Safe Bank 2(99) 2025

DOI: 10.26354/bb.12.2.99.2025

M. Konrad Borowicz*
ORCID: 0000-0001-5088-106X
M.K.Borowicz@tilburguniversity.edu

What Crypto Risks Can Bank Take (in the EU)?

Abstract

This article examines the types of crypto-asset risks that EU banks can prudently take under the transitional regulatory regime introduced by Article 501d of CRR3 and supplemented by the EBA's draft regulatory technical standards (RTS). The analysis is grounded in the evolving EU legal framework, particularly MiCAR and CRR3, and considers how banks may engage with crypto-assets through custody, payments and trading, and issuance. It also reviews industry responses to the draft RTS and highlights key accounting challenges, especially the tension between fair value and cost models under IFRS. It concludes that while crypto offers strategic and technological opportunities for banks – particularly in custody and tokenized finance – their ability to scale such activities remains heavily constrained by prudential rules and regulatory uncertainty.

Keywords: crypto-assets, crypto custody, Capital Requirements Regulation (CRR3), Markets in Crypto Assets Regulation (MiCAR), prudential regulation, stablecoins, Basel framework

JEL codes: G21, G28, G32, O33, M41

Introduction

Banks – traditionally conservative and heavily regulated entities – are increasingly pressed to determine if and how they should participate in the crypto-asset market. But what crypto risks can banks take? This question has taken on particular relevance as regulators develop new rules to govern banks' crypto exposures. The Basel Committee for Banking Supervision (BCBS) has developed a comprehensive standard for the prudential treatment of crypto-asset exposures (BCBS 2022). In the European Union, regulators have responded with a transitional prudential regime for crypto-assets in banks, included in the latest banking regulation reforms. Notably, Regulation (EU)

* M. Konrad Borowicz – Assistant Professor, Tilburg Institute for Law, Technology and Society, Tilburg University.

2024/1623 (the Capital Requirements Regulation's "quick fix" often dubbed CRR3) introduced Article 501d, which sets out transitional provisions on the prudential treatment of crypto-asset exposures. Article 501d became applicable on 9 July 2024, meaning that from that date EU banks are subject to specific capital requirements and limits for any crypto-asset exposures they hold. This was ahead of most other CRR3 measures (which entered into force on 1 January 2025) and reflects EU regulators' desire to immediately constrain bank crypto-risk pending a full framework.

Article 501d tasks the European Banking Authority (EBA) with developing regulatory technical standards (RTS) on how banks should calculate and aggregate their crypto exposures during this transitional period. In response, on 8 January 2025 the EBA published a draft RTS on the calculation and aggregation of crypto exposure values. This draft RTS, which until recently was at the consultation stage – comments were open until 8 April 2025 – specifies detailed methodologies for categorizing crypto-assets, applying risk weights, recognizing hedges, and computing exposure values across risk types. The final version is expected to be submitted to the European Commission by 10 July 2025. Once submitted, the Commission is anticipated to adopt the RTS as a regulation, which will supplement and give technical effect to the broader requirements set out in Article 501d of CRR3.

In parallel, and adding some complexity to the regulatory landscape, the European Commission is expected – pursuant to recital 59 of CRR3 – to propose a separate legislative act by 30 June 2025 to implement the 2024 version of the BCBS standard for the prudential treatment of crypto-asset exposures. While this forthcoming proposal is likely to align with the EBA's draft RTS, its precise scope remains unknown as of May 2025. The analysis that follows is based on the draft RTS, which, although not yet adopted, offer useful insight into how a bank's risk function – illustrated here using the example of SAFE Bank – should interpret and apply prudential rules for crypto-assets during the transitional period. Throughout this article, I examine the rationale behind these rules, assess industry feedback on the draft RTS, and explore related considerations such as accounting treatment, all of which inform how banks weigh decisions to engage with crypto-asset exposures in the EU.

1. How do banks engage with crypto-assets, and why would they want to?

1.1. Modes of bank crypto-asset engagement

In EU law, the Markets in Crypto Assets Regulation (MiCAR) defines the range of possible crypto-asset engagements, which it defines as "crypto-asset services."[1] These can be categorized into: (1) custody, (2) payment and trading services,[2]

1 Article 3(1)(16).

2 These range from transmission of order on behalf of clients, through exchange of crypto-assets for funds or other crypto-assets, transfer services, to execution of orders on behalf of clients and operation of trading platforms.

(3) issuance and (4) portfolio management and advisory services. For the discussion, I will disregard (4) as it does not trigger any prudential requirements, which are the core focus of this article. Under Article 59, to perform any and all of crypto-asset services, a person must either be an authorized crypto-asset service provider or a credit institution (or another licensed provider of financial services). MiCAR thus allows credit institutions (refer to hereinafter, for simplicity, as banks) to provide these services but only if, in line with Article 60, they notify their competent authority in advance and ensures full compliance with MiCAR's conduct, prudential, and organizational requirements.

1.2. Custody

In this model, the bank acts as a custodian of crypto-assets on behalf of its clients, similar to how a traditional custody bank safeguards stocks or bonds for asset managers (Chan et al. 2007).[3] The bank does not own the crypto-assets but provides secure storage and related services, presumable leveraging specialized digital vaults or third-party custody solutions to manage and protect the private keys controlling access to these assets. When structured correctly, the crypto-assets remain the legal property of the clients (Low and Teo 2017), and the bank functions purely as a service provider – even though, as Zetzsche and Nikolakopoulou (2025) have shown, the terms of custody agreements vary enormously.

For example, if SAFE Bank's corporate client deposits 10 BTC, the Bitcoin would typically be recorded off the bank's balance sheet as a client asset. The bank might reflect this through a custodial liability or off-balance-sheet disclosure[4], depending on jurisdictional accounting practices.[5] Critically, the bank does not assume market risk from the price volatility of the crypto-asset; any gains or losses accrue solely to the client. However, the bank does take on *operational risk* – particularly cybersecurity and key management risks – and could face legal exposure if it fails to safeguard the assets appropriately. Under CRR3, the operational risk associated

[3] An alternative to the custodial model is the non-custodial or self-custody model, in which the client – not the bank – retains exclusive control over the private key and thus maintains full control over their crypto-assets. This model falls outside the scope of the regulations analyzed, as it does not constitute a service provided by a financial institution and does not generate any balance-sheet exposures or capital requirements for the bank.

[4] Staff Accounting Bulleting (SAB) 121, issued in 2022 in the U.S., required crypto custody assets to be on the balance sheet with a liability. 17 CFR Part 211. Interestingly, shortly thereafter it was rescinded through SAB 122. As Krause (2025) notes, this shift was driven by factors such as the adoption of Fair Value Accounting and the Trump administration's pro-crypto stance.

[5] Basel III requires banks to report crypto-assets held under custody within Template CAE1, providing a clear view of the volume and nature of crypto-assets for which the bank acts as custodian (Basel Committee on Banking Supervision 2024). Although these assets are off-balance-sheet, banks are still expected to disclose them in aggregate form in the narrative accompanying the CAE1 template, reinforcing transparency around the scale and scope of custodial crypto activities.

with such services my trigger Pillar 2 add-ons, if supervisors assess the bank's control framework as insufficiently mature.

The custody model also encompasses reserve assets deposited at a bank by issuers of a crypto assets, the value of which is backed by such reserve assets, such as e-money tokens (EMTs referencing the value of a single currency) or asset-referenced tokens (ARTs – a stablecoin that is not an EMT, for example, because it purports to maintain a stable value by referencing multiple currencies rather than a single currency.). MiCAR requires the issuers of such crypto assets to deposit reserve assets either with banks or investment firms authorized to provide the ancillary service of "safekeeping and administration of financial instruments for the account of clients." While such custody services fall outside of the definition of crypto-asset services under MiCAR, they can have an impact on the bank's prudential obligations. Like crypto custody, market and credit risk for the bank are limited, as the reserve assets are not held on the bank's own account, and any fluctuations in value or credit events are borne by the issuer or token holders. However, operational risk remains material – the bank must ensure the safekeeping, segregation, and availability of reserve assets at all times, particularly under stress scenarios.

Crucially, because these deposits are intended to be available on demand to support token redemptions, they may also introduce liquidity risk for the custodian bank. When assessing the liquidity risk profile of deposits received from stablecoin issuers, regulators and banks must consider both the behavioral characteristics of these deposits and the operational role they serve. Under the liquidity coverage ratio (LCR) framework, there may be grounds to classify such deposits similarly to those from other financial institutions, given the nature of the depositor and the potential volatility of the balances (Coste 2024). Specifically, deposits from stablecoin issuers – used to back the issuance of EMTs or ARTs – could be characterized either as: (i) operational deposits from financial institutions, where the deposit supports clearing, custody, or cash management services provided by the bank, or (ii) non-operational deposits from financial institutions, which are generally assumed to be more volatile and subject to higher outflow rates under the LCR (Coste 2024).

The appropriate classification depends on the underlying contractual arrangements and the degree of operational integration between the issuer and the bank. For example, if the reserve account is used solely for regulatory segregation without supporting additional operational services, it may be more appropriate to treat it as non-operational, attracting a higher assumed outflow rate. Conversely, if the bank is providing broader transactional services to the stablecoin issuer, an operational deposit classification may be justified – potentially resulting in a lower outflow rate for LCR purposes.

In either case, the key consideration for risk and treasury teams is that these deposits are potentially unstable, especially during periods of market stress or redemption pressure. Supervisors may therefore expect banks to hold high-quality liquid assets against these liabilities and demonstrate that they have adequate liquidity buffers to accommodate sudden outflows linked to stablecoin redemptions.

1.3. Payment and trading services

Banks may take incremental steps toward the intermediation of crypto-asset transactions, starting with services that most closely resemble traditional payment activities. Among these, the most accessible initial offerings are likely to be the exchange of crypto-assets for funds or other crypto-assets, and the transfer of crypto-assets on behalf of clients. These functions – permitted under MiCAR – are operationally comparable to fiat currency conversion and payment initiation. They can be structured in ways that limit the bank's direct exposure to crypto-assets, particularly where transactions are client-driven and settled on a delivery-versus-payment basis.

As banks gain confidence and build internal capabilities, a natural progression is to expand into the reception and transmission of client trading orders,[6] and ultimately, the execution of those orders. In the reception and transmission model, the bank forwards a client's instruction to a third-party trading venue – such as a MiCAR-registered crypto exchange or broker – without executing the trade itself. This is a relatively low-risk, off-balance-sheet service that avoids proprietary exposure and is therefore considered a conservative entry point for banks exploring crypto-asset markets under MiCAR.

However, once a bank begins offering exchange, transfer, or execution services, it may start to incur on-balance-sheet exposures, depending on how those services are delivered. For example, if SAFE Bank facilitates the exchange of crypto-assets for euros or transfers tokens on behalf of clients using its own wallet infrastructure, it may temporarily hold either fiat or crypto-assets during the settlement process. Similarly, if the bank uses its own liquidity to fulfill an execution order – such as pre-funding a trade or facilitating internal matching – these positions may qualify as exposures under CRR3, with corresponding capital requirements.

Where these exposures are short-term and linked to client facilitation or market-making, they are generally booked in the trading book and must be capitalized under the revised market risk framework,[7] as adapted for crypto-assets. If the exposures are held longer-term – such as for settlement or reserve management purposes – they may fall into the banking book, attracting capital charges under the credit risk framework.[8] In either case, the regulatory expectation is clear: as banks

[6] MICAR, Article 3(1)(9)(g). In 2024, Deutsche Bank has been reported to expand its partnership with Austrian fintech unicorn and cryptocurrency exchange Bitpanda, granting the bank's clients the ability to deposit or withdraw their fiat currencies from Bitpanda through Deutsche Bank accounts (Montager 2024).

[7] Banks must also calculate the counterparty credit risk charge for over-the-counter (OTC) derivatives, repo-style and other transactions booked in the trading book, separate from the capital requirement for market risk. Basel Framework, CRE55, available at https://www.bis.org/basel_framework/chapter/CRE/55.htm.

[8] To mitigate risk and regulatory burden, banks will often seek to structure these services so that settlement occurs on a delivery-versus-payment (DvP) basis, with pre-funded accounts or trusted intermediaries reducing or eliminating counterparty credit exposure. When structured in this way, and if the bank does not retain inventory or take principal risk, the resulting exposures may be minimal or temporary, and the associated capital requirements correspondingly low.

expand their crypto service offerings beyond pure intermediation, they must assess how each activity impacts their prudential metrics and ensure that the relevant capital, liquidity, and risk governance requirements are fully integrated into their operational model.

1.4. Issuance

MiCAR also allows banks to issue crypto-assets, specifically either EMT (Article 48(1)(a)) or ART (Article 16(1)(b)). If a bank – such as SAFE Bank – were to issue either an EMT or an ART, it would assume the role of guarantor of the token's value, much like an e-money institution issuing e-money in exchange for the receipt of funds. In this context, it is important to note that MiCAR requires issuers of EMTs and ARTs to fully back (cover) the value of issued tokens with reserve assets on a 1:1 basis, explicitly ruling out the possibility of employing a fractional reserve model. The reserve assets backing the tokens – held on balance sheet but legally segregated – must be capitalized according to their risk weights under CRR3. For example, cash held at a central bank would receive a 0% risk weight, while deposits with commercial banks or non-sovereign bonds may attract higher charges.

Furthermore, these reserve assets contribute to the leverage ratio exposure measure and may affect the bank's LCR and Net Stable Funding Ratio (NSFR), especially given the EMT's and ART's redeemable-on-demand nature. Crucially, the issuance of such tokens does not trigger *new* capital, LCR or NSFR requirements as SAFE bank to the extent reserve assets comprise an existing pool of SAFE Bank's assets. When the issuer of an EMT or an ART is a bank, as Coste (2024) notes, the bank has no change in the total amount of assets it holds, only a change in the structure of its liabilities.

Beyond these Pillar 1 considerations, supervisors may also assess Pillar 2 capital requirements, particularly where EMT or ART issuance introduces material operational, liquidity, or reputational risk. For example, the bank must ensure that it can meet large-scale redemptions under stress. To that end, MiCA requires banks to develop robust redemption and recovery plans, for EMT, under Article 55 and, for ART Article 46 (recovery) and 47 (redemption), outlining how reserves would be liquidated and token holders made whole in the event of market disruption or insolvency. The EBA has issued accompanying guidelines (2024/13) on orderly redemption planning, essentially requiring banks to prepare a "stablecoin living will" to protect token holders and preserve financial stability.

Banks can also issue tokenized securities – for instance, a digital bond issued as a blockchain-native token rather than through a traditional securities depository. From a prudential standpoint, the key consideration is that the tokenized form does not alter the underlying economic characteristics of the instrument. As long as the token represents a traditional financial instrument (e.g., a debt security issued under standard legal terms), its treatment under CRR/CRD remains the same as its conventional equivalent.

Each of these three modes crypto-asset engagements can entail different on-balance-sheet exposures. Pure custody might keep crypto off the balance sheet but requires disclosure; trading and settlement on behalf of client will put some assets on balance sheet; token issuance does not create any new assets on the balance sheet but acceptance of reserve assets on deposit creates new liabilities. The EBA's draft RTS and CRR3 Article 501d are primarily concerned with *exposures* – i.e., where the bank itself is at risk from crypto-asset value changes or counterparty defaults. In our scenario, SAFE Bank's relevant exposures would include any crypto-assets it owns under the trading or banking book (like the BTC inventory), any credit exposures to counterparties in crypto trades on behalf of clients, and reserve assets for the stablecoins it has accepted on deposit.

1.5. Business case for banks: opportunities vs. risks

Why would SAFE Bank even consider getting into such a complicated and risk-fraught business as crypto services? First, there is growing demand from certain client segments – high-net-worth individuals, institutional investors, corporates dealing with blockchain projects – for custody and banking services related to crypto. Banks fear that if they do not offer these services, clients will turn to alternative providers (such as fintech companies or foreign banks). For example, SAFE Bank's wealth management clients might already be buying Bitcoin through crypto exchanges; by offering an in-house custody solution, SAFE could keep those assets within its ecosystem, earning fees and deepening the client relationship.

Second, crypto services can be fee-driven. Custody can generate safekeeping fees; trading services earn commissions or spreads; tokenization could lead to investment banking fees. If the crypto market grows, this could be a new stream of non-interest income. Some banks also see the possibility of market-making in crypto or offering crypto-structured products to clients, which come with trading profits and arrangement fees.

Third, beyond immediate revenue, banks have a strategic interest in blockchain and digital assets. Many in the industry believe that finance is gradually tokenizing – e.g., securities and even currencies might largely operate on distributed ledgers in the future. Being involved early allows a bank to build expertise and technology. For instance, by mastering how to custody crypto, SAFE Bank also builds capability to custody future central bank digital currencies (CBDCs) or tokenized stocks. There's a first-mover advantage argument: a bank that successfully integrates crypto could become a leader in the next generation of financial services, whereas those that abstain entirely might struggle if and when digital assets become mainstream.

Finally, some banks are exploring crypto (particularly stablecoins or blockchain networks) to improve payment and settlement efficiency. International payments using a well-designed stablecoin or blockchain can be faster and cheaper than legacy correspondent banking. A bank might not necessarily take on significant

crypto holdings to use these benefits – it could simply use the technology – but in practice to use, say, a USD stablecoin, the bank has to hold some of that stablecoin and interact with its issuer. The business case here is operational improvement and potentially offering near real-time cross-border payments as a product.

However, against these potential upsides, the profitability of banks' crypto ventures remains highly uncertain and likely low in the short term. Several reasons contribute to this skepticism. First, as I will detail in the next section, the prudential treatment of crypto exposures can be punitive. Compliance costs are also significant – banks need robust anti-money laundering (AML) controls for crypto transactions, monitoring systems for blockchain activity, new IT infrastructure, and training for staff. All these investments may not be justified by the small scale of revenues from an emerging market[9].

Second, it's not guaranteed that mainstream bank clients will flock to bank-provided crypto services at prices that make it profitable. Many crypto enthusiasts prefer self-custody or using specialized crypto firms. On the flip side, risk-averse bank clients might not be interested in crypto at all. So banks could find either low uptake or that they are competing against crypto-native companies with lower cost structures.

Third, offering crypto services exposes banks to risks that can lead directly to financial loss – for example, a cyber breach resulting in theft of crypto-assets might cost the bank money (either directly if its own assets are stolen or via liability to clients). Unlike traditional assets where infrastructures and legal frameworks are well-established (e.g., theft of stocks from a custodian is extremely rare and usually insured), crypto is a newer domain. Banks may need to spend heavily on technology and insurance to mitigate these risks, further cutting into any profits.

Finally, the evolving regulatory landscape itself is a risk. Banks could invest in setting up a crypto trading desk only to find regulations tighten further, or conversely invest in capabilities that become redundant if regulation shifts in favor of a different model (for example, if central bank digital currencies reduce the need for private stablecoins).

In conclusion, while banks do have plausible reasons to engage with crypto – client demand, new business lines, staying future-proof – the actual profitability of such ventures is highly uncertain and likely low under current conditions. As we move to the next sections, which detail the regulatory capital requirements, it will become even clearer why only a very measured exposure to crypto may be feasible. In the case of SAFE Bank, suppose the bank's strategy team forecast €5 million in

[9] With respect to EMT issuance, adherence to MiCAR's rules on full reserve backing and redemption rights means the bank is converting some of its funding into a narrow, ring-fenced structure: it raises funds via stablecoin issuance and must hold those funds in cash and high-grade bonds. This could be viable for offering new digital payment instruments to clients or for on-chain settlement use cases, but it limits the bank's ability to use those funds for lending. From a profitability standpoint, an issuing bank might earn a small return on the reserve assets (e.g. interest on bonds) but cannot pay interest to stablecoin holders, meaning the business model resembles a utility (like a payments service) rather than a traditional spread-lending approach.

annual fees from a new crypto service. The risk team would weigh that against the potential capital charge: if SAFE needs to allocate, say, €50 million of capital to back the exposures and operational risks, and hold perhaps another few million for operational risk, the return on that capital might be quite unattractive. Moreover, if a single incident or market crash could wipe out several years' worth of fees, the risk/reward calculus might suggest that the bank *cannot take* much crypto risk at all without endangering its safety and soundness standards.

2. Prudential treatment of crypto under CRR3

With an understanding of why a bank might limit its crypto activities, we now turn to the crux of the regulatory constraints: the prudential rules that determine how crypto exposures are treated for capital and risk management purposes. The European Union has moved swiftly to impose an interim regime via CRR3's Article 501d, acknowledging in recital 59 that a fully fleshed-out framework will take a few more years to implement. In this section, I explain the transitional prudential framework in place from 2024 onward, focusing on, first, the categories of crypto exposures defined in Article 501d(2) and, second, the specific capital requirements (risk weights and limits) attached to each.

2.1. Categories of crypto-asset exposures under Article 501d(2)

Article 501d(2) CRR3 breaks down crypto-asset exposures into three main categories, aligned largely with the types of crypto-assets defined in MiCAR: (1) tokenized traditional assets, (2) asset-referenced tokens and (3) other crypto-assets.

2.2. Tokenized traditional assets (Article 501d(2)(a))

These are crypto-assets that represent traditional assets. In simpler terms, if an asset exists on a blockchain but its value is derived from or backed by a non-crypto asset (e.g. a share, a bond, a commodity, or a *single* fiat currency), it falls under this category, provided it doesn't depend on other crypto-assets for value. This includes things like security tokens (digital representations of stocks or bonds) and EMTs. The regulatory logic here is that the risk of these exposures should mirror the risk of the traditional asset they represent. For example, if SAFE Bank holds a token that represents a sovereign bond, the primary risk is that (credit) of the issuer, not something fundamentally new.

2.3. Asset-referenced tokens (Article 501d(2)(b))

ARTs under MiCAR are essentially stablecoins or similar tokens that maintain a stable value by referencing a pool of assets, which can include fiat currencies, or commodities. Examples: a stablecoin backed by a mixture of cash and government bonds, or a token pegged to gold (with physical gold in reserve). The prudential treatment for banks' exposures to such ARTs is meant to be less strict than for completely unbacked crypto, but (as we'll see) still significantly more conservative than treating them like the actual underlying assets.

2.4. Other crypto assets (Article 501d(2)(c))

This is the catch-all category. It includes all crypto-assets that are *not* covered by (a) or (b). In essence, this means cryptocurrencies with no intrinsic backing (like Bitcoin, Ether, etc.), utility tokens, and any exotic crypto assets, as well as any asset-referenced tokens or EMTs or ARTs that *fail* certain criteria (e.g., perhaps an EMT issued by a non-compliant firm, or an ART that references crypto instead of traditional assets). As noted, even some tokens that would otherwise be (a) or (b) drop into (c) if they depend on crypto for value or are non-compliant. The EU regulators clearly view this category as the riskiest, since it captures volatile, speculative assets.

2.5. Capital requirements and exposure limits in the transitional regime

Under Article 501d's transitional provisions (effective July 2024 onwards), the classification described above directly translates into capital charges and quantitative constraints for banks.

2.6. Tokenized traditional assets (Article 501d(2)(a))

As mentioned, these are treated as exposures to the underlying assets. If the underlying is a cash claim or a traditional security, existing CRR2 rules for credit, market, and counterparty risk apply. In practice, if SAFE holds a tokenized government bond within its trading or banking book, the risk weight is the same as if SAFE held the actual bond (so if it's a high-quality sovereign, likely a 0% or low risk weight).

A similar treatment would apply to an EMT issued by a AAA-rated bank. In this case, holding the EMT is economically equivalent to holding a deposit balance with the issuer, fully redeemable at par in fiat currency. If the EMT meets all MiCA classification criteria – including full reserve backing, legal redemption rights, and transparency – the bank's exposure to the token could be treated as a deposit

with a AAA-rated bank, likely attracting a 20% or lower risk weight, depending on maturity.

However, the bank must also consider whether the holding introduces market or counterparty risk, depending on how the tokenized asset is structured and used. If the token is held in the trading book and is subject to fair value fluctuations, it may give rise to market risk under the trading book rules – especially if it is actively traded or valued mark-to-market. This would typically apply to tokenized securities whose prices vary in response to interest rates, credit spreads, or liquidity factors, even if the underlying asset is conventional.

In addition, counterparty credit risk may arise if the tokenized asset involves contractual settlement with a third party, such as through smart contracts or when exposures are cleared or margined via an intermediary. For example, if the token is held through a bilateral or centrally cleared structure involving deferred settlement or collateralized margining, then the bank must calculate exposure-at-default under the standard counterparty credit risk rules, as it would for any other OTC financial instrument.

2.7. Asset-referenced tokens (Article 501d(2)(b))

According to Article 2 of the EBA draft RTS, exposures to such ARTs (assuming the issuer complies with MiCAR, etc.) should be given a 250% risk weight for credit risk. This applies to banking book exposures (like if held as an investment or loan equivalent) and also informs the default treatment for trading book if not otherwise specified. Notably, as Häring, Ruof, and Blemus (2025) pointed out, the draft RTS ignores paragraphs 60.32 and 60.33 of the Basel framework, which allowed banks to *look through* to the backing assets to determine capital. For instance, if an ART was 100% backed by multi-currency deposit balances kept at a AAA-rated bank, depending on the specific terms of the custody arrangement, the risk should be akin to a deposit balance with that institution (low risk weight). EU, in transitional 501d, did not adopt that nuanced approach, arguably *overweighting* the risk of ARTs.

The draft RTS indicates in recital 25 that for market risk on ARTs, until the EU implements the new Fundamental Review of the Trading Book approach, banks should use the existing simplified standardized approach for market risk.

2.8. Other crypto assets (Article 501d(2)(c))

This is where the strictest rules apply. There are two key components: (i) a 1250% risk weight for credit risk (and by extension, a similar capital charge for other risk types if not otherwise covered), and (ii) an aggregate exposure limit of 1% of Tier 1 capital for all such exposures combined. What does 1250% risk weight mean in practice? It is effectively the maximum risk weight under CRR3 – it corresponds to

a capital requirement equal to the exposure value. In other words, *if using an 8% minimum ratio*, for every €100 of a category (c) exposure, SAFE Bank must hold €100 of capital because (100 × 12.5) × 0.08=100. This is akin to treating the exposure as if it were deducted from capital. The logic is that such crypto-assets are so volatile and potentially capable of total loss that the bank should not be leveraged against them at all – every euro exposure should be backed by a euro of capital, ensuring the bank could theoretically absorb a total wipeout.

For market risk, the draft RTS Article 3(4) allows a "Risk-Types Approach" for some of these point (c) exposures, but only if they meet certain criteria. If those criteria are not met, 1250% applies. The second component, the 1% Tier 1 limit, is crucial. Article 501d(3) of CRR3 (and mirrored in Basel's standard) says that a bank's total exposure to these "other crypto-assets" must not exceed 1% of its Tier 1 capital, and they shall be calculated on a net basis as specified by EBA.

To connect this to the overarching question – *what crypto risks can banks take?* – the answer from this regulatory section appears to be, not too surprisingly: only very limited and heavily capitalized risks. Under these [transitional] rules, a bank can engage with crypto in forms that mimic traditional assets (tokenized bonds, EMTs etc.) without extra capital, but that's not really new risk. For anything else (ARTs, other crypto-assets), the bank can take on some exposure but must equity-fund it and cannot let it grow beyond a trivial slice of its balance sheet (1% of Tier 1 is typically far less than 1% of assets; e.g., if Tier 1 ratio is 15%, 1% of Tier 1 is 0.15% of assets – a tiny slice). This essentially limits banks to a toe-hold in crypto to serve niche client needs primarily in the area of custody and, perhaps, payments.

The next part of the article will consider the reactions from the industry to these requirements and proposals – gleaned from the 2025 consultation responses.

3. Industry response to the EBA's draft RTS

This section offers a focused review of the responses submitted during the EBA's public consultation, which concluded in April 2025, with particular attention to how the broader industry – rather than the banking sector specifically – has responded to the draft proposals. With the notable exceptions of Fédération Bancaire Française (FBF), Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken (BDVR) and the European Association of Co-Operative Banks (EACB), none of the major national banking federations, pan-European banking associations, or individual banks submitted comments on the draft RTS. This absence may reflect limited engagement or capacity, or perhaps a strategic disengagement, particularly as some in the banking sector view crypto-assets – especially stablecoins – as a competitive threat to core banking services. In contrast, responses came primarily from crypto firms, trading venues, and market infrastructure providers. These are stakeholders more directly exposed to crypto markets and therefore more immediately affected by regulatory design.

Despite this, the feedback provides useful insight into how the industry – particularly market-facing participants – interprets the EBA's draft. Most respondents welcomed the EBA's effort to clarify and operationalize the Basel crypto-asset framework in the EU and broadly supported the goal of harmonization with international standards. However, the tone of the feedback was largely critical of specific features of the draft RTS, in particular the proposed 1% aggregate exposure limit. Industry associations – including the Association for Financial Markets in Europe (AFME) (AFME 2025, 1) – noted that the cap could unintentionally stifle low-risk, regulated activities, such as payments. Several respondents suggested that the 1% limit should be recalibrated over time, or at least include exemptions for low-risk and fully collateralized exposures, particularly where banks are not bearing underlying crypto price risk.

A related concern was the EBA's failure to explicitly permit netting of long and short crypto-asset positions when calculating exposures toward the aggregate limit. Respondents noted that Article 501d(5) of the CRR mandates the EBA to specify how to aggregate exposures, yet the draft RTS was silent on whether hedged positions could be offset. (AFME 2025, 2) emphasized that net exposures, not gross, should count toward the 1% Tier 1 capital limit. Without the ability to offset long and short positions, particularly those entered into for risk management purposes, the exposure metric becomes overly conservative and inconsistent with market risk principles applied elsewhere in the CRR framework.

Another area of concern was the treatment of client clearing exposures. In this context, client clearing refers to a service where the bank facilitates the clearing and settlement of crypto-asset derivative transactions on behalf of its clients – similar to providing execution, transfer, or post-trade services – but does not itself take a directional position in the underlying crypto-assets. The bank's role is limited to ensuring the client's trade is properly processed and risk-managed, often backed by initial and variation margin as well as participation in a default fund, which collectively mitigate the bank's exposure to client defaults. and Futures Industry Associations (FIA) (FIA 2025, 1–3) emphasized that, because the economic risk resides with the client and is already covered under the counterparty credit risk and large exposure frameworks, including these exposures in the crypto limit would amount to regulatory double-counting and unnecessarily constrain central clearing activities.

Finally, where the EBA offered policy options, industry respondents clearly preferred approaches that align with existing CRR frameworks over bespoke crypto-specific treatments. For example, the draft RTS proposed two alternatives for assigning risk weights to crypto derivative counterparties: either apply a flat 250% risk weight, or apply the standard risk weight of the counterparty, as used in the general CCR framework. Respondents – including FBF, BDVR, AFME and EACB – overwhelmingly favored the latter, arguing that it is more risk-sensitive and consistent with the principle of regulatory neutrality – i.e., same risk, same treatment. FBF and others emphasized that the 250% flat rate has no basis in the

Basel framework, and its inclusion would introduce unjustified conservatism and divergence from international norms. In general, the desire for full alignment with the Basel standard – and against EU-specific overlays – was a recurring theme across submissions.

4. Crypto valuation and accounting challenges

A bank's risk assessment is only as good as its measurement of exposures, and that in turn relies heavily on both accounting values and fair value determinations (Barth, Hodder, and Stubben 2008). Accurate exposure measurement ensures that risk managers have a clear picture of a bank's financial vulnerabilities, enabling them to allocate capital appropriately and maintain effective internal controls. However, crypto-assets present significant challenges in this context because they do not fit neatly into traditional accounting categories (Sterley 2019). There is currently no specific International Financial Reporting Standard (IFRS) fully tailored to crypto-assets. In practice, most standard-setters have concluded that cryptocurrencies (and similar digital assets) do not qualify as cash or cash equivalents, financial instruments, or inventory (except in certain cases for brokers) (Parrondo 2023). Consequently, under IFRS, in line with the 2019 decision of IFRS Interpretation Committee, the default treatment for crypto-assets has been to classify them as intangible assets (IFRS-IC, Holdings of cryptocurrencies 2019).

Under IFRS-IAS 38, banks have two models available for measuring intangible assets such as crypto-assets: the cost model and the revaluation model (IFRS – IAS 38 Intangible Assets 2025). With the cost model, crypto-assets are recorded at their initial acquisition cost and are subsequently carried at that value, less any impairment losses. This approach is conservative; even if market prices for crypto-assets fluctuate significantly, the balance sheet value remains unchanged until a decline is recognized through impairment. For example, if a bank acquires 10 Bitcoins at a given price, that historical cost will continue to represent the asset's value until a market downturn triggers an impairment loss. While this provides stability, it may result in a disconnect between the recorded value and the asset's current market risk.

Alternatively, the revaluation model allows banks to carry intangible assets at a revalued amount, provided an active market exists for those assets. Under this model, IFRS requires the use of IFRS 13 Fair Value Measurement to determine the current market value of crypto-assets. An active market is one in which there is sufficient trading frequency, liquidity, and observable price data (Palea and Maino 2013). When an active market is present, crypto-assets can be periodically revalued so that their carrying amounts on the balance sheet reflect current market conditions. This approach leads to greater transparency by more accurately mirroring the true economic risk of the crypto-assets. However, it also introduces earnings volatility and requires the bank to exercise significant judgment in determining whether

an active market exists for each cryptocurrency, as this decision may vary from one digital asset to another.

Under the draft RTS Article 1, MiCAR-compliant crypto-assets are included within the scope of the prudent valuation rules. This means that, for regulatory capital purposes, banks must apply additional valuation adjustments to such assets. Whether a bank uses the cost model or the revaluation model, these prudent valuation adjustments help ensure that the risk weightings assigned to crypto-assets are appropriate given their current market risk. The cost model tends to understate the dynamic market risk because it does not reflect real-time changes, forcing banks to rely on internal mark-to-market systems to supplement their risk assessments. The revaluation model, by contrast, allows banks to incorporate current market data directly, albeit at the cost of increased volatility in reported earnings.

Incidentally, the issue of prudential valuation rules was one of the features of the draft RTS that received considerable pushback from the industry. The view of respondents – including FBF, AFME and EACB – was that, at least with respect to EMTs and ART, the rules for exposures are sufficiently prudent and an additional margin of conservatism, such as the prudent valuation adjustment, seems excessive.

Conclusion

This article answered the question what crypto risks banks can take in the EU. Under the transitional framework, banks can take only carefully circumscribed and well-capitalized crypto risks. In the EU, this reflects a deliberate regulatory choice: crypto-assets – particularly unbacked or highly volatile ones – are treated as high-risk exposures subject to stringent capital, liquidity, and operational constraints. The rules under CRR3 and the EBA's draft RTS impose 1250% risk weights on most unbacked crypto-assets and a 1% Tier 1 capital cap on total exposure, effectively limiting banks to only minor positions – if any – unless those positions are hedged, fully collateralized, or supported by offsetting controls. From an internal risk perspective, crypto is allowed, but only in tiny, contained, and fully buffered quantities. The rationale is clear: any bank activity involving volatile crypto-assets must be ring-fenced, risk-mitigated, and subject to real-time oversight.

From a bank's perspective, the strategic value of such tightly controlled activity lies not in short-term profit, but in preparing for future opportunities. For now, most banks are treating crypto as an experimental domain – offering client custody or facilitating access while keeping proprietary exposure negligible. Yet the regulatory framework is evolving in anticipation of more institutional involvement. The design of CRR3, along with MiCA's treatment of stablecoins, assumes that banks will eventually play a larger role in issuing and handling tokenized assets, particularly those that resemble traditional financial instruments. The most promising near-term opportunity lies in tokenized traditional assets – such as digital bonds, tokenized deposits, or syndicated loans on private blockchains – which can be

treated under CRR3 as their conventional equivalents. These assets offer the benefits of DLT (efficiency, programmability, faster settlement) without exposing the bank to new types of market risk.

In contrast, stablecoins represent a middle ground: familiar in function but novel in structure. MiCA opens the door for banks to issue EMTs and ARTs, provided they meet strict backing and redemption requirements. For credit institutions, the existing CRR/CRD capital framework applies, but supervisors may still impose additional Pillar 2 capital buffers to reflect liquidity and operational risks. While the capital cost may be lower than for unbacked crypto-assets, issuing a stablecoin or accepting in custody reserve assets from another stablecoin issuer still requires careful reserve management, redemption planning, and technological oversight. Still, this category may prove strategically important in the long run – particularly if stablecoins become widely used in payments, settlement, or wholesale finance.

While the EU moves forward with implementing the Basel crypto-asset framework through MiCA and CRR3, it is worth noting that regulatory developments in the United States are progressing along a different but parallel path. U.S. banking regulators – primarily the Federal Reserve, OCC, and FDIC – have taken a cautious, supervisory-led approach to crypto-asset exposures, emphasizing safety and soundness over formal rulemaking. Notably, there is no finalized prudential framework for crypto-assets equivalent to the EU's RTS under Article 501d CRR. However, U.S. authorities have issued a series of policy statements, interpretive guidance, and supervisory procedures, including the Federal Reserve's supervisory nonobjection process for banks engaging in crypto activities.

As global regulators continue to converge around the Basel Committee's standards, the divergence in implementation timelines and methods – particularly between the EU and the U.S. – may create regulatory fragmentation, posing challenges for internationally active banks and financial institutions more generally. Respondents to the EBA consultation on the draft RTS – such as Deutsche Börse Group (2025) – highlighted the risk of regulatory fragmentation. While this underscores the value of ongoing cross-jurisdictional dialogue and coordination, the prospect of achieving a truly globally coherent approach to crypto prudential regulation may be increasingly unrealistic in today's fractured geopolitical landscape. In such an environment, regulatory divergence may prove more likely than convergence, challenging efforts to maintain consistency across major financial jurisdictions.

Bibliography

AFME (2025). "AFME Response to EBA CP RTS on the Calculation and Aggregation of Crypto Exposure." (May 1, 2025).

Barth M.E., Hodder L.D., Stubben S.R. (2008). *Fair Value Accounting for Liabilities and Own Credit Risk*, The Accounting Review, 83(3), 629–664. doi:10.2308/accr.2008.83.3.629

Basel Committee for Banking Supervision (2022). *Prudential Treatment of Cryptoasset Exposures*. https://www.bis.org/bcbs/publ/d545.htm (April 15, 2025).

Basel Committee on Banking Supervision (2024). "Disclosure of Cryptoasset Exposures."

Chan D., Fontan F., Rosati S., Russo D. (2007). "The Securities Custody Industry".

Coste C.-E. (2024). *Toss a Stablecoin to Your Banker – Stablecoins' Impact on Banks' Balance Sheets and Prudential Ratios*. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op353~11120d3428.en.pdf (May 1, 2025).

Deutsche Börse Group (2025). *Response to Consultation on Regulatory Technical Standards on the Calculation and Aggregation of Crypto Exposure Values* (May 1, 2025).

FIA (2025). *FIA Response to EBA CP on Bank Exposures to Crypto Assets* (May 1, 2025).

Häring W., Ruof C., Blemus S. (2025). "CRR III – Prudential Treatment of Crypto Exposures." *White & Case LLP | Insight Alert*. https://www.whitecase.com/insight-alert/crr-iii-prudential-treatment-crypto-exposures (May 1, 2025).

"IFRS – Holdings of Cryptocurrencies" (2019).

"IFRS – IAS 38 Intangible Assets." 2025. https://www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/ (May 1, 2025).

Krause D. (2025). *The Repeal of SAB 121: A Turning Point in Cryptocurrency Regulation and Accounting*. doi:10.2139/ssrn.5115080

Low K.F.K., Teo E.G.S. (2017). *Bitcoins and Other Cryptocurrencies as Property?*, Law, Innovation and Technology, vol. 9, issue 2. https://www.tandfonline.com/doi/abs/10.1080/17579961.2017.1377915 (April 15, 2025).

Montager D. (2024). *Banks Explore Crypto Partnerships in New Trend*. The Banker. https://www.thebanker.com/content/82871244-634a-5646-9d7e-09360e5a799b (April 15, 2025).

Palea V., Maino R. (2013). *Private Equity Fair Value Measurement: A Critical Perspective on IFRS 13*, Australian Accounting Review, 23(3), 264–278. doi:10.1111/auar.12018

Parrondo L. (2023). *Cryptoassets: Definitions and Accounting Treatment under the Current International Financial Reporting Standards Framework*, Intelligent Systems in Accounting, Finance and Management, 30(4), 208–227. doi:10.1002/isaf.1543

Sterley A. (2019). *Cryptoassets: Accounting for an Emerging Asset*, The CPA Journal; New York 89(6), 6–7.

Zetzsche D., Nikolakopoulou A. (2025). *Crypto Custody: An Empirical Assessment*, Journal of Financial Regulation: fjaf004. doi:10.1093/jfr/fjaf004