Ava Labs.

1177 Avenue of the Americas, 5th Floor, Suite 50922
New York, NY 10036

July 2, 2026

Matthew Thomson-Ryder
Capital Markets Division
Financial Conduct Authority
12 Endeavour Square
London E20 1JN

Copied to the Bank of England

RE: Response to the Call for Input - *The future of tokenisation: a joint vision from the authorities for UK wholesale financial markets* (May 2026)

Dear Mr Thomson-Ryder,

Ava Labs and the Avalanche Policy Coalition commend the Financial Conduct Authority, the Bank of England and the Prudential Regulation Authority for their clear and forward-looking vision on tokenisation. We particularly welcome the technology-neutral, outcomes-based approach that runs through the Call for Input. We believe that the capabilities required for safe, well-regulated tokenised wholesale markets are achievable on public, permissionless infrastructure today, and the most valuable step the authorities can take is to confirm that accountability for regulated activities attaches to the firms performing those activities, not to the neutral infrastructure on which they run.

We would be pleased to discuss any aspect of this response, and to assist the authorities' further work in any way that is useful.

Yours sincerely,

Signed by:
Lee A. Schneider
EBA43E0DF74346A...

Lee A. Schneider
General Counsel
Ava Labs, Inc.
lee@avalabs.org

Introduction

Avalanche Policy Coalition welcomes the opportunity to respond to the joint Call for Input published by the Financial Conduct Authority ("FCA") and the Bank of England (the "Bank"), including the Prudential Regulation Authority (together, the "authorities"), on the future of tokenisation in UK wholesale financial markets (the "Call for Input").

We strongly support the authorities' ambition to enable the safe adoption of tokenisation while preserving the standards of market integrity, financial stability and investor protection on which the United Kingdom's reputation as a leading global financial centre rests. We particularly welcome the paper's commitment to technology neutrality, its outcomes-based approach to regulation, its recognition that traditional and tokenised infrastructures will coexist, and its explicit acknowledgement that public, permissionless networks can play a role in the issuance, transacting in and settlement of tokenised securities. This is a thoughtful and constructive vision, and one we are pleased to support.

Our response focuses on the questions most relevant to our perspective as a developer of blockchain software and related infrastructure - principally Questions 2, 3 and 5 - and offers more concise observations on the remaining questions.

About Ava Labs and Avalanche

Ava Labs is a technology company focused on blockchain and related technologies. Its first major software release was the open-source code for Avalanche blockchain, which resulted in the launch of the Avalanche primary network in September 2020 by a distributed group of independently operated validator nodes around the world. The primary network remains decentralised, public, and permissionless, with a proof-of-stake based consensus mechanism. As such, there is no issuer of, or central authority over, the protocol's native token, known as AVAX.[1] Ava Labs continues to contribute software and research to the primary network, which functions in accordance with its own protocol rules and the operations of that decentralised validator set.

Ava Labs is also the convenor of the Avalanche Policy Coalition ("APC"), a resource for policymakers, regulators and trade associations on blockchain and tokenisation. Several of the principles set out below draw on APC's published policy framework, including its "Tree of Web3 Wisdom" and its work on token classification and on the distinction between infrastructure and intermediation.[2]

---

[1] Technical white papers are available at https://www.avalabs.org/whitepapers and network statistics at https://stats.avax.network.

[2] Avalanche Policy Coalition, Tree of Web3 Wisdom, https://avalanchepolicy.com/en/tree/ (including the principle of "same asset/activity, same risks, same regulation" and the definition of decentralisation as a system with no single point of failure, no single source of truth, and no single authority with the power or obligation to change data or transactions); and Sensible Token Classification, https://avalanchepolicy.com/en/stc/.

Why Avalanche is well-suited to wholesale markets

The capabilities the authorities identify as prerequisites for tokenised wholesale markets are already achievable today on public, permissionless infrastructure like Avalanche:

- **Settlement finality.** Avalanche consensus delivers rapid, deterministic finality which is aligned with the auditable, reliable point of transaction commitment the Call for Input identifies as essential for regulated settlement.
- **Permissioning and privacy without sacrificing public-network benefits.** Avalanche's architecture allows institutions to deploy bespoke Layer 1 chains with their own validator sets, permitted-participant lists, compliance rulesets and privacy configurations, while remaining interoperable with the wider network. It demonstrates that decentralisation does not necessarily mean "permissionless and public at all times and in all forms". Networks can be designed to meet KYC, anti-money-laundering ("AML"), privacy and other regulatory or business outcomes while retaining the resilience and other benefits of a public network.
- **Interoperability and composability.** Native interoperability between Avalanche L1s, and with external networks, supports the authorities' concern to minimise liquidity fragmentation, and does so through open, market-led design rather than a single mandated network, consistent with the authorities' express wish to avoid "picking winners."
- **Operational resilience.** A decentralised validator set means there is no single point of failure, no single source of truth, and no single entity with the power or obligation to change data or transactions. On this technical definition of decentralisation, these are resilience features that support the authorities' operational-resilience principles, rather than risks to be regulated away.
- **Proven institutional adoption.** Tokenised fund and securities products from leading institutions including BlackRock, Franklin Templeton, Apollo and KKR are already deployed on Avalanche, providing real-world evidence that public-network tokenisation can meet the institutional-grade standards the Digital Securities Sandbox ("DSS") is designed to test.

The blockchain ecosystem has moved beyond a simple choice between public and private networks. Today, blockchain infrastructure can be configured in a range of ways to meet different regulatory, operational and business requirements. This situation heightens the need to be clear about the nature of the asset and the nature of the activity when determining what and who is regulated, because it maintains the technology neutral posture the authorities rightly value. We have submitted comment letters, both individually and jointly with others, to the FCA on these topics, including last month, in February, and last year.

The key point about the nature of the asset is that tokenisation allows for the digital representation of anything, not just financial instruments. Treating all assets alike simply because they are tokenised would be neither legally sound nor technology neutral.

The nature of the activity test looks at, among other things, whether a person is functioning as an intermediary or an infrastructure provider to determine their regulatory status. This distinction has been clearly made by the authorities in traditional markets and should therefore carry over into the regulations associated with tokenisation.

You will see these twin themes below throughout our responses to the questions in the Call for Input.

Responses to Questions

Question 1: Where do you see the most potential benefit from tokenisation, and the main opportunities for your business?

In our view, the most significant UK-specific opportunity is to position the United Kingdom as a jurisdiction that allows securities (indeed, all specified investments) to be tokenised, issued and settled on public, permissionless networks, not solely on private or permissioned ones. This would allow the UK to capture global liquidity, support the interoperability the paper rightly prioritises, and avoid the fragmentation that arises where activity is siloed across closed systems.

The benefits the authorities identify, such as a shared "golden source" ownership record; atomic and extended-hours settlement; automation through smart contracts; and the removal of duplicate ledgers and reconciliations, are realisable on public infrastructure of the kind described above. Moreover, the use of public infrastructure will lower costs and, thereby, barriers to entry, resulting in robust, competitive markets. As a developer and provider of such infrastructure, the opportunity we see is the UK expressly recognising public, permissionless networks as eligible infrastructure for issuance and settlement, building on the Call for Input's acknowledgement that securities outside the scope of the UK CSDR may already be recorded and settled using public blockchains.

Question 2: Do you agree with the vision and regulatory principles set out in the paper?

We agree with the vision and with the great majority of the regulatory principles. We welcome in particular the principle of technology neutrality, the commitment to outcomes-based rather than prescriptive requirements, and the recognition that public chains can meet market integrity, compliance and privacy outcomes. These are consistent with the principles, which APC has long advocated, that regulation should follow the nature of the asset and the activity such that the same risk results in the same regulatory outcome, regardless of the technology used.

We would note that the nature of the asset has always been important across many dimensions, including utilisation, valuation and classification for legal and regulatory purposes. Not every tokenised asset is, or should become, a specified investment by virtue of the technology. Tokenisation changes the form in which an asset is represented, recorded and transferred; it does not change the underlying nature of the asset itself. A tokenised concert ticket remains a ticket, and a tokenised interest in real estate remains an interest in real estate; neither becomes a specified investment or other form of financial instrument merely because it is represented on a blockchain. Classifying tokens by reference to the technology used to record them, rather than the nature of the underlying asset, would blur well-established legal categories and risk drawing within the perimeter assets that have no place there. We therefore encourage the authorities to recognise expressly, alongside the nature of the activity, a nature of the asset test, so that the regulatory treatment of a token follows from what the underlying asset is, and not from the fact that it has been tokenised.

As regards the nature of the activity, we broadly support the principle that, for each regulated activity, there should be a responsible, identifiable, regulated person. We agree this does not require every participant in the ecosystem to be a regulated person. This is a core point that deserves close attention because it goes to the heart of the activity test and the distinction between intermediaries, who are regulated, and infrastructure providers, who are not. Infrastructure providers exist across the spectrum from public, permissionless networks to private, permissioned networks, so it is important to make clear which activities constitute infrastructure so they can be applied in a technology neutral fashion.

These issues come to a head in the crucial open question the Call for Input raises at paragraph 3.3: who that responsible person "defaults to" where regulated activity appears to take place on a public, permissionless ledger or a decentralised exchange. This is one of the most important points for the authorities to resolve clearly, and we offer the following observations:

1. **Accountability should attach to the regulated activity,** not to the network, or its validators, developers, and other infrastructure providers. The responsible person should be the entity actually performing the regulated activity: the issuer, the digital securities depository ("DSD"), the intermediary, or the regulated firm making use of the chain. It should never default to be the underlying network, its validators or node operators, those who develop the protocol software, or providers of communications, APIs, block explorers or analytics providers, among others. Those participants provide a passive infrastructure layer: they enable systems rather than effecting transactions or custodying assets.

   In cases where regulated activity genuinely has no identifiable person undertaking it, accountability must default to the regulated firms relying on the infrastructure, just as is the case in traditional financial services activities. Reaching into the infrastructure layer to manufacture a responsible person where none exists would be inconsistent with analogous regulatory treatment, difficult to enforce, and likely to produce unintended consequences.

2. **The infrastructure-versus-intermediary distinction.** Ecosystem and network participants who provide and maintain the infrastructure that allows blockchain networks to function are not engaged in the activities of a financial intermediary and should fall outside the regulatory perimeter. These infrastructure activities include, but are not limited to: hardware, software and communications providers; validators, delegators and node operators; and providers of APIs and RPCs, block explorers and other data services. Such participants do not effect or execute transfers, control the movement of cryptoassets, or provide custody or control of those assets. They are, in effect, invisible and indiscriminate in verifying, recording and enabling transactions.

   The UK has not traditionally regulated technology infrastructure provision (building hardware, developing software, facilitating communications), even where this infrastructure is used in connection with the undertaking of regulated activities. Performing those activities in connection with a blockchain does not transform the providers into intermediaries. Firms that use the infrastructure to undertake regulated activities may, of course, themselves require authorisation, which is the right place for regulation to occur due to the nature of those activities.

   We therefore encourage the authorities to provide explicit guidance confirming that infrastructure provision in connection with blockchains sits outside the perimeter, so that stakeholders have certainty, consistent with the rules in non-blockchain contexts, as to which activities are, or are not, regulated.

3. **Authority and discretion, not technical capability.** The same boundary applies to those who operate infrastructure on behalf of regulated firms, including both centralised and decentralized blockchain infrastructure. In the centralised context, such providers will frequently possess the ***technical means* but not the legal right** to act on assets, orders or settlement processes; indeed, this is often inherent in, for example, hosting the systems or providing software as a service to facilitate regulated activity. What matters is ***not*** the technical capability, but whether the provider holds legal authority or discretion of its own. Where a provider is bound to exercise its technical capabilities only on the instruction of an accountable regulated entity, and retains no independent discretion over whether or how to act, it performs an operational function rather than an intermediary one. The relevant line is *de jure* authority and discretion, which attract regulation, not *de facto* technical means held under a binding obligation not to control, which do not.

   The authorities already apply this distinction in connection with traditional systems, and have indicated that the same principles hold true in the blockchain context. In particular, with respect to tokenised funds, the Call for Input confirms that a fund manager may delegate the operation of the fund register to a third party using distributed-ledger technology, but that the manager must always retain authority over that register regardless of

the technology used to operate it, and that a legally accountable person remains responsible for the integrity of the register (see also the FCA's earlier position in PS26/7 on tokenisation in fund and asset management). The significance of this is that the regulated activity is located in the manager's retention of authority, not in the operation of the register by the technology or the entity that provides it: the operator may run the system, hold access to it, and execute changes to it on instruction, yet it is the manager, the entity with directing authority, who remains accountable for the regulated function, and the operator is not thereby a regulated intermediary.

The same logic should be confirmed across tokenised market infrastructure generally. It is reflected, too, in the paper's recognition that regulated firms may make use of DeFi solutions while remaining responsible for maintaining regulatory standards, and that they continue to be responsible and accountable for their activities in connection with those systems.

This approach is consistent with the policy anchor that HM Treasury has articulated for the regulatory perimeter, namely that authorisation should apply where there is a "sufficiently controlling party" involved in the relevant activity, a limiting principle that grounds regulation in meaningful control, discretion or influence over outcomes. It is consistent, too, with the functional test set out by the Bank for International Settlements' Financial Stability Institute, which distinguishes activities related to infrastructure and system operation, such as validation, settlement and technical services, from financial intermediation, which involves taking custody or control of customer assets, creating liabilities or redemption obligations, or deploying assets in a way that transforms credit, liquidity, maturity or collateral risk. We recently advanced these points, together with other layer 1 protocol organisations, in our joint response to the FCA's Consultation Paper CP26/13 on Cryptoasset Perimeter Guidance[3].

In our view, an infrastructure provider should be deemed to remain outside the regulatory perimeter, provided two conditions are met:

1. **The provider holds no legal authority or discretion of its own.** It is legally and contractually bound to exercise its technical capabilities only on the instruction of the accountable regulated entity, and retains no independent judgment over whether or how to act.

2. **The accountable regulated entity retains directing authority.** That entity holds the legal right to direct, to withhold or override

[3] Joint response of Aptos Labs, the Avalanche Policy Coalition, the Cardano Foundation, the IOTA Foundation, the Sui Foundation and the Stellar Development Foundation to FCA Consultation Paper CP26/13, Cryptoasset Perimeter Guidance (2026), available at https://assets.ctfassets.net/eynrhjw8vyk9/3z8Y0KhU2JqITu5oZq2j1S/41bfad2744a5a0246eb1bdd2c5383b35/FCA_CP_26-13_comment_letter__1_.pdf. That submission discusses both HM Treasury's "sufficiently controlling party" anchor and the Financial Stability Institute's functional distinction between infrastructure and intermediation.

instructions, and - consistent with the exit-planning expectation in paragraph 3.5 - to replace the provider or migrate away from it.

Where these conditions hold, the infrastructure provider performs an operational function: it acts on instruction from the regulated entity and without making decisions of its own. It does not perform an intermediary function. Intermediation in this sense involves the exercise of discretion or authority and the assumption of a customer-facing financial relationship; in other words, the features that underlie the regulated activities of, for example, safeguarding and administering investments, arranging deals, or dealing as principal or agent. The mere technical ability to operate a system or software, coupled with a binding duty not to exercise that ability independently, does not constitute any of these.

This is the distinction we ask the authorities to recognise. It is not capability versus no capability. It is de jure authority and discretion, which attract regulation, versus de facto technical means held under a legal obligation not to control, which do not.

For the avoidance of doubt, this distinction cuts both ways. Where a provider does hold authority or discretion, for example, where it decides whether to move, freeze or release client assets, or operates a system that exercises matching or execution functions on its own account, it is performing a regulated activity and should be within the regulatory perimeter. Our submission is directed only at the provider that is bound to act on instruction and retains no such authority.

We recognise the legitimate concern underlying the paper. The authorities are right that there can be cases where regulated activity is taking place but no identifiable person is performing it, “such as on a decentralised exchange (DEX) or a public permissionless ledger” (paragraph 3.3), and that the perimeter may need to adjust to capture “some form of tokeniser acting for issuers.” We also recognise that, in the SIC custody context, the entity that controls cryptoassets through means of access such as private keys is exercising the safeguarding function itself (paragraphs 4.26–4.29). Our submission is fully consistent with both concerns.

The objection the authorities may raise is that the ability to control is itself the risk, regardless of any legal obligation not to exercise it: a contract supplies only a remedy after a breach, and a key-holder can in principle be compromised or compelled. We accept the premise but draw a different conclusion. Where a provider holds technical means but no authority, the residual risk that it might nonetheless act, in breach of contract or due to external compromise, is an operational resilience and outsourcing risk, properly borne and managed by the accountable regulated entity in accordance with well-established standards. That is precisely the model the paper already adopts: the regulated firm must assess the suitability of the blockchains it uses, including their governance, cybersecurity and performance, and undertake appropriate exit planning (paragraphs 3.4–3.5);

and it remains "responsible and accountable" for the activities those systems support (Figure 2).

It follows that if a bound-on-instruction provider were to act outside its mandate, it would have acted unlawfully and in breach; the accountable regulated entity would remain answerable, would be expected to have managed that contingency under its resilience and outsourcing obligations, and contractual and enforcement remedies would apply. None of this requires the provider to be authorised and regulated as an intermediary in advance.

This also distinguishes the SIC custody case. There, the key-holder is the safeguarding entity: it holds and decides. In the arrangement we describe, the regulated entity holds the directing authority and the provider executes on instruction. The substantive question the authorities should ask is the right one - who, in substance, controls the asset? - and the answer determines status. Our proposed clarification does not weaken that test; it sharpens it and keeps it consistent with existing regulatory principles in analogous contexts, thereby holding true to the nature of the activity test.

4. **Operational resilience.** We support the maintenance of high standards for operational risk management, cybersecurity and resilience. We suggest that these requirements should fall on the regulated firm that chooses to make use of a given blockchain, including its initial and ongoing assessment of that blockchain's suitability, and its exit planning, rather than on the protocol or its validators. Network-level concerns such as code vulnerabilities or majority-control ("51%") attacks are appropriately addressed through the regulated user's due diligence and through the network's own consensus security; on a sufficiently decentralised network, the absence of a single point of failure or single source of truth is itself a core resilience property.

Question 3: Do you agree with the priority areas and long-term ambition?

We broadly agree with the priority areas identified, with three observations:

1. **We propose an additional workstream on the regulatory perimeter and infrastructure.** We encourage the authorities to include, within the forthcoming roadmap, an explicit workstream that codifies the infrastructure-versus-intermediary boundary for public networks and resolves the paragraph 3.3 question and its offshoots with legal certainty, rather than leaving it to case-by-case judgement. In particular, and consistent with our response to Question 2, we ask the authorities to:

    - Confirm that the network, its validators and node operators, and protocol developers are not the "responsible person" for regulated activities that others conduct using the network.
    - Ensure that the future settlement end-state regime for DSDs (paragraph 3.12) expressly permits technical settlement on public,

permissionless networks, with regulatory obligations attaching to the regulated DSD or responsible person, not to the chain itself.
- Confirm that meeting the outcomes the paper itself contemplates, particularly with respect to permitted-list wallets, freezing and clawback functionality, zero-knowledge proofs and remote attestation, does not, in and of itself, render the underlying network a regulated entity.
- Confirm that whether a participant conducts a regulated activity is determined by whether it exercises authority or discretion over client assets, orders or settlement, and not on the technology it uses or the fact that it provides supporting infrastructure.
- Confirm that a provider may possess the technical means necessary to operate infrastructure without thereby becoming a regulated intermediary, where it is legally bound to exercise those means only on the instruction of an accountable regulated entity and retains no independent authority or discretion, with the residual risk addressed through that entity's operational resilience and outsourcing obligations rather than by separately regulating the provider.
- Confirm that this allocation of responsibility applies across tokenised market infrastructure generally, consistent with the position taken on the fund register, and is not confined to any single asset class or function.

2. **We welcome the commitment to equivalent prudential treatment of tokenised and non-tokenised assets** where legal rights are identical and underlying risks are comparable. This "same asset, same treatment" approach is directly beneficial to the tokenisation of government and corporate debt on public networks, and it reflects a technology-neutral direction now evident across major frameworks.

3. **We welcome the openness to settling "new digital asset ledgers"** in central bank money through the Bank's synchronisation service, and ask that this be expressly open to public, permissionless ledgers and not confined to private ones.

Question 5: Where and how is interoperability most important, and which initiatives would be most valuable?

Interoperability is fundamental, and we strongly endorse the authorities' recognition that there is a risk of regulators "picking winners" and that the solution lies in open, market-led standards rather than mandated networks.

Interoperability matters in three dimensions: between tokenised and non-tokenised infrastructures; between different tokenised versions of the same asset; and between UK and international infrastructure. Avalanche's architecture, under which independent, customisable L1s interoperate natively with one another and with external networks, is one example of how composable interoperability can be delivered without concentrating activity on a single chain. We would caution against any approach that designates a particular network or technology as the standard; the more durable path is to support emerging, openly developed

interoperability standards and to remain neutral between the networks that adopt them.

That said, interoperability should not be the sole or most important goal. The context remains crucial for evaluating how important interoperability is in a given situation and at what layer. For example, interoperability is needed to ensure clearing and settlement of transactions between custodians, but it may require staging in order to maintain privacy, proper custody protocols, and segregation of assets.

Question 7: Do you agree with the roadmap of initiatives and next steps?

We broadly agree with the roadmap and welcome the commitment to a coordinated, cross-authority approach. We would ask the authorities to prioritise, within that roadmap, the perimeter and infrastructure clarification described in our response to Question 2, and express eligibility of public, permissionless networks both in the settlement end-state regime and in the Bank's central bank money synchronisation service. We would also welcome an express statement that the future DSD authorisation regime will not exclude public networks.

Question 8: Are there any new products or early-stage initiatives you would like to discuss?

We would welcome the opportunity to engage with the authorities on the use of public infrastructure for the issuance and settlement of tokenised securities, including how such infrastructure can meet the outcomes the DSS and the future DSD regime are designed to secure, and on non-custodial settlement and safeguarding models. We would be glad to share our experience of institutional tokenisation already taking place on Avalanche, and to support the authorities' workshops and engagement groups as the roadmap develops. There is much detail in each implementation that makes the authorities' "first principles" approach important and we would be happy to share more information as appropriate.

Conclusion

We appreciate the Call for Input and the level of engagement shown by the authorities. The core principles that have governed financial regulation since its inception, a focus on the nature of the asset and the activity, continue to apply with equal force in a tokenised world. They support the outcomes-based, workable approach reflected in the Call for Input and long advocated by the Avalanche Policy Coalition.