Financial Conduct Authority

Consultation Paper CP25/28

Published October 2025

Response by 12th December 2025

Progressing Fund Tokenisation

RESPONSE FROM:

United Kingdom Shareholders' Association

Submitted 11 December 2025

UKSA, 1 Bromley Lane, Chislehurst, BR7 6LH

Phone: 01689 856691

Email: admin@uksa.org.uk

Web: www.uksa.org.uk

Progressing Fund Tokenisation

To: Joshua Castle
Funds and Asset Management Policy; Wholesale Buy Side
Financial Conduct Authority
12 Endeavour Square London E20 1JN
Email: cp25-28@fca.org.uk

The UK Shareholders' Association are pleased that the FCA is looking at new technologies but are wondering why the FCA is considering blockchain/distributed ledger technology (DLT) when the Digitalisation Taskforce under Sir Doulgas Flint (Digitisation_Taskforce_Final_Report.pdf, page 54) has decided against it for equities. The Digitisation Task Force concluded it was unsuitable for the UK equities market based on Australia's now cancelled DLT project "due to its scale, complexity and transition challenges".

We are concerned that equities and funds will be seeking different technological solutions, causing potentially complex and incompatible operations. We ask that the FCA discuss with the Digitisation Task Force why the Digitisation Task Force has dismissed DLT as a solution and share that information with us. Not understanding the differences undermines the proposals in this consultation and raises two overarching questions:

1. Why does the FCA consider blockchain/DLT technology to be suitable for funds whilst The Digitisation Task Force believes it is unsuitable for equities?
2. Is fund tokenisation for the moment an 'investigative' consultation, with no foreseeable implementation date?

We request answers to the questions but, for now, the rest of our response assumes that DLT is a potentially worthwhile solution.

Please feel to contact us at admin@uksa.org.uk if a conversation would be useful.

Signed.

Sue Milton, External Relations Director and Policy Team member, the UK Shareholders' Association.

Mathew Whymark, Specialist Adviser.

1. **Introduction:** we highlight our main points.

1. We ask that the FCA learns from other regulators that have already implemented DLT as they have already solved many of the problems the UK will now face. The FCA should learn from these regulators that have already established comprehensive frameworks, token standards and DLT governance models. For example:
    a. Dubai (UAE) VARA, Switzerland has already defined DLT based securities International collaboration.
    b. Tokenisation is already live and at scale in Singapore, Switzerland and the UAE (Dubai and Abu Dhabi).

2. Leveraging these lessons will reduce risks and help accelerate adoption in a safer way. Otherwise, there is a risk that, if it takes too long to provide clarity and frameworks for tokenised markets, investors will gravitate toward jurisdictions with regulation and maturity for tokenised products.

3. Nations are seriously competing to become global hubs and leaders in innovation for tokenised finance. This raises a conundrum: we know that to protect our technologies, we need to learn from each other, which requires information-sharing, yet competitiveness leads to secrecy. Protocol risks are global risks, e.g. vulnerabilities in smart contract standards, cryptographic weaknesses, chain outages and emerging threats such as quantum cryptographic threats. We ask that the FCA takes the opportunity to participate on the global stage, to set standards, share intelligence and protect investors.

4. An essential question for this consultation is whether the DLT ledger becomes the official, legally recognised fund register, or is deemed to be just a digital copy of a legally recognised one kept elsewhere. This matters because it determines which record is relied upon in the event of a dispute.

5. Another essential question is the UK's definition of a stable coin and how it will operate in practice. The United States, summer 2025, has passed a stablecoin law, with Canada this month proposing its Stablecoin Act.

6. Investor privacy, security across the eco-system, transactional finality, assurance, and redress will be major factors is enabling trust. DLT may provide that immutable record, but trustworthiness extends beyond that to all relevant people, operations, processes and regulation.

7. Smart contracts make fund operations more efficient and transparent so long as they operate under robust oversight. The FCA should clarify expectations for audits, upgrades and data dependencies to ensure that automation enhances, not undermines, trust and investor protection.

8. Key-management over access to the DLT and assets is a vital component for trust in the system.

9. Solutions to transaction and settlement failure is vital.

10. Regulation will have to be agile.

11. New skills will have to be honed swiftly and continuously updated.

12. Quality of the technology is paramount, requiring virtually zero-risk tolerance. This requires finding both governance and technical solutions that enable the technology, processes and regulation to absorb and resolve with minimum disruption the impacts arising from all of the above.

2. Answers to your numbered questions

Q1: Does the proposed guidance provide adequate clarity on how firms can use DLT to support the operation of fund registers?

1. The FCA's guidance takes the right approach by being open to DLT for fund registers, but investors still need clearer direction on how it will work in practice.

2. A key question being whether the DLT ledger itself becomes the official, legally recognised fund register or just a digital copy of one kept elsewhere. This matters because it determines which record is relied upon if there's ever a dispute about who owns what.

3. Not all DLT networks are the same. A private or "permissioned" network allows tight control and governance, whilst a public blockchain offers openness but raises new questions around data security, resilience and jurisdiction. The FCA should explain what level of assurance and control is expected for each type.

4. Investor identity and privacy also need careful handling. If investors use digital wallets, firms must link those wallets to verified identities but without putting personal information directly on the blockchain. This protects privacy and meets the requirements of data protection regulation.

5. Many investors, especially retail investors, may be new to DLT networks and will need guidance in how it works and what assurance they will receive in knowing that what they see is what others see. This is especially important in any query about the relevant holdings but also applies to other aspects, such as the revised back-office roles and processes. Our answers to Q2 expand on this.

6. We need to understand the expected level of operational resilience. Even though DLT is decentralised, firms still need strong controls for managing keys, validating transactions and recovering from failures.

Q2: Are there any challenges in meeting the current requirements where DLT platforms are used, or in respect of emerging use-cases?

1. Using a DLT in fund management exposes several practical issues that existing regulations do not yet fully cover.

2. Fund rules today assume a single central register, whereas DLT spreads the record across many nodes. This makes it harder to define which version of the

ledger is the official one and when a transaction is truly "final". Without this clarity disputes over ownership or timing could arise.

3. Investor identification becomes more complex. Many retail investors access funds through online platforms that hold pooled wallets. Tracing who owns what while still meeting AML and investor protection rules requires new standards to link verified identities with digital wallets safely and privately.

4. Smart contracts create governance challenges. These self-executing pieces of code can automate fund operations but are difficult to update or correct if something goes wrong. Regulations assume a human approval process. DLT introduces automation that needs new oversight models and new communication frameworks so investors understand the 'what, when, why and how' smart contracts make adjustments (i.e. the meeting of the terms and conditions of a transaction that then triggers the smart contract to self-execute that transaction).

5. We can see the advantages. The blockchain records the details that are permanent and traceable, providing a highly reliable audit trail as nothing can alter them. Smart contracts can be created quickly and efficiently, without an intermediary, thereby reducing costs, saving time, and improving security.

6. The shift to DLT changes operational roles. It removes manual reconciliation and back-office tasks, improving efficiency but also reshaping jobs. Firms will need people skilled in DLT governance, digital custody and cyber security in place of manual processing.

Q3: Do our existing rules and proposed guidance provide sufficient flexibility to allow for firms operating the register to use smart contracts for the purposes above?

1. Smart contracts make fund operations more efficient and transparent but they must operate under robust oversight.

2. We understand that creating and auditing smart contracts requires specialist skills, usually undertaken by smart contract and/or blockchain developers. Retail investors will need to understand how the FCA, and other relevant regulators, can ensure maximum security and that the smart contract process complies with digital and computer-related legislation such as GDPR, the Cyber Security and Resilience (Network and Information Systems) bill (Summary of the Bill - GOV.UK) and DSIT's software security code of practice (Software Security Code of Practice - NCSC.GOV.UK).

3. The FCA should clarify expectations for audits, upgrades and data dependencies to ensure that automation enhances and does not undermine trust and investor protection.

Q4: What role can regulators play in supporting the development of token standards that promote effective governance and positive consumer outcomes?

1. Making sure usability, privacy, safety, security and redress remain in the forefront by having:

   A) Token standards that make tokenised funds safe and transparent.

   B) Principles that every regulated fund token must adhere to i.e.:
   a. Clear governance and upgrade processes.
   b. Privacy-by-design to protect investor data (it is actually privacy-by-design-by-default).
   c. Robustness-by-design to ensure the ecosystem (this includes the technology, the data, plus the key people necessary to keep systems running) and related procedures can withstand shocks.
   d. Resilience-by-design to ensure that all parts of the ecosystem and procedures can be recovered swiftly or, when this is not possible, have relevant contingency plans in place.
   e. Traceability for audit and compliance.
   f. Interoperability between platforms to avoid closed ecosystems (limits competition, increases costs and creates a fractured/fragmented market).
   g. Transparent, relevant and easy to use processes and contacts to real people in the event of a query or concern, including escalation.

   C) Industry collaboration with standards bodies and international groups so that UK tokenisation aligns with global practices to reduce cross-border friction.

Q5: Do our COLL rules and proposed guidance provide sufficient flexibility to support fund tokenisation use-cases that use public networks?

1. Public networks offer greater transparency, accessibility and interoperability, benefitting fund managers and retail investors. However, they also introduce new risks and responsibilities that are not fully addressed in the existing framework, such as:

   A) **Custody and Key Management**

In a tokenised environment, losing a private key can mean losing access to assets. The FCA should set expectations for regulated custodians, multi-signature arrangements and how firms handle key loss or compromise.

B) **Data privacy**

Public blockchains are transparent, meaning that transaction data could be linked back to individuals and used for profiling. Firms must ensure that no personal or sensitive information is placed/stored on-chain and that off-chain systems handle investor identities securely.

C) **The COLL framework**

This will need to flex to support carefully controlled public network use cases.

Q6: Do the proposals in this Chapter provide adequate flexibility for firms considering tokenisation and the migration to T+1 securities settlement?

1. Yes. Tokenisation supports faster more efficient settlements cycles (such as T+1).

2. The transition to T+1 would require:
   a. Interoperability between traditional and tokenised systems to overcome bi-model complexity.
   b. Interacting between traditional and tokenised systems.
   c. Overcoming the challenge of funds/assets being held on-chain and off-chain and how to manage and synchronise them, e.g. reconciliation and handling misalignments.

Q7: Do you support the introduction of an optional regime to allow for direct dealing in authorised funds?

1. In principle, yes, as the D2F (Direct 2 Fund) would allow investors to purchase or sell directly with the fund rather than the authorised fund manager, suggesting more investor autonomy and greater efficiency.

2. Retail investors, especially, need to understand better how responsibilities, currently with the authorised fund manager/depositary/trustee, will be split between the D2F, the investor and the fund manager/depositary/trustee.

Q8: Do our proposed requirements for operation of the IAC provide a proportionate control environment while ensuring funds are operated, and overseen, in line with principles of segregated liability?

Unable to comment.

Q9: Do you agree with our proposals in respect of overdrafts and limits on fund exposure to a given bank or group? If not, why?

Sounds sensible and appropriate from a retail investor perspective.

Q10: Do you agree we should include all cash held at a given bank within our spread of risk rules for UCITS and NURS? If not, why?

Unable to comment.

Q11: Do you agree with our proposed accounting controls in respect of use of IAC? If not, why?

Unable to comment.

Q12: Do you agree with our proposal to provide additional clarity on cash held by LTAF and the requirement to appoint an external valuer? If not, why?

Unable to comment.

Q13: Do you agree with our proposals in respect of investor disclosures and communications? If not, why?

Yes, based on our understanding at the moment.

Q14: Do you agree that fund AFMs should bear the cost of exercising discretion for late payments? If not, why?

Unable to comment.

Q15: Are there scenarios where this may not be appropriate or such costs should be allocated differently?

Unable to comment.

Q16: Do you support introducing broader powers to deal with historic orphan monies? What legal or regulatory barriers might prevent introducing such a process?

Unable to comment.

Q17: Are there any other purposes for which funds, fund managers, or investors may need to hold cryptoassets to support fund operations on-chain?

1. It is difficult to say until HMT's upcoming definition is revealed as to what is a stablecoin, along with the associated criteria for what makes a particular stablecoin be suitable for use in settlement (see the consultation's paragraph 4.23). The number of decisions outstanding makes it difficult to identify an optimum solution.

2. We see operational collateral and margin in tokenised funds as the on-chain equivalent of existing processes such as securities lending, settlement account float and margin accounts. Asset Managers will need to post collateral into smart contracts, liquidity pools and settlement layers.

3. This introduces new risks and will require new governance, disclosures and custody controls.

Q18: Would our potential amendments to COLL provide sufficient flexibility for firms to use digital cash and money like instruments for operational purposes, including unit dealing?

Unable to comment.

Question 19: Would a limited sandbox or standard waivers/modifications be appropriate routes to allow us to develop a final regime in collaboration with industry? What features may be desirable in such a regime?

Unable to comment.

Question 20: Do any other areas of our rules conflict with or prevent use of digital cash instruments or money-like instruments for unit dealing, distribution payments, or for payment of charges and fees?

Unable to comment.

Question 21: Would our existing rules, including the Consumer Duty, provide enough protection for investors if we allow a fund to hold cryptoassets for settlement and fund operational purposes only?

1. Yes, as existing FCA rules, including the Consumer Duty, form a strong foundation/baseline to protect investors where funds are using cryptoassets for operational purposes. They already embed core principles around fair value, transparency, operational resilience and oversight.

2. However, 'operational only crypto' creates a new class of hidden exposure for investors. Areas requiring further clarification are:

   A) Disclosure and Transparency.
      a. Investors will need to understand how cryptoassets are used operationally and the risks that this introduces, such as chain outage, keys compromised.
      b. *Why this matters:* operational crypto risks could delay redemptions and fund operations.
      c. *What must be done:* tell investors what is happening behind the scenes. Investors should know the fund uses crypto to operate. Explain operational risks in plain language.

   B) Custody Key Management and Accountability.
      a. Operational digital assets must adhere to clear custody and safeguarding requirements/controls (such as key rotation, backup, recovery and accountability).
      b. *Why this matters:* if operational keys are compromised or lost investors may lose access to the fund or experience significant delays.
      c. *What must be done:* protecting the keys (the crown jewels); these are not IT tools. They are high-security custody assets.

C) Operational Resilience and Stress Testing.
   a. Tokenisation-related operational risks should be included in:
      i. Business Service mapping.
      ii. Scenario testing.
      iii. Recovery plans.
      iv. Incident reporting.
   b. *Why this matters:* tokenisation can fail in ways that are very different to traditional systems. Firms need to demonstrate that they can continue to operate through disruption without harming investors.
   c. *What must be done:* firms must explicitly recognise that DLT dependencies become material to their operations.

Question 22: Are there other associated regulatory, operational or commercial barriers to investing in tokenised assets? What could we do to address these issues?

1. Tokenisation faces regulatory, operational and commercial barriers that limit adoption.

A) Regulatory and Legal:

a. When an investor holds a token what do they legally own?
b. How are tokenised assets handled if a fund, custodian or DLT operator fails?
c. Legal uncertainty discourages use of tokenised funds.

What it needs: a clear definition of legal status of a tokenised fund/units.

d. Operational and Technological: lack of standardisation leads to interoperability challenges between DLT networks.

What it needs: operational and governance standards for DLT funds, and expectations for chain selection, key management standards and controls.

B) Dependence on New Critical Providers:

a. Tokenised funds would rely on new third parties that are not currently established in governed frameworks e.g. DLT operators, cloud hyperscalers, digital custodians.
b. This is important as these providers could become a single point of failure/concentration risk.

*What it needs: d*efined classification for DLT operators and resilience expectations.

C) Skills, Capability and Talent Gap:

a. Tokenisation fundamentally changes the skills profile required to operate regulated funds and is not an incremental step. The Asset Managers are moving from heavy manual operational processes to one that requires highly technical and deep engineering skills (e.g. software engineering 'as code' and cryptographic security).
b. There will be a significant workforce transformation, shifting from manual fund operations (People and Process) to Code and Infrastructure.
c. The talent required is already scarce and demand is already outpacing supply.
d. Over the past 3-5 years the UK has lost a significant portion of its most experienced talent (Web3 engineers, Smart Contract developers and DLT security specialists), as they have relocated/or taken remote roles for companies based in the UAE, Singapore, Hong Kong and US where these regions have aggressively invested in regulatory clarity (e.g. VARA, the 'Virtual Assets Regulatory Authority' in Dubai, UAE), tokenisation pilots for payments, and attracting the talent through incentives and residency schemes.
e. The UK Asset Management industry has not traditionally hired this type of expertise. Competition from the Big Technology players and crypto-native firms will intensify scarcity.
f. There are not enough junior engineers being trained in the pipeline with the relevant skills to fulfil the demand. This is also a consideration for UK Universities.

What it needs: our suggestions reduce technical risk, talent dependency, create standardisation and significantly reduce cost and time-to-market:

i. Certification Frameworks.
ii. Regulators to standardise what good looks like to mitigate the risk of every Asset Management firm defining and hiring what they think they need.
iii. Create certification frameworks for tokenisation roles, e.g. Smart Contract Specialist, Digital custody and key management Specialist, DLT operation Risk Specialist.
iv. Repeatable, standardised and trusted skills.

v. Reference Model templates to provide baseline architectural templates e.g. smart contract templates for tokenised fund units, and key-management governance models.
vi. Regulated, industry sandboxes to allow firms to test tokenisation in a low risk environment to encourage shared learning with regulators learning alongside the industry.

Question 23: How are changing investor habits and expectations influencing the design of tokenised products?

1. Investor habits are changing but the trick will be to keep on-side those who cannot embrace tokenisation alongside appealing to those who embrace a totally digital approach.

2. Younger investors are more comfortable with digital assets and want direct, flexible and transparent ways to invest. This is often through mobile Apps and Digital wallets.

3. There is an expectation of real-time access to portfolios, settlement and the ability to hold both crypto and traditional assets in one place. Tokenisation supports this modern approach.

4. The recent change to the United States 401(k) scheme now allows limited exposure to crypto investments that the FCA should monitor to help the UK build useful, safe and secure systems and processes that avoid short-term thinking and impulsive behaviour.

Question 24: Do you agree with the three phases described? Are these developments industry is looking to pursue?

1. There are several assumptions identified as 'may' in this section of the consultation. We would like to see these become more concrete before fully assessing the benefits and how sensible the proposals are. On what we understand, the approach is one of maturity, offering a logical and progressively gradual level in complexity and risk management.

2. As things stand, we believe that:

   A) Phase 1 - Tokenisation of funds:

   a. This makes sense as firms start to test and establish methods, the emphasis being on using DLT to improve operational efficiency. A non-disruptive first-step.

B) Phase 2 – Tokenisation of assets:
   a. This introduces the tokenisation of funds and of smart contracts to automate more processes.
   b. This phase is highly dependent on getting the design, build and interactions of smart contracts established. See our answers to Q2 and Q3.

C) Phase 3 – Tokenisation of cash flows (end-state):
   a. Full portfolio tokenisation with instant settlement, transparency and programmatic compliance.
   b. More significant regulatory maturity and oversight.

3. But what is the impact if new entrants accelerate to highly tokenised models in a "run before you can walk" approach?

Question 25: What processes within the fund and investment management lifecycle do firms want to begin to make 'composable'?

1. Any approach that allows less liquid assets to become more liquid, and enables assets to be broken down into small parts, is a good thing as it makes additional assets more affordable as well as allowing investors to both increase diversity and experiment in assets typically not available to them for reasons of size, costs and risk.

2. We have more questions which we believe need answers to progress with consumer-focused fund tokenisation:
   a. What is the full extent of how would tokenisation and DLT transform fund operations?
   b. Will is simplify KYC checks?
   c. Can using verifiable, digital identities be used across multiple funds or platforms?
   d. Will we achieve real-time fund valuation and real-time pricing?
   e. Will Immutable transaction records simplify audit and assurances?
   f. How will firms retire legacy (obsolescent) infrastructure?
   g. How will firms be able to reduce operational errors/risks?

Question 26: How does 'composability' impact the liquidity profile of assets we currently think of as less liquid or illiquid?

1. Tokenisation with composable smart contracts has a direct impact on how illiquid or less liquid assets can be made more accessible (those smaller, affordable units) and operationally efficient within a tokenised ecosystem. It changes the mechanics of access, settlement and fractional ownership:
    a. More investors can enter or exit positions.
    b. The liquidity increases even though the underlying liquidity remains unchanged.
    c. Composability improves the mechanics of liquidity but not the fundamental liquidity constraints. There will be cases of creating the illusion that investors can exit instantly, but the underlying asset cannot be liquidated quickly.
    d. This could also encourage Automated Compliance. Today, transferring units in less liquid funds can take weeks for checks to complete.

Question 27: How might the tokenised portfolio management vision enhance consumer outcomes?

1. If it keeps the consumer, especially the retail investor. in the forefront of any solution, this could be an amazing benefit to all. The formulation of great outcomes is very dependent in firming-up the aspects defined as 'may' in the consultation into 'will'.

2. Every asset in a portfolio (equities, bonds, crypto) represented digitally on a distributed ledger, will provide real-time visibility of holdings, pricing and performance. It also facilitates fractional ownership of investments that may previous have been out-of-reach to many investors.

Question 28: Do you foresee any other major changes to the role of asset managers or other market participants in a tokenised flows 'end-state'? What are the opportunities and risks?

1. We foresee a broader reshaping of financial services with many changes, often for the good. We predict the removal of large portions of low value operational activity, shifting from being operationally heavy to specialist technology engineering, increasing the value per employee.

2. We have identified four areas:

- Governance and risk.
- Organisational infrastructure impacts.
- Automation in the back-office functions.
- Changing roles.

1. Governance and risk.

a. A key risk is that technology outpaces governance. In reality, technology is already doing so. The BIS' 2023 paper Crypto, tokens and DeFi: navigating the regulatory landscape, section 6, identifies key risk areas that still apply today, which makes us concerned about:
   i. Risks to current regulatory and risk management practices.
   ii. Potential adjustments to the regulatory perimeter, to include new actors involved in these services.
   iii. Anti-competitive behaviour in crypto asset activities.
   iv. Keeping regulation in step with firms using public permissionless DLTs, either to develop applications, or to actually use them, in the provision of services.
   v. Authorities needing to develop legal frameworks to enforce agreements coded in smart contracts and related liabilities of direct and indirect parties involved in providing and running the technology that manage token-related services.

b. Technical issues that cause transactions to fail, such as timeouts, often occurring after one area of the system has been updated with throughput efficiencies that then cause bottlenecks elsewhere; or functional incompatibilities from business updates that cause other parts of the once-working system to fail.

c. Because of increased cyber exposure, other areas that will need to be looked at are:

d. How new participants will provide technology-led services, such as to manage and hold keys.

e. What new technologies, such as a powerful quantum computer, could break the private keys allowing attackers to steal or sign fraudulent transactions (note that transitioning to quantum resilient DLT architectures is still a long way off).

f. If an asset manager became the custodian of private keys, how would they achieve the necessary robust infrastructure? 'Robust' includes having the right quality of security and controls with adequate insurance, as a breach could be significant (increased cyber exposure).

g. Key protection because keys are high value targets for hackers, including insider threats.

2. Organisational infrastructure impacts.

There are organisational and operational impacts that must be managed. Some are beneficial but there will be some trade–offs, too:

a. Benefit: as asset managers and financial institutions adopt DLT, the need to maintain their own infrastructure will decline because the data centres and technologies, used today for their operations (transaction records, settlement etc), will be displaced by DLT.
b. Benefit and risk: this shift will increase reliance on cloud-hosted technologies, such as the hyperscalers (AWS, Azure, GCP), the outcome being a reduction in infrastructure spend (CapEx) and data centre space where asset managers previously stored their own technology systems, whilst increasing 3rd party risks.
c. Benefit: a reduction in computational provision from financial service companies would also reduce power consumption, examples being less duplicated data processing and reconciliation, significant smaller data centre footprints, and no overnight batch processing.
d. Risk/benefit balancing act: many of these existing systems/technologies may also be a reason that financial service companies maintain an on-premises footprint (their own data centres) as they, and the data they hold, are considered 'material' systems. The adoption of DLT may facilitate further cloud native adoption/acceleration, to leverage new technologies and security features but add the risk factor that hyperscalers are a bigger target and could inject concentration risk.

3. Automation of back-office functions.
   a. DLT and smart contracts automate a number of existing manual back-office functions. The impact would become significant with maturity and adoption; however there would be a requirement for new skills, a need for a workforce transformation.

4. Changing roles.
   a. Roles that are highly likely to decline:
      i. General fund administration.
      ii. Custody and settlement.
      iii. Manual KYC/AML processing teams.
      iv. Account servicing.
      v. IT Infrastructure and Operations.
   b. New skills required:
      i. DLT architecture and integration engineering roles.
      ii. Compliance engineers.
      iii. Data scientists (data and model).
      iv. Cloud security, Key management and AI based monitoring specialists.

Question 29: How might market integrity and financial stability risks evolve in the future tokenised portfolio management model?

1. Retail investors are relying on the BIS' findings Financial stability implications of tokenisation - Executive Summary. In essence, the current small-scale use of tokens currently poses no such risk, but scaling will lead to complexity, requiring changes to governance and oversight.

2. We assume that the existing principles, as set out by FSB (the Financial Stability Board) (Key Standards for Sound Financial Systems - Financial Stability Board hold true for tokenised management too.

3. On the technical side, providers of the DLT and providers of the user interfaces will have to identify the key systems and processes that must demonstrate continual confidentiality, integrity and availability.

Question 30: What areas of the current funds framework will need to be recreated in the future vision? What areas could be simplified across different parts of the Handbook?

Unable to comment.

Question 31: What areas of the Handbook, or wider rules and legislation, do we need to reconsider to support the growth of the proposed tokenisation models?

Unable to comment.

Question 32: What should the FCA's role look like in this future vision?

1. We want an FCA that is a knowledgeable enabler, fostering trust through outcome-based rules and enforcement to achieve holistic benefits whilst avoiding the micro level such as picking the technology. We recognise that this is a difficult balancing act, spelt out in B). We do believe that the balancing of innovation with trust will keep the UK competitive with benefits that flow directly to the investors.

2. The future-state role for the FCA is not just about financial regulation, it accelerates to digital infrastructure supervision and to achieve this the FCA needs to expand its own skillset in DLT engineering, blockchain security, cryptography, smart-contract analysis, real-time data analytics and keep pace with innovation e.g. emerging horizon of quantum

3. In a tokenised world the FCA would be required to supervise:
   a. Smart contracts.
   b. DLT networks.
   c. Digital custody models and key management controls.
   d. Data integrity.
   e. Cyber and cryptographic resilience.
   f. Operational dependencies on critical third parties.

4. The FCA would require new skills and capabilities, deep technical expertise across a number of domains including and not limited to:
   a. DLT - Immutability and state, Smart contracts and protocol upgrades.
   b. Crypto-Security and Key Management – HSMs, Key lifecycle management.
   c. Smart Contract Engineering – reading and understanding code.
   d. Cyber security – threat modelling, attack vectors, supply chain attacks on DLT, post-quantum risk threats.

5. The FCA should look at Digital Operational Resilience and Third-Party Oversight:
   a. Assess cloud operational architecture.
   b. Failover and Disaster Recovery for chains.
   c. Cross chain dependencies and systemic risk.

6. The FCA should investigate Technology Policy Engineering (Regulatory Engineering):
   a. Evolution from rule-writing to protocol shaping.
   b. Collaborating with standards bodies on interoperability.
   c. Publishing guidelines for digital custody, key sharing models.

7. The FCA must set the foundations for a unified, open tokenised market, which should include:
   a. Guardrails and resilience that:
      i. Provides the principles for tokenised funds, e.g. recoverability, auditability and data-minimisation.
      ii. Sets expectations for key management.
      iii. Clarifies accountability across the fund managers, custodians and DLT operators.

b. Protect-Consumers-by-Design:
    i. Having Privacy-by-Design standards, such as disallowing personal data on the chain by default, with consent controls for investors to explicitly approve how their personal data used across tokenised operations.

c. Core Token Requirements/Behaviour that**:**
    i. Avoids closed ecosystems and duplicated effort.
    ii. Must be done by the FCA through convening industry and technology experts to define core token requirements for authorised funds covering Auditability and Event Logging.

d. Open APIs and Data Models that:
    i. Ensure connectivity as value can only be achieved if all participants are able to connect.
    ii. Require open and publicly documented APIs (Application Programming Interfaces).
    iii. Demand standard API endpoints for reading register data, and having a shared schema for investor identity checks, distributions, etc.

e. Registers and Custodians to align data structures for:
    i. Investor identity references (preserving privacy, e.g. personal identifiable information or PII for short).
    ii. Regulatory reporting.
    iii. Transfer instructions.
    iv. Token metadata.

f. Key Management:

    Tokenisation shifts risk from traditional infrastructure to key management security, whomever controls the key controls the asset. Therefore, set these standards for:

    i. Key storage, rotation and renewal.
    ii. The use of Hardware Security Modules (HSMs) for physical cryptographic devices designed to generate, store and use the keys.
    iii. Governance requirements over keys with formally documented processes that are fully recorded, auditable and audited.
    iv. Real-time monitoring, alerting and detection of anomalies.
    v. Behavioural analytics, with immediate alerting for unusual requests.
    vi. Multiple Signature approval so that a transaction requires approval from multiple parties to prevent unilateral control. This mitigates insider risk/bad actor threats, theft and adds a layer of governance.

8. The FCA needs to develop compliance logic for regulatory, contractual and operational controls embedded directly into smart contracts and DLT infrastructure to ensure that UK funds operate within the UK regulation automatically (defined in machine readable formats) e.g.:
    a. Restrictions on who can hold units.
    b. Restrictions on how units can be transferred.
    c. Restrictions on when transfers can occur.
    d. KYC/AML triggers/rules.
    e. Sanctions.
    f. Investor protection.
    g. Smart contract management.
    h. 3rd party service levels.

9. The FCA needs to develop error handling and recovery so must consider:
    a. Tokenisation changes how errors occur and are corrected.
    b. With DLT, immutability is core feature as, once written, it cannot be changed, deleted or overwritten. It is permanent (you cannot alter the past with a value in a field). Errors are corrected by adding new transactions to offset or reverse using structured mechanisms.

10. In addition to all the above, additional questions that need answers:
    a. How do you fix a mistaken transfer, the wrong investor, the wrong wallet, a wallet that is frozen or inaccessible (which could include sanctioned)?
    b. What happens when an investor loses their private keys?
    c. What happens when transactions fail? As we stated in our response to Q28, this could be as a result of network delays/ outages/ congestion/ planned downtime.
    d. What are the governance and approval processes for recovery? Who can initiate? What are the approvals and conditions? Will there be regulatory oversight?
    e. What level of transparency must there be in the processes that are regulated? How clear must the types of errors be that can be resolved/reversed?
    f. With consumer protection in mind, which roles have what responsibilities for managing corrective action, timescales for implementing solutions, and escalation and redress activity?

11. The FCA needs to prepare for future risks:
    a. Guidance on a post quantum world.
    b. Stress test concentration risks.

12. The FCA will need to support workforce transformation and transition, and industry reskilling.