ANDREESSEN
HOROWITZ

18 November 2026

VIA EMAIL

Cryptoasset Policy Team

Financial Conduct Authority

12 Endeavour Square

London E20 1JN

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

Dear Cryptoasset Policy Team:

I. INTRODUCTION AND ABOUT A16Z

Andreessen Horowitz ("a16z" or "we") appreciates the opportunity to respond to the Financial Conduct Authority's ("FCA" or "Authority"): (i) consultation paper CP26/36 relating to cryptoasset perimeter guidance (the "PERG Guidance" or "CP 26/36") and (ii) guidance consultation GC26/7 relating to decentralised finance ("DeFi") (the "DeFi Guidance" or "GC 26/7").

We welcome the FCA's continued engagement with industry on the development of the new UK cryptoasset regulatory regime. The guidance the FCA adopts on the cryptoasset perimeter and DeFi will play a significant role in determining whether the UK becomes a hub for responsible blockchain innovation or an outlier that pushes activity offshore. While we appreciate the significant progress the FCA has made in drafting detailed PERG Guidance, especially with respect to the concept of decentralisation and the technical service provider ("TSP") exclusion, we still have certain material concerns that, if left unaddressed, could lead businesses and capital to build elsewhere in the near-term, and stymie innovation in the UK in the long-term.

As drafted, the PERG Guidance risks materially extending the perimeter of the new intermediary licensing regime to capture software providers that do not give rise to the intermediary risks this regime is intended to address. Requiring such providers to comply with the licensing regime would effectively result in a "re-intermediation" of a disintermediated system. Because such providers cannot comply without abandoning their model, the practical effect would be to exclude the technology from the UK market, with negative consequences for access to, and investment in, blockchain businesses and technology in the UK. The PERG Guidance likewise risks introducing uncertainty with respect to the application of the perimeter of the UK cryptoasset regulatory regime to businesses by not providing clarity on the concepts of "*decentralisation*", "*substantive participation*" and "*substantive intermediation*", which are susceptible to subjective interpretation and inconsistent application. This subjective interpretation and lack of clarity could further lead to regulatory arbitrage, which can be avoided and prevented by providing further clarity to the PERG Guidance, as explained below.

Our main concern is that the current draft of the PERG Guidance creates indicative criteria without providing the clarity required to enable the industry to clearly assess, and understand, whether certain providers, and protocols, fall within or outside the regulatory perimeter. However, we think that requisite clarity can be provided within the existing PERG Guidance in a manner that is aligned with HMT's intent as described in its policy notes and explanatory memoranda. We elaborate on those changes in the appendix where we provide suggested language amendments to the PERG 18 provisions in order to implement the changes discussed below. Those amendments are designed to build on the FCA's existing draft language with minimal changes and to reflect the scope of the powers authorised by the statutory instrument.

Significantly, we do not ask the FCA to create perimeter tests or exclusions that are not present in the statutory instrument. Instead, we ask the FCA to interpret the statutory tests and the TSP exclusion in new article 9Z2A, which HMT has laid before Parliament in the draft Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026 (the "Amending Regulations")[1] so that the perimeter guidance clearly distinguishes between business models that give rise to the risks the regime is intended to address (and are thus intended to be captured by the perimeter) and those that do not (and are thus not intended to be captured by the perimeter). We are of the opinion that this is necessary to achieve the faithful implementation of HMT's guiding principle of "*same risk, same regulatory outcome*".[2]

a16z is a venture capital firm that invests in seed, venture, and growth-stage technology companies, focused on AI, bio and healthcare, consumer, crypto, enterprise, fintech, games, infrastructure, and companies building toward American dynamism. As of 2026, a16z has more than £75 billion of regulatory assets under management across multiple funds, with more than £7 billion in committed capital for investing in crypto and other frontier technologies. In crypto, we primarily invest in companies using blockchain technology to develop protocols that people will be able to build upon to launch internet businesses.

We are committed to working with officials and regulators to address the specific risks and opportunities of blockchain technology. To that end, we have engaged actively in the FCA's consultation exercises on the design of the new regime. We participated in the FCA's Crypto Policy Roundtables and responded to several of its discussion papers and consultation papers. Most recently, we responded to Discussion Paper DP 25/1 and Consultation Papers CP 25/40, CP 25/41, and CP 26/13. We also provided detailed technical comments to HM Treasury ("HMT" or "Treasury") on the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (the "Cryptoasset Regulations"). We welcome additional opportunities to meet with FCA staff and to discuss our comments in more detail.

This response focuses on selected questions provided in CP 26/36 and GC 26/7. In relation to CP 26/36, we focus on the decentralisation guidance in PERG 18.1 to 18.3

---

[1] Draft Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026, laid before Parliament on 15 September 2026, https://www.legislation.gov.uk/ukdsi/2026/9780348287233; HM Treasury, Explanatory Memorandum to the Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026 (the "Explanatory Memorandum"); HM Treasury, Policy note: Draft statutory instrument amending the Cryptoasset Regulations (April 2026) (the "2026 Policy Note"), https://assets.publishing.service.gov.uk/media/69e63339de262afd82fcf96e/Policy_note.pdf.

[2] Explanatory Memorandum, para. 5.3 (retaining lending and borrowing involving UK qualifying stablecoin within the perimeter "*in line with the principle of 'same risk, same regulatory outcome'*").

(Questions 1 to 3) and the TSP exclusion in PERG 18.8.25 to 18.8.35 (Question 14). We then respond to selected questions in GC 26/7 on operational resilience and financial crime risks and guidelines. We recognise and respect that the FCA cannot change the perimeter through guidance, but only interpret it, and frame our recommendations accordingly.

II. EXECUTIVE SUMMARY

In this response:

- In Section III, we recommend that the FCA adopt an objective, control-based decentralisation framework to address how decentralisation can affect perimeter analysis, consistent with HMT's Policy Note to the Cryptoasset Regulations. We agree with the FCA's technology-neutral, substance-based framing, but the draft PERG 18.1 guidance relies on vague and open-ended factors. As such, draft PERG 18.1 does not provide administrable criteria that can be objectively applied to assess whether the operation of a given protocol should be attributed to a person when determining whether they are carrying out regulated activities. In particular, we recommend that the guidance:
    - includes objective, measurable criteria relating to operational, economic and governance control and states that, where the criteria indicating the absence of operational control are met, the FCA would not generally expect the autonomous operation of the protocol to cause any person to be deemed to be carrying on a regulated activity. We believe that this approach balances clarity with the need to preserve regulatory flexibility. We do not ask the FCA to state that certain criteria *automatically* exclude a protocol from the perimeter, but instead only to affirm that, where certain *indicia* of decentralisation are present, the FCA would not generally expect the autonomous operation of the protocol to cause any person to be deemed to be carrying on a regulated activity;
    - recognises that the absence of operational control in relation to a protocol means: (i) the operation of the protocol does not give rise to intermediary risks in relation to any person, and (ii) no person would be able to comply with the ongoing requirements of the intermediary licensing regime in relation to the operation of the protocol;
    - explains that the operation of a protocol over which no person has operational control should not be attributed to any person when conducting perimeter analysis, including to persons who develop, maintain or participate in the governance of the protocol without controlling it, or to a legal entity (such as a foundation or a decentralised unincorporated nonprofit association) through which such participants organise themselves;
    - clarifies how the application of this control-based approach forms part of the application of the ordinary perimeter tests that determine whether authorisation is required and is not a separate, *de facto* perimeter test.
- In Section IV, we respond to the new TSP exclusion in Article 9Z2A. We welcome this exclusion, but ask the FCA to interpret it consistently with HMT's Explanatory Memorandum to the Amending Regulations, so that it does not capture genuinely

non-custodial, non-discretionary software which enables users to access "*one or more*" services provided by "*one or more*" third-party providers—a particular concern given the expanded territorial scope of the new regime and the absence of the overseas persons exclusion. In particular, we recommend that the FCA:

- focus the analysis on the three intermediary risks the regime is intended to address: (i) the mishandling of users' assets, (ii) conflicts of interest, and (iii) the misuse of confidential or price-sensitive information;
- confirm that standard, objective user-interface features (dashboards, default routing, pre-integrated algorithmic routing, objective ranking and risk information) are technical in nature, and do not amount to selection, discretion or substantive participation;
- give the concepts of "*substantive participation*", discretion and transaction fees objective, administrable limits, including by reference to the "qualifying non-custodial software" and "*held out*"/assumption of responsibility tests previously suggested by a16z, and by permitting route-, venue- and counterparty-agnostic fees; and
- apply the control-based criteria when assessing whether a protocol is decentralised for purposes of relying on the TSP exclusion so that decentralisation turns on whether there is control over a protocol. Furthermore, the FCA should specify that the maintenance of a protocol does not, in and of itself, amount to control. It should also clarify that a person who develops or maintains a protocol without controlling it is not treated as the protocol itself (the "*A is not V*" problem), and should describe the reasonable precautions and due diligence that a provider should take so that it is not exposed where a protocol's decentralisation status changes without its knowledge (the status-over-time problem).

- In Section V, we respond to GC 26/7 on DeFi. We broadly agree with the operational-resilience and financial-crime risks the FCA identifies, but ask it to distinguish application-layer and bridge-layer failures from the base-layer consensus of permissionless networks, which can be more resilient than centralised or permissioned alternatives. In particular, we recommend that the FCA:
  - on operational resilience (Questions 1 and 2), identify controls at the application layer that firms operate, treat permissionless networks as shared infrastructure subject to network-level diligence, and recognise that non-custodial network participants such as validators, builders and remote procedure call ("RPC") nodes are not the right locus of control and that security and emergency mechanisms are resilience-enhancing; and
  - on financial crime (Questions 3 and 4), give operational content to the distinction between direct and indirect exposure to illicit activity, recognise on-chain transparency as a mitigant, confirm that SYSC 6 and the Money Laundering Regulations ("MLRs") require reasonable, risk-based controls located at the customer and application layer, and confirm that network-level participants such as validators do not stand in a customer relationship with any firm or user and are not financial-crime gatekeepers.

- This response also includes an appendix where we provide suggested language amendments to the PERG 18 provisions in order to implement the changes discussed below. Those amendments are designed to build on the FCA's existing draft language with minimal changes, and to reflect the scope of the powers authorised by the statutory instrument.

III. FCA CP 26/36 - A CONTROL-BASED DECENTRALISATION APPROACH TO THE UK CRYPTOASSET REGULATORY REGIME

Technology-neutral, substance-based approach

We agree with the FCA that "*[t]he perimeter is technology neutral*", and "*[t]he use of software, smart contracts, distributed ledger technology, distributed governance mechanisms or other technological arrangements does not determine whether there is a person carrying on a regulated activity for which authorisation is needed.*" We also agree that the analysis turns on "*the substance of the arrangements, rather than the terminology used to describe them.*"

However, guidance is only genuinely helpful if it sets out clear, objective criteria that can be applied predictably across different factual scenarios. Guidance that, in substance, does not go further than affirming that the application of the perimeter depends on all the facts and circumstances in each case does not advance the FCA's stated objective of giving market participants a clear view of when they will need authorisation, nor does it reduce the risk of them breaching the perimeter. Our comments below are therefore focused on how the FCA can buttress its decentralisation guidance with the objective criteria necessary to provide reasonable certainty to market participants.

The guidance needs objective, administrable criteria

As drafted, the PERG Guidance will necessitate subjective, case-by-case assessments of whether the operation of a protocol should be attributed to a person when determining whether they are carrying out regulated activities. This is because, although the current drafting mentions various factors that "*may be relevant to determining the perimeter*", it lists these in a non-exhaustive manner without providing guidance on *why* the factors are relevant to the statutory questions for determining whether a person should require authorisation under the intermediary licensing regime, or how they should be considered relative to one another.

Our prior responses to HMT and the FCA identified the specific risks that arise from the absence of objective decentralisation criteria. First, it enables bad actors to engage in "decentralisation theatre". We agree with the FCA that the final guidance should prevent this but, without objective control-based criteria, such actors will be able to claim that a protocol is decentralised when, in fact, it is not. Second, the absence of objective decentralisation criteria leaves entrepreneurs uncertain about whether and when the operation of protocols will be attributed to them for licensing purposes, which risks incentivising entrepreneurs to leave the UK for jurisdictions offering regulatory clarity. Offering objective decentralisation criteria also promotes the development of decentralised protocols, bringing about benefits including promoting competition, safeguarding rights, and more equitably rewarding stakeholders. Finally, the absence of such criteria may lead the regulator to inadvertently pick winners and losers. A clear, objective, merit-neutral framework guards against each of these outcomes, while engendering the benefits of decentralisation.

The following aspects of the current draft guidance are problematic in this regard:

- PERG 18.1.12 injects subjectivity into the interpretation of core statutory terms. It states that cryptoasset-specific terms such as "validator node" and "decentralised protocol" "*are not defined and they represent relatively novel concepts*", and that "*the meaning will likely depend on the objective facts and circumstances of the arrangements in question at the relevant time, as well as* ***the reasonable understanding of the parties involved***" (emphasis added). It also states that the meaning of these terms might change over time. The reference to "*the reasonable understanding of the parties involved*" is particularly problematic since, without a clear standard, different parties are likely to have different interpretations of core statutory terms. It also does not bear on whether a protocol is, in fact, decentralised. Anchoring the meaning of a statutory concept to the parties' subjective understanding, and stating that the meaning might change over time, injects precisely the uncertainty that the guidance needs to remove in order to achieve its goals. The guidance should tie the meaning of these terms to verifiable facts about the arrangement, not to parties' perceptions of them. This matters all the more because the Amending Regulations make "decentralised protocol" an operative condition of the TSP exclusion in article 9Z2A(2)(b) without defining it, so whether a provider can rely on the exclusion will turn on how the term "decentralised protocol" is read.

- PERG 18.1.17 is too open-ended and general to be useful. It identifies three categories of features that commonly arise in relation to decentralised arrangements which "*may be relevant to determining the perimeter*", but only "*as part of the overall factual matrix,* ***alongside many other potentially relevant considerations****"* (emphasis added). The three categories of features identified are*: (1)* ***governance and decision-making****, including whether a person has formal or legal control, discretion over decisions, or liability in relation to the service; (2)* ***operational and technical structure****, including whether anyone has control over its design and maintenance, or discretion over operations; and (3)* ***economic and commercial structure****, including whether anyone has financial or economic control, financial benefit, or control over expenditure*" (emphasis added). We agree that these three categories identify the right themes. However, as presently drafted they are a list of considerations without explanation of how they may bear on the statutory questions for determining whether a person should require authorisation under the intermediary licensing regime. In effect, they tell a market participant what the FCA may look at, but they do not tell the market participant what answer any given configuration of facts will produce or why. PERG 18.1.17 separately includes vague references to whether persons "*influence*", "*maintain*" or "*update*"—or materially influence the design of—relevant arrangements. PERG 18.1.17 further notes that these considerations *may* be relevant to determining whether a person should require authorisation under the intermediary licensing regime without explaining why this should be the case. For decentralised protocols and providers offering access to them, this introduces unworkable uncertainty. It is common for decentralised protocols to involve multiple persons performing actions such as upgrading software for cybersecurity purposes. However, involvement in such activities does not, in and of itself, amount to the ability to control a protocol and therefore does not give rise to any of the three intermediary risks that the regime is intended to address (*i.e.* the misappropriation or mishandling of users' assets, conflicts of interest between the provider and the user, and the misuse of confidential or price-sensitive information). Such persons should not be at risk of

requiring authorisation just as a result of such involvement. By contrast, persons who possess mechanisms of control over a protocol, such as the ability to unilaterally prohibit access to the system, should require authorisation. Objective decentralisation criteria enables market participants and regulators, alike, to distinguish between protocols that are controlled by persons and those which no one controls.

- The same open-endedness affects PERG 18.1.20 on "true DeFi". The draft states that the FCA "*has deliberately not sought to prescribe a comprehensive, deterministic test of what constitutes 'true DeFi'*", that "*[d]ecentralisation exists on a spectrum and does not give rise to a separate or distinct perimeter framework*", and that "*[a]ctivities relating to the development, operation, governance, maintenance, promotion or use of such arrangements will still require consideration under the ordinary perimeter tests.*" We do not ask the FCA to declare particular protocols "true DeFi" and others not. Instead, we ask it to give objective content to the one question that matters for the perimeter: Whether, on the facts, and as a general matter, any person carries on a specified activity merely as a result of the protocol's operation.

We acknowledge, and build on, the parts of PERG 18.1.17 to 18.1.20 that are helpful. For example, the PERG Guidance draft rightly accepts that "*[i]n some cases, technological arrangements may continue to operate without any person performing functions that are relevant to the carrying on of a regulated activity*", that "*the fact that a person developed software or performed a technical function does not, in itself, mean that the person is carrying on the particular regulated activity*", and that "*arrangements described as 'DeFi' may involve no person carrying on a regulated activity.*" Our recommendation is not to displace these statements. It is to supply the objective criteria that allow an entrepreneur, an investor, an adviser, and the FCA to determine, consistently, when they apply.

A control-based decentralisation framework

Consistent with HMT's Policy Note to the Cryptoasset Regulations, we recommend that the FCA introduce an objective, measurable control-based framework for determining whether a protocol is decentralised.

The FCA's PERG Guidance draft sits in the broader statutory and policy context of the Cryptoasset Regulations and HMT's accompanying policy notes and explanatory memoranda. In its Policy Note to the first draft Cryptoasset Regulations in April 2025, HMT explained that where specified activities are undertaken on a "*truly decentralised basis, i.e. where there is no person that could be seen to be undertaking the activity by way of business*", the requirement to seek authorisation will not apply. The Policy Note added that "*the FCA will determine in any given case whether there is* ***a sufficiently controlling party or parties*** *that ought to be subject to the requirement to be authorised in line with section 19 of FSMA*" (emphasis added).[3] In other words, the HMT's analysis states that, to determine whether specified activities are undertaken on a decentralised basis (and therefore sit outside the regulatory perimeter), the FCA will determine whether there is "*a sufficiently* ***controlling*** *party or parties*" (emphasis added). HMT thus clearly indicates that the core question in deciding whether a protocol is decentralised is control.

[3] We note that the approach to decentralisation in the HMT's Policy Note to the first draft of the Cryptoasset Regulations from April, 2025 does not appear to be amended by any subsequent explanatory memoranda issued alongside amendments to the statutory instrument that followed. Nor do the 2026 Policy Note or the Explanatory Memorandum depart from it, and the Amending Regulations now refer to decentralised protocols expressly in article 9Z2A(2)(b).

A truly decentralised protocol falls outside the perimeter precisely because there is no person operating or controlling it, and so no person conducting the activity by way of business. The Amending Regulations rest on the same premise. Article 9Z2A(2) makes the TSP exclusion available where the service accessed is provided either by a person that "*is carrying on a regulated activity*" and is authorised or exempt, or by "*a decentralised protocol*". Only the first limb requires any person to be authorised or exempt, which assumes that, where a protocol is decentralised, no person carries on the regulated activity through its operation. The extent and nature of a person's involvement are relevant only insofar as they demonstrate such control. The FCA's PERG Guidance is consistent with this approach. It accepts that the "*involvement of persons in developing, maintaining, governing or using*" an arrangement does not necessarily prevent it from being a decentralised protocol, and that "*the extent and nature of their involvement*" will be relevant.

The difficulty with the PERG Guidance is that, although it is applying a control test, it neither says so nor specifically defines control. Instead, it provides an open-ended list of features in PERG 18.1.17, and, in the TSP context, discusses the degree to which a person engages in "*ongoing maintenance and adaptation*" of a protocol in PERG 18.8.32. This approach risks misclassifying decentralised protocols. As with all open-source software, almost every decentralised protocol is maintained by someone. The difference is that, while maintainers of traditional open-source software in many cases retain substantial control over that software, maintainers of decentralised protocols do not and, therefore, their involvement (*e.g.* maintenance without operational control) does not give rise to intermediary risks and they should, accordingly, not be subjected to the ongoing requirements of the intermediary licensing regime in relation to the operation of the protocol. The crucial point is that a person may maintain a protocol without controlling it. A test based on the fact of maintenance, rather than control, would draw protocols that are decentralised into the regulatory perimeter, even though no person controls them.

What is relevant about a person's involvement is whether that involvement amounts to control. Although the HMT approached the question from the perspective of whether an activity should be regulated, and the FCA approaches it from the perspective of whether an arrangement is a decentralised protocol, the two are in substance asking the same question. We therefore recommend that, in alignment with HMT's stated intention, the FCA explicitly make *control* the organising concept for its decentralisation guidance.

We recognise that the draft guidance seeks to address the legitimate concerns that a group of participants, none of whom individually controls a protocol, might nevertheless collude to operate it jointly, or that a person who sets a protocol's parameters might remain the person carrying on the activity those parameters implement.[4] However, the control-based criteria address each of these concerns directly in three ways.

First, the criteria are not satisfied by the mere absence of a single controller. They ask whether any person, or any "*group under common control*" or "*coordinated group acting together*", has the ability to override, alter or direct the operation of the protocol or to determine the outcome of governance. A founding team, a foundation together with its

[4] PERG 18.1.17 states that a relevant person "may include a person who determines or materially influences that design or those inputs, criteria or parameters", that "the fact that decision-making, governance, operation or other functions are distributed between multiple persons does not necessarily prevent those persons from carrying on regulated activities", and that the fact that "no single person exercises unilateral or complete control" does not necessarily determine the perimeter outcome. It also notes that a person "can also include unincorporated associations".

contracted developers, or a small number of multi-signature signers acting in concert can be such a group if they can override, alter or direct the operation of the protocol or determine the outcome of governance, and a protocol that can be altered at will is controlled. Open, permissionless governance, in which any holder of a widely distributed token may propose and vote and in which no person or coordinated group holds the voting power needed to amend the protocol, is not. The distinction is one of fact, and it is verifiable onchain.

Second, a person who designed or deployed a protocol but has irrevocably relinquished the ability to alter its functionality, operation or rules has no ongoing role in its operation. PERG 18.1.18 correctly recognises that "*the fact that a person developed software or performed a technical function does not, in itself, mean that the person is carrying on the particular regulated activity.*" The choices embodied in an autonomous protocol are, after deployment, the protocol's and not the deployer's, in the same way that the author of an open-source library does not carry on the activities of everyone who later runs its code. Where a deployer retains an administrative key, an upgrade or pause right that it can exercise unilaterally, the position is different, and the criteria should identify that as operational control.

Third, the criteria distinguish participation in governance from control over a protocol, addressing the FCA's concern about unincorporated associations without treating every governance participant as if they are carrying on a regulated activity. Holding or voting a governance token does not, by itself, establish control, and this is so whether or not the participants have organised themselves through a legal entity for the purposes of limited liability, tax compliance, and contracting; the question is whether a person or coordinated group can direct the protocol's operation or determine governance outcomes. Governance participants increasingly use purpose-built vehicles, such as the decentralised unincorporated nonprofit association ("DUNA") recognised under the law of Alabama, West Virginia and Wyoming precisely so that participation in governance carries the legal protections of an entity without conferring on the entity or its members control over the protocol. Such an entity holds no administrative keys, cannot alter the protocol's operation, and does not intermediate any transaction. Treating the entity or its members as the person carrying on the activity merely because governance has been given a legal form would penalise the legal structuring that improves accountability, and would be inconsistent with the FCA's recognition in PERG 18.2.3 that the '*by way of business*' assessment is to be performed separately in relation to each person's activities. We therefore ask the FCA to confirm expressly that neither governance-token participation nor the use of a legal entity is sufficient, without evidence of control, to attribute the protocol's activities to the entity or its members.

We therefore recommend that the FCA define control objectively and assess it according to whether a protocol is operationally controlled. This approach builds upon the control-based decentralisation framework a16z has set out in its prior responses and publications,[5] and which the SEC and the CFTC adopted in March 2026 when they defined a

[5] *See* a16z, Recommendations Regarding a Safe Harbor for Applications from the Broker Registration Requirements of the Securities Exchange Act of 1934 (13 August 2025), https://www.sec.gov/files/ctf-written-a16z-def-safe-harbor-proposal-applications-081325.pdf; a16z and DeFi Education Fund, Recommendations Regarding a Safe Harbor for Certain Applications From the Exchange Registration Requirement of the Securities Exchange Act of 1934 (14 September 2026), https://www.sec.gov/files/ctf-written-input-andreessen-horowitz-a16z-defi-education-fund-def-091426.pdf; Miles Jennings, The CLARITY Act: Why It Matters, What to Know, and What to Do, a16z (18 July 2025), https://a16zfrontier.com/posts/article/genius-act-clarity-act-crypto-legislation-explained/; Miles Jennings, What Builders Need to Know About the CLARITY Act, a16z (14 May 2026), https://a16zfrontier.com/posts/article/clarity-act-what-why-matters/.

"*decentralized*" crypto system as one that "*functions and operates autonomously with no person, entity, or group of persons or entities having operational, economic, or voting control of the crypto system*":[6]

- ***Operational control*** is the ability of a person to override, alter or direct the operation of the network;

- ***Economic control*** is the ability of a person to extract value from the system through privileged rights, such as preferential token allocations or asset-creation authorities; and

- ***Governance control*** is the ability of a person, or of a coordinated group acting together, to determine the outcome of governance decisions unilaterally or through off-chain influence.

Assessing whether a protocol is decentralised for purposes of the intermediary perimeter only requires determining if it is operationally controlled because a protocol that is not operationally controlled does not give rise to intermediary risks. If no person can unilaterally override, alter or direct the operation of the network, then users of the protocol are not subject to common intermediary risks. Moreover, since such a protocol is not overseen by any person, no one would be able to comply with the ongoing requirements of the intermediary licensing regime in relation to it.

Although economic and governance control are not directly relevant to the intermediary perimeter, here we provide a brief overview of all three categories. Each category can be assessed against objective, verifiable criteria that can serve as indicators of control rather than a separate definition of a decentralised protocol:

- a network is **open source** where its code is freely and publicly available;

- **autonomous** where it operates and enforces transactions without human intervention and no person has unilateral authority to alter its functionality, operation or rules (operational control criteria);

- **permissionless** where no person can restrict or prohibit access to or operation of it (operational control criteria);

- **credibly neutral** where its code grants no person privileged rights to discriminate among users or use-cases (operational control criteria);

- **non-custodial** where participants retain sole control of their cryptoassets through their private keys (operational control criteria);

- **economically independent** where its value-driving mechanisms do not depend on any development company or issuer; and

[6] Securities and Exchange Commission and Commodity Futures Trading Commission, Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets, Release No. 33-11412, File No. S7-2026-09 (17 March 2026), n. 50 ("a crypto system is 'decentralized' if the crypto system functions and operates autonomously with no person, entity, or group of persons or entities having operational, economic, or voting control of the crypto system").

- **distributed** where no person or group under common control holds the voting power needed to amend it.

All three categories matter when assessing the risks involved with a specific token: economic and governance control bear directly on whether a token's value depends on the continuing efforts of an identifiable group. For the intermediary perimeter, *however*, the question is narrower. What makes a person an intermediary is the ability to control users' assets or transactions, and the category that is pertinent to that is operational control, *i.e.* whether the protocol is autonomous, permissionless, credibly neutral, and non-custodial. Of these, the non-custodial criterion is the most important, as it ensures that the user, and not any intermediary, retains control of their assets and that it is the user's instruction that initiates each transaction. As long as no person or coordinated group retains the ability to control users' funds or transactions, or to censor or override the operation of the protocol, the risks that the intermediary perimeter is intended to address are eliminated. This is the position we took in our submissions to the SEC on broker and exchange safe harbours for applications—the criteria that introduce intermediary-type risks are custodial and operational control, and a protocol that has eliminated both gives rise to none of those risks, whatever the position on economic control.[7]

Governance control is relevant to the intermediary perimeter in one respect, which we acknowledge. Where a protocol can be modified through governance, a person or coordinated group that controls governance could in principle change the protocol's operation, and so acquire operational control by that route. The criteria address this directly, and the guidance can resolve it by reference to objective design features rather than open-ended assessment. A protocol that is immutable, or whose governance can adjust only defined parameters (such as a fee tier or a collateral ratio) without the ability to move users' assets, censor transactions or replace the protocol's logic, presents no such risk. A protocol whose logic can be upgraded through governance presents the risk only if an upgrade can take effect before users are able to react to it, and standard mitigants resolve it: a mandatory timelock between the approval of an upgrade and its execution, together with the ability of users to withdraw in the interim, and the absence of any person or coordinated group holding the voting power needed to approve an upgrade alone. We ask the FCA to recognise these features in the guidance as indicators that governance participation does not amount to operational control. The Drift exploit described in GC 26/7, in which a small administrator group could execute critical changes under a zero-timelock configuration, is an example of a protocol that would fail these criteria, and it illustrates why objective criteria of this kind protect consumers rather than merely relieving providers.

Where operational control is absent, the operation of the protocol does not give rise to the intermediary risks this regime is intended to address in relation to any person. It also reflects a practical reality: a person cannot meet the ongoing obligations of an authorised intermediary for a protocol they do not control, so licensing such a person protects no one and simply results in innovation migrating offshore.

Significantly, the FCA need not make decentralisation dispositive, nor prescribe the deterministic test of "true DeFi" it has deliberately avoided. The control-based criteria can be

[7] *See* the a16z and a16z–DeFi Education Fund submissions to the SEC Crypto Task Force cited above, which identify custodial and operational control as the criteria that introduce intermediary-type risks and propose non-custodial design, automation, permissionless access and credible neutrality as the objective conditions for relief from broker and exchange registration.

expressed in the form the FCA already uses elsewhere in PERG 18: as indicators that tend to show that a protocol is not controlled by any person, such that, where they are met, the FCA would not generally expect the operation of the protocol, in and of itself, to cause any person to carry on a regulated activity. A statement of that kind creates no presumption of law and alters no statutory test. It tells market participants how the FCA will approach the ordinary perimeter questions in the one context in which the current draft offers no guidance beyond a list of considerations. Framed in this way, the criteria are merit-neutral and technology-neutral as they ask only whether control has been eliminated, not whether a protocol is useful or desirable, which protects the FCA from the risk, and the perception, of picking winners and losers.

Making control the organising concept is compatible with the statutory questions in PERG 18.1.11 that determine whether authorisation is required. Doing so does not create a *de facto* "*separate perimeter test*", which the FCA rightly disclaims, and it is not an alternative to the perimeter analysis. Instead, it forms part of the application of the ordinary perimeter test which determines whether authorisation is required. It simply gives an objective means of answering the first of the questions in the context of a protocol's operation—whether, on the facts, any person controls the protocol such that its operation should be attributed to that person and such person be subject to licensing.

Finally, the FCA's existing factors should be reframed as subordinate *indicia* of control rather than as free-standing tests. We ask the FCA to confirm expressly that the governance, operational, and economic feature lists in PERG 18.1.17 are non-determinative, that they are tied to the statutory questions in PERG 18.1.11, and that they are given objective, control-based content, so that they are not a "*separate perimeter test*" the FCA says it does not intend to create. In particular, the degree to which a person engages in ongoing maintenance and adaptation should not be determinative, because, as explained above, a person may maintain a protocol without controlling it. What should matter in every case is whether such involvement amounts to operational control.

Questions 2 and 3 – the 'by way of business' and 'in the UK' tests

We agree with PERG 18.2.3 that the "*by way of business*" assessment "*should be performed separately in relation to each person's activities*" and that "*the question is not whether an arrangement is decentralised, but what role the relevant person performs within it.*" That is the right approach, and it follows from the control-based analysis above. We ask the FCA to add that contributing code to an open-source protocol, running a node or validator, or proposing and voting on governance matters is not, in and of itself, the carrying on of a regulated activity by way of business by the contributor, node operator or voter, because none of those activities involves the person dealing in, arranging deals in or safeguarding the cryptoassets of any other person. A person who performs those functions and also controls the protocol is assessed on the basis of that control, not on the basis of the function.

On PERG 18.3.1A, we ask the FCA to reconsider the statement that the presence of "*persons established in the UK who are involved in (among other things) the governance, operation, maintenance, or development of decentralised arrangements*" may "*be sufficient to establish a territorial link with the UK.*" The territorial question arises only once a person has been identified as carrying on a regulated activity. Where no person controls a protocol and no person carries on a regulated activity through its operation, the location of its developers, node operators or governance participants is not relevant, because there is no

activity whose location calls to be determined. Read literally, the statement would mean that a UK-resident developer who contributes code to a protocol used worldwide, or a UK-resident token holder who votes on a governance proposal, could be sufficient to establish the UK nexus for an activity carried on by someone else, or by no one. That would give UK-based contributors a reason to relocate, which is the opposite of the outcome the FCA and HMT intend, and it would do nothing to protect UK consumers. We ask the FCA to confirm that the UK presence of persons involved in a decentralised arrangement is relevant to the territorial analysis only where those persons are themselves carrying on the regulated activity in question, and to tie that question to the control-based criteria.

IV. FCA CP 26/36 – The Technical Service Provider Exclusion

We welcome the new Article 9Z2A exclusion and the way the FCA has framed its purpose. PERG 18.8.25 states that "*article 9Z2A distinguishes the provision of technical access from substantive intermediation in respect of transactions in qualifying cryptoassets*", and that the exclusion "*addresses the risk that a person whose role is confined to supplying non-discretionary technical functionality could otherwise fall within the potentially broad activity of arranging deals in qualifying cryptoassets*". The FCA also rightly observes that the exclusion gives effect to the broader purpose of the legislation, expressed in HMT's Explanatory Memorandum accompanying the legislation, of removing unnecessary regulatory barriers while maintaining regulation of activities presenting material risks to consumers or market integrity. That is the correct approach, and it is the one we ask the FCA to follow consistently throughout PERG 18.8.26 to 18.8.35.

We also welcome two further statements of principle from the FCA. Namely, PERG 18.8.26 confirms that the exclusion does not fall away merely because a service adds value: "*[t]his does not mean that any added value or additional feature, or any feature that makes the service more useful, removes A from article 9Z2A and makes the exclusion unavailable.*" Furthermore, PERG 18.8.27 confirms that "*[a] service does not cease to be technical because it is designed specifically for cryptoasset transactions, operates commercially, charges a fee or provides a convenient means of access*". These statements are important correctives to the "*added value*" reasoning that industry provided input on in response to CP 26/13, and we ask the FCA to uphold them.

That approach should be anchored in HMT's intent and the "*same risk, same regulatory outcome*" principle. Non-discretionary technical functionality that involves no substantive intermediation does not create intermediary risk. We therefore ask the FCA to frame the whole TSP exclusion analysis around the three intermediary risks the regime is intended to address: (i) the misappropriation or mishandling of users' assets; (ii) conflicts of interest between the provider and the user, and (iii) the misuse of confidential or price-sensitive information. We ask the FCA to read the "*merely provides*", discretion and substantive-participation tests in PERG 18.8.26 to 18.8.31 so that a provider falls outside the exclusion only if its service actually gives rise to one or more of those risks. A genuinely non-custodial, non-discretionary software provider that does not hold private keys, take custody, exercise execution discretion, solicit or recommend transactions, negotiate terms, arrange financing for users, or take or route orders creates none of the three abovementioned risks, and the TSP exclusion should be available to it.

We remind the FCA that a workable reading of the TSP exclusion matters all the more because of the expanded territorial scope of the new regime. Unlike the equivalent TradFi regime, the overseas persons exclusion does not apply to the new regulated cryptoasset

activities. PERG 18.3.6, as specified in FCA's policy statement PS26/18 relating to the cryptoasset perimeter guidance (the "PS 26/18"), confirms that "*[t]he Cryptoassets Regulations do not apply the OPE to the new regulated cryptoasset activities.*" In addition, section 418(6C) of the Financial Services and Markets Act 2000 (the "FSMA") deems an overseas person to be carrying on regulated activity in the UK where it is involved in the sale or subscription of a qualifying cryptoasset to, or by, a consumer in the UK and no authorised principal dealer or qualifying cryptoasset trading platform operator is interposed as intermediary. The combined effect is that an overly narrow TSP exclusion interpretation would sweep a vast number of offshore non-custodial software providers into the UK perimeter. Faced with intermediary licensing requirements they cannot meet without "re-intermediating" their systems, those providers are likely to geofence UK users rather than restructure as authorised intermediaries, with the practical effect of excluding the technology from the UK market. The result would be to reduce UK user access to widely used, non-custodial software, with no corresponding consumer-protection benefit.

"Merely provides" and "added value" concepts interpretation

PERG 18.8.26 sets out the FCA's view of when a person "*merely provides*" a technical service by offering a list of indicators for when A is more likely to be merely providing a technical service. Conversely, the exclusion is said to be "*less likely to apply where A's service is part of the process by which transactions are selected, shaped, directed, negotiated, routed or brought about.*" We generally support the indicators' focus on who selects and who decides.

However, several of the indicators risk undermining the exclusion for the very business models it was enacted to protect. We ask the FCA to confirm the following, which are analogous to the conditions established by the SEC CUI Statement[8]:

- ***Standard user-experience features remain merely technical.*** We ask the FCA to confirm that dashboards, the display of prices and market data, estimated transaction costs such as network or gas fees, and pre-filled fields are the provision of "*non-substantive and non-discretionary technical functionality*" within PERG 18.8.26, and remain within the exclusion. None of these features involve custody, discretion or control. None give rise to any of the three aforementioned intermediary risks. This also sits comfortably with the FCA's final guidance in PERG 18.8.8 (as made in PS26/18), which already accepts that "*[t]he provision of information, analytics, research, market data or dashboard services does not, of itself, amount to arranging deals in qualifying cryptoassets.*"

- ***Default routing is not "selecting".*** We ask the FCA to confirm that offering a default route does not, by itself, mean that A "*selects the service provider or decentralised protocol to be accessed*" within the third indicator provided in PERG 18.8.26. Where the user can select options other than the default, and the default is given no special prominence beyond being the default, it is the user who selects, not the provider. This also mirrors the SEC CUI Statement in the US, which expressly permits a covered user interface provider to "*select[] one or more default trading venues[...]or distributed ledger trading systems*", provided that, where only one route is displayed,

[8] Staff Statement Regarding Broker-Dealer Registration of Certain User Interfaces Utilized to Prepare Transactions in Crypto Asset Securities, SEC, Division of Trading and Markets, April 13, 2026 (the "SEC CUI Statement").

the user can see additional routes, and provided the provider discloses and periodically reassesses its default parameters.

- ***Computing and displaying routes from objective data is not selecting, shaping, or routing.*** A wallet or front-end commonly uses pre-integrated application programming interfaces ("APIs") and an algorithm to identify, from publicly available onchain data, the exchanges, liquidity sources or decentralised protocols through which a user-specified transaction could be executed, and the price available through each. Such software computes candidate routes by applying disclosed, objective logic to data such as pool reserves, quoted prices and network fees, and then displays the results to the user. The user selects a route and signs the transaction with keys the provider does not hold, and the signed transaction is broadcast from the user's wallet to the smart contract the user has chosen (*i.e.* the user initiates the transaction).

  At no point does the provider receive an order, hold it, decide its destination, or transmit it on the user's behalf. In the sense in which those terms are used in PERG 18.8.26(2) and PERG 18.8.31(3), the provider neither "*transmits C's instructions*" nor "*receives, combines, modifies or routes orders*"— there is no order in the provider's hands to route. That is also why the "*qualifying non-custodial software*" criteria we describe below, which exclude a provider that takes or routes orders, are consistent with this model rather than in tension with it.

  The right distinction is between two different models. On one side is a platform that accepts an order and assumes responsibility for obtaining a particular execution outcome, such as best price, and that exercises judgement and discretion to do so. Such a platform takes on a responsibility to the user of the kind a broker assumes, and its activity could appropriately be treated as substantive participation. On the other side is software that applies disclosed, objective, pre-programmed logic to compute and display options, where the user selects the option and the user's signed instruction initiates the transaction. The latter does not constitute substantive participation or discretion, and that is so whether the logic computes a single swap route, a time-weighted or volume-weighted average price schedule that the user has chosen and that a smart contract executes, or a comparison of liquidity across venues. We provide more detail on this point further below, as it is of central importance to drawing the scope of the TSP exclusion correctly.

- ***Objective ranking is permissible.*** We ask the FCA to confirm that ranking or ordering options on an objective, quantitative basis—such as by lowest cost, highest liquidity, or fastest settlement—does not take a provider outside the exclusion, and to amend indicator (4) of PERG 18.8.26 and indicator (1)(d) of PERG 18.8.30 so that they say so. Indicator (4) in PERG 18.8.26 refers to selecting, recommending or ranking "*by reference to the circumstances of a proposed transaction or other qualitative features.*" As drafted, the words "*or other qualitative features*" treat the circumstances of a proposed transaction as themselves a qualitative feature, so that sorting quotes by price for the transaction the user has specified could be read as qualitative ranking. Indicator (1)(d) of PERG 18.8.30 goes further and lists as an indicator of discretion the selection or adjustment of routing "*by reference to an assessment of price, liquidity, speed, transaction costs, counterparty risk or likely outcome*", which sits uneasily with indicator (2)(c) of the same provision, under which routing that "*follows predetermined objective rules*" points towards a non-discretionary service.

Sorting routes alphabetically, by quoted price or by speed, on independently verifiable criteria that are disclosed in advance and applied in the same way to every user, involves no qualitative judgement. The same inputs produce the same output without any assessment by the provider, which is the test the FCA itself sets in indicator (2)(d). We therefore ask the FCA to make clear that indicator (4) of PERG 18.8.26 and indicator (1)(d) of PERG 18.8.30 are directed at a qualitative assessment by A of the merits or suitability of a route, and that ordering options on objective quantitative criteria falls within indicators (2)(c) and (2)(d). This is consistent with the SEC CUI Statement, which permits filtering or sorting tools that display potential routing destinations based on objective factors (such as alphabetically, lowest/highest price, or speed), so long as the interface "*does not provide commentary on any potential execution route(s)[...]such as indicating that an execution pathway offers the 'best price' or is the 'most reliable'*." Labelling the lowest quoted price as such is a display of data, whereas representing that the provider will obtain the best price is a representation about outcome, and the two should be distinguished in the same way.

- ***Objective risk information is permissible.*** A user interface should be able to provide objective information or warnings about the risks of different routings, such as potential slippage, without that being treated as discretion or substantive involvement. Presenting objective risk information helps the user make their own decision. It does not transfer the decision to the provider.

We also ask the FCA not to use the word "*shaping*" a transaction in PERG 18.8.26. "*Shaping*" has no settled meaning in this context, inviting the subjective, case-by-case assessment that the PERG Guidance should avoid, and it sits awkwardly alongside the more precise verbs—"*selected, directed, negotiated, routed or brought about*"—around it.

Furthermore, we consider that a connection to a decentralised platform is not, by itself, disqualifying. A TSP may have some form of connection or role in relation to a decentralised platform. But that should not, by itself, disqualify reliance on the exclusion, provided the TSP does not control the protocol. We note the statement in PERG 18.8.28 that "*where A's involvement with the protocol extends beyond merely facilitating access to it, A may not be able to rely on this exclusion.*" We ask the FCA to confirm that involvement which does not amount to control over the protocol does not defeat the exclusion, and to tie the assessment of "*involvement*" to the control-based criteria we recommend in Section III above.

As mentioned above, the central analytical point for this part of the PERG Guidance is that a non-custodial wallet or front-end displays the prices available through the venues and protocols to which it connects. The user then selects a price and signs a specific instruction to buy or sell. On that analysis, it is the user, not the provider, who makes the arrangements and gives the execution instruction, and therefore indicator (1) of PERG 18.8.26 is satisfied as "*the service responds to instructions initiated by C*". That is the arrangement article 9Z2A(1) describes—a technical service that "*allows another person ("C") to access services provided by a third person or a decentralised protocol*". We ask the FCA to confirm that there is no discretion or substantive participation from the provider in such a scenario, and that clear terms of use describing the objective routing methodology and the choices available to the user support that analysis.

Moreover, even if the display of a price by a non-custodial wallet or front-end were regarded as involving an element of discretion, it could only be discretion over what is shown

to the user, not discretion over the transaction itself. The discretion with which Article 9Z2A and PERG 18.8.30 are concerned is the exercise of qualitative judgement capable of materially affecting a transaction or a person's participation in it. A provider that merely decides which venue, protocol or price to display makes no decision about whether, where or how any transaction takes place—that decision remains with the user, who selects the option shown and signs the instruction that initiates the transaction. Discretion over what is presented to the user is therefore not discretion over the transaction, and only the latter is relevant to the availability of the TSP exclusion. This is so even where the non-custodial wallet or front-end integrates with only one venue or protocol, provided that fact is disclosed to the user, the provider's remuneration does not vary with the use of that venue or protocol, and the user remains free to transact elsewhere.

This interpretation is aligned with the HMT's intention, as expressed in the Explanatory Memorandum to the Amending Regulations, paragraph 6.10, which provides that article 9Z2A excludes arrangements under which a person "*merely provides a technical service enabling another person to access **one or more** services provided by **one or more** authorised or exempt persons or decentralised protocols*" (emphasis added), and that the effect is to ensure that "*tech interface providers are not treated as arranging transactions*". The reference to "*one or more*" is important as it shows that HMT intended that a provider (*e.g.* non-custodial wallet or front-end) relying on the TSP exclusion might offer access to only a single service, venue or protocol, and did not intend the TSP exclusion to not be available merely because a provider makes available, or displays, only one option. It follows that the design-time choice of which protocols or venues to integrate into an interface is not what indicator (3) of PERG 18.8.26 and factor (1) of PERG 18.8.31 are directed at. Those provisions ask who selects the service provider or protocol with respect to a transaction, and that remains the user, who can see which venues the interface offers and may choose to go elsewhere. The concern behind those provisions, that an interface might steer users to a venue in which the provider has an interest, is addressed by the conditions described above, in particular disclosure of the integration and remuneration that does not vary with the venue used, and not by treating every integration decision as discretion. For the same reason, displaying the price of a single provider or protocol that the provider has chosen to show cannot, in and of itself, amount to discretion over, or substantive participation in, a transaction. It is instead the user who exercises discretion over the specific transaction, deciding whether to transact at the price displayed and whether to sign the instruction that gives effect to it. We ask 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, consistent with HMT's stated intention. Finally, the two passages of the Explanatory Memorandum should be read together. The same memorandum that describes the exclusion as unavailable where a provider "*exercises discretion over or is substantively involved in the relevant transactions*" describes the excluded service as one enabling access to "*one or more*" services of "*one or more*" providers or protocols. HMT therefore did not regard the number of services or providers made available as bearing on discretion or substantive involvement, and the FCA's guidance on those concepts, which paraphrases the Explanatory Memorandum, should be read consistently with it.

This reinforces a more fundamental distinction between brokers who take responsibility for customer orders and funds and technical service providers who do not. A broker accepts an order and assumes responsibility for obtaining a particular execution outcome, and the law attaches duties to that assumption of responsibility. A non-custodial wallet provider does neither, and the user retains the choice.

The FCA's own formulation in PERG 18.8.30 points the same way as the relevant question is "*whether, considering the design and operation of the service as a whole, A exercises or has assumed responsibility for judgement materially affecting the transaction.*" We ask the FCA to make this the organising test for discretion and substantive participation, so that the more subjective indicators of discretion and participation are read as evidence of whether A has assumed such responsibility. Common front-end design, including a routing display the user can inspect and override, is evidence that it has not. The SEC CUI Statement, although a staff-level statement confined to the broker registration provisions of the US Securities Exchange Act, draws the line in the same place.

Finally, an objective algorithm is not discretion merely because the provider wrote it. We ask the FCA to revisit the statement in PERG 18.8.30 that "*[p]redetermined software may implement judgements previously made by A, and an algorithm may select among alternatives by reference to criteria determined or adjusted by A*", and that "*[t]he fact that software uses an algorithm does not necessarily make the service non-discretionary.*" The same paragraph goes on to state that the relevant question is whether "*A exercises or has assumed responsibility for judgement materially affecting the transaction*", which is the right question. Interpreted broadly, however the preceding sentences suggest that even an objective, pre-written routing algorithm can involve discretion simply because the provider created or maintains it. That reading is too broad as every non-custodial software model necessarily involves software that someone wrote and maintains. If authorship of an objective algorithm were itself discretion, the exclusion would be unavailable to the entire class of business models it was enacted to protect. We ask the FCA to confirm that an objective, pre-written routing algorithm, applied consistently and disclosed to the user, does not amount to discretion merely because the provider created or maintains it, and that the relevant question is whether the provider retains and exercises the ability to vary the routing for particular users or transactions, or has assumed responsibility for the outcome.

Discretion and "substantive participation" need objective, administrable limits

We support the discretion and non-discretion indicators in PERG 18.8.30 and the factors in PERG 18.8.31. However, we raise one structural caution. "*Substantive participation*" and "*substantive intermediation*" are not statutory conditions in Article 9Z2A. They paraphrase HMT's Explanatory Memorandum, which describes the exclusion as unavailable where the firm "*exercises discretion over or is substantively involved in the relevant transactions*". The FCA acknowledges this in PERG 18.8.31. These concepts must be used to interpret the statutory term "*merely*", not to expand the perimeter beyond the statute.

On discretion, we ask the FCA to clarify, in the context of a non-custodial wallet and by reference to the SEC CUI Statement conditions, that several common features do not amount to discretion:

- Presenting and ordering information on objective, independently verifiable criteria, such as lowest-cost or highest-liquidity route, is not discretion;

- The FCA should also clarify what counts as the provider "*representing*" that it will achieve an "*optimised result*", referenced in PERG 18.8.30, bearing in mind that many wallet features are designed to assist users to optimise their own transactions by accessing, filtering and sorting relevant information;

- We recommend framing the test around a16z's "*qualifying non-custodial software*" criteria. A qualifying provider does not control private keys, take custody, exercise execution discretion, solicit or recommend transactions, negotiate terms, arrange financing for users, or take or route orders;[9] and

- We also recommend reinforcing the analysis with a "*held out*" test grounded in whether, on the representations made and the functionality offered, A has assumed responsibility to the user for the outcome of the user's transactions. A neutral software tool assumes no such responsibility.

We offer two refinements drawn from our prior response with respect to the "*held out*" test. First, the mere fact that software is held out as enabling users to transact in qualifying cryptoassets is not, by itself, an assumption of responsibility for the outcome of those transactions. Only representations or functionality that hold the provider out as an intermediary, or by which it assumes responsibility for execution outcomes, should cross the line. This maps to the factor in PERG 18.8.31(6) concerning a provider that "*holds itself out as arranging, executing, optimising*" transactions. Second, consistent with the SEC CUI Statement, soliciting users to enter into specific transactions should take a provider outside the exclusion, but soliciting users to use the interface generally should remain permissible.

However, we agree that there needs to be a line drawn. Software remains a tool in the user's hands where it executes a strategy the user has selected, on terms disclosed in advance, and by means of a smart contract whose logic the provider cannot alter. The user chooses the strategy, the code applies it mechanically, and the provider exercises no judgement over the user's assets. That is so even where the strategy involves periodic rebalancing across protocols, because the rebalancing follows rules the user accepted rather than decisions the provider makes. By contrast, the position changes where a person exercises ongoing judgement over a user's assets, deciding for the user, from time to time and by reference to its own assessment, where those assets should be deployed and reallocating them without a user instruction. That person has assumed responsibility for the user's strategy, and its activity may amount to substantive intermediation or to managing the user's assets. The distinction is the one the FCA itself draws in PERG 18.8.30 between judgement exercised by A and the automatic application of predetermined objective rules. It leaves self-directed tools, including automated strategies the user has chosen, outside the perimeter while capturing discretionary management by a person.

On substantive participation, the treatment of fees requires particular care. PERG 18.8.31(7) lists, as a relevant matter, whether A "*receives remuneration calculated by reference to whether, or on what terms, transactions take place.*" Read broadly, that could capture a percentage-based fee per transaction even where the fee is execution-route, venue- and counterparty- agnostic. We welcome the FCA's own qualification, in PERG 18.8.31, that

[9] With respect to the conditions that the software provider does not exercise discretion over whether or on what terms a transaction is executed and does not take or route orders, it is important to note that these are consistent with situations where the software displays potential execution routes, so long as it displays these based on objective, pre-disclosed and independently verifiable criteria. Displaying a single or multiple execution route(s) according to objective, pre-defined optimisation criteria—such as lowest cost or highest liquidity—and based on an objective calculation or computation of publicly available market data, should not by itself constitute discretion or a recommendation, so long as the user retains the ability to review, approve, or reject the transaction. As a result, intermediary-based risks like conflicts of interest risk are not implicated (particularly bearing in mind the additional condition that the software provider's compensation from the user may not vary based on the user's selection of product, execution-route, venue and counterparty).

"*transaction-linked remuneration may be relevant but will not determine the issue without considering the functions for which the remuneration is paid.*" We ask the FCA to make that qualification explicit and operative. Article 9Z2A contains no condition relating to remuneration, and HMT's Explanatory Memorandum does not mention fees in describing it. The FCA itself accepts in PERG 18.8.27 that a service does not cease to be technical because it "*charges a fee*". Transaction-based compensation should thus be permissible where it is a flat fee, or a fixed fee or percentage per transaction that is applied on a consistent basis, and that is execution-route, venue and counterparty agnostic. Charging per-transaction or per-message fees should not, by itself, convert technical provision into arranging. What matters is custody, discretion and control, and the presence of conflicts of interest.

A flat per-transaction fee charged by a provider that exercises no custody, discretion or control, and that has no conflict of interest in the execution route used, presents a materially different risk profile than a commission-based intermediary whose remuneration creates incentives to steer clients. A fee should be relevant only where it is structured so that the provider assumes a responsibility to the user for that outcome, such as the platform that accepts responsibility to obtain a particular execution outcome, or where it varies with the user's choice of product, route, venue or counterparty, which would introduce a conflict of interest. The SEC CUI Statement draws the line in the same place, permitting a fixed charge to the user based on objective factors, applied consistently, that is agnostic to product, execution route, execution venue, and counterparty. The Statement likewise treats remuneration that varies with those choices, such as payment for order flow, as outside the relief.

Finally, we welcome the FCA's recognition in PERG 18.8.31 that "*limiting access for technical security or legal compliance reasons will not necessarily amount to substantive intermediation.*" That is an important and correct point, and we ask the FCA to retain it. Security and compliance controls protect users, and their use should not, by itself, cause a provider to be treated as an intermediary or presumed to create the risks that the intermediary regulation is intended to address.

The "decentralised protocol" limb—status over time and the A/V problem

PERG 18.8.32 addresses how the exclusion applies where V is a decentralised protocol. We ask the FCA to cross-refer to, and apply, the control-based factors we recommend in response to Questions 1 to 3, in Section III above. The current guidance is overly broad and vague. PERG 18.8.32 states that, in considering whether arrangements amount to a decentralised protocol, it may be relevant to consider the degree to which a person or persons "*(a) engage in its ongoing maintenance and adaptation; (b) generate remuneration by reference to a service provided in connection with use of the protocol; and (c) hold themselves out as providing a protocol for trading purposes.*"

The first of these is particularly problematic. Virtually every decentralised protocol is subject to some ongoing maintenance and adaptation. As a general matter, open-source software requires ongoing maintenance in order to function effectively. It is not the existence of ongoing maintenance that should be the deciding factor, but the degree to which a person controls the protocol through the mechanisms described above. We welcome the FCA's own recognition, later in PERG 18.8.32, that the term 'decentralised protocol' is unlikely to describe what is, in substance, a service controlled and operated by an identifiable person merely because that service uses smart contracts or distributed infrastructure. *However*, we

ask the FCA to make control, rather than maintenance, the organising concept, and to apply the objective control criteria we discuss in Section III above.

Without objective criteria, a TSP faces practical difficulty in determining whether a protocol is decentralised, and therefore whether it can provide access to that protocol while retaining the benefit of the exclusion. As drafted, a provider connecting to a widely used protocol has no way to form a confident view of whether the FCA will later regard that protocol as controlled by reference to the open-ended factors.

A related point concerns security. A protocol that allows not one person, but a majority vote, to correct an issue to prevent a hack, or to halt the operation of a protocol in the event of a cybersecurity exploit, should be capable of being considered decentralised. Such powers support cybersecurity and resilience and protect users. If the FCA treated the mere existence of such powers as defeating decentralisation, it would disincentivise exactly the processes that can correct faults and prevent hacks. Moreover, such powers can be accountable to decentralised governance without undermining decentralisation.

We also flag the "*A is not V*" issue in PERG 18.8.28, which states that, because "*[t]he structure of article 9Z2A distinguishes A's technical service from the services provided by the third person, and from the decentralised protocol to which access is given[...]a person cannot be both A and V for the purposes of this exclusion.*" This creates uncertainty for anyone who develops or maintains a protocol, whether as an open-source contributor, under a contract with a foundation, or as the foundation or other entity through which governance participants have organised themselves. Such a person risks being characterised as the protocol itself, and so disqualified from providing an interface to it. A protocol is software, not a person; developing or maintaining it does not make a person the protocol. The text of article 9Z2A(1) confirms the point: V is "*a third person or a decentralised protocol*", and only the first of these is a person. We ask the FCA to clarify that developing or maintaining a protocol, with or without a formal arrangement, does not in and of itself make the developer or maintainer the protocol; that a foundation, DUNA or other entity through which participants organise themselves is legally separate from the protocol and is not itself the protocol; and that such involvement should not, by itself, defeat the availability of the exclusion. The right question is whether the person controls the protocol, assessed against the control criteria. Where it does, the protocol is not a decentralised protocol for purposes of article 9Z2A(2)(b), and that, rather than any identity between A and V, is the reason the exclusion would be unavailable.

A protocol's status can also change over time, and the guidance should address that. For example, a protocol's status may shift where founders or a limited group come to hold a controlling share of governance, where token-holder participation declines so that a small group of holders can pass governance proposals, or where a third party acquires enough tokens to control governance. A protocol widely regarded by the market as decentralised could, on these facts, later be assessed as controlled. We ask the FCA to clarify how a provider should assess this on an ongoing basis, and what steps it can take to avoid being in breach if a protocol ceases to be decentralised. In practice, we anticipate that a provider relying on the exclusion would maintain a documented, periodic monitoring process using publicly available information, regulator publications, and warning lists, and would act promptly to restrict access if a connected protocol ceased to be decentralised.

Furthermore, there is an additional risk that the PERG Guidance leaves unresolved. Because status is assessed at a point in time, the FCA could later determine that a protocol was controlled from an earlier date unknown to the market. As currently drafted, the guidance

would appear to leave a provider in breach of the general prohibition under section 19 of FSMA—a criminal offence under section 23—for a period during which it could not have known the protocol was controlled, and during which no public information would have revealed it.

We recognise that the FCA cannot alter the consequences that FSMA attaches to a breach of the general prohibition. Section 23(3) of FSMA already provides a defence where the accused shows that it "*took all reasonable precautions and exercised all due diligence to avoid committing the offence*".[10] We therefore ask the FCA to explain what it would regard as reasonable precautions and due diligence for a provider relying on the exclusion. These could include a documented, periodic assessment of the protocol against the control-based criteria using publicly available information, and prompt action to restrict access where that assessment changes. The FCA should also confirm that its supervisory and enforcement approach to a provider that has followed such a process will take into account that the provider relied in good faith on the information reasonably available to the provider at the relevant time, and that it would not expect to take enforcement action against a provider that has taken reasonable steps to monitor the status of a connected protocol in respect of a period of undisclosed control that the provider could not reasonably have detected.

Consumer protection via the financial promotions regime

We acknowledge that there may be residual risks of consumer harm from software that, under our recommendations, would not require authorisation. Such risks can arise even where the software involves no intermediary relationship between the provider and the user, for example where the software is marketed in a way that encourages users to deal in qualifying cryptoassets. These risks are already addressed by the UK financial promotions regime as it applies to qualifying cryptoassets. This is consistent with PERG 18.8.34, which confirms that the TSP exclusion does not extend to the financial promotions regime, so that communications made through or in connection with the technical service remain subject to the restriction in section 21 of FSMA. That was a deliberate legislative choice. The Explanatory Memorandum records that the Amending Regulations mirror the exemptions from the Regulated Activities Order in the financial promotions regime, "*except that the exclusion for technical services providers is not replicated, meaning those services remain subject to the regime*". HMT has therefore already decided where any residual consumer risk from technical service providers is to be addressed, and the arranging perimeter need not be read expansively to address it again.

V. FCA GC 26/7 – Decentralised Finance ("DeFi")

We broadly agree with the operational-resilience and financial-crime risks the FCA identifies in GC 26/7, and we support its focus on consumer protection and market integrity. However, we ask the FCA to make one important clarification. The guidance should distinguish between failures at the application layer and the bridge layer, the subject of its own case studies, from the base-layer consensus of permissionless networks, which did not fail in those incidents.

The case studies in GC 26/7 illustrate the point. The KelpDAO attack exploited a single-verifier bridge configuration and monitoring gaps; the Polygon Plasma Bridge bug was a flaw in a bridge; the Bybit incident, in which, as GC 26/7 notes, the victim was a

[10] Financial Services and Markets Act 2000, s. 23(3).

centralised exchange, targeted the user interface and approval process of wallet software through social engineering; the $SQUID "rug pull" exploited a token contract designed to prevent holders from selling and the absence of admission controls on a permissionless venue; and the Drift exploit turned on compromised governance signers and a zero-timelock configuration. Each of these was a failure of a bridge, an interface, an approval process, a token contract, or a governance arrangement. None was a failure of the base-layer consensus of the underlying permissionless network. The Sui outage is an example of a genuine base-layer disruption, but across major permissionless networks it is the exception rather than the rule, and Sui's validators halted, repaired and resumed the network within hours.

The description of DeFi risk should also acknowledge that permissionless base-layer networks can be more operationally resilient than traditional or permissioned ledgers. Decentralised architecture removes single points of failure. Resilience scales with the number, independence and diversity of validators. A network that runs across numerous independent validators with aligned incentives has no single operator whose failure can halt it. The FCA, the Bank of England , and the Prudential Regulation Authority have recognised this, as have regulators in other jurisdictions.[11] The Office of the Comptroller of the Currency in the US has observed that independent node verification networks "*may be more resilient than other payment networks because of the decentralized nature of INVNs.*"[12] We ask the FCA's guidance to reflect this evidence, rather than treating decentralisation itself as a source of operational-resilience risk.

Our response to questions 1 and 2—Operational resilience risks and guidelines

We endorse placing operational-resilience controls at the layer the firm actually operates: the application layer. The permissionless network should be treated as shared infrastructure, much like the internet or the telephone network, rather than as something the firm must itself control. A firm can control the base layer of a major permissionless network no more than it can control the public internet. The right question under SYSC 15A is therefore how the firm manages its own important business services, built on top of that infrastructure. This is consistent with the FCA's own framing in GC 26/7, which, under SYSC 15A.2.1R, directs firms to identify "*the service delivered to the client, rather than treating the underlying technology or protocol as the important business service.*"

We recommend that practice under SYSC 15A recognise network-level diligence as the appropriate response to base-layer dependencies. Relevant diligence includes validator client diversity, validator and stake distribution, finality characteristics, upgrade governance and historical resilience. A firm should evaluate these in the same way it evaluates any other critical infrastructure on which it depends. Firms can also reduce third-party and concentration risk by running their own nodes, and should manage node, staking, custody and analytics providers as vendors under existing third-party risk-management guidance, including SYSC 8 where the arrangement constitutes outsourcing. We welcome the FCA's recognition, in GC 26/7, that its operational-resilience requirements "*apply to relevant third-party arrangements whether or not they constitute outsourcing.*"

---

[11] Financial Conduct Authority, Bank of England and Prudential Regulation Authority, Written evidence to the House of Commons Treasury Committee inquiry into IT failures in the financial services sector (OPR0012) (2019), para. 15.3, https://committees.parliament.uk/writtenevidence/99804/html/.
[12] Office of the Comptroller of the Currency, Interpretive Letter No. 1174 (4 January 2021), https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf.

However, we ask the FCA to make it clear that a firm's responsibility is to understand and manage these dependencies, not to guarantee the performance of autonomous infrastructure it cannot control. Where a firm cannot obtain contractual rights or technical powers that do not exist, it should be able to rely on documentation, code review, assurance and monitoring instead. We also respectfully ask that the FCA:

- Recognise that core network participants are not the right locus of control. For example, validators, searchers, builders, sequencers, relayers and RPC nodes are non-custodial. They generally have no contact with, or knowledge of, the firm's users. They function like communications infrastructure, with RPC nodes analogous to internet service providers. Resilience controls therefore belong at the application layer the firm operates, not with these participants. The FCA's own Firm B example, which maps reliance on oracles, decentralised-exchange aggregators and RPC node providers and which responds to a single-RPC-provider dependency by reducing reliance on that provider, illustrates that the firm's resilience work is properly located at its own service layer.

- Clarify one aspect of its Firm B example, which describes a firm providing "*a number of regulated financial services as well as access to DeFi through a non-custodial wallet*" that uses decentralised exchange ("DEX") aggregators "*to offer users the best swap prices*". Read together with CP 26/36, the example should not be taken to suggest that providing a non-custodial wallet with access to decentralised exchanges through an aggregator is itself a regulated activity. Firm B is within SYSC 15A because of the other regulated services it provides. We ask the FCA to clarify this, and to confirm that the wallet and aggregation function, considered alone, is the kind of technical service to which article 9Z2A is directed, so that the example does not undercut the perimeter guidance in CP 26/36.

- Treat security and emergency mechanisms as resilience-enhancing features that firms should assess positively. These include pause controls and the ability of decentralised governance to act to correct a fault or prevent a hack. This is consistent with our position that such powers can be reserved through decentralised governance without undermining decentralisation, as discussed in Section IV above. We note, however, the tension in the current draft where GC 26/7 rightly identifies, in its case studies, both the absence of effective emergency response and the concentration of administrative control as risks. The right response is to assess the security and misuse risks of any intervention mechanism in context, not to treat either the existence or the absence of such a mechanism as determinative. Treating the mere existence of a safeguard as a negative factor would perversely discourage firms from integrating protocols that are better able to withstand and recover from incidents.

Our response to questions 3 and 4—Financial crime risks and guidelines

Furthermore, GC 26/7 observes, at paragraph 4.8, that responsibility for financial crime controls "*may be fragmented across developers, governance participants and infrastructure providers, creating potential gaps*". We ask the FCA to carefully consider and be clear about where, within that list, obligations can reasonably sit. For example, a protocol-selected, pseudo-randomly assigned validator that processes a transaction is not a counterparty of the firm or its customer and has no relationship with either. In a permissionless network, the right to propose a block, the fee and the validator are all assigned automatically by the protocol. This is analogous to the relationship between an email sender

and the owner of a router that carries the message, or between a caller and the owner of a switch that completes the call. A firm whose transaction is processed by such a validator has not selected, contracted with, or dealt with that validator, and the absence of controls at the validator is not a gap in the firm's controls.

GC 26/7 correctly identifies "*direct or indirect exposure to sanctioned persons, wallets, protocols or services*" as a relevant factor in ongoing monitoring (paragraph 4.23) and in assessing higher-risk situations (paragraph 4.19). But, we ask the FCA to give that distinction operational content, so that firms are not led to treat every historical connection as equivalent. A firm does not inherit the sanctions status of every address an asset has touched in its history. Blockchain analytics practice distinguishes direct exposure, where an asset comes immediately from a designated wallet or illicit address, from attenuated, multi-hop exposure separated by intervening legitimate transactions, and calibrates risk scoring accordingly. The guidance of the Office of Financial Sanctions Implementation and the enforcement approach of the US Office of Foreign Assets Control ("OFAC") both treat the quality of a firm's screening and its response to identified exposure, rather than the bare fact of a distant connection, as what matters. We ask the FCA to confirm that a risk-based approach to indirect exposure, with documented thresholds for escalation, enhanced due diligence and reporting, is consistent with SYSC 6 and the MLRs.

We also strongly urge the FCA to reframe transparency as a mitigant. The public ledger lets a firm trace the provenance of incoming assets with a precision unavailable in traditional payments. As evidenced by the immediate and detailed forensic information gleaned from both recent and historical cybersecurity incidents alone, this is a tremendous financial-crime advantage of permissionless, public networks, not a disadvantage. The ability of private sector participants to have this visibility to take action, identify illicit assets in transit, and at intermediary points freeze, seize, or burn those funds, is a significant and unique benefit of permissionless, public networks when compared with the traditional financial system in identifying and preventing illicit transactions.

We also ask the FCA to confirm that network-level participants are not financial-crime gatekeepers, and to do so consistently with cross-border precedent. A similar approach has already been taken in the EU, where the European Securities and Markets Authority, in its final report on the technical standards under the Markets in Crypto-Assets Regulation on the prevention and detection of market abuse, explained that miners, validators, searchers and builders are not "*persons professionally arranging or executing transactions*".[13] We ask the FCA to adopt a consistent approach, so that due-diligence, screening, monitoring and reporting controls GC 26/7 describes, each of which presupposes a firm and a customer, are not placed on neutral infrastructure participants who have no customers.

We welcome the risk-based framing of the financial crime chapter. We ask the FCA to make explicit that SYSC 6 and the MLRs require reasonable, risk-based programmes, not the total elimination of risk. That is already the position under regulation 19 of the MLRs, which requires policies, controls and procedures that are proportionate to the size and nature of the

[13] European Securities and Markets Authority, Final Report on the draft technical standards specifying certain requirements of the Markets in Crypto-Assets Regulation (third package), explanatory text on the regulatory technical standards on the prevention and detection of market abuse. Eur. Sec. & Mkts. Auth., Final Report: Draft Technical Standards Specifying Certain Requirements in Relation to the Detection and Prevention of Market Abuse Under the Markets in Crypto Assets Regulation (MiCA), ESMA75-453128700-1278, at 12 (Dec. 17, 2024), https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75-453128700-1278_Final_Report_STOR_MiCA_Article_92_2_.pdf.

firm's business, and under the FCA's Financial Crime Guide; and it mirrors the approach of the US Financial Crimes Enforcement Network and OFAC, which focus enforcement on systemic, knowable deficiencies rather than on isolated or inadvertent contacts. A firm should not be expected to achieve a zero-tolerance outcome that no compliance programme can deliver. Furthermore, we recommend that the guidance locate controls at the customer and application layer that the firm operates. That means customer identification, customer due diligence and enhanced due diligence tied to customers' wallet addresses, screening of deposit sources and withdrawal destinations against sanctions and illicit-address lists, transaction monitoring tuned to on-chain typologies such as structuring across addresses and rapid layering through mixing or bridging, and suspicious activity reports that capture transaction hashes and addresses. These are the familiar pillars of a financial-crime programme, adapted to on-chain data.

In response to Questions 2, 4 and 5, we ask the FCA to credit the emerging practices that firms already use quite effectively. These include blockchain analytics providers, for direct and indirect exposure scoring, and the "Know Your Wallet", "Know Your Asset" and "Know Your Transaction" techniques. We also ask the FCA to recognise that token-level controls, such as transfer hooks and allowlists, and privacy-preserving identity tools, such as reusable KYC, verifiable credentials and zero-knowledge proofs, allow firms to meet their anti-money-laundering goals while reducing the "honeypot" data-security risk created by repeated collection of identity information.

On the Travel Rule, we agree with the position stated in GC 26/7 that the obligations in regulations 64A to 64H of the MLRs apply to cryptoasset businesses, and we note that regulation 64G already provides a proportionate, risk-based approach to transfers involving non-custodial wallets, under which the firm may request originator or beneficiary information from its own customer. We ask the FCA to confirm that the Travel Rule does not require a firm to obtain information from, or impose obligations on, the protocol or the network participants involved in a transfer , and that on-chain transfers can carry originator and beneficiary data through interoperability protocols. Industry-standard solutions, including the Travel Rule Universal Solution Technology ("TRUST"), the Travel Rule Information Sharing Alliance ("TRISA") and the Travel Rule Protocol ("TRP"), allow institutions to transmit the required identifying information alongside on-chain transactions, using the transaction hash as a common identifier. Permissionless networks present no inherent obstacle to compliance.

Finally, in response to Question 6, we ask the FCA to recommend placing anti-money-laundering obligations, and the sanctions screening and reporting controls that GC 26/7 describes, only on identifiable, controlling entities at the application layer that hold "account" relationships with their customers, whereby customers must undergo onboarding and provide documentation as to their identity. Such controls should not be placed on the permissionless network itself or on providers that do not hold such relationships. To be clear, we do not suggest that the prohibitions in the UK sanctions regime, which apply to all persons irrespective of any customer relationship, are displaced; our point concerns where the due-diligence, screening and reporting controls that GC 26/7 describes can sensibly sit. This is reinforced by domestic precedent. The Joint Money Laundering Steering Group guidance approved by HMT treats the "*making arrangements*" formulation as not capturing software developers who merely provide an application or platform without intermediary activity.[14]

[14] The Joint Money Laundering Steering Group Guidance, Prevention of money laundering/combating terrorist financing — Guidance for the UK Financial Sector, Part II, Sector 22 (Cryptoasset exchange providers and custodian wallet providers), paras 22.11–22.12 and 22.25.

Imposing onboarding and know-your-customer obligations on non-custodial software or autonomous protocols is impractical. It would force providers to reconstitute themselves as intermediaries, which would reintroduce the very counterparty and custody risks that disintermediation removes.

VI. Conclusion

We appreciate the opportunity to comment on these important matters. The FCA's guidance on decentralisation, the TSP exclusion and DeFi will have a significant and lasting impact on the development of the UK cryptoasset market. We respectfully urge the FCA to:

- adopt objective, control-based criteria for decentralisation, framed as objective indicators tied to the statutory questions in PERG 18.1.11,
- interpret the Article 9Z2A exclusion in PERG 18.8.26 to 18.8.35 to give effect to HMT's deliberate policy choice and avoid re-capturing genuinely non-custodial, non-discretionary software, and
- adopt an application-layer, risk-based approach to operational resilience and financial crime in DeFi that distinguishes base-layer networks from application-layer and bridge-layer failures.

Each of these recommendations is anchored in HMT's principle of "*same risk, same regulatory outcome*", gives firms clear and administrable criteria they can apply to their own position, and supports the competitiveness of the UK as a place to build with blockchain technology. None of them asks the FCA to change the perimeter, and instead each asks the FCA to interpret it so that it captures the risks the regime was designed to address and no more.

We welcome engagement with the FCA on these issues and would be pleased to discuss any aspect of this response in more detail, including by walking through common wallet, front-end and DeFi models with FCA staff.

Respectfully submitted,

Miles Jennings
Head of Policy & General Counsel, a16z frontier

Michele R. Korver
Head of Regulatory, a16z frontier

Jai Ramaswamy
Chief Legal Officer, a16z

Scott Walker
Chief Compliance Officer, a16z

APPENDIX

This appendix sets out suggested amendments to specific provisions of PERG 18, as proposed in CP 26/36, to implement the changes discussed in this response letter. For ease of reference, we reproduce only the specific sentence or passage of each PERG provision in which we propose a change, rather than the full provision.

*Please note that text shown in ~~strikethrough~~ represents language proposed for deletion, and text shown in **bold underline** represents language proposed for addition. The current language reproduced below is taken from the draft guidance set out in Appendix 1 to CP 26/36.*

I. Decentralisation – provisions that fall short of an objective, control-based standard

PERG 18.1.12 (meaning of cryptoasset-specific terms). To tie the meaning of statutory terms to objective facts about the arrangement rather than to subjective perceptions, we propose deleting the reference to relevant time as well as the parties' understanding:

"*In these cases, the meaning will likely depend on the objective facts and circumstances of the arrangements in question ~~at the relevant time, as well as the reasonable understanding of the parties involved~~.*"

PERG 18.1.17 (introducing control-based framework for decentralisation concept). In order to introduce objective, measurable control-based framework for deciding whether a protocol is decentralised or not, which is consistent with HMT's Policy Note to the Cryptoasset Regulations, we propose adding the following:

"**In assessing whether a protocol or other arrangement is decentralised, it should be assessed whether any person has a sufficient degree of control over the arrangement, such that a party or parties with such degree of control ought to be within the scope of the regulatory perimeter. Where no person has a sufficient degree of control, the arrangement is decentralised and its operation does not, in and of itself, cause any person to carry on a regulated activity.**

Whether there is sufficient degree of control should be assessed across three criteria:

1) **operational control, which gives a person the ability to override, alter or direct the operation of the arrangement;**

2) **economic control, where it is able to extract value from the arrangement through privileged rights, such as preferential token allocations or asset-creation authorities; and**

3) **governance control, where it, or a coordinated group acting together, is able to determine the outcome of governance decisions unilaterally or through off-chain influence.**

For the intermediary perimeter, and the technical services provider exclusion in particular, operational control is the relevant criterion, and its absence is indicated where the arrangement is autonomous, permissionless, credibly neutral and non-custodial, the non-custodial indicator being of particular importance. Governance control is relevant to the intermediary perimeter to the extent that it can be exercised to

alter the operation of the arrangement. It is not so exercisable where the arrangement is immutable, where governance can adjust only defined parameters without the ability to move users' cryptoassets, censor transactions or replace the arrangement's logic, or where changes to the arrangement's logic are subject to a mandatory delay before taking effect, during which users may withdraw, and no person or coordinated group holds the voting power needed to approve them alone.

Whether any of these three criteria is present may be further assessed against the following objective, source-verifiable indicators, none of which is determinative, namely whether the arrangement is:

1) **open source, in that its code is freely and publicly available;**

2) **autonomous, in that it operates and enforces transactions without human intervention and no person has unilateral authority to alter its functionality, operation or rules (operational control criteria);**

3) **permissionless, in that no person can restrict or prohibit access to or operation of it (operational control criteria);**

4) **credibly neutral, in that its code grants no person privileged rights to discriminate among users or use-cases (operational control criteria);**

5) **non-custodial, in that participants retain sole control of their cryptoassets through their private keys (operational control criteria);**

6) **economically independent, in that its value-driving mechanisms do not depend on any development company or issuer; and**

7) **distributed, in that no person or group under common control holds the voting power needed to amend it.**"

PERG 18.1.17 (features relevant to perimeter analysis). To give the governance, operational and economic feature lists objective, control-based content, and to anchor them to a presumption rather than an open-ended weighing of factors, we propose adding the following:

"*The FCA does not consider that any of these features is necessarily determinative, nor that they constitute a separate perimeter test.* ***These features should be assessed by reference to objective criteria of operational, economic and governance control. Where operational control over the arrangements has been eliminated, in that they are autonomous, permissionless, credibly neutral and non-custodial, the FCA would not generally expect the operation of those arrangements, in and of itself, to cause any person to carry on a regulated activity. Nor would the FCA generally expect a person to be carrying on a regulated activity merely because it has contributed to the development or maintenance of such arrangements, operates a node, or holds or votes a governance token, whether directly or through an entity formed for that purpose .***"

PERG 18.1.20 ("true DeFi"). We do not ask the FCA to prescribe a deterministic test of "true DeFi", instead, we propose only a minimal addition linking the relevant question to the objective criteria in PERG 18.1.17:

"*The relevant question is whether the conditions for carrying on a regulated activity (including a regulated cryptoasset activity) are met.* ***Where the objective operational-control criteria described in PERG 18.1.17 are satisfied, the FCA would not generally expect the operation of the arrangement, in and of itself, to cause any person to carry on a regulated activity.***"

II. Technical service provider exclusion – key provision changes

The "merely provides" concept (PERG 18.8.26)

To confirm that common, objective user-interface features are not substantive participation, we propose adding the following immediately after the list of six indicators in PERG 18.8.26:

"***Standard, objective user-interface features remain merely technical and do not, of themselves, mean that A selects the service provider or decentralised protocol to be accessed, or that A exercises discretion or participates substantively in a transaction. For example, offering a default route that C can override and that is given no special prominence beyond being the default, using pre-integrated application programming interfaces and an algorithm to compute and display, from objective data, the exchanges, liquidity sources or decentralised protocols through which a transaction specified by C could be executed, ranking or ordering those options on an objective, quantitative basis such as by lowest cost or highest liquidity (which is not ranking by reference to qualitative features within indicator (4)), and providing objective information or warnings about the risks of different routings such as slippage, are each of this character, provided C selects the option and C signs the instruction which initiates the transaction.***

What matters is whether A accepts an order and assumes responsibility for obtaining a particular execution outcome, such as best price, exercising judgement and discretion to do so (for example, as a broker would). Software that applies disclosed, objective, pre-programmed logic to compute and display options, including a strategy that C has selected and that a smart contract executes, does not do so. The distinguishing line should be drawn by reference to whether A controls C's cryptoassets or transactions or has assumed responsibility for their outcome, and the indicators of discretion and participation in PERG 18.8.30 and PERG 18.8.31 should be read as evidence informing the response to that question. For example, a broker that holds customer funds and accepts orders assumes such responsibility, whereas a non-custodial wallet provider does not, and the user retains the choice."

We also propose deleting the undefined term "*shaped*", which has no settled meaning and invites the subjective assessment the guidance should avoid:

"*Conversely, the exclusion is less likely to apply where A's service is part of the process by which transactions are selected,* ~~*shaped*~~*, directed, negotiated, routed or brought about.*"

We also propose amending indicator (4) in PERG 18.8.26 and indicator (1)(d) in PERG 18.8.30 so that ordering options on objective, quantitative criteria is not treated as qualitative ranking or as discretion:

"*(4) A does not select, recommend or rank counterparties, service providers, protocols, liquidity sources or execution routes by reference to* ***a qualitative assessment of*** *the circumstances of a proposed transaction or other qualitative features* ***(ordering options on***

objective, independently verifiable quantitative criteria that are disclosed in advance and applied consistently is not such a ranking);"

"*(d) selects or adjusts routing by reference to an assessment of price, liquidity, speed, transaction costs, counterparty risk or likely outcome****, other than by the application of predetermined objective rules disclosed to C***;"

Connection to a decentralised platform (PERG 18.8.28). A TSP may have some form of connection or role in relation to a decentralised platform. That should not necessarily disqualify reliance on the exclusion, for example where the TSP does not control the protocol. We propose amending the following sentence in PERG 18.8.28 so that it is control, not mere involvement, that defeats the exclusion:

"*Similarly, where A's involvement with the protocol extends beyond merely facilitating access to it,* ***such that A controls the protocol,*** *A may not be able to rely on this exclusion.*"

Discretion and substantive participation (PERG 18.8.30 and 18.8.31)

To confirm that the neutral display or presentation of information to C does not equal discretion, we propose adding the following clarification immediately after the list of discretion indicators in PERG 18.8.30(1), making clear its relationship with indicator (1)(e):

"***The display or presentation of information to C, including the display of a price or quote or of the service providers, protocols or execution routes through which a transaction specified by C could be executed, does not, in and of itself, reflect a qualitative assessment of their suitability or merits within indicator (1)(e) and does not amount to discretion over a transaction. At most it is a choice as to what is shown to C, and not a decision by A as to whether, where or how a transaction takes place. Such decision is made by C, who selects the option shown and signs the instruction that initiates the transaction.***"

To confirm that authorship of an objective algorithm is not, by itself, discretion, we propose adding the following to PERG 18.8.30:

"*The fact that software uses an algorithm does not necessarily make the service non-discretionary. Predetermined software may implement judgements previously made by A, and an algorithm may select among alternatives by reference to criteria determined or adjusted by A.* ***However, an objective, pre-programmed algorithm that is applied consistently and disclosed to C is not discretion merely because A created or maintains it, nor because the criteria it applies were determined by A, where those criteria are objective, disclosed to C and applied in the same way to every user and transaction. The relevant question is whether, considering the design and operation of the service as a whole, A exercises or has assumed responsibility for judgement materially affecting the transaction.***"

To ground the "*held out*" factor in an assumption of responsibility for the outcome of transactions, we propose amending factor (6):

"*(6) holds itself out as arranging, executing, optimising or otherwise taking responsibility for transactions,* ***such that a reasonable user would understand A to have assumed responsibility for the outcome of the user's transactions (the mere fact that software is held out as enabling users to transact in qualifying cryptoassets is not, in and of itself, sufficient);***"

To mark the boundary of substantive participation at discretionary management of a user's assets by a person, we propose adding the following:

"*In the FCA's view, substantive participation or intermediation may arise where A performs a material role in the arrangements through which transactions are facilitated or entered into, rather than remaining a neutral means of access.* ***This includes a person that, without instruction from C, and by reference to its own ongoing judgement, decides where C's cryptoassets should be deployed and reallocates them. It does not include a non-custodial tool that applies a disclosed, pre-programmed strategy that C has selected, including one that rebalances automatically according to predetermined objective rules, and that responds to instructions initiated by C.***"

To reflect HMT's intention, expressed at paragraph 6.10 of the Explanatory Memorandum to the Amending Regulations, that a person enabling access to "*one or more*" services of "*one or more*" providers or protocols is not for that reason arranging, we propose amending factor (1) in PERG 18.8.31 by adding the following:

"*(1) determines which services, providers or protocols C can access* ***(the selection, in the design of A's service, of the services, providers or protocols made available through it, whether one or several, is not of itself such a determination or substantive participation where that selection is disclosed to C, is not varied by reference to subjective factors relating to particular transactions or users, and where: (i) A's remuneration is not affected by which service, provider or protocol executes the user's transaction, for example, A does not receive inducements or payment for order flow from the provider or protocol)****;*"

To confirm that a route-, venue- and counterparty-agnostic fee does not defeat the exclusion, we propose making the FCA's own qualification operative:

"*Likewise, transaction-linked remuneration may be relevant but will not determine the issue without considering the functions for which the remuneration is paid.* ***A fixed fee, or a fixed fee or percentage per transaction, that is product-, execution-, route-, venue- and counterparty-agnostic does not, in and of itself, indicate substantive participation. Remuneration is relevant only where it varies with C's choice of product, route, venue or counterparty, or is otherwise structured so that A assumes responsibility for the outcome of the transaction.***"

The "decentralised protocol" limb (PERG 18.8.28 and 18.8.32)

To address the "*A is not V*" problem, we propose confirming that developing or maintaining a protocol, and organising governance participants through a legal entity, do not make a person the protocol:

"*Therefore, a person cannot be both A and V for the purposes of this exclusion.* ***A person is not to be treated as the decentralised protocol (V) merely because it develops, maintains or adapts the protocol, whether or not under a formal agreement, or because it is a foundation or other entity through which participants in the protocol's governance have organised themselves. The relevant question is whether that person controls the protocol, assessed against the criteria described in PERG 18.1.17.***"

To make control, rather than the existence of maintenance, the organising concept, we propose amending factor (a):

"*(a) engage in its ongoing maintenance and adaptation**, to the extent that doing so amounts to control over the protocol;***"

To resolve the point-in-time and status-over-time problem, under which a provider could be found in breach for a period of undisclosed control it could not reasonably have detected, we propose adding the following to PERG 18.8.32, framed by reference to the defence in section 23(3) of FSMA:

"***In the FCA's view, a person relying on article 9Z2A(2)(b) should assess, and keep under periodic review, whether the arrangements to which it provides access are a decentralised protocol, applying the considerations in this Question and in PERG 18.1.17 to the information publicly available to it. A documented process of that kind, together with prompt action to restrict access where the assessment changes, is relevant to whether the person has taken all reasonable precautions and exercised all due diligence for the purposes of section 23(3) of the Act, and the FCA will take it into account in deciding whether to take action.***"