



Response EC Consultation

**Targeted consultation on the review of regulation on the
Markets-in-Crypto-Assets (MiCA)**

PART 1. Scope and definitions, Title II. Crypto-assets

1.1. MiCA scope and crypto-asset classification

Question 1. Should crypto-assets that qualify as financial instruments as defined in [Directive 2014/65/EU](#) of the European Parliament and of the Council⁵, continue to be governed by sectorial legislation ([MiFID/MiFIR/MAR/Prospectus Regulation](#), etc.), or should all assets that are recorded and transacted on distributed ledgers and that meet the definition of a crypto-asset, or the services provided on such assets, in principle be covered by MiCA?

- ☒ Yes, they should remain under the main sectorial legislation
☐ No, all crypto-assets, or the services provided on such assets, should be covered by MiCA

If the answer is “Yes”, is the distinction between financial instruments governed by MiFID and crypto-assets governed by MiCA sufficiently clear, also taking into account ESMA’s guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments?

- ☐ Yes, sufficiently clear
☒ No, clarification is needed

If the answer to the previous question is “No” please explain your response and suggest any policy actions for clarification if needed.

We support maintaining the distinction between the MiCA and MiFID regimes, rather than expanding the scope of MiCA to encompass all types of crypto-assets and related services.

We advocate for a framework that preserves the existing separation between **a)** crypto-assets that qualify as financial instruments and the services associated with them under sectorial financial services legislation; and **b)** crypto-assets and services that fall within the scope of MiCA.

The European regime should continue to rely on the principle that the regulatory treatment of an asset should depend on its economic function and characteristics, irrespective of the technology used to record or transfer it. The contrary will lead to inconsistencies in the treatment of economically equivalent products and services, where they fall under different regimes just because of the underlying technology, contrary to the principle of “*same activity, same risk, same rules*”. However, we acknowledge the convergence between both regimes. Products and services regulated under both frameworks serve similar trading and investment purposes. As a result, it is natural for market participants to expand the range of products and services they offer to carry out activities that fall within the scope of both regimes.

In this context, rather than seeking to merge MiFID and MiCA, regulatory efforts should focus on:

- **First**, any remaining interpretative uncertainties should be addressed through further guidance and, where necessary, targeted legislative amendments to the Level I text.
- **Second**, given the interaction between the two regimes, the regulatory framework should endeavor to provide a more harmonised and streamlined licensing process for firms. A similar approach, e.g. a streamlined notification process, already exists under Article 60 of MiCA, which allows investment firms authorised under MiFID to provide crypto-asset services that are equivalent to the investment services and activities for which they are already authorised. However, this mechanism only operates in one direction. While MiFID firms benefit from a streamlined route under the MiCA framework, CASPs do not have access to a comparable pathway when seeking to provide equivalent services under MiFID.

We therefore support expanding the range of services that can be recognised as equivalent across the MiCA and MiFID regimes. In addition, a simplified authorisation process should be introduced for CASPs wishing to obtain permissions for equivalent MiFID services, following the same logic as Article 60 of MiCA. This would reduce licensing burdens for activities substantially equivalent, while preserving the safeguards and regulatory standards applicable.

Question 2. To what extent have ESMA's MiCA Article 2(5) guidelines and the joint ESA standardised classification test reduced uncertainty in practice? Which borderline cases remain difficult? Please explain your response and suggest any policy actions for clarification if needed.

We consider that, at the time of their publication and adoption, ESMA's Guidelines on crypto-assets that qualify as financial instruments provided meaningful legal indications and were instrumental in supporting a consistent interpretation of the MiCA framework by both National Competent Authorities (NCAs) and market participants. However, in light of the rapid evolution of crypto-asset markets, we believe that these guidelines should be reviewed and updated. Such updates would help ensure that the regulatory framework remains aligned with market developments, addresses emerging token structures, and continues to promote supervisory convergence across the EU. In addition, we note the recent [guidelines](#) issued by the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC), which provide comprehensive and up-to-date interpretations in the same regard. While the EU framework should remain grounded in its own legislative objectives, future ESMA guidance could usefully take into account relevant developments in other major jurisdictions. This would facilitate greater regulatory convergence internationally, where appropriate, and would enhance legal certainty for cross-border market participants, reducing compliance complexity, and contributing to the development of more consistent international standards for crypto-asset classification.

Furthermore, we note that MiCA does not address ancillary services and activities, unlike other EU financial services legislation. Providing greater clarity in this area would help ensure a more comprehensive regulatory framework and could also prove beneficial in addressing the interaction between MiCA and MiFID but also with the PSD3/PSR framework, particularly with respect to the issues raised in response to Question 55 below.

1.2. Transparency rules and ex post supervisory control regime

Question 3. Title II establishes disclosure, marketing, conduct and liability rules for public offers and admission to trading of crypto-assets other than ART and EMT. How appropriate or effective is the design of Title II in balancing investor protection, market integrity and innovation?

Adan did not answer this question.

Question 4. Based on initial implementation experience under MiCA, please assess the extent to which the following issues remain a concern.

(1 = Not serious concern at all, 5 = Extremely serious concern)

N°	Issue	1	2	3	4	5
1	Inadequate or non-comparable disclosure clarity or complexity to retail investors in Title II white papers					
2	Fraudulent or misleading crypto-asset offerings affecting EU investors					
3	Lack of clear and enforceable investor rights for crypto-asset holders					

4	Insufficient issuer governance or accountability in crypto-asset projects e.g. monitoring of the use of funds by issuers after the offering period					
5	Regulatory arbitrage, including activity shifting outside the EU					
6	Promotions by social media, influencers, sponsorships					
7	Post-issuance token value erosion or project failure affecting EU retail investors					
8	Market manipulation practices (e.g. wash trading, price manipulation) in crypto-asset markets					
9	Misaligned incentives between crypto-asset issuers and investors (e.g. insider allocations, weak lock-ups)					
10	Difficulty in assessing issuer quality and project credibility for EU investors					
11	Cross-border enforcement and supervisory coordination challenges within the EU					■
12	Cross-border enforcement and supervisory coordination challenges with third countries authorities outside of the EU					

Please explain your ratings above, focusing on the issues you deem most significant and add any additional issues that you deem highly important.

We note that divergent interpretations and applications of MiCA requirements by NCAs have emerged in the context of authorisation procedures. This creates legal uncertainty for applicants, and results in inconsistent licensing expectations across Member States, as firms are required to adapt their applications to jurisdiction-specific supervisory approaches despite relying on a directly applicable EU Regulation. This undermines the objective of establishing a genuine single market for crypto-asset services by creating an uneven regulatory landscape, and potentially encourages regulatory arbitrage, influencing firms' decisions on where to establish. In addition, inconsistent supervisory expectations can lead to delays in authorisation and supervision processes, creating an unlevel playing field. To promote greater supervisory convergence, ESMA should strengthen coordination among NCAs.

Regulatory arbitrage: regarding tokenised derivatives- while the Guidelines appropriately classify tokenised perpetual futures and similar products as financial instruments under MiFID II, a practical challenge remains in ensuring that this classification is effectively enforced against third-country platforms that actively target EU investors without being authorised under MiFID II and without being subject to the corresponding investor protection framework.

Question 5. Should additional measures either at the issuance stage or during the marketing and distribution of crypto-assets, be considered? Based on your experience or expertise, please evaluate the potential effectiveness of the following additional measures in relation to Title II crypto-assets.

1. Not at all effective
2. Slightly effective
3. Moderately effective
4. Highly effective
5. Extremely effective

Potential measure	1	2	3	4	5
Marketing restrictions for high-risk or speculative crypto-assets aimed at retail investors e.g. restricting or banning the use of algorithmic or "gamified" marketing tactics for new token launches			X		
Lock-up periods (e.g. 12 months) or vesting schedules for founder and early investor tokens			X		

Please explain your ratings above and what (other) regulatory or supervisory actions you would consider useful either at the issuance stage and during marketing or distribution.

Lock-up periods: Lock-up periods may be a more effective measure in promoting orderly markets and enhancing investor protection. Restricting the immediate sale of tokens can eventually help to mitigate the risk of sell-offs immediately following issuance, reducing excessive price volatility; and thereby to reduce incentives for short-term speculative behaviour. However, too strict requirements on token offerings with limited flexibility for issuers and offerers would limit flexibility in how tokens are launched, regardless of whether the project presents real investor harm. This could also lead to fewer token launches being performed under MiCA's framework and protections, while still remaining available for EU investors from outside of the EU. For this reason, we generally think that current disclosure and governance requirements attached to the issuance and distribution of crypto-assets under MiCA Title 2 are sufficient. Rather than introducing subjective and hard-to-apply restrictions, the framework should focus on clear disclosure standards, fair communications, and enforcement against misleading or abusive practices.

Marketing restrictions: The marketing restrictions proposal relies on concepts, including "*highly speculative*" and "*gamified*", which are not clearly defined. That creates legal uncertainty and risks inconsistent or overly broad application. Moreover, we note that marketing restrictions are in place in some EU Member States whereas other jurisdictions have introduced a less restrictive approach in this regard. This should be further clarified in order to achieve convergence and a level playing field.

Question 6. What administrative simplification or burden reduction measures should be considered under title II and its implementing measures and technical standards?

We propose shortening the 20-working-day period under **Article 8(5)**. Because crypto-asset white papers are not reviewed or approved by competent authorities in any Member State, that period is disproportionate to the notification obligation. It also places trading platforms at a competitive disadvantage relative to MiCA-authorised brokers, which are not subject to an equivalent white paper publication requirement and may enable trading as soon as a crypto-asset is available on an EU or non-EU execution venue or otherwise supported by their liquidity providers. This creates an uneven playing field without a corresponding investor protection benefit.

Whatever the length of the period, the offeror or person seeking admission to trading should be permitted to publish the white paper as soon as it appears in ESMA's register, rather than only once the notification period has expired where publication in the register occurs earlier. In practice, publication in ESMA's register is the clearest indication that the competent authority has not objected. Requiring the offeror to wait out the balance of the notification period after that point serves no regulatory purpose and creates unnecessary delay.

We also propose removing fields **F.9** and **F.10** from the white paper template, at least where the white paper was prepared by the trading platform seeking admission of the crypto-asset to trading. A procedure should also be established to remove a white paper from the ESMA register. Where a trading platform operator has admitted a

crypto-asset to trading on its own initiative and later decides to delist it, no procedure currently exists to request removal of the related white paper from the register. This is disproportionate. The operator remains liable for the white paper and is implicitly expected to maintain and update it even though the crypto-asset is no longer traded on its platform.

Question 7. Which specific categories remain most difficult to classify in practice? (e.g. hybrid tokens, wrapped assets, tokenised fund interests, tokenised money-market instruments, governance tokens, synthetic exposures, or assets marketed as NFTs but issued in series)?

In particular, the following: remain among the most difficult crypto-assets to classify in practice.

- **Hybrid tokens**, particularly tokens that combine payment, investment, utility and store-of-value functions. Challenges may also arise where a token was legitimately classified as a utility token at issuance but later develops characteristics typically associated with financial instruments as a result of governance changes, the introduction of additional rights or changes in its economic functions.
- **Tokenised fund interests**, i.e. tokenised interests in collective investment undertakings.
- **Liquid staking tokens**: it remains uncertain whether these arrangements may qualify as units in collective investment undertakings. In decentralised staking protocols, the lack of an identifiable manager, collective management activity or investment strategy makes it particularly difficult to apply traditional fund concepts.
- **Wrapped or synthetic exposures**, including representative or mirrored token structures.
- **Instruments with money-market or derivative-like characteristics.**
- **Certain NFTs**: uncertainty remains around the concepts of fungibility, uniqueness and a "*large series*". Questions include how a "*large series*" should be determined, whether NFTs with minor value-affecting differences should nevertheless be regarded as non-fungible, and how highly interchangeable NFTs should be treated from a regulatory perspective.
- **Tokens incorporating governance or profit-right features.**
- **Stablecoins with contractual rights resembling financial claims.**
- **Tokenised derivatives**: while the Guidelines appropriately classify tokenised perpetual futures and similar products as financial instruments under MiFID II, a practical challenge remains in ensuring that this classification is effectively enforced against third-country platforms that actively target EU investors without being authorised under MiFID II and without being subject to the corresponding investor protection framework.
- **Receipt tokens/ wrapped tokens**, i.e. tokens representing a position in a vault, are a technical accounting representation of a user's own deposited assets. They are minted and burned by an autonomous smart contract upon the user's own deposit and withdrawal, have no issuer or offeror within the meaning of Title II, and represent nothing beyond the user's proportional claim on the assets held in the vault smart contract. ESAs could clarify through guidance that they should neither be treated as a distinct crypto-asset offered to the public nor trigger white paper obligations of their own.



In addition, further guidance is needed on the regulatory treatment of **Simple Agreements for Future Tokens (SAFTs)**, similarly to **Simple Agreement for Future Equity (SAFE)**, but the investor receives crypto-tokens rather than shares. SAFTs are widely used in market practice as an early-stage fundraising mechanism, including by institutional investors and asset managers. However, there remains significant uncertainty as to whether, and under what circumstances, a SAFT should qualify as a financial instrument. This unclarity may discourage the development of asset management investment in the crypto market. The qualification of a SAFT needs thus further guidance.

Question 8. Are the current Title II mechanisms sufficient to ensure meaningful updates to investors after issuance, including where project governance, tokenomics, vesting schedules or control rights change materially?

Adan did not answer this question.

Part 2. Requirements applying to Assets referenced tokens (ART) and electronic money tokens (EMT) and their issuers (MiCA Titles III and IV)

MiCA establishes a bespoke regulatory regime for so-called “stablecoins” by distinguishing between asset-referenced tokens (ARTs) and e-money tokens (EMTs).

This section seeks stakeholders’ feedback on stablecoins (EMTs and ARTs) in general, notably on the future role they may play both within the EU and beyond. It also asks more specific questions related to their prudential regime, their reserve requirements, the redemption rights of their holders and whether MiCA’s stablecoin regime remains fit for purpose or requires adjustment in view of market and international regulatory developments.

2.1. The future role of stablecoins

Question 9. Looking 5-10 years ahead, how strongly do you agree with the following visions for the role of stablecoins in the EU?

For each vision below, please indicate on a scale of 1 to 5.

1 = Strongly disagree 2= Rather disagree 3 = Neutral 4 = Rather agree 5 = Strongly agree

	1	2	3	4	5
A mainstream digital means of payment for retail transactions within the EU				■	
A mainstream digital means of payment for wholesale transactions within the EU				■	
A complement to existing payment instruments, used mainly in specific use cases especially in international, cross-border payments			■		
A core infrastructure layer for the digital economy and tokenised financial markets especially for settlement				■	
A niche or transitional product, eventually displaced by other forms of digital money (e.g. CBDCs or commercial bank money innovations)		■			
No clear long-term role can be identified at this stage		■			
Others					

If your answer is “Others”, please elaborate.

Stablecoins will be useful for retail transactions, particularly in corridors that are underserved by traditional banking infrastructure, as they offer an efficient way to make cross-border payments. They could become a core infrastructure layer for the digital economy, provided they are well integrated with CBDCs. Stablecoins can also be very efficient for corporate payments.

Further, stablecoins are likely to become an important settlement infrastructure for tokenised capital markets. The EU’s DLT Pilot Regime and the broader tokenisation agenda make a strong case for programmable, on-chain settlement assets. Stablecoins are well positioned for this role, as they combine the familiarity of fiat currency with

the programmability of blockchain-based assets. Indeed, the [launch of Pontes on 21 September 2026](#) confirms the architecture: central bank money as the anchor, settled through the Eurosystem's own infrastructure with finality in T2, and MiCA-compliant e-money tokens as the practical settlement asset natively available on market DLT platforms for continuous, automated markets. The two are complements, not substitutes. Ongoing negotiations on the MISP already support the use of all MiCA-compliant EMTs for the cash leg of DLT transactions.

Lastly, stablecoins will be particularly useful where global, digital, open and fully programmable infrastructure is needed, for example, in the emerging agentic economy, for programmable micropayments, or as 24/7 available working capital in crypto capital markets.

Question 10. The following question explores the current and potential benefits of stablecoins (both EMTs and ARTs) for different use cases. For each use case below, please indicate on a scale of 1 to 5 how beneficial stablecoins would be for EU users:

1= Not Beneficial, 2= Moderately Beneficial 3= Neutral 4= Beneficial 5=Very Beneficial

Use Case	1	2	3	4	5
International payments (non-EU cross-border remittances or transfers)					☒
Intra-EU payments (domestic and EU cross-border payments)			☒		
Crypto trading and liquidity provision					☒
Retail payments - Person to Person			☒		
Retail payments - Person to Business (POI payment to merchants including e-commerce)			☒		
Retail payments - Business to Business				☒	
Wholesale payments (between financial institutions)			☒		
Settlement of tokenised financial instruments (e.g., digital bonds, securities)					☒
Corporate treasury management					☒
Access to programmable or smart contract-based financial services (DeFi applications)					☒
Provision of financial services in underserved regions in the EU					☒

If your answer is "Others", please elaborate.

Please explain shortly your assessment and expectations as regards the benefits of stablecoins for EU users and, where relevant, any potential risks.

The benefits of stablecoins for domestic retail payments compared to existing payment instruments and channels such as SEPA Instant are somewhat more limited, and limited adoption can be expected in this area.

In turn, using stablecoins for non-EU cross-border payments is the cheapest and safest way for retail users to transfer money, without being tied to a single institution or national payment system. This is particularly valuable for international remittances, global e-commerce, 24/7 settlement of tokenised assets, and access for users in markets with underdeveloped banking infrastructure. Retail users are also already making extensive use of stablecoins for crypto trading, as a risk-free asset.

Stablecoins offer significant benefits as working capital and settlement vehicles in crypto capital markets and DeFi. The increased use of stablecoins as the cash leg for tokenised securities can improve efficiency, as they enable atomic settlement and access to European securities outside the EU, while simultaneously growing the overall deposit base of EU banks, particularly where euro stablecoins are held outside Europe.

Asset managers can use stablecoins to settle transactions involving tokenised financial instruments, such as digital bonds and securities. This use case is relevant for cross-border payments within the EU when one of the countries involved is not within the SEPA area.

Regarding corporate treasuries, stablecoins offer clear benefits for corporate treasury movements, with several large corporates already requesting licences for this purpose. They will play a greater role once intraday liquidity is valued.

Stablecoins, however, do not replace the role of CBDCs.

☐ Prudential regime and capital requirements

MiCA sets out different capital requirements for issuers of EMTs and ARTs, with additional requirements applying where tokens are classified as “significant”. Article 35 and 46 require that non-bank issuers of ARTs and EMTs shall, at all times, have own funds equal to an amount of at least the highest of the following: **(a)** EUR 350 000; **(b)** 2% of the average amount of the reserve of assets referred to in Article 36; **(c)** a quarter of the fixed overheads of the preceding year.

Question 11. To what extent do you think the calculation methods are relevant and appropriately calibrated?

- 1 = Not at all relevant/appropriately calibrated
- 2 = Slightly relevant/appropriately calibrated
- 3 = Moderately relevant/appropriately calibrated
- 4 = Mostly relevant/appropriately calibrated
- 5 = Highly relevant/appropriately calibrated

MiCA capital/own funds elements	Relevant					Appropriately calibrated				
	1	2	3	4	5	1	2	3	4	5
Minimum own funds of EUR 350,000			■					■		
2% of the average reserve of assets				■					■	
25% of the fixed overheads of the preceding year			■				■			
Additional own funds for “significant” tokens				■				■		

Please explain your responses to the preceding question, including your reasoning and any suggestions for recalibration or alternative approaches (e.g. greater risk sensitivity, differentiation by business model, or interaction with reserve and liquidity requirements).

Overall, the existing multi-criteria approach is difficult to implement and is not particularly effective.

1° As a general principle: capital requirements should reflect the actual risks borne by EMT issuers

Own funds requirements applicable to electronic money institutions issuing EMTs should be calibrated by reference to the **actual risk profile of the activity**.

In the case of EMT issuance, own funds are not primarily intended to cover financial losses on reserve assets. Such risks are already addressed by MiCA through dedicated requirements on the composition, quality, liquidity, segregation, custody and management of the reserve of assets. MiCA and the related technical standards already impose detailed safeguards designed to ensure that reserve assets remain highly liquid, diversified and protected for the benefit of token holders.

Therefore, the main purpose of own funds for EMT issuers should be to cover **operational risks**, including technology risk, cyber risk, fraud risk, business continuity risk, outsourcing risk, governance failures and risks linked to blockchain-based infrastructure.

Against this background, the current calibration should be reviewed to ensure that it is **risk-based, proportionate and economically justified**.

The current rigid 2% own funds requirement is disproportionate for EMT issuers.

2° Proposed calibration of the own funds requirement

The current rigid 2% own funds requirement is disproportionate for EMT issuers. While simple (minimum calibration generally corresponds to **2% of the reserve**, and increasing to **3% for significant EMTs**), the current approach does not fully reflect the nature of the risks borne by EMT issuers. We suggest replacing the rigid 2% with a risk-based own funds methodology that assesses actual market, credit, and operational risks specific to the token.

A more risk-sensitive approach would therefore be to draw on the simplified operational risk methodology applicable under the CRR ($K = 15\% \times \text{average gross income}$).

We therefore recommend replacing the current reserve-based **calibration with a 1% own funds requirement based on the outstanding amount of EMTs**. This would better reflect the actual risks associated with the activity while maintaining a prudent level of protection.

We also propose introducing regulatory options to reduce the required own funds by 20-40% where an issuer can demonstrate that its risk profile is limited. This would align the own funds requirements for EMTs with the flexibility already available to traditional e-money issuers under the E-Money Directive. Removing this option for EMT issuers simply because e-money is issued on a different infrastructure would not be technology-neutral.

3° Proposed progressive add-on for significant EMTs

The additional uplift for "*significant*" EMTs creates an unsustainable cliff-edge effect that will undermine the long-term viability of successful EU EMT issuers.

A sudden increase in own funds requirements upon classification as significant could create disproportionate incentives for issuers to limit their growth below the significance thresholds, thereby undermining the development of regulated European EMTs.

A more proportionate approach would be to introduce **a progressive add-on tiered system** similar to the G-SIB framework for banks- where additional own funds requirements scale proportionately with assessed systemic risk, not with a single threshold trigger. This graduated structure would better reflect the progressive increase in operational and systemic relevance while avoiding disproportionate threshold effects. It would also preserve strong prudential safeguards for large EMT issuers without discouraging the emergence of European-regulated stablecoin issuers.

4° Recognition of capital requirements already covered under other regulatory licences

The prudential framework should avoid the mechanical accumulation of capital requirements where the same entity is subject to several regulatory regimes.

We would like to highlight the overlap of capital requirement for those EMT-issuing EMIs that also offer other PSP services (e.g. payouts) under their EMI license. Those EMIs face additional, cumulative own funds requirements of 10% of the total fixed overheads (which include overheads stemming from the EMI activity). Given the EMT-related own funds requirements (2-3% of EMT reserves) already covers the main risks, the additional requirement relative to total fixed overheads does not seem justified.

This cumulation of own funds requirements discriminates against EMT-based businesses. In practice, if a PSP is an EMI issuing a regulated EMT, its fixed overhead might be significantly larger than a traditional PSP overheads, with no clear economic/risk-based rationale. We believe that the fixed overheads should be explicitly limited to overheads related to the PSP activity.

It should therefore be possible, subject to appropriate supervisory validation, to **net or offset capital requirements arising from different regulatory licences**, including requirements falling outside MiCA, where the underlying risks are already covered.

Also, the consolidated own funds requirement should correspond to the highest applicable capital requirement across the relevant regulated activities, rather than the systematic addition of all requirements, where the risks covered substantially overlap. Such an approach could be subject to conditions, such as a documented mapping of the risks covered by each regulatory capital requirement; confirmation that no material risk is left uncovered; supervisory validation by the competent authority; appropriate governance and internal capital allocation arrangements; or periodic reassessment in light of the institution's risk profile. This would avoid double counting of the same operational risks, support regulatory neutrality across business models and preserve the competitiveness of EU-regulated EMT issuers while maintaining a robust prudential framework.

5° Fixed-overheads

The fixed-overheads component is itself calibrated too low and backward-looking; a sound operational-risk floor would be 50% of the expenses forecast for the coming year, to cover the operating costs of maintaining continuity through a Redemption Plan activation scenario (Article 47).

Question 12. After being in effect for close to two years, no ARTs have been licensed in the EU under MiCA. In your view, does this absence primarily reflect low market interest in ARTs or other reasons? Please rate each factor below on a 1–5 scale, where: 1: Not at all a factor, 3: Neutral/Uncertain, 5: A major factor.

	1	2	3	4	5
Market interests for ARTs				■	
Licencing and regulatory requirements for ARTs				■	

The absence of licensed ARTs reflects the highly restrictive and operationally burdensome regulatory requirements for ARTs under MiCA. The reserve requirements, own funds requirements, governance obligations, and the complexity of the authorisation process create an extremely high compliance bar that, in practice, discourages market entry. The time required to bring a new ART to market—often exceeding 100 days—is not well aligned with the pace and expectations of financial markets and business needs. The significant ART regime further compounds this by creating cliff-edge deterrents to growth. If these requirements are not recalibrated, ARTs are likely to remain commercially non-viable for the foreseeable future. Furthermore, the EBA guidelines on ARTs are not sufficiently clear and may lead to the potential requalification of ARTs as derivatives, asset-backed securities, or debt instruments.

Overall, this regulatory burden is likely a major factor hindering the development and uptake of ARTs in the EU.

Question 13. If ARTs were to come to market, what do you think is the primary purpose from a consumer/investor perspective: investment or alternative means of exchange/payment? Please explain your answer.

This largely depends on the specific use case being considered. An ART backed by a diversified basket of fiat currencies would likely be used primarily as a means of exchange, similar to a synthetic stablecoin. An ART backed primarily by assets such as real estate or commodities would have a more investment-like character. MiCA should accommodate both, with regulatory requirements calibrated accordingly.

At present, ARTs appear to be primarily positioned as investment instruments, often linked to underlying assets such as gold, physical commodities, or specific financial assets. That said, this investment-oriented perspective should not obscure the potential for ARTs to function as efficient means of exchange or payment. In particular, in certain contexts, they could offer relevant alternatives, provided that appropriate market infrastructure and user demand develop over time.

Because the value of ARTs may fluctuate, unlike EMTs, commercial demand for ARTs is likely to be concentrated in investment-related use cases, which naturally involve a narrower issuer and user base than payment-oriented applications.

☐ **Liquidity and reserve requirements**

Question 14. MiCA requires issuers of ARTs to establish, maintain, and prudently manage a reserve of assets and appropriate liquidity arrangements to ensure orderly redemptions and mitigate financial stability, liquidity, and operational risks. Additional and enhanced requirements apply to ARTs classified as “significant” under Article 45. How do you think, if at all, each of the following elements of the MiCA liquidity and reserve regime for ARTs should be adjusted?

Please rate each aspect on a scale from 1 to 5, where “1” indicates that requirements should be significantly relaxed (e.g. lower liquidity buffers or remove specific obligations), “3” indicates that the current framework is appropriate and should remain unchanged, and “5” indicates that requirements should be made substantially more stringent (e.g. higher reserves, tighter risk controls, or enhanced safeguards).

Requirement element	Non-significant ARTs					Significant ARTs				
	1	2	3	4	5	1	2	3	4	5
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks (Article 36(1))				■					■	
Liquidity composition and maturity structure of the reserve (Article 36(4), RTS)				■				■		

Minimum amount of deposits held (30% and 60%) (Article 36(4), RTS)		■					■			
Auditing requirements (Article 36(9))				■					■	
Custody requirements (Article 37)				■					■	
Enhanced liquidity management, stress testing, monitoring, and reporting obligations for significant ARTs (Article 45(3)–(4))								■		
Excessive exposure / concentration between bank and token (Article 36(4) MiCA) Do you consider the 1.5% binding limit adequate? (RTS)			■					■		

Please explain your responses, including your reasoning and any suggestions for recalibration or alternative approaches (e.g. greater risk sensitivity, differentiation by business model, or interaction with reserve and liquidity requirements).

Such a review could be relevant to better differentiate the regulatory treatment of ARTs and EMTs, given that their use cases and risk profiles differ significantly. Any potential recalibration should remain technology-neutral and focus on investor protection, operational resilience, and legal certainty, rather than on the specific technological infrastructure used.

The 30% (non-significant) and 60% (significant) minimum bank deposit requirements are the most problematic elements of MiCA's reserve framework for both ARTs and EMTs. As the EBA itself acknowledged in its RTS, these minima *"might trigger concerns from the perspective of the liquidity of the reserve assets overall and their exposure to credit risk"* and raise concerns about the *"interconnectedness between the banking system and crypto-asset sector."* Requiring a significant portion of reserve assets to be held as bank deposits introduces exactly the kind of credit and contagion risk that a well-designed reserve framework should seek to eliminate.

We strongly recommend removing the minimum bank deposit requirement entirely, and instead:

- Focusing reserve requirements on HQLA eligibility criteria (safety and liquidity of each asset class) without prescribing concentration in any single asset type.
- Treating asset managers on a look-through basis, as their underlying holdings - rather than the fund wrapper - should determine HQLA eligibility. The current 5% per-fund concentration limit applied at the fund wrapper level defeats the purpose of UCITS money market funds as a reserve vehicle. By comparison, insurance and banking regulations require a look-through approach for the risk assessment of UCITS, further supporting our argument above.
- Allowing crypto-backed ARTs to back their tokens with crypto-assets. For example, a wrapped BTC ART should be allowed to hold BTC as its only backing, as otherwise its value will always slightly deviate from the underlying.

Currently, the inability to fully back wrapped or staked tokens with the underlying crypto-asset makes the ART category unviable from a market point of view. Regarding the enhanced stress-testing and liquidity-management obligations for significant tokens (**Article 45(3)–(4)**), we consider the requirement itself appropriate, but the framework needs to be clarified at Level 2 to ensure that it applies uniformly across all issuers.

At present, the stress-testing methodology, scenario design, severity calibration and frequency are largely left to the discretion of the individual competent authority. This creates the risk of materially divergent supervisory

expectations for functionally identical tokens depending on the issuer's home NCA - an unlevel playing field that could disadvantage issuers and encourage regulatory arbitrage. We recommend that the EBA develop harmonised Level 2 RTS or guidelines specifying a common stress-testing methodology, a minimum set of prescribed scenarios and severity parameters, and a standard frequency, to be applied consistently to all issuers of significant ARTs and EMTs.

The prescribed scenarios should be precise and harmonised, and should not leave too much room for interpretation or deviation with respect to the associated assumptions (e.g. regarding structural assumptions such as the issuer's ability to activate the recovery plan or the time horizon of the scenarios). Uniform application would strengthen supervisory convergence and ensure that the enhanced requirements protect holders based on the actual risk of the token rather than the discretion of the supervising authority.

Finally, custody requirements for reserve assets should not be relaxed. On the contrary, they should remain robust and, for significant ARTs, be strengthened where appropriate. In particular, the framework should ensure strong legal and operational segregation, high-quality safekeeping arrangements, clear allocation of responsibilities along the custody chain, and the ability to ensure rapid restitution or transferability in stressed scenarios.

Question 15. MiCA sets out liquidity and reserve requirements for issuers of EMTs to ensure immediate redemption of tokens, mitigation of credit and operational risk, and resilience under stress scenarios. Additional requirements apply to EMTs classified as "significant" (Article 56). Should any of the following aspects of the MiCA regime for EMTs issued by e-money institutions be adjusted?

Please rate each aspect on a scale from 1 to 5, where "1" indicates that requirements should be significantly relaxed (e.g. lower liquidity buffers or remove specific obligations), "3" indicates that the current framework is appropriate and should remain unchanged, and "5" indicates that requirements should be made substantially more stringent (e.g. higher reserves, tighter risk controls, or enhanced safeguards).

Requirement element	Non-significant EMTs					Significant EMTs				
	1	2	3	4	5	1	2	3	4	5
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks (Art 36(1))			■					■		
Legal and operational segregation of reserve assets from the issuer's own estate and from other token reserves (Art 36(2)–(3))			■					■		
Liquidity composition and maturity structure of the reserve (Art 36(4), RTS)			■					■		
Minimum amount of deposits held (30% and 60%) (Art 36(4), RTS)			■					■		
Auditing requirements (Art 36(9))			■					■		
Custody requirements (Art 37)				■					■	
Enhanced liquidity management, stress testing, monitoring, and reporting obligations for significant EMTs (Art 45(3)–(4))								■		

Excessive exposure / concentration between bank and token (Article 36(4) MiCA) Do you consider the 1.5% binding limit adequate? (RTS)

--	--	--	--	--	--	--	--	--	--

Please, explain your responses, including your reasoning and any suggestions for recalibration or alternative approaches.

Overall, It would indeed be desirable to make more flexible the prudential and liquidity regime of fiat reserves deposited by financial institutions in order to facilitate their proper use to finance the economy.

Composition of the reserve and minimum deposit requirements

We support the objectives of MiCA in ensuring full backing, continuous redeemability, and strong protection of EMT holders. However, the current reserve asset framework is considerably more prescriptive than the regimes emerging in other major jurisdictions and may place European issuers at a competitive disadvantage. MiCA could evolve towards a more risk-based and outcome-focused framework that provides greater flexibility in reserve management while preserving financial stability and investor protection.

1° Broadening the universe of eligible reserve assets

The current MiCA framework relies heavily on bank deposits and highly liquid assets subject to restrictive maturity requirements. While this approach supports liquidity, it may also create unnecessary concentration risk and limit the efficiency of reserve management.

We therefore propose broadening the range of eligible reserve assets, provided that a strict maturity limit is maintained (e.g. instruments with a residual maturity of less than 90 to 180 days), to include short-dated sovereign securities, government money market funds, government-backed reverse repurchase agreements and, where accessible, central bank deposits or reserves. These instruments are widely recognised as high-quality liquid assets and already form the basis of reserve frameworks under consideration or implementation in major jurisdictions.

A broader set of eligible assets would improve diversification, reduce reliance on commercial bank deposits, strengthen resilience across different market conditions and support more sustainable business models for regulated issuers.

2° Introducing more flexibility in reserve maturity profiles

MiCA currently places significant emphasis on very short-term maturities. While maintaining sufficient liquidity to meet redemptions remains essential, we consider that the framework places unnecessary constraints on reserve management.

A more proportionate approach would allow a greater portion of reserves to be invested in short-dated sovereign securities with maturities beyond the current limits, provided that issuers maintain a prudent weighted-average maturity, conduct regular liquidity stress tests and demonstrate their ability to meet redemption requests under both normal and stressed conditions. Allowing investments in sovereign instruments with residual maturities of up to one year would remain highly conservative while improving reserve efficiency, reducing rollover risk and enhancing the economic viability of EMT issuance.

3° Moving towards an outcome-based liquidity framework

We believe that regulation should focus primarily on prudential outcomes rather than detailed prescriptions on asset categories or maturity buckets. The key supervisory objective should be to ensure that EMT holders can redeem

their tokens at par value at any time. Supervisors should therefore assess whether issuers can meet redemption requests under stressed conditions, liquidate reserve assets quickly without significant losses, maintain effective liquidity management arrangements and preserve a diversified portfolio of high-quality assets. Such an approach would give supervisors greater flexibility while encouraging robust risk management practices tailored to the specific characteristics of each issuer.

4° Revisiting the mandatory deposit requirement

A particular concern relates to the requirement that at least 30% of reserve assets, and 60% for significant EMTs, be held as deposits with credit institutions.

According to Adan, this requirement is based on the assumption that bank deposits are inherently safer and more liquid than alternative reserve assets. In practice, however, highly rated sovereign Treasury bills, central-bank-eligible instruments or repos collateralised by sovereign debt may present lower credit risk, greater market liquidity and lower concentration risk than unsecured deposits held with certain banking counterparties.

The mandatory allocation to deposits may therefore unintentionally encourage concentration of reserve assets in the banking sector and prevent issuers from adopting more prudent and diversified reserve structures.

The specific concentration limits introduced via the EBA's Level 2 RTS must be addressed in the Level 1 review:

- (i) the 35% per-issuer concentration limit for government bonds disproportionately affects foreign-currency EMT issuers (such as USD-backed EMTs) for whom a single sovereign bond market (e.g. US Treasuries) is the only appropriate HQLA.
- (ii) the per-bank deposit concentration limits create significant operational complexity as EMTs scale, requiring significant EMT issuers to maintain 12+ banking relationships simultaneously. In particular, the 1.5%-of-total-bank-assets limit is poorly calibrated because it is measured against a single legal entity rather than the consolidated banking group.
- (iii) The 5% per-fund concentration limit for UCITS/CIU investments is applied at the fund-wrapper level rather than to the underlying assets, which limits the usefulness of UCITS money market funds as a reserve vehicle. UCITS MMFs are already highly regulated and diversified instruments holding HQLA, so treating each fund as a single 5%-capped exposure does not meaningfully reduce risk and instead forces issuers to spread allocations across multiple funds, increasing operational complexity and cost.

We recommend removing or substantially raising the 5% limit for MMFR-compliant UCITS funds and applying concentration limits on a look-through basis to the underlying assets. This would also reduce the operational risk created by having to manage and rebalance multiple fund positions simultaneously.

The Commission should provide an explicit Level 1 mandate for these more proportionate Level 2 concentration limits in the MiCA review.

Adan recommends replacing these fixed thresholds with a principles-based regime under which each issuer would determine the appropriate level of cash holdings based on its redemption profile, customer base, observed redemption behaviour, contingency funding arrangements, liquidity stress tests and overall risk-management framework. Supervisors would retain the ability to challenge these assumptions and require adjustments where necessary.

5° Alignment with international regulatory developments

Recent developments in the US and the UK demonstrate a growing international consensus that fully backed stablecoins can safely hold a broader range of high-quality sovereign assets. These frameworks prioritise reserve

quality, transparency and redemption capacity without imposing the same degree of rigidity as MiCA. We therefore consider that a recalibration of the European framework is necessary to avoid creating a structural competitive disadvantage for European EMT issuers.

6° Enhanced transparency and preservation of safeguards

Greater flexibility should be accompanied by stronger transparency requirements. Adan supports periodic public disclosure of the credit institutions holding cash reserves and of the custodians or securities depositories safeguarding reserve assets, while avoiding disclosure of the amounts held with individual counterparties. At the same time, custody and segregation requirements should remain a cornerstone of the framework. Legal and operational segregation of reserve assets from the issuer's estate must continue to provide strong protection to token holders.

Question 16. Under MiCA, credit institutions issuing EMTs are not subject to the reserve asset segregation requirements or the requirement to maintain a reserve of assets applicable to non-bank EMT issuers (Article 58 MiCA). This is consistent with the approach to the regulation of traditional e-money. Should MiCA be adjusted to introduce a requirement to maintain a reserve of assets and segregation requirements for reserve assets of EMTs issued by credit institutions?

Please select one option.

- ☐ Yes - require reserve maintenance and segregation of EMT reserve assets within the credit institution's balance sheet
- ☐ Yes - require issuance through a legally separate entity of the credit institution with full segregation of EMT reserve assets
- ☐ No - keep the current MiCA approach unchanged
- ☒ Others / alternative approach

Please explain your response, including your reasoning and any suggestions for other/alternative approaches.

Rather than making it mandatory to segregate funds for Credits Institutions, we suggest providing guidelines for institutions who want to create a reserve of assets.

☐ **Criteria for determining significance**

Under MiCA, ARTs and EMTs may be classified as "*significant*" based on a set of quantitative and qualitative criteria set out in Article 43 (ARTs) and Article 56 (EMTs), which trigger enhanced prudential, governance, and supervisory requirements. The Commission has adopted a [delegated act](#)¹ to further clarify the criteria for determining significance.

Question 17. Do you think the following quantitative criteria thresholds used to classify EMTs or ARTs as "significant" should be adjusted? If so, how?

- 1 = Significantly decreased (thresholds should be much lower / classification triggered earlier)
- 2 = Somewhat decreased
- 3 = Kept as is (current MiCA thresholds are broadly appropriate)
- 4 = Somewhat increased
- 5 = Significantly increased (thresholds should be much higher / classification triggered later)

¹ Commission Delegated Regulation (EU) 2024/1506 of 22 February 2024 supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council by specifying certain criteria for classifying asset-referenced tokens and e-money tokens as significant, OJ L, 2024/1506, 30.5.2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1506>

Significant token criterion	EMTs					ARTs				
	1	2	3	4	5	1	2	3	4	5
Number of holders / users exceeding 10 million (Articles 43(1)(a) and 56)				■					■	
Total outstanding value / market capitalisation exceeding EUR 5 billion (Articles 43(1)(b) and 56)			■					■		
Transaction volume or value per day (average 2.5)				■				■		
Million transactions and EUR 500 million) (Articles 43(1)(c) and 54)			■					■		

Please explain your responses, including your reasoning and any suggestions for recalibration or alternative approaches.

Overall, for EMTs, the existing market capitalisation thresholds appear broadly appropriate. The criteria relating to the number of users and transaction volumes are more problematic in practice, as they do not necessarily reflect the actual risk profile of EMTs and ARTs. They also depend on data that can be difficult to obtain and measure consistently, especially where tokens are distributed through decentralised or intermediated channels.

These metrics can also change significantly over time, potentially resulting in tokens moving in and out of the “significant” category on a frequent basis. This would create additional operational complexity and regulatory uncertainty. Market capitalisation, by comparison, provides a more stable measure of a token’s economic size and potential systemic relevance, and better reflects the scale of the exposure associated with a particular issuer.

We therefore believe that user and transaction-based thresholds should be removed from MiCA, with greater reliance placed on market capitalisation as the main quantitative measure of significance. The framework could consequently be based on a smaller number of more robust indicators, while leaving supervisors sufficient flexibility to address specific risk situations.

The existing thresholds for transferring supervisory responsibility to the EBA should be maintained, as they are broadly appropriate and consistent with the corresponding SSM and PISA thresholds. However, the thresholds for applying enhanced prudential requirements should be set materially higher, so that they are reached only where an issuer has reached a genuinely systemic scale. The current binary approach to significance could also be replaced by a tiered system, with prudential requirements increasing depending on the issuer’s contribution to systemic risk. Once responsibility has transferred to the EBA, it should be able to determine the appropriate level for each issuer and apply the corresponding requirements.

This would provide a more proportionate approach than applying the same requirements once a single threshold has been crossed. There should also be greater scope for supervisory discretion. An issuer may meet the significance criteria without yet creating material systemic risk, and the EBA should therefore be able to adjust the applicable prudential requirements accordingly. This would allow the framework to better reflect the individual circumstances of each issuer.

The application of the significance criteria should also be clarified for multi-issuance models and global tokens circulating in the EU under a future equivalence regime. The legislation should specify whether the relevant data should be limited to the EU. If global figures were used, MiCA thresholds could be reached below the equivalent thresholds under the SSM and PISA frameworks, resulting in stablecoins being classified as significant despite not reaching the level that would trigger enhanced oversight under other EU frameworks

The indicators themselves should also be reviewed. For interconnectedness in particular, absolute aggregate values would be preferable to relative market shares. A relative measure can lead to an issuer crossing a threshold simply because the overall market has grown more slowly than the issuer, rather than because the issuer has become more systemically important. Absolute thresholds would provide greater predictability and would better reflect the underlying purpose of the significance criteria.

Finally, given the global nature of stablecoins, greater consistency between the main regulatory frameworks is important to avoid market fragmentation and ensure a level playing field. The EU should take into account developments in the UK and US where relevant and ensure that the MiCA framework can be recalibrated if material differences emerge once those regimes are finalised. This would help maintain the competitiveness of EU issuers while preserving high regulatory standards and supporting the cross-border use of stablecoins.

Question 18. Do you think the qualitative criteria used to classify EMTs or ARTs as “significant” under MiCA should be adjusted?

- ☒ Yes
☐ No

If yes, please explain how you think the qualitative criteria for classifying EMTs or ARTs as “significant” should be adjusted.

In particular, some qualitative criteria, such as interconnectedness with the financial system, the significance of cross-border activities, substitutability, and importance for payment and settlement activities, may be subject to broad interpretation and create uncertainty for issuers when assessing whether a token is likely to be classified as significant.

The criterion set out in **Article 43(1)(g)** - namely, that the same issuer issues at least one additional asset-referenced token or e-money token and provides at least one crypto-asset service - should also be reconsidered. The fact that an issuer provides additional crypto-asset services or issues more than one token does not in itself indicate systemic relevance or financial stability risk. This criterion may disproportionately affect integrated business models and create incentives for artificial organisational fragmentation without providing a corresponding prudential benefit.

In addition, certain criteria, such as the issuance of multiple tokens, may be met relatively easily and do not appear sufficiently discriminating to reflect the actual risk profile or systemic importance of an issuer.

In this context, it would be appropriate to remove the set of qualitative criteria from MiCA.

Question 19. Are there any additional criteria or metrics that should be added to determine “significant” tokens?

- ☐ Yes
☒ No

If yes, please specify which criteria or metrics and explain why.

☐ **Interest payment**

MiCA currently prohibits the granting of interest or any interest-equivalent remuneration of stablecoins by either the issuer, offeror or crypto asset service provider. This prohibition applies to ARTs under Article 40 and to EMTs under Article 50 of MiCA.

Question 20. In your view, should the MiCA prohibition on granting interest or any interest-equivalent remuneration be modified?

Option	EMTs	ARTs
Interest and interest-equivalent remuneration should continue to be prohibited		
Interest or interest-equivalent remuneration should be allowed (fully or under defined conditions)	■	■

If you selected “allowed”, please explain your reasons (including any benefits and risks) and specify the conditions under which remuneration should be permitted.

The current MiCA prohibition on interest applying to issuers, offerors and CASPs is much broader than warranted and is not technology-neutral. The comparable prohibition under the *Electronic Money Directive* (EMD) applies specifically to the issuer itself, based on the risk that interest-bearing e-money could function as a substitute for deposits and undermine monetary policy. It does not prevent secondary market participants from offering reward products linked to e-money.

By extending the prohibition to CASPs and all third parties, MiCA goes well beyond the rationale of the EMD and effectively prevents EU consumers from accessing reward products on MiCA-regulated stablecoins. This creates a material competitive disadvantage for MiCA-compliant EMTs compared with other types of crypto-assets, traditional financial instruments and non-MiCA-compliant global stablecoins, and risks driving EU users away from EU-regulated EMTs.

We recommend aligning MiCA’s interest prohibition with the EMD. The prohibition should apply to issuers only and focus on ensuring that issuers cannot structure commercial arrangements to circumvent the restriction. In particular, MiCA framework should distinguish prohibited remuneration linked to holding stablecoins from ordinary commercial arrangements such as transparent fee discounts, loyalty benefits not linked to holding period or token balance, and interest paid on separate fiat cash accounts held with credit institutions, subject to appropriate limitations, as well as appropriate disclosures and prudential requirements applicable to the CASP’s existing licence.

The emerging regulatory approach in other major jurisdictions, including the *US GENIUS Act*, *UK Stablecoin proposals* and the *Singapore MAS framework*, confirms that issuer-level interest prohibitions are appropriate, while third-party reward products are generally not prohibited. This should also be viewed as a strategic issue: a well-designed framework for euro stablecoins could help strengthen the euro’s international role.

From a level playing field perspective, and in a context where the EU aims to foster the development of euro-denominated stablecoins vis-à-vis the current dominance of US dollar-denominated stablecoins, it would be important to reopen the dialog on this issue, should this reward indirect remuneration be confirmed and have significant effect on the attractiveness of €-denominated stablecoins or substitution effects between stablecoins and traditional bank deposits, or the implications for banks’ funding structures and lending capacity. The pace and scale of this potential shift should be carefully assessed. In the US, a recent research paper of the Council of Economic Advisers concludes that a yield prohibition would do very little to protect bank lending, while forgoing the consumer benefits of competitive returns on stablecoin holdings², which explains the position in favour of indirect yield proposed on the Clarity Act. In addition, it would be useful to analyse the behaviour of reserve assets backing stablecoins, including the extent of outflows (“leakage”) from bank deposits depending on the profile of stablecoin holders, as well as the impact of segregation or ring-fencing requirements on liquidity dynamics.

² [Effects of Stablecoin Yield Prohibition on Bank Lending – The White House](#)

In this context, closer coordination between issuers, credit institutions and public authorities would be desirable, in order to manage the transition effectively and optimise the role of stablecoins in supporting the real economy while preserving financial stability.

□ **Redemption**

MiCA establishes distinct redemption regimes for ARTs and EMTs. For ARTs, redemption rights are primarily governed by Article 39, supported by operational and prudential requirements in Articles 36-38 and 47. For EMTs, redemption rights are set out in Article 49, with supporting provisions in Articles 46 and 47.

Question 21. Based on your experience either as a holder of EMTs or as an issuer of EMTs, how have redemption requests been processed and executed in practice by issuers or their agents? What practical problems, if any, have been encountered?

Adan did not answer this question.

Question 22. If you hold EMTs and wish to dispose of them, which of the following options would you most likely choose? Please select only one for each market situation.

Adan did not answer this question.

Question 23. For each of the redemption rights and rules listed below, please indicate whether the existing MiCA rules should be amended or specified or kept as they are. Please consider, in particular, implications for financial stability, consumer protection, and cross-border usability.

	Weaken	Keep as is	Strengthen
Permanent right of redemption against the issuer, either at market value (ARTs) or at par (EMTs)		■	
Timing of redemption (timeframe for redemption by the issuer)		■	
Prohibition of redemption fees	■		
Conditions, procedures, and transparency of redemption policies disclosed to holders		■	
Supervisory powers to intervene in or trigger redemption plans		■	

Please explain your assessment, including if a different approach is warranted for significant vs non-significant tokens, or in crisis scenarios and share any suggestions for adjustments you may have.

The direct redemption right against the issuer should apply in times of stress and where there is no reasonable (timely and cheap) way to off-ramp the EMT back into fiat through secondary markets. In normal circumstances, users will generally use CASPs as their user-facing layer for EMT on-and off-ramping. However, in times of stress, it is important that the issuer can guarantee 1:1 redemption and maintain confidence in the market.

The absolute prohibition on fees should also be adjusted to allow for reasonable operational fees to cover compliance and onboarding costs (e.g. KYC). Any such fees should, however, be strictly capped at the level of the operational costs incurred. This would also bring MiCA more in line with traditional e-money redemption conditions and other global stablecoin frameworks.

Prohibition of redemption fees: Last, for level playing field considerations it would be desirable to be able to ask for redemption fee as the *Genius Act* allows it. The EBA Guidelines on Redemption Plans ([EBA/GL/2024/13](#)) acknowledge that implementing a redemption plan generates costs (such as appointing consultants, intermediaries, or executing the liquidation of the reserve). But EBA does not draw the necessary conclusion as it severely restricts how these costs are covered. Therefore, the prohibition on passing them directly to the holder during the ordinary course of business or deducting them proportionately from the redeemed amount contradicts market reality. MiCA and the corresponding Guidelines should be amended to explicitly permit issuers to pass transparent, proportionate, and verifiable execution and liquidation costs to the redeeming holder. Providing this clarification would ensure that issuers are not forced to subsidize third-party network and liquidation expenses, while still fully protecting consumers from arbitrary or hidden redemption penalties.

☐ **Stability issues**

Stablecoins have the potential to reshape part of the financial service value chain as they can offer faster, cheaper, and more direct global payment and settlement transactions by bypassing certain financial intermediaries. They can also pose risks. This subsection aims to explore the adequacy of the safeguards provided by MiCA, especially regarding redemption and resolution plan.

Question 24. Articles 46 and 47 require issuers of ARTs and EMT to prepare a recovery plan and a redemption plan in case an issuer cannot comply with reserve requirements, e.g. due to significant and sudden requests for redemptions. Please indicate whether the current MiCA requirements are fit for purpose in those regards or should be amended.

	ARTs			EMTs		
	Weaken	Keep as is	Strengthen	Weaken	Keep as is	Strengthen
Recovery plans					☒	
Redemption plans					☒	

Please explain your assessment, including if a different approach is warranted for significant vs non-significant tokens, and share any suggestions for adjustments you may have.

Question 25. EMTs issued by authorised e-money institutions (EMIs) could potentially operate with enhanced monetary and financial safeguards.

Please rate the appropriateness and desirability of the following policy options for EMTs issued by e-money institutions on a scale of 1 to 5, where:

- 1 = Not at all appropriate / desirable
- 2 = Slightly appropriate / desirable
- 3 = Moderately appropriate / desirable
- 4 = Mostly appropriate / desirable
- 5 = Highly appropriate / desirable

	1	2	3	4	5
Allowing EMT issuers to deposit their reserve assets directly into central bank accounts					■
Providing clear rules that ensure the continuity of redemption rights (reserves are safeguarded for the benefit of token holders and are ring-fenced in insolvency, giving these holders an exclusive claim against those assets) in case of insolvency of the issuer					■
Establishing a dedicated resolution regime for EMIs issuing EMTs	■				
Allowing emergency liquidity support / lender-of-last-resort (LOLR) facilities for EMIs issuing EMTs					■
Others					

If your answer is “Others”, please elaborate.

Please explain your ratings, including potential benefits, risks, or implementation challenges.

1° EMT issuers’ access to central bank accounts

Only banking issuers - *i.e.* either credit institutions or EMIs that are subsidiaries of sufficiently rated credit institutions and subject to SSM/ECB supervision - should be granted access to remunerated central bank accounts to deposit part of their reserves. Extending such access more broadly could disrupt the current monetary and financial system and introduce new risks that could be detrimental to financial stability.

Allowing EMIs that are subsidiaries of well-rated credit institutions to hold reserves in a remunerated account would encourage a shift of deposits away from the banking system and could positively support monetary policy transmission. It would simply facilitate the flows between the banking subsidiary EMI and the ECB, provide additional comfort to holders regarding the safety of the reserves, particularly in times of stress, and make the overall process more transparent, without otherwise hindering the banking industry. The non-remuneration requirement should therefore be limited to issuers belonging to non-banking groups. Remuneration should be possible for banking subsidiary EMIs.

This approach would need to be further assessed and validated.

2° A dedicated resolution regime for EMIs issuing EMTs

The current framework, combining the Electronic Money Directive with the safeguards already provided under MiCA, appears broadly satisfactory.

3° Emergency liquidity support for EMIs issuing EMTs

The role of the ECB as lender of last resort to credit institutions, which hold the majority of reserve assets backing stablecoins, combined with MiCA’s redemption mechanisms, provides a solid basis for managing potential stress situations. This is further supported by the direct and timely supervision exercised by the SSM, unlike situations such as the SVB failure, where earlier supervisory intervention could have been beneficial.

Finally, we believe that for significant EMTs, allowing access to emergency liquidity support could provide a powerful facility to calm liquidity-driven market panic around widely used EMTs. Conditions could be attached to such access for significant EMTs in order to avoid moral hazard.

Question 26. How appropriate is it to require EMT-issuing EMTs to hold 30-60% of their reserve assets in bank deposits? Please explain your ratings and add any suggestions for recalibration or alternative approaches.

- ☐ Not at all appropriate / desirable
- ☒ Slightly appropriate / desirable
- ☐ Moderately appropriate / desirable
- ☐ Mostly appropriate / desirable
- ☐ Highly appropriate / desirable

As previously outlined, the mandatory minimums for bank deposits are among the most problematic provisions in MiCA's stablecoin framework. They introduce counterparty risk, limit the ability to optimise reserves, reduce the return potential for issuers and therefore affect the competitiveness of EU issuers. Most importantly, they are not consistent with sound prudential design. The safest reserves are the most liquid and highest-quality sovereign assets, rather than commercial bank deposits.

We suggest, among other measures, that the framework explicitly recognise central bank deposits as an eligible and preferred form of reserve holding, whether through fiduciary accounts or direct access to central bank accounts, in particular for significant issuers. As set out in our response to Question 25, central bank deposits eliminate commercial bank counterparty risk and provide the strongest available liquidity safeguard. Where such access is available, it should count towards or replace the bank deposit requirement, so that issuers are not required to concentrate large balances with commercial banks precisely as their systemic importance increases.

☐ **Global stablecoins arrangements and interactions with other regulatory frameworks**

Global stablecoins are stablecoins that have a wide existing or potential reach and use across multiple jurisdictions.

Question 27. What are the potential benefits of global stablecoins for different use cases? For each use case below, please indicate on a scale of 1 to 5 how beneficial global stablecoins would be for EU holders:

- 1= Not beneficial
- 2= Moderately beneficial
- 3= Neutral
- 4= Rather beneficial
- 5= Very beneficial

	1	2	3	4	5
International payments (cross-border remittances or transfers,)					
Intra-EU payments (domestic and cross-border EU payments)					
Crypto trading and liquidity provision					
Retail payments - Person to Person					
Retail payments - Person to Business (POI payment to merchants including e-commerce)					

Retail payments - Business to Business					
Settlement of tokenised financial instruments (e.g., digital bonds, securities)					
Corporate treasury management					
Access to programmable or smart contract-based financial services (DeFi applications)					
Provision of financial services in underserved regions in the world					
Other potential use cases (please specify)					

Please explain shortly your assessment and expectations as regards the use cases of global stablecoins (EMTs/ARTs) and the benefits for EU users.

Global stablecoins enable seamless and low-cost cross-border payments with relatively limited risks, as they can function as a form of international currency that can be used by a wide range of participants worldwide for different types of transactions. While the most immediate and obvious use cases are international and corporate payments, we believe that, over time, stablecoins could also compete effectively with domestic retail payment systems.

Global stablecoins have the potential to bring significant benefits to EU users by enabling faster, more efficient and potentially lower-cost transfers of value across jurisdictions and different types of financial infrastructure. Their benefits are particularly clear for cross-border transactions, corporate payments, treasury management and the settlement of tokenised financial instruments, where traditional payment and settlement processes can involve multiple intermediaries, fragmented operating hours and higher costs. Stablecoins can enable near real-time settlement, more efficient liquidity management and greater interoperability between traditional and digital financial markets.

Stablecoins also offer a particularly relevant solution for settlement on DLT, notably as the “cash leg” of tokenised transactions.

Question 28. How important is it for EU users (both people and businesses) to be able to access global stablecoins via EU-based and licenced issuers and CASPs? Please indicate on a scale of 1 to 5.

	1 Not important at all	2 Moderately important	3 Neutral / no clear preference	4 Rather important	5 Highly important
EU-based and licenced stablecoins Issuers					■
EU-based and licenced CASPs					■

Please explain shortly your reply.

It is critically important that EU users, both retail and business, can access global stablecoins through EU-based and licensed issuers and CASPs. This is more than a consumer choice issue. In practice, access to globally

significant stablecoins is increasingly a precondition for participating in tokenised financial markets, where the cash leg of settlement, liquidity, and collateral often depends on globally liquid stablecoins. This also matters for cross-border B2B settlement, DeFi liquidity access, corporate treasury and FX management, and trading execution quality, where global liquidity remains concentrated in major stablecoins. If EU-based firms cannot provide that would weaken the EU's competitiveness objectives and leave EU users and businesses at a disadvantage.

Without access to global stablecoins through regulated EU venues, EU users and businesses face two undesirable outcomes: either being cut off from global market liquidity and cross-border payment flows, or continuing to access these instruments through unregulated offshore venues. Either scenario could undermine MiCA's objectives and deprive EU users of the consumer protections and local rights-including redemption rights, disclosures, and governance safeguards-that MiCA was intended to provide for major global stablecoins.

Question 29. Based on your experience and assessment, how significant are the following risks associated with a multi-issuance model³ of global stablecoins for the EU financial system?

Please rate each risk on a scale from 1 (Irrelevant) to 5 (Very significant).

Identified Risk	1	2	3	4	5
Run risk and reserve depletion in the EU (e.g. cross-border migration of tokens during stress leading to sudden increase of redemption pressure on EU issuers)					
Unbalanced reserve distribution across jurisdictions (e.g. fragmentation of reserves between EU and non-EU entities)					
Cross-border reserve transfer restrictions (e.g. third-country limitations on moving reserves during stress events)					
Regulatory arbitrage due to fungibility of tokens (e.g. operation across regimes exploiting differences in prudential or conduct rules)					
Supervisory monitoring and data-tracking challenges (e.g. difficulty measuring EU-holdings, especially holdings in self-custodial wallets)					
Risks resulting from the stablecoin issuer home jurisdictions not having prudential or conduct rules that meet internationally accepted standards or that are significantly lower than those set out in EU law.					
Others					

If your answer is "Others", please elaborate. Please explain the reasoning behind your ratings above. Describe the nature and importance of these risks, the underlying assumptions, market dynamics, or regulatory factors informing your view.

³ Under a multi-issuer model, the global stablecoin issuer operates subject to the requirements of the EU MICA framework for stablecoins offered or held in the EU (EU establishment, EU reserve requirements, redemption obligations, EU supervision) and the requirements of third country jurisdictions, if any, where it also issues or offers stablecoins. Protection of EU holders relies on EU prudential, operational, and consumer protection safeguards set out in MiCA.

Run risk and reserve depletion in the EU: could be mitigated through a more structured approach to the localisation of reserves backing stablecoins, as well as through an appropriate composition of those reserves.

Unbalanced reserve distribution across jurisdictions: could be addressed by limiting- or, subordinating- the redemption rights of non-EU holders in proportion to the reserves available in the relevant jurisdiction, aligning liabilities with the corresponding allocation of reserves.

Regulatory arbitrage due to fungibility of tokens: close monitoring of international regulatory developments (especially in the US) is essential.

Issuer home jurisdictions lacking adequate prudential or conduct standards

Question 30. MiCA does not currently prohibit multi-issuer models, nor does the EU have jurisdiction to determine how third country entities, that also have licensed entities in the EU, should be regulated in third country jurisdictions. Given your assessment of the advantages or disadvantages of global stablecoins and multi-issuance models, do you think that MiCA should continue to be open to multi-issuance models?

- ☒ Yes, the multi-issuance model for stablecoins should be permitted under MiCA
- ☐ No, MiCA should disallow the multi-issuance model for stablecoins

Please explain the reasons for your response and describe the potential implications for the EU market and relevant stakeholders.

MiCA should remain open to multi-issuance models. A prohibition would force MiCA-compliant networks either to ring-fence EU liquidity into a siloed pool or to withdraw the EU leg altogether, reducing liquidity depth, weakening utility for payments and trading, and leaving EU users with a less efficient product than users elsewhere.

A blanket ban risks driving crypto activity offshore, and undermining the competitiveness of EU-regulated issuers and CASPs. Blocking access could push users toward unregulated or non-supervised channels, moving transactions beyond the reach of EU oversight. Ultimately, this reduces supervisory visibility, heightens consumer protection risks, and impairs the EU's ability to manage global risks.

More broadly, the risk is less acute than it may first appear because major jurisdictions are now rolling out increasingly similar stablecoin requirements on reserves, redemption, disclosure and supervision. Recent regulatory developments support a cooperation model rather than a ring-fencing model. The *UK-US Joint Statement on Stablecoins* explicitly warns against disproportionate jurisdiction-by-jurisdiction ring-fencing of assets because it would fragment cross-border stablecoin arrangements and reduce operational efficiency. The *US GENIUS Act* provides for interoperability standards and reciprocal arrangements with comparable jurisdictions, while the *UK framework* also contemplates deference to home-authority supervision for some non-sterling overseas coins. MiCA should take the same approach: remain open to multi-issuance where third-country regimes are robust and comparable, and manage the risks through equivalence, supervisory cooperation, reserve attribution and reporting requirements, rather than forced fragmentation.

Question 31. MiCA considers that all EMTs that are pegged to or denominated in an EU currency are offered to the EU and therefore fully subject to MiCA issuer requirements. Does this approach continue to be justified in view of market developments? Does it discourage the international role of the euro?

- ☒ Yes
- ☐ No

Question 32. What are the advantages and disadvantages of this approach for the EU and the international role of EU currencies?

The main advantage of this approach is that it prevents the issuance of euro-denominated EMTs outside the EU

regulatory framework. In practice, issuing these tokens offshore without regulation is not a viable business model anyway, as EU CASPs, banks, and other financial institutions are prohibited from supporting or offering services for them. This approach would strengthen EU supervision over euro-denominated flows and related foreign exchange activities. It would also contribute to reinforcing the international role of the euro by asserting a greater degree of monetary and regulatory sovereignty

Disadvantages: MiCA provisions enforce a rigid jurisdictional perimeter, mandating local EU issuance and continuous retention of a substantial portion of reserve liquidity within EU-authorized credit institutions. For cross-border settlement architectures requiring off-shore liquidity placement, this framework presents a critical operational hurdle, as positioning euro EMT reserves outside EU-supervised banking channels contradicts such requirements.

☐ **Interaction with the EU's economic security and the international role of the euro**

Question 33. To what extent do you believe that euro-denominated stablecoins can contribute to the following objectives?

Objective	1 Not at all	2 Small extent	3 Moderate extent	4 Large extent	5 Very large extent
Strengthening EU payment autonomy in retail payments			■		
Strengthening EU payment autonomy in wholesale payments				■	
Enhancing the international role of the euro				■	

Please explain your reply.

Convinced that stablecoins will become vital financial and payment instruments over the next 5 to 10 years, we strongly advocate for EU support in developing euro-denominated stablecoins. Among other benefits, this would help EU authorities maintain oversight over euro flows and their associated service providers. However, while euro EMTs have immense potential to expand the euro's global reach in cross-border payments, this can only happen if the regulatory framework allows them to scale globally -backed by international supervisory cooperation- and remain globally competitive. In this regard, the "double reserve" requirement imposed by MiCA leads issuers to maintain separate reserves or smart contracts depending on the jurisdiction, which fragments liquidity and prevents the creation of a critical mass comparable to that observed in US markets, where issuers can centralise their reserves. As a result, euro-denominated stablecoins risk seeing their capitalisation plateau and remain structurally less competitive than their dollar-denominated counterparts, which are able to capture global volumes more easily.

While it is necessary to ensure that reserves remain fully backed by the euro and available at all times, it is essential to offer issuers a minimum of flexibility in the management of their assets.

In line with this approach, it should be possible for part of the reserves to be deposited with a foreign subsidiary of a European credit institution. Provided that this subsidiary is subject to equivalent prudential requirements and integrated into consolidated supervision, such an arrangement does not in any way reduce the level of protection for European users. On the contrary, it would support the international development of European issuers, while ensuring continuity of protection and supervision. Rejecting this option would amount to artificially limiting the ability of European players to operate on a global scale, giving their non-European competitors an unfair competitive advantage.

☐ **Current safeguards in MiCA**

Question 34. MiCA provides safeguards to mitigate the risks of multi-issuance stablecoins. For each safeguard listed below, please indicate how effective you consider it to be on a scale where 1 means 'Not effective at all' and 5 means 'Highly effective'

Safeguard	1	2	3	4	5
Restriction of widely used ARTs and EMTs denominated in a currency that is not an official currency of a Member State (Articles 23, 58)				■	
ECB binding opinion powers on withdrawing authorisation and limit the amounts of ARTs and EMTs (Articles 24(2)(3), 58)				■	
EU establishment requirement for ART and EMT issuers (Article 16)				■	
Reserve location, composition and liquidity requirements for ARTs and EMTs (Articles 36–38, 45, 54)				■	
The powers of competent authorities listed in Article 94, especially to suspend or prohibit the trading of crypto-assets				■	
National supervisory intervention powers (Article 105)					
EBA temporary intervention powers (Article 104)					

Question 35. MiCA requires that the reserves of the EMTs and ARTs issued, offered or held in the EU should be held in the EU. Can the tokens held in the EU be determined or estimated with sufficient accuracy and frequency?

- ☐ Yes, EU holdings can be determined with sufficient accuracy and frequency
- ☒ Partially, but with some limitations (e.g., delays, estimation challenges)
- ☐ No, current methods are insufficient for reliable compliance
- ☐ Uncertain

Please explain your reply to the above question, including any specific remarks with regard to tokens held in unhosted wallets.

The primary challenge is self-custodied (unhosted) wallets. As the EBA noted in its Article 22 RTS work, these wallets can't be reliably linked to a specific country. Supervisory expectations need to be realistic and risk-based, accepting that 100% precision isn't feasible across every model. As for timing, current CASP reporting gives us enough lead time to keep EU reserves properly sized, with the mandatory rebalancing rule acting as a solid backup. We'd advise against pushing for high-frequency recalculations on unhosted holdings- it simply inflates costs without making the data any better.

Question 36. Should MiCA redemption rights be explicitly limited to EU holders only?

- ☐ Yes
- ☐ No

Please explain your response.

If you indicated “Yes, what criteria should be used to determine who qualifies as an EU holder? Please also provide a rationale for your proposed approach.

The EU-reserve held by a multi-issuer or foreign stablecoin provider is calibrated to match anticipated EU circulation, rather than the total global outstanding supply of the token. Allowing non-EU holders to redeem against this EU reserve would immediately create a mismatch between reserve size and redemption risk, potentially compromising its role as a liquidity safeguard for EU users. Limiting redemptions exclusively to EU residents also helps eliminate cross-issuer arbitrage risks associated with multi-issuance structures. Regarding eligibility criteria, EU holder status should be verified at the level of EU EMI/CI entities using existing KYC/AML procedures, which already include residence and identity verification for onboarded clients.

Lastly, the “double reserve” requirement imposed by MiCA leads issuers to maintain separate reserves or smart contracts depending on the jurisdiction, fragments liquidity and prevents the creation of a critical mass comparable to that observed in US markets, where issuers can centralise their reserves. As a result, euro-denominated stablecoins risk seeing their capitalisation plateau and remain structurally less competitive than their dollar-denominated counterparts, which are able to capture global volumes more easily. While it is necessary to ensure that reserves remain fully backed by the euro and available at all times, it is essential to offer issuers a minimum of flexibility in the management of their assets. In line with this approach, it should be possible for part of the reserves to be deposited with a foreign subsidiary of a European credit institution. Provided that this subsidiary is subject to equivalent prudential requirements and integrated into consolidated supervision, such an arrangement does not in any way reduce the level of protection for European users. On the contrary, it would support the international development of European issuers, while ensuring continuity of protection and supervision. Rejecting this option would amount to artificially limiting the ability of European players to operate on a global scale, giving their non-European competitors an unfair competitive advantage.

☐ **Potential additional safeguards**

Question 37. In a multi-issuance model, reserve assets may be located across jurisdictions and legal entities. Concerns have been expressed that in times of market stress, the transfer or rebalancing of reserves between issuers may be delayed or restricted. Is this concern valid or substantiated in your view?

- ☐ Valid-substantiated
☒ Not valid-not substantiated

Please explain your response

This binary option looks a bit simplistic to us.

The existing framework already addresses this risk. Daily CASP reporting and dynamic reserve rebalancing requirements ensure that the EU-side reserve is continuously calibrated to actual EU circulation, rather than being adjusted reactively in periods of stress. Moreover, the concern identified here applies with equal, if not greater, force to the reserve structures of many existing financial institutions operating across borders, where such risks are routinely managed through intragroup liquidity arrangements, access to central bank facilities, and supervisory coordination.

Further, more than 99% of the global stablecoin market consists of foreign-denominated, foreign-regulated tokens issued outside the EU. Excluding the dominant form of stablecoin activity from MiCA's regulatory perimeter therefore represents a material and substantiated risk to EU consumers and businesses, as well as to the international competitiveness of EU crypto-asset markets.

The proposed approach would also introduce a structural mismatch between the near-instantaneous nature of token redemptions and the comparatively slower processes involved in liquidating reserves and transferring funds

across borders. This could create additional liquidity risks, particularly under stressed market conditions, when the timely transfer or rebalancing of reserves may be constrained by differences in collateral quality, eligibility requirements, or regulatory treatment. Such constraints could create frictions in liquidity management and, in turn, affect the efficiency and resilience of multi-issuance models.

Question 38. How effective would the following possible additional measures be in mitigating such concerns?

- 1 = Highly ineffective
- 2 = Somewhat ineffective
- 3 = Neutral / uncertain
- 4 = Somewhat effective
- 5 = Highly effective

Possible additional mitigation measure	1	2	3	4	5
Introducing requirements that would favour or strengthen the redemption rights of holders of stablecoins that are genuinely circulating in the EU, as opposed to redemption rights associated with stablecoins transferred to the EU in times of stress to take advantage of MiCA protections (including redemption rights)					■
Restricting direct redemption rights in the EU to holders who are clients of EU-authorized CASPs, while holders that keep the tokens in un-hosted wallets do not have a MiCA guaranteed redemption right in the EU.	■				
Differentiating redemption rights in crisis situations between retail and wholesale/professional holders	■				
Requiring a dedicated liquidity buffer or additional reserve tranche specifically calibrated to cover short-term redemption spikes in the EU		■			
Strengthening real-time or high-frequency reserve and liquidity reporting to EU competent authorities, including granular disclosure of reserve location and transfer constraints		■			
Establishing binding cooperation arrangements between home and host supervisors to ensure rapid approval and execution of cross-border reserve transfers in stress scenarios					■
Others					

If your answer is “Others”, please elaborate.

Regarding the measure consisting of: *“restricting direct redemption rights in the EU to holders who are clients of EU-authorized CASPs, while holders that keep the tokens in un-hosted wallets do not have a MiCA guaranteed redemption right in the EU”*; we would like to stress that redemption at par is the holder's right against the issuer (Art. 49), not a feature of the wallet the token sits in. Making it depend on holding through an EU CASP would create two classes of the same token, break fungibility, and push users into intermediaries to keep a right they already have. A self-custodied holder can prove a holding on-chain as easily as a custodial one.

Question 39. If you referred in your response to question 38 to adjusting redemption rights, please provide any comments on the operational feasibility, legal implications, proportionality, or potential intended or unintended consequences of such amendments to the redemption rights in MiCA as listed above or in any other way.

From an operational standpoint, differentiating EU holders from non-EEA holders during the redemption process is straightforward. Additionally, in worst-case scenarios, a snapshot taken on a specific day can be used to assess EU holdings when claims are submitted by both CASPs and non-custodial holders. Legally, MiCA is designed to provide EU users and holders with consumer protections, including local redemption rights. As with other EU financial regulations, MiCA does not possess extraterritorial authority—except in the case of euro EMT issuance, which is considered an EU offer to the public. Therefore, it is legally feasible to restrict redemption rights within the EU to EU holders and liabilities only, consistent with MiCA Recital 54. Non-EU (EEA) holders would continue to retain their global redemption rights associated with the same token outside the EU.

Question 40. Do you see merit in introducing an [equivalence regime](#)⁴ for global stablecoins in the EU?

- ☐ Yes but only if other mitigation measures are not introduced
- ☒ Yes, in addition to mitigation measures
- ☐ No

Please provide reasons for your response, including any perceived advantages or disadvantages of equivalence regimes.

An effectively crafted equivalence framework -drawing on the EU's proven equivalence structures under EMIR, CSDR, CRR, and Solvency II- would provide a more legally sound and operationally consistent alternative to the current multi-issuance approach.

Question 41. Equivalence regimes can rely on the third country's regime to various degrees. How far, in your opinion, should a possible equivalence regime go in terms of relying on a third-country regime? What rights or benefits should EU issuers derive from equivalence of a third country and what rights or benefits in the EU should issuers from an equivalent jurisdiction receive in the EU?

An equivalence regime should oblige the third country issuer to respect EU obligations on redemptions, composition of the reserve and own funds.

Equivalence should not be granted solely on a theoretical basis, but should reflect the ability to effectively enforce rules in practice, including in stress scenarios.

As regards reciprocity, where a third country has granted equivalence to MiCA, EU issuers should benefit from genuine and effective market access in equivalent jurisdictions, under conditions that are not materially more restrictive than those granted within the EU. Conversely, access for third-country issuers to the EU market should remain conditional upon strict compliance with EU objectives, and could be limited or calibrated where necessary.

Liability in stress and wind-down should remain with the foreign-regulated primary issuer that issued the token and carries the core reserve and prudential obligations, with the EU framework relying on recognition, supervisory coordination, and cross-border insolvency mechanisms to ensure that those obligations are effective vis-à-vis EU holders. That approach provides EU authorities meaningful local oversight and enforceable local protections without creating the dual-liability, double-capitalisation, and reserve fragmentation.

Question 42. What administrative simplification or burden reduction measures should be considered under titles III and IV and their implementing measures and technical standards? Do you believe that MiCA level 1 provisions lay down proportionate rules for issuers of EMTs and ARTs?

⁴ https://finance.ec.europa.eu/eu-and-world/equivalence-non-eu-financial-services-frameworks_en

1. Strongly disagree
2. Rather disagree
3. Neutral
4. Rather agree
5. Strongly agree

MiCA Level 1 requirements for ARTs and EMTs issuers	1	2	3	4	5
Authorisation of ARTs and EMTs issuers			■		
Prudential requirements		■			
Governance arrangements				■	
Obligations in respect of specific crypto-asset services		■			

Question 43. Do you believe that below specified MiCA level 2 acts lay down proportionate and simple-to-apply rules for ART and EMT issuers, taking into account their different size, scope of activity and risk profile?

1. Strongly disagree
2. Rather disagree
3. Neutral
4. Rather agree
5. Strongly agree

MiCA Level 2 acts for ART and EMT issuers	1	2	3	4	5
RTS on complaint handling by issuers of ARTs (Article 31(5))			■		
RTS on the minimum content of governance remuneration (Article 45(7)(a))			■		
RTS on the information to be submitted in an application for authorisation to issue ARTs (Article 18(6))			■		
COM Delegated Act on ART/EMT significance criteria (Article 43(11))		■			
RTS on own funds for issuers of ARTs and EMTs (Article 35(6))		■			

Please motivate your answers and briefly explain what the problems are for your highest-rated issue(s) and suggest how they should be addressed (e.g. legislative clarification, supervisory guidance, industry standards).

Significance criteria: The current framework for determining “significant” ARTs and EMTs lacks clarity and precision. Some of the criteria remain open to interpretation, which may lead to inconsistent application across jurisdictions and supervisory fragmentation. In addition, certain indicators do not appear to be closely aligned with the actual risk profile or systemic relevance of issuers. Simplifying these criteria, together with clearer supervisory guidance, would improve consistency and legal certainty.

Own funds requirements: The current own funds framework appears relatively rigid and may not adequately reflect the actual risk profile of issuers. In particular, it does not sufficiently distinguish between different business models, reserve structures and risk exposures. A more risk-sensitive and proportionate calibration would therefore be desirable, allowing capital requirements to be better aligned with the underlying economic and operational risks.

ARTs approval timeline: the current 100-day period for the regulator to approve an application is too long and should be shortened.

EMTs wallets and licensing requirements: EMIs issuing EMTs should be authorised to provide wallets to clients without this being considered a cryptoasset transfer service requiring an additional CASP licence, as is currently the case.

MiCA-PSD: Similarly, the custody and transfer of cryptoassets are currently also considered payment services. This can result in two licences being required for the same activity: one CASP licence and one PSP licence. This double licensing requirement should be abolished, with the provision of these services being categorised under either one or the other regulatory framework.

Question 44. Do issuers identify any need to further standardise reporting requirements for issuers/information flow between CASPs and issuers for the purposes of MiCA?

- ☐ Yes
☒ No

Please explain:

Despite the extensive Level 2 work on reporting templates, there are still significant gaps and inconsistencies in CASP data submissions. For example, issuers receive data from CASPs in different formats, making reconciliation difficult and costly. This creates operational challenges and may lead to inconsistencies in implementation across market participants. Industry initiatives have already been undertaken to standardise these reporting frameworks. These efforts should be further leveraged, formalised and endorsed at the regulatory level to ensure greater harmonisation, legal certainty and operational efficiency. A key example is the reporting by CASPs to EMIs on the use of stablecoins. Some of the required data are difficult, if not impossible, to produce. For example, reporting the distribution by country of EMT holders using unhosted wallets is particularly challenging. This reporting is also very burdensome for EMIs, which may ultimately become responsible for the quality of data provided by CASPs.

A single, machine-readable standard template developed by the EBA, with input from major compliant issuers and similar to the white paper template, would be desired. Given the frequency and confidentiality of the reporting data, we also suggest making it mandatory for CASPs to share these data points via API endpoints provided by the issuer, where the issuer offers this option. MiCA should be amended to ensure that CASPs report this information directly to supervisors, allowing them to assess and ensure the quality of the data.

In addition, the treatment of multi-issuance models remains unclear. Ongoing work in this area, notably the ESAs' recent reflections and proposals put forward by certain Member States, including Germany and Italy, should be taken into account and further developed to provide a clearer and more consistent regulatory approach.

Overall, further standardisation and clarification would significantly improve the effectiveness and proportionality of the MiCA reporting framework.

Part 3. Legal framework CASPs

MiCA created a legal framework for crypto-asset service providers. While provisions governing crypto asset service providers have been in operation only since the end of 2024 and a transitional period for service providers that were already on the market ended in a number of Member States, a substantial number of crypto asset service providers have now been authorised across a range of Member States and service categories 9.

This section accordingly seeks stakeholders' feedback on the adequacy of the current scope of crypto-asset services regulated under MiCA and seeks views on the merits of simplification of the framework, any risks not properly accounted for and on the functioning of certain CASP business models in light of MiCA.

3.1. On crypto-assets services

Question 45. Is the list of crypto-asset services as defined in Article 3(16) of MiCA adequate to effectively cover crypto-asset markets and provide sufficient legal clarity for businesses?

- ☐ Yes
☒ No

We observe a lack of detail in the definitions of several services, notably reception and transmission of orders, exchange of crypto-assets, and transfer services, particularly in relation to less common business models such as OTC trading. Notably, the definition of transfer services (Art. 3(1)(26)) is the most affected. It should be clarified that a transfer service requires the provider to control the crypto-assets or the means of access to them during the transfer. The mere technical transmission of an instruction is not a transfer service.

Regarding their relation to business models such as OTC trading, the lack of clarity comes primarily from the definition of "exchange" and "execution" and their application in practice. Within the EU, there is a divergence, particularly regarding the application of these definitions to OTC services and "hedging". Many OTC desks are registered only for exchange in their home countries, while a few jurisdictions, such as France, consider "hedging" to be an execution service. Furthermore, we observe some NCAs tend to classify exchange services as "execution of orders on behalf of clients" relying on the concept of "matched principal trading" as defined in Article 4 (1) point 38 of the MiFID II Directive, even though most business models based on an exchange service do not fit this definition. This sometimes forces applicants for CASP license to include an execution service in their application, even though they use their own capital as described in the definition of an exchange service in Article 3(1)(20) of MiCA.

Overall, this lack of clarity also results in inconsistent interpretations of these services among National Competent Authorities (NCAs).

Question 46. If additional services should be added, what should those be and what requirements should be applied to these services and service providers? If you believe that certain services should be removed, please specify which ones and why.

Yield of stablecoins: MiCA framework should distinguish prohibited remuneration linked to holding stablecoins from ordinary commercial arrangements such as transparent fee discounts, loyalty benefits not linked to holding period or token balance, and interest paid on separate fiat cash accounts held with credit institutions, subject to appropriate limitations, as well as appropriate disclosures and prudential requirements applicable to the CASP's existing licence.

Please refer to our response in *Question 20* for further details and justification.

Overall, **we support maintaining the distinction between the MiCA and MiFID regimes, rather than expanding the scope of MiCA to encompass all types of crypto-assets and related services.** As further explained in our response to Question 1 of this Consultation, we advocate for a framework that preserves the existing separation between crypto-assets that qualify as financial instruments and the services associated with them under sectoral financial services legislation, and crypto-assets and services that fall within the scope of MiCA.

We strongly support maintaining a clear carve-out on non-custodial service where providers that facilitate or orchestrate transfer flows without having access to, possession of, or control over clients' crypto-assets. Where a provider merely enables the transmission of transaction instructions or provides technical infrastructure, without holding private keys, and cannot on its own transfer the client's crypto-assets, such activity should not be requalified and scoped by the Regulation. We therefore encourage the regulator to confirm this explicitly in the Level 1 text. Accordingly, we suggest recital 83 should be moved into an operative provision in an Article, and Articles 73 and 75(9) should confirm that a CASP's use of a provider that cannot move client assets on its own is an outsourcing arrangement, not sub-custody. We apply the same control-based test to certification schemes for non-custodial wallet software in our response (see *Question 64, Part 4.1*).

Question 47. Would the introduction of appropriateness test for the crypto-asset services of reception and transmission, execution and placing of crypto-assets increase the protection for CASP clients, especially retail clients?

- ☐ Yes
- ☒ No

Such a requirement would treat crypto-assets as a uniquely problematic asset class without a clear policy justification. Certain segments of equity markets can be equally, and at times more, volatile. More fundamentally, there is no general rule that an entire asset class, such as equities, bonds, gold or real estate, is automatically subject to an appropriateness test. More broadly, capital markets are evolving towards greater integration across asset classes, including through the increasing use of distributed ledger technology and tokenisation. Over time, crypto-assets and traditional financial instruments are likely to converge further. If tokenisation becomes the norm over time, this raises the prospect that an appropriateness-test approach initially aimed at crypto-assets could in practice extend across an ever wider range of assets, potentially making such tests a feature of mainstream capital markets rather than an exception. In practice, this would create additional friction and barriers for retail participation, rather than delivering meaningfully better outcomes for clients. This friction is not theoretical: many retail clients are reluctant to go through additional assessment processes, so the requirement would likely deter participation in practice rather than improve protection in a meaningful way. From a policy perspective, the objective should be to support informed participation in capital markets, not to create unnecessary obstacles that discourage individuals from investing and leave them holding idle savings. Cryptoassets play a legitimate role in helping retail investors participate in capital markets, provided that firms meet appropriate standards on disclosure, conduct, and operational resilience.

Question 48. The provision in the EU of crypto asset services covered by MiCA requires that the service provider is authorised under MiCA and complies with its requirements. Do you have evidence of non-EU authorised crypto asset services providers continuing to offer their services in the EU? How do they promote their services in the EU? What tools would supervisors or enforcement authorities have, or should they have, to stop non-authorised service providers from offering their services in the EU or to EU customers? * Currently, there are

around 170 CASPs listed in the ESMA register (including both authorised CASPs and other entities that have notified to their national competent authorities their intention to provide crypto-asset services). These authorisations or notifications come from 18 different Member States.

If your answer is “No”, please explain what in your view could be a relevant alternative.

- ☒ Yes
☐ No

While the reverse solicitation principle allows crypto-asset services to be provided at the exclusive initiative of the EU client, we consider it essential that competent authorities closely supervise its use to prevent it from becoming a de facto channel for circumventing MiCA requirements by non-EU providers.

We recognise that enforcement across borders is inherently challenging in the crypto-asset sector due to its online and borderless nature. **However, we also observe that cross-border enforcement tools remain fragmented and are not applied consistently across Member States.** In this context, a more coordinated approach at EU level would significantly strengthen supervisory effectiveness. **We therefore support greater cooperation between ESMA and national competent authorities, including enhanced information-sharing on non-compliant firms, coordinated cross-border investigations, and more aligned enforcement actions across the Union.** In addition, regulators should be able to request or require the removal of applications from unlicensed crypto-asset service providers from the EU version of app stores. Also, regulators should take into account promotion through social networks and digital marketing.

We also believe that assessments should take into account factual indicators like the existence of an establishment within the EU, such as the rental of office space in a Member State or the presence of employees or contractors performing commercially oriented functions within the EU.

At the same time, particular situations should be considered where the application of MiCA is not yet fully operational at national level. For example, in certain Member States, such as Poland, a lack of domestic implementation of MiCA prevents fully authorised firms from fully passporting services into this country. In such cases, reverse solicitation may serve as a necessary and proportionate mechanism to avoid market disruption and ensure continued access for clients.

Overall, the global nature of CASPs and CASP products should incentivize EU policymakers and regulators to bring as many global CASPs with as much global market share as possible under its regulatory perimeter.

On Prudential requirements for CASPs

Article 67 of MiCA provides that prudential safeguards for crypto-asset service providers shall be equal to an amount or at least the higher of an amount of permanent minimum capital or one quarter of fixed overheads of the preceding year, reviewed annually.

Question 49. Is the prudential regime for crypto-asset service providers appropriate to capture the risks associated with the provision of crypto-asset services, or would it be warranted to adjust the prudential stance, e.g. by aligning it with the requirements for own funds applicable to investment firms (including K-factors) that provide services that are broadly similar?

- ☒ It is appropriate to capture the risks associated with the provision of crypto-asset services
- ☐ It would be warranted to adjust the prudential stance

We consider that the current prudential framework under MiCA is acceptable. However, any future adjustments should be carefully targeted only for smaller CASPs to better reflect their specific risk profile of crypto-asset activities, in order to avoid creating disproportionate burdens .

In particular, exporting requirements for own funds applicable to investment firms (including K-factors) may penalize smaller CASPs in a disproportionate manner. K-factors were calibrated for MiFID investment firms risk profiles rather than crypto activities. Thus, rather than applying a broad K-factor framework, a risk-sensitive schema could be introduced. We suggest scaling own funds requirements to accommodate smaller players in proportion to the identified operational and safekeeping risk that activities carry. This targets the genuine risk and is more suitable for small entities.

In light of this, such a schema should measure the control environment (e.g., segregation of client assets, a key-control set-up that prevents unilateral transfer, insurance, audited controls) rather than the value of assets under custody. A charge that grows with assets under custody would penalise growth in regulated EU custody without reducing the risk of loss.

Question 50. Is the amount of minimum capital provided for each class of CASP listed in Annex IV of MiCA adequate or should it be recalibrated?

Please rate each minimal requirement on a scale from 1 to 5, where:

- 1 = Significantly decreased (much lower than current MiCA requirements)
- 2 = Somewhat decreased (moderately lower than current MiCA requirements)
- 3 = Kept roughly as is (current MiCA calibration is broadly appropriate)
- 4 = Somewhat increased (moderately higher than current MiCA requirements)
- 5 = Significantly increased (much higher than current MiCA requirements)

CASP minimum capital requirements	1	2	3	4
Minimum initial capital for Class 1 (EUR 50.000)		■		
Minimum initial capital for Class 2 (EUR 125.000)				
Minimum initial capital for Class 3 (EUR 150.000)				

Please explain your answer, indicating, if necessary, how the amount of minimum capital should it be recalibrated?

Specifically and exclusively for MiCA services that are also to be classified as payment services, we suggest aligning the requirements with those applicable to payment institutions in relation to fixed overheads under MiCA. To ensure proportionality and reduce the burden associated with dual licensing, we support the use of the same percentage methodology (preferably Method A) as applied to the calculation of own funds requirements for payment institutions.

Likewise, it would also be critical to authorize to net the various capital requirements between licenses, eg CASP, EMI, PSP, Investment Firm, and not add them.

1° On multi-function groups

MiCA recognises and supports multi-function groups in which issuers, crypto-asset service providers (CASPs) may provide multiple MiCA-scope crypto-asset services, or may also carry out other types of financial activity, based on proper governance and management of the conflicts of interest this may generate.

Question 51. Should the current approach be maintained or should there be enhanced oversight and coordination in relation to entities that in addition to providing crypto-asset services, offer (1) other unregulated services or (2) other types of regulated services, (3) a combination of crypto-asset services?

- ☒ The existing approach should be maintained
- ☐ There should be enhanced oversight and coordination in relation to such entities

If you chose the second option, which of the following enhanced oversight and coordination mechanisms do you consider may be appropriate?

- ☐ Group-level reporting to a centralised authority
- ☐ Enhanced supervisory cooperation between ESAs / NCAs
- ☐ Operation of new supervisory colleges
- ☐ Consolidated supervision
- ☐ Other

Please provide any comments on the operational feasibility, legal implications, proportionality, or potential unintended consequences of the measures above. If your answer is "Other", please elaborate.

The multi-function group option should still be possible. Regulated institutions, such as credit institutions, payment institutions, investment firms, enter crypto-asset services by adding MiCA permissions under an existing governance framework. Group-level oversight already exists for them under sectoral law, so a parallel MiCA-specific layer would add cost without adding control.

2° On reporting

Apart from the obligation to report any reasonable suspicion regarding an order or transaction where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed, there are no formal reporting obligations for CASPs in MiCA.

Question 52. Should CASPs report regularly their activities? If yes, what kind of reporting would be useful? How often?

	YES	NO
Direct holdings of crypto-assets by CASPs		☒

Large exposures to derivatives with crypto-assets as the underlying asset		■
Volumes of leveraged contracts and the extent to which leverage is actually used on trading platforms		■
Information on counterparty risk		■

CASPs already have very extensive reporting obligations under Articles 22 and 23 of MiCA. We believe that the implementation of reporting requirements should be proportionate and appropriately sequenced to avoid imposing unnecessary reporting burdens or requiring the submission of data that does not provide meaningful insights or material changes compared with previously reported information. This approach would help ensure that supervisors receive high-quality, meaningful, and comparable data while minimising unnecessary operational burdens for CASPs.

3° Environmental and sustainability reporting

MiCA strengthens transparency on the environmental impact of crypto-assets. It does so by (1) requiring white papers to contain information on the main adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism used to issue the crypto-asset, and (2) requiring CASPs to make that information prominently available for each crypto-asset where they provide services.

Question 53. Based on your experience to date, how do you assess the current environmental/sustainability disclosure regime under MiCA (including the relevant Level 2 RTS)?

- ☐ Fully appropriate and proportionate
- ☐ Broadly appropriate, with limited areas for clarification
- ☒ Partially appropriate, but improvements could be considered
- ☐ Not appropriate

Please explain your assessment.

MiCA strengthens transparency on the environmental impact of crypto-assets and also closes a gap in the EU Sustainable Finance landscape which was based on the Sustainable Finance Disclosure Regulation and the Corporate Sustainability Reporting Directive. However, given that permissionless networks lack corporate issuers to provide primary data, the current framework makes the process redundant because multiple platforms separately calculate and publish competing energy metrics for the exact same blockchain network, resulting in duplicated administrative costs without adding any consumer value.

We also identify that not all MiCA licensed CASPs in the EU are currently meeting this requirement. This is explained by different (or inexistent) enforcement practices across EU Member States. Some NCAs granted licenses without checking how this requirement has been or will be met before granting the license; or without oversight on this requirement after providing the license. The long list of optional indicators has mostly been ignored by market participants so far.

In addition, reporting periods have not been clearly defined leading to different approaches in the market. Thus, methodological guidance regarding reporting periods will benefit from further clarifications. ESMA template requests to report for certain values where it is not clear if should the reporting relates to A: “the last calendar year”, B: “12 months previous of reporting”, or C: “most recent data, e.g. 2 weeks, annualized”.

We also consider that further methodological clarification would be beneficial. In particular, the applicable reporting period is not always clearly defined in the ESMA disclosure template, resulting in divergent market practices. For certain metrics, it is unclear whether reporting should relate to **(A)** the previous calendar year, **(B)** the 12 months preceding the reporting date, or **(C)** the most recent available data annualised where appropriate. Greater clarity on the expected reporting reference period would improve consistency across market participants.

Finally, there’s a quite long list of optional indicators that only few CASPs meet. Further clarification on the purpose of those would also be beneficial.

To further improve both the utility and the proportionality of these sustainability disclosures, we recommend two changes:

- **Simplify white paper disclosures to a single key indicator.** The public white paper disclosure should focus on electricity consumption as the primary and most user-relevant environmental indicator. A single, clearly presented data point , accompanied, if appropriate, by a simple traffic-light classification (e.g. green / amber / red) calibrated to actual consumption levels - would do significantly more to inform users and businesses than the current approach of disclosing multiple approximative data points derived from complex and often contested methodological heuristics.
- **Establish centralised ESMA data publication for major crypto-assets.** ESMA should engage directly with one or more leading third-party data providers to centrally publish the key sustainability indicator(s) - ideally the single electricity consumption figure recommended above, or the full set of required indicators if a simplified approach is not adopted - for the top 50 to 100 crypto-assets by market capitalisation. This would allow issuers and CASPs to reference centrally audited and harmonised data for the assets that represent the overwhelming majority of their activity, rather than each actor independently contracting with a third-party provider and producing divergent results for the same asset. The benefits would be threefold: harmonisation across the industry, a material reduction in compliance burden for smaller market participants, and greater credibility of the published figures. ESMA could fund this service through modest fees levied on the major CASPs, consistent with the cost-recovery model used in other areas of EU financial market infrastructure oversight.

4° On other issues

Question 54. Given that crypto-asset service providers are entities subject to the regulatory framework of the Digital Operational Resilience Act (DORA), are there any additional issues/challenges that need to be addressed in relation to cybersecurity?

DORA has introduced significant implementation costs for CASPs. A large share of that cost is bilateral negotiation of Article 30 contractual terms. Standard contractual clauses for the ICT services most used by CASPs (as foreseen in Art. 30(4) DORA), and recognition of established certifications (*SOC 2 Type II, ISO 27001*) as due-diligence evidence, would reduce this cost for CASPs and providers alike without lowering the bar.

In addition, certain crypto-specific cybersecurity risks are not always adequately addressed within the existing operational resilience framework. Crypto-specific ICT risks, in particular smart-contract risk and cryptographic key

management, deserve explicit treatment. That treatment should be outcome-based and technology-neutral, i.e., no single person or component can unilaterally move client assets, key material is segregated per client, keys are recoverable under tested procedures, every signing decision is logged and auditable, and so on and so forth. It should not prescribe a storage medium or technology. There are many technologies and methods, including technologies in development, that can deliver these outcomes when properly implemented. A rule written around one of them would concentrate rather than distribute risk.

Also, despite DORA being broadly appropriate as a baseline framework for digital operational resilience, further clarification regarding the interaction between MiCA's operational continuity requirements and DORA's ICT risk management obligations would help reduce regulatory uncertainty and ensure consistent implementation. Also, between both of these and the outsourcing requirements of Article 73 (outsourcing) of MiCA. One set of rules should govern a CASP's relationship with an ICT provider, where an arrangement falls within DORA, compliance with DORA should satisfy Article 73.

Question 55. The Payment Services Directive has been substantially reviewed recently, bringing notably more clarity on the interplay between the MiCA rules applying to the transfer services in relation to e-money tokens and the rules under the payment services framework which apply to the provision of payment services. As a result, the PSD3/R will clarify which crypto-asset services may qualify as payment services, including targeted exclusions from the scope of PSD3/R for specific types of transactions/exchanges involving EMTs, and will specify the authorisation process under PSD3 in cases where CASPs are required to obtain a PSD3 authorisation. Do you consider these changes to bring sufficient clarity or are there other issues that remain to be addressed? If so, please explain your response

☐ Yes

☒ No

We disagree that the PSD3/R clearly delineates which crypto-asset services qualify as payment services distinctly from MiCA services. On the contrary, PSD3/R confirms that certain services with EMTs qualify twice as MiCA and payment services, effectively requiring service providers to obtain a dual authorisation to conduct a single activity. The application of dual regimes for the same service contradicts the principle of proportionality and undermines the usability and - in the long term - the offer of services with these types of crypto-assets, as makes them more burdensome and costly for providers, to the detriment of the European consumer.

In the PSD2/3-R context, the EBA has highlighted that obliging CASPs to obtain a second authorization for the purpose of conducting the same economic activity is *"undesirable"* because the compliance burden would be *"disproportionate"* arguing that *"any given financial activity should be regulated by one piece of financial services law (...), to avoid "undue compliance burdens."* We note that certain provisions in the PSD3/R framework introduce a simplified authorisation process (Article 13 PSD3) for CASPs already authorised under MiCA that provide services overlapping with payment services. However, this procedure mainly streamlines administrative steps and reduces processing timelines, without addressing the more substantive burden related to own funds and prudential requirements.

This is, CASPs are required to fulfill such obligations both for PSD and MiCA regime. It is also worth noting that payment service providers benefit from a more favourable regime under MiCA Article 60, which grants them a streamlined notification procedure when providing equivalent crypto-asset services. In contrast, CASPs do not benefit from an equivalent simplification when seeking to provide payment services under PSD3/R, resulting in an asymmetry between the two regimes. A fundamental and urgent issue remains unresolved: the custody and transfer of e-money tokens qualify as payment services under PSD3/PSR, effectively requiring every CASP that

wishes to offer EMT-related services - including custody and transfer of euro stablecoins - to obtain both a MiCA authorisation and a payment services authorisation. This creates a structural dual-licensing burden that represents one of the most significant regulatory barriers to stablecoin adoption in the EU, and it has not been adequately addressed by the PSD3/PSR package as currently framed. The problem is not merely administrative. Requiring two separate licences - each with its own capital requirements, governance obligations, supervisory relationships, and compliance infrastructure - for what is, in economic substance, a single integrated activity makes the offering of stablecoin services materially more costly, more complex, and more time-consuming for every market participant, from large CASPs to the smallest fintech startups seeking to build stablecoin products and services in the EU. It is particularly damaging for innovation and competition in the euro stablecoin ecosystem, where reducing barriers to entry is essential if euro-denominated stablecoins are to compete effectively. The resolution is straightforward in principle. MiCA, as the *lex specialis* governing crypto-assets including EMTs, should be clarified to operate as the sole applicable framework for custody and transfer of EMTs by MiCA-authorised CASPs. The most direct legislative fix would be an explicit carve-out in PSD3/PSR - or a corresponding clarification in MiCA - confirming that the custody and transfer of EMTs by MiCA-authorised entities does not constitute a payment service for the purposes of PSD3/PSR, and that MiCA authorisation is sufficient for these activities. An alternative, if a full exclusion is not pursued, would be to ensure that EMT-related services are fully and exhaustively covered under the EMI licence framework, such that a single authorisation suffices. In either case, the objective is the same: one economic activity, one regulatory framework. Failure to resolve this will continue to suppress euro stablecoin issuance and adoption in the EU, disadvantage EU-based CASPs relative to competitors operating under simpler regulatory regimes, and undermine the broader objective - shared by the Commission, the EBA, and MiCA itself - of positioning the EU as a leading jurisdiction for regulated stablecoin markets.

In addition, several questions remain given the double nature of EMTs as electronic money and crypto-assets, as there's no clear indication of which qualification prevails for the purpose of the applicable tax and accounting regime. Furthermore, the same logic should apply at the perimeter: MiCA and PSD3/PSR should both confirm that technical service providers that never hold or control EMTs or funds fall outside both regimes, consistent with the technical-services exclusion in payment services law. Finally, we note that MiCA does not address ancillary services and activities, unlike other EU financial services legislation. Providing greater clarity in this area would help ensure a more comprehensive regulatory framework and could also prove beneficial in addressing the interaction between MiCA and PSD3/PSR or even MiCA/ MiFID framework.

Question 56. Do MiCA provisions governing crypto asset service providers sufficiently allow, or unduly restrict, access for EU consumers and investors to non-EU and global crypto asset trading and liquidity pools? What are the advantages and disadvantages of focusing on EU liquidity or full access to global liquidity?

Yes, MiCA licensed CASPs should be allowed to access global liquidity on a principal basis for hedging purpose) (not as an agent); it will offer EU consumers to invest in deeper liquidity and tighter spread while ensuring that transactions remain subject to the oversight and investor protection requirements applicable to authorised EU CASPs.

Question 57. Do you believe that the below specified groups of MiCA level 1 provisions lay down proportionate and simple-to-apply rules for CASPs, taking into account their different size, scope of activity and risk profile?

1. Strongly disagree
2. Rather disagree
3. Neutral
4. Rather agree
5. Strongly agree

MiCA Level 1 requirements for CASPs	1	2	3	4	5
Authorisation of crypto-asset service providers					■
Prudential requirements					■
Governance arrangements		■			
Obligations in respect of specific crypto-asset services			■		
Other Title V rules					■

Please explain your ratings and suggest how rules could be made simpler and more proportionate (e.g. legislative clarification, supervisory guidance, industry standards).

Regarding governance arrangements: we believe that rules do not take the size into consideration but for governance particularly. They are not precisely defined, leading to different interpretations across NCA. For example, the supervisory board- which is required in France but not in other jurisdictions.

Question 58. Do you believe that below specified MiCA level 2 acts lay down proportionate and simple-to-apply rules for CASPs, taking into account their different size, scope of activity and risk profile?

MiCA Level 2 acts for CASPs	1	2	3	4
RTS on complaint handling for CASPs (Article 71(5))				
RTS on offering pre-trading and post-trading data to the public (Article 76(16)(a))				
RTS on content and format of order book and records to be maintained (Article 76(16)(b))				
RTS on records to be kept of all crypto-asset services, activities, orders and transactions undertaken (Article 68 (10)(b))				
RTS on the continuity and regularity in performance of crypto services (Article 68 (10)(a))				

Please explain your ratings and suggest how rules could be made simpler and more proportionate.

Adan did not answer this question.

Part 4. Decentralised Finance

This section refers to decentralised finance (DeFi), understood as software programs deployed on blockchains or other types of DLT that operate autonomously without intermediaries and offer financial functionalities such as trading, lending, borrowing or portfolio management. In the broader sense, DeFi also refers to any blockchain-based application, including an application that does have an identifiable intermediary or person exercising control over its operation. MiCA excludes from its scope 'crypto-asset services that are provided in a fully decentralised manner without any intermediary'.

This section seeks feedback on whether and how to complement MiCA as regards DeFi considering potential opportunities and challenges.

Question 59. In case you are aware or make use of DeFi currently beyond the regulatory perimeter of MiCA, what are the main services you (would) use and for which of them do you consider they bring benefits compared to similar intermediated digital assets services?

1. DeFi applications present limited interest and are moderately used for this service
2. DeFi applications present important potential benefits for this service but their use remains limited due to some non-mitigated weaknesses
3. DeFi applications present important benefits for this service and are already significantly used, despite important non-mitigated weaknesses
4. DeFi applications present important benefits for this service, they are already significantly used and present limited risks

	1	2	3	4
Exchange services				☒
Payments and transactions services				☒
Trading and Investment services				☒
Lending and borrowing services				☒
Custody services				☒

Please detail the benefits or weaknesses you associate with the use of DeFi applications for these different services, and the actions you would consider appropriate to optimise these benefits or address the possible issues they raise.

As a preliminary observation, we note that the comparison implicit in this question (DeFi services vs. intermediated services) no longer reflects how the market actually operates. Regulated exchanges, banks and fintech increasingly build their own client-facing products on top of decentralised protocols, using them as shared, open infrastructure rather than competing with them. Also, we note DLT market infrastructures authorised under the EU's Pilot Regime (*Regulation (EU) 2022/858*) already rely on automated market-making protocols as part of their technical stack, operating within the regulated perimeter rather than outside it, and the SEC's Innovation Exemption, issued on 17 September 2026, permits on-chain trading of tokenised securities in the US specifically on condition that the underlying smart contracts run on a public, permissionless ledger. The more relevant comparison is therefore not between decentralised and intermediated services as such but between services built on this kind of open, common infrastructure and those built on closed proprietary systems that a single institution controls end to end.

About the table:

- **Exchange services:** The wording should be changed. “Executing asset trades” is too broad and creates ambiguity for systems where off-chain components coordinate settlement proposals but do not themselves execute user transactions. Exchange-related DeFi applications may reduce intermediary and settlement risks by allowing asset transfers to be enforced on-chain through transparent smart-contract logic, according to parameters authorised by users. In some architectures, off-chain components may coordinate information, batching, routing or settlement proposals, but this coordination should not be equated with execution, custody or discretionary control where the transaction only takes effect through on-chain validation and settlement. This service materially reduces certain intermediary, custody and counterparty risks intermediary and settlement risks by executing asset trades transparently and programmatically through autonomous smart contract protocols.
- **Lending and borrowing services:** terms, collateral requirements and liquidation rules are published onchain and enforced automatically, giving every participant (from individual users to regulated institutions building products on top of these protocols) equal, real-time visibility on the conditions of the market they use. This replaces discretionary credit-risk assessment with verifiable, over-collateralised positions and permissionless liquidations that resolve insolvency instantly rather than letting hidden exposures accumulate. Because these markets are open and borderless, they also give users and institutions access to deep, unfragmented global liquidity rather than jurisdictionally segmented pools.
- **Custody services:** we raise attention on this because self-custody isn’t really a competing DeFi service. It is the base layer that both direct and intermediated access sit on top of. A user holding their own keys isn’t exposed to a provider’s insolvency and their assets can’t be reused without their consent and that holds true whether they’re using a standalone wallet or a regulated custodial service built on that same wallet infrastructure underneath.
- **Payments and transactions services:** stablecoin-based payment rails offer near-instant, 24/7 settlement finality at lower cost than traditional cross-border rails, though this benefit is partly offset by network congestion and price volatility for non-stablecoin transfers.
- **Trading and investment services:** we note that most of what drives efficiency here comes from the properties of the asset used (e.g. *stablecoins*), a topic addressed separately in this consultation.

Question 60. What do you consider to be the main risks associated with DeFi?

[échelle 1-5 : Strongly disagree → Strongly agree]

Risk	1	2	3	4	5
Operational risk				■	
Money laundering and terrorist financing risk		■			
Market abuse		■			
Investor protection risk (information asymmetry, no redress, opacity of functioning)				■	
Financial stability	■				

Please explain your answers.

On operational risk, it is true that technical vulnerabilities (e.g., smart contract exploits, oracle dependencies, key management, cyber incidents, and so on) represent the primary area of vigilance in DeFi. However, these risks should be addressed in a manner that reflects the layer at which control is exercised. Where software or coordination mechanisms do not custody assets, bind users, determine economic terms or exercise discretionary control over settlement outcomes, intermediary-style obligations are unlikely to be an appropriate regulatory tool. We also should take into account that code security and operational resilience are economic survival conditions dictated by reputation and market discipline. The ecosystem has developed important risk-mitigation mechanisms, including independent audits, bug bounty programmes, open-source verification, public monitoring and market discipline. These mechanisms do not eliminate operational risk, but they demonstrate that DeFi risk management often operates through technical transparency and economic incentives rather than through discretionary intermediary controls. These mechanisms are not reputational or *ex-post* in nature. In fact, in well-designed protocols, several of them are embedded directly into the technical architecture in ways that are permanent, publicly verifiable, and cannot be discretionarily circumvented or captured by any party, including the protocol's own developers. Concretely, this can include timelocks that impose a mandatory waiting period between a governance decision and its execution, giving users a guaranteed window to exit before any parameter change takes effect; risk parameters (e.g. liquidation thresholds) that, once set, cannot be degraded after a user has posted collateral; supply caps that mechanically limit maximum exposure on a given market; and permissionless liquidation mechanisms that allow any external actor to resolve an insolvent position, rather than depending on a central operator, which removes the risk of liquidations being selectively delayed or triggered for the benefit of insiders. Modular architectures that isolate risk market-by-market further ensure that an operational failure in one market does not propagate to others, in contrast to the pooled-risk profile of monolithic structures. This structural approach to risk management is, in several respects, more resilient than purely *ex-post* supervisory enforcement, since its rules are known to all participants in advance and are not subject to discretionary application, political pressure, or regulatory capture. Since most operational parameters are determined *ex ante* through contract automation, risk is embedded within the technical architecture instead of being subject to discretionary management. Therefore, policy efforts must focus on providing clear guidance to entities that give access to, distribute, or interact with DeFi protocols.

On money laundering and terrorist financing risk, Such risks exist but are neither unmitigated nor specific to DeFi's decentralised nature. Illicit activity remains a small share of on-chain volume, representing less than 1% of total attributed on-chain transaction volume (*Chainalysis, 2026 Crypto Crime Report*⁵), and the recent growth in absolute illicit volumes is overwhelmingly driven by nation-state sanctions evasion through bespoke infrastructure (not by the use of decentralised protocols). Set against the wider financial system, this is also a small part of global illicit finance: blockchain analytics attributed roughly USD 154 billion to illicit crypto activity in 2025 (*Chainalysis, 2026 Crypto Crime Report, see above*), a fraction of the estimated USD 4.4 trillion of illicit funds flowing through the global financial system that year (*Nasdaq Verafin, 2026 Global Financial Crime Report*⁶). On-chain transparency and immutability give analytics providers and supervisors real-time traceability that traditional finance does not offer, and AML-CFT controls are already effectively enforced at the points where fiat on/off-ramps and regulated CASPs intersect with DeFi. We would caution against treating this risk as evidence for regulating the protocol layer itself, since doing so would not address the actual point of exposure. This is why AML-CFT controls should be located at the level of regulated intermediaries, through blockchain analytics and sanctions screening (*See our response to Question 62*). Bringing more EU users within the scope of EU-authorised CASPs strengthens, rather than weakens, AML-CFT effectiveness.

On market abuse, on-chain transparency and the immutability of public ledgers provide supervisors with unprecedented tools to detect and trace market manipulation in real time. Consequently, market abuse risks are best mitigated through the deployment of blockchain analytics and the oversight of regulated access points (e.g., CASPs) rather than unfeasible restrictions at the protocol level.

On investor protection risk, Unlike operational or market abuse risks, investor protection concerns specific to DeFi, such as smart contract vulnerabilities, loss of assets through user error (e.g. lost keys, phishing, malicious front-ends), and the general complexity of protocol mechanics for non-technical users, are not yet matched by

⁵ <https://www.chainalysis.com/reports/crypto-crime-2026/>.

⁶ <https://verafin.com/nasdaq-verafin-global-financial-crime-report/>.

adequate disclosure or safeguard practices across the ecosystem. We therefore see room for targeted improvement here, particularly through standardised, accessible risk disclosures at the point of user interaction.

On financial stability. DeFi remains marginal when compared to the traditional financial system and there is no demonstrated structural interconnection between DeFi and the EU's critical financial infrastructures. Consequently, the characterisation of DeFi as a threat to financial stability would be factually inaccurate and would direct regulatory resources towards the wrong priorities. This becomes clear when examining the actual scale of the ecosystem based on consolidated data from the European Banking Authority ('EBA') and the European Securities and Markets Authority ('ESMA'). DeFi accounts for only a very small share of the crypto-asset sector, representing approximately 4% of its total market capitalisation, with a total value locked of around €40 billion worldwide⁷. Within the European Union, adoption remains limited, as the 7.2 million recorded users represent only 1.6% of the population. DeFi should therefore be viewed more as a laboratory for technological innovation rather than a source of macroeconomic risk. Furthermore, we also note that blockchain transparency and non-custodial models inherently eliminate certain traditional risks, such as counterparty risk and information asymmetries; liquidations are executed automatically, transparently, and instantaneously through code, preventing the accumulation of hidden toxic debt. Current interconnections are largely confined to regulated entities exploring these technologies to optimise collateral management or liquidity provision, without exposing critical financial infrastructures. Any attempt to regulate DeFi through the lens of financial stability is therefore fundamentally misguided. This assessment also appears to be shared by the French supervisory authorities. On 2 June 2026, during a hearing before the French Senate⁸, the Financial Markets Authority ('AMF') Chair Marie-Anne Barbat-Layani explained that the lack of direct interactions between the crypto-asset ecosystem and traditional finance makes it difficult to envisage a shock in digital asset markets triggering a major systemic financial crisis. If the absence of systemic risk holds true for the digital asset sector as a whole, it applies even more strongly to DeFi, where there is currently no evidence of material systemic risk at EU level for the reason explained above; otherwise, it is clear that this analysis may need to evolve if DeFi architectures become more structurally interconnected with regulated financial markets.

Question 61. In case you consider the criteria for establishing whether a DeFi application is not fully decentralised not sufficiently clear, which of them should you consider should be used to assess the degree of decentralisation?

[échelle 1-5 : Strongly disagree → Strongly agree]

Criteria for establishing absence of full decentralisation	1	2	3	4	5
Existence of an identifiable intermediary (person or group of persons) providing a crypto-asset service		■			
Presence of control by an identifiable person or group of persons (e.g. via admin keys) over the key functionalities of a DeFi protocol (e.g. upgradeability of protocol)			■		
Significant concentration of governance power over the key functionalities of a DeFi protocol			■		
Custody of user assets by the DeFi protocol					■

⁷https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1391_Joint_Report_on_recent_developments_in_crypto-assets_Art_142_MiCA.pdf.

⁸ https://videos.senat.fr/video.5860306_6a1fbf9f031c4.audition-de-l-autorite-des-marches-financiers?timecode=1695540 and the minutes (FR) <https://www.senat.fr/compte-rendu-commissions/20260601/finc.html#toc6>.

DeFi protocol code is not open source			■		
Marketing of a DeFi protocol by an identifiable entity or person	■				
Other					■

Preliminary observations:

First, it is important to note that the phrasing of this question reflects a flawed and overly binary approach that opposes "*full decentralisation*" to a total absence of decentralisation. In fact, decentralisation is not a fixed, binary state or a homogeneous legal category. It exists along a dynamic spectrum where projects evolve according to varying degrees of distribution of control, governance, and critical functions. As observed in market practice, there is no universal threshold at which a protocol becomes "*fully*" decentralised instantaneously. For this reason, Adan always supports a functional approach to DeFi, based on the functions effectively exercised rather than on an abstract or theoretical definition of decentralisation.

The relevant question is therefore not "*Is this protocol sufficiently decentralised?*", but "*Is there a legal entity that exercises unilateral and independent control over this protocol such as to impose MiCA obligations on it?*". This shift in perspective is the only one consistent with the wording of Recital 22 of MiCA, which refers to services provided by an identifiable intermediary - not the abstract absence of decentralisation.

Adan therefore recommends that European institutions acknowledge the following:

- Decentralisation results from the identification of effective control (the key indicator) exercised by an entity, which can be assessed by indicators such as asset custody, the existence of discretionary powers, control over governance, or the ability to modify the protocol.
- Many protocols follow a progressive trajectory. An initial structuring phase is often necessary, during which a development entity assumes a central role in technical design, smart contract deployment, and project coordination. This phase, which may involve a traditional corporate structure intended to frame legal and operational risks, frequently precedes a gradual decentralisation phase. As the protocol is deployed and governance expands, decision-making functions transfer to distributed mechanisms, including on-chain governance frameworks. Technical decentralisation occurs alongside economic and organisational decentralisation, until no identifiable entity exercises discretionary control over the system as a whole. This evolutionary dynamic illustrates that decentralisation is a continuum, where certain functions may remain structured while others are fully distributed. That is why "control" should remain the key indicator.

We apply this test consistently throughout our response, to non-custodial services and wallets (*see our response in Questions 46 and 64*), to staking (*See our response in Question 66*), and, as regards the classification of crypto-assets, to the criteria-based approach we propose in *Question 7*.

1. Existence of an identifiable intermediary providing a crypto-asset service (score: 2)

Adan considers it essential to clarify what definition of "*intermediary*" is being used here. The term is left undefined in the consultation, yet the answer to this criterion depends entirely on it. The same remark applies to "*providing a crypto-asset service*".

Therefore:

- Does "*intermediary*" refer to any legal entity identifiably associated with a protocol (e.g. a founding team, a DAO's associated legal wrapper, a front-end operator), regardless of the function it performs? Or is it limited, as Adan believes it should be, to an entity that exercises effective, discretionary control over a MiCA-defined regulated activity, i.e. an entity with which end-users are in an identifiable contractual relationship?
- What is meant by "*providing a crypto-asset service*" here, that is to say, what conduct does this actually cover? Does it capture any entity that develops, deploys, maintains, or operates a front-end for a protocol,

irrespective of whether it exercises discretionary control over the regulated activity itself? Or is it limited to entities that actually determine how the service is rendered to end-users, by setting terms, controlling access, or exercising discretion over execution and settlement? Without clarification on this point, the criterion risks being applied inconsistently: a founding team publishing open-source code and a CASP executing client orders would be treated identically, despite performing entirely different functions in relation to the regulated activity.

Without clarification on both points, the criterion is not scoreable in a consistent manner, since respondents would be assessing fundamentally different things depending on which definitions they assume. Left unresolved, it causes the criterion to produce false positives. If the identifiable intermediary in question in fact controls the protocol, the protocol is simply not decentralised, and the presence of an intermediary as a separate criterion adds no information beyond what the "control" criterion already captures. If the intermediary provides a regulated service but does not control the protocol itself, the protocol remains decentralised, and treating the intermediary's existence as an indicator of centralisation produces an incorrect result. It is not a marginal scenario and a licensed CASP may lawfully offer its clients a MiCA-covered service, such as the exchange of crypto-assets, and route execution to a fully decentralised protocol over which it exercises no control whatsoever. In that case, an identifiable intermediary undeniably exists, and it undeniably provides a crypto-asset service, yet the protocol it interacts with is not thereby rendered any less decentralised. Any risks arising from CASP's use of the protocol are properly addressed through the CASP's own conduct-of-business and due diligence obligations, not through the mischaracterisation of the protocol's decentralisation status.

To sum up and put together, this shows that '*existence of an identifiable intermediary providing a crypto-asset service*' adds nothing once the control-based criteria discussed elsewhere in this response are applied (1) where the intermediary controls the protocol, the 'presence of control' criterion already capture this; and (2) where it does not, its existence has no bearing on the protocol's decentralisation status (as the CASP example above).

2. Presence of control by an identifiable person or group via admin keys over key functionalities (score: 3)

Adan considers this criterion operationally significant but scores it '3' because of how the Commission has worded it. Read literally, with upgradeability given as its own example, the criterion would capture protocols where no identifiable party holds discretionary power at all. Technical maintenance of a protocol's code, security safeguards, and governance rights that remain constrained, because they cannot reach existing markets, positions or user funds, or because no single identifiable party can exercise them alone, are not equivalent to discretionary intermediation, custody or execution of client transactions, and should not be scored as such.

However, admin keys or similar rights that can change how smart contracts perform regulated functions, or move user assets held by those contracts are an indicator that an identifiable entity retains discretionary control over the protocol and may therefore qualify as a legal entity subject to MiCA obligations.

The decisive element is not the mere existence of administrative rights, but their scope in relation to the regulated activity. Rights that enable an entity to determine which users may access the service, which assets are eligible for exchange, how prices are formed, or how the protocol's architecture can be modified are rights over the core regulated functions. Their existence suggests that the protocol does not operate autonomously and that its outputs depend on the discretionary decisions of an identifiable party. However, this should not capture mechanisms where prices or settlement terms result from open competition, algorithmic optimisation or independently submitted proposals, provided that the user's signed parameters remain binding and no identifiable person can impose less favourable terms or settle outside those parameters. Rights that cannot modify existing markets or positions, cannot access user funds, or only add new options, do not indicate discretionary control over the regulated activity.

Administrative rights held by a regulated issuer over its own token contract, or by a user over its own smart-contract wallet, are the exercise of issuer obligations or of self-custody, not indicators of an intermediary.

3. Significant concentration of governance power over key functionalities (score: 3)

This criterion is relevant but contextual. Concentration of governance power may indicate centralised control, but only if two conditions are met simultaneously: **(i)** the governance tokens in question confer rights over the core operational functions of the protocol; and **(ii)** their concentration is such that a single entity or coordinated group can effectively determine outcomes unilaterally.

We insist on the first condition, which is absent from the Commission's formulation and risks generating significant confusion. Governance tokens that entitle holders to vote on secondary matters (branding decisions, developer grants, treasury allocations, or interface parameters *etc.*) do not confer control over the regulated activity in any meaningful sense. Treating their concentration as an indicator of absence of decentralisation would capture a wide range of protocols whose core functions are fully automated and non-custodial solely because their off-chain governance is imperfect. This would be both disproportionate and analytically incorrect.

Otherwise, from a strict technical point, if the core financial functionalities of the smart contracts are immutable (non-upgradeable) and hardcoded into the protocol, a heavy concentration of governance tokens on secondary parameters does not indicate a lack of technical decentralisation. In such architectures, no group of token holders (regardless of their voting power) can unilaterally alter user assets, execute discretionary transactions or modify the underlying protocol layer.

Even where governance tokens do confer rights over core functions, the assessment must account for the effective distribution of voting power, the existence of quorum and supermajority requirements, the presence of on-chain timelocks that give users time to exit before changes take effect, and the degree to which decision-making is genuinely open to unaffiliated participants. A protocol where a founding team holds 60% of governance tokens at launch but where those tokens are subject to multi-year vesting schedules and where a timelock of 48 hours applies to all governance decisions presents a materially different risk profile from one where the same concentration enables immediate unilateral changes.

4. Custody of user assets by the DeFi protocol (score: 5)

We consider this criterion the most fundamental of the list. The ability of an identifiable entity to initiate transactions involving user assets without their active consent or participation is the core risk that MiCA is designed to address. It is the condition that makes a contractual relationship between a service provider and a client both possible and meaningful.

For this reason, the mere fact that assets interact with, or are temporarily held by, a smart contract should not be equated with custody by an intermediary. The decisive factor is whether an identifiable person has legal or technical power to control those assets or dispose of them on behalf of users. Adan applies the same test in its response to *Question 46 (see Part 3 of the consultation)* and recommends one functional definition of control across the Regulation: a person controls crypto-assets, or the means of access to them, where it can alone transfer those crypto-assets on the distributed ledger without the participation or authorisation of the client.

In practice, this distinction can be tested against concrete, verifiable technical facts rather than assessed in the abstract. A protocol should be considered non-custodial where it has no technical ability to intervene in, reverse, or condition a transaction once initiated, and where users retain an unconditional right to withdraw their assets at any time, independently of any developer, governance vote, or third party. Where such withdrawal rights are encoded directly into the protocol and cannot be suspended or overridden by any actor, this constitutes strong positive evidence of absence of custody - regardless of whether the entity associated with the protocol is otherwise identifiable. The presence of a mechanism allowing an identifiable party to dispose of user assets, or to redirect them for its own benefit, without the user's participation should weigh heavily in favour of finding custody. Three categories are distinct and are not custody: compliance controls held by a regulated issuer over its own token (pause, freeze, allowlisting, court-ordered transfers), which are issuer obligations under MiCA Titles III and IV or sectoral law; controls a user configures over its own wallet; and the technology that enforces those controls on the user's or issuer's instruction.

5. DeFi protocol code is not open source (score: 3)

We disagree with the inclusion of this criterion as a formal indicator of centralisation. Even if proprietary code involves centralisation, open-source code is a good practical risk factor but does not mean decentralisation.

Open-source code is a transparency mechanism. It enables independent security audits, allows users and researchers to verify protocol behaviour, and reduces the information asymmetry between development teams and end-users. An asymmetry that is precisely one of the risks MiCA seeks to address.

This is consistent with how the industry itself treats open-source code: it is presented as a structural risk mitigant, on the same footing as permissionless access and immutability, precisely because it reduces counterparty risk, eliminates single points of failure, and enables independent security audits and public verification of protocol behaviour; not because it says anything about who controls the protocol. Whether code is open-source and whether an identifiable entity controls the protocol are two entirely independent questions: a protocol can be fully open-source and still be tightly controlled through admin keys. Conflating the two risks penalising exactly the transparency practices MiCA should want to encourage.

Therefore, we recommend that this criterion be removed from the decentralisation assessment entirely, and that open-source publication instead be encouraged as a voluntary disclosure standard within any market label or registry framework the Commission may develop. The absence of published code can still weigh as a practical risk factor warranting closer scrutiny from supervisors and integrators. However, we recognise it does point to a different kind of vulnerability because unverifiable code forces users to place trust in an identifiable operator rather than in behaviour they can independently check, which is a meaningful signal even if it does not establish that this operator exercises control.

6. Marketing of a DeFi protocol by an identifiable entity (score: 1)

We strongly disagree with the inclusion of this criterion. Treating the marketing of a protocol by an identifiable entity as an indicator of the absence of decentralisation is not only analytically unsound but is counterproductive from a policy standpoint. The teams that communicate publicly about their protocols, publish technical documentation, maintain developer forums and engage with regulators are precisely the teams that have chosen transparency over anonymity. As a result, if marketing activity becomes a factor that brings a protocol closer to MiCA qualification, the regulatory framework will create a structural premium on anonymity. Projects seeking to avoid any regulatory characterisation will have every incentive to disappear behind pseudonyms and to minimise all public communication. This outcome is the exact opposite of what the Commission should want to achieve. In addition, the legal foundation for this criterion is weak. Marketing does not create a contractual relationship between the marketing entity and the users of the protocol. A CASP under MiCA is an entity that provides a service to a client pursuant to an identifiable legal relationship. The act of communicating about a protocol (however prominent and however commercial) does not constitute the provision of a crypto-asset service and does not bring the communicating entity within the scope of MiCA. The criterion confuses visibility with control, and association with responsibility.

This position is also consistent with the *"control or sufficient influence"* test that underlies much of the indicator-based thinking on this topic (including in the FATF context), which is clear that marketing terms and self-identification are not determinative of whether an owner or operator exists. In practice, an entity closely associated with, and vocal about, a given protocol may nonetheless have no ability whatsoever to alter its core code while hundreds of independent, unaffiliated wallets and interfaces may communicate about the very same protocol without any of them controlling it. If marketing were treated as an indicator, all of these communications would count against the protocol's decentralisation, a result that reflects who talks about a protocol, not who controls it. The same distortion arises where a regulated CASP markets a product built on top of an immutable, non-custodial protocol: the CASP's commercial communication about that product has no bearing whatsoever on whether it, or anyone else, has any control over the underlying protocol.

Adan recommends that this criterion be removed entirely from any decentralisation assessment framework. Where relevant, marketing activity may be considered as one element of a broader factual analysis aimed at

identifying whether an entity exercises effective operational control over a protocol but it cannot, under any circumstances, be treated as a standalone indicator of centralisation.

Question 62. Do you believe that risks to users of fully decentralised DeFi protocols should be indirectly accounted for by MiCA, e.g. by requiring CASPs to conduct due diligence over DeFi protocols they connect their clients with, or in any other way?

- ☒ Yes
☐ No

Regarding *Questions 62 and 62.1*, the due diligence required from CASPs interacting with DeFi protocols must strictly remain an obligation of means to prevent an unsustainable operational burden. In practice, CASPs already systematically conduct some form of due diligence on the DeFi protocols they connect their clients to, even absent a specific MiCA requirement to do so, in order to protect their own clients and reputation. This confirms that a lightweight, fact-based obligation of means (and not a rigid, prescriptive technical assessment) is both workable and consistent with existing market practice. Indeed, the depth and scope of review naturally varies with the circumstances of each protocol and the framework should formalise and harmonise this existing practice instead of a standardised technical certification that market participants do not currently perform. The framework should focus on a practical technical and informational assessment, without mandating comprehensive code audits or holding platforms liable for smart contract vulnerabilities.

Therefore, this framework should rely on two balanced points:

1. **Standard technical checks:** gathering and disclosing objective, publicly available facts about the protocol, including its audit status, if any, alongside explicit risk disclosures to users.
2. **Targeted compliance monitoring:** leveraging standard blockchain analytics tools to identify and restrict interactions with protocols heavily exposed to criminal financial flows.

On the first point, we would recommend that "*standard technical checks*" be given concrete, verifiable content rather than left as a general principle, so that the obligation remains an obligation of means and does not drift into a de facto technical guarantee. In practice, this could take the form of a defined, non-exhaustive set of objective, publicly verifiable data points that a CASP would be expected to gather and disclose before connecting clients to a given protocol: whether the protocol's code has been independently audited, by which firm, and whether the audit report is publicly available; whether the code is open-source; whether the code is immutable or upgradeable and, if upgradeable, under what governance conditions and with what safeguards (e.g. timelocks, multi-signature requirements); and whether clear, accessible documentation of the protocol's rules and risks exists. Framing the obligation around this kind of factual, verifiable checklist (rather than around a substantive assessment of the protocol's technical soundness) keeps the exercise proportionate and achievable, since a CASP would be reporting on the existence and content of publicly available information rather than certifying the protocol's safety itself.

Consistent with the proportionality principle Adan has advocated for CASP prudential requirements more broadly (*see our response to Question 49 of the Consultation*), this due diligence obligation should also be calibrated to the size and risk profile of the CASP. A smaller CASP connecting clients to a limited number of DeFi protocols should not be expected to maintain the same depth of ongoing monitoring infrastructure as a large CASP integrating dozens of protocols across multiple asset classes. We therefore consider a uniform due diligence checklist risks becoming disproportionately burdensome for smaller market participants relative to the actual risk they introduce, undermining the same objective of avoiding unjustified compliance costs that Adan has consistently defended throughout this consultation.

Any CASP due diligence requirement should remain proportionate and risk-based. It should focus on information reasonably available to the CASP, such as public audits, disclosures, known exploits, sanctions exposure and blockchain analytics indicators. **It should not require CASPs to guarantee the correctness of smart contracts, the conduct of independent protocol participants or the outcome of decentralised settlement mechanisms.**

Question 62.1. Please specify how should MiCA account for risks from fully decentralised DeFi applications.

[échelle 1-5 : Strongly disagree → Strongly agree]

	1	2	3	4	5
CASPs should be able to connect their clients to any decentralised DeFi application, subject to giving appropriate warnings and disclosures on risks					■
CASPs should be liable for certain types of incidents when they have provided access to the relevant DeFi application and clients have been affected		■			
CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service global (permissionless) liquidity	■				
CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service only verified liquidity (verified pools)	■				
CASPs should only facilitate connection of their clients to decentralised DeFi applications that service global liquidity					■
CASPs should be required to discontinue or discourage connecting clients to DeFi protocols that are strongly associated with illicit activity based on blockchain analytics					■
CASPs should not facilitate connection to decentralised DeFi applications	■				
Public bodies should be required, or private organisations incentivised to publish whitelists or blacklists of DeFi protocols based on their risk profile			■		
Other:					

Please explain your responses, including your reasoning and any suggestions for improvement, recalibration, or alternative approaches.

- **CASPs should be able to connect their clients to any decentralised DeFi application, subject to giving appropriate warnings and disclosures on risks (score: 5)**
 - Justification: we scored '5'. We consider this is the right anchor point, since it places responsibility on what the CASP actually does (own due diligence and own client disclosures) instead of asking a protocol it doesn't control to somehow comply.

- **CASPs should be liable for certain types of incidents when they have provided access to the relevant DeFi application and clients have been affected (score: 2)**
 - Justification: we scored '2'. A CASP should answer for failures of its own making (for example: misleading disclosures or weak due diligence), but holding it liable for a smart contract exploit or an oracle failure it neither built nor controls turns it into a guarantor of infrastructure it has no power over.
- **CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service global (permissionless) liquidity (score: 1)**
 - Justification: we scored '1'. We would not make access conditional on certification at this stage. As stated above, the EU certification market lacks the accreditation framework and capacity to absorb this without pricing out smaller protocols and locking in a handful incumbent auditors.
- **CASPs should only facilitate connection of their clients to decentralised DeFi applications that are certified and service only verified liquidity (verified pools) (score: 1)**
 - Justification: we scored '1'. This goes a step further and would cut EU users off from most of global onchain liquidity since the majority of it sits in permissionless pools. We consider this is not a safer solution for users.
- **CASPs should only facilitate connection of their clients to decentralised DeFi applications that service global liquidity (score: 5)**
 - Justification: we scored '5'. Onchain liquidity has no jurisdiction and a pool cannot be labelled "EU" or "non-EU" and this holds even for applications with their own access controls, since they still draw on the same underlying global pool. Then, we acknowledge that EU-liquidity restriction Adan supported in its response to *Question 56 (Part 3)* concerns CASP connectivity to identifiable, centralised third-country venues where routing choices are technically discretionary. It does not extend to permissionless DeFi liquidity pools, which are inherently borderless and cannot be segmented by jurisdiction at the protocol level. Access to such pools should instead be governed by the disclosure and due diligence safeguards set out below. Compliance controls belong at the asset or application layer, never at the protocol layer, which should remain generic and permissionless. For DLT financial instruments, eligibility is enforced at the level of the instrument itself, as securities law requires, without fragmenting liquidity at the base.
- **CASPs should be required to discontinue or discourage connecting clients to DeFi protocols that are strongly associated with illicit activity based on blockchain analytics (score: 5)**
 - Justification: we scored '5' as we support this in principle (and note that analytics-based screening is already standard CASP practice).
- **CASPs should not facilitate connection to decentralised DeFi applications (score: 1)**
 - Justification: we scored '1' with a warning here. Indeed, this would simply drive EU users towards unregulated channels to reach the same infrastructure.
- **Public bodies should be required, or private organisations incentivised to publish whitelists or blacklists of DeFi protocols based on their risk profile (score: 3)**
 - Justification: we scored '3'. Risk information here is useful only as one input into the CASP's own assessment (and not as a substitute for it). However, we consider official lists raise problems because they go stale quickly, notably in this market, and may create liability questions when they get it wrong.

Question 63. Do you support introducing certification schemes for DeFi protocols and smart contracts?

- ☐ Yes, for all DeFi protocols and smart contracts providing any of the crypto-assets services defined under MiCA, and possibly also other services not in MiCA's scope such as lending and borrowing

- ☐ Yes for the DeFi protocols and smart contracts providing some of the crypto-assets services defined under MiCA
- ☒ No

In case you support introducing certification schemes for only certain types of DeFi services, please explain which ones and for what reasons.

We don't support introducing certification schemes for DeFi protocols and smart contracts, for the following reasons:

- (i) DeFi operates in a global and cross-border environment. A mandatory European certification scheme would be easily circumvented by protocols deployed from third-countries, with the result that EU users would continue to access them, but through channels outside the EU regulatory perimeter;
- (ii) smart contracts evolve continuously and operate within complex dependency structures. As a consequence, *ex ante* certification is technically impracticable, as it would introduce delays incompatible with security requirements, particularly the need to rapidly remediate vulnerabilities;
- (iii) the ecosystem already benefits from effective mechanisms (e.g., independent audits, bug bounty programs, market discipline etc.) which address risks in a proportionate manner.
- (iv) a mandatory regime presupposes prerequisites the EU does not currently have (an accreditation framework and sufficient certification capacity) while the leading audit firms remain predominantly US-based. Imposing a mandatory scheme in these conditions would risk creating competitive distortion and entrenching existing incumbents, despite allowing a genuine European certification capacity to emerge.

We favor an approach based on voluntary standards defined by market participants, which promotes transparency and self-regulation. Certification should function primarily as a market signal (a certified protocol being more readily integrated by regulated entities) and not as a regulatory precondition. Any such scheme should apply at the codebase level and be calibrated to the size and maturity of the protocol concerned. Finally, protocols that are open-source, technically decentralised and fully transparent should not require certification at all, as their behaviour remains permanently verifiable by any interested party.

Question 64. Which of the following statements about potential certification schemes of DeFi protocols do you agree with?

[échelle 1-5 : Strongly disagree → Strongly agree]

	1	2	3	4	5
Instead of a full CASP licence, DeFi protocols that are not fully decentralised should be required to obtain a certification before or soon after making the protocol available to the public	☒				
To obtain their certificate, DeFi protocols that are not fully decentralised should be required to integrate specific compliance tools in the design of their protocols	☒				
DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be required to obtain a certificate before making these wallets available to the public	☒				

DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be incentivised to obtain a certificate

--	--	--	--	--

Please explain your responses.

As a preliminary observation, we consider that *Question 64* rests on a false binary that runs through the entire 4.1 section: the implicit premise is that a DeFi protocol which is not "*fully decentralised*" must necessarily fall into one of two boxes - a full CASP licence, which is a framework designed for and calibrated to legal entities providing services within a contractual relationship, not for autonomous software; or an ex ante certification regime. This framing forecloses the more accurate and workable question, which is not "*how centralised is this protocol*" but "*is there an identifiable entity exercising discretionary control over user assets, instructions, or settlement outcomes, and does that entity provide a MiCA-defined service.*" Where the answer is no, neither a CASP licence nor a certification obligation has a coherent addressee.

On the first item certification instead of a full CASP licence, we strongly disagree. We do not consider certification to be the appropriate tool either and as explained under *Question 63* (see above), we do not support the introduction of certification schemes for DeFi protocols in general. A full CASP licence is not the answer for these protocols either and for the same underlying reason. Indeed, if an entity actually controls the protocol and the assets running through it, it already falls under MiCA so no new category is needed. If no entity holds that kind of control, then there's simply nobody to hand a licence.

On the second item, we strongly disagree, and consider this the most problematic proposition in the list. Requiring a DeFi protocol to integrate specific compliance tools into its design as a condition for certification misunderstands both the architecture of these protocols and the nature of the risk it seeks to address, for several converging reasons:

Where a protocol's core code is immutable by design (a deliberate and legitimate architectural choice, not a regulatory gap) compliance logic embedded at deployment cannot subsequently be corrected, updated, or adapted as regulatory requirements evolve. An immutable protocol carrying hard-coded compliance logic is, by definition, unable to track regulatory change. This effectively forces one of two outcomes, both of which are harmful. Either the protocol must be made upgradeable purely to accommodate future compliance requirements, which reintroduces exactly the centralisation and governance risk that immutability was designed to eliminate; or the protocol must be redeployed in its entirety each time a regulatory requirement changes, which destroys continuity of service for existing users and materially increases development costs and fragmentation. From a security view now, every additional line of code embedded in a smart contract constitutes an additional attack surface. Historically, the most damaging DeFi exploits have targeted unanticipated complexity in deployed code; mandating the integration of compliance modules directly into protocol logic would systematically expand that surface, for a category of risk (regulatory compliance) that a smart contract is not designed to manage. This stands in direct contrast to compliance logic implemented at the application or integration layer (e.g. by a CASP, wallet provider, or front-end operator), which can be updated, replaced, or reconfigured independently of the underlying protocol, without compromising its security properties or requiring any redeployment of the immutable code itself.

For these reasons, we recommend that any compliance-related obligation be located exclusively at the layer where it can actually be maintained and adapted over time (the commercial, user-facing layer) **rather than embedded irreversibly into protocol code.**

On the third and fourth items, concerning non-custodial wallets, we draw a clear distinction between a mandatory and an incentivised approach. We strongly disagree that developers offering non-custodial wallet software should be required to obtain a certificate before making that software available to the public. A non-custodial wallet, by construction, does not involve the developer exercising custody or discretionary control over user assets; publishing such software is not the provision of a crypto-asset service. This is consistent with the carve-out for non-custodial services that we support in our response to *Question 46*. Creating it as such would capture a broad range of general-purpose software tools (including those built using freely available, generic development tools) on the basis of their potential use rather than any service actually rendered. Such a requirement would function as a de facto

barrier to entry for open-source development in the EU, with no corresponding reduction in risk, since non-custodial wallets deployed outside the Union would remain freely accessible to EU users.

We support incentivising (rather than requiring) certification for non-custodial wallet software, provided this operates as a genuinely voluntary market label - for instance, evidencing that the wallet's code is open-source, has been independently audited, provides clear documentation of its security model, and that recognises existing independent audits and information-security certifications rather than requiring a new bespoke process; rather than as a *de facto* precondition for market access. We would caution, however, that even a voluntary scheme should be designed so as not to create an implicit two-tier market that disadvantages non-certified but otherwise secure and transparent software.

Question 65. Which of the following statements about potential certification schemes of DeFi protocols or smart contracts do you agree with?

[échelle 1-5 : Strongly disagree → Strongly agree]

	1	2	3	4	5
Certificates should be issued by qualified private sector entities			■		
Certificates should be issued by qualified public sector entities			■		
Any interested party (e.g. persons providing connectivity to or participating in governance of DeFi protocols) should have the possibility to ask for the certification of a fully decentralised DeFi protocol		■			
Only fully decentralised DeFi protocols that reach a certain significance (e.g. based on total value locked) should be required to obtain a certificate		■			
CASPs should not be allowed to connect clients with DeFi protocols that are not certified		■			

Please explain your responses.

As explained above, Adan does not agree about introducing certification schemes. However, we consider the following:

- **Certificates should be issued by qualified private sector entities / Certificates should be issued by qualified public sector entities**
 - Justification: smart contracts are published daily in large volumes and require frequent updates to fix vulnerabilities and public authorities are built to certify static software and not highly dynamic open-source code. For now, public bodies lack the capacity to manage this flow without clogging the system. Specialized private sector auditors possess the necessary technical agility, speed, and expertise. However, the leading smart contract audit firms today are predominantly US-based, so relying primarily on private certification would not resolve the underlying question of European capacity and sovereignty in this field. It would simply shift dependency from public bodies to a small number of foreign private actors. We are not opposed in principle to either model but at this

stage neither is fully satisfactory because on the one hand private certification currently means relying on non-UE firms and on the other hand public certification would require accreditation capacity the EU does not yet have.

- **Any interested party (e.g., persons providing connectivity to or participating in governance of DeFi protocols) should have the possibility to ask for the certification of a fully decentralised DeFi protocol**
 - Justification: we are not favourable to this statement, as it can lead to detrimental side effects or abuses: **(i)** certification scopes defined unilaterally by a requester with no relationship to the protocol; **(ii)** potential conflicts of interest (nothing prevents a competitor from requesting certification hoping for adverse findings); and **(iii)** divergent outcomes where multiple parties certify the same codebase with different certifiers, creating confusion rather than trust. For this reason, should this solution be introduced, three safeguards are indispensable:
 - requesting or facilitating certification must never be construed as evidence of control or influence over the protocol;
 - a third-party request must impose no obligation on developers or associated entities to participate in, respond to, or fund the process as long as certification remains voluntary; and
 - the absence of certification must not restrict any party's ability to use or integrate the protocol.
- **Only fully decentralised DeFi protocols that reach a certain significance (e.g. based on total value locked) should be required to obtain a certificate**
 - Justification: we share the view that certification should scale with how much is actually at stake for users and not applying uniformly regardless of a protocol's size or maturity; younger or lower-usage projects shouldn't face compliance costs that could effectively shut them out of the market. Where we'd push back is on TVL as a metric for drawing that line. In fact, it moves with market prices and liquidity flows alone, so a protocol's regulatory status could change from one week to the next without anything about its actual risk profile changing. That is one of the reasons the UE efforts should encourage a voluntary market label or registry managed by the industry. It would achieve the same proportionality goal without this instability. The statement nevertheless presupposes that a fully decentralised protocol can be "required" to do something. It cannot: an obligation needs an obligor, and where no person controls the protocol there is no one on whom the requirement can lawfully be imposed. Any such requirement can only address identifiable persons that voluntarily seek certification, or the CASPs that integrate the protocol.
- **CASPs should not be allowed to connect clients with DeFi protocols that are not certified**
 - Justification: this prohibition would operate as a *de facto* ban on innovation and isolate the European ecosystem. DeFi protocols are deployed globally, and a European certification scheme cannot bind those deployed from third countries (see *our response to Question 63*). A strict certification requirement would simply force European developers to relocate and push retail investors toward unregulated foreign platforms. Regulated CASPs should only be required to perform voluntary technical due diligence with disclosures obligations and verify that protocols respect recognised market labels.

ON STAKING, LENDING AND BORROWING OF CRYPTO-ASSETS (4.2)

This section seeks stakeholders' feedback on staking, lending and borrowing of crypto-assets, currently not addressed in MiCA regulation. Staking is the process of immobilising crypto-assets to support the operations of proof-of-stake and proof-of-stake-like blockchain consensus mechanisms in exchange for the granting of validator privileges that can generate block rewards.

The provision of staking services often implies that the crypto-assets, or the private keys giving access to them, are held by the staking service provider in custody. Thus, the provision of staking services is ancillary to custody services which are fully covered under MiCA. The provision of staking services therefore requires that the staking service provider is authorised under MiCA to provide custody and administration of crypto-assets on behalf of

clients, as set out in Article 75 MiCA. Furthermore, CASPs should obtain an explicit consent from the clients to stake their crypto-assets, as it may have an impact on their clients' ability to access them.

Respondents are asked to provide concrete examples to support answers provided, and, where possible, quantitative and qualitative information.

Question 66. Do you think the current approach whereby staking services are not separately regulated is adequate? If not, what specific requirements should be applied to staking service providers?

- ☒ Yes
☐ No

We consider the current approach whereby staking services are not subject to a separate regulatory regime to be broadly adequate.

Staking is fundamentally a technological operation that contributes to the security and functionality of a blockchain network. It involves participants locking their assets to validate transactions and maintain the integrity of the network. In order to identify the appropriate regulatory standards, it is paramount to first acknowledge the distinction between the technological activity of staking and a financial service. Staking is a technical function to secure a network; incomes are merely a byproduct of that function. Understanding this distinction is vital for regulatory purposes: while staking is essentially a blockchain security function, some business models offer delegation of its technical aspects as a service ancillary to financial services.

We should therefore distinguish between two dimensions: **A)** custody and administration of crypto-assets, and **B)** staking from a technological point of view.

A) Custody and administration of crypto-assets. Delegated staking - where users delegate their staking rights to a validator node without having to run the validator software themselves - can involve, but not in all cases, custody of crypto-assets by a third party. When staking is ancillary to custody and administration of crypto-assets services, it falls under the scope of the relevant regulations. Custodial staking services are typically provided by crypto-asset exchanges or custodial wallet providers: users deposit their coins with the service and the provider stakes on their behalf. Such custodial services that facilitate delegated staking may involve a contractual relationship between the provider and the delegator, which is governed by MiCA - subjecting the provider not only to the specific requirements of the service but also to prudential and liability rules that provide extra protection for users in cases of misconduct or of external criminal behaviour. This is not merely a matter of principle: the prudential safeguards under Article 67 and the liability provisions under Article 75(8) of MiCA already apply directly to custodial staking providers, ensuring minimum capital requirements and clear liability standards in the event of misconduct related to asset custody. By mandating adequate own funds and establishing clear liability standards, MiCA protects clients' interests and fosters a more secure and trustworthy environment, ultimately benefiting all participants involved. In practice, this means that if the custodian providing staking services fails to uphold its responsibilities, it can be held liable for any resulting damages in cases of misconduct related to asset custody, while users are also afforded protection against the criminal actions of external third parties.

As a consequence, a significant part of the governance and conduct-related risks associated with staking activities is already addressed through the existing regulatory framework.

B) Non-custodial staking. Unlike custodial services, non-custodial staking services do not take possession of users' tokens. They provide software that enables users to stake directly from their self-hosted wallets; the service has no access to user assets and merely facilitates the staking process. The same applies to technology providers whose software enables a CASP or an end-user to stake without the provider itself being able to transfer or dispose of the assets. They are neither custodians nor custodial staking service providers and the authorised CASP or the self-custodying user remains the responsible party. Policymakers should differentiate between custody services and the purely technical process of staking, and

non-custodial services should be excluded from regulatory oversight. It is paramount not to conflate the risks posed by primary activities such as custody with those of ancillary, non-custodial staking services.

Staking should not be analysed through the same lens as financial intermediation. While it may generate economic incomes for participants, it remains a blockchain-based activity whose risk profile differs fundamentally from activities involving credit creation or counterparty exposure. Unlike lending arrangements, staking generally does not involve transferring crypto-assets to a borrower for onward use. In most cases, crypto-assets remain dedicated to protocol-level functions and are primarily exposed to the operational rules of the underlying network rather than to the creditworthiness of a counterparty. Furthermore, to date, no evidence has been provided demonstrating that the current framework has resulted in widespread consumer harm, market dysfunction or regulatory gaps requiring the creation of a dedicated staking regime.

The diversity of staking models must be recognised. The notion of “*staking*” covers a wide range of arrangements that can differ significantly (self-custodial staking, delegated staking, custodial staking, liquid staking and more recent restaking models) which do not involve the same actors, operational structures or risk profiles. Any attempt to define staking as a single homogeneous regulatory category would therefore fail to reflect the diversity of existing, and future, models. A clear line must be drawn between native protocol staking and more complex market designs such as liquid staking or restaking. Native staking, where users operate their own nodes or delegate directly to validators, carries purely network-level operational risk, such as slashing or downtime. Liquid staking and restaking, by contrast, introduce distinct layers of smart contract dependency, potential agent risk and programmatic risk duplication. In a liquid staking setup, users transfer their assets to a third-party smart contract infrastructure in exchange for a liquid token derivative, creating a specific technical vulnerability vector. On the restaking side, restaking pool architectures stack multiple programmatic security layers, meaning that a single smart contract exploit or a cascading slashing event at the middleware layer can affect the underlying principal.

Existing adjacent EU legislation further reduces the case for a bespoke regime. In addition to the requirements already mandated by MiCA, market participants are also implementing practices to offer additional protection and confidence to users - for example, insurance covering certain risks to themselves and their stakeholders. Beyond such voluntary market practices, staking service providers are already subject to cybersecurity and operational resilience standards under three important pieces of EU legislation: the Digital Operational Resilience Act (DORA), the Cyber-Resilience Act, and the Product Liability Directive. This existing body of adjacent regulation further reduces the case for introducing a bespoke staking regime under MiCA.

In our view, greater value would therefore be achieved through targeted clarification of existing MiCA requirements, where necessary, rather than through the introduction of a new regulatory category dedicated to staking services. Existing regulatory standards already applying to the ecosystem must be taken into consideration to avoid over-regulation, disproportionality, and the imposition of hurdles that would slow the emergence of innovative projects and could harm the competitiveness of the market.

Our recommendations are accordingly the following:

- Staking should be recognized as a technological activity and not a financial service.
- Policymakers should differentiate between custody services and the technical process of staking. Non-custodial services should be excluded from regulatory oversight.
- It is paramount not to conflate risks posed by primary activities (eg custody) with ancillary staking services.
- A bespoke staking framework is not required. We encourage policymakers to look at existing requirements and how these can be leveraged to mitigate risks posed as appropriate. Existing regulatory standards already applying to the ecosystem must be taken into consideration to avoid over-regulation, disproportionality, and hurdles imposition which would slow down the nascence of innovative projects and could harm the competitiveness of the market.
- Reinforce existing MiCA requirements on explicit client consent for staking activities;
- Emphasise proportionality and the absence of demonstrated need for additional regulation of staking services.

Question 67. Do you think that lending and borrowing of crypto-assets should be regulated? If "Yes", what do you believe should be the main elements of regulatory requirements applicable to lending and borrowing and why?

- ☐ Yes
☒ No

We do not support the regulation of lending and borrowing of crypto-assets through a new, dedicated regime.

We consider first a clarification of terms is necessary. The use or deployment of client assets does not, necessarily, amount to lending or borrowing when the assets remain attributable to the client and the arrangement does not create a debtor-creditor relationship between the parties. This is the case, for instance, of a custodian deploying assets on the client's instruction, with the client's explicit consent, under the segregation requirements set up in MiCA. In that scenario, the client keeps ownership of the assets throughout, and no debtor-creditor relationship ever arises. Lending in the proper sense exists only where a provider becomes a counterparty, either by lending its own assets or by taking ownership of the client's assets against a promise to return them with yield. The relevant question, in every case, is who takes ownership of the assets and who, if anyone, promises their restitution.

- Where that counterparty relationship genuinely exists, the corresponding safeguards already attach. Providers of client-facing lending and earn products in the EU are, in most cases, already authorised as crypto-asset service providers (CASPs), credit institutions or e-money institutions (EMIs), subject to governance, conduct, custody and anti-money laundering and countering the financing of terrorism (AML/CFT) requirements. A dedicated regime would duplicate what already applies as soon as an identifiable entity bears the risk.
- Crypto-asset lending should not be treated as equivalent to deposit-taking in the traditional banking sense, and importing the corresponding capital and liquidity requirements would not be appropriate either. The useful step now is to clarify, through European Supervisory Authorities (ESA) guidance or a Commission clarification rather than a new authorisation category, the disclosures these entities should give their clients on terms and risks, and the due diligence expected of them when they give access to DeFi lending protocols, as set out in our response to *Question 62*.

Also, we raise your attention that direct, non-custodial use raises no intermediation risk. Positions sit on a public ledger, liquidations run automatically under rules identical for every participant, no balance sheet exists on which assets could be concealed or reused, and no operator holds discretion over user funds. Applying rules built for financial institutions to an immutable protocol would have no addressee, since no entity can hold an authorisation or comply with obligations on anyone's behalf. Consistent with the control-based approach of the Financial Action Task Force (FATF) Targeted Report on Regulatory Challenges from Decentralised Finance (21 July 2026), any framework should confirm that immutable protocols, open-source code, non-custodial interfaces and wallets, and users acting for their own account are not service providers. EU crypto-asset lending remains marginal, and the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) found no current threat to financial stability in their Joint Report on recent developments in crypto-assets (January 2025). Onchain lending represents around 0.08% of euro-area bank lending to households. Legislating now would also mean fixing definitions in a market whose product structures are still moving. For these reasons, and to avoid a unilateral compliance burden that would displace activity rather than protect EU clients, any European initiative on this topic should proceed in step with, not ahead of, the equivalent international workstreams.

ON NON-FUNGIBLES TOKENS (4.3)

Under MiCA Article 2(3), crypto-assets that are unique and not fungible with other crypto-assets (NFTs) are out of the scope of the regulation.

Question 68. In your view, does the current state of the NFT market and the risks and opportunities associated with it justify regulating providers of services related to these tokens?

- ☐ Yes
☒ No

If your reply is positive, what do you believe should be the main elements of regulatory requirements applicable to NFTs?

Prediction markets and perpetual futures

One of the most marked developments in crypto markets since MiCA was adopted is the emergence of DLT-based prediction markets and the volume of trading activity in perpetual futures on crypto-assets. Prediction markets where parties take a bet on a future development in almost any area, often far removed from financial assets or services, are increasingly conducted on or are structured through DLT, smart contracts and crypto-assets.

Question 69. Do prediction markets present opportunities or risks for EU consumer and investors? If so, please elaborate.

- ☒ Yes
☐ No

Prediction markets are peer-to-peer derivative marketplaces that generate valuable data through accurate forecasts of future events. They therefore present unique opportunities for EU consumers and investors, both by providing valuable predictive insights and by enabling innovative trading strategies. It is worth noting that they are legally not defined, but rather understood as a broad label encompassing a range of different market structures. For this reason, we support the clarification of their regulatory treatment to provide greater legal certainty and legal harmonization and convergence among EU Member States, to enhance consumer confidence, and to facilitate the development of a well-functioning EU market for these products.

We believe in expanding access to the financial tools that help people manage their economic futures. We are now seeing a significant evolution in this space through event contracts. These contracts can reference a wide range of real-world events, including - but not limited to - economic indicators, weather, and geopolitical developments. These markets are tools for price discovery and risk management. They aggregate decentralized information into clear market signals, allowing users to hedge against and take views on real-world outcomes that impact their financial lives. At the same time, the pricing for these contracts creates a valuable source of predictive data that will benefit investors, business owners, consumers, economists, policymakers and scientists. Importantly, these products are not novel from a regulatory perspective - we note that these are currently categorized as "swaps" in the United States and available to retail traders when offered on a registered exchange.

As illustrated in the chart below, modern, exchange-traded event contracts should not be mischaracterised as equivalent to the flawed binary options model.

Overview of differences between binary options and event contracts

Feature	Binary Option (Banned)	Regulated Event Contract (Proposed)
Pricing	Fixed, issuer-set odds at inception.	Market-priced and tradable based on supply/demand dynamics.
Trading	Offeror is counterparty. Customer often forced hold-to-expiry; limited secondary market.	Exchange-traded, counterparty is another market participant. Highly liquid and tradable (price movement drives P&L).
Risk/Settlement	All-or-nothing payout; high counterparty risk (OTC).	Centrally cleared (mitigating counterparty risk); P&L is based on price fluctuations, coupon payment, not solely final outcome.

The EC should therefore seek to bring this activity within the regulated perimeter through a framework that protects consumers, supports market integrity, and allows legitimate use cases to develop. We would welcome further clarity from the EC on the scope of MiCA and MiFID as they apply to event contracts, particularly following [ESMA's recent public statement](#).

Question 70. Should prediction markets, where they are DLT enabled and facilitated through smart contracts be governed by MiFID or MiCA?

- ☒ By MiFID
- ☐ By MiCA

The applicable framework should depend on the economic function and legal characteristics of the product, consistent with the principles of technology neutrality and "*same activity, same risk, same regulation*." The fact that a prediction market is enabled by DLT or operated through smart contracts should not, in itself, warrant its inclusion within the scope of MiCA. MiCA should not serve as a substitute regulatory framework for products that are functionally equivalent to instruments or services already governed by the broader financial services acquis. The appropriate regulatory approach should instead be determined by the rights and obligations attached to the product, as well as its economic and market function.

Where a prediction market contract qualifies as a financial instrument- such as a derivative- it should remain subject to MiFID II, rather than MiCA. This is consistent with ESMA's July 2026 [public statement](#), which reaffirms that MiFID authorisation is required for the provision of investment services relating to event contracts that meet the definition of derivatives, irrespective of whether such services are provided to retail or non-retail clients.

Where a DLT-based prediction market does not fall within the scope of MiFID, this should give rise to a separate legal and regulatory assessment. It should not, however, result in MiCA becoming the default framework for such arrangements simply by virtue of their use of DLT or smart contracts.

Question 71. What substantive requirements should be considered for service providers that provide prediction market services?

We agree to set up a framework that protects consumers, supports market integrity, and allows legitimate use cases to develop. The way these products are structured, they perform functions comparable to futures and other derivative instruments and should be treated accordingly. This is also broadly the approach taken in the United States, where comparable products are generally regulated as derivatives. From a practical standpoint, there is value in maintaining regulatory convergence between the EU and the US. In this regard, we advocate for tokenised prediction markets to fall under MiFID II, in line with ESMA's recent [public statement](#).

However we do not agree with the manner in which the ESMA statement addresses all prediction markets, as labels them all under a singular category failing to recognise all the range of products offered, and thus their substantive characteristics and risks associated, which merit a different regulatory treatment. It is key to distinguish between different types of prediction markets. The fact that a contract relates to an event with a binary outcome does not, in itself, mean that it is equivalent to a binary option for regulatory purposes. Treating all event contracts as binary options risks overlooking material differences in how such products are structured, traded and settled, and consequently in the risks they present to participants.

The regulatory concerns that have historically underpinned restrictions on binary options include, among others, consumer protection, transparency, fairness, conflicts of interest and conduct risks. These can be particularly pronounced where a provider acts as principal and counterparty to its customers, potentially has an information advantage over them, provides leverage, and stands to profit from customer losses. Traditional binary options are also generally not transferable before expiry and typically provide a predetermined payout or no payout depending on the outcome of the underlying event. By contrast, certain prediction-market contracts may have materially different characteristics: where a platform does not act as counterparty or take proprietary positions against its users, the potential for conflicts of interest arising from the provider's exposure to customer losses is reduced.

Where participants trade positions with one another and can buy or sell those positions before the relevant event is resolved, participants are able to manage or exit their exposure prior to settlement rather than being required to hold the position until expiry. The value of a position may also fluctuate with market expectations, allowing participants to realise variable gains or losses before the event is resolved, rather than receiving only a predetermined payment or nothing at expiry.

Furthermore, where such contracts are not leveraged, a participant's maximum loss is generally limited to the amount initially committed. These characteristics can materially alter the risk profile of an event contract and distinguish it from the type of binary option that has been subject to restrictive regulatory measures. **Accordingly, whether an event contract should be regarded as presenting the risks associated with binary options should be assessed by reference to its substantive characteristics and economic function, rather than solely by reference to the fact that the underlying event has a binary outcome.**

Having said that, we believe that MiFID II Annex I, Section C(10) already contemplates derivative contracts relating to non-financial underlyings. We therefore believe there is sufficient scope within the existing MiFID II framework for prediction markets to be accommodated, subject to appropriate clarification to ensure that the regulatory regime can account for different types of products, their respective risk profiles, and the corresponding consumer protection safeguards accordingly. For the reasons previously outlined, we consider that certain aspects of the MiFID framework governing derivative contracts generally, and CFDs and binary options in particular, were not designed with event contracts in mind and may therefore apply in ways that produce unintended consequences. Specifically, our recommended approach is to include event contracts explicitly within Annex I, Section C of MiFID as a standalone derivative, distinct from OTC binary options, as proposed below. This would preserve the retail ban for harmful product structures in which investors effectively bet against the issuer and are locked into odds set by that issuer. These changes could be supplemented with event-contract-specific limits, including strict restrictions on contracts linked to harmful events such as war, terrorism, and illegal activity, as well as on specific contracts that are particularly prone to market abuse. Likewise, it should also be taken into account that a MiCA license, compared to a MiFID one, does not preempt NCAs to potentially assert jurisdiction over a specific product. If that is the case, the platform cannot rely on its MiCA licence alone. It could also potentially need to comply with the applicable MiFID II requirements (and obtain the relevant authorisation).

In parallel, a relevant factor to look at from a regulatory standpoint, is whether a certain actor sets prices or not. There are certain products in which prices are fixed whereas this may not apply to prediction markets.

Question 72. Should perpetual futures on crypto-assets and services towards such perpetual futures be governed by MiCA or MiFID.

- ☒ Yes, by MiFID
- ☐ Yes, by MiCA
- ☐ No

Question 73. What substantive requirements should be considered for perpetual futures on crypto-assets and service providers providing service for such perpetual futures?

Equivalent requirement to derivatives under MiFID; the service provider should be regulated as an investment firm.

Perpetual futures on crypto-assets, and services relating to those products, should fall under MiFID rather than MiCA. Perpetual contracts referencing crypto-assets fall within Section C(10) of Annex I to MiFID II, which covers derivative contracts where the underlying is a crypto-asset, and should be classified and regulated accordingly.

Products that are, in substance, derivatives should not be brought within the scope of MiCA simply because they reference crypto-assets or are issued, traded or settled using DLT. Where a product has the characteristics of a derivative or another financial instrument, the "same activity, same rules" principle should apply, with the relevant sectoral legislation remaining the applicable regulatory framework.

Using MiCA as the sole regulatory framework in these circumstances would risk undermining legal certainty by

blurring the distinction between the regulation of crypto-assets and the regulation of financial instruments. The preferable approach is therefore to retain MiFID/MiFIR as the relevant framework for financial instruments, while further clarifying the boundary between the two regimes where needed.

On tokenised deposits

The terms ‘tokenised deposit’ and ‘deposit tokens’ are not defined terms and are sometimes used interchangeably.¹² For the purposes of the following questions, ‘tokenised deposits’ are digital representations of traditional commercial bank deposits recorded on a blockchain or distributed ledger, allowing for programmable, instant 24/7 settlements.

Question 74. Tokenised deposits could be deployed in support of a range of use cases across payments, capital markets, and on-chain financial activities. Based on your experience and expectations, please assess the potential relevance and benefit of tokenised deposits for each of the following use cases in the EU.

Scale used:

- 1 = Not relevant / no meaningful benefit
- 2 = Low relevance / limited benefit
- 3 = Moderate relevance / moderate benefit
- 4 = High relevance / high benefit
- 5 = Very high relevance / transformative benefit

Potential use case or benefit	1	2	3	4	5
Person to person payments					
Retail POI payments (domestic, day-to-day point of interaction transactions)					■
Intra-EU cross-border payments (non-POI)			■		
International payments and remittances (third countries)					■
Settlement of tokenised securities and other financial instruments					■
Delivery-versus-payment (DvP) and atomic settlement					■
Intraday liquidity management (real-time funding and liquidity optimisation)				■	
Treasury and liquidity management services for corporates and financial institutions				■	
Programmable payments and smart-contract-based use cases				■	
On-chain collateral or margining in regulated markets				■	
Improved settlement speed and operational efficiency				■	
Reduction of counterparty and settlement risk				■	

Question 75. Please select one or two use cases and benefits above that you consider most promising in the EU and explain why.

Adan did not answer this question.

Question 76. What factors, if any, constrain the development and uptake of tokenised deposits in the EU?

The factor that constrains the development and uptake of tokenized deposits in the EU is the lack of regulatory clarity. MiCA doesn't clearly address tokenised deposits (they may fall outside its scope as they're not "crypto-assets" but representations of bank deposits). It is thus unclear which rules apply: banking law, e-money rules, or securities law.

This lack of clarity translates concretely into the absence, to date, of any credit institution in the Union offering a standardised tokenised-deposit solution adapted to DLT market infrastructures. In the absence of such an offering, each infrastructure must negotiate a bespoke bilateral banking arrangement (segregated account, automated reconciliation between the bank balance and the DLT ledger) and obtain, case by case and from several authorities, validation of the legal qualification of the technical token representing those funds - exactly the type of uncertainty that constitutes today's main constraint. There's also uncertainty regarding its settlement finality: arising legal questions about when payments are final on-chain vs. traditional banking systems.

Also, there's a cross-border complexity embedded, due to different national implementations of EU banking rules; AML/KYC compliance across jurisdictions remains complex.

Tokenised deposits and central bank money should be designed to work together: wholesale settlement in central bank money, including through the Eurosystem's DLT settlement initiatives, is what allows deposit tokens from different banks to settle with finality.

The closed-loop design. For tokenised deposits, holders must be customers of that bank, and the deposit cannot circulate freely outside the issuing institution's network. Tokenized deposits remain tied to the issuing bank's balance sheet and operating perimeter. Beyond the issuing bank, they cannot circulate seamlessly without interbank coordination and reconciliation. Their broader use would require the creation of a dedicated interbank clearing and settlement infrastructure. Another factor is the Integration with existing payment systems, the need to work alongside SEPA, TARGET2, and other EU payment infrastructure.

Question 77. If you identify any regulatory issue(s) in your answer to the previous question, please indicate what regulatory action is appropriate to address the issue(s) identified.

The main question is about the legal characterization and certainty that the market needs to have. A legal definition is critical to ensure their development. In the event of a given regulatory definition, tokenized deposits must fall outside MiCA, as they are not EMTs, they represent a tokenised form of commercial bank deposit, not tokenised electronic money, so the clarification on this exclusion should be expressly stated. A clarification should also distinguish between Tokenized deposits (a digital, account-based representation of an existing commercial bank deposit) and deposits tokens (token-based instruments whose legal nature, transferability and settlement arrangements may differ materially). There are also nuances between deposit tokens and tokenized deposits whereas you can say one corresponds to an account base while the other is a token base instrument so the consequences can be really different.

Clarifications should also outline in particular the transferability of the instrument: where it is transferable, a central-bank-money compensation mechanism between institutions should be provided to guarantee settlement finality - a feature that distinguishes it from an ordinary bank deposit. The clarification should be neutral as to how the bank operates the token (public or permissioned ledger, in-house or through a technology provider), and should confirm that the use of a technology provider to issue or operate a deposit token changes neither the legal nature of the deposit nor the bank's responsibility for it. Transfer restrictions, allowlists and freeze functions on such tokens are the bank's compliance controls, not indicators of custody by anyone.

In line with the principle of technological neutrality, tokenised deposits should receive the same prudential treatment as traditional bank deposits under the CRR/CRD framework.

Finally, we suggest including through targeted adjustments to the DLT Pilot Regime (Article 5(8)) or CSDR-credit institutions to offer a standardised tokenised-deposit solution interoperable with DLT market infrastructures, rather than leaving each operator to negotiate an isolated bilateral arrangement as is currently the case.

Question 78. Do tokenised deposits raise any specific issues under the CRD/CRR framework? If so, please indicate what issues arise and what regulatory or supervisory action may be appropriate to address the issue(s) identified.

If the legal characterisation of tokenized deposits as deposits is confirmed, no specific issues should arise under the CRD/CRR framework.

Question 79. Do tokenised deposits raise any questions and challenges from a deposit insurance perspective? If you identify any questions or challenges, please indicate which supervisory or regulatory action is appropriate to address the issues identified.

Normally not, it all depends on the legal characterization. If tokenized deposits are legally characterised as deposits, no specific issues should arise from a deposit insurance perspective. In such a case, tokenized deposits would remain within the scope of the existing deposit protection framework applicable to eligible deposits.

On legal treatment of tokens

Legal certainty in the treatment of tokens in the EU and in the Member States is crucial in supporting predictable outcomes in financial markets in Europe and is vital to avoid stifling innovation, both in relation to MiCA crypto-assets (crypto-assets) as well as for the tokenisation and issuance of financial instruments in the form of tokens, currently governed by MiFID/R or asset management regulation (DLT financial instruments). Tokens in this section generally refer to both DLT financial instruments and crypto-assets, unless specified otherwise. In relation to legal certainty in the treatment of tokens, at least several issues have been noted by stakeholders, supervisors and academics. These include questions on whether tokens can be objects of property, which rules apply to the title and transfer of tokens, their treatment in the event of insolvency, custody relationships, and security rights in crypto-assets.

There are different ways to categorise tokens depending on the type of rights they confer to the holder. There are two general types of tokens, native tokens and non-native tokens. Native tokens tend to represent an asset (such as a share or security) that only exists on-chain (i.e. without a physical or traditional paper-based equivalent). Non-native tokens tend to represent an on chain right over an asset that is legally constituted and represented elsewhere (off chain) allowing this right to be held and transacted on DLT. Regarding non-native tokens, legal uncertainties may arise because, depending on the legal framework and the way the token was created, the tokenisation often leads to the simultaneous existence of two assets: the token representing the asset and the asset that the token asset represents. Native tokens too may raise important legal questions about their nature as many jurisdictions of today do not explicitly recognise existence of on-chain assets and it is often unclear if and how they fall under current rules on taxonomy and creation of traditional financial assets.

One of the key questions concerning legal certainty is whether holding (or controlling) a token on a blockchain constitutes ownership, and whether holding (or controlling) a non-native token constitutes ownership or merely a claim on the underlying asset that it represents. MiCA contains clear requirements for issuers or offerors of crypto-assets but it does not directly regulate the ownership of such assets, which remains a matter of (national) property laws. Similarly, MiFID does not define the proprietary nature of financial instruments or transfer of ownership, which is left to the discretion of national laws. Some Member States have implemented specific regulations to ensure legal certainty for tokens, including to provide for statutory “bridges” that synchronise the technical state of the ledger with the legal status of the asset.

Question 80. Is there legal uncertainty as to the private law treatment of issuance, holding and transfers of tokens, under national law?

- ☒ Yes
☐ No

If you believe there is material legal uncertainty in issuing, holding and transferring tokens (i) which of the following issues are most significant and (ii) what is the urgency with which each issue should be addressed by regulators?

Scales used:

Significance of legal uncertainty: 1 = None or Not significant · 2 = Low · 3 = Moderate · 4 = High · 5 = Very high

Urgency of regulatory clarification or action: 1 = None or Not urgent · 2 = Low urgency · 3 = Moderate urgency · 4 = High urgency · 5 = Immediate / critical

Issue	Significance of legal uncertainty					Urgency of regulatory action				
	1	2	3	4	5	1	2	3	4	5
Issuing a crypto-asset token in compliance with national law	■					■				
Issuing a tokenised financial instrument					■					■
Transferring ownership (acquisitions, dispositions, earmarking, etc.) over a token, including good faith acquisition / bona fide ownership					■					■
Recognising ownership in a token towards third-parties					■					■
Using tokens as collateral				■						■
Possibility to differentiate between native and non-native tokens in national law					■					■
Recognising tokens as objects of property				■						■
Rights of token holders in intermediated custody chains					■					■
Enforcement and exercise of rights arising from /over tokens or the underlying assets					■					■
Custody of tokens					■					■
Treatment of tokens in insolvency proceedings including intermediary risk					■					■
Others					■					■

Please explain your reply and provide examples from national law. In particular specify if any of the answers is specifically referring to native or non-native tokens and specify if any of the answers would be different depending on if the token is recording a tokenised financial instrument or crypto-assets.

We identify divergent interpretations across national regimes, which may result in inconsistent legal treatment across Member States. Providing further legal clarification in this area is therefore important to ensure a consistent and harmonised approach at EU level. However, as the current legal framework and relevant clarifications largely stem from national laws, the in-depth assessment should be first conducted at a national level before considering legislative action at European level. Such an assessment should identify the existing approaches across Member States, determine where legal uncertainty or inconsistencies arise at every national regime, and assess which issues require further clarification or harmonisation at EU level.

Following this analysis, a targeted regulatory action, potentially through for example a Directive, could be considered to provide greater alignment while preserving the necessary interaction with national frameworks. Such an approach would allow for harmonisation of key principles while continuing relying on national legal regimes.

The identified areas of uncertainty include, in particular, the treatment of tokens used as collateral, the recognition and treatment of tokenised assets in insolvency proceedings, and the legal implications of intermediated custody chains.

Any EU clarification should recognise that segregation of client assets can be evidenced directly on the ledger (distinct addresses and distinct key material per client), give clients a proprietary claim to segregated assets in the insolvency of a custodian or intermediary, and keep control and ownership apart: the party technically able to move an asset is not for that reason its owner.

Examples:

- **Germany:** property status of crypto-assets outside the eWpG perimeter. Germany's Electronic Securities Act (eWpG, 2021) provides a clear statutory framework for tokenised bearer bonds and fund units registered on qualified DLT systems, treating the register entry as constitutive of legal title. However, the eWpG covers only a defined category of securities. For crypto-assets falling outside that perimeter (including EMTs and ARTs under MiCA) no equivalent statutory recognition exists. The German Civil Code (BGB) limits the concept of property (Eigentum) to physical objects (Sachen). Crypto-assets do not satisfy this definition, meaning their ownership cannot be established under the BGB's standard property framework.
- **France:** civil law treatment of crypto-asset transfers and bona fide purchasers. France has made significant progress through the PACTE Act and Ordonnance 2017-1674 for certain tokenised financial instruments, establishing a blockchain-based registration mechanism for unlisted securities. However, for crypto-assets more broadly, fundamental questions under French civil law remain unresolved. Most significantly, where tokens are transferred following theft or fraud, French property law's treatment of the bona fide purchaser (acquéreur de bonne foi) rule is unclear: in traditional movable property law, a bona fide purchaser can acquire good title even from a non-owner. It is uncertain whether and how this principle applies to token transfers recorded on a public blockchain, where the chain of prior transfers is transparent but legal attribution of ownership is not. A victim of token theft may therefore face significant difficulty establishing a proprietary remedy, as against both the thief and any subsequent transferee.

Question 81. Would you recommend increasing the legal certainty in the treatment of tokens through EU law?

- ☒ Yes
☐ No

Question 81.1 If YES, what are the 3 most important elements that should be addressed in EU law? Please explain your answer and provide examples.

As explained in the previous question, the current legal framework relies on national laws. Thus the in-depth

assessment should be first conducted at a national level to identify the existing approaches across Member States, determine where legal uncertainty or inconsistencies arise at every national regime, and ultimately assess which issues require further clarification and harmonisation at EU level.

Question 81.2 If you believe there is a lack of legal certainty regarding tokens, can legal certainty (ownership or entitlement, transfer and enforceability of rights recorded as tokens) be achieved under EU law in one of the following manners?

Rank the below possible measures from 1 to 5.

1. Strongly disagree
2. Rather disagree
3. Neutral
4. Rather agree
5. Strongly agree

	1	2	3	4	5
Implementation of a 28 th regime recognising legal effects of DLT registers holding tokens, including good-faith acquisition rules and rules on opposability/enforceability to third parties (erga omnes effects)			■		
Full harmonisation of private law treatment of tokens in Member States			■		
Partial harmonisation of private law treatment of tokens in Member States					■
Introducing a conflict of law regime for tokens under EU law					■
Other model					

Please explain your response and provide examples, in particular from national law. Where you favour full or partial harmonisation or the introduction of a conflict of laws regime, please specify which legal instrument would be most appropriate for that purpose (a new Regulation or the use of existing regimes, such as MiFID or MiCA). Also consider if there are risks with establishing an ownership regime at EU level and how these risks could be mitigated.

Without a clear understanding of what full harmonization would mean here, we think it may not be feasible to achieve. Whereas full harmonisation is desirable in theory is not achievable in any realistic legislative timeframe given the depth of divergence between Member States' civil law traditions. We suggest the combination of all these proposals to enhance harmonization. This way is more likely to achieve some level of harmonization.

Question 82. There are different "ownership models" that could be used to increase legal certainty over tokens. Please indicate maximum two models listed below that you think EU law could apply if it were to improve the legal certainty of tokens in the EU.

Ownership model	
Model 1: The token is the asset by law, the law recognises a ledger-based asset and the ownership rights are constituted directly by the ledger entry.	
Model 2: The token is the asset by law, where the law recognises that e.g. securities (dematerialised or physical) can be replaced by an entry into a DLT register and by this “replacing” (immobilisation) of the securities the function of the initial security is substituted by entry into a DLT register and the ownership rights are constituted by the representation on the ledger.	
Model 3: Token is the asset by law. In this case the law does not actively regulate legal aspects such as what property is or how transfer of ownership occurs, etc. but instructs on the legal consequences of entries in a DLT register (this is often called a functional approach). The law could at EU level stipulate who may exercise rights, i.e. the person recorded in the DLT register as holder of a tokenised asset, that these rights have full	■
Model 4: The token is the legal carrier of rights associated with a related (often off-chain) asset. The law defines tokens as legal objects that do not create new rights, but can –like a “container” –represent various kinds of rights, such as membership rights, ownership, intellectual property rights, usage rights or rights of lien, etc.. The token would represent the rights stemming from the underlying assets and the law would ensure that the transfer of a token on the ledger legally transfers ownership of the rights stemming from the underlying asset ¹⁴ .	■
Model 5: Any other legal ownership structures, for example based on the approaches taken by different countries, including France, Germany, Luxembourg or adopted in other jurisdictions or internationally, that could be implemented in EU law.	

Please explain your answer and provide examples, and in answering the question, please answer the following sub-questions:

- **What would be the legal interoperability of any such EU level measure with national private laws of Member States, or at least laws of the Member State that you are familiar with?**
- **Is it preferable to establish constitutive rules of ownership based on the asset being recorded on chain or functional rules regulating the effects of recording an asset on chain?**
- **Are the different ownership models better suited for native or non-native tokens?**

The suitability of different ownership models depends significantly on whether the token is native or non-native as these structures involve different legal, operational, and market considerations. For non-native tokens, the ownership model may need to reflect the legal relationship between the token and the underlying asset. In turn, a native tokenized instrument may allow for different ownership and transfer mechanisms, as the token itself forms an integral part of the asset structure. Therefore, ownership models should not be assessed independently from the nature of the token.

Specifically on Model 4- under which the law would ensure that the transfer of a token on the ledger legally transfers ownership of the rights stemming from the underlying asset- any such presumption must attach to the person who can direct a transfer for their own account. Custodians and technology providers holding key material for a client do not benefit from it, the client does.

Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments) and if not, what would need to be different depending on the type of the token?

We have selected Model 3 as it provides a more flexible and multi-purpose framework capable of accommodating the diversity of token models. However, for intermediated holdings, the rule should extend to the person for whose

account a recorded holder holds under a custody arrangement, as evidenced by the custodian's register of positions (MiCA Art. 75(2)).

Overall, **we do not support the establishment of a single, uniform ownership model applicable to all types of tokens, as this could impose unnecessary constraints on market development and limit innovation.** A “one-size-fits-all” approach or the search for a common denominator across all token types may result in an overly restrictive framework. Tokens can be structured in different ways, with varying rights and obligations attached to them, and not all token models are designed to represent or confer full ownership rights.

Instead, we recommend maintaining regulatory flexibility by allowing different ownership models to apply depending on the nature of the token, the underlying asset, the rights represented by the token, and the relevant market context. This approach would better accommodate the diversity of tokenization use cases and preserving the ability to develop structures that are appropriate for their specific needs.

Question 83. Comparing national laws of Member States, what are the main differences in how national laws governs the issuance, holdings and transfers of tokens? Please explain your answer and provide examples.

Questions on conflicts of law

Financial Collateral Directive (FCD) and Settlement Finality Directive (SFD) entails targeted conflict of law rules, mainly applicable to financial instruments hence broadly relevant for DLT financial instruments, however the current regime leaves a potential gap where the token does not qualify under the scope of FCD and SFD or where existing conflict rules do not easily lend its application to tokens. As noted in the UNIDROIT. Art 5 TVTG states that the TT Key holder has the power of disposal over the Token. It is further assumed that the person possessing the power of disposal over a Token also has the right to dispose of the Token. For every previous holder of the power of disposal, it is presumed that he was the person possessing the right of disposal at the time of this ownership.

Principles on digital assets and private law the usual connecting factors for choice-of-law rules, such as the location of persons, offices, activity, or assets have less of a useful role for DLT financial instruments and crypto-assets and the approach would rather be to identify connecting factors relevant to such instruments and assets.

Question 84. Should EU law introduce a conflict of law rule for tokens?

- ☒ Yes
- ☐ No

Question 84.1 If you answered “YES” please explain why the current conflict of law rules applicable in EU are not enough or sufficiently clear in its application to tokens?

While we support further clarification of conflict-of-law rules at EU level, we believe that any such development should first be based on a clear identification and analysis of the specific conflict scenarios that may arise in relation to tokens. Only once these are properly identified should appropriate connecting factors and criteria be considered and defined at a European level.

Question 84.2 If the EU would introduce conflict of law rules for proprietary aspects of tokens, what would be the preferred connecting factors.

Rank the below listed connection factors from 1 to 5 (1 being the most relevant connecting factor and 5 the least relevant connection factor). Connecting factors without a ranking will be considered not relevant.

Connecting factor	Waterfall
	1-5
The law of the state specified in the token or in the principles (if any) expressly specified in the token	3
The law of the state specified in the rules or in the principles of the system on which the token is recorded	
The law of the state in which the legal entity operating the DLT-based system on which tokens are recorded	
In relation to a token for which there is an issuer, the law of the state where the issuer is established	3
In relation to tokens for which there is an issuer, the law of the state under whose supervision the issuer operates	
In relation to tokens for which there is a provider of the technologies creating or issuing the tokens, the law of the state under whose supervision such technology operates	
Where a token shall be registered, the law of the state under whose supervision the register is maintained	5
The law of the state of the relevant operating authority/administrator (PROPA), meaning a state authority or a body (e.g., a foundation) that takes over the administration of the system onto which the token is registered	
The law of the state of the primary residence of the encryption private master keyholder (PREMA), meaning the seat of a body that holds a system-relevant master key, with the help of which coercive transactions can be carried out, for example, based on a court order.	
Any other?	

Please explain your response and provide examples. In answering this question, please consider if the suggested scope of the conflict of law rule in your view is the right one, and whether there are aspects missing.

We would like to provide a clarificatory comment on the factor in relation to tokens for which there is a provider of the technologies creating or issuing the tokens, the law of the state under whose supervision such technology operates. The location of a technology provider and the residence of a 'master keyholder' are unsuitable connecting factors. Threshold and multi-party signing schemes have no master key; key material is split between parties that may sit in different countries and that cannot move the asset alone. Tying the property law of a client's assets to the supervisor of its technology provider would let a service contract change the applicable law.

Question 85. Are there any other issues relating to legal certainty which are not mentioned above?

Adan did not answer this question.

Final open question

Question 86. Interested parties that wish to bring other relevant issues, not raised in this consultation, to the Commission's attention, should feel free to communicate them here.

1- Basel Committee CRR: The Basel crypto standard's treatment of tokenised traditional assets and stablecoins on permissionless networks, which generally cannot qualify for Group 1 treatment, is what keeps banks from using public-network tokenisation and euro stablecoins at scale. The current capital treatment of crypto-assets for banks

may be considered disproportionate for the banking sector compared to MiCA entities. In particular, the differentiation in regulatory treatment between banks and non-bank CASPs raises concerns regarding the creation of an uneven competitive landscape, despite both types of entities potentially providing comparable services and operating under regulatory frameworks designed to ensure appropriate risk management and consumer protection. We call for further consideration to have a more proportionate approach and ensure a level playing field between banks and non-bank CASPs.

2- A further issue that should be considered concerns the possibility of introducing greater flexibility in the MiCA framework by allowing arrangements similar to those available under MiFID. Under MiFID, investment firms may rely on certain third-party arrangements, such as agents or brokers, for the distribution of financial instruments. By contrast, MiCA does not currently provide an equivalent mechanism for CASPs, which limits the ability of market participants to structure their distribution models in a comparable manner. We recommend introducing a similar framework under MiCA to provide greater consistency across EU financial services regulation and allow CASPs to benefit from comparable distribution models, while maintaining appropriate regulatory safeguards.

3- Legal uncertainty regarding the concept of "offer to the public" and the written consent requirement: is defined at a high level of generality in MiCA Level 1 and has not been adequately specified in Level 2 measures. This has produced material and persistent inconsistency in market practice.

4- The issuance caps under Articles 22 and 23: It creates negative incentives for issuers to manage their activity artificially to remain below the threshold, and it may prevent commercially viable and systemically non-threatening products from scaling, while providing no meaningful additional protection against genuinely systemic actors who can restructure to avoid triggering the cap.

5- Unclear concept of a token "means of exchange": the concept- which triggers the condition for the caps to apply- is not adequately defined in MiCA Level 1 or in the Level 2 implementing measures. For example, is not clear whether and what kind of trading volume or a transaction between two CASPs for the purpose of liquidity management counts as a "use as means of exchange". This has produced divergent reporting practices across CASPs and issuers, leading to supervisors not applying the cap consistently.

★

About us

Adan brings together more than 150 professionals, both new entrants and established companies, who build the innovations and use cases of the decentralised web across every part of the economy on a daily basis. By removing the obstacles to their growth and competitiveness, Adan works towards the emergence and influence of French and European champions in the service of our digital sovereignty. Adan promotes a regulatory framework that is fit for purpose, proportionate and supportive of innovation, as well as a better understanding of blockchain technologies, crypto-assets and the opportunities they bring.

Adan would like to thank all of its members who contributed to the preparation of this response, and in particular the CASP Committee, the Tokenisation Committee, the DeFi Committee and the Legal Committee for their valuable input.

Contacts for this response:

- Claire Balva, General Director: Claire.balva@adan.eu
- Adriana Torres Vergara, EU Responsible: adriana.torres.vergara@adan.eu
- Alizée Van Den Schrieck, Legal Officer: alizee.vandenschrieck@adan.eu

★