NVC

Dutch CASP Association

30 SEPTEMBER 2026

CONSULTATION RESPONSE · MICA REVIEW

One rulebook, consistent application.

NVC's response to the European Commission's targeted consultation on the review of the Markets in Crypto-Assets Regulation (MiCA)

www.nvc-nl.org

CONTENTS

Table of Contents

	Introduction	3
	About NVC	3
	Management summary	4
1	**Scope and definitions**	5
1.1	MiCA scope & crypto-asset classification	5
2	**Requirements applying to ARTs and EMTs and their issuers**	7
2.5	Interest payment	7
3	**The appropriateness of the legal framework for CASPs**	9
3.1	Crypto-asset services	9
3.2	Prudential requirements for CASPs	13
3.3	Multi-function groups	14
3.4	Reporting	15
3.5	Environmental and sustainability reporting	16
3.6	Other issues	17
4	**Policy areas beyond the current scope of MiCA**	23
4.1	Decentralised finance	23
4.2	Staking, lending and borrowing of crypto-assets	28
4.6	Legal treatment of tokens	29
4.8	Final open question	30
A	Member authorisations	32
B	List of abbreviations	34

Colophon

Submitted: 30 September 2026
Contribution ID: 01f3bbd7-a436-4413-a3d1-0457d3e9cf4c
Status: Public contribution
Writer: Mauro Lorenzo Halve (Chairman), on behalf of the members
Organisation: Dutch CASP Association (NVC), formerly known as VBNL
Respondent type: Business association
Country of origin: Netherlands
Sector: Crypto-asset service providers association

Usage of AI

This report has been generated with Claude Design. The contents of our answers have not been written by an LLM. Due to many members providing input, in different tone of voice and writing style and both in Dutch and in English, Claude has been used to ensure consistent use of wording and tone.

Introduction

Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA) has applied in part since 30 June 2024 and in full since 30 December 2024. With the end of the last transitional periods on 1 July 2026, crypto-asset services can only be provided in the Union under a MiCA authorisation. Against this background, the European Commission has launched a targeted consultation to assess whether MiCA remains fit for purpose, in light of the first implementation experience of supervisors and industry, the development of crypto-asset markets and the frameworks adopted in other jurisdictions since MiCA was agreed.

This document sets out the response of NVC, submitted on 30 September 2026. As NVC represents Crypto-Asset Service Providers (CASPs) rather than issuers, we have focused on the questions that concern crypto-asset services: the scope of MiCA and the classification of crypto-assets, the interest prohibition for stablecoins insofar as it applies to CASPs, the framework for CASPs under Title V, and policy areas beyond the current scope of MiCA, in particular decentralised finance, lending and borrowing, and the legal treatment of tokens. Questions on which we did not take a position are not included.

Our answers draw on the daily practice of our members as authorised CASPs, and were prepared with input from across the membership.

> **HOW TO READ THIS DOCUMENT**
>
> Each consultation question is shown in a shaded box, followed by NVC's position where the questionnaire asked for one, and our explanation. Part, section and question numbers follow the Commission's questionnaire, so that every answer can be traced back to the original consultation.

About NVC

NVC, the Dutch CASP Association, is the industry association in the Netherlands for CASPs with a license from the Dutch Financial Market Authority (AFM) under the Markets in Crypto-Assets (MiCA) Regulation. Founded in 2014 as a self-regulatory organisation, the association is the main contact point for regulators, supervisors, law enforcement and other public stakeholders. It unites our industry with a shared voice.

All 13 of our members are authorised by the AFM as CASPs under MiCA. Together, they represent over 90 percent of the employment, trading volumes and assets under management in the Dutch crypto-asset sector, and serve more than 1.5 million customers in the Netherlands. The Annex sets out, per member, the services for which it is authorised.

> **NVC – Dutch CASP Association**
>
> Bitvavo | Coinmerce | zerohash | MoonPay | Bitonic | Blockrise | BTC Direct | Bitmymoney | BLOX | Acheron Trading | Monflo | Fiat Republic | Finst

MANAGEMENT SUMMARY

MiCA works. Let's make it work the same for everyone.

MiCA has applied in full since 30 December 2024 and its transitional periods have ended. Our members, all authorised by the AFM, consider the framework broadly fit for purpose. The problems we encounter lie less in the text of MiCA than in how it is applied: the same rules are interpreted differently from one Member State to another, and providers without authorisation continue to reach EU clients.

OUR CALL

Apply MiCA consistently, enforce it against those who operate outside it, and close the specific gaps that practice has revealed, before adding new layers of regulation.

NVC and its members are willing to share information and experience with the Commission, ESMA and national competent authorities to support this work.

Our main recommendations:

- **Convergence before new rules.** ESMA should make fuller use of its convergence tools, so that the same application leads to the same outcome in every Member State. Competent authorities should not add requirements on top of MiCA. Q45, Q57
- **Enforcement against unauthorised providers.** Consistent enforcement, a strict reading of reverse solicitation and ESMA's register of non-compliant entities as the single reference, with targeted obligations for digital gateways such as payment processors and search engines. Q48, Q86
- **Clear EU rules for staking and lending, without a new licence.** Express client consent, transparent disclosure and segregation of assets, applied in the same way across the Union. Compensation for lending e-money tokens should remain outside the interest prohibition of Article 50, and that prohibition should not be extended to lending, borrowing or staking. Q20, Q45, Q46, Q67
- **One activity, one authorisation.** EMT-related services under a single authorisation, a workable partnership model between CASPs and payment service providers, and a transfer service authorisation only where transfers are offered as a service in their own right. Q46, Q55
- **Room for tokenization.** Tokenized financial instruments stay under MiFID II, with a limited-scope MiFID II top-up for CASPs that starts with custody, client categories with an opt-up for experienced clients, and a single EU conflict-of-law rule for tokens. Q1, Q84, Q86

NOT NEEDED AT THIS STAGE

A general appropriateness test for spot crypto-assets, a move to the K-factor regime or a recalibration of minimum capital, consolidated supervision of multi-function groups, and bringing DeFi into scope through certification of protocols or liability of CASPs for code they do not control.

Each would add cost and complexity without a demonstrated gain in protection or resilience. (Q47, Q49 to Q51, Q59 to Q63)

Part 1 Scope and definitions

Part 1 of the consultation concerns crypto-assets other than asset-referenced tokens (ARTs) or e-money tokens (EMTs), the category covered by Title II MiCA. NVC addressed one question in this part, on the classification of crypto-assets that display characteristics of financial instruments.

1.1 MiCA scope & crypto-asset classification

> **QUESTION 1**
>
> Should crypto-assets that qualify as financial instruments as defined in Directive 2014/65/EU (MiFID II), continue to be governed by sectoral 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?

NVC POSITION **Yes, they should remain under the main sectoral legislation.**

> **QUESTION 1.1**
>
> 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?

NVC POSITION **No, clarification is needed.**

> **QUESTION 1.2**
>
> Please explain your answer to question 1.1 and suggest any policy actions for clarification if needed.

NVC supports maintaining the current sectoral approach. The sectoral frameworks are calibrated to fundamentally different risk profiles, investor protection needs and market structures. Recording an asset on a distributed ledger is one element in assessing its risk, but not in itself decisive for its regulatory classification. Bringing all DLT-recorded assets under MiCA would blur these regimes and weaken their effectiveness. At least for now, preserving the existing boundary is preferable for legal certainty and regulatory stability. It does, however, require a proportionate route for CASPs to serve tokenized financial instruments, which we address in our answer to Question 86.

While we support maintaining sectoral regimes, the current framework does not provide adequate clarity for all market participants. Despite ESMA's guidelines on the qualification of crypto-assets as financial instruments, significant interpretative uncertainty persists, particularly for instruments that display characteristics of both financial instruments and MiCA crypto-assets.

We therefore recommend that ESMA's guidelines be extended to a defined set of borderline instruments that have proven most difficult to classify in practice:

(i) Hybrid tokens that combine utility or governance rights with features of transferable securities or other financial instruments. We welcome Guideline 9, under which the financial-instrument nature of a hybrid token takes precedence, but it requires elaboration. A feature that is merely ancillary and does not in itself give rise to rights comparable to those of a financial instrument should not trigger MiFID II classification of the token as a whole; classification should follow the economic substance of the token as a whole.

(ii) Governance tokens, in particular where voting rights over a protocol are combined with a share in protocol revenues or treasury assets.

(iii) Tokens that track or are backed by financial instruments, such as tokenized shares issued through a special purpose vehicle, where it is unclear whether the token is a transferable security, a derivative or a crypto-asset.

(iv) Tokenized money-market instruments and fund units, in particular where exposure is held through an intermediate structure and classification partly depends on national law.

(v) Voucher tokens issued by a smart contract that entitle the holder, on redemption, to crypto-assets other than those deposited together with a yield. Their classification should follow the distinction we draw in our answer to Question 67: an arrangement is deposit-like only where the holder has a claim to a nominal amount that is repayable in all circumstances.

For each category, ESMA should publish dedicated guidance setting out the criteria and indicators that determine whether an instrument falls under MiFID II or MiCA. This guidance should be developed in close coordination with national competent authorities, since the classification of certain assets partly depends on national law.

We do not advocate a rigid bright-line test that cannot accommodate market developments. We recommend a principles-based framework with a non-exhaustive list of indicative examples, updated periodically. This would reduce regulatory arbitrage and improve consistency in classification across Member States, without requiring legislative amendment at this stage.

Part 2 Requirements applying to ARTs and EMTs and their issuers

Part 2 concerns MiCA's bespoke regime for so-called "stablecoins": asset-referenced tokens (ARTs) and e-money tokens (EMTs). As NVC represents CASPs rather than issuers, it responded only to Question 20, which applies directly to CASPs.

2.5 Interest payment

> **QUESTION 20(A) — FOR EMTS**
>
> MiCA currently prohibits the granting of interest or any interest-equivalent remuneration of stablecoins by either the issuer, offeror or crypto-asset service provider. In your view, should the MiCA prohibition on granting interest or any interest-equivalent remuneration be modified?

NVC POSITION **Yes, interest or interest-equivalent remuneration should be allowed under defined conditions.**

NVC represents crypto-asset service providers rather than issuers. In Part 2 we therefore respond only to Question 20, as Article 50(2) applies to CASPs directly, and take no position on issuer-specific questions. Our answer applies equally to asset-referenced tokens under Article 40.

Our selection relates primarily to CASPs. On issuer remuneration, we note only that a conditioned possibility for issuers to pass on part of their net reserve income would not, in our view, undermine the objectives of Article 50, and we would engage constructively with any such proposal. Our main concern is a different course, proposed by the ESCB in its response to this consultation: extending the prohibition to lending, borrowing and staking and to "indirect" remuneration. That course would fall on CASPs directly, and we believe it should not be pursued.

Lending does not equal holding

Article 50(3) defines interest as a benefit related to the length of time a holder holds e-money tokens, including benefits received from third parties. When a client lends tokens, title passes to the borrower: the client no longer holds them, is owed the same quantity back, and bears the borrower's credit risk and the token's own risks. The compensation is for that loan and that risk, not for holding. We read Article 50(3) as leaving such compensation outside the prohibition and would welcome confirmation of that reading.

A prohibition would in practice end lending through EU-authorised CASPs. No client lends tokens for nothing while bearing the borrower's risk, and under Article 66 a CASP could not in our view offer an arrangement in which clients carry that risk without reward. This would have two material undesirable consequences.

(i) Loss of oversight. Demand for a return on stablecoin balances would not disappear but move to DeFi protocols and platforms outside the Union, which remain readily accessible to EU users and increase in popularity. As reflected in our answer to Question 59, DeFi lending is already significantly used despite important unmitigated weaknesses. Users would exchange a disclosed arrangement with an authorised counterparty for one without recourse, and supervisors would lose the AML/CFT, transfer-of-funds and conduct safeguards that come with provision by EU-authorised CASPs. The risk would remain while the oversight would not.

(ii) The position of euro stablecoins. Stablecoins are the principal means of trading and settlement in crypto-asset markets, and their natural lenders are clients of EU CASPs. If that supply cannot be lent, spreads in euro pairs widen and activity moves further into US-dollar pairs, which already dominate stablecoin supply and volume. The same borrowing supports the arbitrage that keeps tokens at par, which matters most under stress. An extension would therefore work against euro stablecoins and the deeper EU liquidity we call for in our answer to Question 56.

No deposit substitution

Lending e-money tokens does not raise the deposit-substitution concern behind Article 50, provided no party guarantees repayment at nominal value in all circumstances: the client bears the borrower's and the issuer's risk and has no deposit guarantee. Where such a guarantee is given, the arrangement is deposit-like, as set out in our answer to Question 67. Where the Union has faced comparable questions, as with money market funds, it has regulated rather than prohibited.

Article 50(3) already captures benefits with an equivalent effect to interest, including from third parties. Extending it to an undefined notion of "indirect" remuneration would make fee discounts, loyalty benefits and lending fees uncertain. If circumvention is a concern, a defined rule on issuer-funded rewards for holding, however routed, would address it more precisely.

E-money tokens cannot be staked, as they are not consensus assets. What is marketed as stablecoin staking is lending or liquidity provision and should be treated as such.

Conditions

Compensation for lending should be expressly permitted where the arrangement is a genuine loan: title passes and the same quantity is owed back; no party promises the nominal value; only tokens actually lent are remunerated; the client's exposure is disclosed and the product is not presented as interest, savings or deposit-like; assets not lent remain segregated; and the provider is subject to the framework in our answer to Question 67.

NVC therefore asks the Commission and the co-legislators to confirm that compensation for lending falls outside Article 50(3), not to extend the prohibition to lending, borrowing or staking, and to address circumvention, where needed, through a defined rule on issuer-funded rewards for holding.

> **QUESTION 20(B) — FOR ARTS**
>
> Should the MiCA prohibition on granting interest or any interest-equivalent remuneration be modified for asset-referenced tokens?

NVC POSITION **Yes, interest or interest-equivalent remuneration should be allowed under defined conditions.**

NVC represents crypto-asset service providers rather than issuers. In Part 2 we therefore respond only to Question 20, as Article 50(2) applies to CASPs directly, and take no position on issuer-specific questions. Our answer applies equally to asset-referenced tokens under Article 40 — see our answer above.

Part 3 The appropriateness of the legal framework for CASPs

Part 3 forms the core of NVC's submission, addressing the adequacy of the current scope of regulated crypto-asset services, the prudential framework, multi-function groups, reporting, sustainability disclosure and a number of further Title V issues.

3.1 Crypto-asset 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?

NVC POSITION Yes.

NVC considers the list in Article 3(16) broadly adequate. It is technology-neutral and covers the activities through which EU clients access crypto-asset markets today. MiCA has only recently started to apply, and most remaining uncertainty can be resolved through consistent interpretation, Level 2 and Level 3 measures, supervisory convergence and enforcement; without changing the list.

Staking and lending is where legal certainty is most under pressure. They are not separate services under MiCA, but a CASP that offers them already does so within a regulated client relationship as both its conduct obligations under Article 66 and its custody obligations continue to apply. Some national authorities have nevertheless started to set their own additional requirements. If that continues, the same activity will be allowed in one Member State, restricted in another and subject to different conditions in a third. That undermines the single rulebook and rewards firms that settle where the approach is most lenient.

Whatever the outcome of this review, we therefore ask the Commission and ESMA to:

(i) issue guidelines and/or Q&As on how existing MiCA services and obligations apply to staking and lending, so that all competent authorities apply the same interpretation;

(ii) make clear that Member States should not add national requirements for these activities on top of MiCA;

(iii) follow national practices through peer reviews and convergence work;

(iv) collect data on these activities, so that any later decision to regulate them specifically rests on evidence.

Should staking and lending nonetheless be added to Article 3(16), the Union rules should fully replace national requirements. CASPs already authorised under MiCA should be able to add these services by extending their existing authorisation, with a transitional period for firms that already offer them under national rules. Requirements should reflect the risks of each service rather than the full set of Title V obligations, with disclosure, client consent and segregation of assets at their core. Definitions should be precise and technology-neutral, separating custodial staking from non-custodial or protocol-level activity, and the lending of crypto-assets from deposit-like arrangements. We elaborate on this in our answers to Questions 46 and 67.

Legal clarity is also needed on how existing services apply to newer business models, in particular intermediation in DeFi, the scope of the transfer service where transfers are merely part of custody or exchange, and crypto-asset acquiring. For acquiring, Member States currently differ on how the service is to be qualified, whether it requires custody and who the CASP's client is. In our view acquiring should be possible with and without custody, and these questions should be answered in the same way across the Union without adding another authorisation layer. We come back to this in our answer to Question 86.

> **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.

As set out in our answer to Question 45, NVC does not consider that the list of services requires broad changes at this stage already. If services are nonetheless added, we recommend limiting the additions to staking and to lending and borrowing of crypto-assets on behalf of clients. These activities are already offered at scale, and some national authorities already apply their own requirements to them.

Harmonisation and authorisation

Union rules for these services should fully replace national requirements. Only then will CASPs in Member States with national requirements stop competing on unequal terms with CASPs elsewhere, and only then can CASPs tell clients clearly which regime applies. CASPs already authorised under MiCA should be able to add these services by extending their existing authorisation, with a transitional period for firms that already offer them under national rules. Requirements should reflect the risks of each service rather than the full set of Title V obligations, and definitions should be precise and technology-neutral.

Staking

Staking is closely tied to custody. When a CASP stakes crypto-assets it holds for clients, those assets remain client assets and the CASP's custody obligations continue to apply. The service should therefore cover arrangements in which the CASP stakes client assets held in custody, either itself or through a third-party validator. Non-custodial arrangements, where the client keeps control of its keys, and protocol-level activity without an identifiable provider should not be caught automatically.

Requirements should build on the custody framework. In particular, clients should give prior and explicit consent before their assets are staked, and should receive information in advance on lock-up and unbonding periods, slashing and who bears the resulting losses, the use of third-party validators, and how rewards are calculated and what share the CASP keeps. Staked assets should be clearly identifiable in the client's account. Third-party validators can be overseen under the existing outsourcing and DORA rules; a separate regime is not needed. Staking rewards should not be presented as interest or as a guaranteed return. The framework should also clarify how custody obligations apply while staked assets are locked in a protocol or held through a third-party validator.

Lending and borrowing

The lending of crypto-assets should be clearly separated from deposit-like arrangements. For the elements of a framework we refer to our answer to Question 67, and for e-money tokens to our answer to Question 20.

Existing services and the transfer service

We do not consider that any existing service should be removed. We do ask for clarity on the scope of the transfer service. The transfer service under Article 3(16)(j) MiCA and the notion of a transfer of crypto-assets under the Transfer of Funds Regulation are separate definitions. In practice, however, CASPs are often required to hold a transfer service authorisation even where transfers are simply part of their custody or exchange service, for example a withdrawal to the client's own address. The Commission confirmed this reading in Q&A 2071. ESMA considers the outcome disproportionate for investment firms that notify under Article 60 and proposes relief for them. The same reasoning applies to CASPs whose transfers are merely part of their custody or exchange service. The travel rule does not depend on it, since the TFR applies to any CASP that carries out a transfer of crypto-assets. We recommend extending ESMA's proposed relief, so that a transfer service authorisation is only required where transfers are offered as a service in their own right.

> **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?

NVC POSITION No.

NVC does not consider that an appropriateness test for reception and transmission, execution and placing would materially increase protection for consumers and investors. Should the Commission nonetheless consider introducing one, we set out below the conditions under which it should apply.

MiCA already contains a calibrated set of conduct requirements. Under Article 66, CASPs must act honestly, fairly and professionally in the best interests of their clients, provide information that is fair, clear and not misleading, and warn clients of the risks associated with transactions in crypto-assets. Where a CASP provides advice or portfolio management, Article 81 requires a suitability assessment. The same logic applies under MiFID II, where execution-only services in non-complex instruments are not subject to an appropriateness test. The relevant question is therefore not whether crypto-assets are volatile but whether they are complex. Spot crypto-assets without leverage or embedded derivatives are, in structure, simple instruments.

Protection at the level of the product already exists. Operators of trading platforms must assess the suitability of a crypto-asset before admitting it to trading (Article 76(2)). Many other CASPs apply comparable internal assessments before offering a crypto-asset to clients at all. The priority should be the consistent application and supervision of these requirements across Member States before new obligations are added.

An appropriateness test is also unlikely to address the main risks retail clients face. For spot crypto-assets, the most material harm arises from fraud, scams, hacks and rug-pulls, not from clients misunderstanding what they are buying. Appropriateness assessments rely largely on standardised questionnaires and self-declarations. They offer limited insight into how clients actually behave and

may create a false sense of assurance for clients and firms alike. Clear risk disclosures, fair marketing, robust custody arrangements and effective enforcement against unauthorised providers offer better protection.

Should an appropriateness test nevertheless be introduced, we recommend that:

(i) it is risk-based and targeted at services and products with a higher risk profile, such as those involving leverage, borrowing or rehypothecation, rather than applying to all spot transactions;

(ii) it allows differentiation between crypto-assets on the basis of objective, technology-neutral criteria such as liquidity and market history, rather than treating established, highly liquid crypto-assets in the same way as newly issued, illiquid or meme-tokens;

(iii) e-money tokens and asset-referenced tokens are excluded from its scope, or at least subjected to a light version. The test addresses the risk that a client does not understand the product. The main risks of these tokens are issuer failure, reserve inadequacy and deviation from par in the secondary market, and these are addressed through MiCA's reserve and redemption framework and through disclosure, not through an assessment at the point of sale;

(iv) the outcome of the test is a warning, as under MiFID II, after which the client may proceed, and the assessment is carried out once per client and category of crypto-asset rather than per transaction;

(v) the test and risk warnings operate as substitutes, not as cumulative layers. Where a client has been assessed, generic risk warnings should be reduced accordingly, especially with a positive outcome;

(vi) it is introduced only together with a Level 1 carve-out for professional clients and eligible counterparties, including an elective professional client regime comparable to Annex II of MiFID II. Without such a carve-out, the test would constrain institutional activity and reduce market depth and liquidity in the Union.

> **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?

NVC POSITION **Yes.**

Since the end of all transitional periods on 1 July 2026, there is clear public evidence that crypto-asset service providers without MiCA authorisation continue to attract and serve EU clients. They typically do so through global websites and apps, social media, search engines and payment channels, and in some cases by relying on a broader reading of reverse solicitation than should be acceptable. NVC does not consider it appropriate to name individual firms in this response; the relevant information is largely public, including in recent press reporting and in ESMA's register of non-compliant entities, however not all of those are already included.

This creates an uneven playing field for authorised CASPs that have invested in compliance. It exposes EU retail clients to providers operating with potentially lower standards of governance, custody and investor protection, and it undermines the credibility of the authorisation regime itself.

Identifying and acting against unauthorised providers is primarily the responsibility of NCAs and ESMA. We would welcome:

(i) consistent and visible enforcement across Member States, including against providers that serve EU clients from outside the Union;

(ii) strict application of the reverse solicitation exemption in line with ESMA's guidelines;

(iii) use of ESMA's register of non-compliant entities as the authoritative reference for which providers are unauthorised, so that market participants and digital gateways can rely on it.

Our recommendations on digital gateways are set out in our answer to Question 86. NVC and its members are willing to share information with supervisors where this helps.

3.2 Prudential requirements for CASPs

> **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?

NVC POSITION **It is appropriate to capture the risks associated with the provision of crypto-asset services.**

NVC considers the current prudential regime appropriate. Requiring the higher of permanent minimum capital and one quarter of fixed overheads gives a simple and predictable basis that works across the full range of CASP business models. Because own funds can be combined with insurance, firms can meet the requirement in a way that fits their risk profile.

We do not support aligning the regime with the K-factor framework for investment firms. K-factors were calibrated for traditional financial instruments and would require CASPs to build substantial new and more complex data and reporting processes, without a demonstrated shortcoming in the current regime. MiCA has only recently started to apply, most CASPs have only just been authorised, and changing the prudential basis at this stage would add cost and uncertainty without a clear gain in resilience.

We have taken note of the ESCB's suggestion to make its own funds requirements more risk sensitive. Where specific activities expose a CASP to material (counterparty) risk, for example lending under transfer of title if brought within scope, targeted requirements for that activity are more proportionate than a general recalibration for all CASPs. We set out our views on such activities in our answers to Questions 46 and 67.

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?

Item	NVC assessment
Minimum initial capital for Class 1 (EUR 50,000)	3 — kept as is
Minimum initial capital for Class 2 (EUR 125,000)	3 — kept as is
Minimum initial capital for Class 3 (EUR 150,000)	3 — kept as is

NVC considers the minimum capital amounts in Annex IV broadly appropriate for all three classes and recommends keeping them as they are, for the reasons set out in our answer to Question 49. For most established CASPs the fixed overheads requirement is the binding one, so the Annex IV amounts matter mainly for smaller firms and new entrants. Raising them would increase barriers to entry without a demonstrated gain in resilience, while lowering them would weaken the floor that ensures an orderly wind-down.

3.3 Multi-function groups

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? What kind of action would be appropriate?

NVC POSITION **The existing approach should be maintained.**

We consider that, at this stage, the existing approach should be maintained. MiCA already requires CASPs to identify, prevent, manage and disclose conflicts of interest and to have governance arrangements that ensure effective and prudent management. These requirements apply to the CASP as a whole, whatever other activities the wider group carries out.

The case for group-level or consolidated supervision rests on systemic risk channels such as contagion, interdependencies and cross-sector leverage. These channels are currently limited in crypto-asset markets. Where linkages with the wider financial system exist, they are already addressed by sector-specific rules:

(i) stablecoin reserves held with credit institutions, by MiCA's reserve requirements;

(ii) exchange-traded products and derivatives referencing crypto-assets, by MiFID II/MiFIR;

(iii) banks' crypto-asset exposures, by their prudential treatment.

Introducing consolidated supervision would impose significant compliance and operational burdens on multi-function groups without a commensurate gain in financial stability or investor protection.

Where a CASP offers services that are not regulated under MiCA, such as lending or staking at present, the existing framework already applies. As set out in our answer to Question 67, the CASP remains bound by its conduct obligations under Article 66 for the entire client relationship and must make clear to clients which of its services are regulated. What is needed is consistent application of this approach across Member States, not group-level supervision. If these services are brought within scope, the framework set out in our answers to Questions 46 and 67 applies.

We have taken note of the ESCB's proposals for enhanced group-level oversight of multi-function groups. Should the Commission pursue such measures, we recommend that they:

(i) are limited to groups whose size and interconnectedness justify them, for example by reference to the criteria for significant CASPs, rather than applying to all multi-function groups;

(ii) build on existing cooperation between competent authorities rather than adding a new supervisory layer.

3.4 Reporting

> **QUESTION 52**
>
> Should CASPs report regularly their activities?

Item	NVC assessment
Direct holdings of crypto-assets by CASPs	Yes
Large exposures to derivatives with crypto-assets as underlying	No
Volumes of leveraged contracts and extent of leverage used on trading platforms	No
Information on counterparty risk	Yes

NVC supports regular reporting on direct holdings of crypto-assets by CASPs and on counterparty risk, provided that it is proportionate and harmonised across the Union.

Direct holdings: reporting should cover the CASP's own account holdings, distinguished from client assets held in custody, and should apply only above a de minimis threshold. We recommend setting that threshold relative to the CASP's own funds rather than as a fixed amount, so that it reflects each firm's size and risk profile accordingly. We do not consider reporting more frequent than on a quarterly basis to be fair.

Counterparty risk: reporting should cover exposures to single counterparties, such as trading venues, liquidity providers, sub-custodians and, where relevant, borrowers of crypto-assets. It should be triggered only where an exposure exceeds a threshold relative to own funds, or where a counterparty meets objective criteria indicating that it is at risk. We recommend that ESMA develop regulatory technical standards defining how such exposures are measured and what those thresholds and criteria are. Without such standards, reporting risks becoming vague and inconsistently applied across Member States. For lending and borrowing, the reporting we propose in our answer to Question 67 should form part of the same framework.

Format: reporting should use a single EU template submitted to the home competent authority. National authorities should rely on this template rather than adding separate data requests.

We do not support reporting under MiCA on large exposures to crypto-asset derivatives or on leverage volumes on trading platforms. Derivatives referencing crypto-assets, including leveraged products, are financial instruments already subject to MiFID II/MiFIR and EMIR, including their reporting requirements, as noted in our answer to Question 51. A parallel MiCA obligation would duplicate these regimes. Where leverage is provided through lending within MiCA's scope, it would be captured by the lending reporting set out in our answer to Question 67.

3.5 Environmental and sustainability reporting

> **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)?

NVC POSITION **Broadly appropriate, with limited areas for clarification.**

NVC considers the current sustainability disclosure regime under MiCA, including the Level 2 RTS, broadly appropriate and does not see any need to expand it at this stage. Information on the principal adverse climate and environmental impacts of consensus mechanisms, set out in white papers and made available by CASPs in a prominent place on their websites, all contributes to transparency and helps clients understand the environmental profile of the crypto-assets they use.

Based on our members' experience as authorised CASPs, the challenges lie in the practical application of the regime rather than in its scope. Reliable data is not always available, in particular for crypto-assets without an identifiable issuer or that are issued on multiple networks. Different data providers and methodologies can produce different results for the same crypto-asset, which limits comparability for clients and makes compliance more costly than necessary.

We see the following limited areas for clarification:

(i) consistent methodologies: ESMA guidance or Q&As on calculation methods and acceptable data sources would support comparable disclosures across the market;

(ii) reliance on white papers: where a white paper already contains the required information, CASPs should be able to rely on it, so that the same data is not produced separately by every CASP;

(iii) proportionality: the level of detail could reflect the materiality of the environmental impact, so that disclosures remain meaningful and accessible for clients;

(iv) coherence with other EU sustainability disclosure frameworks, to avoid inconsistencies and duplication;

(v) consistent supervision across Member States, so that all CASPs serving EU clients apply the same requirements.

Once the regime has applied for a longer period, a review based on practical experience would show whether any targeted adjustments are needed.

3.6 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?

Crypto-asset service providers are, by their nature, more exposed to ICT and security risks than many other financial market participants. DORA has had a positive effect on the sector's resilience, and we do not consider that additional cybersecurity legislation at MiCA level is needed. Two clarifications would, however, help DORA work better for CASPs.

First, many CASPs rely on the same specialised ICT providers, for example for custody technology, blockchain analytics and node infrastructure. Supervisors should accept pooled audits of such shared providers where these give equivalent assurance, so that each CASP does not have to repeat the same audit.

Second, guidance is needed on how DORA applies to interaction with public blockchains and smart contracts. A public blockchain is not a contracted ICT service and should not in itself be treated as an ICT third-party service provider. The focus should remain on the CASP's own systems and controls, with smart-contract risk addressed through audits and risk assessments rather than new prescriptive rules.

> **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. Do you consider these changes bring sufficient clarity or are there other issues that remain to be addressed?

NVC POSITION **No — other issues remain to be addressed.**

The PSD3/PSR package is a welcome step. The PSR includes e-money tokens within the definition of "funds", confirms that certain EMT-related transfer services qualify as payment transactions, and excludes trading-style EMT exchanges and EMT transfers without intermediary intervention. This brings welcome clarity on when services involving EMTs qualify as payment services, but it does not remove the risk of overlapping and duplicative requirements under MiCA and PSD3/PSR.

One activity, one authorisation

The EBA Opinion on the interplay between PSD2 and MiCA emphasised that a given activity should be regulated by one framework, and that parallel authorisation requirements for the same activity are disproportionate. NVC shares that view. A firm should be able to provide the same or closely connected EMT-related services under a single authorisation, whether under MiCA or PSD3. Where an activity is genuinely payment-like, such as paying a merchant with an EMT, the relevant PSD3/PSR protections on conduct, transparency, authentication and fraud prevention can be applied through that authorisation by cross-reference. Requiring two authorisations for closely linked activities adds duplicate procedures and potentially cumulative capital requirements, without improving client

protection. It should also be confirmed that custody of EMTs by a MiCA-authorised CASP remains governed by MiCA, and that a custodial wallet does not thereby become a payment account or trigger a second safeguarding regime.

The partnership model

Where a payment services authorisation is nonetheless required, Article 70(4) MiCA allows a CASP to obtain it itself or to partner with an authorised PSP. The EBA Opinion called on NCAs to accept the partnership as a valid alternative by 2 March 2026, and many CASPs set up partnership structures in good faith on that basis. Neither the EBA Opinion nor PSD3/PSR, however, defines what a compliant partnership requires in terms of authorisations, operational responsibilities and supervisory expectations.

A number of NCAs require both parties to hold both licences: the CASP as a PSP and the PSP under MiCA. That makes the partnership model redundant, as it offers no meaningful division of regulatory responsibility, and leaves open which entity bears primary responsibility.

On a correct reading of the EBA Opinion, the CASP provides payment services as a registered agent of the PSP. It retains full responsibility for all crypto-asset activities under its own MiCA authorisation, while the PSP oversees the payment services dimension through contractual monitoring, reporting and intervention powers. This is also the only reading consistent with MiCA's service-by-service authorisation architecture: a crypto-asset transfer can only be provided by one CASP per transaction, and requiring the PSP to hold MiCA authorisation for an activity it does not perform is incoherent.

Clarifications needed

Through EBA Guidelines, a supervisory Q&A or a future legislative amendment, the following should be clarified:

(i) that a CASP acting as a registered payment agent of a PSP satisfies Article 70(4) MiCA without the PSP having to obtain MiCA authorisation, provided the PSP does not itself in fact provide crypto-asset services to the end client;

(ii) that whether the PSP requires MiCA authorisation is a functional, case-by-case assessment, not a presumption triggered by the existence of a partnership;

(iii) the oversight obligations the PSP must maintain over its CASP agent, so that supervisors under PSD3 and MiCA have consistent expectations;

(iv) the disclosure owed to end users in a partnership, including how the respective roles of the PSP and the CASP are reflected in contractual and pre-contractual documentation;

(v) where both parties hold MiCA and PSD authorisations, which party bears primary responsibility for which obligations and how supervisory mandates are delineated.

Without these clarifications, the partnership model will remain unworkable due to divergent NCA interpretations, to the effect of firms that relied on the EBA Opinion in good faith.

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?

NVC POSITION Yes.

QUESTION 56.1

What are the advantages and disadvantages of focusing on EU liquidity or full access to global liquidity?

Focusing on EU liquidity

Maintaining a focus on EU liquidity has clear advantages. It preserves the commercial viability of MiCA-authorised CASPs by ensuring that EU consumers and investors primarily access crypto-asset services through regulated, EU-authorised intermediaries. This supports market integrity, consumer protection and the broader objective of building a robust and competitive EU crypto-asset market. It also prevents regulatory arbitrage, whereby consumers bypass EU-regulated platforms in favour of cheaper, unregulated non-EU alternatives.

The principal disadvantage is that EU liquidity pools alone are not always sufficient to meet the needs of EU consumers and investors, particularly for less liquid crypto-assets where global liquidity is fragmented. This creates a real competitive disadvantage for EU-authorised CASPs relative to established third-country players that are not subject to MiCA's requirements and can offer access to deeper liquidity at lower cost. In this regard, targeted public-sector initiatives, such as pilot programmes for the issuance and settlement of government bonds in EU-regulated stablecoins, would materially contribute to deeper, self-sustaining EU liquidity pools and reduce the structural reliance on third-country liquidity. Euro-denominated e-money tokens issued under MiCA are the natural settlement asset for such pools. Measures that restrict their use, such as the extension of the Article 50 prohibition to lending proposed by the ESCB and discussed in our answer to Question 20, would work against this objective.

Full access to global liquidity

Full and unrestricted access to global liquidity pools would benefit EU consumers in terms of pricing, product range and execution quality, particularly for crypto-assets where EU liquidity is thin. It would also reduce the competitive disadvantage EU-authorised CASPs currently face when competing with non-EU platforms for EU client flows.

However, the disadvantages are significant and in our view outweigh the benefits. Fully opening the EU market to global liquidity pools without appropriate controls would risk undermining the EU's own crypto-asset market infrastructure. If EU consumers can freely and directly access non-EU liquidity pools through unregulated channels, the commercial rationale for obtaining and maintaining a MiCA authorisation is significantly diminished. In the most adverse scenario, this could hollow out EU crypto-asset liquidity altogether, an outcome that would be deeply counterproductive for both market integrity and consumer protection.

Our preferred approach: the broker model

We advocate a targeted, controlled approach modelled on the broker model set out by ESMA, whereby access to non-EU liquidity is provided through MiCA-authorised CASPs acting as intermediaries. Under this model, a MiCA-authorised CASP may access global liquidity pools on behalf of EU clients where necessary, but direct, unmediated access by EU consumers to non-EU platforms operating outside the MiCA framework should not be facilitated or encouraged. This preserves access to global liquidity where needed, while ensuring that EU consumer protection and market integrity standards are maintained throughout and that EU-authorised CASPs remain the primary point of access for EU consumers. This approach depends on effective enforcement against unauthorised providers, as set out in our answers to Questions 48 and 86.

> **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?

Item	NVC assessment
Authorisation of crypto-asset service providers	3 — neutral
Prudential requirements	4 — rather agree
Governance arrangements	4 — rather agree
Obligations in respect of specific crypto-asset services	3 — neutral
Other Title V rules	3 — neutral

The Level 1 provisions are in our view broadly proportionate. Our main concern is not the text of MiCA but the way it is applied: authorisation in particular is still handled differently from one Member State to another.

Authorisation

MiCA lays down one set of authorisation requirements for the whole Union, and an authorised CASP can passport its services to all Member States. That model only works if an authorisation carries the same weight everywhere. In practice, competent authorities differ considerably in the documentation they request, the depth of their assessment, their interpretation of the same provisions and the time an application takes. ESMA's supervisory briefing on authorisation and its peer review of an early authorisation have already shown that these differences are real. The result is an uneven playing field: firms authorised under a demanding process compete, through passporting, with firms authorised elsewhere under a lighter one, and the incentive to seek out the most accommodating authority grows. Divergent interpretation is also visible in the treatment of the transfer service (Question 46) and of CASP-PSP partnerships (Question 55).

Irrespective of the supervisory architecture under discussion in the market integration and supervision package, we therefore recommend that:

(i) ESMA makes fuller use of its convergence tools, including common assessment templates, peer reviews and Q&As, so that the same application leads to the same outcome in every Member State;

(ii) competent authorities do not impose requirements or expectations in the authorisation process beyond those laid down in MiCA and its Level 2 measures;

(iii) timelines are applied consistently, including for extensions of an existing authorisation to additional services;

(iv) ESMA publishes regular overviews of authorisation practice across Member States, so that differences become visible and can be addressed.

Obligations in respect of specific services

These are broadly workable. The main exception is the scope of the transfer service, which we address in our answer to Question 46.

Other Title V rules

Risk warnings are currently applied in the same generic form to all crypto-assets. For e-money tokens used as a means of payment, a general warning focused on volatility can confuse rather than protect. We recommend that warnings be calibrated to the type of crypto-asset, so that warnings for e-money tokens address their actual risks, such as issuer risk, redemption conditions and possible deviation from par in the secondary market. As set out in our answer to Question 47, risk warnings and any appropriateness test should operate as substitutes, not as cumulative layers.

> **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?

Item	NVC assessment
RTS on complaint handling for CASPs (Article 71(5))	4 — rather agree
RTS on offering pre-trading and post-trading data to the public (Article 76(16)(a))	Don't know / not applicable
RTS on content and format of order book and records to be maintained (Article 76(16)(b))	Don't know / not applicable
RTS on records to be kept of crypto-asset services, activities, orders and transactions (Article 68(10)(b))	2 — rather disagree
RTS on the continuity and regularity in performance of crypto services (Article 68(10)(a))	4 — rather agree

Our ratings reflect the experience of members to whom the respective RTS apply. In our experience, the RTS on complaint handling and on business continuity are workable and proportionate.

The RTS on record-keeping is the most burdensome. It prescribes a large number of data fields, several of which follow the MiFID II approach and fit poorly with crypto-asset transactions, and it partly overlaps with records CASPs already keep under the AML framework and the Transfer of Funds Regulation. We recommend that ESMA review these fields for their relevance to crypto-assets and align them with existing AML and TFR record-keeping, so that the same data is kept once and in one format.

Part 4 Policy areas beyond the current scope of MiCA

Part 4 seeks feedback on topics not currently directly regulated by MiCA. NVC addressed decentralised finance, the regulation of lending and borrowing, private-law conflict-of-law rules for tokens, and, in the consultation's final open question, five further issues for the Commission's attention.

4.1 Decentralised finance

> **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?

Item	NVC assessment
a) Exchange services	Limited interest, moderately used
b) Payments and transactions services	Important potential benefits; use remains limited (unmitigated weaknesses)
c) Trading and investment services	Important potential benefits; use remains limited (unmitigated weaknesses)
d) Lending and borrowing services	Important benefits, already significantly used, despite important weaknesses
e) Custody services	Limited interest, moderately used

DeFi-based exchange services can be fast, cheap and easy to access, as users swap crypto-assets directly without a central intermediary. Their use is rather limited, however. Regulated exchanges and brokers serve the mainstream market well. Users mainly turn to DeFi for crypto-assets that regulated platforms do not offer, and they form a small group of experienced users. Depending on the application, weaknesses include lack of information, consumer protection and recourse in case of losses.

DeFi-based payment and transaction services allow peer-to-peer transfers without traditional payment infrastructure. The main benefits are speed, especially for cross-border transfers that settle almost immediately, and a very low cost. This remains relevant for people with limited access to banking services.

DeFi-based trading and investment services are available in the Netherlands and other Member States, but are used by a relatively small group of experienced users. Trading mainly concerns native crypto-assets and is volatile and speculative. On the investment side, tokenized financial instruments and real-world assets are emerging, although most of that activity takes place on permissioned or regulated platforms rather than in DeFi, although such tokens are increasingly used as collateral in DeFi protocols. Faster clearing and settlement is a benefit of blockchain infrastructure in general, including regulated DLT infrastructure. What is specific to DeFi is the lower cost of automating intermediary functions.

DeFi lending and borrowing protocols create on-chain liquidity. The protocol takes over the role of a clearing intermediary through smart contracts and collateral mechanisms, which makes the service accessible and capital-efficient and removes intermediary fees.

Custody in the regulatory sense does not take place in DeFi. A user with a self-hosted wallet keeps control of its keys, and no intermediary takes on safekeeping obligations. Assets locked in a smart contract are not held in custody either, unless an identifiable person can control them. Most market participants still prefer custody by an authorised CASP. Where a CASP stakes client assets on its behalf, its custody obligations continue to apply (see Question 46).

Full decentralisation is rare. With the possible exception of Bitcoin, nearly all DeFi protocols and crypto-assets keep some degree of central control, through governance tokens, developer access or upgrade mechanisms.

We do not think DeFi should be brought into scope at this stage. The first priority should be to enforce the existing framework. MiCA already applies where an arrangement is presented as decentralised but is in fact controlled by an identifiable party, and consistent enforcement in those cases would deal with a large part of the risk. Most DeFi activity is also developed and operated outside the Union. New EU rules would have little grip on the protocols themselves and would mainly affect EU-based developers and service providers, who could move elsewhere. Any future approach will therefore depend on cooperation between supervisors internationally. In the meantime, ESMA guidance on intermediation and on the criteria for full decentralisation (see Question 61) would give CASPs more legal certainty. Market-led measures, such as security audits, better oracle and liquidation design and clearer disclosures, are improving quickly and deserve support, as does user education.

If usage and risks, in particular AML/CFT risks, grow materially, a proportionate response may become necessary. It should then focus on the points where regulated entities, as gatekeepers, interact with DeFi rather than on authorising protocols as CASPs: blockchain analytics and address screening by CASPs, restrictions on connecting clients to protocols strongly associated with illicit activity (see Question 62.1), and the existing TFR rules for transfers involving self-hosted addresses.

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 do you consider should be used to assess the degree of decentralisation?

Item	NVC assessment
Existence of an identifiable intermediary providing a crypto-asset service	4 — rather agree
Presence of control by an identifiable person (e.g. via admin keys) over key functionalities	4 — rather agree
Significant concentration of governance power over key functionalities	4 — rather agree
Custody of user assets by the DeFi protocol	5 — strongly agree
DeFi protocol code is not open source	4 — rather agree
Marketing of a DeFi protocol by an identifiable entity or person	2 — rather disagree
Other	Don't know / not applicable

The criteria for establishing that a DeFi arrangement is not fully decentralised are not yet sufficiently clear, and national interpretations may diverge. Because this assessment decides whether MiCA applies, it matters for legal certainty, for consistent supervision and for a level playing field between authorised CASPs and arrangements that present themselves as decentralised. We would welcome ESMA guidelines or Q&As setting out the criteria and how they should be applied. That would support consistent enforcement of the existing framework, which in our view should come before any new regulation of DeFi (see Question 59).

Avoiding false competition

The test should prevent false competition between regulated services and DeFi arrangements that are in substance centralised. If the criteria are applied too loosely, parties that keep real control over a protocol avoid the obligations that apply to their regulated competitors. The test should therefore look at substance, not at how a protocol is structured or presented.

A cumulative threshold approach

We recommend a cumulative approach rather than treating each criterion as decisive on its own. A protocol would be considered insufficiently decentralised if it meets a minimum number of criteria. This gives legal certainty and prevents protocols from escaping the test by meeting one or two indicators only on paper. The threshold should be set out in guidance or in a delegated act.

Facilitating access

On the control criterion, the party that gives end users access to a protocol is not necessarily the party that controls it. A CASP may offer access to a protocol without any control over it, so offering access should not in itself be treated as a sign of control. The reverse also occurs. Both roles should be assessed separately, and a CASP that intermediates access remains bound by its own MiCA obligations (see Question 62.1).

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?

NVC POSITION Yes.

QUESTION 62.1

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

Item	NVC assessment
CASPs should be able to connect clients to any decentralised DeFi application, subject to appropriate warnings and disclosures	5 — strongly agree
CASPs should be liable for certain types of incidents when clients are affected	1 — strongly disagree
CASPs should only facilitate connection to applications that are certified and service global (permissionless) liquidity	1 — strongly disagree
CASPs should only facilitate connection to certified applications servicing only verified liquidity (verified pools)	1 — strongly disagree
CASPs should only facilitate connection to applications that service global liquidity	1 — strongly disagree
CASPs should discontinue or discourage connections to protocols strongly associated with illicit activity, based on blockchain analytics	5 — strongly agree
CASPs should not facilitate connection to decentralised DeFi applications	1 — strongly disagree
Public bodies should be required, or private organisations incentivised, to publish whitelists or blacklists of DeFi protocols by risk profile	5 — strongly agree
Other	Don't know / not applicable

Our "Yes" to Question 62 should be read narrowly. MiCA regulates services and the firms that provide them, not software. When a client reaches a DeFi protocol through a CASP, the regulated relationship is between the client and the CASP, and that is where risks to the client are already covered. Under Article 66 the CASP must act honestly, fairly and professionally in the client's best interests and give information that is fair, clear and not misleading, including about risks. A CASP that exposes clients to a protocol it does not understand, or presents on-chain activity as if it came with the protection of a regulated service, already falls short of that standard. Supervisors can act on that today.

We therefore do not support a new, formal due diligence obligation for every protocol a CASP connects its clients with. This does not mean that CASPs should connect clients to protocols without care. Where a CASP selects, recommends or integrates a protocol, a proportionate, risk-based assessment is to be expected. We would anchor this at the level of the CASP: a documented policy on how it selects integrations, monitors them and responds to incidents, reviewed by supervisors as part of the CASP's existing governance and risk management. The design of that policy should be left

to the firm, which should be able to rely on independent audits, security research and third-party risk assessments. Should the Commission follow ESMA's proposal for a regulated gateway service for CASPs that give access to DeFi, the obligations should be proportionate to the CASP's control over the protocol, as ESMA itself suggests, and diligence should take the form of this CASP-level policy rather than certification of protocols.

Certification and liability

We strongly disagree with limiting CASPs to certified DeFi applications, whether these serve permissionless or verified liquidity. No workable certification infrastructure exists, it is unclear who would issue certificates (see also Question 63), and a certificate says little about a protocol after the next upgrade, governance vote or exploit. A certification or due diligence requirement would also move the question whether a protocol is decentralised from supervisors to individual firms, while it should be answered on common EU criteria (Question 61). Firms would reach different answers, CASPs would end up offering only the few protocols that can produce formal documentation, and clients would read an integration as an approval.

We also disagree that CASPs should be liable for incidents in protocols they give access to. A CASP controls how it integrates a protocol, not the protocol itself. Liability for code it did not write and cannot change would lead CASPs to stop offering DeFi access. Users would not stop using DeFi. They would go there directly or through providers outside the EU, with less information and fewer safeguards.

Disclosure at the point of access

We support CASPs being able to connect clients to any decentralised DeFi application, provided the client is properly informed. Before a client first uses a protocol through a CASP, it should be told plainly that it is leaving the CASP's regulated service and what that means for custody, recourse and investor protection. A short, standardised disclosure, possibly developed by ESMA, would help clients more than detailed diligence files they will never read. It should not suggest that the protocol has been vetted.

Lists at ESMA level

We support risk-based lists of DeFi protocols, whether whitelists, blacklists or risk tiers, kept by ESMA in the same way as its register of non-compliant entities, so that there is one reference point for the Union. CASPs should be expected to stop or discourage connections to protocols strongly associated with illicit activity on the basis of blockchain analytics. ESMA and national authorities could also collect data from CASPs on DeFi integrations, client uptake and incidents, so that the next review can rest on observed harm rather than assumptions.

> **QUESTION 63**
>
> Do you support introducing certification schemes for DeFi protocols and smart contracts?

NVC POSITION No.

4.2 Staking, lending and borrowing of crypto-assets

> **QUESTION 67**
>
> Do you think that lending and borrowing of crypto-assets should be regulated?

NVC POSITION No.

No, not as a separate regulated service requiring its own authorisation. Lending and borrowing should, however, be subject to clear rules that are applied in the same way in every Member State, within the existing MiCA framework and without national requirements on top. We agree with ESMA's response to the consultation: targeted requirements for CASPs, not a new authorised service.

A CASP that offers lending or borrowing does so within a regulated client relationship. Its conduct obligations under Article 66, its governance and conflict-of-interest requirements and, for assets it holds, the safeguarding and custody rules of Articles 70 and 75 already apply. We understand that custody and segregation no longer protect assets once they are lent out under transfer of title. That is a gap to close and calls for consent and transparency, rather than a new licence.

We would support clarification, through guidelines or, where needed, a targeted provision in MiCA, that a CASP offering lending:

(i) obtains the client's express consent before any assets are lent;

(ii) tells the client, before first use, that lending is not a regulated crypto-asset service, and explains the type and concentration of borrowers, the collateral (if any), the loan and recall terms, and what happens if a borrower or the CASP fails;

(iii) discloses the gross yield and the share it retains, rather than being subject to a cap on that share;

(iv) keeps lent and non-lent assets clearly separated in the client's account, with non-lent assets remaining under the custody rules;

(v) does not present the service as interest, savings or a deposit.

Where borrowing is used for leverage, clients should be told plainly how liquidation works and that losses can exceed the collateral posted. Any appropriateness test should be targeted at such services, as set out in our answer to Question 47. A standardised disclosure format would give clients the same information whichever CASP they use.

In the Netherlands the AFM already applies the conduct requirements of Article 66 to CASPs that offer lending programmes, in line with ESMA's guidance that CASPs remain bound by their MiCA obligations when offering products that are not themselves regulated. NVC supports that approach. It is not yet applied in the same way across the Union, which is why we ask in our answer to Question 45 for common ESMA guidance, no national add-ons and convergence work.

We have also taken note of the ESCB's view that some arrangements may amount to the taking of repayable funds within the scope of the CRD. That can be the case where clients have a claim to a nominal monetary amount that is repayable in all circumstances. It is not the case for the lending of crypto-assets as such, where clients are owed the same crypto-assets back and bear the borrower's and the assets' risks, nor for agency lending, where the CASP lends on the client's behalf without taking title. Guidance should state these distinctions. For e-money tokens, compensation for lending should remain outside Article 50(3), as set out in our answer to Question 20.

Should the Commission nonetheless introduce lending and borrowing as a separate service, the framework should build on the points above and on our answer to Question 46: a clear distinction between agency lending, lending under transfer of title and deposit-like arrangements, recall rights on disclosed terms, limits on and disclosure of on-lending and rehypothecation, and reporting to the competent authority. Requirements should be proportionate to the scale and risk of the activity.

4.6 Legal treatment of tokens

> **QUESTION 84**
>
> Should EU law introduce a conflict of law rule for tokens?

NVC POSITION Yes.

> **QUESTION 84.1**
>
> Please explain why the current conflict of law rules applicable in EU are not enough or sufficiently clear in its application to tokens.

Yes. NVC agrees with the Commission's analysis that the Financial Collateral Directive (FCD) and the Settlement Finality Directive (SFD) only cover part of the market, and their connecting factors, which look to the location of an account, register or intermediary, do not fit well for tokens. For tokens outside their scope there is no harmonised rule at all. Who owns a token, whether a transfer is effective against third parties and whether a security interest is valid are left to the private international law of each Member State. Rome I covers the contractual side of a transfer, but not these proprietary questions.

We recommend a single EU rule, preferably in a regulation so that it applies in the same way everywhere.

One way could be to base it on the approach of the UNIDROIT Principles on Digital Assets and Private Law:

(i) the law specified in the token itself or in the system on which it is recorded applies first;

(ii) where no law is specified, a clear fallback applies, such as the law of the issuer's statutory seat where the token has an identifiable issuer;

(iii) the rule covers transfers, security interests and the treatment of tokens in insolvency, and applies to crypto-assets under MiCA and to DLT financial instruments alike.

We would add two points. First, many crypto-assets, including bitcoin, have no issuer and no specified law. For these the fallback rule decides everything, so it has to be simple and predictable. Second, most EU clients hold tokens through a CASP rather than in self-custody. The rule should therefore also make clear which law governs the client's rights against the custodian and the treatment of client assets if the custodian becomes insolvent, in line with the safeguarding and segregation requirements of Articles 70 and 75 MiCA.

Any new such rule should sit alongside the FCD and SFD without conflicting with them, and the Commission could consider whether their connecting factors should be adapted for DLT-based collateral and settlement. Clear rules on applicable law are a precondition for using tokens at scale,

in secondary trading and as collateral. NVC is willing to contribute to further work on this.

4.8 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.

We welcome this opportunity and would like to raise five further issues.

Top-up authorisations for CASPs

MiCA allows entities authorised under MiFID II or PSD2 to provide crypto-asset services through a simplified notification (Article 60), but there is no equivalent route in the other direction. A CASP authorised for custody of crypto-assets that wishes to hold tokenized financial instruments for clients must obtain a full MiFID II authorisation, despite the functional equivalence of the services. As financial instruments, including shares, increasingly move on-chain, we recommend a limited-scope MiFID II top-up for MiCA-authorised CASPs, with custody as the priority. This follows from our answer to Question 1.2, where we support keeping tokenized financial instruments under MiFID II. For EMT-related payment services, we refer to the single-authorisation approach in our answer to Question 55; where a payment services authorisation nonetheless remains necessary, a simplified top-up would avoid full duplicative licensing.

Enforcement through digital gateways

EU-authorised CASPs bear the full cost of MiCA compliance, while unauthorised providers continue to reach EU users through payment processors, search engines and DeFi interfaces, without those gateways having any corresponding obligation. This asymmetry puts authorised CASPs at a structural disadvantage and may ultimately deter authorisation in the Union. We recommend targeted obligations on gateway operators to take reasonable steps not to promote or onboard providers that serve EU users without authorisation. Because it is not always straightforward to determine whether a provider falls within MiCA's scope, these obligations should be tied to ESMA's register of non-compliant entities, as set out in our answer to Question 48.

Crypto-asset acquiring

Merchants accepting payment in crypto-assets, including EMTs, face legal uncertainty about which services are involved, which entities may intermediate and which framework applies. Member States currently take different views on how acquiring is to be qualified, whether it requires custody and who the CASP's client is. Rather than creating a new MiCA service, which would add to the dual regulation of EMTs under MiCA and PSD3/PSR, we recommend clarifying how existing services apply to acquiring, in line with the single-authorisation approach in our answer to Question 55. In particular:

(i) acquiring should be possible both with and without custody;

(ii) the merchant should be treated as the client of the acquiring provider, consistently across the Union, as under payment acquiring;

(iii) for crypto-assets other than EMTs, it should be clarified which existing crypto-asset services an acquiring model involves.

Client categorisation

MiCA contains no general client categorisation comparable to that of MiFID II. CASPs must therefore apply the same retail-oriented conduct rules, such as risk warnings and information requirements, to banks, investment firms and other institutions that trade crypto-assets professionally. We recommend introducing client categories at Level 1, with the possibility for experienced clients to opt up, so that conduct rules can be applied in proportion to the client's expertise. This would support an EU wholesale crypto-asset market that now has an incentive to operate from third countries, and it would provide the basis for the carve-out we propose in our answer to Question 47.

Services provided to public authorities

CASPs may be required to receive, safeguard and liquidate crypto-assets seized or confiscated in criminal proceedings. In doing so, they act for a public authority rather than for the public. Several requirements, including restrictions on non-EU stablecoins, white paper obligations and the interaction between MiCA, the TFR and payment services rules for EMTs, can create legal uncertainty or obstacles in this context, as can seized privacy-enhancing crypto-assets that EU trading platforms no longer support. We recommend clarification or targeted exemptions for CASPs acting solely on behalf of public authorities in asset recovery and confiscation, while maintaining AML/CFT safeguards.

Annex A Member authorisations

All 13 NVC members are registered with the AFM as CASPs under MiCA.

The table shows, per member, which of the crypto-asset services listed in Article 3(1)(16) MiCA it is authorised to provide, the date of authorisation, and any other relevant financial licence.

Member	MiCA services authorised	Since	Other licence
MoonPay	(c) exchange of crypto-assets for funds (d) exchange of crypto-assets for other crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	30 Dec 2024	EMI
Acheron Trading	(a) providing custody and administration of crypto-assets on behalf of clients (e) execution of orders for crypto-assets on behalf of clients (h) providing advice on crypto-assets (i) providing portfolio management on crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	26 May 2025	
BTC Direct	(c) exchange of crypto-assets for funds (d) exchange of crypto-assets for other crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	18 Jun 2025	
Bitvavo	(a) providing custody and administration of crypto-assets on behalf of clients (b) operation of a trading platform for crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	26 Jun 2025	PSD2
Finst	(a) providing custody and administration of crypto-assets on behalf of clients (e) execution of orders for crypto-assets on behalf of clients (g) reception and transmission of orders for crypto-assets on behalf of clients (j) providing transfer services for crypto-assets on behalf of clients	23 Jul 2025	
Fiat Republic	(a) providing custody and administration of crypto-assets on behalf of clients (j) providing transfer services for crypto-assets on behalf of clients	5 Aug 2025*	EMI
BLOX	(a) providing custody and administration of crypto-assets on behalf of clients (c) exchange of crypto-assets for funds (j) providing transfer services for crypto-assets on behalf of clients	30 Sep 2025	
zerohash	(a) providing custody and administration of crypto-assets on behalf of clients (b) operation of a trading platform for crypto-assets (c) exchange of crypto-assets for funds (d) exchange of crypto-assets for other crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	29 Oct 2025	EMI

Member	MiCA services authorised	Since	Other licence
Coinmerce	(a) providing custody and administration of crypto-assets on behalf of clients (c) exchange of crypto-assets for funds (d) exchange of crypto-assets for other crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	5 Nov 2025	
Bitmymoney	(a) providing custody and administration of crypto-assets on behalf of clients (c) exchange of crypto-assets for funds (d) exchange of crypto-assets for other crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	20 Nov 2025	
Bitonic	(a) providing custody and administration of crypto-assets on behalf of clients (c) exchange of crypto-assets for funds (e) execution of orders for crypto-assets on behalf of clients (j) providing transfer services for crypto-assets on behalf of clients	21 Nov 2025	
Blockrise	(a) providing custody and administration of crypto-assets on behalf of clients (e) execution of orders for crypto-assets on behalf of clients (i) providing portfolio management on crypto-assets (j) providing transfer services for crypto-assets on behalf of clients	25 Nov 2025	
Monflo	(a) providing custody and administration of crypto-assets on behalf of clients (e) execution of orders for crypto-assets on behalf of clients (j) providing transfer services for crypto-assets on behalf of clients	4 Dec 2025	

Sources: AFM register of crypto-asset service providers (overview of 7 September 2026) and ESMA's interim MiCA register. Service letters refer to Article 3(1)(16) MiCA. EMI: electronic money institution licence. PSD2: payment institution licence under the Payment Services Directive.
* Notification under Article 60 MiCA as an electronic money institution.

Annex B List of abbreviations

Abbreviation	Meaning
AFM	Autoriteit Financiële Markten, the Dutch Authority for the Financial Markets
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
ART	Asset-Referenced Token
CASP	Crypto-Asset Service Provider
CRD	Capital Requirements Directive
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EMIR	European Market Infrastructure Regulation
EMT	E-Money Token
ESCB	European System of Central Banks
ESMA	European Securities and Markets Authority
EU	European Union

Abbreviation	Meaning
FCD	Financial Collateral Directive
MAR	Market Abuse Regulation
MiCA	Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114)
MiFID II / MiFIR	Markets in Financial Instruments Directive / Regulation
NCA	National Competent Authority
NVC	Nederlandse Vereniging Cryptodienstverleners, Dutch CASP Association, formerly VBNL
PSD2 / PSD3	Payment Services Directive (second / third generation)
PSP	Payment Service Provider
PSR	Payment Services Regulation
RTS	Regulatory Technical Standards
SFD	Settlement Finality Directive
TFR	Transfer of Funds Regulation
VBNL	Verenigde Bitcoinbedrijven Nederland, the former name of NVC

Contact

Mauro Lorenzo Halve, Chairman NVC · www.nvc-nl.org
NVC – Nederlandse Vereniging Cryptodienstverleners (Dutch CASP Association), formerly VBNL