

September 30, 2026

VIA ELECTRONIC SUBMISSION

European Commission
Directorate-General for Financial Stability, Financial Services and Capital Markets Union
Horizontal Policies, Digital Finance
1049 Brussels
Belgium

Re: Targeted Consultation on the Review of Regulation (EU) 2023/1114 on the Markets in Crypto-Assets (MiCA)

Dear Sir or Madam:

Hyperliquid Policy Center (“HPC”) appreciates the opportunity to respond to the Targeted Consultation on the Review of Regulation on the Markets in Crypto-Assets (the “Consultation”)¹ issued by the European Commission (the “Commission”) through its Directorate-General for Financial Stability, Financial Services and Capital Markets Union. We commend the Commission for undertaking this Consultation at a formative moment for onchain markets, and we have included as an Appendix to this letter the responses HPC submitted through the Commission’s online questionnaire.

HPC is an independent research and advocacy organisation dedicated to a clear, regulated path for the evolution of onchain markets, including those available on Hyperliquid.² The Consultation arrives at a defining moment for financial markets, as public blockchains now serve as infrastructure for markets that trade continuously and in substantial volume, and regulators in several jurisdictions are working through how regulated products can use them. The European Union was the first major jurisdiction to adopt a dedicated framework for crypto-asset markets, and this review is an opportunity to build on that effort. As detailed in our responses, we believe the existing EU frameworks can accommodate onchain products and markets through targeted action without a wholesale revision of their rules.

Three points at the core of our responses merit particular attention:

- **MiCA and MiFID II classification should follow the economic features of an instrument, and the ledger on which it is recorded should not be determinative.** Crypto-assets that qualify as financial instruments should remain under sectoral legislation, and perpetual futures, which carry the characteristics of the derivatives MiFID II already recognises, should be governed by that framework. ESMA has reasoned in the same way, treating the technological format as not determinative at Guideline 1 of its Article 2(5) guidelines and perpetual futures as derivative contracts at paragraph 47, and we support that approach. Perpetual futures have become one of

¹ European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *Targeted Consultation on the Review of Regulation on the Markets in Crypto-Assets (MiCA)*, Consultation Document (20 May 2026), https://finance.ec.europa.eu/document/download/62be7015-f066-4fac-b74e-71bacdbcc9f5_en?filename=2026-mica-review-targeted-consultation-document_en.pdf [hereinafter Consultation]. The Consultation seeks feedback to inform the Commission’s review of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, OJ L 150, 9.6.2023, p. 40 (“MiCA”).

² See Hyperliquid Policy Center, *About*, <https://hyperliquidpolicy.org/about> (last visited 27 September 2026).

the most widely traded derivative products globally, and several jurisdictions have begun to develop regulatory frameworks for them. Empirical research also suggests that perpetual futures are complementary to other derivative types and can expand product choice and improve competition among trading venues, to the benefit of market participants. In crafting a regulatory approach, we also strongly encourage the Commission to take care to distinguish these products from the contracts for difference that shaped the EU's 2018 product intervention measures, as their structure and risk profile differ in several important respects.

- **Regulation of onchain products and markets should be calibrated to the functions market participants actually perform and to the risks each product presents.** Onchain markets distribute functions that a single regulated entity has traditionally performed across a blockchain network itself, the persons who build products and markets on it, and the intermediaries that provide access to them. In considering how to regulate these products and markets, we believe that the Commission should analyse the functions each participant performs, identify where discretion is exercised, and tailor obligations to those functions and to the risks of each product.
- **Public blockchains can both address supervisory concerns natively and help regulated intermediaries meet their obligations more effectively.** Transparency, immutable recordkeeping, and verifiable settlement are properties that public blockchains provide by default, which natively advance many of the supervisory objectives the Commission's frameworks are designed to secure. Public blockchains likewise offer regulated intermediaries a more transparent and efficient technology for complying with the rules that apply to them, and the Commission can recognise the use of that technology as a valid means of compliance.

A further theme of our responses is the convergence of traditional finance and public blockchain networks. Regulated firms increasingly seek to deliver regulated products over public blockchains, and stablecoin issuers, whose reserve and redemption obligations MiCA already governs, are the clearest example. Other products and markets can follow the same path, including onchain derivatives and tokenised securities markets. We describe this development as "onchain finance." It preserves the accountability that regulation expects of a firm while giving that firm, and its clients, the openness, resilience, and verifiability of a public network. Market participants and regulators alike have begun to recognise the advantages this convergence offers and are seeking to accommodate the use of public blockchains in the provision of regulated services. Regulated firms will need clarity on how to meet existing requirements through new technology as this trend continues, and several of our responses are directed to that need.

HPC thanks the Commission for the breadth and care of the Consultation. We would be pleased to assist the Commission, ESMA, and national competent authorities in whatever manner is most useful as they consider these questions, whether through operational data, technical documentation, or comparative analysis of approaches taken in other jurisdictions, and we look forward to continued engagement as the review proceeds.

Respectfully submitted,

/s/ Jake Chervinsky

Jake Chervinsky

Chief Executive Officer

Hyperliquid Policy Center

cc: Adam Minehardt, Chief Policy Officer, Hyperliquid Policy Center
Brad Bourque, Senior Counsel, Hyperliquid Policy Center
Elise Soucie Watts, on behalf of Hyperliquid Policy Center

Appendix: Responses to Consultation Questions

This Appendix contains HPC's responses to selected questions from the Consultation Document.

Part 1: Scope and Definitions, Title II Crypto-Assets

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*

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

☐ *Yes, sufficiently clear*

☒ *No, clarification is needed*

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

Hyperliquid Policy Center (“HPC” or “we”) thanks the Commission for the opportunity to engage in the Targeted Consultation on the Review of Regulation on the Markets in Crypto-Assets (“MiCA”). This initial question is critical, and we welcome the Commission's decision to focus on the perimeter at the outset, as a clear boundary across products will be foundational to all other key issues set out in this consultation as well as the successful implementation of MiCA itself.

HPC supports retaining sectoral legislation for crypto-assets that qualify as financial instruments. Directive 2014/65/EU on markets in financial instruments (“MiFID II”) is a mature, globally respected, and well-functioning framework, and one of its core strengths is that it captures instruments by reference to their substance rather than to their label or their form. Section C of Annex I classifies derivatives by reference to their underlying and their settlement, and it does so in terms broad enough to accommodate instruments which did not exist when it was drafted, including through the categories which turn on whether a contract has the characteristics of other derivative financial instruments.

We believe that the MiFID II classifications should apply to an asset (whether a spot asset or a derivatives contract) recorded on a distributed ledger in the same way they apply to an asset recorded elsewhere. In our view, the MiFID II framework does not need to be rebuilt to accommodate distributed ledger technology (“DLT”). Rather, it should be applied in a technologically neutral manner to support the continued evolution of the European Union's (“EU”) financial market infrastructure, and we encourage the Commission to build on MiFID II's existing strength.

Adopting an approach that treats the recording medium as the classificatory trigger for an asset would sit uneasily with the principle of technological neutrality that this Consultation rightly reaffirms. That approach risks subjecting economically identical instruments to different regulatory frameworks

based solely on the ledger that records them, so that the same instrument is regulated one way when recorded in, for instance, a central securities depository (“CSD”) but faces disparate treatment when recorded on a public DLT-based ledger. The rules that govern an instrument exist to address the risks the instrument creates for investors, for counterparties, and for the market. Those risks flow from the instrument’s economic terms rather than from the database in which it is recorded. A framework that hinges on the recording medium would also invite firms to reclassify an instrument through its choice of ledger, which could result in regulatory arbitrage of the sort that the principle of technological neutrality is intended to prevent.

The Article 2(5) guidelines issued by the European Securities and Markets Authority (“ESMA”) and the joint classification test of the European Supervisory Authorities (“ESAs”) have served market participants well, and we welcome the certainty they have brought. In particular, we support Guideline 1, under which the technological format is not a determining factor and tokenised financial instruments continue to be treated as financial instruments for all regulatory purposes, which we believe rightly establishes technological neutrality as the starting point for classification. Those frameworks focus on the economic characteristics of an asset, and they have worked well in determining whether a given asset is itself a financial instrument.

A single blockchain network will often support assets and instruments of quite different kinds, which is why the classification boundary should be drawn per instrument. Hyperliquid, for example, is a general-purpose layer-one blockchain that supports onchain financial activity, including the trading of spot digital assets and of derivatives such as perpetual futures.³ The Hyperliquid blockchain is neutral infrastructure, and the assets and instruments that trade on it differ in kind. The blockchain’s native token (“HYPE”) functions as network infrastructure. It is used to pay network costs, it supports the security of the network through its use in the delegated proof-of-stake consensus mechanism, and holding and staking it provides users with trading fee discounts. Spot digital assets trade on the network’s onchain order books. Perpetual futures traded on that same network are different, being standardised, fungible, cash-settled contracts which can be offset and whose price converges toward a reference price. The coexistence of these assets and instruments is the ordinary consequence of a general-purpose blockchain that supports a diverse range of onchain financial activity, and it illustrates why classification is best assessed instrument by instrument rather than by reference to the venue or to the underlying technology. We expand on our proposed approach to perpetual futures in our response to Question 73.

In recognition that a variety of instrument types may exist on a single blockchain network, we believe that additional guidance would be most beneficial for cases that appear to fall outside the scope of the guidelines as initially drafted, such as a derivative contract that is traded, concluded, and cash-settled on a DLT-based public ledger and whose underlying, or reference asset, is itself a financial instrument. The Article 2(5) mandate was confined to the qualification of crypto-assets as financial instruments, so the guidelines do not reach that case.

A derivative is a distinct instrument from the asset it references. Its value is derived from the price of that asset, but the holder of the derivative acquires only a contractual right to a cash flow determined by that price, and acquires no ownership of, and no claim against the issuer of, the referenced asset. A perpetual future is a derivative of this kind. It is a standardised, cash-settled contract with no expiry date, in which a periodic funding payment between long and short positions holds the contract price to the price of the reference asset, and we describe the product in detail in our responses to Questions 72 and 73. A derivative that references a transferable security does not itself become a transferable security, and recording that derivative on a public ledger does not render it a MiCA-regulated crypto-asset. Market

³ Hyperliquid Documentation, *About Hyperliquid*, <https://hyperliquid.gitbook.io/hyperliquid-docs/about-hyperliquid> (last visited 29 September 2026). Descriptions of the mechanics of Hyperliquid and of markets available on it in this response are drawn from the network’s public documentation as of that date.

participants, however, are currently left to reason by analogy from an asset-focused test, and that sort of reasoning-by-analogy may produce inconsistent outcomes across Member States. This is the same analytical question the Commission raises with regard to perpetual futures in Question 72. ESMA has reasoned to the same conclusion at paragraph 47 of the Article 2(5) guidelines, treating perpetual futures as derivative contracts because they involve an agreement to exchange the performance of an underlying asset over time, with value derived from that asset's price movements. That reasoning turns on the economic features of the contract rather than on the nature of what it references, and in our view it holds with equal force where the referenced asset is not a crypto-asset. We would encourage the Commission to confirm this through guidance rather than through any change at Level 1.

We would encourage clarification through the existing guidelines, which would be both timelier and more proportionate to the issue. Our proposed policy measures to provide this clarification are set out below:

1. Confirm that the analysis at paragraph 47 of the Article 2(5) guidelines applies to perpetual futures however they are recorded and whatever they reference, and is confined neither to contracts represented by a token nor to contracts referencing crypto-assets. We recognise that the Article 2(5) mandate is limited to crypto-assets, and confirmation through the MiFID II Q&A process would serve equally well.
2. Confirm that classification is assessed per instrument, not per venue. A venue may list both MiCA crypto-assets and MiFID II financial instruments, and the presence of one should not determine the treatment of the other.
3. Include a worked example of a perpetual contract referencing a non-crypto underlying, as the existing examples in the guidelines at paragraphs 46 and 51 to 54 are directed at crypto-assets structured to resemble derivatives. HPC would be pleased to provide market examples and to support their development.

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.

HPC believes that ESMA's Article 2(5) guidelines and the joint ESA standardised classification test have materially reduced uncertainty for market participants, and we commend ESMA and the ESAs for the clarity they have brought.

Two categories of borderline cases remain difficult in our view. The first is the category we describe in our response to Question 1, in which market participants apply the guidelines by analogy to derivative contracts traded, concluded, and settled on a DLT-based public ledger. ESMA addressed perpetual futures directly at paragraph 47 of the guidelines, confirming that they should be treated as derivative contracts and assessed against Annex I Section C, points (4) to (10), of MiFID II. What remains uncertain, however, is the application of that analysis to a contract which is not itself a crypto-asset, the guidelines having been mandated to address the qualification of crypto-assets as financial instruments. The second is instruments whose character may change over their life. Certain perpetual futures permit price discovery on an asset before it exists in a spot market and convert to conventional perpetual futures once that asset is listed. Pre-IPO perpetual futures deployed on markets available on Hyperliquid, for example, begin as cash-settled instruments referencing the anticipated public listing of a private company, priced before the listing by a reference price derived from the contract's own onchain order book because

no external reference price exists.⁴ When the company's shares list on a traditional venue, the contract converts into a standard perpetual future referencing the listed equity and priced from external market data. ESMA recognises at paragraph 75 of the Article 2(5) guidelines that a crypto-asset's functions or attributes may evolve during its life-cycle, and directs that inherent attributes be prioritised over labels in that assessment. What is not addressed is the operational consequence: whether reassessment is required, at what point, and how positions already open are treated.

The guidelines alone cannot resolve every source of divergence. Because the definition of transferable securities rests in national law, the same asset may be classified differently across Member States even where the standardised test is applied consistently and in good faith.

We propose two policy actions to support effective MiCA implementation and reduce uncertainty:

1. Building on paragraph 75 of the Article 2(5) guidelines, provide guidance on the operational consequences where an instrument's classification may change during its life, including whether reassessment is required and the treatment of open positions.
2. Encourage supervisory convergence on the national law dimension, whether through the Q&A process or coordinated statements by national competent authorities.

We remain at the Commission's disposal to discuss any of these points and would be pleased to contribute worked examples in support of the above.

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)?

Our response addresses the categories on which HPC has direct expertise. We defer to other respondents on tokenised fund interests, tokenised money-market instruments, and assets marketed as NFTs but issued in series.

Of the categories the Commission lists, we believe that synthetic exposures are the most difficult to classify in practice and the most consequential to resolve. The difficulty is that "synthetic exposures" may refer to two quite distinct types of financial instruments. A synthetic exposure may include arrangements which provide economic exposure to a reference price, but may also describe instruments which represent an interest in a reference asset. The first are derivatives on any ordinary reading and are properly assessed under MiFID II. The holder of a cash-settled perpetual future referencing an equity obtains price exposure but does not obtain ownership, voting rights, or any other claim attached to the referenced shares. The derivative contract and the referenced instrument are distinct, and the features of the contract should determine its classification. The second case presents more difficult questions, and appropriate classification should depend on the rights such instruments confer. Tokenised equities, for example, may carry conventional shareholder rights such as dividends and voting, may be structured as debt claims against an issuer or intermediary, or may be structured as derivative instruments akin to swaps that track a share price without conferring any interest in the shares. We acknowledge that ESMA addresses several of these cases at paragraphs 50 to 53 of the Article 2(5) guidelines, and we support that analysis. The difficulty which remains is that the term is applied more widely in the market than those

⁴ See Hyperliquid Policy Center and XYZ Ltd., *Comment on IPO Modernization* (SEC File No. CLL-16) (16 August 2026) (describing pre-IPO perpetual futures and their conversion on listing).

paragraphs reach, and treating the whole field as a single category risks classification by label rather than by economic and legal substance.

We would therefore encourage the Commission to approach synthetic exposures by looking at what the instrument actually confers. An instrument that confers economic exposure to a reference price is a derivative and is best assessed under MiFID II. An instrument that confers rights against an identifiable person in respect of an underlying asset is assessed under the framework that governs those rights, whether as a transferable security, a debt claim, or a crypto-asset. We note this position in our response to Question 1, and we expand on this further at Question 73.

Any supplement to the ESMA guidelines contemplated in our responses to Questions 1 and 2 should address synthetic exposures expressly, and HPC would be pleased to support the development of worked examples.

Part 2: Requirements Applying to Asset Referenced Tokens (ART) and Electronic Money Tokens (EMT) and Their Issuers (MiCA Titles III and IV)

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

Use Case	Rating
<i>International payments (cross-border remittances or transfers)</i>	4
<i>Intra-EU payments (domestic and cross-border EU payments)</i>	3
<i>Crypto trading and liquidity provision</i>	5
<i>Retail payments - Person to Person</i>	3
<i>Retail payments - Person to Business (POI payment to merchants including e-commerce)</i>	3
<i>Retail payments - Business to Business</i>	3
<i>Settlement of tokenised financial instruments (e.g., digital bonds, securities)</i>	4
<i>Corporate treasury management</i>	3
<i>Access to programmable or smart contract-based financial services (DeFi applications)</i>	5
<i>Provision of financial services in underserved regions in the world</i>	4
<i>Other potential use cases (please specify)</i>	No entry

Part 3: The Appropriateness of the Legal Framework for Crypto-Asset Service Providers (CASPs)

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

Please explain your answer to question 45:

We consider the current list adequate. Article 3(16) captures the activities which give rise to custody, execution, conduct, and client protection risks, and it does so by reference to the function performed rather than to the technology used to perform it. MiCA has only recently become fully applicable to crypto-asset service providers, and in our view the priority should be consistent application of the existing categories rather than expansion of the list.

We would caution in particular against the addition of new categories directed at derivatives activity. As we set out in our responses to Questions 1 and 72, instruments carrying the economic features of derivatives are properly governed by MiFID II, and ESMA has reasoned in the same way at paragraph 47 of its Article 2(5) guidelines. A new crypto-asset service category addressing activity in relation to such instruments would create an overlapping perimeter for the same instrument, leaving firms to determine which regime governs an activity already within the scope of MiFID II. The unintended consequence would be to reduce rather than improve the legal clarity this question is concerned with, and in our view the risk of overlapping perimeters is a greater problem than any gap in the current list.

Where the boundaries of the existing categories would benefit from clarity, we would encourage the Commission to address this through supervisory guidance rather than through new categories, consistent with the position we set out at Question 1. The boundary we would identify as most useful to clarify is that between the provision of a crypto-asset service and the provision of technology or software which enables a user to transact for themselves, which we address further in our responses to Questions 62.1 and 63.

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?

We support the Commission’s position that the Digital Operational Resilience Act (“DORA”) already provides a comprehensive framework for information and communications technology (“ICT”) risk and digital operational resilience across the financial sector, and in our view it is well designed for the entity-based risks it was built to address. We believe, therefore, that a separate cybersecurity regime for crypto-asset markets is unnecessary.

Three features of DLT market infrastructure do not map neatly onto the DORA framework, and each would benefit from further consideration given the design and capabilities of onchain markets.

First, DORA presupposes ICT systems which an entity operates, maintains, and can patch, whereas software executed by a distributed validator set operates deterministically according to published rules and may not be capable of amendment by any single party. That design also carries resilience and transparency benefits which conventional ICT systems do not offer. The network continues to operate if

any individual participant fails, the rules applied to every transaction are published in advance, and the record of every transaction is public and can be verified by any party without depending on the affected entity. We address the related question of assurance as to the software's operation in our responses to Questions 63 to 65.

Second, DORA's third-party provisions assume a contractual counterparty, whereas such arrangements may not exist or be feasible where an entity instead relies on public DLT infrastructure to perform regulated functions. Article 30 requires the rights and obligations of the financial entity and the ICT third-party service provider to be set out in writing, and, for arrangements supporting critical or important functions, to provide for rights of access, inspection, and audit and for an exit strategy. Each presupposes a provider with whom terms can be negotiated. This position is not unfamiliar. Financial entities have long depended on the public internet and telecommunications networks, and while they contract with connectivity providers they hold no contractual rights over the networks themselves or over the protocols by which they operate. That dependency is managed through their own continuity and contingency arrangements rather than through contractual control, and it has never been thought to preclude the use of the internet or telecommunications infrastructure in financial markets. We encourage the Commission to clarify that operational resilience obligations may be met on the same basis where an entity relies on public DLT infrastructure, through diligence, monitoring, contingency planning, and the ability to migrate, and we caution against an approach requiring greater control over DLT-based infrastructure than an entity could obtain over conventional infrastructure.

Third, onchain derivatives markets depend on price feeds (such as third-party "oracle" arrangements) to enforce margin requirements and to trigger default management processes, including liquidations, and a price feed which functions exactly as specified can still produce disorderly outcomes based on the conditions of the reference market. This is a solvable problem, and market practice has already developed controls which address it. Markets available on Hyperliquid, for example, compute a mark price as the median of multiple independent inputs so that no single feed can determine or disproportionately influence the outcome, and deployers of markets referencing traditional assets apply bounds which limit how far a price may move while the underlying market is closed (analogous to price bands or circuit breakers in conventional markets).⁵ The dependency on third-party price feeds is not novel in kind. Conventional derivatives markets have long determined settlement and valuation by reference to prices constructed by third parties, whether published indices or benchmark assessments, and the governance of those inputs is a familiar supervisory concern. The configuration of a price feed on an onchain venue performs the same function, and the difference lies in how that price is incorporated into the machinery of the market rather than in the nature of the reliance. Consistent with the principle of technological neutrality, the appropriate response is to apply the existing expectations as to the governance of externally constructed price inputs, rather than to treat this as a new category of risk. Our concern is that DORA's ICT third-party provisions do not presently recognise these as the relevant controls, and that there is not yet a consistent cross-EU standard describing what adequate price feed management looks like. We expand on this point in our response to Question 86.

Onchain infrastructure also offers supervisory advantages which the DORA framework does not currently contemplate. Incidents are recorded publicly and in sequence, so reconstruction of an event does not depend on the affected entity producing its own logs. We encourage the Commission to consider how this property might be reflected in incident reporting expectations over time, and how it can be taken

⁵ See Hyperliquid Documentation, *Robust Price Indices*, <https://hyperliquid.gitbook.io/hyperliquid-docs/trading/robust-price-indices> (last visited 18 September 2026) (describing the mark price as the median of the oracle price adjusted for the contract's recent basis, the order book mid price, and the median of external perpetual prices); trade[XYZ], *Documentation*, <https://docs.trade.xyz> (last visited 18 September 2026) (describing per-update clamps on reference price movement and discovery bounds applicable while the underlying market is closed).

into account when evaluating the market participants' ability to meet compliance obligations when utilising DLT-based infrastructure.

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

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

We thank the Commission for raising this question, which in our view goes to one of the more consequential design choices in the MiCA framework. Question 56 is framed by reference to the MiCA perimeter, and we have answered it on that basis. As set out in our responses to Questions 1 and 72, perpetual futures on crypto-assets carry the economic features of derivatives and are most appropriately governed by MiFID II, so access to those markets should be assessed under MiFID II rather than under MiCA. The considerations we set out below as to global liquidity apply in either case.

While we have selected "No" above, we set out below some of the benefits of global liquidity alongside EU liquidity. Access to global liquidity is a question about execution quality for EU investors, and it arises in the same form for any instrument which trades across jurisdictions. The Commission should therefore assess it against the objectives which have guided EU market structure policy since MiFID I, namely best execution, efficient price formation, and the competitiveness of EU venues and participants.

Measured against those objectives, we believe that the advantages of full access to global liquidity are substantial. Liquidity is not evenly distributed, and depth in a single order book produces tighter spreads and more reliable execution than the same interest dispersed across separate venues. Where EU participants access global pools, they transact against the full available depth. Where access is confined, they transact against a fraction of it, and the end investor bears the difference directly. Fragmentation also carries a price formation cost, as a reference price formed from a subset of global interest is a less accurate price, and it becomes less accurate precisely at moments of stress when accuracy matters most. These costs also fall unevenly. Participants with the technology, financial means, and cross-jurisdictional access to operate across multiple pools are well placed to manage fragmentation, while those confined to a single pool are not, so a framework intended to protect EU investors may in practice disadvantage them relative to participants elsewhere.

Access to depth matters most outside conventional trading hours, when the alternative to a global pool is often no venue at all. Where positions must be closed out in volatile conditions, a deep order book absorbs that activity while a thin one transmits it, because forced selling into a shallow market moves the price and can trigger further close-outs. A framework which confined EU participants to a fraction of available depth would therefore have its greatest unintended consequences at exactly the moments when depth is most needed. In our view, these are market integrity and resilience considerations, which should be considered alongside efficiency gains.

Full access to global liquidity pools and defined participation are not mutually exclusive, and a market serving EU participants specifically is practicable today. Onchain market infrastructure is configurable at the level of the person or entity deploying a market. A regulated entity building on such

infrastructure is able to define the parameters of the market it operates, including the scope of participation, to meet the requirements applicable to it.⁶ Where a regulated firm concludes that a market restricted to eligible EU participants is the appropriate structure for its business or its authorisation, that structure is achievable today and we support it.

Our concern is with mandating that narrower structure as a general matter. The capability to build a market with defined participation already exists and can be exercised by the entity best placed to judge what its regulatory position requires, and we see no case for the framework to compel it for every market. Mandating confinement would impose the execution quality and price formation costs described above on all EU participants, including those for whom no supervisory objective requires it, to achieve an outcome which regulated firms can already deliver where it is needed. We encourage the Commission to preserve both options to further promote innovation in EU financial markets.

We recognise that a focus on EU liquidity is motivated by legitimate supervisory objectives, including the ability to supervise activity, to obtain data, and to act where conduct is improper. We do not dismiss these objectives but instead suggest that these are questions about transparency and supervisory access rather than about the geographic location of liquidity, and they are better addressed directly. Onchain markets can support transparency and supervisory objectives as well. In such environments, every transaction is recorded publicly and in sequence, so supervisory visibility does not depend on the venue being located within the Union or on an entity producing its own records.

Our response to Question 62.1 addresses the specific mechanisms through which this question arises, in particular proposals which would confine EU access to verified pools of liquidity.

Part 4: Policy Areas Beyond the Current Scope of MiCA

Question 59

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

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

Service	Rating
Exchange services	4
Payments and transactions services	2
Trading and Investment services	4
Lending and borrowing services	3
Custody services	3

⁶ See our response to Question 73 and the accompanying note describing HIP-3*, an optional deployer configuration for permissioned markets on Hyperliquid.

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

We thank the Commission for framing this question around services and benefits rather than around technology, which in our view is the right approach.

These are market structure questions rather than questions specific to crypto-asset markets, and we encourage the Commission to consider them in that light. MiFID I and MiFID II pursued their transparency objectives through mandated pre- and post-trade disclosure, order recordkeeping, and transaction reporting, because an order book is opaque by default and disclosure had to be imposed on it. An onchain order book, on the other hand, is transparent by default. The state of all transactions is publicly recorded, and no disclosure obligation is needed to make it so.

Given these technological developments, we believe there is now a key opportunity to revisit how supervisory expectations and regulatory objectives can be met, and in some cases improved upon, using technology that is already widely deployed across onchain markets.

We have rated trading and investment services and exchange services most highly, because three core benefits are already realised in onchain markets at scale, including in the markets available on Hyperliquid. First, settlement risk is materially reduced where matching, margining, and settlement occur in a single state transition against pre-funded collateral, as no settlement window accumulates counterparty exposure and no participant can take exposure beyond the collateral posted. Second, margin can be reassessed on every trade and price update rather than at scheduled, periodic intervals, which addresses a timing mismatch that becomes material when prices move while traditional payment systems are unavailable. Third, every order, trade, funding payment, liquidation, and settlement is recorded near-instantly and immutably on a public ledger that any user, researcher, or regulator can independently verify, so a participant can confirm the rules were applied as disclosed and a supervisor can inspect market state directly rather than relying on records produced after the fact.

The transparency inherent to onchain markets appears to also improve investor outcomes rather than merely satisfying a disclosure requirement. Recent independent research by Barone and Lillo of the Scuola Normale Superiore in Pisa⁷ tests sunshine trading theory, which holds that publicly disclosing trading intentions reduces adverse selection and lowers execution costs, using onchain data and markets on Hyperliquid as a case study in which large orders disclose their terms from inception and remain visible while executing. Evidence for that proposition has historically been scarce because such disclosure is rare in traditional markets. We draw this to the Commission's attention as European academic work bearing directly on transparency objectives the EU has long pursued. Separately, where an instrument trades continuously alongside a benchmark which closes, there is evidence that prices formed while the benchmark is closed carry information rather than noise. Research published by HPC in August 2026,⁸ comparing 205 weekend closures in bitcoin markets and 19 in onchain oil markets, found that the benchmark reopening confirmed the price formed in the continuous market during the closure, and found no statistically significant evidence of harm to the benchmark markets referenced. This is consistent with the established finding in the market microstructure literature that trading outside core hours, though

⁷ Davide Barone and Fabrizio Lillo, *Trading in the Sunshine or in the Shade: Market Impact and Adverse Selection on Hyperliquid*, arXiv:2606.15715 (14 June 2026), <https://arxiv.org/abs/2606.15715>.

⁸ Hyperliquid Policy Center, *Perpetual Futures as Complements to Dated Futures* (21 August 2026), <https://hyperliquidpolicy.org/blog/perpetual-futures-as-complements-to-dated-futures>.

lighter, tends to be more informative because it is concentrated among participants acting on new information.

We have rated lending, borrowing, and custody more cautiously, for different reasons. In lending and borrowing, continuous and transparent collateralisation offers clear benefits, and our rating reflects the maturity of risk management practice rather than the merits of the model, as collateral diversification and stress calibration continue to develop. In custody, our rating reflects the stage of development rather than any deficiency in the model. Self-custody removes intermediary and insolvency risk, which is the risk the greater part of custody regulation exists to manage. The corresponding responsibility for key management rests with the user, and we would suggest the appropriate response is continued development of key management tooling alongside clear disclosure, as we address further at Question 64.

Payments fall outside HPC's direct expertise, and we have rated that use case modestly and defer to payment specialists.

We propose two actions:

1. Recognise onchain verifiability as a means of meeting transparency and recordkeeping objectives, rather than requiring parallel reporting which duplicates information already public.
2. Ensure that where supervisory attention is directed at these markets, it is focused on the controls which are determinative of resilience, in particular assurance that the software implementing a market's rules operates as those rules describe, and the governance of the price feeds on which margining and default management processes depend, as we set out in our responses to Questions 54 and 86.

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*

Risk	Rating
<i>Operational risk</i>	4
<i>Money laundering and terrorist financing risk</i>	3
<i>Market abuse</i>	2
<i>Investor protection risk (information asymmetry, no redress, opacity of functioning)</i>	3
<i>Financial stability</i>	2

Please explain your answers.

We thank the Commission for asking this question in a differentiated way, as we believe the risks associated with these markets vary considerably in character and are not well assessed as a single category.

We have rated operational risk highest, and it arises in two main forms. The first is the risk that software executing deterministically according to published rules contains an error, because such software may not be capable of amendment once deployed. The second is price feed dependency, where a feed which performs exactly as specified can still produce disorderly outcomes based on the conditions of the reference market. We address both, and the controls we believe are relevant to them, in our responses to Questions 54 and 86.

We have rated market abuse lower because observability offers both a useful deterrent and a means for post-abuse enforcement. Every transaction on an onchain order book is recorded publicly and in sequence. Abusive patterns such as spoofing, layering, and wash trading do not become impossible, just as they are not fully mitigated in traditional markets, but they become considerably more detectable, and any participant or supervisor can detect them rather than only the venue operator on request. That transparency operates both as an ex ante deterrent, because participants know that their activity is visible and cannot be amended after the fact, and as an ex post means of investigation and enforcement, because the complete record is available for analysis without depending on an intermediary to produce it. The relevant comparison is with a market in which the audit trail is proprietary and often made available to supervisors on a delayed cadence, rather than with a market free of abuse.

We have rated investor protection in the middle because the row combines three matters, two of which onchain markets improve and one of which presents additional challenges. Information asymmetry is materially lower where market data, positions, and liquidations are public rather than intermediated. Opacity of functioning is likewise reduced where the rules of the market are applied uniformly to every account and their application is verifiable, because a participant can confirm from the record that the stated rules were applied to their own position rather than relying on an assurance to that effect. Transparency of this kind is complemented by disclosure. Where a regulated intermediary provides access to these markets, clear disclosure of the characteristics and risks of the products concerned remains an important investor protection tool, and we address the disclosures we consider appropriate for perpetual futures in our response to Question 73. Redress poses additional challenges. Where there is no counterparty against whom a claim can be made, redress cannot follow the path it takes in traditional markets, and that is a risk for the investor.

Our lower rating for financial stability reflects the absence of the credit channel through which stress ordinarily propagates. Where positions are pre-funded and margin is assessed continuously, as is the case in the markets available on Hyperliquid, no participant ends a losing position owing sums to an intermediary, and losses are contained within the market in which they arise rather than transmitted through credit exposures to institutions elsewhere.

We have rated money laundering and terrorist financing risk as neutral. These risks are inherent to financial markets generally rather than specific to crypto-asset markets. The transparency afforded by onchain markets assists here as well, operating as the deterrent and the investigative resource we describe in relation to market abuse above. Supervisory effort is likely to be most effective where it is directed at the points at which value enters and leaves these markets, and at the regulated intermediaries which provide products and services using this infrastructure, rather than at the base layer of the network itself. Preserving the benefits of public blockchains depends on not re-intermediating the infrastructure layer. A regulated business conducts its activities over the internet without controls being imposed on the transport protocols beneath it, and the same allocation is appropriate here. The network is neutral infrastructure, and the obligations belong with the identifiable persons who control the connection between onchain and offchain systems and who offer regulated products and services to clients.

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*

Criteria for establishing absence of full decentralisation	Rating
<i>Existence of an identifiable intermediary (person or group of persons) providing a crypto-asset service</i>	3
<i>Presence of control by an identifiable person or group of persons (e.g. via admin keys) over the key functionalities of a DeFi protocol (e.g. upgradeability of protocol)</i>	5
<i>Significant concentration of governance power over the key functionalities of a DeFi protocol</i>	4
<i>Custody of user assets by the DeFi protocol</i>	4
<i>DeFi protocol code is not open source</i>	2
<i>Marketing of a DeFi protocol by an identifiable entity or person</i>	2
<i>Other</i>	5

Please specify to what other criteria(s) you refer in your answer to question 61:

We believe that the Commission's list of criteria at Question 61 should be supplemented in the following respects. The most operationally meaningful test is whether any person is able to halt, pause, reverse, or settle transactions at a chosen price, as that is the clearest evidence of discretion over a market. Closely related is the ability to alter economic terms unilaterally, including fees, margin parameters, liquidation thresholds, and price feeds. These capabilities are properly understood as features of a particular market rather than of the blockchain on which it operates. A deployer building a market intended to meet the requirements of a given jurisdiction may need precisely these tools, as the ability to suspend trading or to close positions in disorderly conditions is among the powers a regulated intermediary or venue operator would conventionally be expected to hold. Another market on the same blockchain may be deployed without them. Assessing the blockchain as a whole would therefore produce an answer which reflects neither market accurately, and would either attribute to the blockchain powers which only a particular deployer holds, or overlook powers which a deployer plainly does hold. This is why we encourage assessment at the level of the specific function and at the layer at which that function is performed. We also encourage the Commission to provide that assessment is made at a point in time with a duty to notify material change, as decentralisation is not a fixed attribute.

The criterion concerning custody of user assets is a strong indicator of decentralisation status, and one refinement would improve it. As drafted it attributes custody to the protocol, whereas the question which matters, in our view, is whether an identifiable person is able unilaterally to direct or appropriate user assets. Where users deposit funds to a non-custodial contract and those funds are subject to published rules that apply uniformly to every user, and no other person can unilaterally direct them, the arrangement does not raise the concern the criterion is properly reaching for. We would suggest the

criterion is more accurate, and more useful, if framed as unilateral control over user assets by an identifiable person.

Please explain your answers to question 61:

We set out further detail with regards to all categories in response to questions 62.1 as well as 63-65.

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

Question 62.1

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

For the purpose of this question, certification of a DeFi application should be understood as verifying that it robustly mitigates against smart contract vulnerabilities, operational risk in general and functions in accordance with its publicised performance.

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

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

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

In our view, MiCA should account for risks arising from decentralised applications by first identifying the layers at which activity occurs. Obligations can then attach where a person exists to bear them, and those persons sit at different layers and bear different responsibilities across onchain markets.

Onchain markets typically comprise three layers. The first is the blockchain itself, the neutral infrastructure whose network of validators applies a published set of rules (i.e., a protocol) to every transaction deterministically and without discretion. The second is the persons who build on that infrastructure, deploying markets or applications, defining their parameters, and making decisions about how they operate. The third is the regulated financial intermediaries which use those layers to provide regulated products and services to clients, including by offering clients access to them. Hyperliquid illustrates this division. The Hyperliquid blockchain provides the order books, margining, funding, and settlement functionality that every market on the network uses. Independent HIP-3 deployers⁹ build perpetual futures markets on that infrastructure and configure the assets listed, contract specifications, price sources, leverage limits, and risk limits for the markets they administer. A regulated intermediary may in turn offer its clients access to those markets. These are distinct persons making distinct decisions, and a framework which treats them as a single undifferentiated category will attach obligations either too widely or not at all. Applying that approach, we propose three ways in which onchain markets can be analysed, taking into account how they operate compared to traditional markets while still meeting supervisory objectives.

First, crypto-asset service providers (“CASPs”) are regulated and supervised entities, and we agree that risks should be accounted for appropriately at that layer. A CASP which offers its clients access to a decentralised application has made a decision in the exercise of its own commercial judgement, and it is an authorised entity which can properly be held to account for that decision. It should conduct proportionate due diligence, disclose the risks clearly, and be liable where it fails to do so or where its own systems, execution, or client handling fall short. Liability for outcomes a CASP did not cause and could not control is a different matter. Where a market or application fails for reasons entirely outside the intermediary’s influence, attaching liability to the intermediary does not improve the application and is likely only to result in fewer regulated firms offering access, with the predictable consequence that clients access these markets outside the regulated perimeter and without the protections it provides.

Second, the persons who build markets or applications on a blockchain are separate from the blockchain itself and must be assessed on their own facts. Such a person may be a firm that provides regulated financial services, or itself a provider of neutral technology that supports functionality on the blockchain network, and how that person is regulated should depend on what functions it performs and the level of discretion it actually exercises. Defining market parameters, configuring price feeds, and retaining the ability to suspend trading or settle positions are examples of functions such persons may

⁹ Hyperliquid Improvement Proposal 3 (“HIP-3”) is the framework through which independent market operators (“deployers”) design and deploy their own perpetual futures markets on Hyperliquid. The blockchain provides for, and the deployer cannot modify, trade execution, order matching in price-time priority, automatic enforcement of deployer-set margin requirements, funding payment transfers, clearing, and settlement functionality. The deployer configures the assets listed, contract specifications, price sources, leverage limits, and risk limits such as open interest caps. In this way, HIP-3 divides market functions typically split across several intermediaries (i.e., exchange, broker, clearing house) between the blockchain and independent teams. See Hyperliquid Documentation, *HIP-3: Builder-Deployed Perpetuals*, <https://hyperliquid.gitbook.io/hyperliquid-docs/hyperliquid-improvement-proposals-hips/hip-3-builder-deployed-perpetuals> (last visited 18 September 2026).

perform. Some of these functions resemble those a regulated venue operator or intermediary traditionally performs, and others do not. We encourage the Commission to consider the roles actually performed at this layer, whether each is a function that regulation has traditionally addressed, and how responsibility can properly be assigned and obligations tailored to the function performed. That analysis is separate from any determination about the blockchain on which the person builds. The distinction is essential, because a framework which treats the existence of an identifiable deployer as evidence that the underlying blockchain is not decentralised would produce results which do not reflect how these systems are constructed or operate in practice.

Third, at the level of the blockchain itself, where a function is executed according to published rules and no person is able to alter, suspend, or direct it, there is no one to whom an obligation can attach. We are not proposing an exemption from any applicable regulatory frameworks. An exemption presupposes a person who would otherwise be liable and is being relieved of liability. For genuinely deterministic functions, no such person exists, and the appropriate regulatory response is therefore assurance as to how the software operates, obtained by those who offer access to it, rather than ascribing liability. That assurance is the subject of the certification schemes the Commission raises at Questions 63 to 65, which we support.

Finally, we would urge the Commission not to pursue the option of confining CASP connectivity to applications servicing verified pools of liquidity. As we set out in our response to Question 56, a regulated firm may have good reason to operate a market with defined participation, and where it judges that appropriate we support it. A framework which requires it is a different matter. Mandating verified pools would confine EU participants to a fraction of available depth, with consequences for execution quality and price formation borne by the end investor, to achieve an outcome which regulated firms are already able to deliver where it is needed.

Question 63

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

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

☒ *Yes for the DeFi protocols and smart contracts providing some of the crypto-assets services defined under MiCA*

☐ *No*

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

We welcome the Commission's willingness to consider certification, which in our view is a constructive and well-judged proposition. Where certification should apply is best answered in the same way as where obligations attach, which we set out in our response to Question 62.1. The relevant unit of analysis is the activity and the layer at which it is performed. This reflects the approach the International Organization of Securities Commissions ("IOSCO") set out in its Final Report with Policy Recommendations for Decentralized Finance,¹⁰ which directs regulators to analyse an arrangement at the enterprise, functional, and technical levels, and to identify responsible persons by reference to who exercises control or sufficient influence over the particular activity, on the facts and circumstances rather

¹⁰ IOSCO, *Final Report with Policy Recommendations for Decentralized Finance*, FR/14/2023 (December 2023), pp. 35-36, <https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf>.

than by reference to labels. We encourage the Commission to take the same course, and IOSCO expressly contemplates that where only part of an arrangement offers a product or provides a service, the responsible person is to be identified in respect of that part.

We do not support certification as a blanket requirement across all decentralised applications. Certification carries real cost, and where it is applied too widely that cost falls most heavily on smaller and newer projects, with the unintended consequence of consolidating activity among a smaller number of established participants. We believe that the Commission's objective is better served by applying certification proportionately.

The blockchain layer and the persons who build and operate markets on it raise different problems and call for different instruments. Where a function is performed deterministically according to published rules, and no person is able unilaterally to alter, suspend, or direct it, there is no discretion to supervise and nobody to hold to account. What a user needs in that case is assurance that the software operates in accordance with its published specification. In onchain derivatives markets, the core functions the blockchain provides, including order matching, margin calculation, liquidation, and settlement, are applied uniformly to every participant, and no person building on the blockchain can unilaterally modify them. Certification is well suited to functions of this kind, and it is where the concept does the most good.

Where, by contrast, a separate person builds a market or application on a blockchain and retains discretion over how it operates, that person is carrying on an activity to which obligations may properly attach. In onchain derivatives markets the functions ordinarily ascribed to a single regulated entity are commonly distributed across several independent persons and the blockchain itself. Hyperliquid's publicly documented HIP-3 framework illustrates the division. The blockchain provides the deterministic execution functions described above, while a separate deployer specifies the market at deployment, including the referenced asset, the price sources, maximum leverage, and open interest caps, and may adjust certain parameters and halt trading in that market, with all such actions recorded onchain and independently auditable. Discretion of that kind is the type of activity the Commission should consider mapping onto traditionally regulated functions. The Commission should evaluate where discretion exists and over what, and formulate any obligations by reference to the functions each person actually performs, without ascribing responsibility for functions performed elsewhere in the arrangement.

Certification of software is not the right instrument for supervising a person's discretion, and obligations on a person are not the right instrument for assuring that software operates as specified. The two should be kept distinct. Assurance that software operates as specified may be obtained through independent audit, formal verification, or testing against the published specification, and it does not depend on any single method or on any particular licensing model for the software itself. We would encourage the Commission to approach this as the development of technical standards against which software can be assessed, rather than as a new form of authorisation. That is how assurance is delivered in cybersecurity, where standards are developed and applied by the private sector, certifiers are subject to public oversight, and a regulated firm relying on a certified product remains responsible for satisfying itself that the product is fit for the use it makes of it. We believe the same allocation is the right one here, and we develop this approach further at Question 65.

Certification is therefore most appropriate for the deterministic functions of a blockchain which do work analogous to the operation of a trading platform, the execution of transactions, and the holding of crypto-assets under published rules, being the services under Article 3(16) in which user assets are directly exposed to the operation of the software. Certification in this sense is assurance as to how software operates. It is not a form of authorisation, and it does not treat software, or the persons who develop or contribute to it, as providers of a crypto-asset service. We would not extend certification to software which does not allow a third party to hold or direct user assets, and we address non-custodial wallet software

specifically in our response to Question 64. The same analysis applies to lending and borrowing, though whether those activities should be brought within scope at all is a prior question the Commission addresses at Question 67.

We would also encourage the Commission to give careful attention to the element of its proposed definition requiring that an application function in accordance with its publicised performance. It is the most valuable part of the concept, and it addresses a deficiency which has already been identified internationally. IOSCO observed in its 2023 report that a smart contract audit may verify only that code implements a particular design, without providing meaningful assurance that the design is fit for purpose, that it functions as it purports to function, or that it is governed as it purports to be governed. The Commission's formulation speaks directly to that gap. It is also the element which will be hardest to specify, and it merits dedicated technical work rather than treatment as a subsidiary aspect of security auditing. HPC is prepared to contribute to that work.

Finally, we would emphasise that certification will achieve the Commission's objective only if it operates as a genuine alternative to full authorisation rather than as an additional layer applied on top of it, and we expand upon this in our responses to Questions 64 and 65.

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*

Statement	Rating
<i>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</i>	5
<i>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</i>	1
<i>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</i>	1
<i>DeFi protocols and software developers offering the possibility to create and use non-custodial wallets should be incentivised to obtain a certificate</i>	4

Please explain your responses.

HPC strongly supports certification as an alternative to full authorisation, and we encourage the Commission to develop it as a central element of this review.

Obligations belong with persons who exercise discretion and perform regulated functions, and assurance belongs with software that executes deterministically. Our reasoning follows the approach we set out at Questions 62.1 and 63. We agree that where a person builds or operates a market and makes

decisions about how it runs, it is a responsible person in the sense IOSCO describes. In onchain derivatives markets, the functions ordinarily ascribed to a single regulated entity are commonly distributed across several independent persons and the blockchain itself. We encourage the Commission to provide not only for that distribution, but for obligations to be scoped and tailored to the functions each person actually performs. A person who specifies a market and configures its parameters performs functions the Commission should consider in that light, and should not, by reason of performing them, be treated as responsible for functions performed elsewhere in the arrangement.

Where software performs a function according to published rules and no person can unilaterally alter or direct it, authorisation has nothing to attach to, while the user's need for assurance remains. Certification meets that need, and it can be calibrated to what a blockchain or application actually does. This is how EU financial services law already treats technology dependencies. DORA proceeds on the basis that a financial entity relying on a third party for the ICT services which run its business remains, at all times, fully responsible for compliance with its own obligations. Certification should not displace that responsibility, and it should not be designed to. Instead, certification gives a regulated entity a sound basis for assessing the technology it relies on. The entity must still judge for itself whether that technology is fit for the use it intends. On timing, certification should be obtained before or soon after an application is made available to the public, which in our view provides meaningful assurance without becoming a pre-launch licensing gate by another name.

We do not support mandating specific compliance tools in the design of a blockchain network, because prescribed tooling would not achieve the intended supervisory outcomes. Specified tooling dates quickly, and a single set of requirements applied across systems which differ considerably in design and function is unlikely to be well calibrated to any of them. More fundamentally, technology and the risks it faces evolve at a pace that no fixed specification can match, so prescribed compliance conditions risk being rendered inadequate by new risk vectors while development is held to now-outdated requirements. A mandated tool also risks becoming a badge of compliance rather than compliance itself, certifying that a particular component is present without assuring that the outcome it was intended to secure has been achieved. IOSCO raised the same concern about smart contract audits, which it observed may confirm that code implements a design without providing meaningful assurance that the design is fit for purpose. The more significant consequence is that prescription displaces responsibility. Where a system is built with a mandated component, the question of whether it meets supervisory objectives risks being treated as answered, when it is precisely the question the persons building and operating it should be accountable for. We would therefore encourage the Commission to express this requirement as an outcome to be achieved, and to hold the relevant persons accountable for achieving it.

Mandatory certification of software enabling users to create and control their own keys would impose cost without addressing the risk it is aimed at. Such software does not allow a third party to hold or direct user assets. As we noted at Question 59, self-custody removes intermediary and insolvency risk, which is the risk the greater part of custody regulation exists to manage, and a requirement restricting its availability would push users toward intermediated arrangements. We do support incentivised certification. The primary issue in self-custody is key management, and a voluntary scheme setting standards for recovery mechanisms and user disclosure would do considerably more to support consumers.

HPC is prepared to contribute to the technical work certification will require, in particular as regards audit standards, technological and cybersecurity best practices, and the specification of what it means for an application to function in accordance with its publicised performance. We remain at the Commission's disposal to discuss this following the close of the Consultation.

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*

Statement	Rating
<i>Certificates should be issued by qualified private sector entities</i>	5
<i>Certificates should be issued by qualified public sector entities</i>	2
<i>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</i>	5
<i>Only fully decentralised DeFi protocols that reach a certain significance (e.g. based on total value locked) should be required to obtain a certificate</i>	4
<i>CASPs should not be allowed to connect clients with DeFi protocols that are not certified</i>	2

Please explain your responses.

We strongly support certification being delivered through qualified private sector certifiers, assessing against published technical standards, and subject to appropriate public oversight of the certifiers themselves. We would encourage the Commission to build on the approach already taken to cybersecurity assurance rather than to construct something new for this sector.

We are more cautious about public issuance of certification for three reasons, none of which goes to principle. The expertise required is technical and specialised, and at present it sits largely outside supervisory authorities. Building it would take time, and certification is most useful if it is available in a timely manner as onchain finance continues to scale at pace across the EU and globally. Most importantly, a certificate issued by a public authority will in practice operate as an authorisation, and the concern we raise at Question 63, that certification becomes an additional layer rather than a genuine alternative to full authorisation, is considerably harder to avoid where the supervisor is also the issuer. A competitive market in certification is also better placed to keep pace with how quickly these systems change, although we acknowledge that this balance may shift in time as supervisory capability develops.

We would also encourage the Commission to be clear about where responsibility sits once a certificate exists. Certification should inform the assessment a regulated entity makes and should not replace it. This is the allocation DORA already adopts, under which reliance on a third party for ICT services does not transfer regulatory responsibility. A regulated entity which builds a market on a protocol, or which connects its clients to one, should be responsible for satisfying itself that the software meets the relevant standard and is fit for the use it makes of it, and certification gives it a reliable basis on which to do so.

We would place particular emphasis on the proposal that any interested party be able to request certification of a fully decentralised application. As we set out at Question 62.1, where no person exercises

discretion over a function there is by definition no applicant, and a scheme which requires one would be unavailable precisely where the assurance is most needed. Allowing a deployer, an intermediary, or another interested party to seek certification resolves that gap, and we encourage the Commission to retain it.

We also support a significance threshold. Certification carries real cost, and directing it to systems of material scale reflects both where user exposure is greatest and the proportionality the Commission has applied elsewhere in MiCA.

Finally, we are more cautious about preventing CASPs from connecting clients to uncertified applications. As we set out at Questions 56 and 62.1, our concern is with certification operating as a condition of access. A CASP should conduct proportionate due diligence and disclose risks clearly, and certification would be a valuable input to that assessment. That is consistent with the allocation described above, under which the responsibility remains the CASP's and certification informs it rather than discharges it. Making it a precondition, however, converts an alternative route into a licensing gate, so that software which cannot be certified because no person can apply is foreclosed from the EU market regardless of how it operates. It may also remove software from the market that falls below the significance threshold. An artificial constraint of that kind would undo much of the benefit the Commission is seeking to create.

Question 69

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

☒ *Yes*

☐ *No*

Prediction markets present both opportunities and risks for EU markets. The principal opportunity is informational. Prediction markets aggregate dispersed information into a single observable price, and that price has demonstrated forecasting value which financial terminals, media organisations, and researchers use. They also allow participants to hedge exposures to real-world events which existing instruments do not address well, which is a legitimate risk management function rather than a speculative novelty. Where such markets operate onchain, settlement is verifiable and positions are publicly observable, which supports both market integrity and supervisory oversight.

The risks are equally real and we acknowledge the concerns underlying ESMA's public statement of 3 July 2026.

Our submission, which we set out further at Question 70, is that contracts referencing financial variables carry the economic features of derivatives and are properly treated as financial instruments under MiFID II. Prediction markets are not the principal focus of this response, and we have therefore not set out detailed views on how such contracts are best calibrated, though HPC would be pleased to assist the Commission on those questions.

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*

Please explain your answer to question 70:

We thank the Commission for raising this question, and consistent with our analysis throughout this response, we encourage it to begin from the distinction between the contracts in question rather than the technology on which they are recorded.

A contract referencing a financial variable, such as an interest rate, an inflation print, or a commodity price, serves a risk transfer and information aggregation function and belongs within financial regulation. Such contracts carry the economic features of derivatives, and they are properly treated as financial instruments under MiFID II. Contracts that reference other events which are not inherently financial, however, could raise additional regulatory and public interest considerations that may be better addressed by frameworks Member States have developed over many years. We therefore encourage the Commission to resist any approach which treats DLT-enabled prediction markets as a single category, as the ledger on which a contract is recorded does not determine which of these it is. This is the same argument we make in our response to Question 1.

While calibration of these contracts is not our principal focus in this response, we would be happy to continue to discuss this topic with the Commission as its thinking and position continue to evolve. Onchain markets can improve consumer outcomes in meeting supervisory objectives for prediction markets. Where contracts, positions, and resolution are recorded publicly and in sequence, the resolution of a contract rests on verifiable and auditable sources bolstered by onchain transparency, and a participant or a supervisor can confirm that the stated rule was applied to the stated facts. We encourage the Commission to take this into account in considering what assurance requirements are proportionate.

On distribution, we recognise the existing product intervention framework and ESMA's recent supervisory statement, and we are not asking for either to be revisited in this review. As ESMA and the Commission consider these instruments further, and as the responses to this Consultation inform that work, HPC would support a phased approach to distribution under which participation could broaden as evidence accumulates on how these markets perform.

Question 71

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

Please see our response to Question 70 above.

Question 72

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

☒ *Yes, by MiFID*

☐ *Yes, by MiCA*

☐ *No*

Please explain your answer to question 72:

Please see our full response to Question 73 below, which also addresses this question.

Question 73

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

We thank the Commission for engaging with perpetual futures directly, and we welcome the decision to address them in this review rather than leaving their treatment to be worked out case by case across Member States.

A perpetual future is a standardised, cash-settled derivative with no predetermined expiry date. Its terms are uniform for every participant, with a fixed unit quantity, a specified reference asset and price source, a specified settlement currency, and defined margin parameters, and contracts within a listing are fungible. A participant enters a position by buying or selling the contract on a central order book and exits by offset, entering the opposite position in the same contract. Holding the contract conveys price exposure to the reference asset without conferring ownership of it, and a position may be held indefinitely so long as adequate margin is maintained.

In place of an expiry date to force final settlement, as is standard in dated futures contracts, a perpetual future uses a periodic funding payment between long and short positions to hold the contract price to the price of the reference asset. At fixed intervals, the premium or discount of the contract's trading price is measured against the reference price. If the contract trades above the reference price, holders of long positions pay holders of short positions a funding amount proportional to the gap, and if it trades below, shorts pay longs. Funding is calculated under a published formula and settled on an aggregate basis between all longs and all shorts. In the markets described in this response, funding is not a fee, and no venue, deployer, or intermediary collects any portion of it. The mechanism creates a continuous incentive that pulls the contract price toward the reference price, which is why the contract requires no terminal settlement date.

These design features give perpetual futures a market profile distinct from dated futures, and they expand the choice of instruments available to market participants. Perpetual futures offer market participants several advantages compared to dated futures, including that:

- Liquidity concentrates in a single contract per reference asset rather than spreading across successive dated tenors;
- A hedger maintaining exposure over a long horizon holds one position continuously, without the mandatory rolls of a dated contract and the transaction costs, timing risk, and operational overhead they carry;
- Contract sizes are typically tied to a single unit of the reference asset, which broadens access for participants whose desired exposures do not fit benchmark contract denominations; and
- Position management is simpler, with no tenor selection at entry and no expiry monitoring over the life of the position.

Empirical work also indicates that perpetual futures are additive to the dated futures markets they reference. HPC's research comparing continuous perpetual futures markets with benchmark dated futures found that prices formed while the benchmark was closed predicted the benchmark's reopening price, and found no statistically significant evidence of degradation in the quality of the incumbent dated markets.¹¹ Research studying nearly a decade of trading data finds that perpetual futures hold their

¹¹ Hyperliquid Policy Center, *Perpetual Futures as Complements to Dated Futures* (21 August 2026), <https://hyperliquidpolicy.org/blog/perpetual-futures-as-complements-to-dated-futures>.

liquidity better than dated futures during large price movements and track spot prices more closely through them.¹²

Assessed by their economic features, perpetual futures are derivatives, and they carry the characteristics of the derivatives MiFID II already recognises. They are standardised, fungible, and cash-settled; they can be offset; they provide exposure to a reference price without conferring ownership of the underlying; and they are anchored to that reference through a published mechanism. There is no good reason to depart from the MiFID II framework for an instrument of that description. Perpetual futures are another derivative type, and MiFID II, a globally respected framework built to accommodate instruments of that kind, is appropriately situated to govern them, as we indicated at Question 72. ESMA reached the same view at paragraph 47 of its Article 2(5) guidelines, and as we set out at Questions 1 and 2, that reasoning turns on the economic features of the contract rather than on what it references.

The Commission should not create a new instrument category in Annex I. A new category would require amendment at Level 1, which is the same objection we understand the Commission to be weighing in relation to MiCA, and in our view it is unnecessary. The existing Annex I categories are drafted by reference to economic characteristics rather than to particular product names, and they accommodate these contracts already. Clarity in application, rather than new legislation, is what would assist in regulating perpetual futures appropriately and proportionately, and HPC is prepared to support the development of guidance to that end.

The calibration developed for contracts for difference (“CFDs”) is not the right starting point for perpetual futures. The two products differ in ways which bear directly on the risks the 2018 measures were designed to address, and we set out the principal differences below.

First, the two products differ in market structure. The measures adopted in 2018 were directed at a market in which the firm offering the product is typically the counterparty to its client, with the conflicts of interest and information asymmetries that arrangement creates. A CFD is a bilateral contract whose terms, pricing, and closure the provider controls, and the provider profits when its client loses. A perpetual future trades on a central order book against other participants at market prices, the venue does not take the other side, and the relationship is multilateral. The conflicts which motivated the original calibration do not arise in the same way, and that is relevant to what proportionate treatment looks like.

Second, the two products differ in the transparency of their pricing and costs. ESMA’s 2018 intervention identified the complexity and lack of transparency of CFDs, including the costs and charges embedded in the provider’s price, as a source of investor detriment.¹³ A perpetual future’s price forms on a public order book, its funding methodology is published in advance, and each funding payment is calculated under that formula and, in onchain markets, recorded on a public ledger. The participant observes the price at which the contract trades and the cost of holding the position rather than accepting a provider’s quote. Onchain markets also record every transaction publicly, so a participant can verify that the rules governing execution, margining, and close-out were applied to their own position as disclosed.

Third, several of the protections the 2018 measures impose are, in a pre-funded market, present by construction rather than by requirement. It may assist the Commission to have a worked description

¹² Will Gornall et al., *Perpetual Futures and Basis Risk: Evidence from Cryptocurrency* (last revised 19 May 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5036933.

¹³ See ESMA Decision (EU) 2018/796 of 22 May 2018 to temporarily restrict contracts for differences in the Union, OJ L 136, 1.6.2018, p. 50 (identifying, among the features of CFDs giving rise to investor protection concerns, the complexity and lack of transparency of the product and the costs and charges borne by retail clients).

of how this operates in practice, and we describe below how a perpetual future in a market available on Hyperliquid operates, as its mechanics are publicly documented:

A participant posts collateral in a U.S. dollar-denominated stablecoin before any position can be opened, and margin is reassessed on every trade and on every reference price update rather than at scheduled intervals. Maintenance margin is set at half the initial margin at the maximum leverage for the asset. Where account equity falls below the maintenance requirement, the position is first sent to the order book for closure, and where that succeeds the participant retains any remaining collateral. For larger positions, only a portion of the position is sent to the book initially, with a cooldown period before further action, which is designed to avoid a single close-out moving the price and triggering others. Liquidation is triggered on a mark price constructed as the median of several independent inputs, one of which is derived from the live order book, so that no single feed can determine it. Only where closure through the book does not restore the account above a defined fraction of the maintenance requirement does the position pass to a backstop liquidator, and only beyond that is any residual loss allocated against profitable positions on the other side, at the previous mark price rather than at a stressed print.

In practice, exposure cannot exceed the collateral posted, a losing position cannot end in a debt owed to an intermediary, and close-out occurs automatically under rules which are published in advance and applied uniformly across all accounts. Negative balance protection and margin close-out are therefore outcomes of the architecture of the blockchain rather than obligations imposed upon a provider. Where a position reaches backstop liquidation, the maintenance margin is not returned to the participant. That treatment is clearly disclosed, and it is not different in kind from the treatment of a defaulting participant's margin on traditional derivatives exchanges, where the clearing house applies the defaulter's margin to the cost of closing out its positions. Given these differences in market structure, MiFID II should be applied to perpetual futures with attention to how onchain markets operate and to how entities can meet supervisory expectations in different ways, rather than by duplicating the CFD requirements wholesale.

The functions described above are provided by the Hyperliquid blockchain itself. Its validator network applies the published protocol rules for order matching, margin calculation, liquidation sequencing, funding computation, and settlement uniformly to every user, and a deployer building a market on the blockchain cannot configure those functions. A market inherits them in the sense that the deployer takes them as given, in the way a participant on an exchange takes the exchange's matching engine and clearing arrangements as given. The deployer specifies the market at deployment, including the referenced asset, the price sources, the maximum leverage, the margin tiers, open interest caps, and funding multipliers, and may thereafter adjust certain of those parameters, update the price feeds, and halt trading in that market.¹⁴ Those decisions are recorded onchain and independently auditable. This distinction identifies the layer at which each of the considerations we set out below arises, and we encourage the Commission to scope any obligations to the functions actually performed at each layer.

¹⁴ In a future network upgrade, the Hyperliquid blockchain will support optional deployer configuration for permissioned markets, collectively referred to as HIP-3*. HIP-3* activation involves an onchain allowlist managed by the deployer and is designed to give deployers additional functionality to operate deployments consistent with requirements applicable to them. Like HIP-3 deployers, HIP-3* deployers are independent operators who use Hyperliquid as the onchain infrastructure layer for their own markets while retaining control of, and responsibility for, their deployment. See Hyperliquid Documentation, *HIP-3 Deployer Actions*, <https://hyperliquid.gitbook.io/hyperliquid-docs/for-developers/api/hip-3-deployer-actions> (last visited 18 September 2026).

The substantive requirements the Commission should consider follow from what determines key outcomes for participants, namely convergence, margin calibration and default management, loss allocation, and disclosure. Consistent with our response at Question 62.1, we encourage the Commission to consider, for each, the layer at which the relevant decision is made and how any obligation should be scoped to the function performed there. Where an identifiable person chooses a parameter, the Commission should consider how that choice maps onto functions regulation has traditionally addressed and how responsibility for choosing and disclosing it should be assigned. Where a function is performed deterministically according to published rules and no person can alter it, the appropriate response is assurance as to how the software operates, which is the subject of the certification schemes we address at Questions 63 to 65.

Convergence is the first consideration. Every futures market requires a mechanism that tethers the price of the contract to the price of the underlying asset. A dated future converges to the cash market once, at expiry, when physical delivery or final cash settlement forces the two prices together. A perpetual future has no expiry, so it requires a different anchor, and that anchor is the funding rate.¹⁵ At each funding interval the contract's premium or discount to the reference price is measured, and the resulting payment between longs and shorts makes it more expensive to hold the side of the market that is pushing the contract away from its reference, drawing the price back toward it. A perpetual future therefore converges continuously, at every funding interval, rather than once at expiry. Because the funding mechanism does the work that terminal settlement does in a dated contract, it should be transparent and predictable. We propose that the funding methodology be published in full, that the interval be defined and applied consistently, and that the reference price be derived from more than one independent input where possible so that no single source can determine it. Where funding is not a fee to the venue, that should be disclosed clearly, as it bears directly on how a participant assesses the cost of holding a position.

Margin calibration and default management procedures, including liquidation, are the second consideration, because a participant who cannot anticipate the terms on which a position will be closed cannot manage it. We propose that maintenance margin requirements and liquidation thresholds be published in advance with notice of change, that the mark price used to trigger liquidation be specified and constructed so as to resist manipulation, and that close-out procedures be designed to avoid amplifying stress. These are not theoretical propositions, and existing onchain markets already implement controls of this kind. Default management processes in the markets available on Hyperliquid are triggered on a mark price which combines external reference prices with the state of the order book, rather than on a single instantaneous book price, which makes the trigger considerably harder to move. Larger positions are not closed out in full at once. Only a portion is sent to the book initially, with a cooldown period before further action, to prevent a single close-out from moving the price and triggering cascading liquidations. Where a position is closed through the book, the participant retains any remaining collateral and no clearance fee is charged. A deployer updating the price inputs for its market cannot dictate the mark price, because the mark price is the median of the deployer's inputs and a component the blockchain computes independently from the live order book, and deployers of markets referencing traditional assets have documented further limits on how far a single update may move the price and how far the price may move while the underlying market is closed.¹⁶

Loss allocation is the third consideration, and the Commission should approach it as a design question rather than an exceptional one. Every derivatives architecture requires a means of restoring a

¹⁵ See Policy Statement Concerning the Listing of Perpetual Contracts, 91 Fed. Reg. 33,160, 33,161 (3 June 2026) (describing the funding rate as the substitute for expiry-based convergence in a perpetual contract).

¹⁶ See trade[XYZ], *Documentation*, <https://docs.trade.xyz> (last visited 18 September 2026) (describing reference price updates clamped to a fixed number of basis points per update, and discovery bounds which limit movement of the mark price around the last externally derived reference price while the underlying market is closed).

balanced book where ordinary close-out does not eliminate a shortfall, and EU law already recognises this. Under Regulation (EU) 2021/23, central counterparties (“CCPs”) are required to provide in their recovery plans, if applicable, for the reduction of gains payable to non-defaulting clearing members, and Article 30 empowers a resolution authority to do the same in resolution. Onchain perpetual futures markets reach the same requirement by a different route. Close-out is attempted first through the order book, then through a backstop liquidator, and only beyond those stages is any residual loss allocated against profitable positions on the opposite side, at the previous mark price rather than at a stressed print. The conditions which trigger that final stage, and the basis on which affected positions are selected, are published in advance and applied uniformly to every account.

Because every margined derivatives market has a mechanism of this kind, the regulatory task is to ensure that it is disclosed in advance, applied without discretion, and designed so as not to compound stress. The Regulation takes the same approach to disclosure, requiring clearing members to communicate clearly and transparently to their clients if and how measures in a CCP’s recovery plan may affect them. We therefore propose that the requirement be publication of the full close-out sequence, including any mechanism of last resort, rather than the mandating of any particular mechanism. That approach is consistent with default management in margined derivatives markets and CCPs globally, which share the objective of restoring a matched book without bad debt but retain discretion over the means, and whose tools differ across jurisdictions.

Disclosure is a necessary aspect of all of these requirements. To meet the requirements above, and to cover the other critical aspects of perpetual futures markets, we suggest disclosure of:

- Funding methodology, including illustrative examples where appropriate;
- The speed and irreversibility of automated close-out;
- The effect of leverage on a position;
- The derivation of the reference price and its limitations; and, where relevant; and
- The risk that a settlement asset deviates from its reference currency.

These matters relate to more complex market dynamics, and market participants would benefit from disclosures explaining them, which generic risk warnings often do not provide.

On client categorisation, we encourage the Commission to calibrate by category rather than apply a single limit uniformly, which better reflects both the variation in participant sophistication and the Commission’s own proportionality principle. We also support a phased approach rather than immediate expansion, which mirrors approaches taken in other jurisdictions and allows calibration to be tested against evidence before it is settled.

The Commission need not develop this calibration from first principles, because the direction of travel internationally is already discernible. Three regulators have begun to address perpetual futures directly:

- **United States.** The Commodity Futures Trading Commission (“CFTC”) approved the first perpetual future listed on a U.S. exchange, as a futures contract, on 29 May 2026, and its accompanying policy statement sets out the Commission’s expectations for the listing of perpetual contracts, including the role of the funding rate as the substitute for expiry-based

convergence and the review of contracts referencing new asset classes.¹⁷ On the same day, CFTC staff issued an interpretation categorising perpetual contracts offered by Deribit, a VARA-regulated exchange, as foreign futures, together with a no-action position permitting digital commodities and payment stablecoins to be deposited with a foreign broker to margin those positions, which supports the use of tokenised collateral in these markets.¹⁸ The CFTC has since sought comment on extending perpetual futures to physically delivered energy commodities and on 24/7 trading.¹⁹

- **Hong Kong.** The Securities and Futures Commission of Hong Kong published a high-level framework for perpetual contracts in February 2026²⁰ which addresses transparent and consistently applied methodologies for mark price, reference price, and funding rate, disclosure of funding inputs and settlement frequency, reference prices drawn from multiple independent sources so that no single entity can influence them, and a clear and pre-defined order of priority for default management and loss allocation with the circumstances triggering each stage disclosed.
- **Dubai.** The Virtual Assets Regulatory Authority has also begun to address comparable ground in its rulebook.

We do not suggest that the Commission adopt any of these approaches wholesale, as jurisdictional differences may be needed for different markets and the EU will need to determine what is proportionate across its Member States. The three regulators which have started to address this product have, however, arrived at a similar architecture, which indicates that the requirements we set out above are workable rather than aspirational. HPC would be pleased to provide a comparative analysis of the approaches taken across jurisdictions, together with operational data on how these mechanisms perform in practice, and we remain at the Commission's disposal to discuss this further following the close of the Consultation.

Question 86

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

We are grateful for the opportunity to raise matters not addressed elsewhere in the Consultation. We begin with a development which the Consultation's framing does not fully capture, and then turn to price feed governance and three further matters.

A distinct category of financial activity, which we describe as onchain finance, is emerging alongside decentralised finance and traditional finance, and it does not fit neatly within either.

¹⁷ Order Approving KalshiEX LLC BTCERP Futures Contract (CFTC, 29 May 2026), <https://www.cftc.gov/filings/documents/2026/orgdcmkexbtperporder26601.pdf>; Policy Statement Concerning the Listing of Perpetual Contracts, 91 Fed. Reg. 33,160 (3 June 2026), <https://www.govinfo.gov/content/pkg/FR-2026-06-03/pdf/2026-11020.pdf>.

¹⁸ CFTC Staff Letter No. 26-17, *Staff Interpretation Regarding the Categorization of Deribit Perpetuals as Foreign Futures and No-Action Position Regarding Digital Commodities and Payment Stablecoins Deposited to Margin Customer Positions with a Foreign Broker Under a Right of Re-Use* (29 May 2026), <https://www.cftc.gov/csl/26-17/download>.

¹⁹ Request for Comment on the Extension of Standard Futures Contracts to 24/7 Trading and on Perpetual Contracts Referencing Physically Delivered or Storable Energy Commodities, 91 Fed. Reg. 38,334 (25 June 2026).

²⁰ Securities and Futures Commission of Hong Kong, *A high-level framework for virtual asset perpetual contracts offering by virtual asset trading platforms* (11 February 2026), paragraphs 12 to 14 and 19, <https://www.sfc.hk/-/media/EN/files/ER/SFC-Perpetual-Framework/SFC-Perpetual-Framework-ENG.pdf>.

Decentralised finance, as the Consultation describes it, consists of software deployed on blockchains that operates without intermediaries, and it optimises for eliminating the need to trust any third party. Traditional finance rests on accountable institutions that customers trust to stand behind a product, operating on infrastructure those institutions own and control. Onchain finance pairs the two. It uses public blockchains, open to every participant on identical terms, as the infrastructure on which an identifiable and accountable firm offers a product it stands behind. The firm retains only as much control as its product requires, and the product inherits the properties of the public network on which it runs, including transparency, continuous operation, near-instant settlement, and verifiability by any party.

Stablecoins are the clearest example of onchain finance operating at scale. A regulated issuer holds reserves offchain and stands behind redemption at par, while the token itself moves across public blockchains that anyone can use, at any hour and in any country. MiCA's own architecture reflects this allocation. The Regulation places reserve, redemption, governance, and conduct obligations on the issuer, the identifiable person who backs the asset, and leaves the networks over which the token moves to operate as neutral infrastructure. The United States reached the same allocation in its federal stablecoin legislation, the Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025 (the "GENIUS Act"), which placed reserve, redemption, anti-money laundering, and sanctions obligations on permitted issuers and did not seek to regulate the public blockchain networks on which stablecoins are used.

Regulated derivatives markets illustrate how the same model extends beyond payment instruments. A public blockchain such as Hyperliquid provides deterministic order matching, margining, funding, clearing, and settlement functionality to every market deployed on it. A regulated firm can build a market on that infrastructure, configure the assets listed, the price sources, the leverage limits, and the scope of participation to meet the requirements applicable to it, and offer that market to its clients as a regulated product. Optional deployer functionality on Hyperliquid supports permissioned markets in which the deployer manages an onchain allowlist of eligible participants, which gives a regulated deployer the means to operate its deployment consistent with the requirements applicable to it. The regulated firm remains accountable for the product it offers and for the discretion it exercises, and the network beneath it remains open and neutral. The recent innovation exemption granted by the United States Securities and Exchange Commission reflects the same structure, providing a conditional, five-year pathway for permissioned onchain trading of tokenised listed equities in which identified firms set eligibility standards and bear the conditions of the exemption while the public ledger provides the trading and settlement infrastructure.²¹

The Consultation's framing does not fully capture this category. Part 4 approaches activity on public blockchains through the lens of decentralisation, asking whether an application is fully decentralised, which criteria establish the absence of full decentralisation, and how CASPs should treat applications that fall outside the perimeter. Those are important questions, and our responses to Questions 59 to 65 address them. Onchain finance presents a different case. The relevant activity involves an identifiable and accountable person from the outset, that person is or can be a regulated firm, and the applicable analysis is how existing sectoral regulation applies to a regulated product delivered over neutral public infrastructure, rather than whether the infrastructure itself is decentralised. A framework organised around the decentralisation of applications risks treating the firm's use of a public blockchain as a reason to doubt the firm's accountability, when the firm is accountable in exactly the way traditional

²¹ U.S. Securities and Exchange Commission, Order Granting Temporary Conditional Exemptive Relief, Pursuant to Section 36(a)(1) of the Securities Exchange Act of 1934, from the Definition of "Exchange" in Section 3(a)(1) of the Exchange Act for the Use of Certain Distributed Ledger Trading Venues for Tokenized NMS Stocks and from the Definition of "Dealer" in Section 3(a)(5) of the Exchange Act for Certain Liquidity Providers for Tokenized NMS Stocks, and Request for Comment, Exchange Act Release No. 34-106402 (17 September 2026), <https://www.sec.gov/files/rules/exorders/2026/34-106402.pdf>.

regulation expects and the blockchain supplies benefits that the firm's own infrastructure could not. Onchain finance strikes the balance between openness and regulatory accountability that this Consultation is designed to achieve. We encourage the Commission to recognise it expressly, by confirming that a regulated firm's use of public blockchain infrastructure to deliver a regulated product is assessed under the sectoral rules applicable to that product and that firm, and does not, of itself, alter the classification of the product or the status of the infrastructure.

Price feed dependency is a further operational risk in onchain markets, as we set out in our responses to Questions 54 and 60, and we encourage the Commission to consider it as part of this review. The risk arises even where a feed performs exactly as specified, because a feed can produce disorderly outcomes without being manipulated or failing. Where a reference market is thin, a single unrepresentative transaction can move a published price materially, and where that price determines margin requirements and triggers liquidations, the consequence falls immediately and irreversibly on participants who have done nothing wrong. As a starting point we propose three disclosure categories, attaching to the person which selects the price source for a market rather than to the provider of that source. The first is the basis of the reference price, covering which sources a market uses and how they are combined. The second is change control, so that a change to that choice is disclosed rather than made without notification. The third is behaviour where an underlying market is closed or an input fails, including any bounds on price movement, their consequences for liquidation, and the treatment of a disputed or erroneous price. Market deployers on Hyperliquid already follow practices of this kind. trade[XYZ], for example, publishes the sources and methodology of its reference prices, the clamps applied to each price update, and the bounds within which prices may move while the underlying market is closed, and every update it makes is recorded onchain.²² The Securities and Futures Commission of Hong Kong addresses each of these categories in its February 2026 framework for perpetual contracts, albeit directed at licensed platform operators rather than at the layered structures we describe at Question 62.1. What is absent is a common basis against which these arrangements can be assessed, and HPC would welcome the opportunity to contribute to developing one.

The Commission's certification concept, and in particular its requirement that an application function in accordance with its publicised performance, is well placed to address this risk and to include these categories of disclosure. We encourage the Commission to treat price feed governance as a component of that work rather than as a separate matter.

We also raise two further matters:

The first concerns the interaction between this Consultation and the Benchmarks Regulation warrants clarification. Where a reference price is constructed from multiple inputs and published for use in determining amounts payable under a contract, we encourage the Commission to consider how clarity can be provided as to the boundary with the benchmarks requirements.

The second is that permissionless deployment is a genuinely novel feature which future work should address expressly. As we set out at Questions 62.1 and 73, onchain infrastructure permits a separate person to deploy a market on a blockchain without the permission of, or any relationship with, the persons who develop or operate that blockchain. A framework which does not account for this will either attach obligations to a blockchain which cannot discharge them, or fail to attach them to the person which can.

²² See trade[XYZ], *Documentation*, <https://docs.trade.xyz> (last visited 18 September 2026). All deployer actions, including reference price updates, parameter changes, and trading halts, are recorded onchain and independently auditable.

In closing, we reiterate our thanks to the Commission for the breadth and care of this Consultation. Across our responses we have set out three positions:

- Classification is best assessed instrument by instrument and by reference to economic features, which is why we support retaining sectoral legislation for instruments which qualify as financial instruments and why we believe MiFID II is the appropriate framework for perpetual futures;
- Obligations are best attached to the persons who exercise discretion and perform regulated functions, at the layer at which each function is performed, which is why we support accountability both for regulated intermediaries and for persons which build and operate markets, and assurance through certification where a function is performed deterministically and no person can direct it; and
- Supervisory objectives are increasingly capable of being met in new ways, as onchain infrastructure makes observable by default much of what EU regulation has historically had to mandate.

We encourage the Commission to build on the strength of the existing framework rather than rebuild it, and to calibrate proportionately where market structure genuinely differs.

As reiterated throughout our response, we would be glad to support the Commission's work following the close of this Consultation. We would be happy to provide operational data on how the mechanisms described in our responses perform in practice, comparative analysis of approaches taken in other jurisdictions, worked examples to support any supplement to the ESMA guidelines, and technical input on certification standards and price feed governance. We remain at the Commission's disposal and would welcome the opportunity to discuss any aspect of this response.