CONSULTATION PAPER NO.138

REGULATION OF SECURITY TOKENS

29 MARCH 2021

PREFACE

Why are we issuing this Consultation Paper?

1. This Consultation Paper (CP) seeks public comment on our proposals for regulating Security Tokens. These proposals are designed to provide a regulatory regime for activities relating to Investments that:

    a) are a digital representation of rights and obligations, created, stored and capable of being transferred electronically – using distributed ledger technology (DLT) or similar technology; and

    b) confer rights and obligations which are either the same as those conferred by Investments (e.g., a share, debenture or futures contract), or are substantially similar in nature, purpose or effect as those conferred by Investments.

    These Investments are collectively referred to as 'Security Tokens' (although the rights available to their holders can vary).

What is not covered under this Consultation Paper?

2. There are other tokens, in addition to Security Tokens, which are created, issued and distributed using DLT and similar technology, which are not covered in these proposals. These other tokens are commonly referred to, by regulators, as exchange tokens, utility tokens, etc. They also have more colloquial names such as stablecoins and cryptocurrencies.

3. While we recognise the importance of these other tokens, and the need to have an appropriate regulatory framework for them, we have decided first to develop a regulatory framework for regulating Security Tokens, for a number of reasons:

    a) the enquiries we have received to set up in the DIFC are mainly from persons proposing to conduct business activities relating to offering and trading Security Tokens;

    b) the precise manner, form and extent of regulation of other tokens is still evolving, although regulators across the globe are taking significant steps to cover this area; and

    c) the policy position on tokens that purport to act as money or quasi-money, i.e. providing means or proxy for legal tender, needs to be carefully designed to be aligned with the approach of the monetary authorities in the UAE, which are currently developing their own policy in this area.

    We propose to release in the near future a second set of proposals setting out our approach to regulation of other tokens, such as exchange tokens and utility tokens.

Who should read this CP?

4. The proposals in this paper will be of interest to:

    a) issuers of Security Tokens;

    b) Authorised Market Institutions (AMIs) wishing to admit Security Tokens to trading, or clearing or settlement, on their facilities;

c) Operators of Alternative Trading Systems wishing to trade Security Tokens on their facilities;

d) digital wallet service providers who provide custody and storage of Security Tokens;

e) Authorised Firms wishing to undertake other Financial Services relating to Security tokens, such as dealing in, advising on, or arranging transactions relating to, Security Tokens, or managing discretionary portfolios or collective investment funds investing in Security Tokens;

f) persons undertaking technology support or provision;

g) persons who intend to carry out the activities specified above; and

h) persons providing legal, accounting, audit, or compliance services in the DIFC.

Terminology

5. Defined terms have the initial letter of the word capitalised, or of each word in a phrase. Definitions are set out in the Glossary Module (GLO). Unless the context otherwise requires, where capitalisation of the initial letter is not used, the expression has its natural meaning. Some commonly used terms in this paper are noted below.

Term	Meaning
Crypto asset or token	a digital representation of value, rights and obligations that are created, stored and transferred electronically, using distributed ledger technology (DLT) or similar technology
Distributed Ledger Technology (DLT)	a class of technologies that support the recording of encrypted data: (i) held on a distributed ledger; (ii) electronically accessible, from multiple locations, by a network of participants; and (iii) that can be updated by those participants, based on agreed consensus, protocol or procedures (i.e. distributed consensus).
Security Token	a token that confers rights and obligations that are: (i) the same as those conferred by a share, debenture or futures contract (Investments); or (ii) substantially similar in nature purpose or effect, to those conferred by Investments.
Safeguarding and administration (custody) of Security Tokens	holding or controlling Security Tokens on behalf of third parties by holding or having access to those assets through private keys
Operating a facility that trades Security Tokens	operating or managing an infrastructure or facility where multiple third party buying and selling interests for Security Tokens

	can interact in a manner that results in a contract for the sale or purchase of the Security Tokens
Digital Wallets	a software application or other tool which is used to control, safeguard or manage public and private cryptographic keys (or their equivalent) associated with Security Tokens
Distributed consensus	the agreed consensus, protocol or procedures for verification, confirmation and updating data stored on a DLT application by its participants

What are the next steps?

6. Please send any comments using the online response form. You will need to identify the organisation you represent when providing your comments. The DFSA reserves the right to publish, including on its website, any comments you provide. However, if you wish your comments to remain confidential, you must expressly request so at the time of making comments, and give your reasons for so requesting. The deadline for providing comments on this consultation is 29 April 2021.

7. Following the public consultation, we will proceed to make the relevant changes to the DFSA Rulebook, reflecting as appropriate points raised in consultation. You should not act on the proposals until the relevant changes are made. We will issue a notice on our website when this happens.

Structure of this CP

Part I – Background;

Part II – Definitional issues relating to Security Tokens;

Part III – Operating a facility for trading and clearing Security Tokens;

Part IV – Issuers of Security Tokens;

Part V – Other Financial Services relating to Security Tokens;

Part VI – Other issues;

Appendix 1 – Benchmarking;

Appendix 2 – Draft Amendments to the Markets Law;

Appendix 3 - Draft amendments to GEN;

Appendix 4 – Draft amendments to AMI;

Appendix 5 – Draft Amendments to COB;

Appendix 6 – Draft amendments to PIB;

Appendix 7 – Draft amendments to MKT;

Appendix 8 – Draft amendments to CIR;

Appendix 9 – Draft amendments to IFR;

Appendix 10 – Draft amendments to FER;

Appendix 11 – Draft amendments to GLO; and

Annex 1 – Questions in this consultation paper.

Part I Background

Introduction

8. Security Tokens are a sub-set of a class of assets referred to as digital assets, virtual assets, crypto assets, digital tokens and other similar terms. There are no definitive or exhaustive definitions of these terms, but there are many descriptions, and for the purposes of this paper we will use the generic terms crypto assets or tokens. This is reflective of the evolving nature of DLT and similar technologies that underpin these instruments, and the challenge that regulators face in identifying and addressing risks resulting from the use of such technologies.

9. The aim of our proposals, as with the other regulators we have benchmarked against, (see below), is to:

   a) clarify the application of the financial services regime to persons undertaking activities that involve or relate to Security Tokens; and

   b) put in place a consistent, risk based and proportionate application of the financial products and financial services regulation to Security Token-products, services and activities, which addresses:

      i. investor and consumer protection needs;

      ii. market integrity risks;

      iii. financial stability risks (although these are not considered by most commentators to be widely prevalent at this stage); and

      iv. crucially, AML/CTF considerations.

Benchmarking

10. We have reviewed the range of approaches adopted in other jurisdictions relating to the regulation of Security Tokens. The jurisdictions that we looked at are at different stages of development of their regulatory response in this area, such as the UK, EU, ADGM, Singapore, Japan, Gibraltar and Malaysia. We have also looked at the international standard setters, particularly IOSCO,[1] where their approach is still at a tentative stage. We considered in detail the EU approach[2] and relevant ESMA[3] material, which is relatively advanced. We have included relevant jurisdictional practices and approaches in reference to the specific recommendations proposed, and attached a summary of benchmarking at Appendix 1.

What are Crypto Assets?

11. We set out below what crypto assets are, including their key characteristics, before turning to what Security Tokens are, to which the proposals in this paper apply.

---

1 IOSCO released in February 2020 a final report on 'Issues, Risks and Regulatory considerations relating to Crypto-Asset Trading Platforms'.

2 Proposal for regulation of Markets in Crypto Assets (MICA), issued by the European Parliament and the European Council in September 2020.

3 'Initial Coin Offerings and Crypto-assets' – 9 January 2019, ESMA50-157-1391 ('the ESMA advice').

What are crypto assets?

12. The Financial Stability Board's report on crypto asset markets[4] describes:

    a) a crypto asset as '*a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value*';[5]

    b) distributed ledger technology (DLT) as '*a means of saving information through a distributed ledger, i.e., a repeated digital copy of data available at multiple locations*'; and

    c) cryptography as *'the conversion of data into private code using encryption algorithms, typically for transmission over a public network'*.

13. There are other descriptions of crypto assets. For example, the ESMA advice notes that crypto assets are a relatively new class of assets, where the market is evolving, and goes on to provide an expansive description of crypto assets as:

    '… a type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT). There are a wide variety of crypto-assets. Examples of crypto-assets range from so-called cryptocurrencies or virtual currencies, like Bitcoin, to so-called digital tokens issued through Initial Coin Offerings (ICOs). Some crypto-assets have attached profit or governance rights while others provide some consumption value. Still others are meant to be used as a means of exchange. Many have hybrid features. Crypto-assets are relatively new and the market is evolving.'

14. IOSCO, in its final report on 'Issues, risks and regulatory considerations relating to crypto-asset trading platforms', describes crypto assets as '*a type of private asset that depends primarily on cryptography and DLT or similar technology as part of its perceived or inherent value, and can represent an asset such as a currency, commodity or security, or be a derivative on a commodity*.'

What is Distributed Ledger Technology (DLT)?

15. Distributed Ledger Technology (DLT) is a mechanism for recording authoritative information on a distributed ledger by means of an agreed consensus process. DLT uses cryptography to validate and store transaction information through pairs of keys: a public key, which is publicly known and essential for identification, and a private key, which is kept secret and used for authentication and to claim ownership rights over crypto assets.

16. A crypto asset is created, stored and transferred using a DLT application, using three fundamental pieces of information:

---

4 Financial Stability Board's report on 'Crypto-Asset markets – potential channel for future financial stability implications' – October 2018.

5 HM Treasury (UK), in its January 2021 consultation, describes a crypto asset as a 'digital representation of value or contractual rights that can be transferred, stored or traded electronically, and which may (though does not necessarily) utilise cryptography, distributed ledger technology or similar technology'. This description does not specify that DLT and cryptography are necessary features, while the EU specifically refer to the use of DLT and similar technology, as well as cryptography, as an essential element of crypto assets.

a) an address;

b) a public key corresponding to that address, and

c) a private key, also corresponding to that address.[6]

Functionally, the person holding the private and public key can claim ownership of the crypto asset, recorded on the distributed ledger. The most common types of crypto assets at present appear to be those issued using DLT applications that are permissionless (i.e. allowing public access), such as Bitcoin and Ether.

17. However, as noted before, the proposals in this paper are not designed for cryptocurrencies or virtual currencies, or other instruments of exchange. Instead, these proposals are designed for Security Tokens, because they have attributes of investments (such as governance or participation rights attaching to shares, debentures or other investments), and are created, stored and transferred using DLT applications.

What is a Security Token?

18. Security Tokens are described (not formally defined), for the purposes of applying the UK regime for financial services and markets, as:

'…tokens that provide rights and obligations akin to specified investments under the Regulated Activities Order (RAO), including those that are financial instruments under MIFID II. For example, these tokens have characteristics which mean they are the same or akin to traditional instruments like shares, debentures or units in collective investment scheme.' [7]

19. Under the ESMA advice on the MiFID II approach to regulating crypto assets that are 'financial instruments', it is proposed that the specified 'financial instruments' under MiFID, such as shares and debentures, be expressly extended to cover 'such instruments [issued or created] by means of distributed ledger technology'.

Why regulate Security Tokens?

20. The rationale for regulating Security Tokens is the same as for regulating issuance and the conduct of financial services activities that involve the offer, distribution and marketing of, investments. This is because Security Tokens are, in essence, financial instruments that confer, or purport to confer, rights and obligations that are the same or substantially similar in nature, purpose or effect to conventional investments. However, an additional layer of regulation is needed to address issues and concerns relating to the use of DLT or similar technologies that underpin Security Tokens. In particular, we seek to promote investor protection by addressing information asymmetry problems and market integrity issues through disclosure requirements relating to DLT by issuers, as well as the disclosure and conduct requirements imposed on key service providers such as operators of facilities on which Security Tokens are traded, as well as Digital Wallet Service providers who hold custody of Security Tokens. We consider the level of

[6] As explained in the ESMA advice, the private key is generated first, with the public key derived from the private key using a known one-way algorithm which varies across protocols. The address, which is used to send and receive crypto assets, is a cryptographic hash (i.e. a shorter representation) of the public key (longer bit representation). The private key is what grants the user the right to dispose of the crypto asset at a given address. Losing the private key usually results in the loss of ability to move the crypto asset.

[7] See also the proposed amendments to EU directive 2014/65/EU, in conjunction with MiCA proposals.

proposed regulation, without additional prudential requirements on these key players, to be sufficient, but will monitor whether this remains the case.

Part II – Definitional issues relating to Security Tokens

Proposed approach to bringing Security Tokens within DFSA regulation

The current DFSA regime

21. Under the current DFSA regime, the question of whether an activity is regulated often involves determining whether it relates to Investments, as defined in GEN App 2. Investments fall into two categories, Securities (such as Shares and Debentures), and Derivatives (such as Options and Futures). We regulate Investment-related activities conducted in or from the DIFC by requiring persons, who:

    a) offer Securities to the public, or seek to have their Securities admitted to trading on a market, to meet the prospectus disclosure obligations; and

    b) conduct Financial Services activities (such as trading and clearing of Investments, dealing in Investments, arranging deals in investments or providing custody services relating to Investments) to be licensed and regulated by the DFSA.

22. The Financial Promotions regime that applies to the marketing in or from the DIFC of financial products and services applies across both Investments and the other financial products (e.g., credit facilities, contracts of insurance) that we regulate.

Analysis

23. In line with the approach adopted in the benchmarked jurisdictions, our aim is to ensure that the DFSA regime for regulating financial products and services will apply in an appropriate and robust manner to those tokens that we consider to be the same as, or sufficiently similar to, existing Investments to warrant regulation.

24. We propose to achieve that aim:

    a) by making use of the existing DFSA regulatory regime as far as practicable, whilst addressing specific risks associated with Security Tokens, especially technology risks;

    b) without being too restrictive, so that we can accommodate the evolving nature of the underlying technologies that might drive and propel tokenisation of traditional financial products and services;

    c) by addressing risks to investor/consumer protection and market integrity, and systemic risks (should they arise), where new technologies are used in the provision of financial products and services in or from the DIFC; and

    d) whilst remaining true to the underlying key characteristics and attributes of regulated financial products and services as far as practicable.

25. To achieve the above objectives, we propose expressly to bring, within the scope of Investments, instruments issued or created using DLT or similar technology, where such instruments have the same or substantially similar characteristics as Investments, in purpose or effect. These instruments are to be called Security Tokens. While we are influenced by the initiatives in other jurisdictions to regulate tokenised investments

issued and distributed using DLT and similar technologies, our approach is tailored to suit the structure of the DFSA regime, and the needs and expectations of the DIFC financial services sector.[8]

26. Ambiguities are likely to arise if a Security Token does not confer the rights and obligations that are the same or substantially similar as those conferred by a specified type of Investment (for example, conferring some rights, but not all), or has hybrid characteristics of a number of specified Investments.[9] In such cases, the issues that are likely to arise would include not only whether a token can be classified as a particular type or types of a specified Investment, but also how, in practice, our existing specific regulatory requirements would apply to them.[10]

27. We recognise that DLT and similar technologies allow issuers of Security Tokens to be innovative, and create tokens that have hybrid characteristics, including those of different Investments. Our proposals are not designed to inhibit innovation. However, if a Security Token does not confer rights and obligations that are in purpose or effect, substantially similar to those conferred by at least one type of an existing Security or Derivative, it would not constitute an Investment, and be regulated as such. The proposed Guidance in this area is designed to enable industry participants using DLT and similar technologies in their financial products and services to be able to fall clearly within the scope of regulation, to promote protection both for their activities through enhanced certainty and clarity, and also those who invest in their financial products and associated financial services.

28. Finally, we considered whether it is appropriate to use the term Security Token, given that our proposals are designed to cover both types of Investments, i.e. not just Securities, but also, Derivatives (e.g. Options and Futures, such as contract for differences). However, as the industry practice is to include Derivatives within the term Security Tokens, we anticipate there will be an expectation that the term Security Token includes Derivatives, and not just Securities.

Proposal 1 – Bringing Security Tokens within Investments

29. In light of the above considerations, we propose to extend the current definitions of Investments by:

---

8 For example, the UK FCA regime brings within its definitions of Investments, '*Security Tokens that provide rights and obligations akin to investments*', without amending the definitions of Investments. The term 'akin to' is treated under the FCA approach as having characteristics that are the same as, or similar to, conventional financial instruments, such as shares, debentures, warrants, certificates, options or financial or commodity futures. The EU approach encompasses amending the definition of 'financial instruments' under MiFID II (which include transferable securities such as shares, debentures) to cover instruments that are issued or created using distributed ledger technology.

9 Already, different classes of securities that confer different rights on their holders exist within a particular type of a security, such as preference shares or directors shares. Examples include convertible debt – i.e. debt securities that can be converted to shares, and different classes of a particular type of security, such as preference shares, which confer specified returns (like debt) and rank above ordinary shares in a company winding up, or shares that confer some but not all the rights normally attaching to ordinary shares, an example of which is directors shares that may exclude the right to appoint new directors, or vote on matters relating to directors' remuneration, or to participate in dividends of the company in the same way as other shareholders. This provides flexibility for some variation of rights and obligations attaching to a particular Security or Derivative and, similarly, to a Security Token that confers substantially the same or similar rights and obligations as the particular type of Security or Derivative.

10 As recognised by the FCA in its perimeter guidance on crypto assets issued in July 2019, practical difficulties arise in applying the definitions of Investments to Security Tokens due to a number of reasons. For example, this can happen because a Security Token has characteristics of a number of Investments, or due to the evolving nature of the rights and obligations attaching to it in different phases of its issue and distribution.

a) defining a Security Token as a cryptographically secured digital representation of the rights and obligations, issued, stored and transferred using DLT or other similar technology, that:

(i) confers the same rights and obligations as those conferred by one or more existing Securities or Derivatives; or

(ii) confers substantially similar rights and obligations or has a substantially similar purpose or effect to one or more existing Securities or Derivatives; and

b) issuing Guidance that:

(i) the DFSA considers a Security Token to be an Investment of the type or types as defined in GEN App 2, if it confers rights and obligations as noted under a); and

(ii) set out factors that are to be taken into account when determining whether a Security Token is a particular type or types of a Security (such as a Share or Debenture) or a Derivative (such as an Option or a Commodity Future).

Draft GEN Rules A2.1.1(2)(b) and (c), A2.1.1(3) and Guidance, and draft Gen App 6 – at Appendix 3.

Questions:

1. **Do you agree with our proposal to treat as Investments Security Tokens that confer rights and obligations that are the same as, or similar in nature to, those conferred by Investments? If not, why not?**

2. **Do you agree with us that the term Security Token is appropriate if the token confers rights and obligations under a Derivative contract? If not, should they be referred to as Derivative Tokens? Please explain your thinking.**

3. **The proposed definition of Security Tokens would not apply to tokens with hybrid characteristics of a number of different types of Securities and Derivatives, but with no substantially similar rights and obligations relating to any one of them. Do you think our definition of Security Tokens should capture such hybrid products as Investments? Please explain your thinking.**

Administration of guidance

30. As guidance is indicative and not exhaustive and as Security Tokens can have varying characteristics, a case-by-case analysis will often be needed to determine whether a particular Security Token is an Investment or not and, if so, what type of Investment. We considered three options:

a) Option 1 – to place the onus solely on persons proposing to conduct activities relating to Security Tokens in or from the DIFC to determine whether their tokens are regulated Investments of a particular type or types, using the Guidance issued by the DFSA;[11]

[11] The FCA's approach is Option 1.

b) Option 2 – the DFSA to undertake an assessment upon a request made by a person proposing to undertake activities relating to Security Tokens in or from the DIFC; or

c) Option 3 – adopt a hybrid approach combining Option 1 and 2.

31. We recognise Option 2 is administratively more burdensome for the DFSA than Option 1, and is likely to give rise to delays due to resource constraints. We also recognise that Option 2 could raise uncertainties for persons proposing to undertake Security Token related activities in or from the DIFC, as to how their activities will need to be regulated under the DFSA regime, particularly given the potential complexity and hybrid nature of rights and obligations associated with Security Tokens. Our experience so far also shows that many industry participants prefer to have the view of the regulator on their proposed activities relating to tokens. That preference must, however, be balanced against the fact that, as is the case with any other Investment, a Person proposing to conduct activities involving Security Tokens by way of business, in or from the DIFC, will ultimately be responsible for ensuring that it has the required authorisation or other approvals from the DFSA to do so.

Proposal 2 – Assessing if a Security Token is an Investment

32. We propose to adopt Option 3, so that the DFSA will make its own assessment of whether the proposed token is a Security Token that confers rights and obligations that are the same or substantially similar in form and effect as particular type or types of Investments, based on a properly considered self-assessment submitted by an applicant, using the proposed DFSA Guidance as appropriate.

See draft Guidance in GEN App 6 – at Appendix 3.

Question

4. Do you agree with our proposed approach to assessing whether a Security Token is an Investment and, if so, what type or types of an Investment? If not, why not?

Exclusions and prohibitions relating to Security Tokens

Analysis

33. We have considered whether the DFSA should prohibit activities, relating to crypto assets, which are not within the ambit of Security Tokens. There is some merit in doing so, particularly if such instruments can be mistaken or perceived as regulated Investments. There is also a risk that once there are regulated and unregulated tokenised financial instruments, it is possible for market participants to deliberately structure their tokenised financial instruments to fall outside the scope of regulated Security Tokens. While such a prohibition could hinder legitimate developments in this evolving area, we also recognise that allowing unregulated tokens to be offered or distributed in or from the DIFC exposes the DFSA and the DIFC to an unacceptable degree of risk.

34. We are in the process of developing our regulatory approach to tokens other than Security Tokens (such as exchange or utility tokens). Once those proposals are developed, we will be in a better position to establish what other tokens (if any) fall outside the perimeter of financial services regulation. Such tokens could, nevertheless,

need to be subject to appropriate regulation to address, for example, ML/TF risks that could arise relating to activities involving such tokens in or from the DIFC.

35. A related risk is that issuers and distributors may label as Security Tokens instruments that may not have any legal rights or obligations of, or characteristics belonging to, any specified Investment. This could lead to investor confusion and detriment. Therefore, we consider it appropriate to prohibit mislabelling.

Proposal 3 – Exclusions and prohibitions

36. Once our proposals relating to other tokens, which are not Security Tokens, are developed, we expect to provide an express exclusion from regulation as Security Tokens for those other forms of regulated tokens.

37. As part of the proposals in this paper, we propose to expressly prohibit the use of the labels Security Tokens, Derivative Tokens or Investment Tokens (or any derivative of these terms such as securitised token), in relation to a financial instrument, unless it is a Security Token that meets the definition under Proposal 1.

See draft GEN Rules 3.5.1 and 3.5.3 and Guidance – at Annex 3.

Question

5. Do you think it is appropriate to prohibit the use of the labels Security Tokens, Derivative Tokens or Investment Tokens (or any derivative of those), unless the tokens meet the definition of Security Tokens? If not, why not?

Part III – Operating facilities for trading and clearing Security Tokens

The type of Licence needed to operate a facility for trading/clearing Security Tokens

Background

38. Operating facilities or platforms, on which Security Tokens are made available for trading, are the most common type of intermediary service that enables the distribution (buying and selling) of tokens. Some of the considerations in this section may also be relevant to platforms that allow third-party buying and selling of other crypto assets that are not Security Tokens.

39. We consider that our regulatory regime for trading facilities i.e., Exchanges, Multilateral Trading Facilities (MTFs), and Organised Trading Facilities (OTFs) for conventional Investments, as well as for Clearing Houses (i.e. undertaking the clearing and settlement of Investments) should continue to apply to platforms that trade and/or clear Security Tokens.[12] However, there are some additional risks and concerns that are more specific or unique to trading and clearing Security Tokens using DLT and similar technologies that need to be addressed.

[12] This includes requiring that the trading facility has sufficient resources (technology, human and capital resources) and mechanisms (rules, surveillance and enforcement) to ensure efficient, fair and orderly trading in securities; the ability to address risks that could harm buyers and sellers of securities and market integrity, due to conflicts of interests; market abuse; fair access to markets issues; and the risks of money laundering and terrorism financing and other crimes that can be perpetuated through trading.

40. The key areas that need to be addressed arise not just due to the technology being used, but due to varying degrees of reliance on DLT and similar technology applications that are used in the issue and trading of Securities Tokens. These include:

    a) the convergence of the boundaries between crypto assets and conventional financial assets;

    b) the varying and evolving business models that use DLT;

    c) the user perception that crypto assets are as safe as, or even more so, than conventional financial assets or instruments; and

    d) industry participants riding on this perception, at times with little reliance on DLT for their products and services, yet labelling their products and services as DLT based.

41. We seek to identify and address in this paper, in addition to the above risks that inevitably give rise to investor protection and market integrity issues, other additional risks, such as:

    a) operational resilience of trading facilities in times of adverse market conditions, especially due to the volatility in token trading; and

    b) ML/TF and other crimes and misconduct risks.

    The current DFSA regime

42. Under the current regime:

    a) a person conducting the Financial Service of Operating an Exchange must be licensed as an Authorised Market Institution (or AMI);

    b) a person conducting the Financial Service of Operating a Clearing House must be licensed for that activity as an AMI. An AMI can have licences for both Operating an Exchange and Operating a Clearing House;

    c) a person conducting the activity of operating a MTF must hold a licence as an Operator of an Alternative Trading System (ATS). An AMI that is licensed to Operate an Exchange can also undertake the activity of operating a MTF, provided it has an endorsement on its licence to do so; and

    d) a person conducting the activity of operating an OTF must hold a licence as an Operator of an Alternative Trading System (ATS). An ATS operator can operate a MTF or an OTF. Unlike a MTF, which can be operated by an AMI or an ATF operator, an OTF is a trading facility that can be operated only by a Regulated Firm, to bring together third party buying and selling interests based on its discretionary rules.

    Analysis

43. Given that Security Tokens confer rights the same or substantially similar in nature, effect or purpose to Investments (see Proposal 1), operating a facility that trades such tokens is, in substance, nothing other than a trading facility and, if transactions relating to such tokens are cleared and settled on the facility, none other than a clearing house. Therefore, we believe that a person authorised to operate an Exchange or an ATS

should have the ability to operate a facility on which Security Tokens are admitted to trading, and an AMI authorised to operate a Clearing House should be able to clear and settle transactions relating to Security Tokens on their clearing facility, provided the additional requirements proposed in this paper are met.

44. We also consider that persons operating a trading or clearing facility for Security Tokens should have the flexibility to do so exclusively for trading and clearing Security Tokens, or as a facility where both conventional Investments and Security Tokens are traded and/or cleared. The label 'Security Token Market' should, however, only be used by a facility if it is dedicated to trading only in Security Tokens, as to use that label for a facility on which both conventional Investments and Security Tokens are traded may become confusing or misleading.

45. We also considered the issue whether the trading and clearing facilities require two separate legal entities, to provide a greater degree of separation between trading and clearing functions. We are not sure whether DLT and similar technologies that are yet available for trading and clearing of Security Tokens can effectively provide such separation, or not.

Proposal 4 – Type of Licence and labelling

46. We propose that:

a) a holder of an AMI or ATS licence be permitted to operate a trading facility (i.e. an Exchange, MTF or OTF), for the trading of Security Tokens, subject to the additional requirements proposed in this paper;

b) a holder of an AMI licence to operate a Clearing House be permitted to clear and settle transactions in Security Tokens, subject to the additional requirements proposed in this paper;

c) only a trading facility that trades exclusively Security Tokens be permitted to call itself a Security Token Market, or similar labels such as a Derivative Token Market or Investment Token Market (or any abbreviation or derivative of those terms); and

d) only a facility that clears exclusively Security Tokens be permitted to call itself a Security Token Clearing House, or a similar label such as a Derivative Token Clearing House or Investment Token Clearing House (or any abbreviation or derivative of those terms).

See draft AMI Rule 5.12.3 – at Appendix 4, draft COB section 9.8 and Guidance – at Appendix 5.

Questions:

6. Do you agree with our proposal to allow AMI and ATS operators to operate facilities to trade Security Tokens, subject to the additional requirements proposed in this paper? If not, why not?

7. Do you agree with our proposals to allow only an AMI holding a licence to Operate a Clearing House to clear Security Tokens? If not, why not?

8. Do you think we should require an AMI to establish two separate legal entities for trading and clearing of Security Tokens? If not, what are your reasons?

9. Do you agree with our proposal to prohibit the use of the terms such as Security Token Market or Security Token Clearing House (or similar terms and abbreviations) as noted in paragraph 46(c) and (d)? If not, what are your reasons?

Enhanced requirements for trading and clearing Security Tokens

The current DFSA regime

46. The current requirement for operating trading facilities vary depending on whether its operator is an Authorised Market Institution (AMI), or an Authorised Firm operating an Alternative Trading System (ATS).

47. GEN Chapter 5 contains the detailed overarching management, systems and controls requirements that an Authorised Person (i.e. an AMI or Authorised Firm) must meet to obtain and maintain a Licence to conduct any Financial Services. These requirements are cast in broad terms so that they can be applied to any regulated firm, taking into account the nature, scale and complexity of its business. They include requirements relating to fitness and propriety, human resources, authorised/key individuals, corporate governance, financial resources, technology resources, systems and controls for managing risks, and the regular review of the adequacy of such systems and controls.

48. AMI Chapter 5 contains the additional requirements applicable to persons operating an Exchange or a Clearing House that trades or clears Investments. An Authorised Firm Operating an ATS is subject to the additional conduct requirements in COB Chapter 9.

49. The DFSA requirements for trading and clearing of Investments are in line with the applicable IOSCO and CPSS standards, and modelled on the EU regime, (e.g. MiFID, MiFIR and the Prospectus and Transparency Directives).

Business models used for trading and settlement of Security Tokens

50. As noted in the ESMA advice, many issues inherent in secondary trading of crypto assets (including Security Tokens) may not be, in essence, different from those arising in respect of trading venues for traditional securities,[13] but they may arise in a different way due to the DLT or similar technology underpinning the trading and clearing models that are being used, which can be 'centralised' or 'decentralised' platforms to varying degrees, some containing hybrid characteristics.

51. Centralised platforms. These trading and settlement models are, according to the EU/ESMA findings, considered to be the more common model. They typically take control of clients' tokens by holding their private keys in a single distributed ledger account under their own private key (although accounts with multiple private keys can also be created). When the customers place and withdraw their tokens at the platform,

[13] For example, whether the trading or clearing facility has the necessary resources to effectively conduct its activities and address the risks that may arise from them; whether it has established and maintains adequate arrangements and procedures to ensure fair and orderly trading; whether it has adequate measures to prevent potential conflicts of interest and whether it provides access to its services in an undiscriminating way, whether price discovery mechanisms for pre- and post-trade information available on the platform is sufficient to support market efficiency, fair and orderly trading and whether the platform has adequate rules, surveillance and enforcement mechanisms to deter potential market abuse. These issues are not unique to crypto assets trading platforms, but they may be exacerbated for crypto assets because of their high price volatility and often low liquidity. Also, market integrity issues may arise where investors typically access crypto asset trading platforms directly, without an intermediary intervention, such as whether crypto asset trading facilities can adequately address client screening for AML/CTF purposes.

the transaction is usually recorded on DLT (on-chain). The rest of the events that culminate in a transaction on the platform, i.e., the matching of the orders, the execution of the orders, and the corresponding transfer of the ownership of the token, is typically recorded in the books of the platform (off-chain). This model of trading is close to the trading on a conventional trading facility as the transaction settlement occurs in the books of the market (i.e. off chain settlement). As the ESMA advice notes:

a) there is a heightened risk of hacking, with a single point of access to where the clients' private keys are centrally stored; and

b) as only placement and withdrawals are recorded on-chain, the full potential benefits of the use of DLT are not achieved, with the operator/platform bearing counterparty risk vis-à-vis the customers.

52. Decentralised platforms. These trading and settlement models (also known as DEXs) are designed to address the vulnerabilities of centralised platforms by building fully DLT based markets. These platforms have no central authority or middle man and, instead, rely on smart contracts that have self-executing components. Typically, investors control their tokens, and the transaction settlement occurs using DLT (on-chain). These systems sometimes use so-called 'atomic swaps' (i.e. time locks for all parties to a transaction to fulfil their obligations before the assets are transferred).[14] Unlike centralised platforms, DEXs can transfer virtual-to-virtual, as they are not required to do virtual-to-*fiat* only.[15] Such fully fledged DLT based platforms are still in a nascent stage of development, and face a number of challenges and associated risks, such as:

a) tending to be slower than centralised platforms, as every transaction needs to be processed and validated using the DLT on which they are built;

b) governance and accountability issues associated with the lack of centralised control, which can have additional costs; and

c) introducing new kinds of security vulnerabilities due to technical complexity and stages of evolution, however, with capacity, unlike centralised platforms, to transfer crypto-to-crypto, rather than crypto-to-fiat only.

53. Other permutations can encompass hybrid features using DLT. Some platforms may have order books and some may operate without. Decentralised platforms may use smart contracts or a liquidity pool that simply fills submitted orders algorithmically, either on-chain or off-chain. Some platforms may be trading facilities operated by an investment firm for its own proprietary dealing (systematic internaliser) and may use any combination of activities using DLT applications, and would be regulated (under the DFSA regime) as an Authorised Firm Dealing in Investments as Principal, rather than as an operator of an AMI or ATS.[16]

---

[14] By using atomic swaps, the exchange of the two crypto assets resulting from a trade will initially be locked and can only be retrieved by the relevant counterparty using a cryptographic hash function. A time-lock function ensures the refund of the two crypto assets to the original holders in the case that one of the counterparties did not retrieve the crypto asset within a predefined time period.

[15] As noted in the ESMA advice, decentralised platforms do not typically have the ability to convert fiat into crypto assets and centralised exchanges are often used as an initial stepping stone to purchase crypto assets with fiat even for those ultimately planning to trade on decentralised, rather than centralised, exchanges.

[16] Some platforms that display buyer and seller interests, and do not execute orders, are bulletin boards and are not regulated markets. However, the persons providing these bulletin boards will likely need to be regulated as arrangers of Investments.

54. We propose to apply the general requirements applicable to market operators under the current regime to address the issues and concerns that arise in trading and clearing of Security Tokens using DLT, whilst focusing on enhancements to the current regime, on the following areas, as done in the benchmarked jurisdictions:

a) IT-related requirements;

b) External independent audit of technology governance;

c) Access to facilities for trading and clearing Security Tokens;

d) Direct access in conventional markets;

e) Investment criteria to admit Security Tokens for trading/clearing;

f) 'Proper Markets' related requirements;

g) Business Rules and Operating Rules;

h) AML/CTF;

i) Clearing and settlement function; and

j) Custody of Security tokens – Digital Wallets.

IT-related requirements

The current DFSA requirements

55. We already have a range of overarching requirements relating to technology resources for AMIs and ATS operators. These encompass:

a) having sufficient technology resources to operate, maintain and supervise its facilities;

b) establishing and maintaining its technology resources in such a way so as to ensure that they are secure and maintain confidentiality of the data they contain;

c) ensuring the participants on its facility have sufficient technology resources which are compatible with its own; and

d) adequate procedures and arrangements for the evaluation, selection and ongoing monitoring of information technology systems which, at a minimum, provide for:

i) problem management and system change;

ii) testing of the systems prior to live operations;

iii) monitoring and reporting on system performance, availability and integrity; and

iv) adequate measure to ensure resilience, business continuity in the event of failure, protection against damage, tampering, misuse and unauthorised access and the integrity of data stored and processed through the system.

56. While we believe that these requirements are sufficiently wide to regulate operators of facilities on which Security Tokens are traded, some enhancements are needed, due to the unique characteristics of DLT.

Permissioned and unpermissioned access to data and right to update ledger

57. Instead of using a completely decentralised model (discussed in paragraph 52), relying on 'open' access (i.e. unpermissioned access) to an application of DLT, it is common, so far, for many trading facilities to adopt a form of permissioned access. This involves the operator allowing only some participants full access to its network to conduct all the functions contemplated by the relevant DLT application/software (e.g. full node client), with the other participants allowed access to more limited functions (e.g. lightweight client). These trading facilities do not operate on an 'unpermissioned' basis, with open access to data and the right to update records by any participants (e.g., miners).[17] This approach allows the operator of a market that admits Security Tokens to trading on its facility to have a degree of control over the persons who have access to trading related data (e.g. offer and bid prices on its facility) for fulfilling its obligations as the operator of the market (including settlement finality and fair and efficient markets).

58. We expect an operator of a market, on which Security Tokens are admitted to trading, to be able to demonstrate to the satisfaction of the DFSA that the particular DLT configuration and associated rules and protocols it proposes to use, contain:

a) clear criteria for persons accessing and updating records on the platform that encompass integrity/credentials/competencies of such persons;

b) measures to address risks, including to network security, and network compatibility, that may arise through persons permitted to access the platform; and

c) processes to ensure that the operator undertakes:

i) sufficient due diligence; and

ii) adequate monitoring of ongoing compliance, relating to the matters referred to in a) and b).

Technology design

59. Technology design of the DLT implementation adopted by the operator of a market proposing to trade Security Tokens should be able to address how the rights and obligations relating to the tokens are properly managed and discharged.

60. For example, depending on the type of rights and obligations conferred by a Security Token, the operator should be able to demonstrate that the person responsible for the

[17] The May 2019 consultation paper from the Jurisdiction Taskforce of the UK LawTech Delivery Panel stated: *'At a high level, a "permissionless" DLT implementation is one in which anyone can participate in the network without prior authorisation (i.e. anyone can operate a node on the network). In contrast, in a "permissioned" DLT implementation, prior authorisation is required in order to participate in the network. This prior authorisation may be provided in different ways, for example by all other participants in certain implementations, or, in others, from some form of central authority which has superior credentials to, and certain authority over, other nodes (often referred to as "master nodes"). Where a DLT implementation relies on a form of central authority, it may also be that such central authority has the ultimate say in how data is updated on the distributed ledger. This may be because it is the sole user with the ability to update the distributed ledger, or because it has a unique ability to change or override records which other users have previously validated.'*

admission to trading of the Security Tokens (usually the issuer) can meet, or secure the fulfilment of, the legal rights and obligations conferred by the relevant Security Tokens. For example, if a Security Token confers rights and obligations that are the same as or substantially similar to a Share or Debenture of a company, this would generally require the shareholders' rights, such as to call and hold shareholder meetings, receive interest or dividends (if declared), and the right to participate in the assets of the company in a winding up, to be fully met. See also the draft Guidance at GEN App 6 at Annex (A) for determining how a Security Token is to be classified as a particular type of Investment.

Technology governance

61. To ensure fitness for purpose of the DLT implementation adopted by the operator for its trading facility, it must, at a minimum, have regard to the following areas:

a) development and maintenance of systems and architecture of the IT system in terms of its code version control, implementation of updates, issue resolution, and externally carried out technology testing procedures;

b) security measures and procedures for the safe storage and transmission of data in accordance with agreed protocols;

c) procedures to address forks (hard or soft), and access to information where such a fork is created; [18]

d) procedures to deal with system outages, whether planned or otherwise;

e) decision-making protocols and accountability for decisions;

f) procedures for the establishment and management of interface with providers of digital wallets (see the detailed discussion below relating wallets); and

g) ensuring that the means (such as the protocols and smart contracts) that are built into the DLT application adopted by the operator meet at least minimum reliability and safety requirements, including to deal with cyber-attacks and hacks, and how the aftermath of such an interruption is to be dealt with.

Proposal 5 – IT-related requirements

62. We propose, instead of being too prescriptive, to give Guidance on the DFSA's expectations of technology resources which an operator of a trading facility on which Security Tokens are traded or cleared (or both) needs to have, that covers:

a) matters relating to the particular DLT implementation and the associated rules and protocols it proposes to adopt for its facility, referred to in paragraph 58;

b) technology design issues referred to in paragraphs 59 and 60; and

c) technology governance issues referred to in paragraph 61.

63. This approach is consistent with the approach adopted in the benchmarked jurisdictions and the recommendations of the standard setters, as hard wired rules are generally difficult to apply due to the variable models of DLT that can be adopted by operators of

[18] A 'fork' is a change to the DLT protocol. A hard fork is defined as a change that requires all nodes or users to upgrade to the latest version of the protocol software, or creates two versions of the protocol going forward.

markets on which Security Tokens are traded and cleared, and due to the evolving nature of DLT and similar technologies.

See draft COB section 14.1 and Guidance – at Appendix 5, and draft AMI section 5A.5 – at Appendix 4.

Question

10. Do you agree with our proposal to give detailed Guidance relating to IT-related requirements for operators of facilities that trade and/or clear Security Tokens as noted in paragraph 63? If not, why not?

Independent audit of technology governance

64. Technology governance, which includes IT-related enhancements proposed under Proposal 5, is of critical importance to the proper operation of a facility that trades or clears Security Tokens (or does both). It is also likely that the specific applications of DLT adopted will vary from firm to firm, and also evolve as technology advancements are made, making it difficult for the DFSA to remain up-to-date with the specific challenges and changes that affect the operation of the DLT applications and protocols adopted by a firm. Hence, this is an area where it is appropriate to have an independent audit of the firm's compliance with the proposed IT requirements, carried out by a suitably qualified external IT expert.

65. In view of the above, we believe that a firm operating a facility which trades or clears Security Tokens (or does both) should be required to have an annual audit, conducted by an independent third party IT expert specialising in DLT and similar technology applications, to provide assurances to the firm's Board and to the DFSA that the firm continues to meet the requirements proposed in Proposal 5, and submit that audit report to the DFSA along with its annual report.

Proposal 6 – Independent audit of technology governance

66. We propose that an operator on whose facility Security Tokens are traded and/or cleared be required to have an annual audit of its compliance with the technology resources and governance requirements applicable to it, as part of its annual audit report to be filed with the DFSA, for the reasons set out in paragraphs 64 and 65. The operator will need to demonstrate to the DFSA that the independent expert who issues the report has the relevant expertise, including the diligence undertaken by the operator to satisfy itself of the expertise of the third party service provider. We also propose to seek public comment on who should be considered competent to perform this IT audit.

See draft COB section 14.5 and Guidance – at Appendix 5, and draft AMI section 5A.5 – at Appendix 4.

Questions:

11. Do you agree with our proposal to require an independent audit of technology governance? If not, what other options can provide the necessary degree of assurance that is required in this area?

12. Should the IT audit be carried out by a Registered Auditor? If so, what accreditation should such an auditor have?

Access to facilities for trading and clearing Security Tokens

The current DFSA requirements

67. Only certain persons who meet specified criteria can have access to a regulated trading or clearing facility (i.e., an Exchange, Clearing House or ATS) under the current regime applicable to their operators. The access to trading criteria are designed for an intermediated model of trading, limited to regulated firms (i.e., an Authorised Firm or a Recognised Person). However, an ATS operator may, in addition to regulated firms, allow certain institutional Professional Clients to trade on their facilities, subject to the additional controls set out in this section. The intermediated model of trading in conventional markets stands in contrast to direct access to trading on platforms where sellers and buyers of securities can transact on a peer-to peer basis, rather than through intermediaries who transact on their behalf.

Risks/benefits of the current intermediated model of trading

68. The current model that requires intermediated access to regulated trading facilities by investors (whether retail or professional, or individual or institutional) is designed to address:

a) *systemic risks* that may arise from counterparty failure. These are mitigated by only regulated firms, which are subject to prudential requirements, and regulatory oversight, being able to trade on behalf of customers who wish to buy and sell investments;

b) *market integrity risks* arising from disorderly conduct of markets. These are mitigated through the market operator's rules (Business or Operating Rules) designed to ensure fair, transparent and orderly markets that apply to regulated firms who are members of the market, as well as the regulatory requirements applicable to such firms as providers of financial services to buyers and sellers of securities; and

c) *money laundering and terrorism financing risks* that are mitigated by AML/CTF requirements imposed on the operator of the exchange/ATS and the regulated firms who trade on the markets.

69. However, the current intermediated model is increasingly challenged by innovative platform solutions which offer reduced total transaction costs, expedited clearing and settlement cycles, as well as efficient post-trade reporting opportunities.

Risk/benefits of allowing direct access to trading in Security Tokens

70. DLT and similar technologies that underpin trading, especially in unpermissioned trading venues:

a) remove the need for intermediation, allowing direct access to buyers and sellers of securities on the platform, regardless of whether such buyers and sellers are retail or professional, or individual or institutional; and

b) enable issuers of securities to raise capital by making their offers of securities, using smart contracts and similar technologies, an automated process for complying with the applicable regulatory requirements, such as the issue and updating of prospectus disclosure (see also the discussion under Issuers of Security Tokens in Part IV).

71. Risks that need to be addressed, if direct access to trading facilities were to be allowed for buyers and sellers of Security Tokens, include counterparty failure/systemic risks, market integrity risks and AML/CTF risks. We believe that some of these risks are either insignificant, or can be addressed through alternative means, as discussed below.

72. Systemic risks – Security Token trading is unlikely to pose significant systemic risks, at least for the time being, because of the 'low volume/value' transactions undertaken by direct participants who are generally retail. This is the view held by many regulators and standard setters.[19] However, should institutional investors with significant connectivity to the larger economy/markets enter markets that trade tokens, potential systemic risks arising from large defaults would need to be addressed, using measures to address such risks in conventional markets.

73. Market integrity risks – Such risks are heightened in a direct market access model to trading, because the regulation applicable to regulated firms transacting in intermediated conventional markets is absent. This risk can be mitigated by the operator of the trading facility having adequate systems, controls and resources to undertake appropriate due diligence (including KYC and AML/CTF screening) and having the ability to take appropriate enforcement action without adverse risk to the facility and other users of the facility for trading. Although direct access in a non-intermediated model involves a diffuse group of participants trading on the facility, the underpinning technology may have the potential to support automated procedures to detect and prevent disorderly or unfair conduct, diminishing scope for unacceptable or unfair practice.[20] We note that DLT and similar technologies can enhance an operator's monitoring capabilities, by giving the operator access to real time trading through an operator's node.

74. AML/CTF risks are particularly significant, especially given the degree of anonymity that can be achieved in a *completely automated*, direct access environment with no central operator responsible for its operations, where the identity (including the ultimate beneficial ownership) of the buyers and sellers, and the source and flow of funds resulting from trading transactions, may become non-transparent. However, these risks can be mitigated by prohibiting completely decentralised platforms with no central operator accountable for its operations. We would also focus on the measures and procedures that can be adopted by the operator of the facility on which Security Tokens are traded, and the associated service providers, particularly those providing clearing and settlement functions or custody or wallet providers, as discussed later in this paper.

75. Investor/consumer protection risks are likely to arise in direct access markets, such as:

    a) the counterparty risk having to be directly borne by the participants in trades (being peer-to-peer transactions), which can be addressed through the operator being required to establish adequate collateral management mechanisms to reduce the counterparty risk, based on the settlement cycle adopted;

    b) participants' lack of clear understanding of the nature and risks of trading on a peer-to-peer basis, which can be mitigated through appropriate disclosure; and

---

[19] FSB, BIS, ESMA, BoE and FCA have stated that - at present - the markets for crypto assets do not pose systemic or (global) financial stability risks and/or are small or negligible in their jurisdiction with so-far minimal participation by large financial institutions. However, MiCA, published in September 2020, which sets out EU proposals to regulate crypto assets other than security tokens, such as exchange tokens and utility tokens, espouses the view that in areas such as 'stablecoin' may raise systemic risks.

[20] See also IOSCO consultation paper, referred to in footnote 3, which identifies the conduct of business risks (e.g. client on-boarding/AML/CTF/Suitability) that arise in direct access markets.

c) the lack of investor remedies against the operator of the facility, which can be addressed by clear accountability of the operator for the operation of the facility.

We note that while limiting access to direct trading to Professional Clients only could, to some extent, address concerns about the ability to appreciate risks and bear losses that may result from trading in Security Tokens, but, to do so would remove the cost benefits potentially available to Retail Clients in disintermediated markets, and we do not propose to do so.

76. However, with the DLT based technology used in many models, facilities that trade in Security Tokens are not intended to be completely decentralised, unpermissioned open-access models, but instead to be a facility with a central operator accountable for its proper operation. Hence, the market integrity, ML/TF and investor protection risks identified above can be effectively addressed by the operator through its systems and controls. When authorising and supervising a market which allows direct access to trading, we will require the market operator to have and maintain adequate, well-defined resources that allow them to carry out their role as the front-line supervisor of the participants on the facility, who include retail participants.

Proposal 7 – Allowing direct access to trading in Security Tokens

77. We recommend that an operator of a facility on which Security Tokens are to be traded on a direct access model (without orders having to come through a regulated firm that is a member of the relevant market) be required to demonstrate to the DFSA that it has, and will be able to maintain, adequate systems and controls to address market integrity, AML/CTF and investor protection risks. These would include DLT/IT technology that has built-in procedures (including, if possible, an operator's node referred to in paragraph 73) that:

a) enables the operator to clearly identify those accessing the facility for trading, and to undertake appropriate customer due diligence to address ML/FT risks;

b) contains mechanisms to detect and address market manipulation and abuse (through monitoring bid and offer prices and volatility);

c) provide adequate disclosure through prospectus/on-going disclosure relating to the Security Tokens that are admitted to trading/clearing on the platform (see the discussion in Part IV); and

d) set out clear lines of accountability, and disclosure of investor redress mechanisms, available to persons trading on the facility.

78. In addition to the IT-related requirements above, we also propose that an operator of a facility that admits Security Tokens to trading, and permits direct access, has:

a) a direct customer relationship with the persons who can directly trade in Security Tokens on its facility;

b) mechanisms to identify and distinguish orders that are placed by persons using direct access to trade in Security Tokens and, if necessary, the ability to stop orders of, or trading by, persons allowed direct access;

c) rules that prevent persons referred to in a) from allowing access to other persons to trade on the trading facility and procedures to prevent this occurring;

d) establishes and maintain adequate and effective systems and controls, including policies and procedures, to ensure that persons allowed direct access to trade in Security Tokens fully comply with the business/operational rules of the facility and that where gaps and deficiencies are identified, they are promptly addressed; and

e) adequate mechanisms to carry out the front-line monitoring of trading activities by persons trading in Security Tokens using both direct and intermediated access to its markets.

79. Should the operator be unable to build some or all these requirements into their DLT application, then they must put them in place in some other way that achieve compliance with the requirements.

See draft COB Rules 9.3.1(1)(e) and (4), 9.3.2, 9.3.3 and section 14.2, and associated Guidance – at Appendix 5, and draft AMI Rules 5.7.1 (Guidance only), 5.7.2(1) and (4), 5.7.3(1)(d) and section 5A.3 and associated Guidance – at Appendix 4.

Questions:

13. Do you agree with our proposal to allow direct access to Security Token trading subject to the additional requirements in paragraphs 77 and 78? If not, why not?

14. Should we confine direct access to trading in Security Tokens for Professional Clients only? If so, what are your reasons?

15. Should we limit the participation of Retail Clients in these markets, as an investor protection measure, by placing limits on the parcel size or volume of their trading activity? If not, why not?

16. Are there any other concerns which need to be addressed in allowing direct access to trading in Security Tokens? What are they and, how should they be addressed?

Direct access to trading on conventional trading facilities

Background and analysis

80. While not directly relevant to Security Tokens, because facilities that trade conventional Investments may themselves allow access to trading in Security Tokens, as a matter of parity in regulation of similar arrangements, it is necessary to consider whether direct access to conventional markets should also be permitted.

81. Arguments in favour of such direct access across the board for all Investments, including Security Tokens, are the need to create a level playing field between trading in all Investments, tokenised or otherwise, and the need to be technology neutral in our regulation. We already adopt a technology neutral approach by not prohibiting conventional market operators to use DLT in operating their markets using the intermediated model. We also do not prohibit operators of trading facilities to admit to trading both conventional Investments and Security Tokens.

82. We have not undertaken any detailed assessment of whether it is practicable for the intermediated and direct access models to run side-by side, and whether they pose any issues in terms of segregating the roles and functions of the operator of the market, vis-à-vis the direct access clients, and intermediated participants, and other participants. In

particular, segregation of Client Assets and the responsibility for safe custody of Client Assets are likely to require further analysis in such an environment. We do not think that these are insurmountable issues. Given the evolving nature of DLT and similar technologies on which direct access models are built, rather than pre-empting how the existing regime needs adjustments to accommodate such a situation, we consider it appropriate to seek public comment, whilst also being prepared to entertain applications relating to direct access in conventional markets addressing the issues noted.

83. In doing so, we will consider how market integrity and systemic risks that could arise (e.g., from significant trade failures) could be effectively addressed in an environment where persons other than regulated firms could be counterparties to market transactions. We would also do so in a manner so that any move to allow direct access in conventional markets would not lead to difficulties for the DFSA in meeting, in future, the applicable IOSCO/CPMI[21] standards.[22]

84. We note that an ATS operator can operate an MTF or OTF with direct access to trading on its platform by persons other than regulated intermediaries, although such access is restricted to certain 'institutional professional clients'.[23] An ATS operator has a client/operator relationship with those institutional investors having direct access. While an ATS can currently only trade on its facility securities that are already admitted to trading on an AMI or a Regulated Exchange, we consider that the model for allowing direct access to facilitate trading conventional securities can be adapted to accommodate direct access in tokenised Investments, including to retail clients.

Proposal 8 – Allowing direct access in conventional markets

85. We propose to:

a) seek public comments, including from industry participants, as to how direct access to trading in conventional markets could be allowed, and what risks that arise at operational level in operating such a model, before being able to develop regulatory requirements that are appropriate for direct access trading; and

b) at this stage, to consider on a case-by-case basis an application if a person wishes to operate a conventional market that allows direct access trading in Security Tokens, either side-by-side with trading in conventional Investments, or solely in conventional Investments. For this purpose, an applicant is expected to provide to the DFSA a business plan,[24] which includes (in addition to the other material required, including requirements proposed in Proposal 7 for direct access to trading in Security Tokens), how the roles and accountabilities of the operator vis-à-vis the direct access participants are intended to operate, and in particular, how the Client Assets are segregated and safe custody provided, if the same client is to have both direct and intermediated access.

Question

17. Do you agree with our proposals on direct access to conventional markets?

[21] Committee on Payments and Market Infrastructures.

[22] This does not mean such a change would necessarily lead to non-compliance with IOSCO Standards, but we have not undertaken the analysis, or benchmarking, to verify whether and how disintermediated models work.

[23] Professional Clients who are Large Undertakings, companies listed on an exchange in an IOSCO member jurisdiction or whose main business is investing in financial instruments.

[24] An AMI may do so as part of a notification of Material Changes to its licence. We do not have any licensed ATS operators and a fresh application for such a licence will need to include its new Business Plan.

If not, why not?

Investment Criteria to admit Security Tokens to trading/clearing

The current DFSA requirements

86. The proposed classification of certain Security Tokens as Investments would not, in itself, suffice for such tokens to meet the 'Investment criteria' for admission to listing and trading on an AMI or ATS. To be admitted to trading on an AMI or ATS, the relevant Investments must also meet the specified 'investment criteria' in AMI or COB Chapter 9.

87. There are a number of tests[25] applicable for an Investment to qualify as suitable for admission to trading. For an AMI, two different criteria apply:

    a) if the Investments are Securities, they must first be admitted to the Official List of Securities (the List), maintained by the DFSA, before admission to trading by the AMI; and

    b) if the Investments are Derivatives, they must meet the contract specification criteria before being admitted to trading on the AMI.

88. An ATS can only admit to trading on its facility Investments if:

    a) for Securities, they are admitted to trading either on an AMI or a foreign exchange regulated by a regulator outside the DIFC; and

    b) for Derivatives, they meet the same contract specification criteria as for trading on an AMI.

89. The Listing Rules contain a range of qualifying and ongoing criteria that need to be met by a Security and the issuer (or the person responsible for the listing application) of those Securities to be eligible for admission to the List, and to maintain such admission.[26] These include requirements relating to audited financial statements for the past three years, sufficient working capital, the suitability of the business, directors' management experience, validity and transferability of the securities, clearing and trading arrangements that are acceptable to the DFSA, at least 25% of the Shares to be publicly distributed, and a DFSA Approved Prospectus. There are less stringent eligibility criteria for a SME to be admitted to the List.[27]

90. Once listed, the Reporting Entity (or Listed Entity in the case of a SME) is required to ensure that all the necessary information and facilities are available to its shareholders to enable them to exercise the rights attaching to their holdings on a well-informed basis. These include information relating to the exercise of their votes and documents containing rights attaching or affecting their rights.

91. Exchanges generally play a public interest role, which stands in contrast to the trading venues operated by Authorised Firms for their clients, where the ATS operator has a client/firm relationship with buyers and sellers who transact on its market (where

[25] See AMI 5.8.1 and COB 9.4.1 for Investment criteria to be admitted to trading on an AMI or ATS.
[26] See MKT Chapter 9.
[27] A SME, for these purposes, is an enterprise with an aggregate market value of all its listed shares that is less than USD 250 million at the time of admission. See MKT 1.3.3.

clearance of such transactions must still be through a Central Securities Depository (CSD) or a Clearing House).

Options

92. In considering how Security Tokens can be admitted to trading on an Exchange, MTF or OTF, we have considered two options:

a) Option 1 – to maintain the current differentiation between an Exchange and an ATS with regard to admission to trading, in the case of Security Tokens. This would mean that an AMI could act as a primary venue for listings, whereas an ATS operator would only be able to trade Security Tokens that had already been admitted to trading elsewhere (if they are Securities and not Derivatives); or

b) Option 2 – not to apply the current differentiation, so that Security Tokens can be admitted to trading on an Exchange, MTF or OTF operated by an AMI or ATS operator, with both facilities being able to host initial token offerings/and secondary trading.

93. We do not see a strong case for Option 1. The reliance on DLT and similar technology for tokenisation of Investments generally stems from the desire to remove costs (such as those resulting from intermediated market access) and we should not prevent this provided it can be done safely. We also note that businesses raising capital through DLT and similar technologies tend to be small to medium sized business, rather than larger, more established businesses.

94. We are of the view that the current admission criteria in Chapter 9 of the MKT module should be applied to Security Tokens and their issuers or persons seeking the trading of Security Tokens on the relevant trading facility (the Reporting Entity), including the prospectus and on-going disclosure relating to Security Tokens in Part IV. This will allow both Exchanges and MTFs and OTFs to admit Security Tokens for trading on their facilities.

95. We consider that the eligibility criteria for SMEs provide sufficient flexibility to accommodate smaller businesses using DLT and similar technologies to tokenise their securities. We also note that the DFSA has the discretion to amend the listing requirements, which can accommodate any practical difficulties arising in the context of an application to have Security Tokens admitted to trading. This approach would give an ATS operator the choice of admitting to its MTF or OTF Security Tokens admitted to trading elsewhere (as provided under the current regime), or admitting Security Tokens that meet the listing criteria in MKT Chapter 9, which can be achieved through a minor amendment to COB section 9.4.[28]

Proposal 9 – Investment criteria for admission to trading of Security Tokens

96. We propose that operators of Exchanges, MTFs and OTFs be permitted to admit to trading on their facilities Security Tokens that meet:

a) the Investment criteria in AMI 5.8.1, if it is an Exchange; and

[28] Under the EU regime, it is not necessary to have securities admitted to an official list for the purposes of admission to trading on a regulated exchange, MTF or OTF.

b) the Chapter 9 Investment criteria, modified to allow primary listings of Securities, if it is an ATS,

with appropriate case-by-case modifications as may be required. This also removes the current restriction that an ATS remains a secondary trading venue. However, we consider that the prospectus and on-going disclosure obligations that apply to persons responsible for admission to trading of Security Tokens (discussed in the Proposals 15 - 19), should apply to admission to trading of Security Tokens on an ATS.

See draft COB Rule 9.4.1(a) – at Appendix 5, draft AMI Rule 5.8.1(3) – at Appendix 4, draft amendments to Articles 10, 14 and 38 of the Markets Law – at Appendix 2 and, draft MKT Rules 1.3.2(c), 2.1.1(c), 2.2.1(a), 2.4.2(2), 6.1.1, 6.3.6 and associated Guidance – at Appendix 7.

Questions:

18. Do you agree with our proposal to allow an ATS operator to admit to trading Security Tokens on its facility, as proposed in paragraph 96? If not, why not?

19. Do you think that it is appropriate to allow an OTF, a facility operated by an ATS operator, to be a primary venue for admission to trading of Security Tokens? If yes, please explain why?

'Proper markets' related requirements

The current DFSA requirements

97. A market operator is currently required to have rules and procedures to ensure only Investments (Securities or Derivatives) in which there is a 'proper market' are traded on its facilities. The proper market concept encompasses information relating to the relevant Investments being available to persons dealing in them on an equitable basis, including pre-trade and post-trade orders, adequate controls to manage volatility (e.g. due to speculation), and so on, and adequate mechanisms to discontinue, suspend or remove investments that do not meet the proper markets requirements.

Analysis

98. As ESMA advice notes, it is not unique to facilities that trade tokenised securities that there are issues relating to:

a) the adequacy of pre- and post- trade information made available to the markets that underpin market efficiency and market integrity through fair and orderly trading; and

b) whether a market has adequate rules, surveillance and enforcement mechanisms to deter potential abuse that can arise relating to trading.

However, these concerns can be exacerbated due to the high price volatility and often low liquidity in Security Token trading. This could be further exacerbated where investors have direct access to trading, without an intermediary being involved on whom obligations relating to pre- and post- trading obligations can be imposed.

99. The DLT or similar technology application used may enable an operator of a trading facility that trades Security Tokens to meet the current pre- and post-trade transparency requirements in relation to Security Tokens. For example, pre-trade transparency can

be achieved by allowing the public access to current bid and offer prices, and the volume, including depth of trading and interest shown in the relevant Investments. Making such information available on a continuous basis may be easier because there would only be on-exchange transactions, with no 'off-order book' transactions of brokers with disintermediated access. We will expect those proposing to operate a facility, on which Security Tokens are traded, to demonstrate to the DFSA's satisfaction how they would meet the pre- and post-trade transparency requirements using their DLT applications.[29] They may use an operator's node to carry out some of these functions.

100. However, it is possible that in practice, some difficulties may arise. We are aware that delays in confirmation of transactions may arise (preventing disclosure in real-time) for various reasons when using DLT. For example, due to a 'fork'[30] resulting from a change to the protocol used in the DLT application used by the operator of the market, or due to the average time that it may take to add new blocks on purely decentralised blockchain platforms (for which we have no regulatory risk tolerance). These are areas which are still evolving. Again, instead of hard wired rules, we propose to address any practical issues that need to be addressed, as they arise, with guidance, if needed, in due course.

Proposal 10 – Proper Markets requirements

101. We propose that the operator of a trading facility, on which Security Tokens are to be traded, be required to comply with the DFSA's current requirements relating to 'proper markets', but seek public comment on whether there are any areas which require additional rules or guidance to address practical issues arising as a result of the use of DLT or similar technology.[31]

Question

20. Do you agree with our Proper Markets proposal in paragraph 101? If not, why not?

Business Rules and Operating Rules

102. Under the current regime, the relationship between persons trading on an AMI or ATS, who are mainly regulated intermediaries, is governed by the Business Rules or Operating Rules of the relevant AMI/ATS. With the proposed direct access to trading on markets, where Security Tokens are admitted to trading, some of the obligations that are placed upon the intermediary who transacts on behalf of buyers and sellers of securities on the relevant markets will need to be adjusted, so that those obligations become the obligations or duties of the operator of the facility. See the proposed requirement for direct operator/client relationship for direct access market, in paragraph 78a).

103. Consequences of the direct operator/client relationship include, the operator of the facility allowing direct access to trading by clients having to:

a) undertake a client classification of each client;

---

[29] Potential applicants have indicated that they could meet the relevant pre- and post-trading transparency requirements applicable to an AMI/ATS.

[30] See footnote 18.

[31] Other controls which an AMI or ATS needs to comply with in order to ensure orderly, fair and transparent markets include volatility controls and mechanisms to address short selling. We will adopt a similar approach to such requirements as proposed for pre- and post-trade transparency.

b) enter into an agreement with direct access clients to ensure that those clients comply with the business or operating rules of the facility/operator; and

c) undertake monitoring to ensure that clients having direct access abide by the business or operating rules.

Proposal 11 – Business and operating rules

104. We propose that the requirements relating to business or operating rules of an AMI/ATS (in AMI module and Chapter 9 of COB) be applied, with adaptations as proposed in paragraph 103, where the facility allows buyers and sellers to be direct access participants on the trading facility.

See draft AMI section 5A.3 – at Appendix 4, and draft COB section 14.2 – at Appendix 5.

Question

21. Do you agree with our proposal to apply the current rules relating to business/operating rules, subject to adaptations to cater to direct access clients, as proposed in paragraph 104? If not, why not?

AML/CTF

Background

105. Preventing financial crime is one of the key issues that needs to be addressed. Regulators are concerned that tokenised instruments (including Security Tokens) pose higher risks of potential illicit activities such as laundering money, evading tax, or financing terrorism, due to the ability of the technology to:

a) effect anonymous transfer of funds between parties; and

b) mask the origin or destination of the flow of funds, in the same way as cryptocurrencies could do.[32]

106. These risks can be exacerbated where technology allows execution of transactions and payment of funds across many jurisdictions, involving multiple parties with differing degrees of AML/CTF regulation. Convergence of roles played by participants on facilities transacting in tokens, and the rapidly evolving nature of technology, make it even harder for regulatory and enforcement agencies to identify and deal with perpetrators of illicit activities effectively.

Analysis

107. We believe that the following measures are needed to mitigate the risk of ML/TF and other illicit activities that can arise where Security Tokens are traded on a facility, on the operator of the facility, where the operator is required to:

[32] The FCA's recently released draft Guidance states '*Cryptoassets can sometimes offer potential anonymity and the ability to move money between countries and individuals. This lack of transparency and regulatory oversight for certain cryptoassets means that there are risks from financial crime, including money laundering and the financing of terrorism*'.

a) comply with the AML/CTF regime in respect of customers who have direct access to trading on the facility (other than regulated firms), such as the obligation to undertake KYC/due diligence on each customer to ascertain and verify, among other things, the identity of the customer and the source and the destination of their funding and assets; and[33]

b) impose, through operating rules, requirements on direct access customers to ensure the maintenance of proper markets, which include standards of conduct designed to mitigate misconduct.

108. We believe that the requirements applicable to persons who are eligible to have their Investments admitted to trading on a facility also act as key mitigants against ML/TF risks. These include the criteria applicable to the company and its controllers and the board. In addition to those criteria, we consider that an operator of a facility that admits Security Tokens to trading must have in place adequate due diligence procedures to identify and ascertain who has the ultimate beneficial ownership of direct access members who are trading Security Tokens.

Proposal 12 – AML/CTF

109. We propose to address ML/TF risks by:

a) not allowing the operation in or from the DIFC of trading facilities that allow anonymous trading (so called privacy-focused tokens), due to high risk of money laundering, terrorism financing and tax evasion such facilities pose, and take appropriate enforcement action against such activities; and

b) requiring that an operator of a facility that permits trading in Security Tokens to:

i) fully comply with the DFSA AML regime with respect to participants, including customers who are allowed direct access to their market, and include Guidance to that effect;

ii) have in place operating rules that apply to direct access customers to ensure the maintenance of proper markets, which include standards of conduct designed to mitigate ML/TF and other misconduct; and

iii) have systems and controls to identify and ascertain the ultimate beneficial ownership of participants trading on its facility.[34]

See draft COB Rule 14.2.3 and Guidance – at Appendix 5, and draft AMI Rule 5A.3.2 and Guidance – at Appendix 4.

Question

22. Are our proposals in paragraph 109 sufficient? If not, what else is needed?

[33] We note FATF recommendations include a 'travel rule', where transaction information for each single record above USD 1000 should be established and maintained.

[34] UBO requirements are generally applied under the companies law regimes, and operators need to ensure that these requirements are fully met by the issuers whose Security Tokens are admitted to trading.

Clearing and settlement

The current DFSA requirements

110. An AMI is currently required to establish and operate satisfactory arrangements for securing the timely discharge of the rights and liabilities of the parties to transactions conducted on its facility. An AMI can conduct this activity under its own licence, if it has an authorisation for 'Operating a Clearing House', or obtain the services of an appropriately licensed and regulated entity to carry out the function.

111. The 'clearing and settlement' is the process by which the rights and obligations of the buyers and sellers of Investments are, upon the execution of contracts to buy or sell Investments, cleared and settled between those parties. This process entails:

    a) establishing settlement positions by calculating net positions;

    b) checking the availability of Investments and funds to secure the discharge of rights and obligations under an executed transaction; and

    c) securing the timely discharge of such rights and liabilities.

112. Clearing and settlement functions can be undertaken by becoming a central counterparty to the transactions (CCP), or by operating a Securities Settlement System (SSS) or Central Securities Depository (CSD), with the latter two being facilities where transactions are recorded or cleared, without the operator of the facility stepping in as a counterparty.

Analysis

113. Trading and clearing facilities may consider moving from the traditional centralised model, for which the current regulatory regimes are designed, to a completely decentralised or less centralised model, using DLT and similar technologies, as noted in paragraphs 51 and 52. Our proposals are not designed for facilities with no operator accountability, as such models raise significant market integrity and investor protection concerns.[35]

114. The conventional model of clearing generally involves the netting of transactions, so clearing members would receive a 'cash leg' instruction and a 'security leg' instruction for all transactions executed by their clients on that day, with the novation of the transaction if the clearing house assumes the role of the central counterparty (i.e. places itself in the centre between all buyers and sellers).

115. In a DLT-based facility, we expect the clearing and settlement to be by a gross settlement model where:

    a) instructions are directly settled in the account of the relevant customer/client; or

    b) the operator of the facility takes control of the clients' crypto assets (Security Tokens) by holding clients' private keys on their behalf or keeping clients' assets in a single DLT address under the platform operator's own private key.

[35] This is consistent with the EU approach, which requires a securities settlement system (i.e. a formal arrangement among three or more participants for clearing and execution of transfer orders, under common rules and standardised arrangements) to have a legally accountable system operator.

116. Issues arise in relation to clearing and settlement of Security Tokens, which revolve around settlement finality and counterparty risk. We are not aware of a clearing facility model for Security Tokens (or crypto assets more broadly) where the operator would mitigate counterparty risk by novation of matched contracts through the introduction of a central counterparty (CCP), as is the normal practice in conventional markets. However, a clearing facility may choose off-chain settlement taking place in the books of the clearing facility, as in the conventional model, while the custody of the client's virtual assets is controlled through the use of private keys, as noted in paragraph 115b).

117. The models used for clearing and settlement of Security Tokens can vary, depending on the DLT configuration or application that is being used. To accommodate such variations in an appropriate manner, whilst requiring that confirmation, clearance and settlement processes adopted by an operator of a clearing facility properly address settlement finality and counterparty risks, the systems and controls of the operator of the facility should include:

    a) mechanisms to ensure that order entry into the system can only be made after a pre-validation check which confirms that:

        i) the client assets to meet the security leg and cash leg of the transaction are within the full control of the platform operator; and

        ii) those assets are available for same day settlement, regardless of whether the operator chooses real-time settlement or not, and they cannot be used for any other purposes of, or by, the client;

    b) if the pre-validation control referred to above is to be deviated from, adequate margin requirements or other mechanisms that could act as a defence against default, whether technical or financial;

    c) procedures to be followed by the operator relating to:

        i) how it would deal with delays in settlement due to technical disruptions (malevolent or otherwise, such as hacks or forks), failure to pre-validate, or other causes; and

        ii) whether it has the powers to cancel, amend or reject orders and matched transactions, pre-trade; and

    d) procedures to be followed in the case of unsettled transactions, including whether the operator has the ability to unwind such transactions.

118. The facility operator's business rules or operating rules must also clearly identify the settlement model adopted, in terms of clearing and settlement of Security Tokens on its facility. We expect any changes to the model to, as is normally the case for all conventional facilities, require prior approval of the participants on the facility, particularly where contractual rights and obligations are adversely affected by a proposed change.

Proposal 13 – Clearing and settlement of Security Token transactions

119. We do not propose to accommodate a fully automated clearing and settlement model with no licensed operator responsible for its operation. Where an AMI wishes to clear and settle Security Tokens on its facility, we expect the firm to comply fully with the requirements proposed in the recommendations in this Part III, as applicable to that firm.

120. However, as there could be variations in the models proposed to be used by an operator of a clearing facility, we expect to adopt a case-by-case approach. This would allow us to examine the particular model being proposed for clearing and settlement of Security Tokens, and consider whether any amendments to the current requirements applicable to clearing houses are needed. Following public consultation, we propose to issue further Guidance.

121. We seek public comment on, particularly in a direct access trading environment:

a) how an operator of a clearing and settlement facility for Security Tokens should determine qualifying criteria for participants so that they can meet all the relevant requirements, including the settlement periods and settlement discipline of the facility;

b) what measures and procedures are needed to be adopted by an operator to address settlement failures; and

c) how the operator should achieve settlement finality, in the DLT application used, from an operational and legal perspective. For example, how, in the consensus validation process associated with DLT, risks resulting from 'forks' are being addressed, and how delivery versus payment (DvP) is achieved, given only the Security Token leg, and not the cash leg, can be processed on DLT.

Questions:

23. Do you agree with our proposal in paragraph 120 to adopt a case-by-case approach to assessing whether a clearing and settlement facility for Security Tokens can meet the applicable requirements? If not, why not?

24. How should the issues identified in paragraph 121 be addressed?

Custody of Security Tokens - Digital Wallets

The current custody requirements applicable to Client Assets (Investments and money)

122. AMI section 5.10 contains the obligations of an AMI operating a trading or clearing facility for the safeguarding and administration of assets belonging to persons who are members and other participants on their facility.[36] Under these requirements, an AMI is required to have safe custody arrangements, to ensure, among other things, the following:

a) member assets (Investments and money) to be properly segregated from its own assets and those of the other members/participants;

b) the operator having prompt access to the assets held under the safe custody arrangements;

c) the use or transfer of assets of members only in accordance with the instructions of the relevant owners of those assets and applicable rules and legislation;

[36] Members of an AMI are regulated firms as the current regime is designed for intermediated access, and not direct access.

d) the reconciliation at appropriate intervals and frequency between the assets and accounts held under the safe custody arrangements; and

e) accurate records relating to the assets held under the safe custody arrangements to be kept, including the identity of the legal and beneficial owners of the relevant assets, records of any additions, reductions and transfers in each individual account of assets, and the identity of the assets owned by different persons.[37]

123. An ATS operator is not authorised under its licence to provide clearing and settlement of transactions of the facility it operates (MTF or OTF). Instead, an ATS operator is required to have satisfactory arrangements in place for securing the timely discharge of the rights and obligations of the client transactions conducted on or through its facility. This essentially means that if the ATS operator were to hold Client Assets for fulfilling client orders, then it will be subject to the Client Asset provisions in COB sections 6.11 and 6.13 as a firm having custody or control of Client Assets.

124. A firm authorised to Provide Custody can also hold Client Assets, where it may do so for an individual or another regulated firm (such as an AMI or ATS operator).

Digital wallets

125. Digital Wallets provide the means by which persons can acquire, hold and transact crypto assets (including Security Tokens). This involves storing/holding the public and private cryptographic keys that enable users to interact with DLT to transact and monitor their balances. As noted before, a public key allows other participants on a distributed ledger to send crypto assets to an address associated with the public key. A private key provides full control of the crypto assets associated with the public key.

126. Wallets come in different forms, for example:

a) a software wallet is an application which may be installed locally, e.g., on a computer or mobile phone or be run on the cloud, which can be accessible by any computing device or location. As software wallets are generally connected to the internet, they are usually 'hot wallets'; and

b) a hardware wallet is a physical device, like a USB stick, which has to be connected to the internet first, before it can interact with DLT to transact. These tend to be kept disconnected from the internet as 'cold wallets'.[38]

Generally, while transacting on a hot wallet is quicker, they are considered less secure due to their propensity to be hacked.

127. DLT networks generally provide their own wallet functions,[39] but there are also specialised wallet providers, who are custodial wallet providers who hold their clients' crypto assets on their behalf.

---

[37] An AMI operating a facility to trade or clear Investments can only delegate the custody function relating to member assets to a DFSA licensed custody provider, or to an appropriate entity licensed and regulated by a Financial Services Regulator to provide custody and depository services, subject to proper due diligence relating to that third party service provider.

[38] The ESMA Advice, paragraph 25.

[39] For example, Bitcoin Core for Bitcoin or Mist Browser for Ether. Ethereum defines its wallet along the lines of a gateway to decentralized applications on the Ethereum blockchain that allows to hold and secure ether and other crypto assets built on Ethereum, as well as write, deploy and use smart contracts.

Analysis

128. The recommendations in this paper apply to custodial wallet providers, who provide the service of custody of crypto assets (e.g. Security Tokens) in a digital wallet, which they may do so either on behalf of a facility that trades and/or clears Security Tokens, or on behalf of clients who trade their Security Tokens on such facilities.

129. There are three aspects that warrant consideration:

a) the provider of the 'Digital Wallet' service;

b) self-custody; and

c) the role of the operator of a facility that trades and/or clears Security Tokens.

130. Providers of Digital Wallet services: A third party who provides the Digital Wallet service that stores Security Tokens falls within the definition of 'Providing Custody' and so we propose to apply the general requirements that apply to such a service provider as a custodian, with some additions set out in paragraphs 136 and 139.

131. Self Custody: If the client has 'self-custody' of the Security Tokens held in the Digital Wallet (by a Digital Wallet service provider to the client), and has the private keys that enable the client to access the wallet, the Security Tokens in the wallet are held at their own risk. Therefore, we do not think it is necessary to apply to the operator of such a facility the custody-specific requirements that apply to custodial wallet providers.

132. Operator holding custody of Digital Wallets: If a facility operator has the custody of clients' Security Tokens by holding their private keys in a DLT-based account under the operator's own private key, we consider that the custody related requirements need to apply to the operator of the facility. As noted in paragraph 51, one model that can be used by the operator of the facility is for the client to be able to deposit or withdraw their tokens on the platform account, with the transaction being usually recorded on DLT (on-chain). This could mean that the rest, i.e. the matching of the orders, the execution of the orders, and the corresponding transfer of the ownership of the crypto assets, is typically recorded in the books of the platform (off-chain). This model may also mean that the operator bears the counterparty risk, vis-à-vis the clients. There may be other models that operators may prefer to use to hold custody of Security Tokens.

133. If the operator has the custody or control of the Security Tokens of the client, notwithstanding the particular DLT model/application being used by the operator, we consider that the operator of the facility should comply with:

a) the custody related requirements under the current DFSA regime fully;

b) the proposed additions set out in paragraphs 135 and 136; and

c) if a direct access model is used, the requirements proposed in paragraph 136.

134. Digital Wallet service providers referred to in paragraph 130 and operators of facilities referred to in paragraph 132 should, as part of their technology governance, be required to ensure the compatibility, resilience and reliability of their DLT applications and the ability to clearly identify and segregate clients' Security Tokens, including the procedure to confirm instructions and transactions, to maintain data relating to such instructions and transactions, and the reconciliation of transactions.

135. As part of their technology governance, the operators and third party Digital Wallet service providers referred in paragraph 134 need to consider, in developing and deploying technology relating to custody of Security Tokens of clients:

a) architecture of the wallets;

b) security measures (including cyber security) and procedures for the safe storage and transmission of data relating to the crypto assets;

c) cryptographic keys and wallet storage, taking into account password protection and encryption that are to be used;

d) methods of usage and storage of keys available under the DLT application used; and

e) procedures and protocols built in to their operating rules to ensure the above.

136. As noted at the outset, the current regime for AMIs is built on intermediated access, and not for direct access for trading and clearing. Direct access to trading and clearing of Security Tokens is generally an accepted form for trading and clearing of such tokens as a class of virtual assets. Taking into account the direct client relationship arising under this model, we consider it appropriate that:

a) an operator of a facility trading Security Tokens be subject to the Client Asset provisions in COB sections 6.11, 6.12 and 6.13, if they hold or control Client Assets, which harmonises the custody of client assets requirements applicable to both AMIs and ATS operators (as the latter is already required to meet the Client Asset provisions in COB sections 6.11 and 6.13, if they have the control or custody of client Investments): and

b) an operator of an ATS (who are not currently permitted to hold client money), be permitted to hold Client Money, as this would be needed to trade Security Tokens, and apply to them the Client Money provisions in COB section 6.12.

We also consider it necessary to apply to an ATS operator referred to in b) prudential requirements that are appropriate for a firm holding Client Money (see Part VI).

137. Where an operator of a facility on which Security Tokens are traded outsources or delegates to a third party service provider the Digital Wallet provider function, the current requirements that generally apply to delegation and outsourcing of functions by a licensee should continue to apply.

138. Even where clients have self-custody of their Digital Wallet, the operator of a facility that trades Security Tokens needs to ensure that the technology used for self-custody of Digital Wallet does not impair the integrity of its own technology for operating the facility and carrying out its obligations as the operator. Due diligence and testing and other procedures would need to be undertaken in relation to technology used by or for the client's self-custody Digital Wallet.

Proposal 14 – Custody of Security Tokens and wallet services

139. We propose that an operator of a facility on which Security Tokens are traded be subject to the requirements in paragraphs 134 to 138. In addition, we note that some case-by-case adjustments may be required to the DFSA regime to accommodate different

models of holding Client Assets for trading purposes that are to be used by an operator of such facilities.

See draft AMI section 5A.4 – at Appendix 4 and, draft COB section 14.3 – at Appendix 5.

Question

25. Do you agree with our custody of Security Token proposals set out in paragraph 139? If not, why not?

Part IV – Issuers of Security Tokens

Prospectus disclosure for public offer, or for admission to trading, of Security Tokens

The current requirements

140. An issuer of Securities (e.g. Shares, Debentures and Warrants) is required to have a Prospectus meeting the DFSA requirements in the Markets Law, and if it is a Unit, a Prospectus under the Collective Investment Law[40] for:

a) making an offer of its Securities to the public; or

b) admitting their Securities to the Official List of Securities (maintained by the DFSA) and, to trading on an AMI.

141. The DFSA prospectus regime is modelled on the UK/EU framework, including the Prospectus Directive. A prospectus for public offer, or listing and trading, must contain certain disclosures specified in the MKT module (and if a Fund, in the CIR module), and be approved by the DFSA.[41] The prospectus disclosure is designed so that prospective investors in Securities have sufficient information to make an informed assessment of the assets and liabilities, financial position, profits and losses, and prospects of the issuer and any guarantor, and the nature of the Securities and the rights and liabilities attaching to the relevant securities.[42] The DFSA regime prescribes detailed prospectus disclosure requirements and also provides appropriate flexibilities.

142. The full prospectus requirements apply, unless it is an 'Exempt Offer' of Securities permitted under the Markets Law. In the case of offers of Units of Funds, the Information Memorandum requirements apply to offers that are made exclusively to Professional Clients by private placement, unless an exemption applies. The issuers and persons responsible for the disclosure in a Prospectus or Information Memorandum face the legal liability regime under the Markets Law or the Collective Investment Law for prospectuses.

Analysis

143. Consistent with Proposal 1, we consider that the prospectus requirements that normally apply for a public offer of Securities (Initial Public Offerings or IPOs), or for having the Securities admitted to trading on a trading facility in the DIFC, should apply to the public offer, or admission to trading, of Security Tokens. We will consider, any documents used

[40] The DFSA's regulatory regime applies to issuers which are domestic companies, as well as to foreign issuers if they are making a public offer in or from the DIFC, or they seek to list on an AMI.
[41] If the securities are Islamic securities there are additional prospectus requirements in the IFR module.
[42] See Article 15 of the Markets Law and Article 52 of the Collective Investment Law.

for mass marketing of Security Tokens that are Investments, which are often called a 'white paper', to be a prospectus if it offers Security Tokens to the public, unless it is an Exempt Offer (see Exempt Offers in paragraphs 151 to 153).

144. While we do not propose any fundamental dilution to the current prospectus regime for the offer to the public and admission to listing and trading of Security Tokens, we consider that there is a need for clarification relating to how the current disclosure regime applies to persons making a public offer or making an application to have Security Tokens admitted to trading on a trading facility.[43]

145. We note that persons developing or providing technology for the creation of Security Tokens using DLT may not necessarily be the persons offering those tokens as a means of investment or, for that matter, for use for other purposes. As noted before, the DFSA prospectus regime provides flexibility for Securities to be offered to the public, or the Securities to be admitted to listing and trading on a trading venue, either by the Issuer (for example, the company that issues the shares or debentures), or another person who takes the responsibility for the offer. These persons are required to make disclosures relating to the relevant Security, including on to whom the rights and obligations associated with the Security of the type offered will attach, and how those will be fulfilled or discharged. This essentially means that the offer to the public or admission to trading of a Security Token, which confers rights and obligations that are the same, or substantially similar in nature, purpose or effect, as an Investment, will be prohibited, unless the Prospectus regime is fully complied with[44] or an exemption applies.

146. Generally, as mentioned before, white papers are used for the offer of Security Tokens. Such a white paper will attract the prospectus obligations, including legal liability, under the DFSA regime, if the offer relates to rights and obligations that qualify as a Security Token, and if it involves an offer to the public, or an application to have the tokens admitted to trading and clearing on a trading venue. Such an offer may involve rights to the development of technology to create an application/token, or an offer of rights and interests (equity or debt) in a business (not just the rights to a DLT application to be developed), where the title to those rights and interests are stored, recorded, and are transferable, using DLT. We propose to apply to the person making the offer to the public, or the application to have the Security Tokens admitted to trading, the prospectus obligations in full, with some additions proposed (see paragraphs 147 to 149).

147. We believe that in the DLT environment, the prospectus, which is the offer document (whether called a white paper or not), and the application forms to invest in Security Tokens, may well be distributed as some form of smart contract.[45] The platform on which Security Tokens are offered may also be the trading/clearing venue for those Security Tokens. Regardless of these differences, we expect the underlying obligations relating to the prospectus obligations, including publication to be fully met by the issuer and other persons responsible for the prospectus, with the enhancements proposed in paragraphs 148 and 149.

148. We consider that, in addition to meeting the current prospectus disclosure obligations, a person making an offer of Security Tokens to the public, or seeking to have the Security

[43] See Recommendation 11 where we propose that both ATS and AMIs be allowed to admit to trading Security Tokens on their facilities, without maintaining the current distinction.

[44] See Article 11 of the Markets Law and Article 50 of the Collective Investment Law.

[45] 'Smart contracts' are computer code in which contracts are written in to the distributed ledger. There can be different models, for example, a smart contract can solely consist of a code, or a combination of a code and natural language contract. It is important to recognise that a smart contract, written in part or otherwise in code, is not necessarily a smart *legal* contract, but this risk needs to be addressed by the operator of a facility that facilitates the issue of Security Tokens.

Tokens admitted to trading, should include in their offer documents the following disclosure:

a) the type of rights and interests attaching to the Security Tokens offered – for example, whether the Security Tokens offer rights and interests that are as same as, or substantially similar in nature, purpose or effect, to a Share, Debenture, Unit or Warrant, and who is responsible for the discharge of the rights and obligations attaching to the Security Tokens (see also the Guidance on criteria for determining whether a Security Token is a particular type of Investment); and

b) if a Security Token referred to in a) raises capital to create a new type of crypto asset, using the capital from investors, detailed information about:

   i) the issuer's venture to be funded;

   ii) whether it is the issuer or some other third party who will receive and apply the capital raised towards that venture (and if a third party, what rights and obligations the investor has in respect of it);

   iii) the features and rights attaching to the crypto asset being created;

   iv) the terms and conditions and expected timetable for completion; and

   v) risks, including those associated with the DLT or other similar technology being used.

149. Further, a Prospectus for the offer to the public of, or for admission to trading on a facility for Security Tokens, needs to include the following information and sign-offs:

a) the nature of the DLT, or similar technology, application that is being used;[46]

b) whether the Security Tokens are to be listed and traded on a facility, details relating to the facility, and who is responsible for the operation of that facility, including, as relevant:

   i) whether and what form of smart contracts are being used or executed on the facility;

   ii) if, and how, any smart contract confers legal rights and obligations;[47] and

   iii) when the settlement finality occurs (on line, or off line on the books of the facility operator); and

c) the manner in which, and by whom, Security Tokens are to be held, including:

   i) who provides the Digital Wallet services;

---

[46] A particular DLT implementation used for the issue and distribution of Security Tokens and their trading, and the DLT implementation of the operator of a facility on which those Security Tokens are traded and/or cleared, can have different functionalities. For example, the facility operator may use a DLT implementation which, in addition to the functions of matching buy and sell orders, can be designed to carry out the clearing and settlement functions through connectivity to Digital Wallets and investor funds held in their bank accounts.

[47] A smart contract is not necessarily the full legal contract. Only a part of the full contract may be written in code to be embedded in the DLT implementation used by the STM. In this context, the relationship between the smart contract and the full legal contract would need to be clarified.

ii) by whom the Digital Wallets are maintained, including whether the wallets are held by the investor (self-custody), or by or on behalf of the operator of the facility; and

iii) risks associated with Digital Wallet, such as the consequences of loss of cryptographic keys (private and public), hacking of hot wallets, loss, theft or destruction of cold wallets and whether and how such risks are addressed;

d) how the evidence of title to Security Tokens will be established/certified/evidenced;

e) issues relating to governance of the technology underlying the Securities Token as outlined in paragraph 61;

f) cyber-attack risks, and the possible loss of Security Tokens and how they can be mitigated;

g) any other information that would enable investors to make an informed judgement about investing in the Security Tokens offered; and

h) a sign-off by a technology expert ('technology sign-off')[48] of the authenticity, validity and workability of the technology being used to meet the obligations relating to the offer of Security Tokens.

The above list is not exhaustive and, following public consultation, we may make further refinements to this.

Proposal 15 – Prospectus for Public Offer/Admission to trading

150. We propose that a prospectus, for the offer to the public or for admission to trading, of Security Tokens comply with all the current disclosure requirements under the DFSA regime, and, in addition, comply with the disclosure and technology sign-off set out in paragraphs 148 and 149.

See draft MKT Rules 2.5.1(3)(d) and App 7 Guidance – at Appendix 7.

Question

26. Do you agree with our proposed additional prospectus disclosure in paragraph 150? If not, why not?

Exempt Offers and Exempt Securities

The current requirements

151. The DFSA regime, in line with the EU regime under the Prospectus Directive, permits a number of Exempt Offers to be made to the public without a full prospectus. The key categories of exempt offers are:

a) an offer made or directed at only Professional Clients other than individuals;

[48] Meeting the same standards as proposed for the person providing the technology audit under Proposal 6.

b) an offer directed to fewer than 50 persons over 12 months, excluding Professional Clients other than individuals;

c) an offer where the total consideration to be paid by a person for acquiring the Securities is at least USD 100,000;

d) an offer where the denominated value of the Security is at least USD 100,000;

e) an offer where the total aggregate capital raised over a period of 12 months is less than USD 100,000;

f) a conversion of existing Securities that does not involve any additional capital raising;

g) a conversion of convertible securities already issued; and

h) an offer associated with a takeover or merger where the takeover/merger disclosure requirements are met; an offer without consideration to existing shareholders; and employee share scheme offers.

See MKT 2.3.1 for the full list.

152. Similarly, certain Securities are Exempt Securities and can be admitted to trading on a facility without being subject to the full prospectus requirement. These Exempt Securities include:

a) Shares representing, over a period of 12 months, less than 10 per cent of the number of Shares of the same class already admitted to trading on the same facility;

b) offers of Securities associated with an on-market takeover or merger that is accompanied with a document containing equivalent disclosure as in a prospectus; and

c) Shares resulting from a conversion or exchange of Securities, where the Shares are of a class already admitted to trading on the facility.

See MKT 2.4.1 for the full list.

Analysis

153. We recognise that not all the above Exempt Offers may be appropriate for a public offer of Security Tokens. For example, even if it is a small scale offer of Security Tokens to the public, investors would need adequate disclosure relating to the Security Tokens that are being offered. An example is an offer of a Security Token where the aggregate capital raised over 12 months will be less than USD 100,000.

Proposal 16 – Exempt Offers

154. While we propose to apply the majority of exemptions noted above to Security Token offerings, the need for adequate consumer protection, especially for retail clients, in this new area suggests that some exemptions may not be appropriate. Therefore, we seek public comment on whether any current Exempt Offers should not apply to the offer of Security Tokens directed to retail clients.

Questions:

27. Do you agree with our proposal in paragraph 154 to apply the majority of current exemptions to Security Token offerings? If not, why not?

28. What are, if any, the types of exemptions from the prospectus disclosure that should not apply to retail offers of Security Tokens?

Fund prospectuses

The current requirements

155. Where the Units of a Fund are offered to the public, the Prospectus regime that applies to a Collective Investment Fund (Fund), and not the MKT prospectus disclosure regime, applies. The detailed disclosure required in a Fund prospectus is set out in CIR chapter 14. Whilst MKT chapter 6 contains bespoke requirements for Listed Funds, the Fund prospectus must still be prepared in accordance with the disclosure requirements in chapter 14 of CIR.

Analysis

156. If a Security Token represents rights and obligations that are the same as, or substantially similar in nature, purpose or effect to, a Unit in a Fund, then, the Security Token would be a regulated as a Unit of a Fund (see Proposal 1). We consider, that in addition to the current prospectus disclosure required under the Funds regime, the Fund Manager should be required to comply with:

a) the additional disclosure and the technology sign-off set out in paragraphs 148 and 149, in the case of an offer to the public, or admission to trading of the Fund Units which are Security Tokens; and

b) the additional disclosure in a) above, in an Information Memorandum used for an offer of Units which are Security Tokens of an Exempt Fund or Qualified Investor Fund (i.e. offers to Professional Clients by private placement).

157. We note that if the Fund Manager proposes to operate an open-ended Fund, using DLT or similar technology to issue and redeem Fund Units, the Fund Manager does not need to be regulated as an operator of a facility for trading Security Tokens. This is because the Fund Manager is the counterparty in the issue and redemption of Units, and hence its activities do not constitute operating a facility on which third party buying and selling of Units is facilitated.

158. We also note that some Funds may invest in Security Tokens or other types of crypto assets. If this is the case, the Fund Prospectus or Information Memorandum will need to meet the disclosure and technology sign-off of the kind referred to in paragraphs 148 and 149 relating to its underlying assets to the extent they are Security Tokens, with some adaptations as needed, if they are other type of crypto assets.

159. We note that a *de minimis* threshold applies for the additional disclosure to be needed in some jurisdictions. For example, Hong Kong SFC requires the additional disclosure only if 10% or more of the underlying assets of the Fund are crypto assets. We seek public comment on whether such a threshold is warranted.

Proposal 17 – Fund Prospectuses

160. We propose to apply to offers to the public, or admission to trading, of Security Tokens that are Units in a Fund the additional disclosure set out in paragraph 156, and if the underlying assets of the Fund are Security Tokens or other crypto assets, the disclosure of the kind referred to in paragraph 158, subject to a *de minimis* threshold as proposed in paragraph 159.

See draft CIR Rules 14.3.1(1)(f) and (g) and Guidance at 14.3.2 – at Appendix 8.

Questions:

29. Do you agree with our proposed disclosure requirement in paragraph 160? If not, why not?

30. Should we impose a 10% threshold, or some other threshold, before a Fund is required to make the disclosure in paragraph 159?

Distribution of Foreign Security Tokens

The current requirements

161. In the case of an offer of Securities to the public, or admission to listing and trading, of foreign Securities (other than Units in Funds), a foreign prospectus that is approved by the DFSA and meeting the requirements in MKT section 2.7 is required. If Security Tokens that are Units of a Foreign Fund are to be admitted to trading, the prospectus disclosure requirements referred to in paragraph 155 apply. These require equivalence of information with the DFSA prospectus regime.

162. Units of Foreign Funds cannot be offered in or from the DIFC, unless the Foreign Fund meets the criteria for a Designated Fund from a Recognised Jurisdiction or, the other criteria prescribed in CIR are met (see Article 54(1) of the Collective Investment Law and CIR section 15.1).

Analysis

163. We believe that the above requirements should continue to apply to the offer to the public in or from the DIFC, or admission to trading on a facility in the DIFC, of foreign Security Tokens, with the additional disclosure and technology sign-off set out in paragraphs 148 and 149. In the case of offers of Security Tokens that are Units in Foreign Funds in or from the DIFC, the criteria for Foreign Funds should continue to apply, with the prospectus requirements meeting those under Proposal 17.

Proposal 18 – Distribution of Foreign Security Tokens

164. We propose to adopt the approach set out in paragraph 163 to offerings of foreign Security Tokens.

See draft MKT Rules 2.7.1(3), 6.3.3(3) – at Appendix 7 and, draft CIR Rule 14.2.6(3) and (4) and associated Guidance – at Appendix 8.

Questions:

31. Do you agree with our proposal in paragraph 164? If not, why not?

32. Are there any additional controls that should apply to the distribution of foreign Security Tokens? What are they and why should they be applied?

33. Alternatively, should we prohibit the offering of foreign Security Tokens in or from the DIFC?

Ongoing disclosure and market conduct

The current requirements

165. Where Investments are admitted to trading on an AMI, the persons responsible for having the Investment admitted to trading must keep the market informed of all the relevant information that would impact on the price of the relevant Investments. In addition to the ongoing disclosure, there are on-market conduct requirements that apply to Investments that are admitted to trading, such as those relating to additional offers of an existing class of Securities already admitted to trading (e.g., pre-emption rights related obligations), the procedures relating to buy-back of Securities, and takeovers and mergers provisions.

Analysis

166. Where Security Tokens qualify as Investments under Proposal 1, and are admitted to trading, we consider it is appropriate to continue to apply the above requirements to the person responsible for having Security Tokens admitted to trading. In addition, we consider matters that could affect market price due to the use of DLT or similar technology, such as interruptions (e.g., due to forks) and cyber-attacks, would also need to form part of the matters that require disclosure to markets, under these obligations.

Proposal 19 – On-going disclosure

167. We propose to apply to persons responsible for having Security Tokens which qualify as Investments admitted to trading on a trading facility the same ongoing disclosure and conduct requirements as those applying to persons responsible for conventional Investments, including disclosure of factors impacting on the price of the relevant Security Tokens (Inside Information), due to the use of DLT, as noted in paragraph 166.

See draft amendment to Article 38 of the Markets Law – at Appendix 2, and MKT Rules 4.2.1 (Guidance item 17), 6.1.1 and 6.5.1 (Guidance item 16) – at Appendix 7.

Question

34. Do you agree with our proposal in paragraph 167? If not, why not?

Market abuse

The current requirements

168. Part 6 of the Markets Law contains the provisions dealing with prevention of market abuse. These apply to all Investments, whether listed and traded, or otherwise, and include provisions designed to address fraud and market manipulation, use of fictitious devices and other forms of deception, false and misleading conduct and distortion, insider dealing and providing inside information, inducing persons to deal through statements which are misleading, false or deceptive, and misuse of information. The DFSA's Code of Market Conduct provides further guidance on how these provisions apply in given scenarios.

Analysis

169. As our current regime is cast broadly to capture market misconduct, we expect these requirements will apply to Security Tokens to address market abuse. However, we consider that some further explanation may be needed of how the market abuse provisions would apply to various participants in the DLT environment, such as those undertaking the role of validating and updating the distributed ledger, e.g., miners.[49]

Proposal 20 – Market abuse

170. We propose to apply our current market misconduct requirements to persons dealing with Security Tokens as specified in paragraph 169 and to seek public comment on whether further clarifications and enhancements are needed to our regime, including to the Code of Market Conduct, to address risks of market abuse relating to distribution and trading of Securities Tokens.

See draft COB Rule 9.6.9 (Guidance item 4) – at Appendix 5 and draft AMI Rule 5.11.2 (Guidance item 3) – at Appendix 4.

Question

35. Do you agree with our proposal in paragraph 170? If not, why not?

Financial promotions

The current regime

171. The current regime relating to Financial Promotions applies to both financial products (which include Investments) and financial services. Article 41A of the Regulatory Law contains the Financial Promotions Prohibition. Under that prohibition, financial promotions, i.e. the marketing of financial products and financial services, cannot be undertaken, unless the requirements relating to marketing in GEN Chapter 3 are met. These permit Financial Promotions to be undertaken by regulated firms and, in very limited circumstances, by other persons, subject to additional requirements.[50]

172. Where Security Tokens are Investments under Proposal 1, the full Financial Promotions regime should apply to any marketing activities relating to Security Tokens. We note that in the case of web-based offers of Security Tokens accessible by potential investors in the DIFC, we consider such offers, like all other internet based offers of Investments into the DIFC, to be subject to the Financial Services and Financial Promotions Prohibitions, unless the offer expressly states that it is not intended for prospective investors in the DIFC and, will not allow DIFC based investors to accept those offers.

Proposal 21 – Financial Promotions

[49] As is the practice in the benchmarked jurisdictions, we do not currently propose to regulate participants on a DLT application used by regulated entity, such as miners. We also will not allow completely automated, permissionless (public) DLT applications to be used for the distribution, trading and clearing of Security Tokens. The operator of the facility will be responsible for the permissioned participants on its DLT, including any miners. The operator should have mechanisms to address market abuse that can arise, for example, if a particular miner or group of miners is able to control over 51% of the consensus, to address the risk that such miners could reject valid transactions and approve invalid transactions. Misuse of that power could vary from outright theft to generating transactions intended to move the market price. There may also be a potential for miners to have access to, and misuse, inside information related to the timing of clearing of trades transacted.

[50] For example, the marketing material having to be clear, fair and not misleading and, if the marketing material contains forecasts based on assumptions, to contain a balanced view of the financial products.

173. We propose to apply the Financial Promotions Prohibition to marketing of Security Tokens that are Investments, so marketing would be permitted only where the requirements in GEN Chapter 3 are met.

See draft GEN Rule 3.3.1 and associated Guidance – at Appendix 3.

Question

36. Do you agree with our proposal in paragraph 173? If not, why not?

Part V: Other Financial Services relating to Security Tokens

Licensing

174. If a person conducts a Financial Service relating to Investments, by way of business, the person needs to be licensed by the DFSA, unless the activities are excluded from regulation. The Financial Services relevant for Security Tokens are Dealing in Investments as Principal, Dealing in Investments as Agent, Arranging Deals in Investments, Managing a Collective Investment Fund, Managing Assets, Advising on Financial Products, Providing Custody, Arranging Custody, Operating an Exchange, Operating a Clearing House, Operating an Alternative Trading System, Operating a Crowdfunding Platform and Acting as a Representative Office.

175. We have already proposed some substantive requirements applicable to the conduct of some of those Financial Services involving Security Tokens, such as Operating an Exchange, Clearing House or Alternative Trading System, or Providing Custody or Managing Funds.

176. While we do not think that it is necessary to create a bespoke type of Financial Service for persons conducting Financial Services relating to Security Tokens that are Investments, we think that some form of identification of firms that wish to carry on Financial Services relating to Security Tokens is needed, to ensure that firms providing such Financial Services fully meet the relevant requirements, and to indicate to the users and other stakeholders that additional regulatory requirements apply to such firms.

Proposal 22 – Licensing

177. We propose to:

a) apply the current Financial Services requirements as applicable to the activities relating to Security Tokens where such Tokens are Investments, as this approach is consistent with the approach adopted in other jurisdictions we benchmarked against, such as the UK and the EU; and

b) apply the IT/DLT audit requirements in Part III to these firms for their services reliant on DLT or similar application.

See draft COB Rule 14.5.1 – at Appendix 5.

Questions:

37. Do you agree with our proposal in paragraph 177? If not, why not?

38. Are there any additional concerns that should be addressed? What are they, and how should they be addressed?

Disclosure

178. Given some of the unique characteristics of Security Tokens, we believe that firms undertaking Financial Services relating to Security Tokens should be required to provide to their clients, in the form of a key features document, the disclosure set out in paragraph 179. The obligation to issue a key features document should apply to firms that are required under COB section 3.3 to enter into a Client Agreement with their clients, where:

    a) they provide Financial Services relating to Security Tokens; and

    b) the firm does not provide to the client a prospectus (as a prospectus relating to Security Tokens contains additional information relating to such tokens).

179. The key features document should include:

    a) the risks associated with, and essential characteristics of, the Security Token issuer (or other person responsible for discharging rights and obligation relating to Security Tokens), and guarantor if any, of the tokens, including their assets, liabilities and financial position;

    b) the risks associated with, and essential characteristics of, the relevant Security Tokens including rights attaching to those tokens;

    c) whether the Security Tokens are admitted to trading and, if so, the details relating to that facility, and whether the facility is in or outside the DIFC;

    d) whether the client can directly access the trading facility, or whether access is only through the firm, and the process for accessing the facility;

    e) risks associated with the use of DLT or similar technology, particularly those relating to Digital Wallets, whether the client or the firm or a third-party is responsible for providing the Digital Wallet, and any risks the client needs to be aware of (for example, at whose risk the client's Security Tokens are held in the wallet, whether it is a hot or cold wallet, what happens if keys to the Digital Wallet are lost, and what procedures can be followed in such an event);

    f) how the client may exercise their rights relating to the relevant Security Tokens – for example, voting and participation in shareholder actions; and

    g) any other information relevant to the particular Security Tokens that would assist the client to understand the product and technology better and to make an informed decision.

180. The above is an indicative, rather than an exhaustive, list of items to be covered, and gives the flexibility for firms to tailor the level of detail that needs to be disclosed to their clients, based on the particular type(s) of Security Token in respect of which the financial service is provided.

181. Such information may be included in the Client Agreement, or be provided separately as and when the firm provides financial services relating to any Security Token. Repeated disclosure to the client would not be required if the product profile is similar to those in relation to which previous disclosure has been made to the particular client, and there is no significant time gap between the previous disclosure and the current service.

Proposal 23 – Key features document relating to Security Tokens

182. We propose that Authorised Firms who offer Financial Services to clients in respect of Security Tokens be required to, in addition to entering into a Client Agreement with such clients, provide to those clients a key features document relating to Security Tokens, as set out in paragraph 179 to 181.

See draft COB section 14.4 – at Appendix 5.

Question

39. Do you agree with our proposal in paragraph 182? If not, why not?

Islamic Financial Services and products

The current regime

183. Islamic Finance requirements in the IFR module apply to persons conducting in or from the DIFC Islamic Finance Business[51] and, similarly, to persons offering Investments which are held out as Islamic or Shari'a compliant in or from the DIFC. If Security Tokens represent rights and obligations that are the same or substantially similar in nature, purpose or effect to those conferred by Investments (see Proposal 1), and are held out as Islamic or Shari'a compliant, the requirements in the IFR module will apply to such persons. We do not consider any changes are needed to the current Islamic Finance regime to accommodate the conduct of financial services and the offering of Security Tokens which are held out to be Islamic or Shari'a compliant.

Proposal 24 – Islamic Financial Services and products

184. We propose to apply the IFR module to any financial service or product offering involving Security Tokens if they are, or held out as, Islamic or Shari'a compliant and will give Guidance to that effect.

See draft IFR Rules 1.1.1 (Guidance item 3) – at Appendix 9.

Question

40. Do you agree with our proposal in paragraph 184? If not, why not?

Part VI: Other issues

DFSA Fees

185. Once Security Tokens are Investments, persons conducting Financial Services relating to such tokens will face a number of fees. We have addressed below the key areas of Financial Services that are affected by the proposals and how we propose to levy fees.

[51] Any part of the financial business of an Authorised Person which is carried on in accordance with Shari'a.

Issuing, trading and clearing Security Tokens

The current requirements

186. Under the current regime, there are different fees payable by market operators and issuers of Securities admitted to trading, as follows:

a) for operating a market:

i) if it is an ATS operator – an application fee, and an on-going annual fee, each amounting to USD 65,000; and

ii) if it is an AMI – an application fee of USD 150,000, and an on-going annual fee of USD 100,000;

b) for admission of Securities to the List – a fixed fee of USD 2,500;

c) for the approval of a prospectus, a variable fee based on the specified type of Security (e.g. shares, debentures) and nature of the Issuer (SME or non-SME); and

d) for any endorsement, such as for conducting retail or Islamic financial services, different fees.

Analysis

187. We consider that some, but not all, current fees need to be increased for regulated activities involving Security Tokens to reflect the additional work required in administering and monitoring the proposed new requirements.

188. We consider an ATS that acts as the primary venue for admission to trading of Security Tokens should pay the same application fee, and the same annual fee, amounting to USD 150,000, and USD 100,000 respectively, as paid by an AMI (noted in paragraph 186a)ii), as well as a fee of USD 2,500 for the admission to trading of such Security Tokens (noted in paragraph 186b)).

189. We consider that AMIs and ATSs that operate direct access markets for trading Security Tokens would require additional monitoring and supervision and hence warrant a higher fee of USD 10,000 more than the normal supervisory fees noted in paragraph 186a) (with the amendment of ATS fees noted in paragraph 188.

190. We consider the current admission fees for listing and trading should remain at USD 2500.

191. We propose to require a retail endorsement (and the associated fee of USD 20,000) for firms providing Financial Services relating to retail clients, including in direct access to trading models used by operators of trading facilities, as we normally do for retail services, as those firms are required to carry out KYC/AML monitoring of such clients.[52] If a firm is conducting Financial Services that are Shari'a compliant, an Islamic Financial Services endorsement would also be needed.

[52] See also the IOSCO consultation referred to in footnote 3, which emphasises the importance of applying the standards applicable to intermediaries to token market operators with direct access to address AML/CTF, KYC and suitability related risks.

192. We do not propose to make other changes to our fees applicable to firms conducting Financial Services relating to Security Tokens.

Proposal 25 – Fees

193. We recommend applying fees in the manner specified in paragraphs 189 and 190.

See draft FER Rules 2.1.2(2) and (3), 2.1.5, 2.2.4, 3.2.1(d), 3.2.3, 3.4.1, 3.4.4, 3.4.5 and 4.1.2 – at Appendix 10.

Question

41. Do you agree with our proposals in paragraph 193 relating to fees? If not, why not?

Prudential requirements for ATS operators

194. We do not consider any changes to the current prudential requirements are needed for AMIs and other Financial Service providers who will be undertaking activities relating to Security Tokens, except for the current prudential requirements applicable to an ATS operator. This is because an ATS operator would be allowed to hold client money under our current proposals when trading Security Tokens (see paragraph 136). The current capital requirement for an ATS operator is set as the higher of a base capital requirement of USD 10,000 or an expenditure based capital minimum of 6 weeks (6/52).

195. We consider that an ATS operator should be subject to a capital requirement in line with the capital requirement for a Crowdfunding Operator, which is the only similar (i.e., assigned to PIB Prudential Category 4) firm that is allowed to hold client money. This is the higher of a base capital requirement of USD 140,000, but with the higher expenditure based capital minimum of 18 weeks (18/52) instead of 6 weeks (6/52).

196. An ATS operator is not required to hold professional indemnity cover under the current regime. We consider that in a direct access market environment proposed for trading in Security Tokens, it is necessary for an ATS operator to be required to obtain and maintain professional indemnity cover appropriate to the nature, size, complexity and risk profile of its business.

Proposal 26 – Prudential requirements for an ATS operator

197. We propose that an ATS operator permitted to trade on its MTF or OTF Security Tokens be required to:

a) meet the capital requirement proposed in paragraph 196; and

b) obtain and maintain adequate professional insurance cover.

See draft PIB Rules 3.6.2, 3.7.2(e), 6.1.1(c)(xviii) and App 6 (Guidance item 2) at Appendix 6.

Question

42. Do you agree with our prudential proposals in paragraph 197? If not, why not?

Recognition of Foreign Markets

<u>The current requirements</u>

198. Under the REC module, a person that operates an exchange, clearing house or alternative trading system in a jurisdiction other than the DIFC can operate such facilities if that person has been admitted to the DFSA's list of recognised bodies. These recognised bodies may wish to trade and/or clear on their facilities Security Tokens.

Analysis

199. A person operating a facility to trade or clear Security Tokens that confer rights and obligations the same as, or substantially similar in nature, purpose or effect to, Securities or Derivatives are within our classification of Investments under Proposal 1. If the operator of such a facility is subject to similar obligations in its home jurisdiction as those required by the DFSA, we do not see any significant impediments to Security Tokens being traded/cleared on a facility operated by a recognised person, and expect to deal with such applicants on a case-by-case basis in going forward.

Proposal 27 – Recognition of Foreign Markets

200. We propose that recognised persons be permitted to operate facilities on which Security Tokens are cleared/settled, and seek public comment on whether there are any specific issues that need to be addressed in this context.

Question

43. Do you agree with our proposal in paragraph 200? If not, why not?

Transitional issues

Proposal 28 – Transitional arrangements

201. If our proposals to classify some Security Tokens as Investments are to be adopted, it may not be possible for market participants to be able to comply with at least some requirements immediately. Therefore, we propose to seek public comment on whether any transitional arrangements are needed to meet the proposed requirements, the reasons for such a transitional period and the suggested length of any period.

Questions

44. Please explain why a transitional period is necessary. Please also set out what would be an appropriate period of transition, and explain why.

45. Are there any other issues that need to be addressed regarding the regulation of Security Tokens? If so, what are they, and why and how should they be addressed?

Annex 1: Questions in this Consultation Paper

Question 1: Do you agree with our proposal to treat as Investments Security Tokens that confer rights and obligations that are the same as, or similar in nature to, those conferred by Investments? If not, why not?

Question 2: Do you agree with us that the term Security Token is appropriate if the token confers rights and obligations under a Derivative contract? If not, should they be referred to as Derivative Tokens? Please explain your thinking?

Question 3: The proposed definition of Security Tokens would not apply to tokens with hybrid characteristics of a number of different types of Securities and Derivatives, but with no substantially similar rights and obligations relating to any one of them. Do you think our definition of Security Tokens should capture such hybrid products as Investments? Please explain your thinking.

Question 4: Do you agree with our proposal to adopt a hybrid approach to assessing whether a Security Token is an Investment and, if so, what type or types of an Investment? If not, why not?

Question 5: Do you think it is appropriate to prohibit the use of the labels Security Tokens, Derivative Tokens or Investment Tokens (or any derivative of those), unless the tokens meet the definition of Security Tokens? If not, why not?

Question 6: Do you agree with our proposal to allow AMI and ATS operators to operate facilities to trade Security Tokens, subject to the additional requirements proposed in this paper? If not, why not?

Question 7: Do you agree with our proposals to allow only an AMI holding a licence to Operate a Clearing House to clear Security Tokens? If not, why not?

Question 8: Do you think we should require an AMI to establish two separate legal entities for trading and clearing of Security Tokens? If not, what are your reasons?

Question 9: Do you agree with our proposal to prohibit the use of the terms such as Security Token Market or Security Token Clearing House (or similar terms and abbreviations) as noted in paragraph [46] (c) and (d)]? If not, what are your reasons?

Question 10: Do you agree with our proposal to give detailed Guidance relating to IT-related requirements for operators of facilities that trade and/or clear Security Tokens as noted in paragraph 62? If not, why not?

Question 11: Do you agree with our proposal to require an independent audit of technology governance? If not, what other options can provide the necessary degree of assurance that is required in this area?

Question 12: Should the IT audit be carried out by a Registered Auditor? If so, what accreditation should such an auditor have?

Question 13: Do you agree with our proposal to allow direct access to Security Token trading subject to the additional requirements in paragraphs 77 and 78? If not, why not?

Question 14: Do you agree with our proposal to include these requirements as part of the IT- related enhancements proposed for markets trading in Security tokens? If not, why not?

Question 15: Should we confine direct access to trading in Security Tokens for Professional Clients only? If so, what are your reasons?

Question 16: Should we limit the participation of Retail Clients in these markets, as an investor protection measure, by placing limits on the parcel size or volume of their trading activity? If not, why not?

Question 17: Do you agree with our proposals on direct access to conventional markets? If not, why not?

Question 18: Do you agree with our proposal to allow an ATS operator to admit to trading Security Tokens on its facility, as proposed in paragraph 96? If not, why not?

Question 19: Do you think that it is appropriate to allow an OTF, a facility operated by an ATS operator, to be a primary venue for admission to trading of Security Tokens? If yes, please explain why?

Question 20: Do you agree with our Proper Markets proposal in paragraph 101? If not, why not?

Question 21: Do you agree with our proposal to apply the current rules relating to business/operating rules, subject to adaptations to cater to direct access clients, as proposed in paragraph 104? If not, why not?

Question 22: Are our proposals in paragraph 109 sufficient? If not, what else is needed?

Question 23: Do you agree with our proposal in paragraph 120 to adopt a case-by-case approach to assessing whether a clearing and settlement facility for Security Tokens can meet the applicable requirements? If not, why not?

Question 24: How should the issues identified in paragraph 121 be addressed?

Question 25: Do you agree with our custody of Security Token proposals set out in paragraph 139? If not, why not?

Question 26: Do you agree with our proposed additional prospectus disclosure in paragraph 150? If not, why not?

Question 27: Do you agree with our proposal in paragraph 154 to apply the majority of current exemptions to Security Token offerings? If not, why not?

Question 28: What are, if any, the types of exemptions from the prospectus disclosure that should not apply to retail offers of Security Tokens?

Question 29: Do you agree with our proposed disclosure requirement in paragraph 160? If not, why not?

Question 30: Should we impose a 10% threshold, or some other threshold, before a Fund is required to make the disclosure in paragraph 159?

Question 31: Do you agree with our proposal in paragraph 164? If not, why not?

Question 32: Are there any additional controls that should apply to the distribution of foreign Security Tokens? What are they and why should they be applied?

Question 33: Alternatively, should we prohibit the offering of foreign Security Tokens in or from the DIFC?

Question 34: Do you agree with our proposal in paragraph 167? If not, why not?

Question 35: Do you agree with our proposal in paragraph 170? If not, why not?

Question 36: Do you agree with our proposal in paragraph 173? If not, why not?

Question 37: Do you agree with our proposal in paragraph 177? If not, why not?

Question 38: Are there any additional concerns that should be addressed? What are they, and how should they be addressed?

Question 39: Do you agree with our proposal in paragraph 182? If not, why no

Question 40: Do you agree with our proposal in paragraph 184? If not, why not?

Question 41: Do you agree with our proposals in paragraph 193 relating to fees? If not, why not?

Question 42: Do you agree with our prudential proposals in paragraph 197? If not, why not?

Question 43: Do you agree with our proposal in paragraph 200? If not, why not?

Question 44: Please explain why a transitional period is necessary. Please also set out what would be an appropriate period of transition, and explain why.

Question 45: Are there any other issues that need to be addressed regarding the regulation of Security Tokens? If so, what are they, and why and how should they be addressed?