FINANCIAL CONDUCT AUTHORITY

Distributed Ledger Technology

Feedback Statement on Discussion Paper 17/03

Feedback Statement
FS17/4

December 2017

This relates to

Discussion Paper on distributed ledger technology, DP17/3.

Please send any comments or queries to:

Matthias Bauer
Financial Conduct Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Telephone:
+44 (0)20 7066 5640

Email:
dp17-03@fca.org.uk

How to navigate this document onscreen

returns you to the contents list

takes you to helpful abbreviations

Contents

1 Introduction

Why we are issuing this paper

1.1 In April 2017, we published Discussion Paper (DP) DP17/03 on Distributed Ledger Technology (DLT)[1] to stimulate a dialogue on the regulatory implications of current and potential developments of DLT in the financial markets. We explored the potential risks and benefits of DLT applications in financial services and whether it could promote the FCA's statutory objectives of promoting effective competition, financial market integrity and financial consumer protection. We specifically asked about tested DLT use cases and whether the future application of this nascent technology could face undue regulatory hurdles or create undue risk.

1.2 In this feedback statement we:

- summarise the feedback we received on our Discussion Paper
- set out our response to the feedback received, and our views on certain recent developments
- explain our next steps

Context

1.3 DLT was first used in Bitcoin, a digital commodity or so-called currency, as a means to facilitate peer-to-peer payments without a central third party. Today, however, market participants are exploring the benefits and risks of other use cases in financial services, most of which involve sharing data amongst multiple network participants, and do not need to involve digital currencies.

1.4 DLT is a highly customisable and versatile technology that firms can use to underpin the issuance, trading and clearing of financial instruments, to keep and share records and to facilitate regulatory reporting or enhance transaction monitoring. After a period of small scale testing, so called proofs-of-concept (POC), and various initiatives to develop more specific DLT systems for use in financial services, market participants are beginning to start deploying DLT systems.

1.5 Our aim is to be alive to current and potential developments involving DLT, to keep pace with them, and to strike a proportionate regulatory balance between the risks and opportunities they present. We see regulation as an enabler of positive innovation based on new technologies as well as a means of containing undue risk. Our regulatory philosophy (subject to any risks to our objectives) is to be 'technology-neutral', and we asked whether our current rules are flexible enough to accommodate appropriate use of DLT and similar innovative technologies.

1 www.fca.org.uk/publication/discussion/dp17-03.pdf

1.6 In the DP, we noted that using DLT in financial services could enhance administrative efficiency, improve operational resilience and reduce the costs of regulatory reporting. All of these could lower financial and technical barriers to entry and enhance competition. We explored specific DLT applications in various areas such as asset management, payments and regulatory reporting. We also said the distinctive properties of some DLT applications might create new or uncertain risks that could result in consumer harm.

1.7 We received 47 responses from a wide range of market participants including regulated firms, national and international trade associations, technology providers, law firms and consultancies.

1.8 We also hosted an international regulators summit in April 2017 to discuss innovative technology in financial services from a global perspective. We discussed the emergence of new financial markets underpinned by DLT including the use of digital currencies, smart contracts and Initial Coin Offerings (ICOs). This was followed by a two-day industry conference in June 2017 where we further explored the use of DLT in financial services.

1.9 Through our Innovate initiatives, including the regulatory Sandbox[2] and Techsprints[3], we have gathered unique hands-on experience with a wide range of DLT applications. Of 58 Sandbox firms, 22 have used DLT which makes it the most popular technology employed in the Sandbox and highlights the genuine interest and high demand for testing with the FCA.

1.10 We have drawn on this experience, and various cases we have explored through Innovate, throughout this feedback statement.

1.11 We would like to thank all concerned for their feedback and for participating in our events discussing DLT. We would also like to thank smaller start-ups and larger institutions for engaging with us through other channels. Your feedback has played a vital role in informing our understanding of DLT development and of market participants' perceptions of the risks and opportunities of this nascent technology. The views expressed have helped to shape our thinking on next steps and future areas of focus.

Highlights of feedback

1.12 The DP was positively received. Respondents expressed particular support for maintaining our 'technology-neutral' approach to regulation and welcomed our open and proactive approach to new technology, including our Sandbox and RegTech initiatives. They suggested that this will support competition and improve consumer outcomes in financial services.

1.13 The feedback we received suggested that our current rules are flexible enough to accommodate applications of various technologies, including the use of DLT by regulated firms. Nearly all respondents generally agreed there are no substantial barriers to adopting DLT under our regulatory rules and no changes to specific rules

2 www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf
3 www.fca.org.uk/firms/regtech/techsprints

were proposed. But some respondents doubted the compatibility of permissionless networks with our regulatory regime (see chapter 2).

1.14 All respondents suggested numerous benefits and risks of using permissionless and permissioned DLT networks in financial services. But they said those risks heavily depend on the specific application of DLT.

1.15 Respondents who commented on ICOs agreed with our view on the risks to consumers and that the legal and regulatory position of each ICO proposition has to be assessed case by case (see chapter 3).

1.16 Most respondents were particularly interested in the use of DLT in the capital markets sector, for example underpinning market trading infrastructure, including the use of smart contracts. They said they would have to be clearer on legal issues such as the legal status of digital assets and the enforceability of smart contracts before they considered using those solutions at scale (see chapter 4).

1.17 Many respondents suggested that DLT solutions could deliver regulatory requirements more efficiently than current systems, substantially reducing costs for firms and regulators alike (see chapter 5).

1.18 Some said DLT could facilitate the secure sharing of data between multiple participants. However, most said that the current reliance provisions in the Money Laundering Regulations do not incentivise firms to share know-your-customer information or foster any enhanced level of cooperation (see chapter 6).

1.19 Overall, most respondents strongly supported continued direct engagement by the FCA and other financial services regulators to foster innovation and ensure appropriate regulatory safeguards are in place at the outset. They particularly appreciated our practical engagement with innovators and welcomed the Innovate initiatives.

1.20 All respondents highlighted the global nature of DLT. Seeing a consequent need for international cooperation, they urged us to collaborate even more proactively with other national and international regulatory bodies and industry associations, to make possible a globally harmonised approach to DLT.

1.21 In the subsequent chapters, we cover in more detail the following issues that respondents discussed:

- Operational risk (including outsourcing and network security)
- Digital currency (including digital currency derivatives and ICOs)
- Digital asset trading and smart contracts
- Regulatory reporting
- Financial crime
- General data protection regulation

Next steps

1.22 We summarise our next steps in chapter 8. In brief:

- We will continue to monitor DLT-related market developments, and keep our rules and guidance under review in the light of those developments, although we have not identified a need to propose specific changes at this juncture.
- We will continue our close engagement with DLT use cases and industry stakeholders through our Innovate initiative.
- At the international level we will work closely with national and international regulatory bodies to shape regulatory developments and standards.
- At the domestic level we will engage further with other regulatory authorities to ensure a coordinated approach in the UK.
- Having already issued an alert warning consumers of the speculative nature and high risks of ICOs, we will gather further evidence on the ICO market and conduct a deeper examination of the fast-paced developments. Our findings will help to determine whether or not there is need for further regulatory action in this area. We have taken the immediate step of highlighting how an ICO-related innovative business proposition needs to be designed if it is to satisfy the 'consumer benefit' criterion for access to the facilities of our Innovation Hub (see chapter 3).

2 Operational risk

2.1 In our DP we observed that firms use a variety of systems to run their businesses, and that the integrity of these systems is, therefore, vital to our objectives of ensuring market integrity and consumer protection. It's critically important that firms have proportionate safeguards to deliver the availability, resilience, reliability and security of systems underpinning key regulated services. So DLT's prospective integrity and potential to provide such safeguards is key.

2.2 An important distinction when considering the operational risks of DLT is that between permissioned and permissionless networks. DLT networks are highly customisable and broadly distinguished by the type of network visibility and network access permitted:

- *Permissionless* networks allow general public visibility of transactions online and are open for broad participation.
- In contrast, *permissioned* networks typically feature a 'gatekeeper' who controls access.[4]

2.3 In the DP we asked about the prospective benefits and operational risks associated with DLT applications, and raised, in particular, the question of risk management in the context of permissionless networks. We raised issues such as the allocation of responsibilities and vulnerability to breaches of security.[5]

Summary of feedback

2.4 Nearly all respondents highlighted what they saw as the operational benefits of a DLT network, including enhanced resilience and transparency, a shared common view of a ledger, consistent time-stamping, digital signing of transactions and real-time processing. The consensus mechanism used in most DLT systems also ensures, in the view of respondents, that the ledger cannot be corrupted by one participant alone.

2.5 Many respondents thought that *permissioned* networks could enhance the efficiency of operational risk controls and that their deployment would not significantly change the character of the operational and conduct risks firms are already familiar with, particularly in the post-trade sector. Many respondents alluded to our outsourcing regime, saying it provided useful guidance on how to compliantly interact with third parties, including DLT system networks.

2.6 Many respondents also saw various additional benefits of using public, *permissionless* networks (e.g. low transaction fees, enhanced availability, standardisation and interoperability). At the same time they had some main areas of concern – dependence on a public network, the potential lack of a governance, dispute and regulatory framework, probabilistic settlement finality, and the degree of anonymity of interacting network participants.

4 We also note that DLT networks comprise not only permissioned and permissionless networks in their pure forms, but also hybrid forms in which the application of forms of security within an otherwise permissionless network creates a form of permissioned network.

5 In this section we refer to DP questions 1-4, 11, 12, 13 and 14.

2.7 Several respondents preferred permissionless DLT networks because closed DLT networks represented a barrier to market entry that could support oligopolies and anti-competitive behaviours, while potentially reducing operational transparency and network security.

2.8 However, respondents also suggested that applying DLT in financial services at a large scale might trigger some new or increased operational risks that would, in part, depend on the specific circumstances of each application. These risks might include coding errors (regarding whole networks and individual smart contracts), stability risks with newly-developed technology and inter-operability risks, as well as scaling, latency, data privacy and security concerns.

2.9 A few respondents also suggested a range of possible mitigants including improved governance, regulatory requirements and behavioural approaches.

2.10 Nearly all respondents were broadly supportive of our approach to managing operational risks. They recognised that firms – regardless of whether DLT is deployed or not – retain full accountability and responsibility for discharging all of their regulatory obligations and cannot transfer any part of this responsibility to a third party.

Our response

Ensuring operational soundness of firms and activities we regulate is paramount to us achieving our statutory objectives of financial system integrity and consumer protection. The use of DLT may affect firms' exposure to operational risk through changes to, and potentially reduced control over, people, processes and systems.

Nevertheless, we think using permissioned and permissionless DLT networks has the potential to enhance operational soundness. We consider good operational risk management as key to the realisation of operational benefits. Our approach is risk-based and proportionate, taking into account the nature, scale and complexity of a firm's operations.[6] The overall aim of our regulatory obligations is to ensure that firms appropriately identify and manage the operational risks associated with their activities, including their use of technology and third-party providers.

The use of DLT might affect how individual responsibility and accountability is allocated. Firms must allocate responsibilities appropriately, given the shared nature of DLT systems. Individuals' responsibilities under our Senior Managers and Certification Regime (SM&CR) will have to be clearly set out.[7]

Ultimately, specific operational risks will in part depend on the actual application of DLT. We expect firms to mitigate all relevant operational

6 Further general requirements on operational risks for firms are detailed in our Senior Management Arrangements, Systems and Controls sourcebook (SYSC) and apply as rules to all "common platform" firms and as guidance to all other firms. Firms should be aware of other specific requirements that may apply to them based on their business. For example, the Solvency II regulation includes specific obligations for insurers, and domestically we have additional guidance relating to insurers in SYSC.

7 The SM&CR aims at reducing harm to consumers and strengthening market integrity by making individuals more accountable for their conduct and competence. Currently this regime applies to deposit takers, but we are consulting on an extension to FCA solo-regulated firms.

risk appropriately in both a DLT and non-DLT environment, and to undertake appropriate due diligence before deciding to use particular solutions.

Outsourcing

2.11 Some respondents raised a concern about permissionless networks: they thought that permissionless networks could be incompatible with our outsourcing rules. They reasoned that, in their purest form, permissionless networks have limited governance, tend not to identify participants, and depend on a public network to validate and store transactions without any particular organisation supporting the network. These respondents said that only permissioned networks would be able to fulfil our outsourcing requirements.

Our response

Both permissionless and permissioned networks are highly customisable and can be used in a variety of settings to fulfil diverse functions. While some respondents argued that permissionless and public networks appear to be incompatible with our regulatory regime, we do not share this view: we believe that use of permissionless and public networks is not inherently incompatible with our regulatory regime. We do not discern any fundamental incompatibilities between the two.[8]

Our view is that firms will need to assess each case to see whether using a DLT network amounts to 'outsourcing' in the context of our regulatory requirements.[9] We do not consider that using a permissionless network always necessarily amounts to outsourcing in that context.

Thus, we do not consider that regulation necessarily prohibits firms from using public, permissionless DLT networks, provided appropriate risk management is deployed. So a firm's focus in each instance of DLT application should be on identifying and appropriately mitigating the associated operational risks.

The use cases in the box illustrate our openness to all forms of deployment of DLT, permissioned and permissionless, provided the operational risks are properly identified and mitigated.[10]

.

8 We also note that DLT networks comprise not only permissioned and permissionless networks in their pure forms, but also hybrid forms in which the application of forms of security within an otherwise permissionless network creates a form of permissioned network.

9 www.handbook.fca.org.uk/handbook/SYSC/8/?view=chapter and www.handbook.fca.org.uk/handbook/SYSC/13/9.html

10 In addition to our existing rules and guidance on outsourcing, we are also extending the SM&CR regime from banks to all firms authorised under the Financial Services and Markets Act. The timing for the extension will be set by HM Treasury but is expected to be in 2018. Under this regime, where a firm outsources an operational function to a third party, the firm will be required to explain clearly how responsibility for each outsourced function is allocated among its Senior Managers. See Consultation Paper CP17/25: www.fca.org.uk/publication/consultation/cp17-25.pdf

Sandbox use cases

In the Sandbox environment, two firms tested cross-border payments using a digital currency as an intermediate currency, resulting in cheaper and faster payments.[11] Both firms used a public, permissionless network to facilitate their services. We have not discerned any fundamental incompatibilities with the FCA's regulatory requirements in either of the firms' tests.

Another Sandbox firm tested the automated issuance and management of a regulated short-term debt instrument using a public, permissionless network to enhance system resilience and transparency for investors. Again, we have not discovered any fundamental incompatibilities with our regulatory requirements.

Network security

2.12 All respondents emphasised their view that security is at the heart of a DLT network. Potential security benefits were identified but implementing a DLT network could also lead to various security risks.

2.13 Nearly all respondents argued that the benefits mainly derive from the distributed nature of the network which leads to enhanced system and data resilience as well as record keeping and auditability. Respondents identified a broad range of potential security risks which range from simple coding errors (with potential implications for the whole network) through to security of network end points, weakness in encryption (potentially linked to advances in quantum computing) and design matters such as reducing the distributed nature of the network for cost reasons, and risks associated with key management and connections with systems outside the DLT network.

2.14 To mitigate these risks, many respondents suggested adhering to security frameworks and standards, such as the National Institute of Standards and Technology framework from the U.S. Department of Commerce[12], and relevant standards from the International Organisation for Standardisation.[13] Such an approach would provide for upgradable security, appropriate code scrutiny, adequate access controls and a modular or compartmentalised design. In addition, most respondents suggested storing sensitive data off-chain with file hashes and location references stored on-chain instead.[14] However, respondents also observed that models of DLT networks are evolving so there is no single best way to design or implement security.

Our response

Whatever technology is employed, and whatever the potential security advantages of DLT (which we welcome), we expect firms to actively manage their operational risks, including DLT network and security

11 See Sandbox Lessons Learned Report: www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf

12 www.nist.gov/cyberframework

13 The International Organization for Standardization is currently working on a DLT related standards, ISO/TC307. See: www.iso.org/committee/6266604.html

14 We also discuss this concept in connection with GDPR in Chapter 8.

risks, by implementing appropriate systems and controls. In particular, where technology and security are core to the delivery of a regulated service, we expect firms to give full attention to operational risk management.

Enforcement case

We take data security seriously and have fined a number of firms where we considered them to have failed to take reasonable care over its management.

For example, in 2010 we fined a regulated firm £2,275,000 for failing to take reasonable care to manage the security of customer data.[15] In this instance, the firm outsourced the processing of some of its general insurance customer data and the provider subsequently lost an unencrypted back-up tape during a routine transfer to a data storage centre. As there were no proper reporting lines or oversight mechanisms in place, the firm did not learn of the incident until a year later.

The event affected the personal information of 46,000 customers including their personal identity, bank account or credit card information. In some cases details about insured assets and associated security arrangements were also lost.

15 www.fca.org.uk/news/press-releases/fsa-fines-zurich-insurance-%C2%A32275000-following-loss-46000-policy-holders-personal

3 Digital currencies

3.1 The variety of digital currencies and their market capitalisation have grown rapidly over recent years.[16] While financial regulators around the world have taken different approaches to the proliferation of digital currencies and their increased use in financial services, most agree that current developments raise potential consumer protection and market integrity issues, and need to be watched closely. At the current (or recent) size of the digital currency market, compared to the traditional financial markets, the authorities concerned with financial stability[17] do not, at this juncture, see clear evidence of financial stability or systemic risks. We are closely monitoring developments in line with our own statutory objectives (see para 1.1), and have already put out two consumer alerts.

3.2 Digital currencies are not currently regulated by the FCA (nor by the Bank of England), provided they are not part of other regulated products or services. In the DP we asked whether the use of digital currencies for financial services carried different or more benefits and risks than currently available systems. We also broached the legal and regulatory issues associated with ICOs. Digital currencies can be used in various ways. In the DP we discussed two of them – digital currencies as a means of exchanging value, and digital currencies in the context of ICOs.[18] Here we add a third: digital currencies as an underlying or referenced asset.

Digital currencies as a means of exchanging value

3.3 When asked about potential benefits and risks of the use of digital currencies in financial services, most responses cited international payments and micropayments as areas which would most benefit from the use of digital currencies; this is because charging structures of digital currencies are independent of geography and transaction size. Several responses suggested that as digital currencies are not encumbered by legacy technology, they can settle payments more efficiently and improve competition. Respondents also suggested, however, that digital currencies' price volatility in relation to fiat currency exchange rates is a major drawback.

3.4 Most respondents argued that while immutable transactions increase certainty, the irreversibility of transactions removes any margin for error and can lead to the irrevocable loss of funds. This was said to be compounded by the decentralised governance of digital currencies, which eschew traditional corporate leadership structures, and thus make recourse almost impossible without irreversible changes to the protocol.

3.5 A few respondents further suggested that individuals who may be financially excluded – due to a lack of formal identity or insufficient address history – could use digital

16 In the year to date, the global market capitalisation for digital currencies has increased from £13.8bn to £154bn. See: https://coinmarketcap.com/charts/ and University of Cambridge Judge Business School's Global Cryptocurrency Benchmarking Study 2017, available at: www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

17 www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q302.pdf and www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

18 In this section we refer to DP questions 4, 6, 9, 11 and 12.

currencies, and their low barrier to entry, as a potential alternative. However, they thought these could not replace the full repertoire of services provided by existing current accounts.

3.6 Alongside the risks to consumers, wider challenges for integrating digital currencies into established financial services were highlighted. In particular, respondents identified the relative anonymity of digital currency wallets and transactions as a potential means of circumventing anti-money laundering regulations.

Our response

Digital currencies as an alternative or supplement to traditional payment mechanisms may, with sound risk management, enhance the delivery of financial services in the UK to the benefit of consumers. The volatility risk posed by the magnitude and mercurial nature of price fluctuations is of course one of the risks firms must adequately address. In particular, provided the risks are properly managed, permissionless networks have positive competitive potential in the context of value transmission, as our use cases suggest.

Sandbox use cases

Test data from several Sandbox firms have demonstrated the possibility of using digital currencies as intermediate currency to reduce the cost and processing time of money remittance, without compromising on security. The volatility of the digital currency used was, for instance, managed by locking in exchange rates with cryptocurrency exchanges before a transaction was executed.[19] Sandbox firms have further demonstrated that digital currencies and permissionless DLT networks can operate compliantly with the FCA's regulatory requirements to improve operational resilience and market integrity (for example in the context of debt instruments, money remittance, e-money or digital identity).

3.7 We are alive to the money laundering risks identified by respondents and the challenges posed to existing Money Laundering Regulations. The EU's proposed 5th Anti-Money Laundering Directive (5AMLD) will expand the scope of anti-money laundering regulation to certain services using digital currencies. In the meanwhile the FCA is actively exploring the scope for enhancing the efficiency and effectiveness of AML systems and controls through the application of new technologies (see also chapter 6).[20]

Digital currencies as an underlying or referenced asset

3.8 Digital currencies can also function as an underlying asset or point of reference for regulated financial services products, such as contracts for differences (CFDs),

19 www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf

20 In December 2017 we hosted an event discussing fintech innovation in anti-money laundering and digital ID. See www.fca.org.uk/firms/innovate-innovation-hub/events and http://fca.cvent.com/events/fintech-innovation-in-anti-money-laundering-digital-id/event-summary-737cfad59b384a08b2e48781a404e9ae.aspx

futures contracts, options, or exchange-traded funds (ETFs). Digital currencies are not currently regulated by the FCA but, if they are the underlying reference asset in a financial derivative, transferable security or collective investment scheme, the activities of firms relating to these instruments may well be subject to regulation. For example, providers offering CFDs, futures and ETFs may well be conducting regulated activities, and, if so, will be subject to our rules.[21]

3.9 We are aware of a current trend for market participants to introduce novel digital currency-related products. We have specific concerns in relation to CFDs that feature a digital currency as the underlying investment. We therefore cover this topic here even though it was not raised by our DP.

Contracts for differences (CFDs)

3.10 CFDs allow investors to gain indirect exposure to the price movements in an underlying asset, such as an index, a single stock equity, commodities or digital currencies.

3.11 We have noticed steady growth in the volume of CFD trades with a digital currency as the underlying asset, mainly Bitcoin and Ether. The market trend indicates that retail consumers are increasingly investing in these products to gain an exposure to digital currency without having to hold the underlying digital currency. This trend raises significant concerns about potential harm to retail consumers.

3.12 CFD providers contend that retail consumers may benefit from certain features associated with CFDs, such as helping mitigate the risk of losing digital currency funds via hacking or compromised private keys, or the ability to apply risk management tools (e.g. guaranteed stop-losses) that help manage their exposure. Although there is some merit to firms' claims, CFDs on digital currencies remain a complex, high-risk, speculative investment, primarily because of the interaction of high volatility and leverage. They are also vulnerable to manipulation of the value of the underlying asset. So they are unlikely to be appropriate for most retail clients. [22]

3.13 In the light of current market developments and our concerns about digital currency CFDs in particular, we published an investor warning in November 2017[23] to highlight the risks of investing in these products.

Initial coin offerings

3.14 Digital currencies can also be used in the context of ICOs, and the DP asked about the legal and regulatory challenges associated with them.[24]

3.15 An ICO is a digital way of raising finance online using digital currency and DLT. An ICO is an event where digital tokens (or coins) are offered and distributed to the public in exchange for investors' capital. During an ICO, prospective token purchasers usually

21 Consumers who invest in regulated products from FCA authorised firms have access to the Financial Services Compensation Scheme (FSCS) and individual complaints can be referred to the Financial Ombudsman Service.

22 On 6 December 2016, we published consultation paper CP16/40, which proposed a variety of enhanced business conduct rules (including stricter leverage limits and enhanced disclosure requirements). We have decided to delay making final conduct rules for UK firms providing CFDs to retail clients as we await the outcome of discussions regarding the possible use of EU-wide, temporary product intervention powers under Article 40 of the Markets in Financial Instruments Regulation (MiFIR).
See: www.esma.europa.eu/document/product-intervention-general-statement

23 www.fca.org.uk/news/news-stories/consumer-warning-about-risks-investing-cryptocurrency-cfds

24 In this section we refer to DP question 16.

exchange fiat currency or an established digital currency (such as Bitcoin or Ether) for an issuer's newly developed proprietary token that is related to a specific company or project, the nature of which can vary greatly. The value generated through an issue is typically directed towards the funding of projects, development of software or other related initiatives, although in some cases little to nothing materialises after a token issue.

3.16 Depending on a particular token's characteristics, certain rights may (depending upon the terms of the ICO) attach to the token entitling the holder to, amongst other things, a share of an initiative's future earnings, access to services provided by the company, use of a software application, or redemption versus a particular asset represented by the token.

3.17 The rapid proliferation of ICOs as an alternative way of raising funds for DLT projects has increased their profile and attracted significant market and media scrutiny over the last 12 months. Whilst many respondents in the technology community considered ICOs as having the potential to dynamise innovation and the development of the broader DLT and de-centralised application ecosystem, others raised concerns about the variety of attendant risks and potential harm to those who choose to 'invest'.

Our response

We published a consumer alert on ICOs in September 2017, highlighting the risks associated with them.[25] We stressed that ICO investments are high-risk and speculative in nature. The value of tokens may be extremely volatile and most ICOs are not regulated by the FCA and/or might be based overseas. So it is unlikely for most ICOs that investors will have access to UK regulatory protections such as the Financial Services Compensation Scheme[26] or the Financial Ombudsman Service.[27] We further stressed the high potential for ICO-related fraudulent activities and the inadequate documentation in so-called white papers that projects (often only in very early stages of development) tend to provide to prospective investors to assess a particular investment opportunity.

Furthermore, the nature of each token, project, service, company and so on, can vary greatly, making overall classification of ICOs from a legal perspective more difficult.

Depending on how they are structured, the tokens themselves and activities of participants within an ICO may fall within the FCA's regulatory perimeter (and these activities may be subject to relevant regulatory requirements). This needs to be determined case by case, subject to the particular characteristic of each ICO, as we stated in the consumer alert.[28] A more detailed regulatory analysis of ICOs is set out in Annex I.

A well-functioning ICO market, where issuers not only are sensitive to any regulatory obligations they have but actively take appropriate steps to manage the risk of harm to the public and the markets more broadly,

25 www.fca.org.uk/news/statements/initial-coin-offerings
26 www.fscs.org.uk/
27 www.financial-ombudsman.org.uk/
28 www.fca.org.uk/news/statements/initial-coin-offerings

can materially contribute to the development of DLT. We regard it as critical, however, that promoters of ICOs take the steps needed to allow fully informed decision-making by potential acquirers of their tokens.

A limited number of ICOs have engaged with the Innovation Hub when they form part of wider innovative business propositions that we assess to have the potential for consumer benefits. This includes a firm that has entered the regulatory Sandbox for controlled testing. Provided a proposition meets our eligibility criteria, this will continue to be possible. In the context of ICOs our consumer benefit criterion[29] means, among other things, that

- the ICO must fall within our regulatory perimeter and be fully compliant with UK and other relevant regimes, or
- if outside our regulatory perimeter, designed, promoted and governed in line with best practice, so that potential acquirers are properly informed about the proposition that is being marketed to them.

The ICO market is evolving at great speed. We intend to gather further evidence on market developments and to conduct a deeper examination of this fast-paced phenomenon. Our findings will help to determine whether or not there is need for regulatory action in this area.

We will continue to build on our collaborative efforts with industry and other national and international regulators and global standard-setters. And we will welcome further opportunities to engage with the technology and financial services community in relation to the development and the use of ICOs.

Sandbox use cases

A sandbox firm mirrored the traditional issuance process for a short-term debt instrument denominated in GBP, using a public, permissionless DLT network. This served to potentially streamline the traditional approach, for example by removing the need for registrars and nominees. The test was carried out in a way which demonstrated that it was possible to meet legal and regulatory requirements. The firm further tested the issuance of another instrument denominated in a digital currency. This system has the potential to reduce costs, and enhance transparency, accuracy and clarity in relation to the ownership of assets.

29 www.fca.org.uk/firms/project-innovate-innovation-hub/eligibility and www.fca.org.uk/firms/regulatory-sandbox/prepare-application

4 Digital asset trading and smart contracts

4.1 As we pointed out in the DP, possible uses of DLT go beyond digital currency (for the purposes of the exchange of value) and are of particular interest for the trading of assets, whether in the context of fully-digitised markets or as part of the underlying infrastructure of traditional market participants such as stock exchanges, central counterparties in securities clearing and settlement, and consumer-facing distributors. The DP asked for viable DLT use cases in the context of asset management on the one hand, and securities issuance and trading on the other. The DP also asked how market participants viewed the use of smart contracts and whether there were already live examples.[30]

4.2 Most respondents agreed that DLT applications could be beneficial for record-keeping. Several responses described specific use cases that have already been developed, including examples of a custodian bank that began administering a private equity fund using DLT earlier in 2017, and a commercial provider of DLT-based custodial services. One firm has defined and developed a prototype investment book of record (which would enable it to have a single, up-to-date and accurate statement of its investment positions and outstanding transactions). Another is developing DLT-powered fund distribution systems for the collection of investment orders and shareholder record-keeping.

4.3 Several respondents listed a variety of other possible examples of use in areas such as collateral management, corporate actions, loan syndication, short-term debt, improved funding processes and alternative financing, and standardised securities processing. Some suggested that advances in digital currencies and protocols around e-wallets could lead to improved, more cost-efficient clearing processes with reduced settlement times. Some of the potential service improvements claimed for DLT-based solutions include:

- shared views of consumer investments
- faster, more accurate valuation processes, particularly when various parties are inputting data
- automated update notifications and payments
- time-stamped records and an auditable trail of information that can populate multiple databases
- enhanced risk management and reporting

4.4 Some of the above-mentioned improvements could be facilitated by smart contracts.[31] Respondents regarded smart contracts as a powerful workflow management tool that allows the same view of the state of a specific transaction to all participants involved, increasing speed and accuracy of execution with real-time information, while reducing operational costs by eliminating manual checks

30 In this section we refer to DP questions 5, 8, 9, 10, 15 and 17.

31 As set out in the DP, we define smart contracts as 'blockchain functionality to execute pre-determined commands without further human intervention'.

and reconciliation. In some instances, for example in cash securities markets, smart contracts could also reduce settlement risk. However, legal uncertainty remains around the nature and particularly the enforceability of smart contracts. Further, respondents cited the main risks as faulty code, malicious oracles (i.e. external data feeds) and erroneous, unwanted (non-)executions. Although there is general confidence that suitable standards and templates for smart contracts will be developed, respondents noted that smart contract-based trading systems need to integrate short selling, securities lending and borrowing, and netting functionalities.

4.5 A few respondents reported on tested smart contract use cases in the context of automated payments and post-trade processes, insurance claims processing using oracles, mutual funds subscription, trade finance and invoice matching.

4.6 One respondent commented that the greatest potential for DLT to disrupt securities trading is through the decentralisation of exchanges, with orders being placed and filled directly by the DLT network rather than being centrally managed. It was also pointed out that the impact on different types of market participants will become more apparent over time.

4.7 Other possibilities in relation to exchanges and central counterparties include:

- incorporating DLT in replacements for legacy systems and improved existing systems
- offering new products and applications to market participants on a commercial basis
- deploying DLT in market segments or products where there is not yet any sophisticated post-trade infrastructure

Our response

We believe that DLT could bring several benefits to securities markets, notably more efficient post-trade processes and enhanced reporting and data management capabilities, as well as the possibility of reduced costs. It has the potential to form the core of a central securities depository, providing the definitive record of legal ownership and the central infrastructure to maintain this data. It might also help to improve straight-through processing, offer real-time settlement and the elimination of settlement risk, and lead to disintermediation such as the possible removal of the roles played by custodians and settlement agents.

But a number of challenges need to be addressed before substantial benefits can materialise. In particular, it is unclear whether DLT might be adopted broadly across securities markets or remain limited to niche uses, although central banks deciding in future to issue or support a digital currency might spur market participants to invest more resources in DLT. The use of central bank digital currency could enable real-time 'delivery-versus-payment' settlement, reducing potential friction between DLT-based trading and settlement systems on the one hand, and non-DLT based payment systems on the other. Moreover, since it is unlikely that DLT will replace existing market infrastructure for some

time to come, it would be reasonable to assume that a combination of multiple DLT systems and legacy systems would need to operate with one another. Legal issues such as the legal status of digital assets and the enforceability of smart contracts, would have to be clarified.

Moreover, adoption of DLT could bring unintended consequences: for example, DLT-based real-time settlement could eliminate the need for equity clearing, but market users might have a limited appetite for such a development because of the potential loss of opportunities for netting and the absence of the anonymity that clearing currently provides to trading parties. We note there are also UK-specific features of the market that might pose challenges to the deployment of DLT, such as the continued existence of materialised securities held by some smaller private investors in public companies.

It is currently premature to fully appreciate potential DLT–related changes in the securities market as this technology is still evolving.[32] At this juncture we do not intend to propose DLT-driven rule changes in the context of asset management or securities markets. We will continue to monitor market developments closely and directly engage with stakeholders to ensure our rules are keeping pace with technological developments.

Sandbox use cases

A Sandbox firm tested the use of DLT to enable UK private limited companies to digitally represent and manage their shares and corporate governance processes, resulting in improved efficiency and significant cost savings for issuing firms. Changes of share ownership affected on the firm's platform were directly updated in the Companies House register. The test demonstrated that it would be possible to compliantly use DLT in that context, but the firm concluded that the proposition itself was not commercially viable so decided not to pursue it. One function of the Sandbox is to give insights into commercial viability at an earlier stage than would otherwise be possible.

Various Sandbox firms used the smart contract functionality in payments solutions to provide greater transparency to payers and to allow payments to only be made on the fulfilment of certain conditions.

32 We take account of the European Securities Markets Authority's ('ESMA') February 2017 report on the use of DLT applied to securities markets, which provides an insight into potential, future changes DLT could facilitate in securities markets. This report can act as a supplement to our findings.
The report also provides ESMA's analysis of key benefits (more efficient post-trade processes, enhanced reporting and data management capabilities and reduced costs) and challenges (scalability, interoperability, and common standards, access to central bank money, governance and privacy issues) of DLT when applied to securities markets. See: www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

5 Regulatory reporting

5.1 In the DP we suggested that in certain situations DLT might, by enabling a report to be generated at the same time as an order is placed, help to mitigate the potential operational risk of reconciling multiple legacy systems interacting with each other. We asked whether there were already live-tested use cases for regulatory reporting based on DLT, and what challenges firms were facing when implementing those solutions.[33]

5.2 Many respondents suggested that DLT solutions have the potential to facilitate the delivery of regulatory requirements more efficiently than current systems. They said they could offer regulators a direct view of transactional data in real time and on demand, resulting in substantial cost reductions for firms and regulators alike.

5.3 Most of those respondents also suggested that DLT could allow regulatory reporting to be consolidated across various local and international regulators, in cases where data ought to be coherently reported to multiple parties who are interested in any one particular transaction (e.g. financial and tax regulators). They stressed that careful system design would be necessary to ensure the sensitive data contained in regulatory reports are properly handled. This included strong access controls as well as the ability to issue corrections without undermining immutability. Some noted that a failure to achieve a sufficient network effect or 'critical mass' might reduce potential benefits of a DLT system.

5.4 To realise the benefits of DLT, and justify implementation costs, respondents regarded it as crucial that the FCA continues to develop its technological capabilities, including through hiring appropriate technology talent. They suggested that strong international cooperation would be critical to minimise the risk of regulatory arbitrage and avoid the unnecessary fragmentation of technical standards.

5.5 Some respondents shared their experience with various DLT use cases, such as testing the use of smart contracts to conduct internal and regulatory checks or manage derivatives post-trade processing. They encouraged us to develop smart contracts with predetermined codified rules to automatically ensure firms' compliance when reporting data.

Our response

We agree with the potential benefits of adopting DLT as a RegTech solution and also acknowledge the associated risks. In particular, we believe that using DLT for regulatory reporting purposes could reduce costs to both firms and regulators and significantly improve our access to data. This would, in turn, allow us to identify areas of emerging risk more efficiently and improve the speed and accuracy of our response.

We have explored a wide range of RegTech opportunities through our *Supporting RegTech* call for input, technology Showcase events, regulatory Sandbox and our TechSprints. We have observed increased

33 In this section we refer to DP question 6.

interest on the part of RegTech firms in testing their solutions in a Sandbox environment.

We are involved in project 'BARAC' (*Blockchain Technology for Algorithmic Regulation and Compliance*)[34], a 'proof of concept' to thoroughly investigate legal and regulatory implications of the use of DLT for automation of regulation and compliance. This interdisciplinary research group comprises representatives of international policy makers, academia, industry and regulators and is led by University College London. We contribute to the research efforts and provide actual DLT use cases, such as Project Maison (see box below), as case studies for in-depth research. We will continue our efforts around standardised reference data.

DLT is not the only technology that could improve regulatory reporting. So we continue to explore other possibilities, such as model-driven machine-executable regulatory reporting. If successful, this would allow firms to map their regulatory obligations directly to the data they hold, creating the potential for automated, straight-through processing of regulatory returns.

We are encouraged by the strong level of interest in RegTech by industry stakeholders, and as a result will continue to prioritise our RegTech initiatives as part of FCA Innovate. We invite stakeholders interested in working with us on RegTech to review our work programme and consider participating in our TechSprints or Showcase events. More specific information is available at: www.fca.org.uk/firms/regtech.

Project Maison case study

As part of our RegTech initiative, we have worked with the R3 consortium and two major banks to develop a prototype application for regulatory reporting of mortgage transaction data using the Corda DLT platform. By hosting a 'regulator node' on the network, we are able to receive real-time mortgage transaction reports from participating banks in a test environment. The prototype records, executes and manages financial agreements, with DLT used to enable secure communication between participants.

This collaboration has demonstrated how DLT's shared data model can enable continuous regulatory reporting for financial institutions at comparatively low cost. Mortgage data are reported to us within seconds of the transaction being finalised within a bank, which is a marked improvement over current quarterly reporting. As the prototype has been successful with benefits to both us and the banks involved, we are now seeking to move to a pilot with more participants and live mortgage data.

34 http://blockchain.cs.ucl.ac.uk/barac-project/

6 Financial crime

6.1 The DP suggested that a DLT network shared among multiple firms could enable more effective transaction monitoring, for example by replacing paper trails with easily auditable digital ones, or by enhanced traceability of information about transactions. Such developments might reduce financial crime and the cost of countering it. In the DP we asked how DLT might be deployed to mitigate financial crime risks and whether there are barriers to adoption of those systems.[35]

6.2 Most respondents argued that DLT systems – while still in their infancy – could facilitate more effective financial crime monitoring systems through enhanced transparency of transactions and the use of 'big data' analysis. Some said DLT could facilitate the secure sharing of data such as transaction records, concerns about suspicious activity and customer due diligence (CDD) data between financial services firms. By aggregating additional (third party) information, firms could be able to gather a more accurate client profile which supports their efforts to detect and prevent money laundering.

6.3 In particular, it was suggested that DLT networks could be capable of storing already-verified, individual or corporate CDD data to enable 'shared know-your-customer (KYC) solutions' that streamline consumer onboarding processes and eventually could function as a form of digital identity (that could be referenced to every single interaction with the network). But respondents argued that current reliance provisions, in particular the liability rules in the Money Laundering Regulations 2017 (which are legally driven by the underlying EU directive), do not incentivise firms to share CDD information or foster any enhanced level of cooperation.

6.4 A few respondents reported various proofs of concept, including the use of Zero-Knowledge-Proof systems that do not reveal the underlying information to verify one's identity while still confirming it to third parties.

Our response

We oversee steps taken by financial services firms to meet their obligations related to the effective detection and prevention of financial crime.

The responses received often echoed the findings of our recently-published report on how new technologies, such as DLT, could streamline industry's efforts to tackle money laundering more efficiently.[36]

DLT has the potential to provide a more robust, tamper-proof record of transactions and, as a result, improve data quality while reducing the likelihood of fraud. For this reason we believe that using DLT does not automatically introduce or increase fundamental financial crime risks. We have, however, observed the denial of banking services to a

35 In this section we refer to DP question 7.
36 www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf

number of firms, particularly those who leveraged DLT to facilitate their services.[37] Although there might be many and complex drivers behind such decisions, we believe that deploying this technology should not result in a wholesale denial of access to traditional banking services for firms.

Provided firms appropriately assess and mitigate risks associated with the use of innovative technologies, we welcome their application to enhance firms' efficiency and accuracy in detecting and preventing suspicious activity, while lowering firms' compliance costs and streamlining customers' experience.[38] We are very keen to keep exploring how the use of DLT can support firms and regulators in fighting financial crime more efficiently.

Moreover, we believe the use of DLT has the potential to facilitate enhanced and more efficient cooperation amongst firms (and regulators) to aid their fight against financial crime, for example by providing a mechanism for sharing intelligence and data. However, we note that those systems currently face challenges that appear to stem from firms' unwillingness to share sensitive information (such as copies of identity documents or concerns about a customer's potentially criminal behaviour), and their need to comply with, for example, data protection requirements. So we intend to continue contributing to joint efforts to address these challenges, such as the Joint Money Laundering Intelligence Taskforce[39] which aims to aid voluntary information sharing between industry and the regulatory authorities.

In addition to our analytical work on how new technologies could be used to tackle money laundering activities,[40] we have been strongly encouraged to continue our support via Innovate for firms, market participants and technology providers alike, that propose new ways of addressing financial crime risks. On the back of the latest Innovate event in December 2017 where we discussed innovation in the context of AML and digital ID, we are currently planning our first global TechSprint. This event will convene international participants to explore technological solutions that have been presented at our event in December.[41]

In some instances, the current regime may need to evolve as more sophisticated tools become available. One of the challenges, for example, is the current reliance provisions in the Money Laundering Regulations. We believe that changes to this regime are worth exploring further.

This is, however, an idea for longer-term reforms which would require renegotiating of international standards, such as the recommendations set out by the Financial Action Task Force.[42] Our direct engagement with

37 www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf
38 Rob Gruppetta speech, 10 November 2016. See: www.fca.org.uk/news/speeches/effectiveness-proportionality-financial-crime-priorities.
39 www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit
40 www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf
41 www.fca.org.uk/firms/regtech/techsprints
42 www.fatf-gafi.org/

firms experimenting with DLT-based approaches, in the Sandbox and elsewhere, has helped to form our view and shape our contributions to these debates.

We will continue our fruitful dialogue with industry and host particular events for market participants and technology providers to discuss financial crime issues in the future.[43]

Sandbox use case
A Sandbox firm tested DLT-based client onboarding, including automated verification of documents and the possibility of sharing CDD relevant information with third parties. Another Sandbox firm is currently preparing to test a DLT-based money remittance and transaction monitoring system that leverages machine learning to enhance the accuracy of detecting suspicious transactions.

43 In December 2017 we hosted an event discussing fintech innovation in anti-money laundering and digital ID. See www.fca.org.uk/firms/innovate-innovation-hub/events and http://fca.cvent.com/events/fintech-innovation-in-anti-money-laundering-digital-id/event-summary-737cfad59b384a08b2e48781a404e9ae.aspx

7 General data protection regulation

7.1 The DP posed no explicit question about the General Data Protection Regulation (GDPR), but noted the challenge of firms managing their obligations under the data protection regime. Given the possibility of disseminating information to an entire, potentially public and permissionless, DLT network (that is capable of storing immutable data), several respondents suggested that the GDPR, which will be supplemented in the UK by a new Data Protection Act (both effective from May 2018), might be at odds with core features of most DLT applications. Respondents also perceived tension between the right to erasure, commonly known as the 'right to be forgotten', from search engine results, and the immutability of data offered by DLT systems.

7.2 While some respondents challenged the possibility of GDPR-compliant DLT applications, others shared how their particular DLT solution – compared to more traditional database technologies – provided a more efficient way of complying with GDPR requirements (e.g. by storing sensitive data off-chain with file hashes and location references stored on-chain instead). Further, respondents asked for FCA guidance on data protection and compliance rules.

Our response

While we recognise there are concerns, the Information Commissioner's Office[44] oversees, regulates and enforces GDPR in the UK. So we encourage firms to follow available guidance from the Commissioner. We will continue to work with the Information Commissioner's Office as further use cases emerge and develop.

At this stage, we have not identified any substantial incompatibilities between our Handbook, including the management of CDD data or effective access to data obligations, and the GDPR's requirements. Consequently, we do not see a material need for further FCA guidance on this issue and are confident that firms will be able to comply with both our current Handbook and the new GDPR requirements. This holds true for DLT solutions, whose compliance with both regimes can only be determined case by case.

While there are significant changes required by GDPR, we believe that these and the use of DLT have the potential to improve the way in which firms collect, store and process private information, resulting in significantly improved consumer outcomes.

44 https://ico.org.uk/

8 Next steps

8.1 At this stage, we believe that our current regulatory requirements appropriately reflect our strategic objectives of consumer protection, competition and market integrity in the context of expected uses of DLT. Respondents shared with us various use cases in the context of payments, asset management, securities trading, financial crime and regulatory reporting. Having assessed that feedback along with respondents' comments and our own experience with DLT applications, we do not see a clear need to propose any changes to our Handbook at this time. We will keep the position under review.

8.2 The DP started the dialogue on potential benefits and risks associated with the use of DLT in financial services. The responses we received informed our understanding of the stage of development of DLT and the market participants' perceived risks and opportunities of this nascent technology. The findings will inform further discussion with stakeholders and actively shape our decision on future areas of focus (such as AML) and our immediate next steps. We will:

- **Observe** We will continue to monitor DLT-related market developments and engage with stakeholders. We are equally committed to continuing to explore other technological advances, such as machine-executable regulatory reporting, as part of our RegTech initiative.

- **Engage** The responses received encourage us to maintain our level of direct engagement with financial services and technology firms that propose new ways of delivering financial services. We are encouraged by the continued demand for our Innovate initiative. We will continue to host themed events for stakeholders and established new ways of engaging, such as our Showcase days. Further, we intend to continue developing our own technological capabilities and increase participation in testing activities, particularly around the use of new technology for regulatory reporting purposes.

- **Gather evidence on ICOs** We intend to gather further evidence on the ICO market and conduct a deeper examination of this fast-paced development. Our findings will help to determine whether there is need for further regulatory action. Innovative businesses whose proposition includes an ICO can have access to our Innovation Hub, including the regulatory Sandbox, if the relevant eligibility criteria are met.

- **Collaborate internationally** We recognise the international aspect of DLT and therefore intend to work closely with industry and other national and international regulatory bodies and global standard-setters. Our experience with DLT will help to shape international discussions and support efforts towards a globally harmonised approach.

- **Collaborate domestically** We will continue to engage with domestic stakeholders, such as the Bank of England and the Information Commissioner's Office, to ensure a coordinated approach towards DLT in the UK.

8.3 Encouraged by the positive feedback received, we will maintain a proactive and supportive approach to technological innovation. We encourage innovators from all sectors to visit our website www.fca.org.uk/firms/fca-innovate and consider ways of engaging with us.

Annex 1
Regulatory considerations on Initial Coin Offerings

1. Under the Financial Services and Markets Act 2000 (FSMA), it is a criminal offence (punishable by up to two years in prison, or a fine, or both) for a person to carry on activities in breach of the general prohibition in FSMA, which states that no person may carry on regulated activity in the United Kingdom, or purport to do so, unless that person is an authorised person or an exempt person. If an authorised person carries on regulated activity for which it does not have the relevant permission, that person could be subject to disciplinary action by the FCA (levying of fines, removal of permissions, etc). In addition and in either case, agreements may be rendered unenforceable if entered into by persons without the relevant permission(s). Furthermore, a person may not communicate, in the course of business, an invitation and inducement to engage in investment activity unless that firm is authorised or the content of the communication has been approved by an FCA (or EEA) authorised firm.

2. Whether a participant in an Initial Coin Offering (ICO) requires authorisation will turn, generally, on whether they will be carrying on activities by way of business in the United Kingdom that relate to instruments which could be 'specified investments' (such as shares, instruments creating or acknowledging indebtedness like bonds or debentures, units in a collective investment scheme, or derivative instruments like options, futures or contracts for differences) and whether those activities constitute 'regulated activities' (for example, dealing in such specified investments, arranging transactions in those investments, advising on them or operating a collective investment scheme). The categories of specified investment and regulated activities are set out in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 ('RAO').

3. If an ICO does involve the issue of an instrument which is capable of being a specified (i.e. regulated) investment, participants in the ICO (such as intermediaries arranging investment by investors in the issuer, or advising investors) may require authorisation (if they are not authorised already) and may be subject to relevant regulatory requirements which may apply to those regulated activities (such as, for example, conduct of business requirements set out in the Conduct of Business Sourcebook (COBS) of the FCA Handbook, and the FCA's Principles for Business).

4. ICO issuers (and firms acting for the issuer) may also need to consider if promotional materials issued in relation to an ICO amount to a communication which is an invitation or inducement to engage in investment activity (i.e., a financial promotion). As explained above, a firm must not issue a financial promotion unless the content has been approved by an FCA authorised person, or the firm issuing the promotion is an FCA authorised person itself. Authorised firms communicating or approving a communication which amounts to a financial promotion in relation to an ICO will need to comply with the financial promotion provisions in the COBS sourcebook (see COBS Chapter 4).

5. Some tokens may also constitute transferable securities (as defined in the Markets in Financial Instruments Directive) and therefore may fall within the prospectus regime. A prospectus is required in the circumstances laid down by the Prospectus Directive as implemented by sections 85 and 86 of FSMA. Under these provisions, unless an exemption applies, an approved prospectus is required when transferable securities are offered to the public in the UK or are admitted to trading on a regulated market in the UK. Various exemptions from the requirement to produce a prospectus are available in relation to public offers or an admission to trading.

Contravening sections 85(1) or (2) of FSMA is a criminal offence. Those contemplating involvement in the issuance and distribution of tokens should carefully consider whether the tokens constitute:

- transferable securities and whether the prospectus regime will apply
- another kind of specified investment and if their activities could constitute a regulated activity.

6. Firms issuing promotional materials in relation to ICOs should also consider if those materials amount to a financial promotion, or whether a prospectus is required under the Prospectus requirements. In addition, digital currency exchanges that facilitate the exchange of certain tokens should consider if they need to be authorised by the FCA to be able to deliver their services.

7. Ultimately it is a firm's responsibility to assess its position under the relevant law and the regulatory regime. A firm might find the FCA's Perimeter Guidance Manual (PERG)[1] helpful when assessing its regulatory position. If a firm is unclear about its status, we encourage obtaining independent legal advice before engaging in business activities.

1 www.handbook.fca.org.uk/handbook/PERG.pdf

Annex 2
Abbreviations used in this paper

5AMLD	5th Anti-Money Laundering Directive
AML	Anti-Money Laundering
CDD	Costumer Due Diligence
CFD	Contract for Differences
COBS	Conduct of Business Sourcebook
DLT	Distributed Ledger Technology
DP	Discussion Paper
EEA	European Economic Area
ETF	Exchange-Traded Fund
FCA	Financial Conduct Authority
FSMA	Financial Services and Markets Act 2000
GBP	Great British Pound
GDPR	General Data Protection Regulation
ICO	Initial Coin Offering
KYC	Know-Your-Costumer
PERG	Perimeter Guidance Manual
POC	Proof-of-Concept
RAO	Financial Services and Markets Act 2000 (Regulated Activities) Order 2001
RegTech	Regulatory Technology

SM&CR	Senior Managers and Certification Regime
SYSC	Senior Management Arrangements, Systems and Controls Sourcebook

We have developed this Feedback Statement in the context of the existing UK and EU regulatory framework. The Government has made clear that it will continue to implement and apply EU law until the UK has left the EU. We will keep the proposals under review to assess whether any amendments may be required in the event of changes in the UK regulatory framework in the future.

All our publications are available to download from www.fca.org.uk. If you would like to receive this paper in an alternative format, please call 020 7066 9644 or email: publications_graphics@fca.org.uk or write to: Editorial and Digital team, Financial Conduct Authority, 25 The North Colonnade, Canary Wharf, London E14 5HS

Pub ref: 005474

25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk