

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

Fields marked with * are mandatory.

Introduction

Background for this consultation

[Regulation 2023/1114 of 31 May 2023 on Markets in Crypto-Assets \(MiCA\)](#), which sets a dedicated and harmonised framework at Union level to provide specific rules for crypto-assets and related services and activities started to apply in part from 30 June 2024 and in full from 30 December 2024.

Crypto-assets and distributed ledger technology (DLT) offer opportunities for faster cross-border payments, new fundraising methods, and innovative decentralised services, but also entail risks. MiCA was introduced to provide legal certainty through a harmonised EU framework, defining key crypto-asset categories and setting requirements for issuers and service providers, while fostering responsible innovation and mitigating risks related to investor protection, market integrity, and financial stability. As these markets are growing in importance, and traditional financial services providers are also moving into the crypto- and tokenised assets space, a question arises whether the regulatory framework currently governing them remains fit for purpose. The national competent authorities (NCAs), the [European Supervisory Authorities \(ESAs\)](#) and the industry have been sharing feedback on their first implementation experiences. While it may be difficult at this stage to draw conclusions on how MiCA is performing in practice, there have been many policy and regulatory developments globally since MiCA was adopted, and more importantly the crypto-asset markets themselves have significantly developed and continue to evolve since MiCA was designed and adopted. Given these developments, the Commission services consider it necessary to compare and contrast, via this public consultation, the EU framework for crypto-assets with the more recent frameworks of other jurisdictions and with market developments. The results should help assess whether MiCA remains fit for purpose in this evolving policy and market context.

Notwithstanding the objective to promote innovation and digitalisation in European financial systems, financial regulation should remain technology neutral. This is crucial to guarantee the freedom of choice for market participants without inciting them towards using any specific technology and to ensure financial regulation remains adapted to technological advancements without major amendments.

Article 142 MiCA requests the Commission to present a report to the European Parliament and the Council on the latest developments with respect to crypto-assets, in particular, on matters that were left outside the scope of MiCA. The Commission services consider that the review of the Payment Services Directive has largely addressed and clarified some issues emerging from the interplay between the payment services legislation and MiCA following the [advice of the EBA](#).

With this consultation, the Commission services therefore:

- seek to respond to the request in Article 142 of MiCA^[1] and seek to collect the views of the stakeholders on all the market developments not originally covered by MiCA and whether policy or regulatory action would be warranted (see part 5)
- seek feedback to inform the review of MiCA referred to in Article 140 of MiCA^[2], consulting also the [European Banking Authority \(EBA\)](#) and the [European Securities and Markets Authority \(ESMA\)](#) to that effect
- seek to consult on matters that have emerged from the implementation of MiCA to date
- take stock of whether MiCA is fit for the future in the rapidly evolving landscape of digital and tokenised asset markets in a global and internationally competitive context, seizing both the opportunities tokenisation and DLT bring and addressing risks they may generate

In line with its simplification agenda to support EU competitiveness, the Commission services also wish to use this consultation to gather information and assess whether administrative or other burdens emanating from MiCA and its implementation measures can be simplified, reduced or dispensed with.

Beyond questions related to crypto-assets covered by MiCA, this consultation puts forward several questions affecting broader financial acquis. 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 through the open question at the end of this questionnaire. The Commission services welcome specificity and brevity in the replies. The different parts of the consultation cover the following areas:

- **PART 1 - Scope and definitions (title II crypto-assets):** this section includes questions on the current conditions for offering or seeking admission to trading of crypto-assets other than asset referenced tokens (ARTs) or e-money tokens (EMTs)
- **PART 2 - requirements applying to asset referenced tokens (ARTs) and e-money tokens (EMTs) and their issuers (titles III and IV):** this section includes questions on the current conditions for offering or seeking admission to trading of ARTs and EMTs,, their prudential regime, the multi-issuance model of global tokens and considering also the interaction with third country regulatory frameworks, the reserve requirements of ARTs and EMTs, the redemption rights of their holders and crisis management measures
- **PART 3 - the appropriateness of the current legal framework for crypto-asset service providers (CASPs) (titles V and VI):** this section covers questions on the adequacy of the current scope of crypto-asset services regulated under MiCA. Since the supervisory arrangements for CASPs are covered under the current [market integration and supervision package \(MISP\)](#), supervision of CASPs is outside the scope of this consultation
- **PART 4 - topics beyond the initial scope of MiCA:** this final part of the consultation consists of questions relating to decentralised finance, crypto-assets staking, lending and borrowing activities, and non-fungible tokens (NFTs). It also seeks views on whether MiCA should aim to increase legal certainty of crypto-assets and other on-chain assets, particularly in relation to natively issued assets

¹ Regulation (EU) 2023/1114, Article 142(1): 'By 30 December 2024 and after consulting EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the latest developments with respect to crypto-assets, in particular on matters that are not addressed in this Regulation, accompanied, where appropriate, by a legislative proposal'.

² Regulation (EU) 2023/1114, Article 140(1): 'By 30 June 2027, having consulted EBA and ESMA, the Commission shall present a report to the European Parliament and the Council on the application of this Regulation accompanied, where appropriate, by a legislative proposal. An interim report shall be presented by 30 June 2025, accompanied, where appropriate, by a legislative proposal'.

Responding to this consultation

In this targeted consultation, the Commission is interested in the views of a wide range of stakeholders. Responses to this consultation are expected to be most useful where they present a clear and detailed narrative, demonstrated by data (where possible), concrete examples, legal references and qualitative evidence. Specific suggestions for solutions to address issues raised are welcome.

All interested stakeholders are invited to reply by 30 September 2026 via the online questionnaires below.

To the extent that not all questions will be relevant to all stakeholders, respondents are invited to reply only to those questions that are relevant to them.

Please note: In order to ensure a fair and transparent consultation process **only responses received through our online questionnaire will be taken into account** and included in the report summarising the responses. Should you have a problem completing this questionnaire or if you require particular assistance, please contact fisma-mica-review@ec.europa.eu.

More information on

- [this consultation](#)
- [the related public consultation](#)
- [the consultation document](#)
- [crypto-assets](#)
- [the protection of personal data regime for this consultation](#)

About you

* Language of my contribution

- ☐ Bulgarian
- ☐ Croatian
- ☐ Czech
- ☐

- Danish
- ☐ Dutch
- ☒ English
- ☐ Estonian
- ☐ Finnish
- ☐ French
- ☐ German
- ☐ Greek
- ☐ Hungarian
- ☐ Irish
- ☐ Italian
- ☐ Latvian
- ☐ Lithuanian
- ☐ Maltese
- ☐ Polish
- ☐ Portuguese
- ☐ Romanian
- ☐ Slovak
- ☐ Slovenian
- ☐ Spanish
- ☐ Swedish

* I am giving my contribution as

- ☐ Academic/research institution
- ☐ Business association
- ☐ Company/business
- ☐ Consumer organisation
- ☐ EU citizen
- ☐ Environmental organisation
- ☐ Non-EU citizen
- ☐ Non-governmental organisation (NGO)
- ☐ Public authority

☐ Trade union

☒ Other

* First name

donny

* Surname

lewis

* Email (this won't be published)

donny@donnylewis.com

* Organisation name

255 character(s) maximum

Viridis.info

* Organisation size

- ☒ Micro (1 to 9 employees)
- ☐ Small (10 to 49 employees)
- ☐ Medium (50 to 249 employees)
- ☐ Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

* Country of origin

Please add your country of origin, or that of your organisation.

- | | | | |
|-------------------------------------|--------------------------------|-------------------------------------|---|
| ☐ Afghanistan | ☐ Djibouti | ☐ Libya | ☐ Saint Martin |
| ☐ Åland Islands | ☐ Dominica | ☐ Liechtenstein | ☐ Saint Pierre and Miquelon |
| ☐ Albania | ☐ | ☐ Lithuania | ☐ |

	Dominican Republic		Saint Vincent and the Grenadines
Algeria	Ecuador	Luxembourg	Samoa
American Samoa	Egypt	Macau	San Marino
Andorra	El Salvador	Madagascar	São Tomé and Príncipe
Angola	Equatorial Guinea	Malawi	Saudi Arabia
Anguilla	Eritrea	Malaysia	Senegal
Antarctica	Estonia	Maldives	Serbia
Antigua and Barbuda	Eswatini	Mali	Seychelles
Argentina	Ethiopia	Malta	Sierra Leone
Armenia	Falkland Islands	Marshall Islands	Singapore
Aruba	Faroe Islands	Martinique	Sint Maarten
Australia	Fiji	Mauritania	Slovakia
Austria	Finland	Mauritius	Slovenia
Azerbaijan	France	Mayotte	Solomon Islands
Bahamas	French Guiana	Mexico	Somalia
Bahrain	French Polynesia	Micronesia	South Africa
Bangladesh	French Southern and Antarctic Lands	Moldova	South Georgia and the South Sandwich Islands
Barbados	Gabon	Monaco	South Korea
Belarus	Georgia	Mongolia	South Sudan
Belgium	Germany	Montenegro	Spain
Belize	Ghana	Montserrat	Sri Lanka
Benin	Gibraltar	Morocco	Sudan
Bermuda	Greece	Mozambique	Suriname
Bhutan	Greenland	Myanmar/Burma	Svalbard and Jan Mayen
Bolivia	Grenada	Namibia	Sweden

- | | | | |
|--|---|--|--|
| ☐ Bonaire Saint Eustatius and Saba | ☐ Guadeloupe | ☐ Nauru | ☐ Switzerland |
| ☐ Bosnia and Herzegovina | ☐ Guam | ☐ Nepal | ☐ Syria |
| ☐ Botswana | ☐ Guatemala | ☐ Netherlands | ☐ Taiwan |
| ☐ Bouvet Island | ☐ Guernsey | ☐ New Caledonia | ☐ Tajikistan |
| ☐ Brazil | ☐ Guinea | ☐ New Zealand | ☐ Tanzania |
| ☐ British Indian Ocean Territory | ☐ Guinea-Bissau | ☐ Nicaragua | ☐ Thailand |
| ☐ British Virgin Islands | ☐ Guyana | ☐ Niger | ☐ The Gambia |
| ☐ Brunei | ☐ Haiti | ☐ Nigeria | ☐ Timor-Leste |
| ☐ Bulgaria | ☐ Heard Island and McDonald Islands | ☐ Niue | ☐ Togo |
| ☐ Burkina Faso | ☐ Honduras | ☐ Norfolk Island | ☐ Tokelau |
| ☐ Burundi | ☐ Hong Kong | ☐ Northern Mariana Islands | ☐ Tonga |
| ☐ Cambodia | ☐ Hungary | ☐ North Korea | ☐ Trinidad and Tobago |
| ☐ Cameroon | ☐ Iceland | ☐ North Macedonia | ☐ Tunisia |
| ☐ Canada | ☐ India | ☐ Norway | ☐ Turkey |
| ☐ Cape Verde | ☐ Indonesia | ☐ Oman | ☐ Turkmenistan |
| ☐ Cayman Islands | ☐ Iran | ☐ Pakistan | ☐ Turks and Caicos Islands |
| ☐ Central African Republic | ☐ Iraq | ☐ Palau | ☐ Tuvalu |
| ☐ Chad | ☐ Ireland | ☐ Palestine | ☐ Uganda |
| ☐ Chile | ☐ Isle of Man | ☐ Panama | ☐ Ukraine |
| ☐ China | ☐ Israel | ☐ Papua New Guinea | ☐ United Arab Emirates |
| ☐ Christmas Island | ☐ Italy | ☐ Paraguay | ☐ United Kingdom |

- | | | | |
|--|----------------------------------|---|--|
| ☐ Clipperton | ☐ Jamaica | ☐ Peru | ☐ United States |
| ☐ Cocos (Keeling) Islands | ☐ Japan | ☐ Philippines | ☐ United States Minor Outlying Islands |
| ☐ Colombia | ☐ Jersey | ☐ Pitcairn Islands | ☐ Uruguay |
| ☐ Comoros | ☐ Jordan | ☐ Poland | ☐ US Virgin Islands |
| ☐ Congo | ☐ Kazakhstan | ☐ Portugal | ☐ Uzbekistan |
| ☐ Cook Islands | ☐ Kenya | ☐ Puerto Rico | ☐ Vanuatu |
| ☐ Costa Rica | ☐ Kiribati | ☐ Qatar | ☐ Vatican City |
| ☐ Côte d'Ivoire | ☐ Kosovo | ☐ Réunion | ☐ Venezuela |
| ☐ Croatia | ☐ Kuwait | ☐ Romania | ☐ Vietnam |
| ☐ Cuba | ☐ Kyrgyzstan | ☐ Russia | ☐ Wallis and Futuna |
| ☐ Curaçao | ☐ Laos | ☐ Rwanda | ☐ Western Sahara |
| ☐ Cyprus | ☐ Latvia | ☐ Saint Barthélemy | ☐ Yemen |
| ☐ Czechia | ☐ Lebanon | ☐ Saint Helena
Ascension and
Tristan da Cunha | ☐ Zambia |
| ☐ Democratic Republic of the Congo | ☐ Lesotho | ☐ Saint Kitts and Nevis | ☐ Zimbabwe |
| ☐ Denmark | ☐ Liberia | ☐ Saint Lucia | |

* Field of activity or sector (if applicable)

- ☐ Accounting
- ☐ Auditing
- ☐ Banking
- ☐ Credit rating agencies
- ☐ Insurance
- ☐ Pension provision
- ☒ Investment management (e.g. hedge funds, private equity funds, venture capital funds, money market funds, securities)
- ☐

Market infrastructure operation (e.g. CCPs, CSDs, Stock exchanges)

- ☒ Social entrepreneurship
- ☐ Other
- ☐ Not applicable

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, ‘business association’, ‘consumer association’, ‘EU citizen’) country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* Contribution publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

☐ **Anonymous**

Only the organisation type is published: The type of respondent that you responded to this consultation as, your field of activity and your contribution will be published as received. The name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

☒ **Public**

Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

☒ I agree with the [personal data protection provisions](#)

PART 1: Scope and definitions, Title II crypto-assets

MiCA covers three types of crypto-assets: asset-referenced tokens (ARTs), electronic money tokens (EMTs) and crypto-assets other than ARTs or EMTs. The provisions related to the last category are set out in Title II of MiCA. This part of the consultation seeks feedback on the regulation of this category of crypto-assets.

Crypto-assets that fall under other sectoral legislation such as deposits, financial instruments including derivatives, or other regulated products, are outside the scope of MiCA. Therefore, some crypto-assets are regulated under MiCA, while tokenised financial instruments are not.

The distinction between crypto-assets regulated under MiCA and those governed by other sectoral legislation can sometimes be complex, particularly given that the definitions of certain assets, such as securities, are established in national law. Evolving market practices further highlight the convergence between the two areas, as traditional financial institutions increasingly offer MiCA-regulated crypto-assets and services, while MiCA-authorised entities expand into traditional financial products, subject to obtaining the necessary authorisations to do so.

1.1 MiCA scope & 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 Council, 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 sectoral legislation
- ☐ No, all crypto-assets, or the services provided on such assets, should be covered by MiCA
- ☐ Don't know / no opinion / not applicable

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?

- ☐ Yes, sufficiently clear
- ☒ No, clarification is needed
- ☐ Don't know / no opinion / not applicable

Question 1.2 Please explain your answer to question 1.1 and suggest any policy actions for clarification if needed:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The legal treatment The legal treatment should follow the economic function, rights and vulnerabilities of the asset, not the database on which it is recorded. A financial instrument should not become a different legal

object merely because it moves onto a distributed ledger. Technology neutrality requires exactly this restraint. Where clarification is needed, it should focus on functional characteristics and the authority exercised by issuers and intermediaries rather than creating a second regime based on technical form. follow the economic function, rights and vulnerabilities of the asset, not the database on which it is recorded. A financial instrument should not become a different legal object merely because it moves onto a distributed ledger. Technology neutrality requires exactly this restraint. Where clarification is needed, it should focus on functional characteristics and the authority exercised by issuers and intermediaries rather than creating a second regime based on technical form.

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.

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The remaining difficulty is not solved by adding more labels. Hybrid and composable assets can change function depending on how they are used. Classification should therefore be grounded in enforceable rights, economic function, custody, control and the vulnerabilities accepted by users. A token that technically looks identical may create very different trust relationships depending on who can upgrade it, redeem it, custody it or change its economics.

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?

a) Please assess each provision below along their adequacy:

	1 (completely inadequate)	2 (mostly inadequate)	3 (neutral)	4 (moderately adequate)	5 (fully adequate)	Don't know - No opinion - Not applicable
Exemptions for offers to <150 persons per Member State, small offerings (<€1m over 12 months), and qualified investors (Article 4 (2))	☐	☐	☐	☒	☐	☐
White paper disclosure framework (Article 6): issuer information, crypto-asset characteristics, tokenomics, risks, use of proceeds	☐	☒	☐	☐	☐	☐
Marketing requirements: identifiable, fair, clear, not misleading and consistent with the white paper (Article 7)	☐	☒	☐	☐	☐	☐
Ex ante notification model without prior regulatory approval (Article 8)	☐	☐	☐	☐	☒	☐
Obligation to modify/update the white paper for significant new factors, material mistakes or inaccuracies (Article 12)	☐	☒	☐	☐	☐	☐
Retail investor right of withdrawal (14 days), excluding assets already admitted to trading or after subscription period ends (Article 13)	☒	☐	☐	☐	☐	☐
Conduct obligations: honesty, fairness and professionalism, clear communications, conflicts management, and effective systems and security arrangements (Article 14)	☐	☒	☐	☐	☐	☐

Civil liability for inaccurate, misleading or incomplete white paper information (Article 15)						
Overall balance between investor protection, market integrity and innovation under Title II						

Please explain your ratings in question 3 a), focusing on the issues you deem most significant regarding the overall balance between investor protection, market integrity and innovation:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The central problem with Title II is not simply whether each disclosure obligation is individually reasonable. It is the architecture created when disclosure, authorisation, marketing restrictions, issuer obligations and intermediary controls accumulate.

Evidence is useful. Permission is different.

A white paper can make risk inspectable. Liability can make representations accountable. Neither requires the regulator to become the authority that decides in advance which I believe Title II requires substantial redesign rather than incremental adjustment.

Its fundamental problem is architectural.

Article 4 begins from the position that a person shall not make an offer to the public unless that person satisfies a prescribed regulatory structure. Freedom to experiment therefore becomes an exemption from a prohibition rather than the starting condition.

I believe that burden should be reversed.

The starting presumption should be that people are free to build, offer, experiment, invest and voluntarily accept risk unless a specific activity creates a specific vulnerability that justifies intervention.

Fraud should remain fraud. Materially false representations should create liability. Misappropriation should create liability. If an issuer promises particular rights, reserves, governance arrangements or use of proceeds, those representations should be enforceable.

None of that requires the state to become the gatekeeper of the activity itself.

This distinction matters because disclosure can be useful without becoming permission. A simple, proportionate requirement to disclose who controls the project, what rights the asset represents, material risks, insider allocations, upgrade authority, custody arrangements and use of proceeds can provide valuable evidence to a prospective participant.

But the current architecture goes considerably further. It prescribes who may make an offer, the form through which information must be produced, notification requirements, continuing obligations and conduct requirements, while allowing only defined exemptions from that framework.

That is the wrong direction.

I would significantly expand the exemptions, particularly for small offerings and experimental projects, and reconsider whether an arbitrary numerical threshold should determine when voluntary economic activity becomes presumptively subject to the full regulatory apparatus.

The present structure creates another problem: compliance costs are not neutral.

Large institutions can retain lawyers, compliance teams, consultants and regulatory specialists. Small builders

cannot. Every additional mandatory process therefore creates a competitive advantage for actors already possessing capital and institutional access.

That is particularly difficult to justify when regulatory status itself has repeatedly failed to guarantee safety.

European supervisors continue to identify serious AML/CFT deficiencies, regulatory arbitrage and control failures within regulated financial institutions. The lesson is not that there should be no law. The lesson is that certification, licensing and compliance cannot be treated as substitutes for trustworthiness.

The relevant question should therefore be what vulnerability exists and what proportionate defence addresses it, not whether the participant has successfully passed through an institutional gate.

This is the difference between scaffolding and the cage.

Scaffolding would require enough truthful, inspectable information for another person to understand the vulnerability they are being asked to accept. It would establish consequences for deception, theft and breach of clearly assumed obligations. It would expose hidden authority and conflicts.

Then it would leave room for people to decide.

The current approach increasingly starts from the opposite presumption: the activity is restricted unless the participant demonstrates compliance with the architecture the regulator has prescribed.

That is effectively guilty until proven acceptable.

It also creates a dangerous ratchet. Once the principle is established that participation requires satisfying an institutional gatekeeper, the argument becomes only about how many gates should exist and how demanding wful innovation may exist. I would therefore strongly preserve notification without prior approval and resist any movement toward a permission-first model.

MiCA should start from a presumption that lawful activity is permitted unless a specific vulnerability justifies a specific restriction. The opposite presumption, that a new asset, protocol or business model is dangerous until an institution certifies otherwise, is the beginning of the cage described in my Trust Architecture work: formal choice remains, while the practical routes through which that choice can be exercised progressively disappear.

b) Please assess each provision below along the direction of change you consider appropriate:

	1 (should be significantly weakened)	2 (should be somewhat weakened)	3 (should remain unchanged)	4 (should be somewhat strengthened)	5 (should be significantly strengthened)	Don't know - No opinion - Not applicable
Exemptions for offers to <150 persons per Member State, small offerings (<€1m over 12 months), and qualified investors (Article 4 (2))	☐	☒	☐	☐	☐	☐
White paper disclosure framework (Article 6): issuer information, crypto-asset characteristics, tokenomics, risks, use of proceeds	☐	☐	☒	☐	☐	☐
Marketing requirements: identifiable, fair, clear, not misleading and consistent with the white paper (Article 7)	☐	☐	☒	☐	☐	☐
Ex ante notification model without prior regulatory approval (Article 8)	☐	☐	☒	☐	☐	☐
Obligation to modify/update the white paper for significant new factors, material mistakes or inaccuracies (Article 12)	☐	☐	☒	☐	☐	☐
Retail investor right of withdrawal (14 days), excluding assets already admitted to trading or after subscription period ends (Article 13)	☐	☒	☐	☐	☐	☐
Conduct obligations: honesty, fairness and professionalism, clear communications, conflicts management, and effective systems and security arrangements (Article 14)	☐	☒	☐	☐	☐	☐

Civil liability for inaccurate, misleading or incomplete white paper information (Article 15)						
Overall balance between investor protection, market integrity and innovation under Title II						

Please explain your ratings in question 3 b), focusing on the issues you deem most significant regarding the overall balance between investor protection, market integrity and innovation:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I believe Title II requires substantial redesign rather than incremental adjustment.

Its fundamental problem is architectural.

Article 4 begins from the position that a person shall not make an offer to the public unless that person satisfies a prescribed regulatory structure. Freedom to experiment therefore becomes an exemption from a prohibition rather than the starting condition.

I believe that burden should be reversed.

The starting presumption should be that people are free to build, offer, experiment, invest and voluntarily accept risk unless a specific activity creates a specific vulnerability that justifies intervention.

Fraud should remain fraud. Materially false representations should create liability. Misappropriation should create liability. If an issuer promises particular rights, reserves, governance arrangements or use of proceeds, those representations should be enforceable.

None of that requires the state to become the gatekeeper of the activity itself.

This distinction matters because disclosure can be useful without becoming permission. A simple, proportionate requirement to disclose who controls the project, what rights the asset represents, material risks, insider allocations, upgrade authority, custody arrangements and use of proceeds can provide valuable evidence to a prospective participant.

But the current architecture goes considerably further. It prescribes who may make an offer, the form through which information must be produced, notification requirements, continuing obligations and conduct requirements, while allowing only defined exemptions from that framework.

That is the wrong direction.

I would significantly expand the exemptions, particularly for small offerings and experimental projects, and reconsider whether an arbitrary numerical threshold should determine when voluntary economic activity becomes presumptively subject to the full regulatory apparatus.

The present structure creates another problem: compliance costs are not neutral.

Large institutions can retain lawyers, compliance teams, consultants and regulatory specialists. Small builders cannot. Every additional mandatory process therefore creates a competitive advantage for actors already possessing capital and institutional access.

That is particularly difficult to justify when regulatory status itself has repeatedly failed to guarantee safety.

European supervisors continue to identify serious AML/CFT deficiencies, regulatory arbitrage and control

failures within regulated financial institutions. The lesson is not that there should be no law. The lesson is that certification, licensing and compliance cannot be treated as substitutes for trustworthiness.

The relevant question should therefore be what vulnerability exists and what proportionate defence addresses it, not whether the participant has successfully passed through an institutional gate.

This is the difference between scaffolding and the cage.

Scaffolding would require enough truthful, inspectable information for another person to understand the vulnerability they are being asked to accept. It would establish consequences for deception, theft and breach of clearly assumed obligations. It would expose hidden authority and conflicts.

Then it would leave room for people to decide.

The current approach increasingly starts from the opposite presumption: the activity is restricted unless the participant demonstrates compliance with the architecture the regulator has prescribed.

That is effectively guilty until proven acceptable.

It also creates a dangerous ratchet. Once the principle is established that participation requires satisfying an institutional gatekeeper, the argument becomes only about how many gates should exist and how demanding they should become. The wider MiCA review demonstrates precisely why that matters: similar reasoning is now being considered around DeFi certification, CASP access to protocols and even non-custodial software.

The exemptions in Article 4 should therefore be significantly expanded, while the mandatory framework should be rebuilt around actual harm, material representations and actual authority.

I would preserve strong civil liability for materially false or misleading representations. I would preserve proportionate rules against deceptive marketing. I would support simple disclosure of facts necessary to understand an asset's actual trust architecture.

But I do not believe European citizens need a regulatory authority to determine in advance which disclosed risks they may voluntarily accept.

Trust is willingly accepted vulnerability in the presence of risk.

The proper role of regulation here should be to make hidden vulnerability visible, make deception consequential, and intervene where one party possesses authority capable of imposing involuntary vulnerability

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)	2 (rather not serious concern)	3 (neutral)	4 (rather serious concern)	5 (extremely serious concern)	Don't know - No opinion - Not applicable
Inadequate or non-comparable disclosure clarity or complexity to retail investors in Title II white papers	☐	☐	☐	☒	☐	☐
Fraudulent or misleading crypto-asset offerings affecting EU investors	☐	☒	☐	☐	☐	☐
Lack of clear and enforceable investor rights for crypto-asset holders	☐	☒	☐	☐	☐	☐
Insufficient issuer governance or accountability in crypto-asset projects e.g. monitoring of the use of funds by issuers after the offering period	☒	☐	☐	☐	☐	☐
Regulatory arbitrage, including activity shifting outside the EU	☐	☐	☐	☒	☐	☐
Promotions by social media, influencers, sponsorships	☐	☒	☐	☐	☐	☐
Post-issuance token value erosion or project failure affecting EU retail investors	☐	☒	☐	☐	☐	☐
Market manipulation practices (e.g. wash trading, price manipulation) in crypto-asset markets	☐	☐	☒	☐	☐	☐

Misaligned incentives between crypto-asset issuers and investors (e. g. insider allocations, weak lock-ups)						
Difficulty in assessing issuer quality and project credibility for EU investors						
Cross-border enforcement and supervisory coordination challenges within the EU						
Cross-border enforcement and supervisory coordination challenges with third countries authorities outside of the EU						

Please explain your ratings in question 4, focusing on the issues you deem most significant and add any additional issues that you deem highly important:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The most important risks are information asymmetry, hidden control and incentives that are not visible to the person accepting the risk. Disclosure should therefore reveal not only tokenomics but effective control: administrator keys, upgrade rights, insider allocations, vesting, governance concentration, treasury authority and material dependencies. A technically accurate white paper can still conceal the practical trust architecture if it does not show who can change what after the user has committed capital.

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 (rather effective)	5 (highly effective)	Don't know - No opinion - Not applicable
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	☐	☒	☐	☐	☐	☐
Lock-up periods (e.g. 12 months) or vesting schedules for founder and early investor tokens	☒	☐	☐	☐	☐	☐

Please explain your ratings in question 5, and what (other) regulatory or supervisory actions you would consider useful either at the issuance stage and during marketing or distribution:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The burden of proof matters. Regulation should not begin by assuming that every new issuance or marketing technique is abusive and then require the issuer to prove innocence through institutional permission. Where there is deception, undisclosed insider advantage, market manipulation or a material conflict, regulate that conduct directly. Where founders promise vesting, make the promise inspectable and enforceable. But do not turn every legitimate concern into a universal restriction simply because restriction is administratively easier. Traditional finance already demonstrates why this distinction matters. Sophisticated actors have repeatedly found legal and regulatory seams unavailable to ordinary participants. Cum-Ex and Cum-Cum dividend-arbitrage schemes became serious enough that the EBA launched an inquiry and action plan, and later had to review how supervisors integrated tax-integrity risks. More rules do not automatically create equal protection when complexity itself becomes something well-resourced actors can navigate better than individuals. evidence by EU already available.

EBA, inquiry into Cum-Ex/Cum-Cum dividend arbitrage schemes, 12 May 2020.

EBA, Peer Review on Tax Integrity and Dividend Arbitrage Schemes, 6 February 2025.

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

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

MiCA should be simplified wherever compliance asks the same fact to be proved repeatedly to different institutional actors. Every additional collection point creates cost, delay, gatekeeping power and another repository of sensitive information.

Verification does not require possession. If a fact has already been reliably established, privacy-preserving credentials, attestations and selective disclosure should be usable wherever the legal objective can be met without another complete copy of the underlying identity or evidence.

This is not merely an efficiency concern. Financial institutions are high-value cyber targets precisely because they aggregate financial and personal data. ENISA's threat reporting continues to show significant attacks against the finance sector. A rule that creates another compulsory database should therefore be treated as creating a new vulnerability, not merely as creating compliance.

ENISA, Threat Landscape: Finance Sector, 21 February 2025.

ENISA Threat Landscape 2025, finance-sector cybercrime dataset: data breaches represented 64% of cybercrime incidents in that dataset.

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)?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The most difficult categories are those where the token's technical form says less than the legal and economic relationship behind it: wrapped assets, governance tokens, hybrid tokens and tokenised claims on off-chain assets. Classification should ask what right exists, against whom, who can alter it, what backs it, and what happens if the intermediary or bridge fails.

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?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 8:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Material changes to governance, tokenomics, vesting, upgrade authority or control rights can alter the vulnerability a holder originally accepted. Those changes should therefore trigger clear, durable and machine-readable disclosure. A user should not have to discover after the fact that the trust relationship changed while the token name remained the same.

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?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
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	☐	☐	☐	☐	☐	☒

Please explain your answers to question 9:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Stablecoins are not a temporary anomaly to be contained until institutionally preferred digital money replaces them. They are an important experiment in separating money's functions: issuance, reserve management, redemption, custody, programmability and settlement no longer have to be controlled by the same institution. That separation is precisely why overly restrictive stablecoin regulation is dangerous. If reserve rules, licensing costs, geographic constraints and distribution rules make only a narrow class of institutionally approved structures economically viable, Europe can eliminate meaningful monetary experimentation without ever formally banning it.

The relevant question is not whether stablecoins should be unregulated. It is which vulnerability requires which authority. Regulate reserves as reserves, redemption as redemption, fraud as fraud and custody as custody. Do not use those legitimate concerns to justify control of every layer beneath them.

ECB Appia roadmap states central-bank money is to remain the anchor of the tokenised financial system and that Appia will shape the European ecosystem. Direction is right the execution is disturbing when Pontus is asked to preform all layers.

ECB comprehensive payments strategy discusses EU-governed, properly designed and regulated stablecoins as complementary private settlement assets. Properly designed, is where I take some issue. Again, Pontus being a private blockchain is exactly the wrong design. This design makes Appia already a failed trust mechanism since it is built upon a compelled single source of failure or undemocratic choice in selection of the controlling group.

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 how beneficial stablecoins would be for EU users:

	1 (not beneficial)	2 (moderately beneficial)	3 (neutral)	4 (beneficial)	5 (very beneficial)	Don't know - No opinion - Not applicable
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						
Others						

Please explain shortly your assessment and expectations in question 10 as regards the benefits of stablecoins for EU users and, where relevant, any potential risks:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The largest benefit is optionality: stablecoins can provide interoperable settlement without requiring every user or application to belong to the same bank, platform or ledger.

That optionality is itself a resilience property. Europe should be careful not to define 'safety' so narrowly that every safe route converges on the same licensed gateways and settlement anchor. A system with many compliant but genuinely independent routes is often more resilient than a system in which every route is supervised but shares the same failure domain.

2.2 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 11.1 To what extent do you think the calculation methods are relevant?

	1 (not at all relevant)	2 (slightly relevant)	3 (moderately relevant)	4 (mostly relevant)	5 (highly relevant)	Don't know - No opinion - Not applicable
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	☐	☐	☒	☐	☐	☐

Question 11.2 To what extent do you think the calculation methods are appropriately calibrated?

	1 (not at all appropriately calibrated)	2 (slightly appropriately calibrated)	3 (moderately appropriately calibrated)	4 (mostly appropriately calibrated)	5 (highly appropriately calibrated)	Don't know - No opinion - Not applicable
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 answers to question 11.1 and 11.2, 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):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I do not have sufficient issuer-level prudential data to recommend numerical recalibration of these thresholds. My recommendation is that capital requirements remain risk-sensitive and tied to the actual liabilities and authorities of the issuer rather than being used indirectly to privilege one technical architecture over another.

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:

	1 (not at all a factor)	2 (rather not a factor)	3 (neutral/ uncertain)	4 (rather a factor)	5 (a major factor)	Do not know
Market interests for ARTs	☐	☐	☒	☐	☐	
Licencing and regulatory requirements for ARTs	☐	☐	☐	☐	☒	

Please explain your answers to question 12:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The absence of authorised ARTs should be treated as information rather than proof of one cause. Regulation may be one factor, but product-market demand and competition from EMT structures also matter. The Commission should examine whether the framework is protecting against a demonstrated vulnerability or simply making one architecture uneconomic before increasing or relaxing requirements.

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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Where an ART is designed to maintain relatively stable value against referenced assets, its clearest consumer function is likely to be exchange, payment or settlement rather than speculative investment. The legal treatment should nevertheless follow the actual rights, redemption mechanics and risk accepted by the holder rather than the label attached to the token.

2.3 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**
- **“5” indicates that requirements should be made substantially more stringent (e.g. higher reserves, tighter risk controls, or enhanced safeguards)**

a) Please rate each aspect below as regard to non-significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
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)	☐	☐	☒	☐	☐	☐

b) Please rate each aspect below as regard to requirements for significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
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))	☐	☐	☐	☒	☐	☐

Please explain your answers to question 14 a) and b), 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):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I would not recommend broad numerical recalibration without prudential evidence. The important principle is diversification of dependency. Reserve rules should reduce redemption and credit risk without unintentionally concentrating reserves in a small number of banks and transferring systemic vulnerability there. Stress testing and transparent reserve composition are more defensible than architectural mandates that assume one custody or deposit structure is inherently safest. This also leaves open more diversified assets as backing.

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**
- **“5” indicates that requirements should be made substantially more stringent (e.g. higher reserves, tighter risk controls, or enhanced safeguards)**

a) Please rate each aspect below as regard to requirements for non-significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks (Article 36(1))	☐	☒	☐	☐	☐	☐
Legal and operational segregation of reserve assets from the issuer's own estate and from other token reserves (Article 36(2)–(3))	☐	☐	☒	☐	☐	☐
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)	☐	☐	☒	☐	☐	☐
Excessive exposure / concentration between bank and token (Article 36(4) MiCA) Do you consider the 1.5% binding limit adequate? (RTS)	☐	☐	☐	☒	☐	☐

b) Please rate each aspect below as regard to requirements for significant ARTs:

	1 (should be significantly relaxed)	2 (should be somehow relaxed)	3 (current framework appropriate)	4 (should be made somehow more stringent)	5 (should be made substantially more stringent)	Don't know - No opinion - Not applicable
Obligation to constitute and maintain a reserve of assets covering redemption and liquidity risks (Article 36(1))	☐	☐	☒	☐	☐	☐
Legal and operational segregation of reserve assets from the issuer's own estate and from other token reserves (Article 36(2)–(3))	☐	☐	☒	☐	☐	☐
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 EMTs (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 answers to question 15 a) and b), including your reasoning and any suggestions for recalibration or alternative approaches:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The same principle applies to EMTs: the objective should be reliable redemption and resilient reserves, not compulsory dependence on a particular institutional layer. Requirements should be assessed for the vulnerability they reduce and the vulnerability they create elsewhere, including concentration of deposits in banks.

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?

- ☐ 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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 16, including your reasoning and any suggestions for other/alternative approaches:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I would favor functional ring-fencing of the assets and claims necessary to protect EMT holders rather than automatically requiring a separate legal entity or reproducing the non-bank reserve model inside a credit institution. The question should be whether holders have clear, enforceable and insolvency-resilient rights, not whether every issuer uses the same organizational form.

2.4 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](#) 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, and if so how?

Please rate each quantitative criteria thresholds on a scale from 1 to 5, where

- **“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)**

a) Please rate how each quantitative criteria thresholds used to classify EMTs should be adjusted:

	1 (significantly decreased)	2 (somewhat decreased)	3 (kept as is)	4 (somewhat increased)	5 (significantly increased)	Don't know - No opinion - Not applicable
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)	☐	☐	☒	☐	☐	☐

b) Please rate how each quantitative criteria thresholds used to classify ARTs should be adjusted:

	1 (significantly decreased)	2 (somewhat decreased)	3 (kept as is)	4 (somewhat increased)	5 (significantly increased)	Don't know - No opinion - Not applicable
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 answers to question 17 a) & b), including your reasoning and any suggestions for other/alternative approaches:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I do not have evidence supporting numerical recalibration. Significance should not rely on size alone. A token's systemic importance also depends on concentration, substitutability, redemption dependency, interconnectedness and the authority its issuer can exercise over users or markets.

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

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain how you think the qualitative criteria for classifying EMTs or ARTs as “significant” should be adjusted:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Qualitative criteria should explicitly consider concentration of dependency and substitutability. A token can become systemically important before a single numerical threshold captures it if essential settlement, collateral or payment activity becomes dependent on one issuer or infrastructure.

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

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please specify which criteria or metrics and explain why:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Add measures of substitutability, concentration of settlement activity, reserve/custodian concentration, interoperability dependencies and the share of critical applications for which no credible alternative exists. Systemic significance is ultimately about correlated vulnerability, not only market capitalization or transaction count.

2.5 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?

a) for EMTs:

- ☐ No, interest and interest-equivalent remuneration should continue to be prohibited
- ☐ Yes, interest or interest-equivalent remuneration should be allowed under defined conditions
- ☒ Yes, interest or interest-equivalent remuneration should be allowed fully
- ☐ Don't know / no opinion / not applicable

Please explain why you think interest or interest-equivalent remuneration should be allowed for EMTs, (including any benefits and risks) and specify the conditions under which it should be permitted:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A blanket prohibition is another example of regulating the capability rather than the vulnerability. If remuneration creates maturity transformation, liquidity risk, misleading representations or an investment-like exposure, regulate those risks directly.

The danger of prohibition-by-category is that it protects incumbent product boundaries from experimentation. The digital age should not reproduce a financial architecture in which sophisticated structures remain available to institutions and wealthy participants through complex wrappers while simpler programmable alternatives are prohibited for everyone else in the name of protection.

b) for ARTs:

- ☐ No, interest and interest-equivalent remuneration should continue to be prohibited
- ☐

Yes, interest or interest-equivalent remuneration should be allowed under defined conditions

- ☒ Yes, interest or interest-equivalent remuneration should be allowed fully
- ☐ Don't know / no opinion / not applicable

Please explain why you think interest or interest-equivalent remuneration should be allowed for ARTs, (including any benefits and risks) and specify the conditions under which it should be permitted:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Same reasoning as above.

EBA's continuing work on tax-integrity and dividend-arbitrage schemes illustrates that complexity in traditional finance has itself been used to exploit regulatory and tax seams.

2.6 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?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I do not have sufficiently direct issuer-level redemption experience to provide evidence on operational processing problems.

Question 22. If you hold EMTs and wish to dispose of them, which of the following options would you most likely choose?

a) In a normal market situation

- ☒ I would likely spend them (e.g. on goods or services)

- ☐ I would likely sell or exchange them with a broker or at a trading venue
- ☐ I would likely turn to the EMT issuer or his agent to exercise my statutory redemption right
- ☐ Don't know / no opinion / not applicable

b) In a stressed market situation

- ☒ I would likely spend them (e.g. on goods or services)
- ☐ I would likely sell or exchange them with a broker or at a trading venue
- ☐ I would likely turn to the EMT issuer or his agent to exercise my statutory redemption right
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 22 a) and b):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Normal market: exchange/spend. Stressed market: exercise the direct redemption right with the issuer. A redemption right matters most precisely when secondary-market liquidity and confidence are under stress.

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	Don't know - No opinion - Not applicable
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	☐	☐	☒	☐
Supervisory powers to intervene in or trigger redemption plans	☐	☒	☐	☐

Please explain your assessment to question 23, 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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The right itself should remain strong and predictable. The most useful improvements are operational: clear timing, transparent procedures and evidence that reserves and redemption mechanisms work under stress. A nominal right that cannot be exercised when vulnerability materialises is not meaningful protection.

2.7 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 plans.

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:

a) Current MiCA requirements for ARTs

				Don't know -
--	--	--	--	-----------------

	Weaken	Keep as is	Strengthen	No opinion - Not applicable
Recovery plans	☐	☒	☐	☐
Redemption plans	☐	☒	☐	☐

b) Current MiCA requirements for EMTs

	Weaken	Keep as is	Strengthen	Don't know - No opinion - Not applicable
Recovery plans	☐	☒	☐	☐
Redemption plans	☐	☒	☐	☐

Please explain your assessment to question 24 a) & b), including if a different approach is warranted for significant vs non-significant tokens, and share any suggestions for adjustments you may have:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Recovery and redemption plans should be proportional to the scale and dependency created by the token. For significant tokens, plans should be tested rather than merely documented. The goal is inspectable evidence that the issuer can honor the vulnerability it has asked holders to accept under realistic stress.

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:

	1 (not at all appropriate / desirable)	2 (slightly (moderately appropriate / desirable)	3 (moderately appropriate / desirable)	4 (mostly (moderately appropriate / desirable)	5 (highly (moderately appropriate / desirable)	Don't know - No opinion - Not applicable
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	☐	☐	☐	☐	☐	☒

Please explain your ratings in question 25, including potential benefits, risks, or implementation challenges:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The strongest measure is clear insolvency-resilient ring-fencing for token holders. Direct central-bank reserve access may reduce intermediary concentration where appropriately governed. Emergency liquidity or resolution support should not socialise private risk without corresponding prudential obligations and accountability.

Question 26. How appropriate is it to require EMT-issuing EMLs to hold 30-60% of their reserve assets in bank deposits?

- ☒ 1 - Not at all appropriate / desirable
- ☐ 2 - Slightly appropriate / desirable
- ☐ 3 - Moderately appropriate / desirable
- ☐ 4 - Mostly appropriate / desirable
- ☐ 5 - Highly appropriate / desirable
- ☐ Don't know / no opinion / not applicable

Please explain your ratings in question 26 and add any suggestions for recalibration or alternative approaches:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I would not preserve a fixed 30–60% commercial-bank deposit requirement as the default architecture. This is the Trust Architecture problem in miniature. The rule is presented as reducing reserve risk, but it also compels stablecoin issuers to place a large share of their vulnerability inside the banking system. Regulation has not removed risk. It has selected the institution that will receive it. That choice requires evidence. It should not be presumed safe merely because the receiving institution is regulated.

EU authorities themselves continue to report serious AML/CFT and operational weaknesses inside regulated financial institutions. From April 2024 to March 2025, the EBA's EuReCA reporting recorded 1,279 serious deficiencies or material weaknesses exposing financial institutions to ML/TF risk, most commonly involving customer due diligence, systems and controls, and suspicious transaction reporting. In the following reporting window, authorities still recorded 833 material weaknesses.

The lesson is not that banks are uniquely unsafe. It is that regulated does not mean riskless. Stablecoin reserve regulation should therefore specify liquidity, quality, diversification and redemption outcomes rather than compel dependence on one institutional layer.

2.8 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)	Don't know - No opinion - Not applicable
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 to what other potential use case(s) you refer in your answer to question 27:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Democratized global savings.

Please explain your answers to question 27:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Global stablecoins are most valuable where money must cross institutional or national boundaries without rebuilding the settlement stack for every jurisdiction. Their benefit comes from interoperability and shared settlement. Their risk comes from concentrating dependency on a small number of issuers and reserve structures. Both facts can be true at once.

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?

	1 (not important at all)	2 (moderately important)	3 (neutral / no clear preference)	4 (rather important)	5 (highly important)	Don't know - No opinion - Not applicable
EU-based and licenced stablecoins Issuers	☐	☐	☐	☐	☒	☐
EU-based and licenced CASPs	☐	☐	☐	☒	☐	☐

Please explain your answers to question 28:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

European users should not be placed behind a regulatory wall from global stablecoin liquidity.

The EU can impose obligations on actors that actually provide regulated services to EU customers. It should not turn those intermediaries into universal permission gates controlling which lawful assets Europeans may hold or which public networks they may use.

A CASP license should establish obligations for the CASP. It should not silently become a license for the customer's economic life.

Question 29. Based on your experience and assessment, how significant are the following risks associated with a multi-issuance model^[3] of global stablecoins for the EU financial system?

³Under 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.

	1 (irrelevant)	2 (rather not relevant)	3 (neutral)	4 (rather significant)	5 (very significant)	Don't know - No opinion - Not applicable
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						

Please explain the reasoning behind your ratings in question 29. Describe the nature and importance of these risks, the underlying assumptions, market dynamics, or regulatory factors informing your view:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The material risks arise where fungibility masks different legal claims or reserve pools. Users should be able to know which entity owes them what, where the backing sits, and whether redemption remains enforceable under stress. The solution should focus on those claims and dependencies rather than attempting to infer the geographic identity of every self-custodied token holder.

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
- ☐ Don't know / no opinion / not applicable

Please explain the reasons for your response to question 30 and describe the potential implications for the EU market and relevant stakeholders:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Multi-issuance should remain possible if the legal claim, reserve responsibility and redemption obligation are clear to the holder. Prohibiting the model because cross-border trust is difficult would sacrifice interoperability rather than solve the underlying problem. The correct response is to make the trust boundaries inspectable.

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.

a) Does this approach continue to be justified in view of market developments?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

b) Does it discourage the international role of the euro?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 31 a) & b):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Denominating a token in euros should not by itself make every issuance and use anywhere in the world an EU-regulated offering.

There is a deeper strategic contradiction here. Europe says it wants the euro to remain internationally relevant, while simultaneously risking an architecture in which digital use of the euro is acceptable only when it enters through European-approved structures. Monetary relevance comes from people choosing to use a currency, not from making the currency a regulatory perimeter.

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

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The advantage is strong protection and a clear regulatory perimeter for EU users. The disadvantage is that an overly expansive perimeter can make euro-denominated digital money less attractive globally and push innovation toward other currencies. Europe should protect users without making use of the euro conditional on submission to an architecture designed for domestic distribution.

2.9 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?

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

	1 (not at all)	2 (to a small extent)	3 (to a moderate extent)	4 (to a large extent)	5 (to a very large extent)	Don't know - No opinion - Not applicable
Strengthening EU payment autonomy in retail payments	☐	☐	☒	☐	☐	☐
Strengthening EU payment autonomy in wholesale payments	☐	☐	☐	☒	☐	☐
Enhancing the international role of the euro	☐	☐	☐	☒	☐	☐

Please explain your answers to question 33:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Euro stablecoins can strengthen the international role of the euro if they remain usable across genuinely different infrastructures.

Strategic autonomy becomes dangerous when it is allowed to mean institutional enclosure. The ECB openly describes Appia as shaping Europe's tokenised financial architecture, preserving central-bank money as the anchor and strengthening strategic autonomy. Pontes and Appia are described as one strategy, with Pontes ultimately becoming a core component of the Appia ecosystem.

That may be a coherent institutional objective. It should not become the only economically viable architecture. Europe should compete by making the euro useful, interoperable and trustworthy, not by making alternative routes progressively harder to use.

Pontes and Appia are the right idea and the wrong execution.

2.10 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:

	1 (not at all effective)	2 (slightly effective)	3 (moderately effective)	4 (rather effective)	5 (highly effective)	Don't know - No opinion - Not applicable
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)	☐	☐	☐	☐	☐	☒

Please explain your answers to question 34:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Safeguards are strongest when they address a specific vulnerability such as redemption, reserve quality or misrepresentation. Broad intervention powers and usage restrictions should be used carefully because they can create concentrated discretionary authority. The more powerful the control, the clearer its trigger, scope, evidence and appeal should be.

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 35, including any specific remarks with regard to tokens held in unhosted wallets:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Hosted accounts can provide jurisdictional information. A self-custodial bearer asset generally cannot provide reliable residence information without attaching identity or surveillance infrastructure to the holder. That limitation should be accepted where it is intrinsic to the architecture. The solution cannot be to make every wallet persistently identifiable simply because regulation wants a jurisdiction field. IP addresses, metadata, device identifiers and transaction graphs already make privacy fragile. Requiring additional identity linkage increases the consequences of breach, coercion and physical targeting. The fact that information can be collected does not establish that an authority should possess it.

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

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 36:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A fungible token should not lose a core redemption right because it crossed an invisible jurisdictional boundary, particularly where determining the holder's location would require intrusive identity infrastructure. If an issuer has created a redeemable claim, the cleanest trust relationship is that the claim follows the token, subject to lawful sanctions and other specific restrictions.

2.11 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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 37:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The concern is structurally valid. A multi-jurisdiction reserve creates dependencies on banks, legal entities, supervisors and transfer rules that may behave differently under stress. Those dependencies should be disclosed and stress-tested rather than assumed away.

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

	1 (highly ineffective)	2 (rather ineffective)	3 (neutral / uncertain)	4 (somewhat effective)	5 (highly effective)	Don't know - No opinion - Not applicable
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	☐	☐	☐	☐	☐	☒

Please explain your answers to question 38:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I strongly oppose making a hosted wallet, CASP relationship or certified intermediary a condition for exercising a basic redemption right.

That would turn self-custody from a legitimate ownership model into a second-class status. It would also create exactly the control loop Trust Architecture warns against: first impose identity and intermediation as a condition of access, then point to the resulting intermediated system as evidence that intermediation is necessary.

If the concern is reserve distribution, disclose and stress-test reserves. If the concern is sanctions, enforce specific lawful sanctions. If the concern is fraud, prosecute fraud. Do not solve each problem by requiring every person to enter a permanent institutional relationship.

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 the redemption rights in MiCA as listed above or in any other way:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Differentiated redemption rights would create an economic penalty for refusing institutional custody. That is not neutral consumer protection. It is an incentive structure designed to move people into a more controllable architecture.

The walk-away test matters here. A choice is not meaningful merely because the law says I may self-custody if exercising that choice causes me to lose basic rights attached to the asset. The door can remain technically unlocked while the cost of walking through it becomes prohibitive.

Question 40. Do you see merit in introducing an equivalence regime for global stablecoins in the EU?

- ☐ Yes but only if other mitigation measures are not introduced
- ☒ Yes, in addition to mitigation measures
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please provide reasons for your response to question 40, including any perceived advantages or disadvantages of equivalence regimes:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Equivalence can reduce duplicated regulation where another jurisdiction achieves genuinely comparable outcomes. It should be outcome-based rather than requiring institutional or technical structures identical to the EU model. Mutual recognition is itself a trust architecture: evidence of equivalent protection should substitute for redundant control.

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 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?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

An equivalence regime should rely on third-country rules for prudential and conduct obligations where outcomes are demonstrably comparable, while preserving direct EU requirements for activities actually directed at EU users. Equivalence should be reviewable and evidence-based, not a political label or a demand that another jurisdiction copy the EU architecture.

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?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
Authorisation of ARTs and EMTs issuers	☐	☒	☐	☐	☐	☐
Prudential requirements	☐	☒	☐	☐	☐	☐
Governance arrangements	☐	☒	☐	☐	☐	☐
Obligations in respect of specific crypto-asset services	☐	☒	☐	☐	☐	☐

Please explain your answers to question 42:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Reduce duplicate reporting and authorisation evidence, permit reusable verified information, and calibrate obligations to scale and actual authority. Simplification should not mean weaker accountability. It should mean asking for the same proof once rather than repeatedly collecting the same underlying data. This is the copy problem creating more attack vectors.

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)	Don't know - No opinion - Not applicable
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 to question 43 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):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I do not have sufficient issuer-level implementation evidence to score each RTS reliably. The general principle should be proportionality by actual risk and reuse of already-verified information rather than repeated documentary compliance.

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 44:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Standardization is useful where it makes evidence portable and comparable. Reporting formats should be machine-readable and minimize duplicate collection. A common schema for reserve, redemption, control and material-risk information would improve accountability without requiring every participant to rebuild the same verification process.

PART 3. The appropriateness of the legal framework for crypto-asset service providers (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 is still in place 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 (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).

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 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?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 45:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The service list must not become a mechanism for progressively converting every useful interface into a regulated intermediary.

The key test is authority. Does the actor custody assets, execute on behalf of the user, make discretionary decisions, control settlement, or make material representations on which the user is expected to rely? If yes, obligations can follow that authority.

If the actor merely publishes software, writes open-source code or gives the user a tool through which the user exercises their own authority, regulation should not manufacture an intermediary because an intermediary is easier to supervise.

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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I would explicitly exclude neutral software development, protocol publication and non-custodial wallet creation from the CASP perimeter unless the provider separately exercises a regulated function.

This is not a technicality. If regulation forces software developers to acquire control capabilities merely so that

they can satisfy compliance obligations, regulation has changed the architecture. It has created the controller it then claims to regulate.

Being identifiable is not authority. Being able to write code is not custody. Publishing an interface is not possession of the user's assets.

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 47:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Appropriateness tests should not become another permission gate for adults using their own assets. Where a provider recommends a complex product, manages discretion or creates leverage, stronger duties can be justified. Where a person simply instructs an intermediary to execute a lawful transaction, the provider should not become a paternal authority deciding whether the customer is sufficiently sophisticated to exercise their own economic agency. Traditional finance already contains extensive gated categories, professional-investor distinctions and complex exemptions that are far easier for well-resourced actors to navigate. Digital finance should not reproduce that asymmetry by default.

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?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 48, specifying what in your view

could be a relevant alternative:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

A globally accessible protocol or website should not be presumed to be unlawfully soliciting Europeans merely because Europeans can reach it.

The alternative is a European internet in which every global developer must either submit to EU permission or technically exclude Europeans. That is not technology neutrality. It is jurisdiction by accessibility, and it predictably favors large firms capable of maintaining global compliance machinery.

3.2 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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 49:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Prudential requirements should follow the vulnerability created by the service, not the regulator's desire for a familiar institutional form.

A custodian controlling customer assets, an exchange holding counterparty exposure and a non-custodial interface are not variations of the same risk. Treating them as though they are selects for large incumbents able to absorb compliance costs while excluding architectures that deliberately remove custody and counterparty dependence.

That is the opposite of risk-sensitive regulation.

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)**

	1	2	3 (kept roughly as is)	4	5	Don't know - No opinion - Not applicable
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 answers to question 50, indicating, if necessary, how the amount of minimum capital should it be recalibrated:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Capital can protect customers where a firm actually creates balance-sheet, custody or operational exposure. But capital requirements also operate as barriers to entry. The Commission should therefore be able to show which customer vulnerability each capital requirement covers. A requirement that simply makes small entrants nonviable while leaving the underlying risk unchanged is not consumer protection. It is market structure.

3.3 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? What kind of action would be appropriate?

- ☒ The existing approach should be maintained
- ☐ There should be enhanced oversight and coordination in relation to such entities
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 51:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Large traditional financial groups are evidence that institutional scale and regulatory status do not eliminate conflicts, money-laundering risk or sophisticated regulatory arbitrage. The EBA has continued to identify serious AML/CFT weaknesses inside regulated institutions, and its work on dividend-arbitrage schemes exists because complex, highly regulated markets still produced structures capable of exploiting legal and tax seams. The correct lesson is to supervise the actual concentration of authority and conflicts, not to assume that putting more activity inside a regulated group makes the system inherently safer. EBA, Operational risks and resilience: 1,279 material AML/CFT weaknesses reported in the 12 months to March 2025. EBA, Cum-Ex/Cum-Cum inquiry and 2025 tax-integrity peer review.

3.4 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?

	Yes	No	Don't know - No opinion - Not applicable
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	☒	☐	☐

Please specify what kind of reporting would be useful and how often?

Please explain:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I answered yes, but.

Supervisors should collect information that is necessary to observe a defined vulnerability. They should not collect everything that technology makes collectable.

Every reporting mandate creates a dataset, a custodian and a future use case for that information. Financial and identity data are valuable attack targets. The presumption should therefore be data minimisation: collect what is necessary, retain it only as long as necessary, and require a clear purpose for expanding the dataset. ENISA finance-sector threat reporting; ENISA notes financial institutions process significant volumes of financial and personal data and remain high-value cyber targets. We do not want protections to increase blast radius.

3.5 Environmental and sustainability reporting

MiCA strengthens transparency on the environmental impact of crypto-assets. It does so by

- 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
- 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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 53:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Environmental disclosure is useful when comparable and decision-relevant. It should distinguish protocol-level consensus characteristics from the specific activities of issuers and service providers, and avoid repeatedly attributing the same network-wide footprint to every application using the network.

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?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Cybersecurity cannot be separated from the amount of power and information regulation concentrates. The EU can require stronger security controls and should. But a secure central repository of identity and transaction data remains a repository whose compromise, misuse or compelled disclosure can harm millions of people at once.

ENISA continues to document significant cyber threats against financial institutions. This should make the Commission cautious about regulatory designs that require more identity data, more transaction metadata and more persistent linkage to be held by more intermediaries.

The privacy question is not only whether the database is well protected. It is whether the database needed to exist in that form at all.

ENISA Threat Landscape 2025 and Threat Landscape: Finance Sector (2025).

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 bring sufficient clarity or are there other issues that remain to be addressed?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 55:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The objective should be one clear obligation for one real function. Where the same activity is simultaneously captured by multiple frameworks, the result should not be duplicate authorization or data collection. Clarification should continue to follow economic function and actual authority.

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?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Question 56.1 What are the advantages and disadvantages of focusing on EU liquidity or full access to global liquidity?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Europe should not mistake fragmentation from the rest of the world for sovereignty.

If EU rules make global liquidity reachable only through a shrinking set of highly regulated gateways, those gateways acquire enormous power over what Europeans may buy, sell and use. The fact that the gateway is supervised does not remove that vulnerability.

The EBA's own work on de-risking shows the predictable institutional response when compliance risk becomes too costly: institutions exclude categories of customers rather than manage the underlying risk. The same incentive can operate at the asset and protocol level.

EBA, Opinion on de-risking, 5 January 2022.

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)	Don't know - No opinion - Not applicable
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 in question 57 and suggest how rules could be made simpler and more proportionate (e.g. legislative clarification, supervisory guidance, industry standards):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Proportionality should be measured against actual authority, not simply firm size.

A small custodian can create custody risk. A large software publisher may create none. A protocol with an administrator key may contain concentrated authority. A widely used immutable contract may not.

MiCA should stop treating institutional recognisability as a proxy for risk. The thing that can be licensed is not automatically the thing that should be controlled.

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?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
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 in question 58 and suggest how rules could be made simpler and more proportionate:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I do not have sufficient implementation evidence to score each technical standard reliably. Across Level 2, the priority should be interoperable reporting, avoidance of duplicate evidence and proportionality to the authority and vulnerability created by the service.

PART 4. Policy areas beyond the current scope of MiCA

The following sections seek feedback from stakeholders on these areas, as well as some additional topical issues that are not currently directly regulated by MiCA

4.1 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 (MiCA Recital 22: "Where crypto-asset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation").

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?

a) Exchange services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**



DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**

- ☐ Don't know / no opinion / not applicable

b) Payments and transactions services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☒ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

c) Trading and investment services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☒ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

d) Lending and borrowing services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☒

DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**

- ☐ Don't know / no opinion / not applicable

e) Custody services

- ☐ DeFi applications present **limited interest** and are **moderately used** for this service
- ☐ DeFi applications present **important potential benefits** for this service but their **use remains limited** due to some non-mitigated weaknesses
- ☐ DeFi applications present **important benefits** for this service and are **already significantly used**, despite **important non-mitigated weaknesses**
- ☒ DeFi applications present **important benefits** for this service, they are **already significantly used** and **present limited risks**
- ☐ Don't know / no opinion / not applicable

Please detail the benefits or weaknesses you associate with the use of DeFi applications for these different services in question 59, and the actions you would consider appropriate to optimise these benefits or address the possible issues they raise:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

DeFi's most important contribution is not yield. It is architectural competition.

It demonstrates that custody, execution, settlement, liquidity provision, lending and governance can sometimes be separated rather than bundled inside one institution. That does not make DeFi trustless. Smart-contract bugs, admin keys, oracle dependence, governance capture and economic exploits are real vulnerabilities. But the existence of those vulnerabilities does not justify rebuilding the intermediary that the architecture removed.

Traditional finance has not earned a presumption of safety simply because its failures happen inside licensed institutions. EU authorities continue to record serious AML/CFT deficiencies in regulated financial institutions, regulatory-arbitrage problems and cyber incidents. Europol reports that criminal networks exploit weaknesses in financial systems using cryptocurrencies, money-laundering techniques and legal business structures. Crime routes around architecture.

The regulatory question should therefore be: where is the actual authority and vulnerability in this particular system? Not: where can we insert a gatekeeper? The best lock in the world is an annoyance to the criminal but an impossible barrier to the just.

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

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
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 to question 60:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The risks are real. The asymmetry in how they are treated is the problem.

A smart-contract exploit is treated as evidence that permissionless infrastructure is dangerous. A major failure inside a regulated institution is usually treated as evidence that the institution needs another control.

MiCA should apply the same analytical standard to both.

EU authorities recorded 1,279 serious AML/CFT deficiencies in financial institutions in the 12 months to March 2025. EBA reviews have continued to identify weaknesses in risk assessment and enforcement, and divergent supervisory approaches have created opportunities for regulatory arbitrage. None of this means regulated finance should be abolished. It means 'regulated' cannot be used as a synonym for 'safe'.

DeFi should be judged against the risks it actually creates and the risks it removes, not against an imaginary traditional system in which licensing has eliminated crime, failure and corruption.

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?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
Existence of an identifiable intermediary (person or group of persons) providing a crypto-asset service	☐	☐	☐	☒	☐	☐
Presence of control by an identifiable person e 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	☐	☐	☒	☐	☐	☐
DeFi protocol code is not open source	☐	☐	☐	☒	☐	☐
Marketing of a DeFi protocol by an identifiable entity or person	☒	☐	☐	☐	☐	☐
Other	☐	☐	☐	☐	☐	☒

Please explain your answers to question 61:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Decentralization must be judged by effective authority.

Who can seize assets? Who can change the rules? Who holds administrator keys? Who can upgrade the contract? Who controls governance? Who can prevent a transaction? Who can reverse one?

Those are regulatory facts.

The identity of a developer is not.

The existence of a website is not.

Marketing is not.

If regulation treats identifiability as control, it will manufacture intermediaries by imposing duties on whoever can be found. That is administratively convenient and architecturally destructive.

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 62:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No.

This proposal is the clearest example of control creep in the review.

If a protocol is genuinely decentralised, MiCA should not solve the regulator's inability to control it by controlling every regulated gateway through which Europeans can reach it.

That does not regulate the protocol's vulnerability. It creates a new authority: the CASP becomes the institution deciding which lawful protocols the user may access.

Europe does not need to ban permissionless finance if it can make every practical gateway ask permission on the user's behalf.

The Commission should recognize the cumulative architecture being created. CASPs are licensed. Stablecoin issuers are heavily constrained. The review then considers certification of DeFi and non-custodial software and restrictions on CASP connectivity. At the same time, the Eurosystem is openly shaping the architecture, standards and governance of Europe's tokenized financial ecosystem through Pontes and Appia while preserving central-bank money as its anchor.

Taken together, this is not neutral scaffolding around an open system. It is an emerging permission architecture.

The walk-away test is simple: can an individual reject the institutional gateway and still retain a practical lawful route to use their own assets? If the answer progressively becomes no, formal freedom remains while meaningful freedom disappears.

ECB, Appia roadmap, 11 March 2026: Appia will 'shape' development of the European tokenised financial ecosystem and preserve central-bank money as anchor.

ECB, 23 March 2026: Pontes and Appia 'form a single strategy'; Pontes is expected to become a core component of the Appia ecosystem.

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 63:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

No.

Mandatory certification reverses the presumption that should govern an open society. The protocol becomes guilty until an approved institution proves it innocent.

Certification is not safety. Europe already has highly regulated financial institutions, extensive AML rules, prudential supervision and data-protection law, yet EU authorities continue to document money-laundering control failures, regulatory arbitrage, tax-integrity problems and major cyber threats.

The lesson is not that certification is useless. It is that certification is evidence, not absolution.

A voluntary certificate can tell me who inspected the code, what they inspected and what they found. The moment the certificate becomes the legal condition for access, the certifier becomes a gatekeeper. The vulnerability has moved from the protocol into the certification institution.

That is precisely the kind of trust transfer MiCA should be required to analyze before imposing it, and then rightly reject. Here a standard can be beneficial, so long as it is open to change over time as evidence arises.

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

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
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 answers to question 64:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I strongly oppose these proposals.

A non-custodial wallet is a tool through which an individual exercises their own authority. Requiring institutional certification of that tool before it may be distributed or used reverses the relationship. The individual no longer begins with authority over their own asset. Their ability to exercise that authority becomes conditional on institutional approval of the software.

Embedded compliance creates the same problem at the protocol layer. It can force neutral infrastructure to acquire surveillance, blocking or identity functions it did not previously possess. Regulation then points to those newly created control functions as the place where regulatory obligations should sit.

This is not regulating an existing intermediary. It is manufacturing one.

It also creates security consequences. Persistent wallet identity, IP metadata, location data and transaction linkage can make individuals easier to profile, coerce or physically target. Data minimization is therefore not merely a privacy preference. It is personal security architecture.

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

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
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 answers to question 65:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Certification should be plural, voluntary and contestable.

The proposal to prevent CASPs from connecting users to uncertified protocols is particularly dangerous because it converts an informational tool into access control.

The sequence is predictable:

First certification is useful evidence.

Then certified systems are treated as safer.

Then regulated institutions are discouraged from touching uncertified systems.

Then access to uncertified systems becomes a compliance risk.

Eventually the individual remains legally free to use the protocol while every practical regulated route to it has disappeared.

That is the Double-Edged Sword problem. No single step needs to announce capture. The assembled architecture produces it.

A strong trust architecture permits multiple independent assessments and lets evidence accumulate. It does not appoint one master authority whose absence of approval becomes proof of danger.

4.2 Staking, lending and borrowing of crypto-assets

This section seeks stakeholders' feedback on staking, lending and borrowing of crypto-assets, currently not addressed in MiCA regulation ([EBA-ESMA joint report on recent developments in crypto-asset markets - January 2025](#)). 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?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 66:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Staking should not become another excuse to regulate a protocol function as though it were automatically an intermediated financial service.

Where a provider takes custody, pools assets, makes guarantees, exercises discretion or misrepresents risk, regulate those actions. Where a person directly participates in a protocol with their own assets, the absence of an intermediary should be respected rather than treated as a regulatory defect.

Question 67. Do you think that lending and borrowing of crypto-assets should be regulated?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 67:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Do not regulate 'crypto lending' as though the technical substrate itself creates the vulnerability.

If an intermediary takes custody, rehypothecates assets, sets discretionary terms, obscures conflicts or makes misleading representations, regulate those acts.

If autonomous code matches willing counterparties without custody or discretionary control, forcing a license onto an identifiable developer does not make the transaction safer. It merely gives the state someone to punish. This distinction matters because traditional regulated finance has not eliminated lending abuse, money laundering, tax arbitrage or unequal access. The EBA continues to report material AML/CFT weaknesses in regulated financial institutions, and Europol continues to document criminals exploiting legal business structures as well as cryptocurrencies.

The answer to imperfect decentralized systems cannot be to reproduce the weaknesses of the incumbent system while removing the individual's ability to walk away from it.

4.3 Non-fungible tokens

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 68:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

NFTs should not become a regulated financial category merely because they use the same technical substrate as financial crypto-assets. Where an NFT is functionally a financial instrument or a service involves custody, fraud or regulated financial activity, existing functional rules can apply. Regulation should follow the right and vulnerability, not the file format.

4.4 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?

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Please elaborate on your answer to question 69:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Prediction markets can aggregate dispersed information and provide useful signals, but they also create manipulation, consumer-protection and market-integrity risks depending on the market and operator. The DLT implementation is not itself the defining risk. Regulation should focus on the economic activity and the authority exercised by the operator.

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
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 70:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The governing regime should follow the economic nature of the contract. Using a smart contract does not turn a wager or derivative into a different economic activity. Technology neutrality requires the same activity to receive comparable treatment regardless of settlement technology.

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

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Requirements should focus on market integrity, truthful resolution criteria, custody where applicable, conflicts of interest, manipulation and clear disclosure of how outcomes are determined. The resolver/oracle is a critical trust point and should be transparent and contestable where possible.

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

- ☒ By MiFID
- ☐ By MiCA
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 72:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Perpetual futures are economically derivatives. Their use of crypto-assets as an underlying or DLT as infrastructure should not move them into a different regulatory logic. Technology neutrality argues for MiFID treatment where the product is functionally a derivative.

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

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Apply requirements appropriate to leveraged derivatives: margin, liquidation transparency, conflicts, market integrity, custody and clear risk disclosure. Particular attention should be paid to oracle design and liquidation mechanisms because these are technical trust dependencies that can materially alter the user's exposure.

4.5 Tokenised deposits

The terms 'tokenised deposit' and 'deposit tokens' are not defined terms and are sometimes used interchangeably ([EBA Report on tokenised deposits - December 2024](#)). 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:

	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)	Don't know - No opinion - Not applicable
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	☐	☐	☐	☐	☒	☐

Please explain your answers to question 74:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Tokenized deposits can be useful, particularly for wholesale settlement. The danger is that their usefulness becomes an argument for rebuilding digital finance around bank membership.

A tokenized deposit remains a bank liability. If it can only circulate among customers of the issuing bank or inside institutionally controlled infrastructure, tokenization has changed the technology without changing the trust architecture.

The more interesting future is interoperability among genuinely different forms of money and settlement, where users and institutions can choose which vulnerabilities they are willing to accept.

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

Maximum 2 selection(s)

Please select as many answers as you like

- ☐ 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

Please explain why the case(s) you selected in your answer to question 75 are the most promising in the EU:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Delivery-versus-payment and intraday liquidity management are the most promising because they directly reduce time-based counterparty vulnerability. Atomic settlement can replace a period of trust in future

performance with verifiable simultaneous exchange. That is exactly where cryptographic infrastructure adds value.

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

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The largest constraints are fragmentation, interoperability, uncertain legal treatment, limited common settlement infrastructure and the temptation for each institution or jurisdiction to build another closed network. Tokenization adds little if every tokenized deposit can only move inside its issuer's private domain.

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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The EU should provide legal certainty and interoperability without prescribing the topology of the network. This is especially important because the Eurosystem is simultaneously developing Pontes and Appia and openly describes Appia as shaping Europe's tokenized financial ecosystem. The ECB has said Pontes and Appia form a single strategy and that Pontes may evolve into a core component of the Appia ecosystem. That makes architectural neutrality more, not less, important. Public, private, permissioned and permissionless systems should be allowed to demonstrate equivalent outcomes. The institution designing one major settlement route should not, through regulation, also determine that competing routes are illegitimate.

Question 78. Do tokenised deposits raise any specific issues under the CRD /CRR framework?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 78:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I do not have sufficient prudential data to recommend CRD/CRR recalibration. The core principle is that tokenization should not change the underlying prudential treatment merely because the record of the deposit moves to DLT, unless the new architecture creates a demonstrably different operational or liquidity vulnerability.

Question 79. Do tokenised deposits raise any questions and challenges from a deposit insurance perspective?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

Please explain your answer to question 79:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Deposit insurance should attach clearly to the legal claim, not become ambiguous because the claim is represented by a token. Users should be able to know whether a tokenized deposit is insured, against which bank, and whether transferring the token changes that status. The ledger should clarify the trust relationship, not obscure it.

4.6 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^[4]. 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.

⁴ In “complete tokenisation” possession can equate to legal ownership over the asset it represents if the legal system recognises the token as the asset’s representation; the “indirect tokenisation” where the legal ownership depends on the intermediary entity or legal structure, not just the token; and the “incomplete tokenisation” where the token might only act as evidence or an interface to rights that are legally held off-chain. [X. Lavayssière, “Legal Structures of Tokenised Assets”. European Journal of Risk Regulation.](#)

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

- ☒ Yes
- ☐ No
- ☐ Don’t know / no opinion / not applicable

Question 80.1 Which of the following issues are most significant?

	1 (none or not significant)	2 (low)	3 (moderate)	4 (high)	5 (very high)	Don't know - No opinion - Not applicable
Issuing a crypto-asset token in compliance with national law	☐	☐	☒	☐	☐	☐
Issuing a tokenised financial instrument in compliance with national law	☐	☐	☒	☐	☐	☐
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 answers to question 80.1 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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

There is material uncertainty because technical control of a token and legal ownership are not always the same thing. This is a fundamental trust problem: the ledger can prove who controls a key while the law may assign the underlying right elsewhere. Priority should therefore be given to ownership/entitlement, third-party effect, custody, insolvency and enforceability.

Yes. The most significant uncertainty is the gap between a cryptographic fact and a legal fact.

Control of a private key can demonstrate the technical ability to transfer a token. It does not necessarily establish legal ownership, beneficial entitlement, authority to dispose of the asset, or the rights of third parties. This distinction becomes critical in theft, compromised keys, delegated authority, custody, collateral, inheritance and insolvency.

German law provides a useful comparison. The Electronic Securities Act (eWpG) deliberately creates legal certainty for electronic securities within its scope. An electronic security generally has the same legal effect as a certificated security and is treated as a "thing" for purposes of §90 BGB. The Act identifies the registered holder, provides rules for transfers and good-faith acquisition, and establishes an applicable-law rule for rights in electronic securities.

That is useful precisely because it demonstrates the remaining problem. The law has deliberately mapped particular tokenised financial instruments into a defined legal architecture. The same certainty does not automatically follow for every native crypto-asset simply because cryptographic ownership or transfer can be demonstrated.

I therefore distinguish native and non-native tokens.

For a non-native token representing a security, deposit, claim, real-world asset or other off-chain right, the critical question is what legal right the token represents and whether transfer of the token actually transfers that underlying right. The token and the legal claim cannot simply be assumed to be identical.

For a native crypto-asset, there may be no separate issuer or underlying off-chain asset. The central questions instead concern whether the token itself is recognised as property, when ownership legally transfers, the effect of theft or unauthorised transfer, good-faith acquisition, collateral, competing third-party claims and insolvency.

Intermediated custody creates another layer. The law should distinguish clearly between ownership of an asset, a contractual claim against an intermediary and beneficial entitlement to assets held collectively. Insolvency is where ambiguity in that trust relationship becomes most dangerous.

The objective should not be to force every token into the legal model developed for traditional securities. It should be to make the legal consequences of the architecture predictable.

Cryptographic control, legal ownership, beneficial entitlement and authority to dispose should not be treated as automatically synonymous.

That distinction will become even more important as smart accounts, multisignature arrangements and autonomous agents increasingly exercise technically valid authority over assets without necessarily possessing beneficial ownership or unlimited legal authority.

Question 80.2 What is the urgency with which each issue should be addressed by regulators?

	1 (none or not urgent)	2 (low urgency)	3 (moderate urgency)	4 (high urgency)	5 (immediate / critical)	Don't know - No opinion - Not applicable
Issuing a crypto-asset token in compliance with national law	☐	☒	☐	☐	☐	☐
Issuing a tokenised financial instrument in compliance with national law	☐	☒	☐	☐	☐	☐
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 answers to question 80.2 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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The highest urgency should be attached to the questions that determine what a person actually owns and what happens when something goes wrong: property status, transfer, third-party effect, custody, enforcement and insolvency.

These are more fundamental than adding further rules governing issuance.

Again, Germany provides a useful example. The eWpG creates explicit legal effects for electronic securities within its scope, including rules concerning registered ownership, transfer, good-faith acquisition and applicable law. That demonstrates that technological innovation does not require abandoning private-law certainty.

But the solution should not be to require every digital asset to enter an approved register or intermediary structure before receiving legal recognition.

That would solve legal uncertainty by creating another permission architecture.

Native crypto-assets require particular attention because there may be no issuer, register operator or underlying off-chain claim around which traditional private law can organise itself. The law should be capable of recognising ownership and resolving competing claims without manufacturing an intermediary merely because existing legal concepts find an intermediary convenient.

Non-native tokens present a different problem. Where a token represents a security or another off-chain asset or claim, legal certainty is required concerning the relationship between the token and the represented right. A technically valid token transfer should not leave the parties uncertain whether the underlying legal entitlement moved with it.

Custody and insolvency are immediately important because they determine whether someone actually owns an asset or merely holds a claim against an intermediary when that intermediary fails.

I would also treat the distinction between cryptographic control, ownership and delegated authority as an immediate issue.

Possession of a valid signing key establishes technical capability. It should not automatically establish beneficial ownership or unlimited legal authority.

This distinction already matters for custodians, multisignature arrangements, compromised wallets and delegated keys. It will become considerably more important as autonomous software and AI agents transact through smart accounts on behalf of human and institutional principals.

Europe has an opportunity here to provide genuine scaffolding: clear property rights, predictable transfer rules, enforceable ownership, clear treatment of custody and insolvency, and legal recognition of delegated authority.

That increases freedom rather than restricting it.

Legal certainty should tell people what their rights are when they choose an architecture. It should not determine which architecture they are allowed to choose.

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

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion / not applicable

Question 81.1. What are the 3 most important elements that should be addressed in EU law?

Please explain your answer and provide examples:

Most important element number 1:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Ownership/property status and effect against third parties

EU law should clearly establish whether and when a token is an object of property, who legally owns it, and whether that ownership is enforceable against third parties.

Cryptographic control and legal ownership should not automatically be treated as synonymous. Possession of a private key demonstrates technical ability to transfer an asset, but it does not necessarily establish beneficial ownership or legal authority to dispose of it. This distinction matters for theft, compromised keys, multisignature arrangements, delegated authority and increasingly autonomous agents.

Germany's eWpG provides a useful example for electronic securities. Qualifying electronic securities are given the same legal effect as certificated securities and are treated as objects of property under §90 BGB. EU law should provide comparable certainty for digital assets across borders without requiring every token to adopt the institutional architecture of a traditional security.

For native crypto-assets, legal recognition should not depend on the existence of an issuer, custodian or authorised register operator. For non-native tokens representing an off-chain asset or claim, the law should clearly establish the relationship between ownership of the token and ownership or entitlement to the represented asset.

Legal recognition of ownership is scaffolding. It should protect the individual's rights, not become leverage for requiring an approved ledger, custodian or token architecture.

Most important element number 2:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Transfer, including good-faith acquisition and unauthorised transfers

EU law should establish predictable rules for when ownership of a token legally transfers, the consequences of an unauthorised transfer, competing claims, and whether and under what circumstances good-faith acquisition is possible.

A blockchain can establish with considerable certainty that a transaction occurred. It cannot by itself establish that the person controlling the signing key was the beneficial owner or possessed legal authority to make that transfer.

Germany's eWpG again provides a useful example. It expressly defines requirements for transferring electronic securities and provides rules for good-faith acquisition. Similar legal certainty is needed across the EU for digital assets.

The treatment should recognise the difference between native and non-native tokens. For a native crypto-asset, the principal question may be whether transfer of the token transfers the property itself. For a token representing a security, deposit or other off-chain claim, EU law must additionally establish whether transfer of the token transfers the represented legal right.

The objective should be to make the legal consequences of a voluntary transaction predictable, not to require transactions to occur through an approved intermediary simply because intermediated transactions are easier for regulators to categorise.

Most important element number 3:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Custody and insolvency treatment

EU law should clearly establish the rights of token holders when assets are held through an intermediary and what happens to those assets if the intermediary becomes insolvent.

A holder should be able to know whether they legally own the underlying token, possess a beneficial interest in segregated assets, or merely hold a contractual claim against the custodian. The law should also make clear whether assets may be rehypothecated, how shortfalls are allocated, and how additional intermediaries in a custody chain affect those rights.

Germany's eWpG demonstrates one approach by expressly addressing individual and collective registration of electronic securities and the legal position of holders within those structures. The broader EU problem is ensuring that custody does not make ownership ambiguous precisely when the intermediary fails.

This is especially important because self-custody and intermediated custody represent fundamentally different trust relationships. In self-custody, the individual retains technical control and accepts the vulnerabilities associated with that control. In intermediated custody, authority is deliberately transferred to another party and additional counterparty and insolvency risks are created.

EU law should protect people when they choose that intermediary relationship. It should not use those protections to make intermediation mandatory.

The goal should be clear rights in failure, not regulation that eliminates the ability to avoid intermediary risk in the first place.

Question 81.2 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?

	1 (strongly disagree)	2 (rather disagree)	3 (neutral)	4 (rather agree)	5 (strongly agree)	Don't know - No opinion - Not applicable
Implementation of a 28th 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 answers to question 81.2 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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I favor a functional EU layer and clear conflict-of-law rules over wholesale harmonization of Member State property law. The objective should be interoperability between legal systems: predictable consequences for ledger entries, transfers and third-party rights while preserving national law where it does not create cross-border uncertainty.

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:

Maximum 2 selection(s)

Please select as many answers as you like

- ☐ **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 third-party effect and protects from competing claims. This also creates legal certainty for collateral use. The EU law would create a uniform rule of “digital entitlement” that functions across all Member States’ property law structures.

- ☒ **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.

([Inspired by Lichtenstein Law](#). Art 2 TVTG defines token as a piece of information on a TT System which can represent claims or rights of memberships against a person, rights to property, or other absolute or relative rights.

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).

- ☐ **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.

You selected:

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 third-party effect and protects from competing claims. This also creates legal certainty for collateral use. The EU law would create a uniform rule of “digital entitlement” that functions across all Member States’ property law structures.

MODEL 3 - a) 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?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I favor the functional approach in Model 3 for native on-chain assets and the rights-carrier approach in Model 4 where a token represents an off-chain asset or claim. The law should not pretend every token has the same ontology. What matters is that the holder can determine what right the token carries, against whom, and what legal consequence follows from transfer.

Model 3 appears capable of interoperating with German private law and, in my view, offers a useful route to EU-wide legal certainty precisely because it need not replace national property law wholesale.

Germany's eWpG already demonstrates a functional bridge between an electronic register and existing private law. It gives electronic securities the same legal effect as certificated securities, treats them as objects of property under §90 BGB, identifies the registered holder and provides rules governing transfer and good-faith acquisition.

An EU rule of digital entitlement could perform a similar function across Member States: establish defined legal consequences of an on-chain record, including who may exercise rights, third-party effect and protection against competing claims, while leaving broader national property-law systems intact where possible.

The important limitation is that the EU rule should not require an authorised intermediary or centrally approved register merely to obtain legal recognition. A genuinely decentralised ledger must be capable of producing legally recognised evidence and legal effects without the law manufacturing a gatekeeper where the architecture itself has none.

EU law should create interoperability between technical fact and legal consequence, not use legal recognition as leverage to prescribe the technical architecture.

MODEL 3 - b) 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?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☒ Functional rules regulating the effects of recording an asset on chain
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 3 b):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I prefer functional rules regulating the legal effects of recording an asset on-chain.

A constitutive rule stating that the blockchain record itself conclusively creates ownership risks collapsing

several different concepts into one: cryptographic control, registration, beneficial ownership and legal authority.

They are not always the same.

A stolen private key can produce a technically valid transaction. A custodian can control keys without beneficially owning the assets. A multisig participant can possess signing authority without ownership. An autonomous agent may be authorised to execute transactions within a limited mandate without owning the assets it controls.

The law should therefore specify what legal consequences follow from an on-chain record while preserving mechanisms for dealing with theft, fraud, mistake, delegated authority, competing claims and good-faith acquisition.

The ledger can provide exceptionally strong evidence of what occurred technically. The law should determine the legal consequences of that fact rather than pretending the technical fact answers every legal question.

This is also more technologically neutral. It recognises the evidentiary and transactional properties of DLT without making a particular technical record the source of every underlying legal right.

MODEL 3 - c) Are the different ownership models better suited for native or non-native tokens?

- ☒ For native
- ☐ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 3 c):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Model 3 is particularly well suited to native tokens.

For a genuinely native crypto-asset there may be no separate off-chain asset, issuer or legal claim represented by the token. The token is the asset.

In that situation, creating legal consequences around the on-chain record is considerably more natural than attempting to locate an underlying off-chain right that does not exist.

Bitcoin and Ether are obvious examples conceptually: the asset exists natively within the relevant network rather than functioning as a digital receipt for an external asset.

The law should therefore be capable of recognising digitally native property on its own terms.

That does not mean that the ledger should conclusively determine every legal question. Theft, compromised keys, inheritance, insolvency, delegated authority and competing claims can still require legal rules. But those rules should operate around the native asset rather than pretending it represents something outside the network.

MODEL 3 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

MODEL 3 - d) What would need to be different depending on the type of the token?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The same ownership model should not be imposed identically on all tokens because native and non-native tokens represent fundamentally different legal relationships.

For a native crypto-asset, the token can itself be the object of property. There may be no external issuer, security, deposit, physical asset or contractual claim behind it.

For a tokenised financial instrument, the token generally represents or carries rights that already exist within a wider legal relationship: rights against an issuer, shareholder rights, repayment rights, claims to assets or other legally defined entitlements.

EU law should therefore establish common principles of digital entitlement, transfer, third-party effect, custody and insolvency while allowing the legal consequences to reflect what the token actually is.

Technological similarity should not erase legal difference.

Please explain your answers for MODEL 3 and provide examples:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Model 3 is strongest for native digital assets because it allows law to recognise legal consequences of a digital record without inventing an underlying off-chain asset.

Germany's eWpG demonstrates that national private law can successfully connect electronic registration to property-law consequences. It expressly recognises qualifying electronic securities as property and establishes rules for ownership transfer and good-faith acquisition.

I would extend the principle, but not necessarily the institutional architecture.

A public permissionless ledger should not require an authorised central register operator merely to receive legal recognition. The useful principle is that a reliable digital record can have predictable legal effects.

The law should then address the exceptional cases the ledger cannot resolve by itself: theft, fraud,

compromised authority, good-faith acquisition, inheritance, insolvency and competing claims.

The objective should be legal recognition of digital property, not regulatory ownership of its infrastructure.

You selected:

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.

MODEL 4 - a) 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?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Model 4 should be capable of interoperating with German private law, but it requires greater care because the token and the underlying right are legally distinct things unless legislation expressly connects them.

This model is particularly useful where a token represents a security, ownership interest, intellectual-property right, lien, claim against an issuer or another off-chain entitlement.

EU law could establish that a valid transfer of the token transfers the associated legal right, giving the token a legally recognised carrier function across Member States.

Germany's eWpG demonstrates a related approach for electronic securities: §25 provides that transfer of ownership of the electronic security also transfers the right arising from that security.

EU harmonisation could provide similar certainty across borders.

However, the underlying right still matters. A token representing shares, a debt claim, real estate, intellectual property or a bank deposit cannot automatically override every substantive rule governing those different assets.

The objective should therefore be legal interoperability between the token and the underlying right, not the fiction that tokenisation makes every underlying asset legally identical.

MODEL 4 - b) 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?

- ☐ Constitutive rules of ownership based on the asset being recorded on chain
- ☒ Functional rules regulating the effects of recording an asset on chain

- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 4 b):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

I prefer functional rules here even more strongly than under Model 3.

For a non-native token, recording something on-chain cannot by itself determine every aspect of ownership because an underlying legal right exists outside the ledger.

A token representing a share, bond, property interest, intellectual-property right or other claim should have clearly defined legal consequences when transferred. Ideally, the law should make the connection sufficiently strong that transferring the token reliably transfers the represented right.

But the ledger cannot determine whether the underlying right existed validly in the first place, whether the issuer possessed authority to tokenise it, or whether mandatory rules governing that asset have been satisfied.

Functional rules can create a strong legal bridge between token and underlying right without pretending that the digital representation creates reality simply by being written to a ledger.

MODEL 4 - c) Are the different ownership models better suited for native or non-native tokens?

- ☐ For native
- ☒ For non-native tokens
- ☐ Don't know / no opinion / not applicable

Please explain your answer to MODEL 4 c):

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Model 4 is naturally suited to non-native tokens because its purpose is to make the token the legal carrier of a right or asset that exists outside the token itself.

Examples include tokenised bonds, shares, deposits, intellectual-property rights, claims against an issuer, liens or interests in physical assets.

The important legal function is to make the relationship between token and represented right unambiguous.

If I acquire the token, I should know whether I acquired the underlying right.

If I transfer the token, I should know whether that right transferred.

If the issuer becomes insolvent, I should know whether I own an asset, possess a secured claim or merely stand among unsecured creditors.

That is fundamentally different from a native crypto-asset, where there may be no separate underlying right for the token to carry.

MODEL 4 - d) Can the same ownership model be implemented for all types of tokens (crypto-assets and DLT financial instruments)?

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion / not applicable

MODEL 4 - d) What would need to be different depending on the type of the token?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The same model should not be imposed on every token.

For a native crypto-asset, the token itself can be the property. There is no need to invent an underlying right for it to carry.

For a non-native token, the legal architecture must define the relationship between the token and the underlying asset or claim.

For tokenised financial instruments specifically, existing substantive rights and obligations under securities, corporate and financial law continue to matter. Tokenisation should provide a new means of recording, holding and transferring those rights rather than silently changing their substantive content.

The common EU layer should therefore concentrate on legal certainty around digital entitlement, transfer, third-party effect, custody and insolvency, while the specific legal consequences reflect the nature of the underlying asset.

The law should follow the actual relationship rather than forcing different relationships into one model merely because they use the same technology.

Please explain your answers for MODEL 4 and provide examples:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Model 4 provides a useful legal bridge between DLT and existing property and financial law for non-native assets.

A tokenized bond should reliably carry the rights of the bond. A tokenized share should reliably carry the relevant shareholder rights. A token representing another asset or claim should tell the holder precisely what legal entitlement travels with the token.

Germany's eWpG provides a useful example. For qualifying electronic securities, German law connects ownership of the electronic security with the right arising from that security and establishes rules governing

transfer and good-faith acquisition.

The EU could create comparable cross-border certainty without requiring every token to pass through one prescribed institutional architecture.

This distinction between Model 3 and Model 4 is important.

For a native asset, the token may be the thing.

For a non-native asset, the token may carry rights to something else.

Those are different trust relationships and should not be collapsed simply because both are represented using DLT.

The strongest EU framework would recognize that distinction while providing interoperable rules for ownership, transfer, third-party effect, custody and insolvency.

Again, the purpose should be scaffolding: make rights clear and enforceable while preserving architectural choice.

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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The central problem is not that Member States must have identical property law, but that token ownership, transfer, custody and third-party effect can receive different legal treatment while the token itself moves seamlessly across borders. I would therefore prioritize EU rules on cross-border effect and legal interoperability rather than attempting an exhaustive replacement of national private law.

4.7 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 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

☐ Don't know / no opinion / not applicable

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?

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Yes. EU conflict-of-law rules should be introduced for the proprietary aspects of tokens because many traditional connecting factors assume a physical location, identifiable intermediary, central register or system operator.

Those assumptions become difficult to apply to genuinely distributed systems.

A native crypto-asset on a public permissionless blockchain may have no issuer, no central administrator, no single register operator and no meaningful geographic location of the ledger. The same ledger may be replicated and validated across many jurisdictions simultaneously.

Trying to determine the applicable property law from the physical location of nodes, validators, developers or other technical infrastructure would therefore produce uncertainty rather than resolve it.

The problem is different for tokenised financial instruments and other non-native tokens. Where there is an identifiable issuer, regulated register or underlying legal asset, existing connecting factors may remain meaningful. Germany's eWpG demonstrates this approach for electronic securities: §32 generally connects rights and dispositions concerning an electronic security to the law of the state supervising the relevant register operator, with fallback rules where that connection is unavailable.

That works because the architecture deliberately contains a legally identifiable register operator.

EU law should not extrapolate from that model and require every token architecture to create such an operator merely to make conflict-of-law analysis possible.

A conflict-of-law rule for tokens should therefore accommodate both architectures: systems with identifiable legal anchors and genuinely decentralised systems without them.

The purpose of the rule should be to provide predictable legal consequences for architectural choices, not to force architectural choices in order to obtain predictable legal consequences.

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:

at most 5 answered row(s)

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

	1	2	3	4	5
The law of the state specified in the token or in the principles (if any) expressly specified in the token	☒	☐	☐	☐	☐
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	☐	☐	☐	☐	☐
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	☐	☐	☐	☐	☐
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 answers to question 84, 84.1 and 84.2 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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

My preferred hierarchy begins with an expressly specified governing law where that choice is meaningful, transparent and accessible to participants.

1. Law expressly specified in the token or its governing principles.
2. Law specified in the rules or governing principles of the system on which the token is recorded.

These provide predictability without requiring the law to manufacture a geographic location for a distributed ledger.

For systems that intentionally use a regulated register, the law of the state supervising that register is an appropriate additional connecting factor. Germany's eWpG provides an existing example of this approach.

For non-native tokens with an identifiable issuer, the issuer's establishment and supervisory jurisdiction can provide further fallback connecting factors.

I would not use the location of technology providers, validators, developers or other infrastructure providers as a primary proprietary connecting factor. Providing technology does not necessarily confer ownership, custody or authority over the asset.

I would be particularly cautious about PREMA, based on the residence of a system-relevant master-key holder. A genuinely permissionless blockchain may have no such key. Creating legal advantages around the existence of one could perversely encourage systems to introduce precisely the centralized coercive authority that decentralized architectures were designed to remove.

The same concern applies to PROPA. It may be appropriate where a system genuinely has an operating authority or administrator. It should not become a reason to require every system to have one.

Conflict-of-law rules should recognize where authority actually exists rather than manufacture authority because existing law finds a central administrator easier to locate.

Question 85. If there are any other issues relating to legal certainty which are not mentioned above, please describe them here:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

Three emerging legal-certainty issues deserve attention.

First, autonomous agents. A valid signature can prove that a key authorized a transaction without proving that the human principal intended that particular action. Authentication, delegated authority and fidelity to the principal's mandate are different questions.

Second, privacy and physical security. Persistent linkage of identity, wallet activity, IP metadata and location can create risks that extend beyond data protection, including coercion and physical targeting. Regulation should not create these linkages unless they are necessary for a specific vulnerability.

Third, regulatory concentration itself. Where access to assets, protocols or settlement becomes dependent on a small number of licensed gateways or certifiers, the law has created a new systemic trust dependency. That dependency should be assessed with the same seriousness as technical concentration.

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:

5000 character(s) maximum

including spaces and line breaks, i.e. stricter than the MS Word characters counting method.

The greatest issue this review needs to address is not any single MiCA provision. It is the architecture created when they are assembled.

MiCA should be considered alongside Europe's wider direction in digital identity, tokenized finance and settlement, including Pontes and Appia. Licensing, certification, identity, stablecoin, protocol-access, custody and settlement rules can each be justified individually. Together they can create something very different.

A system does not need to prohibit alternatives to eliminate meaningful choice. It can make the cost of exercising them progressively prohibitive.

If participation increasingly requires an approved intermediary, identity, asset, protocol or settlement route, individuals may retain theoretical freedom while losing practical freedom.

The walk-away test has failed.

This is the Double-Edged Sword problem. Technologies that make relationships more verifiable can also make control extraordinarily efficient.

Cryptographic verification is not itself trust.

Trust is willingly accepted vulnerability in the presence of risk. Where vulnerability is compulsory and meaningful exit has disappeared, the relationship is not trust. It is control.

I am therefore particularly concerned by proposals involving certification of DeFi protocols and non-custodial wallets, embedded compliance mechanisms and restrictions on CASPs connecting customers to uncertified protocols.

Certification can produce useful evidence. It should not automatically become permission.

Non-custodial software does not possess the authority of a custodian. A genuinely decentralized protocol does not possess the authority of an intermediary. If nobody can seize assets, reverse transactions, unilaterally change the protocol, custody funds or decide participation, regulation should not require someone to acquire those powers merely to create an identifiable party capable of regulatory control.

That changes the trust architecture itself.

The same applies to money and settlement. Central-bank money for tokenized settlement and interoperability can provide value. But providing an option is different from designing the regulatory environment until it becomes the only economically viable destination.

Europe should not confuse strategic autonomy with architectural enclosure.

Nor should institutional permission be confused with safety. European supervisors continue to document serious deficiencies and control failures within regulated financial institutions. Regulation can reduce particular risks. It does not eliminate vulnerability.

Risk moves.

If the state restricts an individual's ability to hold an asset, use open-source software, interact with a permissionless protocol or choose another settlement architecture, it should identify the specific vulnerability, justify the intervention, make its authority inspectable and preserve meaningful exit wherever possible.

That is the distinction between scaffolding and the cage.

Scaffolding establishes property rights, exposes material risks and hidden authority, protects against fraud and intermediary failure, makes legal relationships predictable, and allows identity to prove what needs proving without requiring every verifier to retain another copy of the person.

Then it leaves people room to choose.

The cage begins when protection becomes permission: disclosure becomes approval, certification becomes access, identity becomes persistent identification, intermediaries become mandatory, and legal recognition becomes conditional upon approved architecture.

Europe needs more legal certainty, not less. But it needs discipline about what legal certainty is for.

Regulate vulnerability where it exists: reserve risk at the reserve layer, issuer risk at the issuer layer, custody risk at the custody layer, fraud at the point of fraud, systemic exposure where it actually exists.

Do not manufacture intermediaries because they are easier to regulate. Do not manufacture control because it is easier to supervise. Do not make permissionless systems permissioned in practice while calling them permissionless in theory.

Specific vulnerability should justify specific authority. That authority should be bounded, inspectable and revocable. People should retain a meaningful ability to refuse it and choose another architecture.

That is Trust Architecture.

MiCA should be judged not only by whether each rule appears reasonable in isolation, but by where they lead when combined.

If every road ultimately leads through institutionally approved identity, intermediaries, assets, protocols and settlement infrastructure, Europe will not have built trustworthy digital finance.

It will have built a sophisticated system of capture and called it trust.

Additional information

Should you wish to provide additional information (e.g. a position paper, report) or raise specific points not covered by the questionnaire, you can upload your additional document(s) below. **Please make sure you do not include any personal data or any information that might identify you in the file you upload if you want to remain anonymous.**

The maximum file size is 1 MB.

You can upload several files.

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

3417a7cc-3c40-48ac-bba1-97921362bb90

/Donny_Lewis_Trust_Architecture_European_Digital_Finance_MiCA_2026.pdf

Useful links

[More on this consultation \(https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-review-mica-regulation_en\)](https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-review-mica-regulation_en)

[Consultation document \(https://finance.ec.europa.eu/document/download/62be7015-f066-4fac-b74e-71bacdbcc9f5_en?filename=2026-mica-review-targeted-consultation-document_en.pdf\)](https://finance.ec.europa.eu/document/download/62be7015-f066-4fac-b74e-71bacdbcc9f5_en?filename=2026-mica-review-targeted-consultation-document_en.pdf)

[Related public consultation \(https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/public-consultation-review-mica-regulation_en\)](https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/public-consultation-review-mica-regulation_en)

[More on crypto-assets \(https://finance.ec.europa.eu/digital-finance/crypto-assets_en\)](https://finance.ec.europa.eu/digital-finance/crypto-assets_en)

[Specific privacy statement \(https://finance.ec.europa.eu/document/download/b6bd37fe-89ad-4e9a-9188-efa9743c4e2e_en?filename=2026-mica-review-targeted-specific-privacy-statement_en.pdf\)](https://finance.ec.europa.eu/document/download/b6bd37fe-89ad-4e9a-9188-efa9743c4e2e_en?filename=2026-mica-review-targeted-specific-privacy-statement_en.pdf)

Contact

fisma-mica-review@ec.europa.eu

