Hyperliquid Policy Center

November 18, 2026

VIA ELECTRONIC SUBMISSION

Cryptoasset Policy Team
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Re: Consultation Paper CP26/36, Cryptoasset Perimeter Guidance, and Guidance Consultation GC26/7, Decentralised Finance (DeFi)

Dear Sir or Madam:

Hyperliquid Policy Center ("HPC" or "we") appreciates the opportunity to respond to Consultation Paper CP26/36, Cryptoasset Perimeter Guidance ("CP26/36"), and Guidance Consultation GC26/7, Decentralised Finance (DeFi) ("GC26/7"), which the Financial Conduct Authority (the "FCA") published in October 2026. We commend the FCA for addressing directly how its perimeter, and its expectations of the firms it regulates, apply where financial activity takes place on public blockchains. Our responses to selected questions in CP26/36 are set out in Appendix 1 to this letter, and our responses to the questions in GC26/7 are set out in Appendix 2.

HPC is an independent, not-for-profit research and advocacy organisation that works with policymakers towards clear regulatory frameworks for onchain markets, including those available on Hyperliquid. The two consultations are timely. The new regime for cryptoasset activities takes effect on 25 October 2027, the FCA's application window is open, and firms preparing applications need to understand how the perimeter applies to arrangements that distribute across several persons the functions a single firm has traditionally performed. Regulated firms in the UK and elsewhere are also beginning to use public blockchains as infrastructure for regulated products, and the expectations in GC26/7 on operational resilience and financial crime will shape how readily they can do so. We welcome the FCA's technology-neutral starting point, under which the relevant inquiry looks to the functions a person performs rather than to the labels attached to an arrangement. In our view, the final guidance can give that principle practical effect in a way that advances the FCA's operational objectives and its secondary objective of international competitiveness and growth.

Public blockchain networks offer several properties that can improve how markets function for the firms and consumers that use them:

- **Transparency and verifiability.** A public blockchain records every transaction publicly, in sequence and in a form that no participant can later amend, so that any user, researcher or supervisor can confirm independently that the rules applied as disclosed.

- **Detection and investigation of financial crime.** Transparent and verifiable records support the detection and investigation of illicit activity, as one of the FCA's own case studies illustrates, and allow a firm or supervisor to reconstruct an incident without depending on the records of the affected entity.

- **Operational resilience.** A network maintained by a distributed set of validators continues to function even when an individual participant fails, which avoids the single points of failure that can arise when a firm relies on a centralised service provider for a critical function.

- **Settlement efficiency.** In onchain derivatives markets, matching and settlement occur in a single state transition against pre-funded collateral, so that no settlement window accumulates counterparty exposure.

- **Continuous availability.** Public blockchains provide always-on infrastructure that firms can use to reduce operational frictions and make their services available outside traditional market hours where appropriate.

Taken together, these properties can give consumers greater confidence in the markets they use and give supervisors a clearer view of those markets, and they can help firms meet their obligations more efficiently than legacy infrastructure allows.

These properties are most valuable when regulated firms can build on them. In what we describe as onchain finance, an identifiable and accountable firm uses public blockchain infrastructure that is open to every participant on identical terms, and retains only as much control as the regulations applicable to its product require. The firm remains responsible for the product it offers, and its clients benefit from the transparency, availability and settlement efficiency of the network beneath it. Open infrastructure also lowers the cost of building new products and interfaces, which supports competition among the firms that serve consumers, and deep, transparent order books with active liquidity provision deliver tighter spreads and more reliable execution for retail and institutional participants alike. Our responses suggest several ways in which the final guidance can preserve these benefits, principally by attaching obligations to the persons who exercise discretion over regulated activities and to the regulated firms that serve clients, while recognising the neutral role of the networks on which they build.

HPC thanks the FCA for the care evident in both consultations. We welcome the opportunity to discuss our responses with the Cryptoasset Policy Team, to provide technical briefings on how onchain markets operate, or to assist in developing the illustrative examples we suggest in our responses. We look forward to continued engagement as the FCA finalises its guidance.

Respectfully submitted,

/s/ Jake Chervinsky
Jake Chervinsky
Chief Executive Officer
Hyperliquid Policy Center

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

Appendix 1: Responses to Consultation Paper Questions

This Appendix contains HPC's responses to selected questions in the Financial Conduct Authority's Consultation Paper CP26/36, Cryptoasset Perimeter Guidance ("CP26/36" or the "Consultation Paper").[1]

Part 1: Decentralisation

Question 1

Do you agree with the FCA's interpretation of the legislative provisions proposed in the draft perimeter guidance in section 18.1? If not, please explain why.

Hyperliquid Policy Center ("HPC" or "we") agrees with the interpretation of the legislative provisions that the Financial Conduct Authority ("FCA") sets out in section 18.1 of the draft perimeter guidance, and we welcome the FCA's decision to address decentralisation directly. We support the FCA's threshold observation that the perimeter is technology neutral, such that the analysis turns on the functions performed and the role of each person, rather than on whether an arrangement is described as decentralised. HPC has supported the same principle elsewhere, including in our response to the European Commission's Targeted Consultation on the Review of Regulation (EU) 2023/1114 on the Markets in Crypto-Assets ("MiCA"), where we encouraged an approach under which the regulatory treatment of an activity follows its substance rather than the technology through which a person carries it on.[2]

Before turning to the specific provisions, we would note that, as the FCA recognises in the consultation, PERG interprets the perimeter rather than sets it. The perimeter itself is established by the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (the "Cryptoassets Regulations") and the related amending instrument, We welcome the fact that the draft guidance already draws on the explanatory memorandum in which HM Treasury ("HMT" or "Treasury") set out the intent of the legislation, notably in its discussion of the technical services exclusion. We would encourage the FCA to maintain that alignment with HMT's materials, including its policy note, as it finalises the guidance, so that the final guidance gives effect both to the legislation and to the policy it was designed to deliver.

We welcome the FCA's decision to apply the analysis person by person, and its recognition in the Perimeter Guidance manual ("PERG") that where no person is carrying on a regulated activity, the question of authorisation does not arise.[3] We believe that this approach will result in the correct allocation of regulatory responsibility in onchain markets. In our view, regulatory obligations belong with persons who have unilateral control over a function that is a regulated activity, and with persons who offer regulated services, products or activities directly to clients. Where software executes a function according to published, non-discretionary rules, and no person is unilaterally able to alter, suspend or direct the application of those rules, there is no person to whom an obligation can, or should, attach. Because those

---

1 Financial Conduct Authority, *CP26/36: Cryptoasset Perimeter Guidance* (October 2026), https://www.fca.org.uk/publication/consultation/cp26-36.pdf. References in this Appendix to provisions of PERG that CP26/36 would add or amend are to the draft text set out in Appendix 1 to CP26/36, and other references to PERG are to the Perimeter Guidance manual as currently published.

2 Hyperliquid Policy Center, *Response to the European Commission's Targeted Consultation on the Review of Regulation (EU) 2023/1114 on the Markets in Crypto-Assets (MiCA)* (30 September 2026), responses to Questions 1 and 45, https://hyperliquidpolicy.org/micaresponse/2026-09-30_hpc_mica_review_consultation_response.pdf [hereinafter HPC MiCA Response].

3 *See* PERG 18.1.17, 18.1.18, 18.1.20.

rules are published and the resulting transactions are publicly visible onchain, any participant can see how such a function operates. Regulated firms that choose to rely on such a function can, in addition and where appropriate, obtain or provide assurance that the software operates as specified, in support of their own obligations, as we describe in our response to Question 2 of GC26/7 in Appendix 2.

This allocation is also consistent with HMT's own analysis of the new regime. In the policy note accompanying the Cryptoassets Regulations, HMT explained that where an activity is carried on with no person who could be said to undertake it by way of business, no authorisation requirement arises, and that the FCA would assess in each case whether there is a "*sufficiently controlling party*" that ought to be authorised. **The FCA's person-by-person approach reflects the same understanding, with control as a central question, and is consistent with the principle of "same risk, same regulatory outcome" that underpins the regime.**. Where no person **holds unilateral control** over a function, the intermediary risks, which we cover in more detail below and which authorisation intends to address, are absent, and attaching obligations to a person who could not discharge them would offer consumers no additional protection.

The person-by-person approach suits the way onchain markets are organised, because those markets distribute across several distinct persons the functions that have historically been ascribed to a single firm. In GC26/7, the FCA draws on the work of the Financial Action Task Force ("FATF") and the International Organization of Securities Commissions ("IOSCO") to describe this type of system as a "DeFi stack" of settlement, asset, protocol, application and aggregation layers.[4] The settlement layer at the base of that stack comprises the foundational distributed-ledger infrastructure on which financial and non-financial applications are built, and general-purpose public blockchains such as Ethereum and Hyperliquid sit at this layer.

On some blockchains, the state transition logic supports functions such as an order book and the margining and settlement of positions. On other blockchains, those functions are left to smart contracts or other software deployed by third parties. As a practical matter and from a regulatory perspective, this is a distinction without a difference. In either case, those functions remain part of the foundational infrastructure, because the validators apply them under the same published rules, uniformly to every user, as they apply to any other transaction, whether that functionality existed at the genesis block or was added later by third-party developers. FATF has recognised that its standards do not apply to underlying software or technology, and attach instead to the persons who use that technology to conduct financial activity as a business.[5]

Validators on a proof-of-stake blockchain perform a neutral and technical role at the settlement layer. Each validator runs node software that contains the state transition logic of the blockchain, which determines, according to deterministic and predefined rules, how transactions are validated, ordered and added to the ledger. On such blockchains, no validator holds unilateral authority to alter or amend those rules. Where the rules call for validators to act collectively, for example in voting on changes to network parameters, the software combines their inputs by stake-weighted vote or median, so that no individual validator exercises discretion over the function concerned.

Separate persons and entities may build a range of applications onchain using a layer-one blockchain's base functionality, defining the parameters of those applications and making decisions about how they operate. Products built in this way are already varied. For example, a stablecoin issuer may use a public blockchain as the infrastructure over which its tokens are issued and transferred, an issuer of

---

4 Financial Conduct Authority, *GC26/7: Decentralised Finance (DeFi)*, annex (21 October 2026), https://www.fca.org.uk/publication/guidance-consultation/gc26-7.pdf (describing the DeFi ecosystem as a multi-layered architecture by reference to reports of FATF and IOSCO) [hereinafter GC26/7].

5 Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, para. 67 (October 2021).

tokenised assets may do the same for the assets it brings onchain, and other persons may deploy markets in which those and other assets are traded, whether through order books or automated market makers, selecting what is traded and the parameters that apply. Some of those persons will themselves be regulated firms, as stablecoin issuers are in many jurisdictions. Regulated firms then use the resulting infrastructure and applications to provide products and services to their clients, including by offering clients access to them. These are distinct persons making distinct decisions. The infrastructure at the base is neutral and open to any person to build on, subject only to published technical specifications, so that a person who builds an application or provides its clients access to the functionality of the network requires neither the permission of, nor any relationship with, the persons who develop the blockchain's software or run its validator nodes. Where a person uses a public blockchain to offer a regulated product to its clients, that person's regulated activity does not bring other participants in the network within the regulatory perimeter. Persons who develop or contribute to the blockchain's software, or validate its transactions, contribute to the infrastructure on which the regulated activity is carried on, but do not, on that basis, carry on a regulated activity, as the FCA recognises in relation to software development at PERG 18.1.20.

The same allocation of functions is familiar from traditionally structured financial activity. A firm that operates a trading venue or offers brokerage services to clients requires authorisation for the regulated activities it performs, and the FCA's requirements apply to that firm in respect of those activities. The firm depends on the public internet, telecommunications networks and cloud computing networks to deliver its services, and it could not offer those services without that infrastructure. The providers of that infrastructure, in turn, are not subject to regulation in the same way as the firm. Instead, the regulated firm remains responsible, under its own operational resilience and outsourcing obligations, for the risks that its reliance on them creates. It manages those risks through due diligence before relying on a provider, ongoing monitoring of the provider's performance and resilience, testing of how its own services would withstand the provider's failure, and contingency arrangements that include the ability to move to an alternative. In our view, a public blockchain occupies the same position in relation to the persons who build on it and the regulated firms that use it.

We would therefore encourage the FCA to confirm in the final guidance that the analysis applies separately to each person by reference to the functions that person performs, wherever in the stack that person sits. The identification of a relevant person who builds on a blockchain, such as a person who configures and sets the parameters of a particular market, should not by itself determine whether any person carries on a regulated activity at the settlement layer. This approach would accord with the FCA's statement at PERG 18.1.17 that the fact that a person is identified in connection with an arrangement "does not, by itself, determine the perimeter outcome," and with the FCA's explanation in GC26/7 that its approach focuses on whether a firm carries on a regulated activity, rather than on where the firm sits in the stack.[6]

The FCA has expressed its view, at PERG 18.1.17, that a relevant person "may include a person who determines or materially influences that design or those inputs, criteria or parameters." In our view, however, setting parameters is not in and of itself sufficient to bring a person within the perimeter. The relevant question is whether, and to what extent, that person retains unilateral control over how a system operates once it is live. A person who develops a protocol's software, or who configures a market at launch with parameters that are published in advance and cannot afterwards be changed by that person or by anyone else, retains no such control, and should not be subject to obligations, or to a requirement for prior approval, either at launch or afterwards. More generally, persons who build on a blockchain perform a wide range of functions. As we set out in our response to the European Commission, how such a person is regulated should depend on the functions it actually performs and the level of control it actually exercises. Such a person may itself be a regulated firm that uses a public blockchain to offer a regulated

---

6 GC26/7, *supra* note 4, annex.

product to its clients, as we describe in our response to Question 5 of GC26/7 in Appendix 2. Any obligations that attach to such a person arise from its own role and remain its own. They do not make that person part of the blockchain on which it builds, and they do not extend to the persons who develop that blockchain's software, validate its transactions or support its wider ecosystem.

We encourage the FCA to confirm that, where a person's activities bring it within the perimeter, the resulting attribution covers the regulated activity to which those activities relate, and does not extend to functions that other persons perform elsewhere in the system. Onchain arrangements may divide the functions of a regulated activity among persons differently from the way in which a single firm has customarily performed them. A person that sets the parameters of a market may, for example, perform only some of the functions of a traditional trading venue operator, while the blockchain performs matching and settlement under published rules. We would also encourage the FCA to consider, in its wider rules for regulated cryptoasset activities, how obligations can be tailored to the functions a person actually performs. This approach accords with IOSCO's Policy Recommendations for Decentralized Finance, which identify responsible persons by reference to those "exercising control or sufficient influence" over a DeFi arrangement or activity.[7]

Among the features the FCA describes at PERG 18.1.17, we would suggest that the clearest evidence of unilateral control over a regulated activity is whether any person is able unilaterally to direct how that activity is carried on. In onchain markets, this may include the ability to halt, pause, reverse or settle transactions at a chosen price, together with the ability to alter economic terms unilaterally. Where these capabilities exist, they are generally held by the person offering a particular product or service, rather than by any person at the level of the blockchain. A public blockchain can support a wide range of financial products and services that carry differing levels of operator control, which is beneficial because it allows a person to use functionality designed to facilitate compliance with the requirements of a given jurisdiction. A person offering a market intended to meet those requirements may need precisely these tools, as the ability to suspend trading or close positions in disorderly conditions is among the powers a regulated venue operator would conventionally be expected to hold, while another product on the same blockchain may operate without them. Assessing the blockchain as a single arrangement could therefore mislead in either direction. It could treat the whole blockchain as subject to control because the person offering one product on it holds such powers, or it could treat every product on the blockchain as free of such powers because the blockchain itself is. The analysis is more accurate where it separates the persons who perform or offer regulated activities from the blockchain network on which they build.

We recognise the FCA's view at PERG 18.1.17 that the absence of unilateral or complete control by any single person does not necessarily determine the perimeter outcome. In our view, however, the presence or absence of such control is among the most significant considerations on the spectrum the FCA describes, because it determines whether any person is in a position to meet the obligations that authorisation would bring. As noted above, this is also aligned with the HMT's intention, expressed in the policy note to the Cryptoassets Regulations, that where an activity is carried on with no person who could be said to undertake it by way of business, no authorisation requirement arises, and that the FCA would assess in each case whether there is a "*sufficiently controlling party*" that ought to be authorised. By unilateral control, we mean the ability of an identifiable person, acting alone, to direct how a material function is performed, for example by suspending it, altering its terms or reversing its outcome. Where a person holds that ability, it holds discretion over the relevant function in a way that supports the attachment of regulatory obligations tailored to the scope of the functions the person performs. Where a function is instead a feature of a blockchain network that a dispersed group of participants maintains, as in a proof-of-stake network in which changes take effect only through the published, stake-weighted agreement of a quorum of validators, no individual holds that ability, and no individual could comply with

---

[7] IOSCO, *Final Report with Policy Recommendations for Decentralized Finance*, FR/14/2023, Recommendation 2 (December 2023), https://www.iosco.org/library/pubdocs/pdf/ioscopd754.pdf.

obligations framed around that function. Obligations should not attach to persons who lack control over a function, as they would have no means of discharging them. Where the FCA concludes that such an arrangement nonetheless involves a regulated activity, the appropriate consequence is that the activity cannot be offered in the UK in that form other than through a person able to meet the relevant obligations, such as a regulated firm offering access to it, rather than that obligations attach to persons who are unable to meet them.

Consistent with this, we agree with the FCA that none of these features "is necessarily determinative," that they do not "constitute a separate perimeter test," and that decentralisation "operates on a spectrum." These principles support an assessment of each function as the arrangement exists at a particular point in time, rather than a single and permanent determination about an arrangement as a whole. Functions that a person controls or administers centrally today may become further decentralised over time, and an initial determination should not remain dispositive if the underlying facts and circumstances change, including whether any person holds unilateral control over a function and the identity of any person who performs the relevant role. This approach accords with the FCA's observation at PERG 18.1.12 that the meaning of novel terms will likely depend on the facts and circumstances of the arrangements in question "at the relevant time." HPC would be pleased to support the FCA with worked examples of how these considerations apply in practice.

Question 2

Do you agree with the FCA's interpretation of the legislative provisions proposed in the draft perimeter guidance in section 18.2? If not, please explain why.

HPC broadly agrees with the FCA's interpretation of the legislative provisions in section 18.2 of the draft perimeter guidance. We support the FCA's confirmation at PERG 18.2.3 that the 'by way of business' test applies separately to each person's activities, and that the relevant inquiry is "not whether an arrangement is decentralised, but what role the relevant person performs within it." This is consistent with the approach we set out in our response to Question 1. Onchain markets redistribute, and in some cases may obviate the need for, the functions that a single firm has traditionally performed in the provision of financial services. Some of those functions are fixed in code that deterministically applies published rules in response to self-directed user inputs, such that no person exercises control over how they are performed. Others are performed by identifiable persons, including those who build on the network and the regulated firms that provide access to it, and those roles may or may not amount to a regulated activity depending on the facts and circumstances. Assessing each person by reference to the role it actually performs ensures that obligations attach only where a person carries on a regulated activity, rather than following the label attached to the arrangement.

We encourage the FCA to confirm in the final guidance that it assesses the factors it identifies, including the commercial character, continuity and scale of a person's activities, by reference to the regulated activity that the person carries on. Onchain arrangements may involve many persons who carry on genuine businesses in connection with them, such as operating validator infrastructure, developing software or providing technical services, without themselves engaging in a regulated activity. A validator may, for example, receive rewards for validating transactions under rules that apply uniformly to every user, without exercising any discretion over the markets or financial activity to which those transactions relate. The FCA already recognises at PERG 18.1.20 that developing software "is not, as such, a regulated activity." The same reasoning should apply to the 'by way of business' test, so that a person whose own activity is commercial is not, for that reason alone, treated as carrying on by way of business a regulated activity that another person performs elsewhere in the arrangement.

Part 2: Proprietary Trading and Market Making

Question 13

Do you agree with the FCA's interpretation of the legislative provisions proposed in the draft perimeter guidance in section 18.8.18A? If not, please explain why.

HPC agrees in general with the FCA's interpretation of the legislative provisions in section 18.8.18A of the draft perimeter guidance, and we support the exclusion it addresses. We agree with the FCA that the exclusion turns on whether a person's dealing is carried on for the purpose of providing a service to another person. A person trading on its own account, without offering any service to a counterparty, should not require authorisation.

We encourage the FCA to consider how its expectation regarding retail counterparties applies to trading on a central limit order book, and in particular how it serves the retail investors it is intended to protect. The draft guidance provides that the FCA "would generally expect" a service to be provided to a counterparty "where that counterparty is a retail investor." That expectation is well founded where a firm deals bilaterally with its own customers, as in the FCA's example of a dealing app or platform, because the retail investor relies on that firm for the price and terms of the transaction. The position differs on a central limit order book, whether it is operated by a company or accessible through a decentralised protocol. On such a book, orders are matched according to predefined and transparent rules, typically in price-time priority, which apply in the same way to every participant. On a conventional venue the operator's matching engine applies those rules. Onchain, the network's state transition logic applies them deterministically in response to user-directed inputs, and validators validate matched transactions in the same non-discretionary manner as they validate every other transaction on the network. Order books are also anonymous or pseudonymous in both onchain and conventional settings, so a proprietary trader posting orders to the book neither selects its counterparty nor generally knows whether that counterparty is a retail investor. Any service to the retail investor in that setting comes from the regulated firm providing access to the market, where there is one, and not from the counterparty whose order happens to match that of the investor.

Treating the presence of a retail counterparty as indicating that a service is being provided would, in this setting, work against retail investors. A proprietary trader cannot prevent its orders on a multilateral order book from matching against those of retail investors, so the only way for it to remain outside that expectation would be to withdraw from order books in which retail investors participate. Proprietary traders and market makers supply much of the liquidity on which order books depend, and the depth they provide produces tighter spreads, lower transaction costs and more reliable execution for every participant. Their withdrawal would reduce that liquidity, and the cost would fall on the retail investors who remain, through wider spreads and poorer execution, most acutely in volatile conditions when depth matters most. That outcome would sit uneasily with the FCA's aim, set out at paragraph 1.8 of the Consultation Paper, of supporting fair, transparent, orderly and resilient markets. Persons who do in fact provide a service to retail investors would remain within the other cases the FCA identifies. We would therefore encourage the FCA to confirm that this expectation applies where a person deals with a retail counterparty on a bilateral basis, and does not apply where the person's orders match against those of a retail investor through a multilateral order book, including where operated on a decentralised basis.

Part 3: Technical Service Providers

Question 14

Do you agree with the FCA's interpretation of the legislative provisions proposed in the draft perimeter guidance in sections 18.8.25 to 18.8.35? If not, please explain why not.

HPC agrees with the FCA's interpretation of the legislative provisions in sections 18.8.25 to 18.8.35 of the draft perimeter guidance, and we welcome the exclusion in article 9Z2A. In our response to the European Commission's review of MiCA, we identified the boundary between providing a regulated service and providing technology that enables a user to engage in financial activity on a self-directed basis as the boundary most in need of clarity, and we welcome the FCA's guidance on where that boundary lies.[8] It may assist to anchor this boundary in the risks that authorisation of an intermediary is intended to address. In our view, there are three intermediary risks: (i) the mishandling or misappropriation of a user's assets, (ii) conflicts of interest between the provider and the user, and (iii) the misuse of confidential or price-sensitive information. A provider that neither holds nor controls a user's cryptoassets, exercises no discretion over the user's transactions, and does not solicit, recommend, price or route them gives rise to none of these risks, and the exclusion should be available to it. Reading "merely," discretion, and substantive participation against these risks keeps the exclusion within its intended scope and avoids drawing neutral software into the perimeter.

We support the FCA's reading of the exclusion, which treats the exercise of discretion and substantive participation in transactions as central indicators, and does not turn on the technology a person uses. A person that merely provides a technical service allowing another person to access services provided by a third person, or to access a decentralised protocol such as one that supports an onchain market, without exercising judgement over that person's transactions or otherwise participating substantively in them, does not act as an intermediary and should not be regulated as one. We agree with the FCA's recognition at PERG 18.8.27 and 18.8.31 that charging a fee, or receiving remuneration by reference to transactions, does not of itself prevent a person from relying on the exclusion. This reflects the principle we set out in our response to Question 2, that the commercial character of a person's own service should not determine whether that person carries on a regulated activity that others perform.

We would note, however, that the treatment of remuneration needs to be further clarified. Article 9Z2A imposes no condition on how a provider is paid, and the HMT's explanatory memorandum is silent on fees, consistent with the FCA's recognition at PERG 18.8.27 that charging a fee does not deprive a service of its technical character. We encourage the FCA to confirm that a charge which is fixed, or a fixed amount or percentage per transaction, and which does not vary with the venue, protocol, route or counterparty the user selects, does not indicate substantive participation. Remuneration should bear on the analysis only where it varies with those choices, and so creates an incentive to steer the user, or where it is structured so that the provider takes responsibility for the execution outcome. A neutral, route-agnostic fee stands apart from the commission of an intermediary whose pay rises and falls based on where it directs a client.

We encourage the FCA to clarify how the third indicator at PERG 18.8.26, that the user ('C') rather than the provider of the technical service ('A') selects the service provider or decentralised protocol to be accessed, applies equally to an interface that connects to a single service provider or protocol or multiple providers or protocols. We agree that this indicator is relevant where a software interface or wallet offers access to several service providers, venues or protocols, if selecting among them involves the exercise of discretion over where a user's instructions are directed in a manner that significantly impacts the cost or quality of the outcome that the user obtains. However, it is clear at the outset that an interface

---

[8] HPC MiCA Response, *supra* note 2, response to Question 45.

that provides access to only one service provider or decentralised protocol involves no such judgement or impact. In that case, the user selects the service provider or protocol by choosing to use an interface that connects solely to it, and remains free to use another interface or none at all. We would encourage the FCA to confirm that an interface of this kind is consistent with the third indicator.

This reading is consistent with the drafting of the exclusion and with HMT's explanatory memorandum. Article 9Z2A of the Regulated Activities Order, inserted by the Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026 (the "Amending Regulations") describes article 9Z2A as taking outside the arranging activity a person who merely provides a technical service enabling another to access "*one or more*" services provided by "*one or more*" authorised or exempt persons or decentralised protocols. The reference to "*one or more*" indicates that the exclusion is as available to a provider that surfaces a single service, venue or protocol as it is to one that connects to several, so the number of options presented should not of itself be determinative. As the FCA recognises, "*discretion*" and "*substantive participation*" do not appear in article 9Z2A itself, instead they are the FCA's interpretation of the statutory word "merely," drawn from the explanatory memorandum, and should be read consistently with the intent that the HMT expresses therein. We therefore encourage the FCA to confirm that offering access to, or displaying the price of, a single provider or protocol does not of itself amount to discretion over, or substantive participation in, a transaction.

HPC's principal comments on this exclusion concern the meaning of 'decentralised protocol.' The legislation leaves the term undefined, and the FCA rightly treats it at PERG 18.8.32 as a novel expression to be interpreted by reference to how the relevant arrangements operate in practice. We welcome the FCA's recognition at PERG 18.8.32 that the legislation does not say that a decentralised protocol must "necessarily provide a service, carry on a regulated activity, or be a person capable of being authorised or exempt." This reading correctly treats the protocol as infrastructure rather than as a regulated party or organisation, consistent with our view that a public blockchain is neutral infrastructure and that any obligations arising in connection with it attach to persons by reference to their own roles, and whether they perform regulated activities, rather than to the infrastructure itself or persons who merely engage in technical activities supporting the network. We commend the FCA for its recognition that the involvement of persons in developing, maintaining, governing or using an arrangement "does not necessarily prevent the arrangement from being a decentralised protocol."

We do, however, encourage the FCA to anchor the considerations listed at PERG 18.8.32(2) to its own view, in the same paragraph, that a 'decentralised protocol' is unlikely to be a service controlled and operated by an identifiable person. As we set out in our response to Question 1, the clearest evidence of unilateral control is whether any person acting alone is able to direct how an activity is carried on, such as by halting, pausing, reversing or settling transactions at a chosen price, or by altering the economic terms on which an arrangement operates. However, we note that halting, pausing, reversing or settling transactions can be exercised through decentralised governance rather than by a single party exercising control and, therefore, the considerations at PERG 18.8.32(2) are relevant insofar as they evidence control of that kind, but should not of themselves prevent an arrangement from being a decentralised protocol. As provided in more detail below in our response to Question 1 of GC26/7 in Appendix 2, treating a safeguard as a mark against a protocol would discourage arrangements that are capable of recovering from an exploit or a hack.

As the FCA recognises at PERG 18.1.17, decentralisation operates on a spectrum. In our view, the relevant inquiry under article 9Z2A(2)(b) is whether, on that spectrum, any person is able to unilaterally control the manner in which protocol rules are applied to user activity. Where any person holds such control, it will typically relate to a particular product or service built on the protocol, rather than to technical functions involving the protocol itself. That a person has sufficient control over a product built on a blockchain to be carrying on a regulated activity should not prevent the blockchain from qualifying as a decentralised protocol, or change the treatment of those who contribute to its software or validate its

transactions. Public blockchains generally require ongoing maintenance and periodic upgrades, among other things to improve their security, performance and resilience, and those who validate transactions receive rewards for doing so. If either feature were sufficient on its own, few if any public blockchains could qualify as a decentralised protocol, and we do not understand that to be the intention of the legislation.

The legislation itself treats the operation of validator infrastructure as a technical function. Article 9Z9 of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (the "Regulated Activities Order") excludes from the activity of arranging qualifying cryptoasset staking a technical service that allows another person to participate in staking, including through the operation of a validator node, and the FCA's guidance at PERG 18.10 treats the operation of a validator node as a technical service.[9] As the FCA observes at PERG 18.1.12, the legislation uses both 'validator node' and 'decentralised protocol' as cryptoasset-specific terms. Read together, these provisions indicate that the legislation contemplates validators as participants that perform technical functions in support of blockchain networks, and that their presence and remuneration are expected features of the arrangements to which the decentralised protocol limb of article 9Z2A applies.

Like a public blockchain, the internet depends on protocols that identifiable persons maintain and upgrade over time, and regulators treat it as neutral infrastructure. Standards bodies and individual contributors develop the protocols on which the internet runs, such as TCP/IP, the Domain Name System and HTTPS, through open processes, and many of those contributors receive payment for that work. Regulators have not generally regarded those persons as providing the services that regulated firms deliver over the internet. We draw the same comparison in our response to Question 2 of GC26/7 in Appendix 2.

The Hyperliquid blockchain illustrates how a public proof-of-stake blockchain of this kind operates in practice.[10] Any person may run a validator node, subject to a published minimum self-delegation, and the network determines the active validator set transparently by reference to stake, which any holder of the network's native token may delegate. The network commits blocks only with the agreement of validators holding more than two-thirds of the total stake, and the composition of the validator set may change at any time. The validators apply the order matching, margining and settlement functions that markets on the network use under published rules, uniformly to every user, and no person who builds on the network can modify those functions. Validators receive rewards from a published emissions reserve. Contributors maintain and upgrade the network's software over time, and a change to the rules the network applies takes effect only if and when the distributed validator set collectively adopts and runs a new version of the node software.

HPC's position on upgradeability is consistent with the distinction we drew in our response to the European Commission, where we strongly supported treating unilateral control over a protocol's key functionalities as evidence that an arrangement is not fully decentralised.[11] The ability to impose a material change unilaterally, for example through an administrative key, is control of that kind. The maintenance of software whose changes take effect only with the agreement of a quorum of validators is not control of that kind, and none of these features gives any person discretion over how the protocol's rules apply to a

---

9 Regulated Activities Order, art. 9Z9 (as inserted by the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, SI 2026/102); PERG 18.10.2.

10 Hyperliquid Documentation, *Staking* and *Nodes*, https://hyperliquid.gitbook.io/hyperliquid-docs (last visited 5 November 2026). Descriptions of the mechanics of the Hyperliquid blockchain in this response are drawn from the network's public documentation as of that date.

11 HPC MiCA Response, *supra* note 2, response to Question 61 (strongly agreeing that control by an identifiable person or group of persons over the key functionalities of a DeFi protocol, such as its upgradeability, indicates the absence of full decentralisation).

particular user or transaction. We consider that an arrangement of this kind should qualify as a decentralised protocol for the purposes of article 9Z2A(2)(b), notwithstanding that persons maintain it, validate transactions on it and receive rewards in connection with it.

One further point on the "*decentralisation*" limb should be clarified by the FCA. As article 9Z2A treats the access provider ('A') and the protocol accessed ('V') as distinct, a person who develops or maintains a protocol, or a foundation or similar vehicle through which its governance participants organise themselves, should not be equated with the protocol and thereby denied the exclusion. A protocol is software, not a person, and the statute confirms this point by referring to "*a third person or a decentralised protocol*," only the first of which is a person. We encourage the FCA to confirm that developing or maintaining a protocol, with or without a formal arrangement, and organising governance through a legal entity, do not of themselves make a person the protocol. Instead, the relevant inquiry in each case is whether that person controls it, assessed against the criteria in our response to Question 1.

Finally, the draft guidance on this exclusion contains no worked examples. Given the novelty of the concepts involved, we would encourage the FCA to include examples in the final guidance. HPC remains at the FCA's disposal to assist in developing them, drawing on how onchain markets operate in practice.

Appendix 2: Responses to Guidance Consultation Questions

This Appendix contains HPC's responses to the questions in the FCA's Guidance Consultation GC26/7, Decentralised Finance (DeFi) ("GC26/7" or the "Guidance Consultation").[12]

Question 1

Do you agree with our description of the operational resilience risks that may arise when firms provide financial services using DeFi? If not, please explain why.

HPC welcomes the FCA's description of the operational resilience risks that may arise when firms provide financial services using DeFi, and we broadly agree with it. In our view, the operational resilience risks associated with DeFi differ from those found elsewhere in financial services in degree rather than in kind. We therefore support the approach at paragraph 3.8 of the draft guidance, which addresses the risks firms face through the familiar categories of technology failure, cyber risk, third-party dependency and concentration risk, and recognises that smart contracts, automated execution and interconnected protocols "may change the nature, scale or speed of those risks." This approach provides the right foundation for the further development of the FCA's expectations of regulated firms that interact with DeFi. It is also consistent with the FCA's statement at paragraph 1.9 of the draft guidance, repeated at paragraph 2.3 with reference to CP26/36, that the use of software, smart contracts or distributed ledger technology ("DLT") does not, by itself, determine whether an activity is regulated. We firmly support these guiding principles and believe that they allow firms to meet their obligations through the existing framework in chapter 15A of the Senior Management Arrangements, Systems and Controls sourcebook ("SYSC"), without a separate regime for DeFi.

To further strengthen the FCA's proposals, we would suggest two refinements which we believe would provide additional clarity and support for firms in carrying out their own assessments.

1. **The FCA's description of operational resilience risks would benefit from identifying the source of each risk.** A vulnerability in an application that a third party builds on a general-purpose blockchain differs from a fault in the functions of the blockchain itself, and both differ from a failure in the systems through which a firm connects to a network. A firm's ability to assess and mitigate each risk will differ accordingly, as will the persons to whom it can look when a disruption occurs. A firm mapping its important business services under SYSC 15A will reach a more accurate picture if it identifies, for each dependency, where the risk originates and whether any person is able to exercise unilateral control in a way that affects it. Our response to Question 1 of CP26/36 in Appendix 1 describes the same arrangements by reference to the persons or technology involved, distinguishing the blockchain itself, the persons who build on it, and the regulated firms that provide access to it.

2. **The difficulty of pausing, amending or reversing onchain functions after deployment, which the FCA notes at paragraph 3.11, reflects a design choice with both costs and benefits, rather than a risk alone.** The benefit is resilience and integrity, because market participants can rely on rules that are published in advance, applied uniformly to every participant and incapable of change by any single party. Conversely, the ability to pause or amend a system may concentrate control in whoever holds that power. Case Study 6 illustrates this, as the loss followed the transfer of administrative control under a zero-timelock configuration. We welcome the considerations the FCA identifies in that case study, including the concentration of administrative control and the use of timelocks, and would

[12] GC26/7, *supra* note 4. References in this Appendix to paragraphs of the "draft guidance" are to the draft non-Handbook guidance set out in GC26/7.

suggest that the description of this risk ask firms to consider in the same way whether intervention powers exist, who holds them and how they are bounded. That refinement would also align the description with the expectations on governance and change-control arrangements at paragraph 3.28.

We encourage the FCA to give comparable weight to the resilience properties that distributed infrastructure offers, so that firms assess the net position rather than the risks in isolation. Where a firm relies on a centralised service provider for a critical function, the failure of that provider can present a single point of failure. In November 2025, for example, a cooling failure at a third-party data centre on which a major derivatives exchange relied forced the exchange to halt its markets entirely.[13] A proof-of-stake network that a distributed set of validators operates continues to produce blocks so long as validators holding the required supermajority of stake remain online, so the failure of an individual validator does not interrupt the network. Because the rules governing the network are published in advance and the network records every transaction publicly and in sequence, a firm or a supervisor can also confirm how those rules were applied and reconstruct an incident without depending on the affected entity's own records, which directly supports the lessons-learned exercise at paragraph 3.33.

We note further that the guidance should not treat the mere existence of an intervention power as a negative feature. A power to pause a protocol or to correct a fault, where it is bounded and exercisable only through decentralised governance rather than by a single party, helps a protocol withstand and recover from incidents. The better approach is to weigh the security benefit and the misuse risk of each mechanism in context, rather than to treat either the presence or the absence of such a power as determinative. Treating a safeguard as a mark against a protocol would discourage firms from integrating the arrangements best able to recover from an exploit.

Question 2

Do you agree with our proposed guidance on how firms should assess and manage those operational resilience risks? Are there other risks or emerging practices we should consider?

HPC welcomes the FCA's proposed guidance on how firms should assess and manage operational resilience risks when providing financial services using DeFi, and we broadly agree with it. We particularly support the allocation of responsibility that the guidance sets out. Paragraph 3.39 recognises that firms "might rely on protocols, infrastructure and service providers that they do not control," and that firms within scope of SYSC 15A nonetheless remain responsible for understanding and managing the risks these dependencies create for their important business services. Paragraph 3.6 also makes clear that firms "cannot delegate any part of this responsibility to a third party." In our view, this allocation is correct. Responsibility rests with the authorised firm that chooses to use the infrastructure and delivers the regulated product or activity to its clients, and that firm can manage its responsibility through its own diligence, monitoring and contingency arrangements.

We also support the requirements at paragraph 3.40, in particular those requiring firms to "understand any limits on their ability to control or recover from disruptions impacting third-party services" and to "assess concentration risk and the availability of alternatives." These requirements fit the position of a firm that relies on a public blockchain, which operates according to published rules that a distributed set of validators executes, and which no single party, including the firm itself, may be able to

[13] *See* CME Group Inc., Annual Report (Form 10-K), Item 1A (26 February 2026), https://www.sec.gov/Archives/edgar/data/1156375/000115637526000009/cme-20251231.htm (stating that the company temporarily halted its markets after a critical cooling failure on 27 November 2025 at its largest data centre, owned and operated by CyrusOne, and that its markets opened the following day on a delayed basis).

amend. A firm in that position can still manage its dependency through measures that mirror existing practice, including by:

- Connecting to several independent nodes, in the same way that firms maintain redundant connectivity providers today;
- Monitoring network performance and proposed software upgrades, as firms already monitor the status and release notes of critical software vendors;
- Including network congestion and outages in its scenario testing; and
- Maintaining the ability to suspend its own client-facing services or migrate activity to alternative infrastructure, as firms do through exit and contingency plans for other critical third-party services.

HPC would encourage the FCA to confirm that firms may meet their regulatory obligations on this basis where they rely on public blockchain infrastructure. Paragraph 3.41 notes that SYSC 15A applies to relevant third-party arrangements "whether or not they constitute outsourcing," and that where they do, firms must also consider SYSC 8. Several of the expectations associated with outsourcing presuppose a provider with whom a firm can agree terms, such as contractual rights of access, audit and exit, and a public blockchain may have no such provider. Financial firms have long managed comparable dependencies on the public internet and telecommunications networks. They contract with connectivity providers but hold no contractual rights over the networks themselves or over the protocols by which those networks operate, and they manage that dependency through their own continuity and contingency arrangements. The FCA and the Bank of England took a similar view in FS26/1, observing that "[i]n line with other types of technology providers (e.g., cloud computing providers), DeFi software providers can play an important role in the provision of financial services."[14] The FCA should not expect firms to obtain greater control over public blockchain infrastructure than they can obtain over the other infrastructure on which regulated firms already rely. A requirement of that kind would place firms that use public blockchains at a disadvantage relative to firms that use conventional infrastructure carrying comparable risks, without improving their resilience. We would therefore encourage the FCA to state expressly that the requirements at paragraph 3.40 are the relevant means of managing that dependency.

As to emerging practices, HPC would draw the FCA's attention to assurance that software operates in accordance with its published specification. Where software performs a function according to published rules, and no person can alter or direct it, a firm relying on that function has no counterparty from which to obtain assurance, and must instead obtain assurance as to how the software operates. Independent audit, formal verification and testing against the published specification can each provide that assurance. Firms should retain flexibility in how they obtain it, because the methods for evaluating software continue to evolve quickly, and a prescribed approach could lock firms into current techniques when newer and better means of verification become available. Assurance of this kind supports several of the practices the FCA identifies at paragraph 3.14, including testing systems before deployment and managing technology and security risks. It should inform the firm's own assessment rather than replace it, consistent with paragraph 3.6, because the firm remains responsible for satisfying itself that the software is fit for the use it makes of it. In our view, this work is best developed through industry technical standards against which software can be assessed, in the way that assurance operates in cybersecurity. HPC would be pleased to contribute to that work and to any further engagement the FCA undertakes on these questions, including its forthcoming guidance consultation on the use of DLT.

---

[14] Financial Conduct Authority and Bank of England, *FS26/1: Tokenisation in Wholesale Financial Markets*, ch. 2 (September 2026), https://www.fca.org.uk/publication/feedback/fs26-1.pdf.

Question 3

Do you agree with our description of the financial crime risks that may arise when firms provide financial services using DeFi? If not, please explain why.

HPC broadly agrees with the FCA's description of the financial crime risks that may arise when firms provide financial services using DeFi. We recognise the risks identified at paragraphs 4.4 to 4.10 of the draft guidance, and we support the FCA's position at paragraph 4.12 that providing financial services using DeFi "does not automatically make firms non-compliant," and that firms should instead consider the risks specific to DeFi within their existing obligations under SYSC 6 and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLRs").

HPC recognises the significant increase in money laundering using cryptoassets that the National Risk Assessment 2025 identifies, and we would encourage the FCA to set the risks it describes in the wider context of financial services, in which financial crime is an inherent risk and not one specific to cryptoasset markets. DeFi-specific guidance on financial crime would be more balanced if it acknowledged this context, so that firms calibrate their controls to the risks their particular activities present rather than to the technology through which they deliver those activities.

HPC would also encourage the FCA to recognise the transparency of public blockchains as a feature that supports the mitigation of financial crime risk. Public blockchains record every transaction publicly and in sequence, and no participant can amend that record after the fact. Illicit activity remains possible on a public blockchain, as it does in traditional markets, but the public record makes such activity considerably more detectable. It acts as a deterrent, because participants know that their activity is visible, and it serves as a resource for investigation, because the complete record is available for analysis without depending on an intermediary to produce it. The draft guidance itself illustrates this in Case Study 4, where blockchain analysis linked those responsible for $SQUID to two further rug pulls. We return to how firms can draw on this property in our responses to Questions 4 and 6.

The growing use of regulated stablecoins in DeFi adds a further safeguard against financial crime. Regulated stablecoins increasingly serve as a primary asset for settlement and collateral on public blockchains, and the law of some jurisdictions requires their issuers to maintain controls capable of freezing and seizing illicit funds. In the United States, for example, the GENIUS Act permits an issuer to issue payment stablecoins only if it has the technological capability to comply, and will comply, with lawful orders to seize, freeze, burn or prevent the transfer of the stablecoins it issues.[15] Where such stablecoins serve as a principal asset for transacting and for collateralising positions, as they do on Hyperliquid, illicit actors face the prospect that funds they hold in that form will be frozen or seized. Issuer controls of this kind are an emerging deterrent to the use of DeFi for financial crime, alongside the transparency of the public record.

Question 4

Do you agree with our proposed guidance on how firms should assess and manage those financial crime risks? Are there other risks or emerging practices we should consider?

HPC agrees with the FCA's proposed guidance on how firms should assess and manage financial crime risks when providing financial services using DeFi, and we welcome its risk-based approach. The draft guidance asks firms to apply their existing obligations under SYSC 6, the MLRs and the FCA's Financial Crime Guide to the risks presented by their own use of DeFi. Paragraph 4.17 then sets out considerations against which firms can assess whether their systems and controls "remain proportionate."

---

[15] Guiding and Establishing National Innovation for U.S. Stablecoins Act, Pub. L. No. 119-27, § 4(a)(6)(B), 139 Stat. 419 (2025) (codified at 12 U.S.C. § 5903(a)(6)(B)).

This approach correctly places obligations with the firm that delivers regulated services, products or activities to its clients, which is also best placed to understand the risks of its own business.

Financial crime controls are likely to work best when directed at the points where value enters and leaves onchain markets, and at the regulated firms that provide products and services using this infrastructure, rather than at the base layer of the network itself. A regulated business conducts its activities over the internet without regulators imposing controls on the protocols beneath it, and the same allocation of governance and responsibility is appropriate here. The network is neutral infrastructure. 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. We support the approach in the draft guidance, which already reflects this allocation.

HPC also supports the expectations illustrated in Case Studies 5 and 6, that firms should assess a protocol's governance arrangements and the risks arising from any third-party interfaces they rely on before integrating the protocol into their services. Those expectations are consistent with the proportionate due diligence that a regulated firm should conduct when it chooses to give its clients access to a decentralised application.

As to emerging practices, HPC would draw the FCA's attention to firms' use of the public record itself. As we note in our response to Question 3, a public blockchain records every transaction publicly and in sequence, and the complete record is available for analysis without depending on an intermediary to produce it. This property directly supports several expectations in the draft guidance, including the consideration at paragraph 4.17 of whether firms' systems and controls "are capable of identifying exposure to illicit activity linked to wallet addresses, smart contracts or protocols," and the risk-sensitive monitoring of the "protocols, transaction flows and blockchain activity" involved at paragraph 4.22. Within a given ledger, firms can trace the source and destination of funds directly, without relying on records that another party produces after the fact.

Two clarifications would help firms apply this risk-based approach with confidence. First, the guidance should state that SYSC 6 and the MLRs call for reasonable, proportionate controls rather than the elimination of risk as regulation 19 of the MLRs already frames the obligation in terms of policies and procedures proportionate to the firm's business, and no programme can deliver a zero-tolerance outcome. Second, a firm should not be treated as acquiring the risk profile of every address through which an asset has previously passed. Blockchain analytics, and the enforcement approach of sanctions authorities in the UK and the United States, distinguish direct exposure, where value comes straight from an illicit or designated address, from attenuated exposure separated by intervening legitimate transactions, and calibrate the response accordingly. We encourage the FCA to confirm that a documented, risk-based programme that screens for such exposure and applies proportionate thresholds for enhanced due diligence and reporting meets the expectations in SYSC 6 and the MLRs.

Question 5

Are there other risks or emerging practices related to DeFi which we should consider?

HPC would draw the FCA's attention to one emerging practice in particular, which we describe as onchain finance. Alongside DeFi as the draft guidance describes it, regulated firms increasingly use public blockchains as the infrastructure on which they offer products for which they remain accountable. Onchain finance combines an identifiable and accountable firm with public blockchain infrastructure that is open to every participant on identical terms. The firm retains only as much control as its product requires, and the product inherits the properties of the 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, and the draft guidance itself anticipates further use cases

at paragraph 1.2, including tokenised financial markets. In such arrangements, the regulated firm remains accountable for the product it offers, and the network beneath it remains open and neutral.

The draft guidance already reflects much of this approach, stating at paragraph 1.9 that the use of software, smart contracts or DLT does not, by itself, determine whether an activity is regulated. Paragraph 3.20 likewise asks firms to treat the service delivered to the client, rather than the underlying technology or protocol, as the important business service. We would encourage the FCA to state expressly that where a regulated firm uses a public blockchain to deliver a regulated product, the obligations attaching to that product rest with the firm, and the firm's use of the network does not of itself bring the network, or network participants who do not engage in regulated activities, within the scope of the regulation that applies to the firm. We address the perimeter questions this raises in our response to Question 1 of CP26/36 in Appendix 1.

We would also encourage the FCA to reflect in its description of DeFi's potential benefits at paragraph 1.5 the properties that public blockchains offer by design. Onchain derivatives markets provide an illustrative example from one area of onchain finance, because matching and settlement occur in a single state transition against pre-funded collateral, so that no settlement window accumulates counterparty exposure. More generally, a public ledger records every order, trade and settlement near-instantly and immutably, and any user, researcher or regulator can independently verify that record. A participant can therefore confirm that the rules applied as disclosed, and a supervisor can inspect market state directly rather than relying on records produced after the fact. As we note in our responses to Questions 1 and 3, these properties also support firms in meeting their operational resilience and financial crime obligations. HPC remains committed to contributing to the FCA's further work in this area.

Question 6

Are there other steps that could be taken to reduce financial crime risks in DeFi? Are there other regulatory measures that we should consider to reduce the financial crime risks in DeFi?

HPC believes the most effective steps to reduce financial crime risk in DeFi build on the approach the draft guidance already takes. That approach directs controls at the regulated firms that provide regulated products, services and activities using this infrastructure, and at the points where value enters and leaves onchain markets, as we set out in our response to Question 4. We would caution against regulatory measures that re-intermediate the infrastructure layer, because such measures would risk losing many of the benefits that public blockchains offer and would not be fit for purpose given the scope of the activities that network infrastructure participants perform.

HPC would caution in particular against any measure that requires developers to build specific compliance tools into the design of a blockchain network or protocol. Prescribed tooling becomes dated quickly, and a single set of requirements applied across systems that differ considerably in design and function is unlikely to be well calibrated to any of them. 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. Controls at the application level, and at the regulated firms that offer products and services to clients, are better suited to the risks those firms manage, and those firms can amend them more readily as the risk landscape changes. We would therefore encourage the FCA to express any such requirement as an outcome and to hold the relevant regulated persons accountable for achieving it, consistent with the emphasis on regulatory outcomes at paragraph 1.1 of the Guidance Consultation.

The public record that blockchains provide is itself a significant resource for reducing financial crime risk, as we note in our responses to Questions 3 and 4. We would encourage the FCA to consider, including in its forthcoming guidance consultation on the use of DLT, how supervisors can formally recognise onchain verifiability as a means of meeting transparency and record-keeping objectives, rather

than requiring parallel reporting that duplicates information that is already public. HPC would be pleased to contribute to that work.