FCA CP 26/13 | GBBC Response

About Global Blockchain Business Council (GBBC)

GBBC is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

GBBC furthers adoption of digital 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 Chains, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

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

FCA CP26/13 — Cryptoasset Perimeter Guidance

1. Executive summary

GBBC welcomes the FCA's objective of providing clear perimeter guidance for the new UK cryptoasset regime. The final guidance will be critical for firms preparing for the authorisation gateway, and for making sure the regime catches the financial services activities Treasury intended without sweeping in software, infrastructure, and protocol-level services that do not constitute financial intermediation.

In our response, we set out some overarching themes and then address the individual questions.

GBBC's principal concern with PERG 19 is the lack of clarity on the treatment of technical service providers, and in particular the risk that the guidance inadvertently brings technical service providers within the regulated perimeter. This concern is cross-cutting: it bears, in different ways, on each of the consultation questions. We have, for ease, set out in the Annex the detail on how the challenge of inadvertently bringing technical service providers into the perimeter affects each consultation question.

A main overarching concern regarding PERG 19 is that the proposed guidance leans on concepts — "added value", "part of the facilities", existing arranging case law from traditional securities markets — that pull in too much when applied straight to cryptoassets. Wallets, APIs, dashboards, validators, routing tools, non-custodial interfaces, and DeFi front ends may be useful to a user, and may sit inside the user journey, without exercising the kind of functional agency that should trigger regulated arranging, dealing, safeguarding, or staking intermediation.

GBBC's central proposal is that PERG 19 should be built around one clear distinction:

- *functional agency* - a person controls, influences, intermediates, arranges, or brings about a specific transaction or staking arrangement; and
- *technical enablement* - a person provides software, data, connectivity, infrastructure, or public on-chain information, but does not control assets, execution, counterparties, transaction terms, or customer decisions.

Theme 1: Arranging should require functional agency, not technical usefulness

The proposed guidance risks treating a service as arranging because it provides "part of the facilities" for a transaction, or because it adds value. That bar is too low for cryptoassets, because almost any software layer adds value in some sense: a wallet makes a transaction easier to construct; a dashboard makes it easier to understand.

GBBC's proposal is that arranging requires more. The indicators we would point to are familiar:

- controls client assets or private keys;

- exercises discretion over execution or routing;
- selects counterparties;
- determines or negotiates transaction terms;
- operates an order book, matching system, or execution system with administrative override capabilities (distinct from a DEX);
- pools or manages client assets;
- receives transaction-linked remuneration for bringing about specific transactions;
- holds itself out as arranging, brokering, or intermediating transactions.

And the things that should not, without sufficient reason, be enough:

- provides software or a user interface;
- displays public on-chain data;
- enables a user to construct or sign a transaction;
- provides non-discretionary connectivity to a protocol;
- runs nodes, validators, APIs, RPC, infrastructure;
- improves usability, security, or operational efficiency;
- charges a subscription, licence, or SaaS / infrastructure fee;
- is one technical component in a wider journey.

Theme 2: "Added value" should not be a perimeter trigger

Existing PERG already uses "added value", but in a narrow sense. It is relevant to whether someone is doing more than mere communication. Doing more than mere communication is not the same as arranging. There is a separate question, which is whether the person's involvement is sufficiently important to bring about the transaction.

CP26/13 reads as if "added value" has been promoted into a free-standing positive indicator of arranging. In crypto markets that catches almost everything. Software, UX, data presentation, routing, security, infrastructure provision — all of them add value. The right question is whether the provider adds transaction-specific intermediation, not whether the service is useful.

This matters most for staking dashboards, wallet interfaces, DeFi front ends, analytics providers, and non-custodial software tools.

Theme 3: Absence of a technical-services exclusion does not mean technical services are in scope

Treasury did not include a general technical-services exclusion for dealing and arranging, so the FCA can't create one through guidance. But the absence of an exclusion is not a positive indicator that technical services are inside the perimeter. The prior question is whether the person is carrying on the elements of the regulated activity in the first place. If they aren't, no exclusion is needed.

PERG 19 must be clear on exemptions: services that do not constitute arranging at all, versus services that do constitute arranging but might rely on an exclusion.

Theme 4: Staking is not inherently arranging

GBBC is particularly concerned by any framing of staking as, "at its heart", an arranging activity. We do not agree with this positioning.

In most proof-of-stake (PoS) networks, validation is a protocol function — not a customer transaction arranged between parties. The right question is whether the provider arranges a customer's participation in staking, by exercising control, discretion, pooling, validator selection, reward management, or other customer-facing intermediation.

Technical staking services include: validator node operation, node infrastructure, solo-staking tools, public validator performance dashboards, reward calculators built on public data, and non-custodial tools where the user keeps control.

Intermediated staking services include: custodial staking, pooled staking, provider-led validator selection, provider management of the staking lifecycle, reward distribution on behalf of customers, and liquid staking models where the provider structures customer exposure.

Theme 5: Tokenisation guidance should avoid double regulation

The FCA has substantial work in hand on DLT and tokenisation. The sequencing concern that arises from setting the perimeter before that wider work is complete is addressed separately under Theme 7 below; the concern in this theme is narrower and substantive, and is directed at avoiding double regulation where DLT is used only as a record of an existing specified investment. Use of DLT should not, by itself, generate a separate cryptoasset safeguarding, dealing, or arranging permission requirement. Tokenised securities, deposits, and fund units are in a variety of cases already captured by regulation. Where DLT is used only as a record, register, settlement, or dematerialisation layer for an existing specified investment, the regulatory analysis should remain inside the existing RAO framework for that investment.

Theme 6: The DeFi problem is about what follows from perimeter capture

The DeFi question is not only whether a wallet, interface, or protocol access tool is in scope. It is also what follows if it is.

If a non-custodial DeFi interface gets treated as arranging, the firm becomes subject to rules designed for firms that can control listings, execution, order handling, asset availability, and venue access. That

assumption may not hold for someone providing access to a decentralised protocol whose parameters they do not select or control. The practical outcome is either a de facto restriction on UK DeFi access or pressure to centralise. Neither is in our view the policy intention.

This is a compatibility issue, not just a definitional one.

Theme 7: PERG 19 should not pre-empt the DeFi consultation or the authorisation gateway

PERG 19 has been consulted on while the FCA's wider industry engagement on DeFi is still underway, with DeFi-specific guidance, as we understand it, not expected to be consulted on until later in 2026. The conceptual work on how automation, control and discretion should be understood in decentralised contexts has not yet been completed with industry. As drafted, PERG 19 nonetheless takes legal positions on what is inside and outside the perimeter ahead of that work.

This creates a sequencing and authorisation problem. On the current draft, a number of firms that did not expect to be in scope — interfaces, non-custodial wallet providers, and similar models that were expected to be part of the DeFi engagement — may need to seek authorisation on the basis of PERG 19, yet will not have clarity until the DeFi guidance is finalised. Against the authorisation window, that risks firms being unable to be authorised in accordance with the FCA's timelines. We ask the FCA to provide flexibility for firms whose perimeter status turns on questions reserved to the forthcoming DeFi work, so that they are not prejudiced by the timing of these two workstreams.

2. Response to the FCA consultation questions

In the responses that follow we set out, for each question, the direction in which we would encourage the FCA to take the guidance and the factors we would encourage it to take into account. Where we refer to particular paragraphs of PERG, we do so to indicate where a point is most relevant, not to propose specific Handbook text. We recognise that any specific drafting would require a fuller legal review to ensure it operates correctly across the relevant provisions, and we would welcome the opportunity to engage with the FCA on that.

Question 1: Do you agree with our proposed guidance set out in the Introduction section?

GBBC supports the FCA's objective of providing practical perimeter guidance to help firms determine whether they require authorisation under the new cryptoasset regime. Clear guidance is essential to support responsible market development, consumer protection, market integrity, and effective preparation for the authorisation gateway.

We recommend that the Introduction section explain more clearly how existing FSMA and RAO concepts should be applied to cryptoasset market structures. The new regime applies familiar financial

services concepts to a market architecture that includes self-custody, non-custodial wallets, decentralised protocols, APIs, validators, dashboards, smart contracts, and public on-chain data. These features do not always map neatly onto traditional models of brokerage, custody, arranging, or venue operation.

The Introduction should therefore include a clear interpretive principle: the provision of software, data, connectivity, or infrastructure should not, in itself, be treated as regulated financial intermediation. The guidance should focus on whether the person has functional agency.

By "functional agency", we mean a role through which a person materially controls, intermediates, or brings about a specific cryptoasset transaction or staking arrangement. Relevant factors include control of client assets, discretion over execution, counterparty selection, transaction-term influence, matching, pooling, reward management, and transaction-linked remuneration. Making that point in the Introduction would help firms understand that the perimeter is focused on financial services activity, not generic technology provision.

Recommendations

- Add a clear intermediation-versus-technical-enablement principle to PERG 19. The Introduction should state that software, data, connectivity, APIs, dashboards, and other technical infrastructure do not amount to regulated activity unless the provider performs the elements of the relevant regulated activity.
- Clarify that existing RAO concepts require crypto-specific application. Existing principles on arranging, sufficient importance, mere communication, and by-way-of-business analysis remain relevant, but should be applied in a way that reflects cryptoasset market structures.
- Clarify that a commercial technology business is not necessarily carrying on a regulated activity by way of business. A provider may act by way of business in supplying software or infrastructure without carrying on the regulated activity of arranging, dealing, or safeguarding by way of business.

To give effect to these points, we would encourage the FCA to use the Introduction — for example the substance-focused guidance already at PERG 19.1.7 — to signal that the provision of software, data, connectivity, user interfaces, APIs, analytics, or other technical infrastructure should not, in itself, amount to carrying on a regulated cryptoasset activity, and that the assessment should turn on the

economic substance of the person's role. In making that assessment, we would encourage the FCA to take into account factors such as whether the person controls client assets, exercises discretion over execution, determines transaction terms, introduces or matches counterparties, operates a system through which trading interests interact, manages staking or reward distribution, or receives remuneration linked to specific transactions.

Question 2: Do you agree with our proposed guidance set out in the New specified investments section?

GBBC supports the FCA's effort to clarify the treatment of qualifying cryptoassets, qualifying stablecoins, specified investment cryptoassets, and relevant specified investment cryptoassets. Firms need clear guidance on how tokenised instruments interact with the existing specified investments perimeter.

We recommend further clarification to avoid accidental duplication between the existing RAO perimeter and the new cryptoasset perimeter. The key issue is whether the guidance could be read as implying that a tokenised specified investment, tokenised deposit, tokenised account, or DLT-based record is automatically a specified investment cryptoasset or relevant specified investment cryptoasset.

Our concern is not that tokenised specified investments should fall outside regulation. The concern is that the guidance may create duplicate or misallocated permissions where the legal and economic exposure remains to an existing specified investment, and the token or DLT entry functions only as a record of ownership, entitlement, or transfer. Where a DLT entry is solely a record of rights in an existing specified investment, the regulatory analysis should ordinarily remain under the existing RAO framework for that specified investment. The use of DLT as a register, custody record, or settlement layer should not automatically create a separate cryptoasset safeguarding, dealing, or arranging permission requirement.

Some of our members have highlighted a practical difficulty with this analysis. Where DLT is used as the official books and records for an instrument, the on-chain transfer of the asset carries the legal and economic rights with it — that is the purpose of using DLT as the record. In that situation it can be artificial to separate the "record" from the rights it moves. In our view this reinforces, rather than undermines, the conclusion above: the perimeter should follow the economic and legal substance of the activity, not the technology used to record it. Where the holder's exposure remains to an existing specified investment, and the use of DLT does not materially change the ownership structure or the way the asset is held or transferred, the activity should remain within the existing RAO framework and outside the cryptoasset perimeter — even where the analytical cases above are difficult to separate on the facts.

On this basis, a token that carries the same legal and economic rights as an existing specified investment — for example a tokenised gilt or bond — should continue to be analysed under the RAO rather than being drawn into this perimeter guidance. The same should hold where there is no off-chain equivalent: a security issued natively on-chain, with no off-chain "digital twin", is still a security and should still attract the protections of the RAO framework. We would caution against an approach that proceeds as though there are always two assets — an on-chain asset and an off-chain twin — each separately regulated. Tokenisation is not developing that way in practice, and guidance premised on the existence of a digital twin risks both unnecessary duplication and a mismatch with how the market actually operates. We recognise that safeguarding is the one area where the legislation itself routes custody of a relevant specified investment cryptoasset into the new article 9N activity by design; our point is directed at the dealing and arranging analysis and at not extending a separate cryptoasset permission requirement merely because DLT is used as a record.

By contrast, a synthetic token that tracks the price of an off-chain instrument (for example, the price of an off-chain equity) without conferring the same legal and economic rights as that instrument is appropriately addressed within this perimeter guidance, precisely because it does not give the holder the underlying rights of a traditional security. Distinguishing these cases would help firms understand where the cryptoasset perimeter is intended to bite and where the existing RAO analysis continues to govern.

We also recognise that recording or issuing a specified investment on DLT can introduce cybersecurity and operational risks that do not arise for the same instrument held off-chain. We acknowledge that there is utility in narrowly-defined additional requirements to address those DLT-specific risks. We would encourage the FCA to scope any such requirements proportionately to specified investment cryptoassets and relevant specified investment cryptoassets that are already within the RAO, and to align them with its wider work on DLT and the forthcoming wholesale tokenisation work, rather than treating the use of DLT as, in itself, giving rise to a new regulated cryptoasset activity.

Points for clarification

The final guidance should distinguish between:

- a token or DLT entry that is *solely a record* — for example, a DLT-based register entry evidencing ownership of a share, bond, fund unit, deposit, or account balance, where the legal rights remain in the underlying instrument;
- a token that itself *confers or constitutes the relevant rights* — for example, a transferable cryptoasset that independently embodies rights, can be traded or pledged separately, or is itself the asset held for the client;

- *safeguarding the underlying specified investment* — where an existing custodian or registrar uses DLT as part of its record-keeping or settlement infrastructure; and
- *safeguarding a relevant specified investment cryptoasset* — where the cryptoasset itself is the client asset being held or controlled.

Recommendations

- Clarify the "solely a record" concept through examples covering tokenised securities, tokenised fund units, tokenised deposits, tokenised accounts, and DLT-based internal registers.
- Avoid automatic SIC/R-SIC treatment. The guidance should avoid language suggesting that any use of a cryptoasset wrapper or DLT record automatically creates a specified investment cryptoasset or relevant specified investment cryptoasset.
- Clarify the custody and safeguarding boundary. The FCA should state when existing permissions for custody or administration of specified investments remain sufficient, and when a separate cryptoasset safeguarding permission is required.
- Prevent double regulation where DLT is only a record layer. Where the token has no independent economic or legal role beyond recording the underlying specified investment, cryptoasset permissions should not be required solely because DLT is used.
- Keep equivalent-rights and native on-chain securities under the RAO. A token carrying the same legal and economic rights as an existing specified investment, and a security issued natively on-chain with no off-chain equivalent, should be analysed under the existing RAO framework and not drawn into the cryptoasset perimeter solely because DLT is used. Synthetic tokens that track an off-chain price without conferring the same rights are, by contrast, appropriately within this guidance.
- Address DLT-specific risks through aligned, narrowly-scoped requirements. Any additional requirements for the cybersecurity and operational risks specific to recording or issuing a specified investment on DLT should be proportionately scoped and aligned with the FCA's wider DLT and

wholesale tokenisation work, rather than treated as a new regulated activity triggered by the use of DLT.

We would encourage the FCA, in its guidance on what is "solely a record" (PERG 19.4.4) and on specified investment cryptoassets (PERG 19.4.6), to make clear that a DLT-based record of ownership or entitlement in an existing specified investment will not necessarily constitute a specified investment cryptoasset or relevant specified investment cryptoasset. We would encourage the analysis to focus on whether the cryptoasset itself constitutes or confers the relevant rights, and whether it can be transferred, traded, pledged, or used independently of the underlying specified investment; and, where the token or DLT entry is solely a record of rights in an existing specified investment, to direct firms to the existing RAO activities applicable to that specified investment.

Question 3: Do you agree with our proposed guidance set out in the New regulated cryptoasset activities section?

GBBC broadly supports the FCA's objective of explaining the new regulated cryptoasset activities. We have material comments in relation to safeguarding and arranging safeguarding; operating a qualifying cryptoasset trading platform; dealing and arranging in qualifying cryptoassets; cryptoasset lending and borrowing; arranging qualifying cryptoasset staking; and DeFi and non-custodial access. The common issue across these activities is that the perimeter set by the guidance can be read as capturing technical services, infrastructure, and non-custodial tools that do not involve functional agency.

3A. Safeguarding and arranging safeguarding

GBBC supports clear guidance on safeguarding where a firm controls client cryptoassets or private keys. The guidance should clarify that safeguarding requires meaningful control over cryptoassets on behalf of another person. It should not capture firms that merely provide software, interfaces, analytics, or technical tools that allow users to self-custody, provided the provider does not hold, control, transfer, or exercise discretion over client cryptoassets or private keys.

Recommendations

- Clarify the control threshold. The FCA should provide examples distinguishing custodial wallets, MPC and key-share models, recovery services, non-custodial wallet software, hardware wallets, and analytics tools.
- Clarify arranging safeguarding. Merely providing a link, integration, or software interface to a third-party custodian should not automatically

amount to arranging safeguarding unless the provider plays a substantive role in bringing about the safeguarding relationship.

- Clarify the treatment of tokenised specified investments. Where DLT is used as a custody record for existing specified investments, the guidance should clarify when existing custody permissions apply and when cryptoasset safeguarding permissions are required.

3B. Operating a qualifying cryptoasset trading platform

GBBC is broadly aligned with the FCA on the trading platform guidance. The final guidance should nevertheless ensure that trading platform operation is not indirectly extended to non-custodial interfaces, protocol access layers, analytics tools, or software that does not organise trading interests, match orders, determine execution rules, or operate a market.

Recommendations

- Clarify the boundary between platform operation and protocol access. A person should not be treated as operating a qualifying cryptoasset trading platform merely because its software allows users to view, access, or interact with a decentralised protocol.
- Focus on control over trading interests. Relevant indicators of platform operation should include control over admission, matching, execution rules, settlement processes, and the interaction of trading interests.
- Add DeFi interface examples. The FCA should distinguish between operating a trading venue and providing an interface to a third-party or decentralised protocol.

3C. Dealing and arranging in qualifying cryptoassets

This is a principal area of concern for us and industry. Not simply that arranging is broad but also a deeper issue is that the guidance risks using the wrong proxies for regulated activity in cryptoasset markets.

Concepts such as “part of the facilities”, “sufficient importance”, and “added value” may be appropriate if carefully applied. Applied too generally, they risk capturing firms whose role is technical rather than intermediation-based. In cryptoasset markets, many services form part of the user journey. A wallet, interface, API, dashboard, RPC provider, routing tool, or analytics service may be necessary or useful in practical terms. Practical usefulness is not the same as arranging a transaction.

We recommend that the FCA clarify that arranging requires functional agency, not merely technical enablement.

The circularity issue

GBBC recognises that arranging is a broad concept in the existing RAO framework, and that existing case law is a useful starting point. It should nevertheless be treated with caution, and the FCA should avoid treating case law as determinative for the new cryptoasset arranging activity, given the substantial differences between cryptoasset markets and the traditional securities markets in which that case law developed. Cryptoasset arranging has been created as a separate activity because cryptoasset market structures differ from traditional intermediated securities markets. If PERG 19 imports the broadest concepts from arranging case law developed for traditional financial markets without crypto-specific calibration, the guidance may itself become the basis on which future courts treat software and infrastructure providers as arrangers. This risks a circular result: the guidance is broad because existing arranging case law is broad; future courts may then treat the FCA's broad crypto guidance as persuasive; and the breadth of the perimeter becomes self-reinforcing, rather than grounded in the economic substance of cryptoasset intermediation. PERG 19 should therefore state expressly that existing arranging concepts should be applied in a crypto-specific manner.

The "added value" issue

We are particularly concerned that "added value" may be treated as a positive indicator of arranging. In cryptoasset markets, almost every technical service adds value: a wallet improves usability, a dashboard improves legibility, a validator performance display improves decision-making, an API improves connectivity, a routing tool improves access, and a security tool reduces operational risk. None of these should be enough to bring the provider within the arranging perimeter. The relevant question should be whether the provider adds transaction-specific intermediation, not whether the service is useful.

Proposed indicators of arranging

A person is more likely to be arranging where it:

- introduces or selects counterparties;
- operates a matching mechanism or order book;
- determines or negotiates transaction terms;
- exercises discretion over routing or execution;
- controls client assets or private keys;
- receives transaction-specific remuneration for bringing about transactions;

- presents itself as arranging or brokering transactions; or
- plays a role without which the transaction, as a transaction between identified trading interests, would not be effected.

Proposed negative indicators

A person should not generally be treated as arranging merely because it:

- provides software or a user interface;
- displays publicly available on-chain data;
- enables a user to construct or sign a transaction;
- provides non-discretionary connectivity to a protocol;
- provides node, validator, API, RPC, or infrastructure services;
- improves usability, security, or operational efficiency;
- charges a subscription, licence, SaaS, or infrastructure fee; or
- is one technical component in a wider user journey.

Recommendations

- Introduce a functional agency framework. The guidance should focus on whether the provider materially controls, intermediates, or brings about a specific transaction.
- Clarify that "added value" is not sufficient. The FCA should state that improving user experience, security, analytics, display, or connectivity does not itself amount to arranging.
- Clarify "part of the facilities". The guidance should distinguish between services that are technically part of a user journey and services that are sufficiently important to the transaction as a regulated transaction.
- Clarify that absence of a technical services exclusion does not imply inclusion. Technical services that do not meet the elements of arranging should be outside scope without needing an exclusion.
- Add examples for wallets, DeFi interfaces, APIs, dashboards, and routing tools. The final guidance should provide practical examples that firms can apply.

- Distinguish the technical-service-provider role without treating it as the only route out of scope. If a technical-service-provider exemption is introduced, the FCA should confirm that the negative indicators falling within it are out of scope on that basis, and that the indicators sitting outside a strict technical-service-provider role are nonetheless outside arranging where there is no functional agency.

These negative indicators also relate closely to the technical-service-provider exemption that GBBC and others have asked HM Treasury to introduce, which would make the FCA's task considerably easier if granted. We would encourage the FCA to draw this distinction in PERG 19. Many of the negative indicators — in particular the provision of software, and the operation of nodes, validators, APIs, RPC or other infrastructure — map directly onto a technical-service-provider role and would fall squarely within such an exemption if it is introduced. Others, such as providing a user interface or displaying public on-chain data, are broader than a strict technical-service-provider role, but should equally not amount to arranging absent functional agency. Importantly, if a technical-service-provider exemption is introduced, the FCA should not treat everything outside that exemption as automatically within the perimeter: the prior question remains whether the person performs the elements of arranging at all.

We would encourage the FCA, in its guidance on arranging deals in qualifying cryptoassets (PERG 19.8.3, including the treatment of software and connectivity at PERG 19.8.3(6) to (9), and the related "added value" language in the mere-communication exclusion at PERG 19.8.19), to make clear that the provision of software, interfaces, APIs, data, analytics, routing tools, or other technical infrastructure should not, in itself, amount to arranging deals in qualifying cryptoassets. In assessing whether a person is arranging, we would encourage the FCA to take into account whether the person controls client assets, exercises discretion over execution, introduces or matches counterparties, determines or negotiates transaction terms, operates a system through which trading interests interact, or receives remuneration linked to specific transactions, and to confirm that improving usability, security, access, or operational efficiency does not, by itself, make a provider an arranger.

3D. Cryptoasset lending and borrowing

GBBC agrees that cryptoasset lending and borrowing may engage regulated activities depending on the structure. The guidance, however, must not treat all lending and borrowing related software, collateral tools, protocol interfaces, dashboards, or risk analytics as regulated intermediation. The analysis should focus on whether the provider offers, arranges, manages, or intermediates a lending or borrowing product, rather than whether it provides tools that users may deploy in relation to lending or borrowing.

Recommendations

- Differentiate product providers from technology providers. The guidance should distinguish a firm offering or arranging a lending product from a firm providing user-operated software or analytics.
- Clarify DeFi lending access. The FCA should explain which factors determine whether any identifiable person is carrying on a regulated activity by way of business where users interact with decentralised lending protocols.
- Clarify the treatment of collateral tools. Tools that display collateral ratios, liquidation risk, or market data should not automatically be treated as arranging lending or borrowing.

3E. Arranging qualifying cryptoasset staking

GBBC welcomes the FCA's recognition that purely technical staking services may fall outside scope. The final guidance should more clearly operationalise that distinction. We do not agree that staking should be framed as "at its heart" an arranging activity. That framing risks treating intermediation as the default and technical service provision as the exception.

In many proof-of-stake networks, validation is a protocol-level activity. A validator, node operator, or solo-staking tool provider may contribute to network operation without arranging a customer's participation in staking. The relevant question should be whether the provider exercises functional agency over the customer's staking activity. Relevant factors include whether the provider:

- takes custody or control of customer assets;
- pools assets;
- selects validators on behalf of customers;
- determines staking terms;
- manages reward distribution;
- exercises discretion over whether, when, or how assets are staked; or
- markets itself as providing a customer-facing staking product.

On public data and dashboards, the guidance should expressly state that displaying public on-chain data does not amount to arranging staking merely because it improves usability. Validator performance, rewards history, slashing history, network participation data, and estimated rewards may all be derived from public sources. Repackaging this information into a dashboard should not, in itself, be treated as "further involvement" sufficient to bring the provider within scope. If such dashboards were treated as arranging because they help users make decisions, then almost any

analytics, explorer, interface, or data visualisation tool could be captured. That cannot be the intended result.

Recommendations

- Remove or qualify any suggestion that staking is inherently arranging. The guidance should focus on the provider's actual role.
- Separate technical staking from intermediated staking. The FCA should distinguish validator operation, node infrastructure, solo-staking tools, and public-data dashboards from custodial, pooled, or provider-managed staking.
- Clarify that "added value" does not defeat the technical services analysis. A technical service can be useful and commercially valuable without becoming arranging.
- Add detailed staking examples covering validator node operators; infrastructure providers; solo-staking software providers; dashboard providers; non-custodial staking interfaces; custodial staking providers; pooled staking providers; liquid staking interfaces; and providers selecting validators on behalf of customers.

We would encourage the FCA, in its guidance on arranging qualifying cryptoasset staking and the technical-service exclusion (PERG 19.10.1 to PERG 19.10.3), to make clear that the provision of technical staking infrastructure, validator operation, solo-staking tools, dashboards, analytics, reward calculators, or other information services based on public on-chain data should not, in itself, amount to arranging qualifying cryptoasset staking. We would encourage the FCA to treat as relevant to arranging factors such as custody or control of customer assets, pooling, discretion over validator selection, management of the staking lifecycle, determination of customer terms, or distribution of rewards on behalf of customers.

3F. DeFi and non-custodial access

We recommend that the FCA clarify how the perimeter applies to DeFi interfaces, non-custodial access tools, and protocol integrations.

The perimeter question cannot be separated from the rule consequences that follow authorisation. If a non-custodial DeFi interface or protocol access tool is treated as arranging, the provider may become subject to rules designed for firms that can control asset availability, listings, execution, order handling, and venue access. That assumption may not hold where the firm provides access to a decentralised protocol whose assets, pools, liquidity, counterparties, or execution logic are not

selected or controlled by the interface provider. The result could be practical incompatibility for DeFi access, or de facto centralisation, even where the policy intention is to regulate identifiable intermediaries rather than decentralised infrastructure.

Recommendations

- Clarify when DeFi access is not arranging. The FCA should provide examples where a person merely provides technical access to a decentralised protocol and does not control assets, execution, admission, matching, or transaction terms.
- Clarify the role of control. The guidance should explain how the FCA will assess whether a person controls or operates a protocol, interface, or transaction flow.
- Clarify the interaction with future conduct rules. The FCA should consider whether treating protocol access tools as arranging would impose obligations that assume control the provider does not have.
- Avoid de facto centralisation. PERG 19 should not create incentives for firms to centralise custody, listings, routing, or protocol access merely to make the perimeter analysis more manageable.

As set out under Theme 7 above, this question also raises a sequencing concern. PERG 19 takes positions on whether DeFi interfaces, non-custodial access tools and protocol integrations are inside or outside the perimeter ahead of the FCA's dedicated DeFi guidance, which we understand is not expected to be consulted on until later in 2026 and which is intended to develop the very concepts — automation, control and discretion in decentralised settings — on which these perimeter outcomes depend.

The practical consequence is that firms which did not expect to be in scope — including interface and non-custodial wallet providers that were expected to engage through the DeFi workstream — may need to seek authorisation on the basis of PERG 19 without the clarity that the DeFi guidance is intended to provide, and against a fixed authorisation window. We ask the FCA to build in flexibility for firms whose perimeter status turns on questions reserved to the forthcoming DeFi work, so that they are not disadvantaged by the timing of these two workstreams.

We also note that the presence of a controlling entity demonstrates commerciality, but does not by itself determine whether a regulated activity is being carried on. What matters is the substance of the commercial function and the outcomes it drives. Where an activity does produce outcomes akin to a regulated activity, or presents comparable financial-services risks, GBBC supports a constructive conversation about how to regulate it, including through bespoke frameworks where appropriate. Our

concern is not to keep identifiable intermediaries out of regulation, but to ensure the perimeter is drawn on substance and follows the policy work rather than pre-empting it.

Question 4: Do you agree with our proposed guidance set out in the Exclusions relevant to the activities section?

GBBC supports the inclusion of guidance on exclusions. The exclusions section should more clearly distinguish between activities that are outside scope because they do not meet the elements of a regulated activity, and activities that meet those elements but may fall within a statutory exclusion. This distinction is particularly important for technical services.

We recognise that Treasury did not include a general technical services exclusion in the revised SI. In the meantime, absence of such an exclusion should not be read as a positive indication that technical services are within scope. Where a technical service does not involve arranging, dealing, safeguarding, or operating a platform in substance, the provider should not need to rely on an exclusion.

Recommendations

- The guidance should state clearly that technical services may be outside scope because the elements of the regulated activity are not met.
- Clarify the goods and services exclusion for software and infrastructure. The FCA should provide examples of when software, analytics, APIs, data tools, hardware wallets, dashboards, or infrastructure provision may be treated as ordinary goods or services rather than regulated activity.
- Clarify that technical services can be commercial. A service should not fall outside technical service treatment merely because it is provided commercially or improves user experience.
- Clarify the distinction between general utility and transaction-specific significance. A service may be generally useful to a user without being sufficiently important to bringing about a specific transaction.
- Recast the "added value" language in the technical-service exclusion. The FCA should make clear, in PERG 19.10.2, that commercial value or usefulness does not defeat the technical-service exclusion; what matters is whether the provider exercises functional agency over the customer's staking.

We would also flag a specific drafting point in the staking exclusion. The guidance indicates that where a service includes "added value" it is unlikely to be excluded as a pure technical service (PERG 19.10.2). Because, by definition, every commercial service adds some value, this framing risks collapsing the technical-service exclusion into nothing. The test should turn on whether the provider performs the elements of the regulated activity — functional agency over the customer's staking — not on whether the service is commercially valuable or useful.

We would encourage the FCA, in its guidance on the effect of exclusions (PERG 19.11.1), to make clear that the fact a technical service improves usability, efficiency, security, or access does not, in itself, mean that the provider is carrying on a regulated cryptoasset activity, and that the assessment should focus on whether the provider performs the elements of the relevant activity in substance. In particular, we would encourage the FCA to recognise that, where a provider does not control assets, exercise discretion, determine transaction terms, introduce or match counterparties, operate a trading system, or receive remuneration for bringing about specific transactions, the service may fall outside the regulated activity without the need to rely on an exclusion.

Question 5: Do you agree with our proposed guidance set out in the Interaction with the current cryptoasset framework for Money Laundering Regulations (MLRs) section?

GBBC supports guidance explaining the interaction between the FSMA cryptoasset regime and the existing Money Laundering Regulations (MLR) framework. MLR registration and FSMA authorisation are separate regimes, and firms should not assume that registration under one determines their status under the other.

The final guidance should nevertheless explain how the FCA expects firms to approach cases where the same activity may be treated as technical infrastructure under existing AML analysis but potentially as regulated arranging under PERG 19. We do not suggest that the MLR and FSMA regimes should be identical: they have different statutory purposes. Where the FSMA perimeter is materially broader for the same underlying activity, however, the guidance should explain the basis for that divergence. Otherwise firms may face a confusing outcome in which a provider is treated as a software or infrastructure provider for AML purposes but as a financial services intermediary for FSMA purposes, without a transparent policy rationale.

Recommendations

- Provide a mapping of common business models comparing likely MLR and FSMA treatment for cryptoasset exchange providers; custodian wallet providers; non-custodial wallet providers; software developers; API providers; blockchain analytics providers; DeFi interfaces; validator infrastructure providers; and staking service providers.

- Clarify treatment of software providers. The guidance should explain whether and when a software provider with no custody, no transaction discretion, no counterparty introduction, and no control over client assets may remain outside both regimes.
- Explain any divergence. If the FCA considers that a firm outside MLR registration may nevertheless be carrying on regulated arranging under FSMA, the final guidance should explain why.
- Support authorisation planning. Firms moving from MLR registration to FSMA authorisation need practical guidance on which permissions may be required and which activities remain outside scope.
- Give examples of when only MLR registration is required. It is currently difficult for firms to tell, from the guidance, when an activity would require only MLR registration rather than FSMA authorisation, since the guidance largely directs firms to assess their own business models. The FCA should set out its view, with examples, of the kinds of cryptoasset business that fall within the MLR perimeter only and do not require authorisation under the Act.

We would encourage the FCA, in its guidance on the interaction with the Money Laundering Regulations (PERG 19.12, including PERG 19.12.9 and PERG 19.12.10), to make clear that firms should consider the FSMA and MLR regimes separately, and to take into account that, where a person provides only software, technical infrastructure, or data services and does not control client assets, execute transactions, arrange counterparties, or operate a trading system, this may be relevant to both the MLR and FSMA perimeter analysis. We would also encourage the FCA to confirm that the fact a person is not an MLR cryptoasset exchange provider or custodian wallet provider is not determinative, but may be relevant to understanding the substance of the activity.

Question 6: Do you agree with our proposed guidance set out in PERG 1, PERG 2 and PERG 8?

GBBC broadly supports the consequential amendments to PERG 1, PERG 2, and PERG 8. We recommend that the FCA strengthen the cross-references between PERG 19 and existing guidance on arranging, sufficient importance, mere communication, financial promotions, and by-way-of-business analysis. Otherwise, PERG 19 may be read in isolation, causing established limiting principles in PERG 2 and PERG 8 to be underweighted.

6A. PERG 2 — sufficient importance

PERG 19 should be expressly tethered to the principle that arranging requires involvement of sufficient importance to the transaction. In cryptoasset markets, many services may be technically useful or practically necessary from the user's perspective without being legally significant as arranging. A wallet interface, dashboard, API provider, RPC provider, or node operator may form part of the infrastructure through which a user acts. That does not mean the provider is arranging the transaction.

We recommend that the FCA clarify the difference between *transaction-specific significance*, where the person materially brings about or influences the transaction, and *general utility*, where the service is useful but does not involve functional agency.

We would encourage the FCA, where it addresses arrangements that do not bring about a deal (PERG 19.8.17), read with the "sufficient importance" guidance in PERG 2.7.7B, to make clear that, in determining whether a person is arranging deals in qualifying cryptoassets, the question is whether the person's involvement is sufficiently important to the transaction as a transaction. We would encourage the FCA to recognise that a service may be useful, convenient, or technically necessary in a general sense without amounting to arranging, where the provider does not control assets, exercise discretion, introduce counterparties, determine transaction terms, operate a matching system, or receive remuneration for bringing about specific transactions.

6B. PERG 8 — financial promotions and mere communication

We recommend that the FCA clarify the relationship between regulated arranging and the financial promotions regime. A person may communicate information that is relevant to a financial promotions analysis without arranging the underlying transaction. This distinction matters for cryptoasset websites, dashboards, analytics platforms, educational tools, market data providers, and interfaces that display information but do not control or intermediate transactions.

Recommendations

- Clarify perimeter-out / promotion-in examples. The FCA should provide examples where a person may need to consider the financial promotions regime but is not carrying on arranging.
- Clarify that mere communication is not arranging. Hosting, transmitting, displaying, or organising information should not normally amount to arranging unless accompanied by further involvement in bringing about the transaction.

- Clarify treatment of public on-chain data. Displaying public on-chain data, validator performance, market information, or protocol data should not, in itself, be treated as arranging.

We would encourage the FCA, in the mere-communication guidance (PERG 19.8.19), read with PERG 8.32, to make clear that a person who communicates information about qualifying cryptoassets, or provides a tool through which such information is displayed, may need to consider the financial promotions regime, but that such communication will not necessarily amount to arranging deals in qualifying cryptoassets. We would encourage the arranging analysis to focus on whether the person plays a substantive role in bringing about, or making arrangements with a view to, transactions.

6C. By way of business

We recommend that PERG 19 clarify that the by-way-of-business test applies to the regulated activity itself, not merely to the provider's broader business. A software provider may be acting commercially in supplying software, but that does not mean it is carrying on arranging by way of business. The relevant question is whether the firm is carrying on the regulated activity of arranging, dealing, safeguarding, or staking intermediation by way of business.

We would encourage the FCA, in the "by way of business" guidance (PERG 19.2, read with PERG 2.3), to make clear that the assessment requires firms to identify the relevant regulated activity with precision, and to recognise that the fact a person operates a commercial technology business does not mean it is carrying on a regulated cryptoasset activity by way of business unless it is carrying on the elements of that regulated activity.

4. Closing position

GBBC supports the FCA's aim of providing clear and practical perimeter guidance before the new UK cryptoasset regime comes into force. The final guidance should better distinguish regulated financial intermediation from technical enablement.

The key question should not be whether a service is useful, whether it forms part of the user journey, or whether it adds value. The key question should be whether the provider has functional agency: control, discretion, counterparty selection, transaction-term involvement, custody, pooling, reward management, or transaction-linked economic participation.

By adopting this framework, the FCA can preserve a robust perimeter for genuine cryptoasset intermediation while avoiding unintended capture of software, infrastructure, public data, non-custodial tools, and protocol-level activity. We recommend that the FCA refine PERG 19 through paragraph-specific clarifications, practical examples, and clearer functional tests. This would support

consumer protection, market integrity, effective competition, and the UK's objective of establishing a credible and proportionate cryptoasset regulatory regime.

Annex 1: Impact of the technical service provider perimeter issue, by consultation question

This Annex sets out, question by question, how the central concern identified in our response — the risk that PERG 19 inadvertently brings technical service providers within the regulated perimeter — bears on each of the consultation questions. It consolidates in one place the detail underlying the recommendations in the body of our response, so that the cross-cutting nature of the issue is visible without that single point overshadowing our wider comments on each question. The common safeguard across every question is the same: technical enablement should not be treated as regulated intermediation, and the assessment should turn on whether the provider has functional agency over a specific transaction or staking arrangement.

Question 1: Introduction

The Introduction sets the interpretive frame for the whole of PERG 19. If it does not state clearly that the provision of software, data, connectivity, APIs, dashboards, or infrastructure is not, in itself, regulated activity, technical service providers risk being read into the perimeter from the outset. That risk is greatest where the guidance treats "added value" or forming "part of the facilities" as sufficient, because almost every technical service adds value of some kind. We ask the FCA to anchor the Introduction in functional agency — control of client assets, discretion over execution, counterparty selection, transaction-term influence, matching, pooling, reward management, or transaction-linked remuneration — so that generic technology provision is not captured.

Question 2: New specified investments

Here the concern takes the form of double regulation. Where DLT is used only as a record, register, or settlement layer for an existing specified investment, the providers of that recording or infrastructure should not be drawn into a separate cryptoasset permission simply because DLT is involved. Treating the use of DLT as itself a trigger would capture record-keeping, registrar, and infrastructure functions that carry no functional agency over a transaction. The analysis should follow the economic and legal substance of the activity, not the technology used to record it.

Question 3: New regulated cryptoasset activities

This is where the perimeter bites hardest on technical service providers, across safeguarding, trading-platform operation, dealing and arranging, lending and borrowing, staking, and DeFi access. In each case the guidance can be read as capturing non-custodial wallets, interfaces, analytics, dashboards, validators, nodes, APIs, and protocol-access tools that do not hold or control client assets, exercise discretion, select counterparties, or determine transaction terms. The safeguard is constant: a provider should be in scope only where it performs the elements of the relevant regulated activity in substance, not merely because its software or infrastructure is useful or sits within the user journey.

Question 4: Exclusions relevant to the activities

The absence of a general technical-services exclusion should not be read as a positive indication that technical services are within scope. The prior question is whether the provider performs the elements of a regulated activity at all; if it does not, no exclusion is needed. The drafting risk is acute in the staking exclusion, where treating "added value" as defeating the technical-service exclusion would collapse the exclusion to nothing, because every commercial service adds value. The test should turn on functional agency, not commercial usefulness.

Question 5: Interaction with the Money Laundering Regulations

A technical service provider may be treated as software or infrastructure for AML purposes yet potentially as a regulated arranger under FSMA. Without a transparent rationale for any such divergence, firms face inconsistent characterisation of the same activity across the two regimes. We recommend the FCA to explain, with examples, when a provider that does not control client assets, execute transactions, arrange counterparties, or operate a trading system falls within the MLR perimeter only, or outside both regimes.

Question 6: PERG 1, PERG 2 and PERG 8

The limiting principles in PERG 2 and PERG 8 — sufficient importance, mere communication, and the by-way-of-business test — are the principal safeguards against capturing technical service providers, and PERG 19 should be expressly tethered to them. A technical service may be useful, or even practically necessary, to a user without being sufficiently important to a transaction as a transaction; communicating or displaying information is not arranging; and operating a commercial technology business is not carrying on a regulated activity by way of business unless the provider performs the elements of that activity.