Global Blockchain Business Council (GBBC): Response to FCA DP25/1: Regulating Cryptoasset Activities

About us:

Global Blockchain Business Council (GBBC) is the trusted non-profit association for the blockchain, digital assets, and emerging technology community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 284 Ambassadors across 124 jurisdictions and disciplines.

GBBC furthers adoption of blockchain and emerging technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chain, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), Food for Crisis, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).

Chapter 2 Cryptoasset Trading Platforms

Q1. What are the operational and practical challenges of applying the suggested trading, market abuse, and other requirements to authorised overseas firms operating branches in the UK? Are there alternative approaches that could equally mitigate the risks?

The proposed application of UK trading, market abuse, and conduct requirements to overseas firms operating UK branches raises significant practical challenges. In particular, enforcement limitations may undermine the regime's effectiveness: FCA jurisdiction over parent entities, data access, and offshore decision-makers remains constrained.

UK branches of global CATPs may lack full operational autonomy to implement trading systems or surveillance tools that meet UK-specific standards, creating risks of ineffective or fragmented compliance.

We suggest that the FCA prioritise structured cooperation agreements and MoUs with overseas regulators, standardised technical reporting frameworks, and where appropriate, equivalence regimes for jurisdictions with aligned market integrity standards. A phased, risk-based supervisory model could also help: higher-exposure UK branches could face stricter local compliance, while lower-risk firms might benefit from a proportionate approach.

These measures would help achieve UK policy goals while avoiding market fragmentation or unnecessary barriers to UK market access.

Q2. What are the challenges and limitations of requiring the establishment of an affiliated legal entity for retail access to trading services by an overseas firm with a UK branch?

While the FCA proposal does not strictly require firms to operate both a UK branch and a UK-incorporated legal entity, members noted that this branch option is designed to allow firms to rely on their parent's capital, potentially reducing the capital obligations that would otherwise apply to a fully UK-incorporated entity. This structure could provide useful flexibility for some firms, but there are concerns that it may also introduce compliance complexity and disincentivise some forms of market entry.

Members further suggested that the FCA's approach should be informed by international precedents, such as those under MiFID2 or equivalent regimes, and by the availability of supervisory MoUs with third-country regulators. Without such alignment, the model could risk creating fragmented or duplicated obligations across jurisdictions.

Finally, it was emphasised that the impact of this model on capital deployment and cross-border liquidity provision must be carefully considered. Where firms choose to operate with a UK branch, it should be clear which Prudential obligations are home- vs host-supervised, and how this interacts with UK consumer protection requirements.

Q3. What conditions should apply to the direct access of trading services of an overseas CATP with a UK branch?

The FCA's proposed approach — requiring overseas firms serving UK retail clients to operate through a UK-authorised legal entity, with the option of establishing an accompanying UK branch — may create operational and commercial barriers for global CATPs, particularly those currently serving UK clients cross-border. While the branch model is intended to provide flexibility and reduce capital duplication, the combined need for a UK legal entity and complex structuring may still deter entry or result in market withdrawal.

An alternative, or complementary, approach could involve allowing direct retail access through a UK branch alone, provided robust supervisory conditions are met. If the FCA adopts such a model, we suggest that the following minimum conditions could be applied to balance market access with regulatory safeguards:

- The existence of a formal cooperation agreement or Memorandum of Understanding (MoU) between the FCA and the CATP's home regulator, covering reciprocal supervision, enforcement cooperation, and data-sharing on trading activity;
  Compliance by the UK branch with UK-specific conduct requirements, including Financial Promotion rules, market abuse prevention standards, and consumer protection obligations;
- Provision of regular, standardised reporting to the FCA on order flow, execution outcomes, and market integrity metrics relevant to UK clients;
- Maintenance of effective governance and operational controls within the UK branch to support compliance with UK rules, including clear accountability for client-facing activities;
- Transparent disclosure to UK retail clients regarding the legal status of the entity, applicable regulatory protections, and any differences from the protections available under a fully UK-authorised firm model.

We believe that such a risk-based and cooperative framework could enable proportionate access to the UK market for overseas CATPs, while maintaining regulatory integrity and consumer confidence.

(We would note that further clarity on the regulatory perimeter for non-retail cross-border activity remains needed — see our response to Q1 — to avoid creating uncertainty for instituional business models.)

Q4. What, if any, additional responsibilities should we consider for CATPs, to address the risks from direct retail access?

Where CATPs provide direct retail access, the platform should bear clear responsibility for core market conduct standards, including real-time surveillance, customer transparency, and post-trade reporting.

However, surveillance and conduct expectations should be calibrated to reflect the specific risks of each CATP model — e.g. whether it operates an open order book, hybrid OTC model, or purely request-for-quote interface.

Platforms should be required to deploy real-time trade surveillance capable of detecting abusive patterns such as layering, spoofing, wash trading, and cross-market manipulation — including where execution spans centralised and decentralised venues.

Enhanced transparency requirements should include order attribution, clear audit trails, and accountability across the trading lifecycle.

Q5. How can CATPs manage the risks from algorithmic and automated trading strategies?

We agree that cryptoasset trading platforms should be required to implement effective real-time surveillance frameworks to monitor and mitigate the risks arising from algorithmic and automated trading strategies. Such frameworks should enable platforms to detect potential market abuse patterns — both on-chain and off-chain — while supporting proportionate and innovation-friendly oversight.

Key capabilities should include:

- Identification of abusive behaviours such as quote stuffing, layering, spoofing, and manipulative order flows that distort price discovery or create misleading market signals;
- Tagging of algorithmic orders to enable clear attribution to specific clients or strategies;
  Behavioural analysis over time to detect evolving patterns and cross-session misconduct;
- Monitoring for cross-platform and cross-asset manipulation where relevant;
  Integration of diverse data sources — including on-chain analytics and off-chain signals — to improve contextual awareness and detection accuracy.

We caution that regulatory approaches to algorithmic trading must clearly distinguish between inherently abusive practices and legitimate, strategy-driven behaviour. For example, latency arbitrage, while often discussed in this context, is not intrinsically abusive and reflects normal dynamics in competitive electronic markets. Regulatory interventions should be targeted and proportionate, avoiding the unintended suppression of lawful market activity.

Q6. Do you agree that CATPs should have contractual agreements in place with legal entities operating market making strategies on their platforms? Are there alternative approaches that could equally mitigate the possible risks to market integrity?

Platforms should be expected to put in place contractual agreements with market makers where the latter receive preferential treatment, including access to APIs, latency advantages, or early

visibility into order books. These agreements should define quoting obligations, minimum spread tolerances, conflict mitigation processes, and transparency requirements.

However, platforms should not be required to contract with all market participants — many liquidity providers operate independently or pseudonymously. A threshold-based approach, such as contracts being required only where market makers receive privileged data or incentives, would mitigate conflicts of interest without overburdening open market dynamics.

In decentralised or permissionless contexts, smart contracts or DAO-vetted frameworks could substitute formal contracts. The FCA could provide a safe harbour where such decentralised market making mechanisms follow publicly disclosed rules and independent audit standards.

Q7. Is there a case for permitting discretionary trading practices for CATP operators? If so, how could the above risks be appropriately mitigated?

The FCA's proposed bias against discretionary execution may overlook legitimate use cases for discretionary trading practices, particularly for block trades or illiquid pairs. A complete restriction could stifle innovation in RFQ or auction-style matching models that are important to institutional and OTC workflows.

Rather than ban discretionary execution outright, the FCA could consider conditional permissions where trades above certain thresholds or under specified liquidity constraints are flagged as discretionary and subject to audit. Transparency obligations — such as real-time public logs of discretionary executions, post-trade disclosures, or customer flagging — could mitigate unfairness while preserving operational flexibility.

Q8. Should firms operating a CATP be permitted to execute transactions on a matched-principal basis? If so, how could the above risks be appropriately mitigated?

Matched-principal trading is a common and legitimate execution model in crypto markets, particularly for maintaining liquidity and price continuity. Banning MPT could disadvantage newer or less liquid markets where external liquidity is absent and internalisation of order flow is the only efficient model.

Rather than prohibit MPT, the FCA could require platforms engaging in it to disclose trade volumes, order types, and matching mechanics, while implementing safeguards to avoid conflict of interest. These could include segregating matched-principal desks from other functions, capping MPT activity relative to platform volume, and disclosing any associated fee benefits to users.

Q9. Have we properly identified the risks from the operator of a CATP also being able to deal in principal capacity off-platform? What is your view on these risks and whether it should be permitted or restricted for an operator of a CATP? If permitted, how should those risks be mitigated?

There is broad recognition of the risk that off-platform proprietary trading by CATP operators could create informational and integrity-related vulnerabilities. However, the risks should be assessed proportionally to the market structure and specific use cases. In particular, blanket prohibitions on principal activity may be inappropriate in less liquid markets or for firms acting as liquidity providers in good faith.

A more calibrated regulatory approach could include:

- Transparency requirements to disclose whether a CATP or its affiliate engages in off-platform principal activity;
- Ring-fencing of data flows between the CATP and trading desks;
- Implementation of robust information barriers, with audit trails and internal monitoring;
- Volumetric thresholds or caps on off-platform principal activity.

This would strike a balance between preserving liquidity and ensuring market integrity, especially given the market-making function that some entities play in early-stage or low-liquidity token markets.

Q10. What are the risks from an entity affiliated with the CATP trading in principal capacity either on the CATP or off the CATP? What additional requirements are necessary to mitigate these risks?

In markets with lower liquidity or for newly listed cryptoassets, matched-principal trading may be necessary to ensure orderly execution and reduce slippage. A categorical prohibition could hinder the development of efficient price discovery and introduce practical barriers for new entrants. A more flexible approach could involve limiting matched-principal activity by percentage of volume or allowing it under specific conditions (e.g., pre-trade transparency and conflict management controls).

On proprietary trading, policy should distinguish between vertically integrated CATPs engaging in own-account trading and affiliated entities providing liquidity under controlled arrangements. Rather than impose a blanket prohibition, regulatory objectives may be better achieved through transparency requirements, volume caps, and structural separation (e.g., distinct legal entities or firewalls).

Trading by affiliated entities should be subject to stringent disclosure and governance controls to avoid perceived or actual conflicts of interest. Platforms should implement rules preventing privileged access, price manipulation, or undisclosed inter-affiliate routing.

One approach could include: (1) mandatory public reporting of affiliated entity trading activity; (2) independent audit trails; (3) restrictions on timing of trades around listing events; and (4) real-time flagging of affiliate orders on the order book.

Q11. What are the risks from admitting a cryptoasset to a CATP that has material direct or indirect interests in it? How should we address these?

The FCA is right to raise concerns over self-listed or materially affiliated cryptoassets, including those where the CATP holds governance rights, token allocations, or equity stakes in the issuer. These arrangements may introduce substantial conflicts of interest.

A proportionate regulatory response could include:

- Mandatory public disclosure of any direct or indirect interests the CATP has in a listed token;
- Requirement for an independent listing committee or external review of listing decisions for affiliated tokens;
- Enhanced governance controls to prevent undue influence over price formation and listing timelines;
- Specific prohibitions on fee rebates, market-making incentives, or liquidity support arrangements for affiliated tokens.

Such controls would mirror best practices in traditional finance for related-party listings.

Q16. Which challenges may emerge for transaction data requirements if there is direct retail participation?

Firstly, transaction data disclosures should be designed with retail users in mind. Retail-facing interfaces should provide clear and intelligible reporting of key transaction metrics — such as execution quality, pricing, and slippage — presented in a user-friendly format. Retail clients cannot reasonably interpret raw technical data; therefore, high-level summaries and intuitive dashboards are essential to support informed decision-making.

Secondly, privacy considerations become more salient when intermediaries and CATPs process transaction data related to retail customers. Data collection and transmission should prioritise the protection of personal identifiable information (PII). In practice, pseudonymisation or tokenisation of user identifiers should be implemented, with PII accessible only under strict conditions for anti-money laundering or regulatory enforcement purposes.

In addition, effective transaction data frameworks should support detection and mitigation of risks particularly relevant to retail participation, such as:

- Monitoring for suspicious activity that may indicate account compromise or abusive trading;
- Providing context on the characteristics and risks of traded tokens, including governance and smart contract integrity, where feasible;
- Disclosing material information about market maker arrangements to support transparency and fair access.

Q17. Are there preferred standards for recording transaction data?

We're of the view that globally recognised industry standards should form the basis of any recording of transaction data. ISO standards provide different levels of structure. While ISO 20022 is expansive in capabilities around standard definitions/processes etc, other ISO standards like DTI and LEI should also be leveraged to provide clear identification of tokens and entities respectively.

The extent of standardisation for smart contracts is limited to specific ledgers, as each ledger has different smart contract data and structure. In terms of identification, data fields such as names, ticker symbols, and even smart contract addresses are not unique and can be duplicated across different ledgers. Instead, the use of DTIs provides a consistent identification method for specific token implementations.

Q18. What opportunities and challenges do you see in trying to harmonise on-chain and off-chain transactions' recording and/or reporting?

A harmonised approach would enable a more holistic view of market activity, supporting improved detection of market abuse, stronger investor protection, and more consistent regulatory oversight. In particular, the integration of execution and settlement data across centralised and decentralised venues would facilitate:

- More accurate monitoring of abusive behaviours such as wash trading, spoofing, and insider dealing;
- Enhanced traceability of asset flows and cross-platform trading activity;
- Improved reliability and auditability of transaction records for regulatory reporting.

Harmonisation could also unlock new avenues for innovation, including the development of compliance-aware smart contracts and the use of verified off-chain data to inform on-chain risk controls and market protections.

However, significant implementation challenges remain. On-chain data structures are typically optimised for cryptographic assurance and decentralised consensus, not regulatory reporting. Achieving interoperability with off-chain transaction records will require:

- Standardisation of identifiers, timestamps, and event classifications across ecosystems;
- Careful management of privacy concerns, particularly where pseudonymous on-chain addresses are linked to real-world identities;
- Collaboration with decentralised communities to develop reporting mechanisms that are compatible with DeFi's governance structures and technological constraints.

The absence of central governance in many DeFi protocols further complicates efforts to impose consistent data standards. Practical approaches may include the adoption of compliance-supporting modules at the protocol level, the development of shared industry

frameworks, and targeted regulatory guidance for relevant actors such as front-end operators or governance participants.

Chapter 3 - Cryptoasset Intermediaries

Q19. What practical challenges might firms face if they are required to comply with these order handling and best execution requirements? Are there any alternative approaches that would deliver the same or better order execution outcomes for retail and non-retail customers respectively? Please explain why they may be preferable.

The FCA proposes to apply best execution rules aligned with COBS 11.2A, requiring intermediaries to take "all sufficient steps" to achieve the best possible result for their clients, considering total consideration. However, crypto markets are fragmented, with execution across decentralised exchanges, OTC venues, and centralised platforms with inconsistent data feeds.

Best execution principles are difficult to operationalise in fragmented crypto markets where price formation occurs across on-chain, OTC, and centralised venues, many of which may not be UK-authorised.

Firms should be permitted to construct execution frameworks based on risk-weighted venue selection, rather than mandating a fixed number of UK platforms. Execution policies should include how firms source prices, how they measure execution quality post-trade, and how they deal with tokens traded only on non-UK venues.

For certain asset types or transaction sizes, firms could provide scenario-based evidence that their execution achieved the best result under prevailing liquidity conditions, even if pricing data was sparse or non-standard.

Q20. What benefits and risks do you see with the proposed guidance requiring firms to check the pricing for an order across at least 3 UK-authorised trading platforms (where available)?

The proposed requirement to check pricing across three UK-authorised trading venues is not practical under current market conditions. The number of UK-authorised CATPs is currently limited, and many do not yet support a comprehensive or representative range of asset pairs. As a result, mandating a three-venue comparison could constrain execution quality, particularly for tokens not widely available across UK platforms.

Members emphasised that this approach is operationally unworkable in many cases. Given the fragmentation of liquidity across both centralised and decentralised platforms, and the varying degrees of transparency, such a rigid requirement is likely to distort execution outcomes and increase costs for retail users. For certain tokens or trading pairs, even a single UK venue may not offer adequate liquidity, and forcing intermediaries to conduct a mechanical venue comparison could result in artificial delays or poorer pricing outcomes.

A more proportionate and effective approach would be to apply a principles-based best execution standard, allowing intermediaries to reference a representative and liquid set of venues based on prevailing market dynamics — including both UK-authorised CATPs and reputable international platforms. This would better reflect the realities of global crypto market structure, while still protecting client interests and promoting effective price discovery.

Q21. What benefits and risks do you see with the idea that best possible results should be determined in terms of the total consideration when firms deal with retail customers?

The principle of total consideration — combining price, fees, venue costs, and related charges — is aligned with the FCA's broader COBS regime, but presents unique challenges in crypto markets. Execution costs in decentralised environments are highly variable and often contingent on third-party gas fees, routing complexity, and even protocol-level changes.

For example, routing a swap via a decentralised exchange aggregator may yield a better nominal price but incur additional smart contract or gas costs. These costs are dynamic and cannot always be known in advance. Consequently, a rigid "total consideration" formula may misrepresent actual user outcomes or penalise certain execution paths that are ultimately more beneficial.

A principles-based standard — requiring firms to document their execution methodology and consider all relevant cost components where reasonably knowable — would offer flexibility while maintaining consumer protections. The FCA could also consider issuing standard templates or reporting formats for total consideration analysis, especially where decentralised trading paths are involved.

Q22. Do you see any potential problems with the proposal to restrict intermediaries to offering regulated services for UK retail customers solely for cryptoassets admitted to trading on a UK authorised CATP?

The proposed restriction would dramatically narrow the range of tokens accessible to UK retail users, especially early-stage or DeFi tokens not yet listed on a UK-authorised venue. While the goal is to align with the A&D/MARC regime, it may produce anti-competitive effects by disadvantaging non-CATP tokens and reinforcing concentration among early CATP entrants.

This restriction may create unintended behavioural dynamics. Sufficiently motivated retail users may bypass UK-regulated venues altogether—using regulated onramps to acquire assets like stablecoins, and then transacting via offshore or decentralised platforms. It remains unclear whether this outcome is consistent with FCA's intended policy goals. On one interpretation, it could be seen as a failure of perimeter design, if it drives users toward unregulated venues; on another, it could reflect a tolerance threshold—where users who navigate DeFi independently are presumed sufficiently sophisticated to bear those risks.

In addition, there is a potential revenue displacement effect. By preventing intermediaries from facilitating access to non-CATP tokens, the rule may push trading volumes toward offshore

platforms, thereby reducing the commercial viability of UK-regulated firms and weakening competition in the domestic market.

We recommend that the FCA explore a more flexible model that permits intermediaries to offer access to high-quality, globally liquid tokens that meet basic due diligence thresholds, even if they are not yet admitted to trading on a UK CATP. This could include enhanced disclosure, firm-level risk assessments, and periodic reviews to ensure standards are met—without sacrificing retail choice or market innovation.

Q23. Are there any specific activities or types of transactions we should expressly carve out of our proposed order handling and best execution rules? If so, why?

Certain activities in crypto markets do not lend themselves to traditional best execution analysis. Examples include:

- **Liquidity pool interactions** in DeFi, where the price is set algorithmically and execution is immediate;
- **Inter-affiliate trades** used for internal treasury management;
- **Smart contract-based redemptions**, e.g. burn-and-mint protocols or programmatic token swaps;
- **Cross-chain bridging**, where execution depends on a sequence of external validator actions.

Applying strict best execution rules to these transactions would be both operationally complex and of limited benefit. Instead, the FCA could adopt a carve-out framework where firms justify exemption based on:

- The absence of discretion in execution;
- The functional equivalence to automated settlement;
- The pre-determined or immutable nature of the pricing logic.

This would reduce unnecessary compliance burdens while focusing regulatory scrutiny on discretionary, client-facing execution scenarios.

In a fragmented liquidity environment, it is crucial to allow carve-outs for certain transactions where routing to a UK CATP would not serve the client's best interest. Specifically, large-cap tokens commonly traded offshore and complex DeFi-based trades (e.g., through DEX aggregators) may not lend themselves to traditional venue-based execution models. The FCA should explicitly permit such carve-outs where firms can demonstrate that routing decisions are based on best outcome principles and robust disclosure to clients.

Q24. What risks arise when specific instructions (for example, specifying which execution venue to use) from retail customers are allowed to override certain best execution requirements? How can these be mitigated?

Allowing specific instructions from retail clients may pose risks of worse execution outcomes or unintended exposure to low-liquidity venues. However, full prohibition could undermine client autonomy or conflict with professional client practices.

One approach would be to require firms to assess the appropriateness of such instructions, and to ensure that they are documented and voluntary. Specific instructions could trigger a mandatory risk disclosure or confirmation of understanding, akin to existing frameworks under MiFID II.

From an operational perspective, firms should also maintain internal controls that flag when client-directed execution routes result in materially worse outcomes compared to benchmarks. This could prompt follow-up disclosures or a revised execution policy.

In line with points raised regarding Q22 and market behaviour, members noted that where clients deliberately choose to access DeFi tokens or use specific venues, intermediaries should be permitted to honour client instructions, provided that risks are clearly disclosed and the client's sophistication is documented. A blanket override of client choice would likely be circumvented in practice by routing via unregulated channels.

Additionally, firms should not ask clients to choose specific execution venues without providing disclosures on the potential impact of such choice, including possible risks of poorer execution outcomes or reduced liquidity. The requirement to inform and disclose should mirror the principles applied in the traditional financial framework, where client instructions override best execution obligations only when properly documented and explained.

Q25. Are there circumstances under which legal separation should be required to address potential conflicts between executing own orders and client orders?

The FCA's concern around front-running, improper sequencing, and internalisation of order flow is valid. However, a mandatory legal separation may not be proportionate for all firms, particularly smaller intermediaries or those acting transparently as principal.

For firms dealing in qualifying cryptoassets as principal — where the firm is the direct counterparty to clients and provides clear transaction pricing and fees before order placement — legal or functional separation should not be required. In such cases, transparency and disclosure, combined with robust internal conflict management policies, can provide proportionate and effective safeguards. We agree with the view that principal-based firms presenting clear fees and pricing upfront should not face legal separation obligations solely to manage these risks.

For firms acting in an agency capacity or where there is a risk of improper order internalisation, functional separation — including physical access controls, independent monitoring of trading desks, and robust surveillance of order sequencing — may achieve the same policy objectives. For larger or vertically integrated entities, a legal separation may still be appropriate, especially where execution conflicts are persistent or material.

An outcomes-based standard could be applied: if a firm can demonstrate that its governance and conflict management policies effectively mitigate these risks, it should not be required to undergo legal restructuring.

Q26. Are there any other activities that may create conflicts of interest and risks to clients if performed by the same intermediary? How can these be managed?

In addition to proprietary trading and order execution, participants noted concerns around:

- **Preferential routing** of orders to affiliated trading venues or liquidity providers.
- **Payment for Order Flow (PFOF)** models, which may incentivise execution based on commercial terms rather than client outcomes.
- **Dual-role agents**, who provide both advisory and execution services in the same transaction chain.

Effective mitigations could include:

- Full **disclosure** of economic incentives tied to routing or counterparties.
- **Prohibitions or caps** on volume routed to affiliated entities without client consent.
- **Independent reviews** of order routing quality and fairness, particularly where firms receive rebates or inducements.

Q27. What benefits does pre-trade transparency provide for different types of market participants and in what form will it be most useful for them? Please provide an analysis of the expected costs to firms for each option if available.

Pre-trade transparency may be difficult to implement in certain quote-driven or RFQ markets. However, it can enable more competitive pricing and reduce information asymmetries.

For firms dealing in qualifying cryptoassets as principal — where they act as the direct counterparty and provide clear transaction pricing and fees to clients before order execution — mandatory public pre-trade transparency obligations are not appropriate. These firms already ensure pricing transparency at the point of client interaction and trade placement, in line with established good practices.

For firms acting in an agency capacity or providing liquidity to broader market participants via an order book model, pre-trade transparency obligations may play a stronger role in promoting market integrity and competition. However, the operational and infrastructure costs of publishing live quotes across multiple venues — particularly for illiquid or volatile tokens — should be carefully considered to avoid adverse impacts on liquidity provision.

A tiered approach may be appropriate:

- For **high-liquidity tokens**, publication of bid/ask quotes across authorised venues could be required, ensuring comparability.

- For **illiquid assets**, exemptions could apply where real-time quoting would impair execution or invite front-running.

Firms could be permitted to use **aggregators or approved publication arrangements (APAs)** to reduce infrastructure costs. Alternatively, smart contract-based quoting systems may offer technical efficiency with automatic quote publication.

Q28. What alternative solutions to the post-trade transparency requirements proposed above could mitigate the risks? Please provide an analysis of the expected costs to firms for each option if available.

Post-trade transparency supports price formation but may be operationally burdensome for firms executing complex trades or acting as principal.

For firms dealing in qualifying cryptoassets as principal — where the firm acts as the direct counterparty to the client and provides full pricing and transaction details at the point of execution — post-trade transparency requirements should not apply. These client-facing principal trades already provide transparency to the affected party, and additional public reporting would create unnecessary operational burden without delivering incremental consumer benefit.

For other trading models, proportionate post-trade transparency requirements could support market integrity. Where applied, such requirements should take account of token liquidity, market model, and potential costs, and could allow for solutions such as batch reporting or anonymised publication.

Q29. Do you believe that certain cryptoassets should be exempted from transparency requirements? If so, what would be the most appropriate exemption criteria which would best balance the benefits from transparency and costs to the firms?

One approach under consideration is to exempt cryptoassets based on a combination of liquidity and market maturity criteria. For example, tokens with extremely low daily trading volumes, those held primarily by a small number of addresses (indicating concentration risk), or those lacking reliable pricing feeds may present limited price discovery benefit from public transparency — while imposing disproportionate technical and compliance costs on firms.

However, caution is warranted in defining such exemptions too broadly. Overuse could undermine transparency objectives and invite regulatory arbitrage. A balanced approach could involve:

- Setting minimum liquidity thresholds (e.g. daily average volume, number of trades per day) below which pre- or post-trade transparency obligations could be waived.
- Considering token age and volatility as part of a risk-based exemption model.
- Applying waivers temporarily for new listings, similar to MiFID's treatment of less liquid instruments.

Transparency requirements should not be applied to qualifying stablecoins. Such stablecoins are designed to maintain a stable value referenced to fiat currencies and generally do not pose the same market transparency risks as volatile cryptoassets. Imposing pre- or post-trade transparency requirements on transactions involving qualifying stablecoins could create unnecessary complexity without improving consumer outcomes or market integrity.

Beyond qualifying stablecoins, exemptions should also be considered for low-volume or illiquid tokens where mandatory transparency would likely impair liquidity or distort execution outcomes.

Q30. What would be the most appropriate exemption threshold to remain proportionate to the size of the firm while balancing the benefits from transparency and costs to the firms?

Proportionality was a recurring theme in the working group discussions. Members noted that transparency-related infrastructure costs — especially around pre-trade publication or real-time reconciliation — may be disproportionately burdensome for smaller or newer firms.

To balance this, the FCA might consider:

- **Volume-based thresholds**: e.g. firms below a defined annual trading volume or market share percentage could be subject to lighter transparency obligations.
- **Client count or user activity thresholds**: recognising that firms serving only a small number of professional or high-net-worth clients may pose lower systemic transparency risks.
- **Token-specific metrics**: such as market capitalisation or listing status on regulated venues.

Several participants expressed support for a tiered regime similar to MiFID's treatment of Systematic Internalisers — where obligations phase in based on a firm's activity relative to defined market metrics.

We recommend that any exemption regime also include regular review mechanisms to reassess firm eligibility and minimise gaming or circumvention.

Firms should be given discretion to determine the application of transparency requirements to their activities based on the specific features of their business, including size, trading volumes, and the types of cryptoassets for which they provide services.

Rigid thresholds may fail to reflect the diverse nature of crypto business models. A more effective approach would be to apply a proportionality principle — allowing firms to calibrate transparency practices in line with their operational scale and the market characteristics of the relevant tokens.

Q31. What are the crypto-specific risks of opting retail customers up? How should these be managed and what additional guidance on how to assess the expertise, knowledge and experience of clients can we give firms to better mitigate risks of harm?

We agree that the Financial Promotion regime already provides important protections regarding retail client communications. To further mitigate risks associated with opting up retail clients, firms should also conduct appropriate knowledge and experience assessments.

Quantitative thresholds can be a useful input to this process, but they should be used as flexible indicators rather than hard minimum criteria. Firms should retain discretion to apply a holistic assessment of client suitability, taking account of factors such as prior trading experience, financial sophistication, and risk tolerance

Q32. What are the benefits of having quantitative thresholds when opting clients up? How should we determine any quantitative threshold? What alternative rules or guidance specific to crypto should we consider?

While quantitative thresholds offer objectivity, traditional benchmarks (e.g. £500,000 in portfolio size or professional client income levels) may be poorly suited to crypto. For example, users with high exposure in self-custody wallets or across decentralised platforms may fall outside these parameters despite demonstrating informed engagement.

Alternative or complementary approaches could include:

- Custom thresholds based on wallet activity over time, number of protocol interactions, or value staked or traded;
- Use of risk-weighted indicators such as collateralised borrowing, multi-signature use, or participation in DAO governance;
- Requiring clients to pass product-specific appropriateness tests before accessing higher-risk features (e.g., leverage, algorithmic strategies, tokenised derivatives).

This would help align opt-up eligibility with user behaviour and system-level sophistication, offering greater flexibility while still supporting consumer protection.

Chapter 4 – Lending and borrowing

Q34. Do you agree with our current intention to restrict firms from offering access to retail consumers to cryptoasset lending and borrowing products? If not, please explain why.

A complete prohibition on retail access to cryptoasset lending and borrowing may be unnecessarily restrictive. Retail access to such products—when offered under appropriately supervised and capitalised conditions—can serve legitimate hedging and yield management needs. Risk mitigation could be better achieved through tiered access models, based on client knowledge assessments, risk disclosures, and clear eligibility thresholds. In particular,

regulated access to lending models using qualifying stablecoins or conservative collateral frameworks may merit exemption.

Chapter 5 – Restrictions on the Use of Credit to Purchase Cryptoassets

Q41. Would restrictions on the use of credit facilities to purchase cryptoassets be effective in reducing the risk of harm to consumers, particularly those vulnerable? Are there alternative approaches that could equally mitigate the risks?

We do not support an outright restriction on the use of credit cards or similar credit facilities for purchasing cryptoassets. The existing cryptoasset regulatory framework — including the Financial Promotion regime, the Consumer Duty, and firms' obligations to account for the needs of vulnerable customers — already provides strong and proportionate consumer protections in this area. A blanket restriction may risk distorting legitimate market behaviour and could unduly restrict consumer choice, while broader consumer protection goals can be more effectively addressed through the existing cross-sectoral regulatory tools.

In addition, it is important to recognise that the use of credit cards for cryptoasset purchases is not always an indicator of consumer vulnerability or speculative behaviour. In many cases, consumers may use credit cards simply because bank transfers or conventional payment methods are not supported by certain cryptoasset service providers or blocked by traditional financial institutions. This makes credit card use a matter of access, not merely a risk-driven choice. The FCA should therefore seek data to distinguish between these differing use cases, as a blanket restriction may inadvertently penalise users who rely on credit cards due to limited payment alternatives.

Furthermore, for genuinely vulnerable customers, a ban on credit card use may not mitigate underlying risks but instead push activity toward less regulated or higher-cost forms of credit, such as payday lenders or informal channels. A more effective and targeted approach would focus on monitoring patterns of use, enhancing disclosures, and ensuring robust protections through the Financial Promotions regime and Consumer Duty obligations, rather than imposing a broad prohibition.

Chapter 6 – Staking

Q42. Do you agree that firms should absorb retail consumers' losses from firms' preventable operational and technological failures? If not, please explain why? Are there any alternative proposals we should consider?

The FCA proposes that regulated staking firms should bear the burden for losses resulting from preventable errors — e.g. slashing or third-party validator failure — unless demonstrably outside the firm's control. This aligns with a principle of consumer protection grounded in operational accountability.

We recommend that the FCA consider international approaches when clarifying the scope of such obligations. For example, the recent **SEC Statement on Certain Protocol Staking Activities (May 2025)** explicitly addresses the role of third-party service providers, including validators and staking-as-a-service firms, in determining accountability. Similarly, **ESMA's guidance under MiCAR** provides initial views on how responsibility should be allocated where third-party actors contribute to operational outcomes.

It will be important for the FCA to clearly articulate which **third-party reliance models** are covered under this standard — including:

- Use of **external validators**;
- **Cloud-based staking services**;
- **Third-party staking-as-a-service providers**;
  Outsourced node operations or delegated staking pools.

Without such clarity, there is a risk of legal uncertainty and inconsistent treatment across business models. In line with good practice from the custody and fund management sectors, we suggest that firms should be required to conduct robust **vendor due diligence** and maintain appropriate contractual protections where they rely on third parties, but should not be held liable for losses resulting from risks outside their operational control—such as protocol-level vulnerabilities or force majeure events.

Our Members emphasised the importance of ensuring that the regulatory treatment of operational failures does not inadvertently penalise firms for events outside their control. It is critical to distinguish failures arising from protocol-level vulnerabilities, force majeure events, or validator malfeasance from those linked to preventable firm-level operational issues.

Moreover, further clarity is needed on the scope of "preventable" failures. Firms should not be held liable for protocol-level vulnerabilities or consensus failures that are external to their systems and beyond their operational control. One possible approach would be a shared-responsibility model where liability is tiered depending on whether failures stem from firm infrastructure (e.g. wallet mismanagement), validator performance (e.g. downtime, double-signing), or protocol code (e.g. smart contract bugs). Firms could be required to implement vendor diligence frameworks for validator selection and to transparently disclose validator risk metrics to consumers.

Q43. Do you agree that we should also rely on the operational resilience framework in regulating staking, including the requirements on accountability?

Proposals to place full liability on regulated firms for preventable operational or technological losses in staking merit further nuance. A strict liability standard may discourage participation by reputable firms or reduce innovation. A proportional approach may instead distinguish between losses due to firm negligence and those arising from protocol-level vulnerabilities or validator-level issues outside the firm's direct control. Leveraging the existing operational

resilience framework under SYSC, alongside risk management expectations tied to validator selection and monitoring, could achieve a more calibrated result.

Q44. Do you agree that firms should have to get express consent from retail consumers, covering both the value of consumer's cryptoassets to be staked and the type of cryptoassets the firm will stake, with each cryptoasset staked by the consumer requiring its own consent?

This proposal responds to concern that consumers do not clearly understand what they are staking, under what model (e.g., pooled, liquid), or whether they retain ownership of staked assets.

Requiring granular consent for each type and amount of cryptoassets staked by retail clients is intended to mitigate misunderstanding. However, this may introduce friction without meaningfully enhancing comprehension. A clearer model may involve periodic, consolidated consents supported by dynamic disclosures—e.g., notification of significant protocol risks, lock-up periods, or slashing events—backed by audit trails and opt-out provisions.

We support allowing customers to provide standing (retractable) consent in respect of staking cryptoassets of a particular type held in particular wallets or accounts, rather than requiring separate express consent for each individual staking transaction.

Standing consent models, combined with clear and accessible disclosures and withdrawal mechanisms, would provide an appropriate and user-friendly balance between informed consent and operational efficiency.

Q45. Do you agree that firms should provide a key features document as outlined above to retail consumers? If not, please explain why? What other means should be used to communicate the key features and risks of staking to consumers?

Firms should be given flexibility to determine the specific content of Key Features Documents for staking services, and the manner in which such documents are provided to clients. A principles-based approach would allow firms to tailor KFDs to the characteristics of the relevant staking services and to consumer needs, rather than imposing a rigid format.

This flexibility will be important in supporting effective consumer understanding, given the wide diversity of staking models and associated risk profiles across the market.

Q47. Do you agree that regulated staking firms should be required to segregate staked client cryptoassets from other clients' cryptoassets? If not, why not? What would be the viable means to segregate clients' assets operationally?

Our members believe it should not be mandatory to segregate staked cryptoassets from other clients' cryptoassets, provided that firms maintain accurate records of each customer's entitlements and exposures.

In many protocol-native staking models, technical segregation of staked assets is not feasible due to the nature of validator pools and staking mechanics. The key regulatory objective should be to ensure accurate and transparent client recordkeeping, rather than imposing a segregation requirement that may be operationally impractical or inconsistent with protocol design.

Q48. Do you agree that regulated staking firms should be required to maintain accurate records of staked cryptoassets? If not, please explain why?

We agree that staking firms should maintain accurate records of staked cryptoassets. Provided that firms keep robust and up-to-date client-level records of entitlements and exposures — consistent with the approach outlined in Q47 — this objective will be met.

Q49. Do you agree that regulated staking firms should conduct regular reconciliations of staked cryptoassets? If not, please explain why? If so, what would be the appropriate frequency?

The proposals around segregation and reconciliation of staked assets raise important operational questions. In practice, validators often pool staked assets across clients or across staking contracts, and the technical segregation of individual users' staked funds may be unfeasible depending on protocol design. To preserve auditability without mandating protocol-level changes, firms could be required to implement off-chain segregation controls (e.g., staking sub-ledgers) and reconciliations that ensure a reliable mapping between customer positions and on-chain exposure.

The feasibility of fully segregating staked cryptoassets is contestable. For Ethereum and other proof-of-stake protocols, assets are commonly pooled and delegated to validators, making technical segregation difficult. Firms could instead be required to maintain real-time client-specific sub-ledgers, conduct daily off-chain reconciliations, and provide audit trails of staking inflows and outflows. Clarification is also needed on how firms should handle slashed or inaccessible assets, and whether these are to be compensated or written down in client accounts.

Chapter 7 –DeFi

The regulation of decentralised finance remains one of the most conceptually and operationally complex areas within the UK's future cryptoasset regime. GBBC welcomes the FCA's recognition of these challenges and its tentative, proportionate approach. As outlined in DP25/1, the FCA proposes two tracks: (i) full application of regulatory obligations to persons or entities identifiable as in control of a DeFi service, and (ii) issuance of guidance where such control is absent. This section responds to Question 50.

Paragraph 7.4 opens the door to broad regulatory discretion by referring to "clear controlling person(s)" without offering technical clarity on what this entails. In most DeFi systems, governance is often distributed across token holders, DAOs, or multisig treasuries—none of which fit traditional definitions of centralized control. Without a well-defined threshold for

what constitutes control, there is significant legal uncertainty for protocol contributors and governance participants.

Further, the assertion in paragraph 7.5 that "activities which pose the same risks should have the same regulatory outcomes" fails to acknowledge how DeFi reconfigures those risks through open-source code, automated smart contracts, and non-custodial design. Risks in DeFi are mitigated not through firm-level oversight, but through transparent and pre-programmed mechanisms. Applying traditional consumer protection models such as creditworthiness checks or explicit consent flows to DeFi is unworkable and misaligned with the technology's architecture.

Paragraphs 7.6 and 7.10 compound this problem by proposing to apply the same regulatory obligations described in Chapters 2–6—designed for centralized lenders, custodians, and trading platforms—to all market participants, regardless of whether they are decentralized. This would be impractical and disproportionate. Most DeFi protocols cannot reasonably comply with requirements like client asset segregation or know-your-customer procedures, nor should they be forced to. These obligations were crafted for businesses with discretionary control over client funds and operations, not for permissionless software systems.

The concerns raised in paragraph 7.7 about operational resilience and vulnerabilities in smart contracts also misplace the source of systemic risk. As the failures described in earlier chapters show, consumer harm overwhelmingly stemmed from centralized custody and poor risk management practices—not from code-based execution.

Q50. Do you consider the proposed approaches are right, including the use of guidance to support understanding? What are the effective or emerging industry practices which support DeFi participants complying with the proposed requirements in this DP? What specific measures have you implemented to mitigate the risks posed by DeFi services to retail consumers?

We highlight the importance of ensuring that the FCA does not pursue a case-by-case supervisory approach in the absence of clear and predictable principles. Without structured guidance, there is a risk of arbitrary enforcement and legal uncertainty for DeFi participants. A more efficient and legitimate approach would be for the FCA to undertake a broader consultation process and establish specific principles to guide its future supervisory posture on DeFi — rather than rely solely on ad hoc guidance and a single roundtable.

A threshold issue is the definitional uncertainty surrounding DeFi and decentralisation more broadly. The term "DeFi" encompasses a broad spectrum of technical architectures and governance models, from heavily centralised platforms with decentralised branding to fully autonomous, non-custodial protocols. We recommend that the FCA adopt a functionality-based taxonomy that distinguishes services according to the degree of control, discretion, and user risk exposure — rather than by labels.

In line with this, the identification of a "responsible person" should be grounded in functional control. This could include:

- Entities or individuals who control front-end interfaces facilitating user access;
- Signatories to multisignature wallets governing protocol upgrades or treasuries;
- Developers or entities engaged in ongoing, centralised management or incentive structuring;
- Off-chain service providers (e.g., node operators, legal wrappers) with operational discretion over critical system components.

It is equally critical that the FCA clearly distinguish **custodial** from **non-custodial** services. The current DP and the Treasury's SI lack sufficient clarity on this point. Members strongly recommend that **non-custodial services should be explicitly excluded** from the scope of full financial services obligations. Applying the full financial services framework to non-custodial or purely protocol-based services — particularly where there is only a front-end interface and no custody or identifiable counterparty — would be practically unworkable. Obligations such as KYC or suitability cannot meaningfully be implemented in such contexts, and the regime must therefore differentiate carefully between types of service provision and layers of control.

Key Risks and Emerging Industry Practices

We agree with the FCA's identification of core DeFi-specific risks, including:

- Inadequate consumer understanding of protocol risk;
- Oracle manipulation and miner extractable value (MEV);
- Lack of recourse or restitution in case of protocol failure or asset loss;
- Regulatory arbitrage via pseudonymous or multisig-controlled systems.

At the same time, DeFi ecosystems increasingly incorporate industry-driven solutions to address market and consumer harm ex ante, which may provide analogous protections, including:

- Code audits and formal verification of smart contracts;
- Insurance or backstop funds governed by DAOs;
- Time-locked governance mechanisms that reduce unilateral upgrade risk;
- Delegate disclosure standards and community-based governance thresholds.

These mechanisms, while non-traditional, could form the basis of a risk-based compliance framework. The regime should consider tiered regulatory engagement based on:

- The extent of on-chain transparency and user agency;
- Whether the protocol exercises custody or discretion over user assets;
- Whether services target retail users or operate in a purely peer-to-peer model.

In addition, industry participants are increasingly developing and deploying advanced tools to enhance transparency, detect abusive practices, and mitigate risks to retail users in DeFi environments. These include:

- Automated risk scoring of protocols and liquidity pools, using metrics such as total value locked, audit history, upgradeability controls, and liquidity health;
- Smart contract monitoring systems capable of detecting malicious code patterns, rug pulls, governance exploits, and exploitative fee structures both at deployment and during ongoing operation;
- On-chain analytics linked to off-chain AML/CFT systems, enabling improved detection of illicit actors engaging with DeFi services;
- Transaction pattern monitoring to identify harmful behaviours such as sandwich attacks and MEV extraction;
- Consumer-facing risk scoring tools that provide retail users with actionable information about token and protocol risks prior to engagement;
- Ecosystem-wide monitoring platforms used by institutional participants to map and assess the risks associated with key actors (validators, liquidity providers, bridges, or on/off-ramp services).

We encourage the FCA to take account of these rapidly evolving industry practices when developing guidance and supervisory expectations. Recognising and encouraging such innovations will help promote a risk-based, technology-neutral regulatory approach, and may provide useful building blocks for a proportionate DeFi framework.

Guidance, Sandboxes, and Safe Harbours

The proposal to engage DeFi through non-binding guidance is appropriate at this stage, but it should be complemented by a regulatory sandbox or "DeFi Engagement Pathway" to:

- Enable responsible innovation under oversight;
- Test how existing conduct rules map onto DeFi operations;
- Encourage open-source, auditable, and transparent practices;
- Identify novel institutional forms (e.g., DAO wrappers, protocol councils) that may benefit from bespoke legal accommodation.

This would mirror similar initiatives such as:

- Project Guardian (Singapore), supporting tokenised assets and DeFi pilots under MAS supervision;
- US CFTC guidance targeting control points (front-ends, UIs) in enforcement;
- The EU MiCA approach, which excludes "fully decentralised" protocols but offers limited clarity on that threshold.

Recommendations

- **Clarify control-based attribution**: Define "responsible persons" by reference to governance rights, operational discretion, and economic influence.
- **Support guidance and sandboxes**: Prioritise exploratory pathways that foster engagement and regulatory literacy among builders and decentralised communities.
- **Recognise self-regulatory innovations**: Encourage adoption of disclosure norms, protocol-level insurance, and open governance tools that promote market integrity.
- **Promote proportionality**: Avoid imposing full firm-like obligations on developers or DAOs absent clear indicators of discretion and user harm.

Finally, we emphasise that the eventual FCA position on DeFi will materially impact the interpretation and feasibility of obligations discussed in Chapters 4, 5, and 6 of this DP. Without clarity on what constitutes a DeFi service and who is responsible for it, applying obligations on lending, borrowing, staking, and credit will be fraught with difficulty. Addressing these questions coherently is critical to the overall success of the future regime.

Chapter 8 – Conclusion/strategic questions

Q52. Do you agree with our assessment of the type of costs (both direct and indirect) and benefits from our proposals? Are there other types of costs and benefits we should consider?

One of the most significant opportunities lies in developing a differentiated regulatory treatment for decentralised systems. The UK has the chance to provide much-needed legal clarity by distinguishing between non-custodial, protocol-level infrastructure—where no single party controls operations—and custodial service providers who hold user assets and exercise discretionary control. Rather than imposing uniform compliance obligations on both categories, a tiered framework could be introduced. This would allow for appropriate oversight of custodial entities while supporting open-source innovation and permissionless financial infrastructure. Such an approach would not only mitigate regulatory overreach but also serve as a strong signal to the global developer community that the UK values decentralisation and understands the operational distinctions that underpin it.

The current proposals risk conflating technological neutrality with regulatory uniformity—treating fundamentally different architectures as if they pose equivalent risks. This one-size-fits-all approach not only suppresses alternative models of financial coordination but also weakens the systemic benefits of DeFi, such as enhanced transparency, algorithmic enforcement, and reduced reliance on discretionary intermediaries. Rather than levelling the playing field, identical rules for dissimilar entities would entrench incumbents and create barriers for innovation.

If recalibrated, the UK's approach could attract top-tier talent, foster open development communities, and cultivate a vibrant domestic ecosystem around decentralised finance, digital identity, tokenised infrastructure, and more. In the long term, such an ecosystem could produce not just commercial gains but also strategic advantages—enhancing financial inclusion, improving data integrity, and creating globally competitive digital public goods.

The current assessment underrepresents the full scope of potential negative impacts—particularly those that affect innovation, market competitiveness, and the long-term viability of the UK's role in the global crypto economy.

A key omission in the analysis is the cost of regulatory misalignment: when rules developed for traditional financial intermediaries are applied without adaptation to crypto-native or decentralized architectures. These mismatches generate compliance burdens that serve little consumer protection purpose while significantly impairing operational efficiency. For instance, applying affordability or creditworthiness assessments to overcollateralised, non-custodial lending protocols does not address any actual credit risk—but does impose overheads that may force smaller, innovation-driven teams out of the UK market or into centralized business models. This undermines the stated policy goals of encouraging competition and enhancing consumer choice.

The FCA should also explicitly distinguish between risks arising from centralised custodial misconduct and those inherent to decentralised, permissionless systems. Many of the most prominent failures referenced in previous chapters—such as misused client assets, opaque leverage, and manipulated yield schemes—stemmed from centralized entities with discretionary control over customer funds.

The risk of regulatory overreach carries a significant jurisdictional cost. If the UK's approach is perceived as overly complex, or hostile to technological differentiation, it will incentivize market participants to relocate operations or limit availability. This would result in loss of talent, capital, and innovation, while paradoxically weakening consumer protection by pushing usage of unregulated offshore platforms.