fulfilling classification conditions) | Out of scope |
|---|---|---|---|---|
| | Group 1a: Tokenised traditional assets | Group 1b: Cryptoassets with stabilisation mechanisms (ie stablecoins) | Cryptoassets that do not qualify as Group 1 (eg bitcoin) | Central bank digital currencies |
| Credit and market risk requirements | Capital requirements at least equivalent to those of traditional assets (with further consideration for capital add-ons) | New guidance on application of current rules to capture the risks relating to stabilisation mechanisms (with further consideration for capital add-ons) | New conservative prudential treatment based on a 1250% risk weight applied to the maximum of long and short positions | N/A |
| Other minimum requirements (leverage ratio, large exposures, liquidity ratios) | Application of the existing Basel Framework requirements with additional guidance where applicable | | | N/A |
| Supervisory review | Additional guidance to ensure that risks not captured under minimum (Pillar 1) requirements are assessed, managed and appropriately mitigated (including through capital add-ons) | | | N/A |
| Disclosure | New requirements for banks to disclose information regarding cryptoasset exposures on a regular basis | | | N/A |

The consultation paper is organised as follows. Section 1 sets out a general approach for determining minimum risk-based capital requirements, where cryptoassets are screened and classified into two groups. Section 2 sets out the capital requirements for those cryptoassets that meet all of these classification conditions, which are termed Group 1 cryptoassets. The minimum risk-based capital requirements for cryptoassets that do not meet any of the classification conditions (termed Group 2 cryptoassets) are outlined in Section 3. Section 4 sets out other regulatory requirements (ie leverage ratio, large exposures, liquidity ratios) for all cryptoassets. Section 5 sets out the responsibilities of banks and supervisors for the supervisory review. Section 6 sets out disclosure requirements for all cryptoassets.

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

# 1. General approach for minimum risk-based capital requirements

In order to determine minimum risk-based capital requirements for credit and market risk, cryptoassets are screened on an ongoing basis and classified into two groups:

- **Group 1 cryptoassets.** Those that meet all of the classification conditions set out below. Group 1 cryptoassets will be subject to at least equivalent risk-based capital requirements based on the risk weights of underlying exposures as set out in the existing Basel capital framework. Section 2 describes how to interpret and apply the existing Basel capital framework to Group 1 cryptoassets. Group 1 cryptoassets include tokenised traditional assets (Group 1a) and cryptoassets with effective stabilisation mechanisms (Group 1b).

- **Group 2 cryptoassets.** Those that fail to meet any of the classification conditions below. As a result, they pose additional and higher risks compared with Group 1 cryptoassets and consequently will be subject to a newly prescribed conservative capital treatment set out in Section 3.

## 1.1 Classification conditions

Cryptoassets must meet all the conditions below in order to be classified as Group 1 cryptoassets on an ongoing basis. Cryptoassets that fail to meet any of the conditions below will be classified as Group 2 cryptoassets.

**1. The cryptoasset either is a tokenised traditional asset or has a stabilisation mechanism that is effective at all times in linking its value to an underlying traditional asset or a pool of traditional assets.**

- Tokenised traditional assets must be digital representations of traditional assets using cryptography, Distributed Ledger Technology (DLT) or similar technology rather than recording ownership through the account of a central securities depository (CSD)/custodian.
- Stabilisation mechanisms must be designed to minimise fluctuations in the value of cryptoassets. In order to satisfy the "effective at all times" condition, banks must have a monitoring framework in place verifying that the stabilisation mechanism is functioning as intended. To this end, banks must monitor daily the difference between the value of the cryptoasset and the underlying traditional asset(s) to assess the effectiveness of the stabilisation mechanism. The difference in value must not exceed 10bp of the value of the underlying traditional asset more than three times over a one-year period. If such a difference occurs the stabilisation mechanism will no longer be deemed to be effective. After a breach of threshold the cryptoasset may only be reassessed as having an effective stabilisation mechanism when the bank has demonstrated to the satisfaction of the supervisors that the cause of breach of the threshold has been addressed and will not reoccur.
- The stabilisation mechanism must enable risk management based on sufficient data/or experience. For newly established cryptoassets, there may be insufficient data and/or practical experience to perform a detailed assessment of the stabilisation mechanism. Evidence must be provided to satisfy supervisors of the effectiveness of the stabilisation mechanism, including the composition of the underlying asset(s) and its valuation.
- Banks must also verify the ownership rights of any underlying traditional asset from which the stable value of the cryptoasset is dependent upon. In the case of underlying physical assets, they must verify that these assets are stored and managed appropriately. This monitoring framework must function regardless of the cryptoasset issuer.[7]
- Stabilisation mechanisms that: (i) reference other cryptoassets as underlying assets (including those that reference other cryptoassets that have traditional assets as underlying); or (ii) use protocols to increase or decrease the supply of the cryptoasset;[8] are not considered to meet this condition.

[7] The monitoring framework must also function for cases where a bank is the issuer of the cryptoasset.

[8] Cryptoassets that use protocols to maintain their value are referred to as "algorithm-based stablecoins". See FSB (2020).

**2. All rights, obligations and interests arising from cryptoasset arrangements that meet the condition above are clearly defined and legally enforceable in jurisdictions where the asset is issued and redeemed. In addition, the applicable legal framework(s) ensure(s) settlement finality.**

- All cryptoasset arrangements must ensure full transferability and settlement finality at all times. In addition, cryptoassets with stabilisation mechanisms must ensure full redeemability (ie the ability to exchange cryptoassets for cash, bonds, commodities, equities or other traditional assets) at all times.
- All cryptoasset arrangements must be properly documented. For cryptoassets with stabilisation mechanisms, cryptoasset arrangements must clearly define which parties have the right to redeem; the obligation of the redeemer to fulfil the arrangement; the timeframe for this redemption to take place; the traditional assets in the exchange; and how the redemption value is determined. These arrangements must also be valid in instances where parties involved in these arrangements may not be located in the same jurisdiction where the cryptoasset is issued and redeemed. At all times, settlement finality in cryptoasset arrangements should be properly documented such that it is clear when key financial risks are transferred from one party to another, including the point at which transactions are irrevocable.

**3. The functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks.**

- The "sufficient" condition would be satisfied if the functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets, and the network on which it runs do not pose any material risks that could impair the transferability, settlement finality or redeemability of the cryptoasset.
- To this end, entities performing activities associated with these functions[9] must follow robust risk governance and risk control policies and practices to address risks including, but not limited to: credit, market and liquidity risks; operational risk (including outsourcing, fraud and cyber risk) and risk of loss of data; and various non-financial risks, such as data integrity; operational resilience (ie operational reliability and capacity); third party risk management; and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT).
- Networks that fulfill this condition would be those where the key aspects are well-defined such that all transactions and participants are traceable. Key aspects include: (i) the operational structure (ie whether there is one or multiple entities that perform core function(s) of the network); (ii) degree of access (ie whether the network is restricted or un-restricted); (iii) technical roles of the nodes (ie whether there is a differential role and responsiblity among nodes); and (iv) the validation and consensus mechanism of the network (ie whether validation of a transaction is conducted with single or multiple entities).

**4. Entities that execute redemptions, transfers, or settlement finality of the cryptoasset are regulated and supervised.**

- Entities covered by this condition are those such as operators of the transfer and settlement systems for the cryptoasset; administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism.

[9] Examples of these entities include but are not limited to: issuers, operators of the transfer and settlement systems for the cryptoasset; administrators of the cryptoasset stabilisation mechanism and custodians of any underlying assets supporting the stabilisation mechanism. Annex 1 sets out descriptions of these entities.

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?

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?

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?

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?

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?

## 1.2 Responsibilities for determining and monitoring compliance with the classification conditions

Banks are responsible for: (i) assessing on an ongoing basis, whether a cryptoasset is compliant with the classification conditions; and (ii) demonstrating to supervisors how a cryptoasset fulfils these conditions. To this end, banks should have in place the appropriate risk management policies, procedures, governance, human and IT capacities to evaluate the risks of engaging in cryptoassets and implement these accordingly on an ongoing basis.

Supervisors are responsible for: (i) reviewing and assessing banks' analysis and risk management and measurement approaches; and (ii) approving the bank's demonstration of whether and if so how a cryptoasset qualifies as a Group 1 cryptoasset. A bank supervisor may rely on: other regulators or supervisors overseeing the entities management of risks attributable to the functions mentioned above; as well as independent third-party assessors determined to have the requisite expertise and skills, to evaluate the specific risk characteristics of cryptoasset arrangements. A cryptoasset must be classified as a Group 2 cryptoasset, unless a bank, through their analysis and risk management and measurement approaches, demonstrates to the supervisor that the cryptoasset meets all the classification conditions. In cases where the same cryptoasset is being sought for approval, bank supervisors may make a decision to approve or disapprove whether a cryptoasset would be a Group 1 cryptoasset, based on their assessments made for cases of the same cryptoasset put forth by other banks.

Requiring supervisory approval is necessary to ensure consistent application of classification conditions by banks. To ensure consistent application across jurisdictions, there is a need for strong

coordination among supervisors. To this end, supervisors should routinely compare and share their supervisory approval criteria.

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?

## 2. Capital requirements for group 1 cryptoassets

This section describes the minimum risk-based capital requirements for credit risk and market risk for Group 1 cryptoassets. The requirements only apply to those Group 1 cryptoassets which have not been deducted from Common Equity Tier 1 (CET1) capital, for example due to classification as intangibles under the applicable accounting frameworks.

Similar to activities related to traditional assets, activities related to cryptoassets will give rise to an operational risk charge within the Basel framework. 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. Such 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. Such a charge could be set in various different ways, eg as a flat percentage of the exposure amount, as a variable amount that depends on the specific features of the cryptoasset, or even as an amount that reduces over a period of time as the underlying technology becomes more established and conditional on it demonstrating robustness through stressed events (eg cyber-attacks, legal challenges etc). Calibrating such a charge would be a significant challenge. The Committee would welcome feedback from stakeholders on the design and calibration of an operational risk add-on for cryptoassets. In addition to the minimum capital requirements for credit risk and market risk set out in this section, Section 5 describes the supervisory review process, under which supervisors may consider applying add-ons to capital requirements if they determine that the bank is exposed to risks that are not adequately captured in the minimum requirements. As such, the capital requirements set out in this section represent a floor on the requirements that apply to Group 1 cryptoassets. Furthermore, regardless of whether the bank has a legal obligation to purchase cryptoassets from holders, banks and supervisors should consider whether in practice the bank would be obliged to step-in and purchase them in order to satisfy the expectations of holders and protect the bank's reputation.

Group 1 cryptoassets will be subject to the requirements set out in the Basel Framework to determine their allocation between the banking book and trading book and to determine whether the exposures are treated according to standardised or internal model-based approaches.[10] Although internal models-based approaches are not prohibited under the proposed treatment set out in this consultation, a high degree of caution should be exercised by supervisors in deciding whether to permit such approaches given the novel features of cryptoassets.

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?

[10] The consultation document does not attempt to define a prudential treatment for cryptoassets in cases where no existing prudential treatment is defined in the Basel Framework for traditional assets. For example, the Basel Framework does not set out a description of the requirements that apply to banks that provide services (eg custody services) to customers that invest in traditional assets.

## 2.1 Group 1a cryptoassets: tokenised traditional assets

Tokenised traditional assets use an alternative way of recording ownership of traditional assets 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.

Cryptoassets may be treated as equivalent to a traditional asset for the purpose of calculating minimum capital requirements for credit and market risk if they pose the same level of credit and market risk as traditional (non-tokenised) assets. In practice, this means the following for tokenised traditional assets to be treated as equivalent:

- *Bonds, loans, deposits and equities*. The cryptoasset must confer the same level of legal rights as ownership of these traditional forms of financing, eg rights to cash flows, claims in insolvency etc. In addition, there must be no feature of the cryptoasset that could prevent obligations to the bank being paid in full when due as compared with a traditional (non-tokenised) version of the asset.
- *Commodities*. The cryptoasset must confer the same level of legal rights as traditional account-based records of ownership of a physical commodity.
- *Cash held in custody*. The cryptoassets must confer the same level of legal rights as cash held in custody.

The above criteria are not met by cryptoassets that first need to be redeemed or converted into traditional assets before they receive the same legal rights as direct ownership of traditional assets. Cryptoassets that can be redeemed or converted into traditional assets (ie Group 1b cryptoassets) are addressed in Section 2.2 below. The above criteria are also not met by cryptoassets that through their specific construction involve additional counterparty credit risks relative to traditional assets.

### Credit and market risk

Tokenised traditional assets, ie cryptoassets that are assessed to be equivalent to traditional assets using the criteria described above, will generally be subject to the same rules to determine credit and market risk-weighted assets as non-tokenised traditional assets. For example, a tokenised corporate bond held in the banking book will be subject to the same risk weight as the non-tokenised corporate bond held in the banking book. Similarly, if a bank holds a derivative on a tokenised asset, it will be reflected in the market risk charge in the same way as a derivative on the non-tokenised asset. These examples are based on the assumption that if two exposures confer the same level of legal rights (to cash flows, claims in insolvency, ownership of assets etc) and the same likelihood of paying the owner amounts due on time, they will likely have very similar values and pose a similar risk of loss.

There are, however, areas of the credit and market risk standards that aim to capture risks that are not directly related to the legal rights of an asset held by a bank or likelihood of timely payment. In general, banks must always assess the tokenised traditional asset against these rules, and not assume qualification for a given treatment simply because the traditional (non-tokenised) asset qualifies. For example, a tokenised asset may have different liquidity characteristics than the traditional (non-tokenised) asset. This could arise because the pool of potential investors that are able to hold tokenised assets might be different to non-tokenised assets. The different liquidity characteristics could give rise to different market values of tokenised versus non-tokenised assets that are otherwise identical. Moreover, there may be insufficient data to model the impact of these different liquidity characteristics on their market values, which would rule out the application of the modelled-based approaches to calculating market risk.

As well as being relevant for the application of the market risk standards, the potential for liquidity characteristics and market values of tokenised assets to differ from non-tokenised assets is important in considering whether Group 1a cryptoassets meet the requirements for the purposes of credit risk

mitigation within the credit risk standards. Also, the speed with which a secured creditor could take possession of cryptoasset collateral may be different to a traditional asset. Therefore, before such assets are recognised as collateral for the purposes of credit risk mitigation, banks must separately assess whether they comply with the preconditions for collateral recognition, such as whether the collateral can be liquidated promptly and there is legal certainty of access to the collateral. In addition to assessing whether tokenised assets held as collateral are eligible to be recognised as credit risk mitigation, banks must analyse the period of time over which they can be liquidated and the depth of market liquidity during a period of downturn. Cryptoassets shall only be recognised as collateral where volatility in values and holding periods under distressed market conditions either can be confirmed to not be materially increased compared with the traditional asset or pool of traditional assets, or where any material increase can be reflected by prudent increases of the parameters applied for the traditional asset. Otherwise the cryptoasset shall not be eligible for recognition of credit risk mitigation.

Chapter CRE22 of the Basel Framework sets out the list of eligible forms of financial collateral for the purposes of recognition as credit risk mitigation under the standardised approach to credit risk. The list is also the basis of eligible collateral under the foundation internal ratings based approach. Only Group 1a cryptoassets that are tokenised versions of the instruments included on the list of eligible financial collateral set out in CRE22 may qualify for recognition as eligible collateral (subject to also meeting the requirements described above). Group 1b cryptoassets (ie stablecoins), including those that can be redeemed for traditional instruments that are included on the list of eligible collateral, are not eligible forms of collateral in themselves for the purposes of recognition as credit risk mitigation. This is because, as discussed further below, the process of redemption adds counterparty risk that is not present in a direct exposure to a traditional asset.

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?

## 2.2 Group 1b cryptoassets: cryptoassets with stabilisation mechanisms

Certain types of Group 1 cryptoassets (Group 1b) may not confer the same level of legal rights as ownership of a traditional asset, but may seek to link the value of a cryptoasset to the value of a traditional asset or a pool of traditional assets through a stabilisation mechanism. Cryptoassets under this category must be redeemable for underlying traditional asset(s) (eg cash, bonds, commodities, equities).

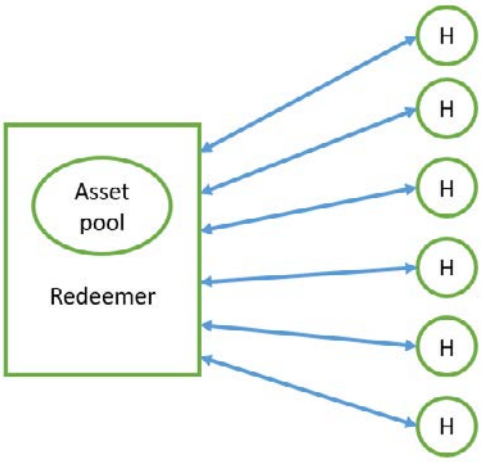
It is not possible for the Committee to set out the capital treatment for every type of cryptoasset structure. As such, this section considers two stylised cryptoasset structures as illustrative examples and examines how capital rules would be applied in these cases. As the issues raised in these generic examples are likely to be relevant for many cryptoasset structures, these examples should serve as an indication of the Committee's current thinking for these types of cryptoassets.

### Illustrative example 1

There is an entity (the "redeemer") that commits to exchange the cryptoasset for: (i) an underlying traditional asset; or (ii) cash equal in value to an underlying traditional asset.[11] The mechanism that the redeemer uses consists of maintaining a sufficiently large pool of assets that it can draw on to honour its commitment. In this example, all cryptoasset holders (H) are allowed to transact directly with the redeemer.

[11] The redeemer is the entity responsible for redeeming the cryptoasset. It does not necessarily need to be the same as the entity responsible for organising the issuance of the cryptoasset.

Case where cryptoasset holders transact directly with the redeemer Figure 1




In this example, the cryptoasset holders are subject to two principal risks: (i) the risk arising from the changing value or potential default of the underlying asset(s); and (ii) the risk arising from the potential default of the redeemer.[12]

This situation is analogous to the risks a bank faces when it lends out a security. In such cases, the bank remains exposed to risk of loss due to the changing value and potential default on the security it has lent, plus it is exposed to the risk that the recipient of the security defaults. In such cases, banks are required by the Basel Framework to calculate risk-weighted assets for both risks. The proposed capital treatment that follows is consistent with this approach.

### Treatment for credit and market risk

To calculate RWA for cryptoassets in illustrative example 1, the bank must include in risk-weighted assets the sum of the following two amounts:

- The risk weighted assets applicable to a direct holding of the underlying traditional asset.[13]
- The value of the cryptoasset holding multiplied by the risk weight applicable to an unsecured loan to the redeemer.

As with exposures to traditional assets, the specific risk weights referenced in the two elements above will depend on factors, such as: (i) the type of underlying asset (eg bond, commodity etc); (ii) the currency of exposure; (iii) whether the exposure is in the banking or trading book; (iv) how the redeeming entity is classified (eg a financial entity or corporate); and (v) the approach the bank uses to calculate RWA for the exposures to the underlying asset and redeemer (eg standardised approach, internal ratings based approach, internal models approach etc).

[12] Illustrative example 1 is based on the scenario in which the holder depends on the redeemer to convert cryptoassets into the underlying reference assets or cash equivalent amounts. Cryptoassets for which this conversion does not depend on the redeemer's ability to pay/exchange but instead is fully backed by direct claims on a pool of traditional assets held in a bankruptcy remote vehicle do not give rise to a credit risk exposure to the redeemer.

[13] For example, in the case of credit risk, the risk weighted assets would be calculated as the value of the cryptoasset holding multiplied by the risk weight applicable to a direct holding of the underlying traditional asset. For market risk, the calculation of risk weighted assets would depend on the extent to which the market risk arising from the underlying traditional asset has been hedged by the bank.

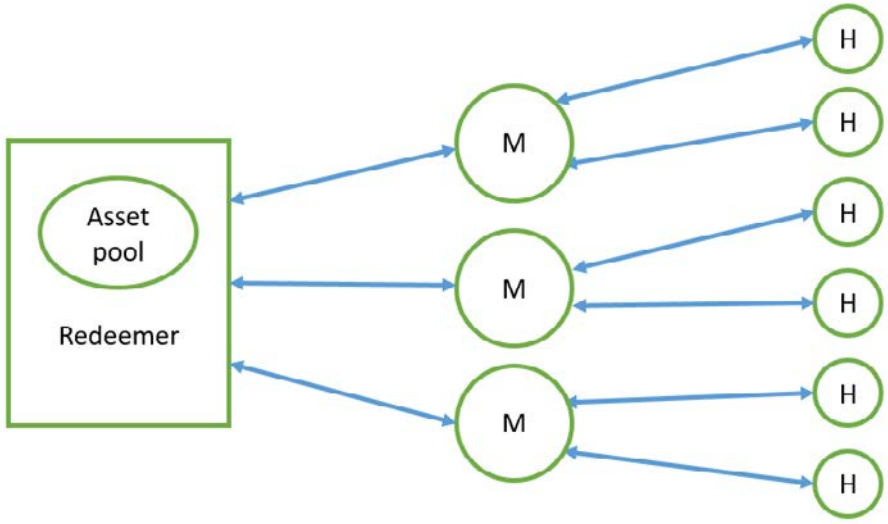
In cases where there is a pool of underlying assets, banks should use the rules for Equity Investments in Funds to determine the risk weight of a direct holding of the underlying exposure.[14]

### Illustrative example 2

This illustrative example is similar to the example above, except that in this case only a subset of holders ("members") are allowed to deal directly with the redeemer to convert the cryptoassets into underlying assets or cash. Holders that cannot transact directly ("non-member holders") are therefore reliant on the members for the cryptoassets to maintain their value relative to the underlying asset.

Two variations are considered for this illustrative example: (a) the members issue a legally binding *promise* to buy cryptoassets from non-member holders at a price equal to the underlying asset(s); and (b) the members do not promise, but are incentivised to buy the cryptoassets because they know they can exchange them with the redeemer for cash/assets (as long as the redeemer remains solvent).

Case where cryptoasset holders transact indirectly with the redeemer — Figure 2




#### *Holders that can transact directly with the redeemer (ie members)*

Members that hold cryptoassets under illustrative example 2 are exposed to the same risks as described in illustrative example 1, and thus should calculate their risk-weighted assets for their exposures in the same way. However, as explained above, members may also have made commitments to buy cryptoassets from non-member holders. If there is such a legally binding commitment in place, there is a risk that if the redeemer defaults the member will have to purchase cryptoassets from non-member holders to comply with its contractual obligations. To take account of this additional "commitment to buy" risk, member banks that have issued such commitments must also include within credit risk-weighted assets an amount equal to:

[14] The rules for Equity Investments in funds held in the banking book are set out in CRE60 of the Basel framework. Equity investments in funds held the trading book are set out in within the MAR standard of the Basel framework.

- The total current value of all existing cryptoassets that the bank could be obliged to purchase from non-member holders multiplied by the risk weight applicable to an unsecured loan to the redeemer.[15]

Even if there is no legal obligation for a bank to purchase cryptoassets from non-member holders, banks and supervisors should consider whether in practice the member bank would be obliged to step-in and purchase them in order to satisfy the expectations of non-member holders and protect the bank's reputation. Where such step-in risk exists, banks should include within risk-weighted assets the amount specified above (ie the amount that applies where legally binding commitments have been made). Exceptions would only be made if it is clear that such step-in risk does not exist.

*Non-member holders*

The risk to cryptoasset holders that cannot deal directly with the redeemer (ie non-member holders) depends on whether the members have committed to buy cryptoassets from non-member holders in unlimited amounts (ie they have made a standing and irrevocable offer to buy all outstanding cryptoassets from non-member holders).

If members have not committed to buy cryptoassets in unlimited amounts, the non-member holders are exposed to: (i) the risk arising from the changing value or potential default of the underlying asset; (ii) the risk that the redeemer defaults (because if it failed, the members would no longer have the incentive to buy the cryptoassets from the non-member holders); and (iii) the risk that all the members default (because if they all fail the non-member holders would have no way to redeem their assets). In such cases, the bank holder must include in risk-weighted assets the sum of RWA for all three separate exposures.

If members have committed to buy cryptoassets in unlimited amounts, the non-member holders are exposed to: (i) the risk arising from the changing value or potential default of the underlying asset; and (ii) the risk arising from the credit risk of the members (as non-members would be left with no way to redeem the cryptoassets). When banks are non-member holders they should sum the RWA calculated for the two risks. The first risk should be calculated as described for illustrative example 1 (ie the RWA that would arise from a direct exposure to the underlying). The calculation of the RWA for the default of the members is more complex given that there may potentially be multiple members that have made promises to purchase the cryptoassets (ie the holder can choose whether to sell the cryptoasset to any one of a number of members). If there is just one member, the risk-weighted assets should be calculated as the cryptoasset holding multiplied by the risk weight applicable to a loan to the member. If there are multiple members, the risk weight to be used should be the risk weight that would be applicable to the member with the highest credit rating (ie lowest risk weight).[16]

[15] If promises to purchase cryptoassets are off-balance sheet, the outlined approach is equivalent to applying a credit conversion factor of 100% to determine an on-balance sheet equivalent amount, and then applying the risk weight of the redeemer. This example assumes that on the insolvency of the redeemer, holders of cryptoassets (including those that member banks were required to purchase) are fixed at the value of the underlying of the cryptoasset at the point of insolvency. This is why the requirement that applies to amounts that the member bank may be required to purchase is based on an unsecured loan to the redeemer. If the claim was not fixed, but could vary with the value of the underlying after the point of insolvency, this would represent an additional risk to member banks in respect of cryptoassets that they may be required to purchase from non-member holders.

[16] For example, consider the situation in which there is only one member and it has a high credit rating (low risk weight). Its low risk weight should be used to determine the credit risk of non-member holders. Now consider an additional member is added that has a low credit rating (high risk weight). The addition of this new member does not increase the risk to non-member holders (in fact it decreases it by giving them more options for redeeming their assets). Thus, the low risk weight of the first member can continue to be used to determine the credit risk to non-member holders.

## 2.3 Treatment of bankruptcy remote vehicles for cryptoassets with underlying pool of assets

As noted in the previous section, the holders of cryptoassets with stabilisation mechanisms are subject to two main risks: (i) the risk arising from the changing value or potential default of the underlying asset(s); and (ii) the risk arising from the potential default of the redeemer. In this case the cryptoasset holder depends on the redeemer to exchange cryptoassets for underlying reference assets or cash equivalent amounts. For cryptoassets that confer direct claims on a pool of traditional assets held in a bankruptcy remote vehicle, if an institution has obtained a legal opinion for all laws relevant to involved parties, including the redeemer, the special purpose vehicle (SPV) and custodian, affirming that relevant courts would recognise underlying assets held in a bankruptcy remote manner as those of the cryptoasset holder, the credit risk exposure to the bankruptcy remote assets of the redeemer may be set to zero.

## 2.4 Equity Investment in Funds approach for credit risk for cryptoassets with a stabilisation mechanism backed by a pool of assets

The Equity Investments in Funds (EIF) approach should be applied for cryptoassets with a stabilisation mechanism fully collateralised by a pool of traditional assets. The look-through approach and the mandate-based approach of the EIF should be available for cryptoassets that fulfil all requirements for these approaches. Otherwise, the fall-back approach (ie a 1250% risk weight) should apply.

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

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?

# 3. Capital requirements for Group 2 cryptoassets

Group 2 cryptoassets pose unique risks compared with Group 1 cryptoassets and as such are subject to the newly prescribed capital requirement set out in this section. The requirements only apply to those Group 2 cryptoassets which have not been deducted from Common Equity Tier 1 (CET1) capital, for example cryptoassets classified as intangibles under the applicable accounting framework. Funds of Group 2 cryptoassets (eg Group 2 cryptoasset ETFs) and other entities, the material value of which is primarily derived from the value of Group 2 cryptoassets, must be treated under this category. Equity investments, derivatives or short positions in these funds or entities must also be treated under this category.

The treatment is by design simple and conservative. It consists of the following elements:

- A risk weight of 1250% (explained further below) is applied to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions to which the bank is exposed. That is:

  RWA = RW x max [abs (long), abs (short)].

- The RWA will be calculated separately for each Group 2 cryptoasset to which the bank is exposed.

- For each cryptoasset derivative (ie a derivative with a Group 2 cryptoasset as the underlying asset), the value used in the above formula is the value of its underlying cryptoassets.[17] If this value exceeds the maximum possible loss on the cryptoasset derivative, the maximum loss can be used instead. Annex 2 provides the rationale for this treatment.
- There is no separate trading book and banking book treatment. The conservative risk weight is intended to capture both credit and market risk, including CVA risk. For consistency, the RWA should be reported as part of the bank's credit risk-weighted assets.
- For the purpose of calculating counterparty credit risk for derivative exposures that have Group 2 cryptoassets as the underlying or that are priced in units of a Group 2 cryptoasset, the exposure will be the Replacement Cost (RC) plus the Potential Future Exposure (PFE), where the PFE is to be calculated as 50% of the gross notional amount. When calculating the RC, netting will be allowed within eligible and enforceable netting sets but not allowed between different cryptoassets. Netting sets with a single counterparty that consists of: (i) only types of derivatives related to cryptoassets; or (ii) derivatives related to cryptoassets and traditional asset transactions, would be treated separately. In (ii), the netting set would be split between the derivatives related to cryptoassets and those derivatives related to traditional asset transactions. However, when calculating the PFE, the 50% of the gross notional amount for exposure should be applied per transaction.[18]
- For securities financing transactions (SFT) and margin loans involving Group 2 cryptoassets, to calculate their counterparty credit risk exposures banks should apply the comprehensive approach formula set out in the credit risk mitigation section of the standardised approach to credit risk. Group 2 cryptoassets are not eligible forms of collateral in the comprehensive approach and therefore when banks receive them as collateral they will receive no recognition for the purposes of the net exposure calculation to the counterparty. As with all non-eligible collateral, banks that lend Group 2 cryptoassets as part of an SFT must apply the same haircut that is used for equities that are not traded on a recognised exchange (ie a haircut of 25%).

The application of the 1250% risk weight set out in the above formula will ensure that banks are required to hold risk-based capital at least equal in value to their Group 2 cryptoasset exposures.[19] In other words, the capital will be sufficient to absorb a full write-off of the cryptoasset exposures without exposing depositors and other senior creditors of the banks to a loss. The application of a 1250% risk weight to an asset is similar in effect to the deduction of the asset from capital. Unlike a deduction, however, a risk weight approach can also be applied to short positions, where there may be no balance sheet asset to deduct.

For simplicity, the above formula also applies the 1250% risk weight to short positions. Theoretically, short positions and certain other types of exposures could lead to unlimited losses[20] and thus, in some circumstances, the formula could require capital that is insufficient to cover potential future losses. Banks will be responsible for demonstrating the materiality of these risks under the supervisory review of cryptoassets and whether risks are materially underestimated. Supervisors will be responsible for considering an additional capital charge in the form of a Pillar 1 add-on in cases where banks have material

[17] For leveraged derivatives (ie a derivative that returns a multiple of the value of the underlying), the value of the underlying position should be adjusted to take account of the leverage.

[18] Cryptoasset exposures would not be part of any hedging set.

[19] That is, a $100 exposure would give rise to risk weighted assets of $1250, which when multiplied by the minimum capital requirement of 8% results in a minimum capital requirement of $100 (ie the same value of the original exposure, as 12.5 is reciprocal of 0.08).

[20] For example, a short position in bitcoin entered into at the at start of the 2020 calendar year would have resulted in a loss equal to three times the size of the original position by the year end.

exposures to short positions in cryptoassets or to cryptoasset derivatives that could give rise to losses that exceed the capital required by the 1250% risk weight. In applicable cases, the capital add-on would be calibrated by requiring banks to calculate aggregate capital requirements under the Committee's revised market risk framework (applying a 100% risk weight for delta, vega, and curvature) and Basic CVA risk framework (BA-CVA) and to use this amount if the result is higher than the requirement based on a 1250% risk weight.

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?

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?

# 4. Other regulatory requirements

At this stage, the Committee is not proposing to prescribe any new regulatory treatment for Group 1a, 1b or Group 2 cryptoassets under the leverage ratio, large exposures framework, or liquidity ratio requirements. In practice, this means the following: [21]

- *Leverage ratio*. Consistent with the leverage ratio standard, cryptoassets are included in the leverage ratio exposure measure according to their value for financial reporting purposes, based on applicable accounting treatment for exposures that have similar characteristics. For the cases where the cryptoasset exposure is an off-balance sheet item, the relevant credit conversion factor set out in the leverage ratio framework will apply in calculating the exposure measure. [22] Exposures for cryptoasset derivatives must follow the treatment of the risk-based capital framework as specified in Section 3 above.
- *Large exposures*. For large exposures purposes, the treatment for cryptoassets will follow the same principles as for other exposures. Consistent with the large exposures standard, cryptoasset exposures that give rise to a credit risk exposure are included in the large exposure measure according to their value for financial reporting purposes. The bank must identify and apply the large exposure limits to each specific counterparty or group of connected counterparties to which it is exposed. Where the cryptoasset exposes the bank to the risk of default of more than one counterparty, the bank must compute for each counterparty the respective amount to which it is exposed to default risk for large exposure purposes. This also applies to the default risk resulting from any exposure to underlying asset(s). Assets that do not expose banks to default risk (such as physical exposures of gold, other commodities or currencies, and exposures of some forms of cryptoassets with no issuer such as Bitcoin) do not give rise to a large exposures requirement.
- *Liquidity ratios*. For the liquidity coverage ratio (LCR) and net stable funding ratio (NSFR) requirements, any Group 1 cryptoasset on the asset or liability side of a banks' balance sheet

[21] If a bank incurs an operational loss related to cryptoassets, this will be reflected in accordance with the Basel framework.

[22] For Group 1b cryptoassets, the Committee is of the view that: if the bank is involved in the cryptoasset network as a member who is able to deal directly with the redeemer and has promised to buy cryptoassets from non-member holders, the member also needs to include the total current value of all the off-balance cryptoassets that the bank could be obliged to purchase from holders (as discussed in "Illustrative example 2" under Section 2.2 of this document).

must follow a treatment that takes account of the risks as set out in the LCR and NSFR standards. The Committee is of the view that cryptoassets would not qualify as eligible high-quality liquid assets (HQLA). However, the Committee will continue to investigate the prospect of recognising as HQLA those cryptoassets that, according to the definition set out in Section 2.1, are deemed to be equivalent to traditional assets that themselves qualify for inclusion in HQLA, as well as the need for adjustments in order to adequately capture the cash flow risks arising from exposures to cryptoassets or any assets and liabilities payable in, denominated in or linked to cryptoassets. Group 2 cryptoassets must be subject to a 0% inflow for the LCR, while cryptoasset liabilities must be subject to a 100% outflow. Group 2 cryptoassets must be subject to a 100% required stable funding factor for the NSFR, while cryptoasset liabilities must be subject to a 0% available stable funding factor (ie liabilities would be assumed to mature in its entirety at the earliest possible date).

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?

# 5. Supervisory review and adjustments to Pillar 1 requirements

## 5.1 Responsibilities of banks

Banks with direct or indirect exposures to any form of cryptoasset are subject to the supervisory review process set out in the Basel framework. In addition to the assessment of compliance with the classification conditions of cryptoassets as set out in Section 1.2, banks should establish policies and procedures that describe the processes used to identify and assess the risks that are unique to cryptoassets or related activities on an ongoing basis and implement these accordingly. In accordance with the policies and procedures, banks should conduct assessments of these risks (ie how material these risks are, and how they are managed). Banks are also expected to inform their supervisory authorities of their policies and procedures, assessment results, as well as actual and planned cryptoasset exposures or 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 such risks.

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. These risks may include, but are not limited to the following:

*Risks attributable to operational and cyber risk*. An institution holding cryptoassets may be exposed to additional operational and cyber risks targeting the DLT platforms that may include but not be limited to: cryptographic key theft; compromise of login credentials; and distributed denial-of-service (DDoS) attacks. The results of cyber-threats may lead to consequences such as unauthorised cryptoasset transfers and personal data breaches. As such, the institution should increase the surveillance of operational risk, including Information, Communication and Technology (ICT) risk, encompassing at least:

- 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

*Risks attributable to the underlying technology*. Banks are expected to closely monitor the safety of and potential changes to the applied technology, including:

- *Stability of the digital ledger technology or similar technology network*. The reliability of the source code, governance around protocols and integrity of the technology are among key factors related to stability of the network. Key considerations include: capacity constraints, whether self-imposed or because of insufficient computing resources; digital storage considerations; scalability of a crypto-platform; whether the underlying technology has been tested and had time to mature in a market environment; and robust governance around changes to the terms and conditions of the distributed ledger or cryptoassets (eg so-called 'forks' that change the underlying 'rules' of a protocol). In addition, the type of consensus mechanism (ie for a transaction to be processed and validated) is an important consideration for the prudential treatment as it relates to the security of the network and whether it is safe to accept a transaction as 'final'.
- *Validating design of the DLT (permissionless or permissioned)*. Cryptoassets may rely on a public ('permissionless') ledger, whereby the validation of transactions can be done by any participating agent, or distributed among several agents or intermediaries, which could be unknown to the users. In contrast, a private ('permissioned') ledger restricts and pre-defines the scope of validators, with the validating entities known to the users. On a permissionless ledger, there may be less control of technology and on a permissioned ledger there may be a small group of validators with greater control.
- *Service accessibility*. One of the distinguishing features of cryptoassets is its accessibility to holders of these assets. A holder of cryptoassets is assigned a set of unique cryptographic keys, which allow that party to transfer the asset to another party. If those keys are lost, a party will generally be unable to access its cryptoassets. Furthermore, if a third party gains access to those keys, that third party may use the keys to transfer the asset to themselves. Furthermore, the risk of a large-scale cyber-attack could leave banks' customers unable to access or recover cryptoasset funds.
- *Trustworthiness of node operators and operator diversity*. Since the underlying technology and node operators facilitate the transfer of cryptoassets and keep records of transactions that take place across the network, their role is essential in designating and sizing the amounts that are held by the holder. Whether nodes are run by a single operator or are distributed among many operators and whether the operators are trustworthy (eg whether the nodes are run by public/ private institutions or individuals) are relevant considerations.

*Risks attributable to money laundering and financing of terrorism*. Banks in their role of providing banking services to Virtual Asset Service Providers (VASP) or to customers involved in Virtual Asset activities or through engaging in VASP activities themselves should apply the risk-based approach as set out by the Financial Action Task Force (FATF) for the purposes of Anti-Money Laundering and Countering the Financing of Terrorism.[23]

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?

## 5.2 Responsibilities of supervisors

In addition to its responsibilities as set out in Section 1.2, based on the information reported by banks,

[23] Financial Action Task Force (2019), "Guidance for a risk-based approach to virtual assets and virtual asset service providers", FATF, Paris http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

supervisors should review the appropriateness of banks' policies and procedures for identifying and assessing those risks not captured by the minimum capital requirements, and adequacy of their assessment results.

Supervisors should have the authority to ask banks to remedy any deficiency in their identification or assessment process of those risks. Although the specific supervisory action may vary according to the circumstances, the types of response that supervisors may consider are the following:

- *Stress testing and scenario analyses*. Supervisors may decide to require banks to include in their stress testing framework or scenario analyses any specific risks not adequately identified and assessed in their risk management framework.
- *Provisioning*. Supervisors may request banks to consider measures such as provisioning for cryptoassets that entail risks not adequately identified and assessed in their risk assessment framework.
- *Additional capital charges*. Supervisors may impose additional capital charges to individual banks for risks not adequately identified and assessed in their management framework, calibrated under the assumption of a stress event that prompts losses stemming from those risks.
- *Supervisory limit or other mitigation measures*. Supervisors may impose on banks some mitigation measures, such as applying an internal limit set by supervisors, in order to contain the risks not adequately identified or assessed in their risk management framework. This approach would ensure banks are not exposed to an excessive amount of cryptoasset exposures that entail risks not sufficiently managed by banks.

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?

## 5.3 Adjustments to minimum Pillar 1 capital requirements

To address additional credit and market risk characteristics of Group 1 cryptoassets that are not sufficiently captured in the capital treatment as stated in Section 2, supervisors should modify the Pillar 1 treatment to reflect an additional degree of conservatism for all banks. Potential modifications that supervisors may consider include:

(i) Prohibiting model-based approaches for all banks (for example, if there is insufficient history to reliably model probability of default, loss given default, exposure at default, market values etc).

(ii) Requiring longer liquidity horizons to be used in the standardised and internal models approaches.

(iii) Require measurement of the basis risk in the market risk framework to account for potential differences between cryptoassets and equivalent traditional assets.

(iv) Applying scalars to Pillar 1 requirements if features of the cryptoasset technology could increase the risk of non-payment or delayed payment relative to traditional assets.

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?

## 6. Disclosure requirements of cryptoassets

The 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.[24] As such, in addition to the quantitative information described above, banks must provide qualitative information that sets out an overview of the bank's activities related to cryptoassets and main risks related to their cryptoasset exposures, including descriptions of: (i) business activities related to cryptoassets, and how these business activities translate into components of the risk profile of the bank; (ii) risk management policies of the bank related to cryptoasset exposures; (iii) scope and main content of the bank's reporting related to cryptoassets; and (iv) most significant current and emerging risks relating to cryptoassets and how those risks are managed.

In accordance with the general guiding principles, banks must disclose information regarding any material Group 1a, 1b and Group 2 cryptoasset exposures on a regular basis, including for each specific type of cryptoasset exposure information on: (i) the direct and indirect exposure amounts (including the gross long and short components of net exposures); (ii) the capital requirements; and (iii) the accounting classification.

In addition to the separate disclosure requirements set out above that apply to all Group 1a, 1b and Group 2 cryptoassets, banks must include exposures to Group 1 cryptoassets in the relevant existing disclosure templates that apply to traditional assets (eg for credit risk, market risk).

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

[24] Principle 1: Disclosures should be clear; Principle 2: Disclosures should be comprehensive; Principle 3: Disclosures should be meaningful to users; Principle 4: Disclosures should be consistent over time; Principle 5: Disclosures should be comparable across banks.

## Annex 1: Definitions

**Cryptoassets:** private digital assets that depend primarily on cryptography and distributed ledger or similar technology.

**Digital assets:** a digital representation in value which can be used for payment or investment purposes or to access a good or service. This does not include digital representations of fiat currencies.

**Nodes:** typically participants (entities including individuals) in distributed ledger networks that record and share data across multiple data stores (or ledgers).

**Operators:** typically a single administrative authority in charge of managing a cryptoasset arrangement, performing functions that may include issuing (putting into circulation) a centralised cryptoasset, establishing the rules for its use; maintaining a central payment ledger; and redeeming (withdraw from circulation) the cryptoasset.

**Stablecoins:** cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

**Redeemers:** entities responsible for exchanging the cryptoasset for the traditional asset. It does not necessarily need to be the same as the entity responsible for organising the issuance of the cryptoasset.

**Validators:** an entity that commits transactions blocks to the distributed ledger network.

# Annex 2: Treatment of derivatives referencing Group 2 cryptoassets

This consultation proposes a simple, conservative approach to calculate RWAs for credit and market risk for Group 2 cryptoassets:

RWA = RW x max [abs(long), abs(short)]

A high risk weight (1250%) will lead to a conservative outcome for direct exposures of cryptoassets. However, for derivatives, care should be taken in defining what the 'value' is in the formula to ensure the outcome is similarly conservative.

## (a) Why do we need to be careful about the treatment of derivatives?

Derivatives can have a very low value, but be at risk of causing losses that are many multiples of their value – using the value of a derivative in the above formula would not always provide a conservative capital requirement. Consider the example of a bank that sells a call option on Bitcoin to a client. The option gives the client the right to buy one Bitcoin at any point in the next month for $40,000. The current value of one Bitcoin is $35,000, and the bank calculates the call option is worth $1,000.

If we use the value of the call option as the basis for the RWA in the above formula, then the bank would need to hold $1,000 of capital for the position (ignoring buffers, and assuming for simplicity this is the only cryptoasset it holds).

But $1,000 is not very conservative. If the value of Bitcoin rose to, for example, $45,000 over the next month then the value of the call option to the client would be at least $5,000 – the bank would have lost more than $4,000.

This is a general problem for derivatives in the above formula – the value of the derivative can be very small, but the risk of loss can be many multiples of it. So applying a high RW to the derivative's value will not necessarily result in a conservative outcome.

## (b) Proposed solution

One solution would be to apply the market risk rules to derivatives of cryptoassets. Market risk rules mitigate the problem by applying conservative shocks to the underlying of derivatives, and calculating how much money the bank would lose on the derivative as a result. This is a more accurate reflection of potential loss, but it would make the approach for Group 2 cryptoassets more complex, and mean two separate approaches – one for credit risk and one for market risk.

A simpler alternative is to use the formula proposed in this consultation, and define the value of a derivative to be the value of the underlying assets the derivative references. In the above example, this would mean that instead of using the value of $1,000 for the derivative in the formula, the bank would use the value of one Bitcoin that the derivative references (ie $35,000). The bank would therefore hold capital of approximately $35,000 against the position – the same as if it held a short or long position in one Bitcoin.

One potential drawback of the approach would be that in some situations it could set a capital requirement that is much larger than the maximum loss on a derivative. For example, in the above example the client who bought the call option cannot lose more than the $1,000 it paid (the worst case scenario is that the Bitcoin value falls and the option becomes worthless). If the client was a bank and had to apply the above approach, holding $35,000 of capital seems overly conservative. In order to address this issue, this proposal allows banks to cap the value in the formula at the maximum loss they could suffer on the derivative; ie a $1,000 cap for the buyer of the option and no cap for the seller of the option.