Freshfields Bruckhaus Deringer

Basel and the prudential treatment of cryptoassets - what is the space for banks and how expensive will it become?

Following a challenging year for cryptoassets, 2023 is the year of legislative reform as legislators calibrate their approach to businesses operating in this space. Banks are still hesitant to take on direct exposures to cryptoassets, however this may change. As we stated in our Fintech predictions for 2023, worries about the governance of some of the largest fintechs that have contributed to a number of high-profile collapses may encourage traditional banks to step in and become the driver of tokenisation. At the same time, distributed ledger technology (DLT) and its promise to carry out financing transactions entirely on a chain without any intermediary, ie decentralised finance, (DeFI) has the potential to transform traditional banking functions and challenge the role of banks as the conventional financial intermediaries. Or does it make banks obsolete altogether?

A central part of the answer lies in the prudential treatment of cryptoasset exposures. Banks – unlike unregulated or less regulated challengers – operate within a comprehensive prudential risk management framework that aims to curtail excess leverage and to ensure adequate liquidity as well as a sufficient capital base proportionate to the risks that a bank takes.

How will cryptoasset activities fit into the regulatory perimeter?

The recently published finalised standard on the prudential treatment of cryptoasset exposures (***Final Standard***) by the Basel Committee on Banking Supervision (***BCBS***), the global final standard setter for the prudential regulation of banks, outlines the future regulatory baseline for banks to address risks from cryptoassets. Incorporated into the Basel Framework as a new chapter 'SCO60: Cryptoasset expsoures' and marked for implementation by 1 January 2025, the Final Standard has already been picked up as part of the current legislative procedure to amend the Capital Requirements Regulation (***CRR***) to implement Basel III. As part of its proposal for changes to the CRR, the European Parliament's Economic and Monetary Affairs Committee (***ECON***) invited the European Commission to submit a legislative proposal by June 2023 on a dedicated prudential treatment for exposures to cryptoassets.

The Final Standard attempts to provide a comprehensive approach to the prudential treatment of cryptoasset exposures, addressing in varying detail aspects ranging from the application of the banking/trading book boundary to cryptoassets, to the large exposure requirements. We are focussing on the **main takeaways** and, specifically, where the Final Standard differs from the regime applicable to 'traditional' assets.

I. Scope of the cryptoasset framework

The Final Standard casts a wide net to capture what it defines as cryptoasset exposures. Cryptoassets are defined as 'private digital assets that depend on cryptography and DLT or similar technology.' Digital assets are, in turn, defined as 'a digital representation of value, which can be used for payment or investment purposes or to access a good or service.' Accordingly, virtually all forms of tokens represented on a DLT are cryptoassets within the meaning of the proposal.

Importantly, the Basel Framework clarifies that cryptoasset exposures include dematerialised securities issued through DLT or similar technologies. In turn, dematerialised securities that rely on electronic versions of traditional registers or databases that are **centrally administered** are not in scope. This may, for example, impact the nascent market for **digital bonds** where it relies on centrally administered registers which would therefore be out of scope of the Final Standard. Central bank digital currencies are not yet within the scope of the Basel Framework and the Committee intends to consider its treatment 'as they are issued.'

The proposal also includes a new definition of the term 'exposure' as 'on- or off-balance sheet amounts that give rise to credit, market, operational and/or liquidity risks'

with certain parts of the Final Standard – such as the risk management requirements – also applying to cryptoasset activities such as the safekeeping or administration of client cryptoassets that do not give rise to any credit, market or liquidity requirements.

II. Cryptoassets: The Good, the Bad…?

The Committee proposes to classify cryptoassets into two categories.

1. Group 1 cryptoassets

Group 1 cryptoassets are those cryptoassets that meet four classification conditions, namely:

(1) They are either tokenised traditional assets ('**Group 1a cryptoassets**') or cryptoassets with an effective stabilisation mechanism ('stablecoins; **Group 1b cryptoassets**').

(2) All rights, obligations and interests arising from the cryptoasset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed. The applicable legal framework must also ensure settlement finality. Banks must conduct a legal review of the arrangements and arrange for an independent legal opinion (if there was no public disclosure approved by a regulator for the offering of the relevant crypto asset).

(3) The functions of the cryptoassets and the network on which it operates are designed and operated to sufficiently mitigate and manage any material risks.

(4) Entities that execute redemption, transfers, storage or settlement finality of the cryptoassets, as well as those entities that manage or invest reserve assets (backing the stabilisation mechanism), must be regulated and supervised (with the exception of note validators, which may instead be subject to appropriate risk management Final Standards) and have in place and disclose a comprehensive governance framework

Banks are responsible, on an ongoing basis, for assessing whether the cryptoassets to which they are exposed are compliant with the classification conditions. Further, the Final Standard requires banks to inform their supervisor of the classification decisions they have reached for each cryptoasset before the implementation date and in advance of any subsequent acquisition of cryptoassets with 'sufficient time for the supervisor to review and, if necessary, **override the classification decision** reached prior to the bank's acquisition of the cryptoasset.' This is a deviation from the consultation proposal which required prior supervisor approval for the classification decision. However, it is not quite clear whether the Final Standard foresees a formal no-objection procedure similar to the procedure required for the acquisition of a significant holding or whether informing supervisors will be sufficient.

Tokenised traditional assets, or Group 1a cryptoassets, are digital representations of traditional assets (eg a corporate bond, a loan, a deposit, or an equity) using DLT or a similar technology to record ownership which pose the same level of credit and market risk as the traditional (non-tokenised) form of the asset. If the classification conditions are met, the treatment of credit risk for Group 1a cryptoassets held in the banking book generally follows the RWA treatment as the non-tokenised traditional asset under the existing Basel Framework subject to a potential RWA capital add-on for infrastructure risk that may be imposed by the regulator (see below). However, banks are required to assess whether the tokenised traditional asset in fact confers the same level of legal rights as a traditional asset. Further, the liquidity characteristics of tokenised traditional assets may differ from the traditional assets which is why the Final Standard emphasises that banks must assess separately whether Group1a cryptoassets comply with the relevant eligibility requirements for collateral used for CRM purposes and not assume qualification for a given treatment simply because the traditional (non-tokenised) asset qualifies.

Cryptoassets with effective stabilisation mechanisms, or Group 1b cryptoassets, are designed to be redeemable at all times for a predefined amount of a reference asset(s) or cash equal to the value of the reference asset(s), ie at a specific 'peg value.' In order to be deemed effective, the stabilisation mechanism must meet certain governance requirements, including that the issuer must be supervised and regulated by a supervisor that applies prudential capital and liquidity requirements. Group 1b cryptoassets are also subject to a specific redemption risk test. Under the test, banks must ensure that the value and composition of reserve assets at all times equals or exceeds the peg value of all outstanding cryptoassets (potentially requiring sufficient overcollateralisation), that reserve assets who are pegged to one or more currencies meet certain asset quality criteria and that the governance arrangements relating to the management of reserve assets must be comprehensive and transparent (including daily disclosure of their value and an internal audit requirement).

Banks that have banking book exposures to Group 1b cryptoassets must analyse their specific structures and identify all risks that could result in a loss ('look through approach'). Credit risk for Group 1b cryptoassets may arise from different sources:

- **Risk from reference asset** – If the reference asset gives rise to credit risk, banks are exposed to the

default of the reference asset's issuer. Banks must therefore include in their credit RWA the RWA that would apply to a direct holding of the reference asset.

- **Risk of default of the redeemer** – Banks may be exposed to a default of the entity that performs the redemption function. If a bank only has an unsecured claim for redemption, the cryptoasset may become worthless. Accordingly, banks must take into account whether they have an unsecured or secured claim or whether they may be able to avoid any credit risk to the redeemer because the reserve assets are held in a bankruptcy remote SPV (which requires a legal opinion affirming that relevant courts would recognise underlying assets held in a bankruptcy remote manner as those of the cryptoasset holder).
- **Risks arising when intermediaries perform the redemption function** – where not all holders of cryptoassets can transact directly with the redeemer but rely on intermediaries to redeem cryptoassets, banks may be exposed to additional risks with the specific risk depending on whether the bank is itself one of the intermediaries or relies on other intermediaries to redeem their cryptoassets for cash/reserve assets.

Importantly, and distinct from Group 1a cryptoassets, Group 1b cryptoassets that a bank receives as collateral are not permitted to be recognised as eligible collateral for the purposes of calculating regulatory capital requirements even where they are redeemed for traditional instruments that are included on the list of eligible financial collateral. This restriction further underlines the conservative approach since the treatment of units or shares in CIU as collateral under the CRM framework demonstrates that it would have also been an option to distinguish further, depending on the type of reference assets (Art. 197(5) CRR).

2. Group 2 cryptoassets

Group 2 cryptoassets are all other cryptoassets that do not meet the classification criteria for Group 1 assets, including unbacked cryptoassets. The Final Standard aims to subject Group 2 cryptoassets to a conservative capital treatment reflecting the additional and higher risks posed compared with Group 1 cryptoassets.

The specific capital treatment of holdings in Group 2 cryptoassets depends on whether a bank is able to hedge its position in the cryptoassets according to specified hedging recognition criteria (which include requirements on market capitalisation and liquidity/trading volume).

Where these hedging recognition criteria are met, banks may apply a modified version of the Simplified Standardised Approach (SSA) or the Standardised Approach (to market risk to all positions affected by changes in Group 2a cryptoasset prices. Group 2a cryptoassets are always treated according to market risk rules independent of whether they result from banking or trading book instruments. The Internal Models Approach is not applicable to Group 2a cryptoassets. Further, even where the hedging recognition criteria are met the Final Standard only provides for a limited amount of recognition: When establishing the net position for a Group 2a cryptoasset under the SSA, the Final Standard only allows for a recognition of the hedge of 65 per cent, further underlining the conservative approach.

Where these hedging recognition criteria are not met, banks are required to apply a conservative prudential treatment, applying a risk weight of 1250 per cent to the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in the cryptoassets, thereby requiring holding of capital at least equal to the value of Group 2 cryptoasset exposure. Thus, the BCBS in effect applies the prohibitive treatment that would apply under the fall-back approach to exposures to fund units or shares in a CIU (Art. 132(2) subsection 2 CRR) and securitisation positions (Art. 254(7) CRR). There is also no separate trading book and banking book treatment for Group 2b cryptoassets and the conservative treatment is intended to capture both the credit and market risk (but the position is only reported as credit risk).

III. Group 2 exposure limits

Banks will be subject to an **exposure limit** for Group 2 cryptoassets that applies to the aggregate direct (cash and derivatives) and indirect (eg investment funds, ETF/ETN) holdings in Group 2 cryptoassets. A bank's total exposure in Group 2 cryptoassets should not generally be higher than 1 per cent of the bank's Tier 1 capital and must not exceed 2 per cent of the bank's Tier 1 capital.

The exposure limit is calculated the same way as exposure to Group 2b cryptoassets, meaning that the greater of the absolute value of the aggregate long positions and the absolute value of the aggregate short positions in each Group 2 cryptoasset must be included in the calculation. This is a relief compared to the second consultation which had applied the aggregate of the absolute values of long and short exposures, and which would have meant that hedge exposures would have counted towards the limit.

A breach of the 1 per cent limit requires a notification of the regulator and all exposures in excess of the threshold will be subject to the 1250 per cent RWA treatment for Group 2b cryptoassets. If a bank exceeds the 2 per cent limit, all Group 2 cryptoassets will be subject to the 1250 per cent RWA treatment for Group 2b cryptoassets resulting in a 'cliff effect' and sudden increase in RWAs. The Final Standard has

IV. Infrastructure Risk Add-on

Even where banks are meeting the stringent requirements for Group 1 cryptoassets, a holding in cryptoassets may become subject to a capital add-on for infrastructure risk compared to holding a traditional asset. The Committee does not specify any particular risk to require an add-on but is concerned that DLT is still new and evolving and may pose various unforeseen risks.

Arguably, the proposal thereby deviates from a technology-neutral approach and adds a risk add-on that is not grounded in the structural arrangements of Group 1 cryptoassets but based on the technology itself. Different from the consultation, and after criticism from the industry, the Committee has agreed to replace a fixed 2.5 per cent RWA add-on with a more flexible approach that allows authorities to initiate and increase an add-on.

V. Other noteworthy aspects

The Final Standard requires banks to reflect direct or indirect exposures to cryptoassets in their risk management policies. Thus, the Final Standard does not deviate from current practice. It further requires that banks inform their supervisory authorities of their policies and procedures, assessment results and actual or planned cryptoasset exposures 'in a timely manner' and to demonstrate that they have fully assessed the permissibility of their activities, the risks and how they have mitigated such risks.

The Final Standard lists certain risks that bank need to consider in their risk management framework, including cryptoasset technology risk (stability of the DLT; its validation design: permissioned or permissionless; service accessibility and the trustworthiness of node operators and operator diversity), information, communication and technology (ICT) and cyber risks (such as cryptographic key theft, compromise of login credentials, and distributed denial-of-service ("DDoS") attacks), legal risks (such as lack of accounting Final Standards, legal uncertainty on ownership), AML/CTF risks and risks in properly valuating/mispricing cryptoassets.

Risks relating to cryptoasset exposures are subject to the Supervisory Review and Evaluation Process (SREP), and the Final Standard makes reference to the full range of action that supervisors may take upon the identification of capital inadequacy or shortcomings in bank risk management, including that additional capital charges may be needed in cases where the bank risk management of cryptoassets is considered inadequate.

The Final Standard also requires banks to disclose an overview of their activities related to cryptoassets and main risks related to their cryptoasset exposures as part of their Pillar 3 disclosure, including descriptions of:

- business activities related to cryptoassets, and how these business activities translate into components of the risk profile of the bank;
- risk management policies of the bank related to cryptoasset exposures;
- scope and main content of the bank's reporting related to cryptoassets; and
- most significant current and emerging risks relating to cryptoassets and how those risks are managed.

Finally, the application of liquidity risk requirements to cryptoassets largely relies on the application of the Net Stable Funding RatioNSFR) and Liquidity Coverage Ratio (LCR) for traditional exposures with economically equivalent risks with a number of clarifications. Importantly, treatment of cryptoassets as high-quality liquid assets (HQLA) is only available to Group 1a cryptoassets and requires that both the traditional asset and its tokenised form meet the HQLA definition.

VI. Conclusion and next steps

The Final Standard marks an important step in reflecting the specific risks posed by cryptoassets within the existing prudential framework. That said, not everyone may be convinced that the BCBS struck the right balance between its guiding principles of mitigating financial stability concerns, providing a framework that is technology-neutral and only accounts for any additional risks arising from cryptoasset exposures relative to traditional assets ('same risk, same activity, same treatment') and a simple design for what is still a relatively small asset class for banks.

Banks will want Group 1 treatment for any exposure to digital assets which, by and large, allows the application of prudential rules for traditional assets that banks are familiar with. For that, the Final Standard provides a mix of bottlenecks (eg that all relevant intermediaries must be regulated and supervised; the applicable legal framework must ensure settlement finality) and a good deal of red tape (such as potential legal opinions; the obligation to inform supervisors of classification decisions for each cryptoasset).

Whether the Final Standard will prove to be impactful depends on a range of factors that are difficult to predict in detail, most importantly on the future role of banks (eg will banks primarily act as an intermediary or hold significant exposure to cryptoassets themselves?) and to which degree and at which pace traditional assets will be replaced by dematerialised assets in scope of the Final Standard.

Contacts

Alexander Glos

Partner

Freshfields Bruckhaus Deringer
Rechtsanwälte Steuerberater PartG mbB
Bockenheimer Anlage 44, 60322 Frankfurt am Main

T +49 69 27 30 85 05
E alexander.glos@freshfields.com

Holger Hartenfels

Counsel

Freshfields Bruckhaus Deringer
Rechtsanwälte Steuerberater PartG mbB
Bockenheimer Anlage 44, 60322 Frankfurt am Main

T +49 69 27 30 83 05
E holger.hartenfels@freshfields.com

Marius Rätz

Principal Associate

Freshfields Bruckhaus Deringer
Rechtsanwälte Steuerberater PartG mbB
Bockenheimer Anlage 44, 60322 Frankfurt am Main

T +49 69 27 30 82 14
E marius.raetz@freshfields.com

freshfields.com