Dubai Financial Services Authority

CONSULTATION PAPER 153

UPDATES ON THE REGULATION OF CRYPTO TOKENS

4 JANUARY 2023

PREFACE

Why are we issuing this Consultation Paper?

1. This Consultation Paper (CP) seeks public comment on proposals for amendments to our regulatory regime for persons wishing to provide financial services activities in respect of Crypto Tokens. The development of these proposals is based on our supervisory experience, recent market events and recommendations from international standard setters.

What is not covered under this Consultation Paper?

2. All the proposals in this paper relate only to Crypto Tokens. The regulation of Investment Tokens is not dealt with in this paper.

Who should read this CP?

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

   a) Authorised Market Institutions (AMI) wishing to admit Crypto Tokens to trading, or clearing or settlement, on their facilities;

   b) Operators of Alternative Trading Systems (ATS) wishing to trade Crypto Tokens on their facilities;

   c) Custodians and Third Parties who safeguard and administer Crypto Tokens;

   d) Authorised Firms wishing to carry on other Financial Services relating to Crypto Tokens, such as dealing in, advising on, or arranging transactions relating to Crypto Tokens, managing discretionary portfolios or collective investment funds investing in Crypto Tokens or effecting or carrying out contracts of insurance using Crypto Tokens;

   e) persons who intend to apply to the DFSA for a licence to carry out the activities specified above;

   f) issuers and creators of Crypto Tokens;

   g) persons providing technology support; and

   h) persons providing legal, accounting, audit, or compliance services to any of the above.

Terminology

4. 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.

What are the next steps?

5. Please send any comments using this 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 **4 March 2024.**

6. Following the public consultation, we will decide which changes to the proposed regime are necessary and amend the proposed draft legislation as appropriate. The final version of the Rulebook modules will be published on our website, and we will issue a notice on our website when this happens. You should not act on the proposals until the relevant changes are made.

Structure of this CP

Part I – Introduction;

Part II – Regulatory requirements in relation to Crypto Tokens;

Part III – Decentralised Finance; and

Part IV – Other discussion points.

Appendix 1 – Draft amendments to the General (GEN) module;

Appendix 2 – Draft amendments to the Conduct of Business (COB) module;

Appendix 3 – Draft Amendments to the Collective Investment Rules (CIR) module;

Appendix 4 – Draft amendments to the Anti-Money Laundering, Counter-Terrorist Financing and Sanctions module (AML);

Appendix 5 – Draft amendments to the Fees (FER) module;

Appendix 6 – Draft amendments to the Auditor (AUD) module;

Appendix 7 – Draft amendments to the Authorised Market Institutions (AMI) module; and

Annex 1 – Questions in this consultation paper.

Part I - Introduction

Background

7. In March 2022, the DFSA published Consultation Paper (CP) 143 on the regulation of Crypto Tokens, with the intention of putting into place a comprehensive regime that addressed a wide range of risks associated with Crypto Token business. This included requirements relating to technology, governance, custody, disclosure, market abuse and fraud.

8. The regime came into force in November 2022, and at that time, we indicated that there were certain areas where we expected our policy to evolve, for example, in relation to Decentralised Finance (DeFi), Money Laundering and Terrorist Financing (ML/TF) and custody.

9. Since then, we have also seen many regulatory developments, including recommendations being published by international standard setters. In May 2023, IOSCO published a consultation with detailed recommendations on the regulation of crypto assets, which were adopted in November.[1] In December 2023, IOSCO also published its Final Report with Policy Recommendations for DeFi[2], and more recently, the Basel Committee proposed amendments to its standard on the prudential treatment of banks' exposures to crypto assets, specifically, a set of changes relating to the composition of the reserve assets of stablecoins in Group 1b.

10. We have also learned a considerable amount about the market since November 2022 having met and engaged with over 100 firms looking to be licenced. In carrying out these engagements, we have received feedback on the regime, and where our regime may benefit from further guidance and, in parts, further requirements or flexibility.

Part II – Regulatory requirements in relation to Crypto Tokens

A. Recognition of Crypto Tokens

(i) Introduction

11. Financial Services can only be carried on in or from the DIFC with a Crypto Token that is Recognised. This restriction extends to derivative transactions relating to Crypto Tokens and to Funds or portfolio managers that invest directly or indirectly in Crypto Tokens. The only exception is for a DFSA licensed custodian, which may safeguard or administer any Crypto Token except for a Prohibited Token (that is, any Privacy Token or Algorithmic Token).[3]

12. We adopted this approach due to the large number of Crypto Tokens that are traded, mainly in unregulated markets, today. Many of these tokens have little to no liquidity, offer limited price discovery and are extremely susceptible to price manipulation. We had considered (and still do) that there had to be some constraints on what types of Crypto Tokens could be permitted to prevent potential higher-risk activities relating to illiquid or less mature Crypto Tokens.

13. When the regime was enacted, we published an initial one-off list of Recognised Crypto Tokens, which was something we had seen other regulators do. The Crypto Tokens on

---

1 Crypto and Digital Asset Markets Recommendations.
2 Policy Recommendations for Decentralised Finance.
3 GEN 3A.2.1(2).

that list were Bitcoin (BTC), Ethereum (ETH) and Litecoin (LTC).[4] We have recently added two more Crypto Tokens to that list, Toncoin (TON) and Ripple (XRP).[5]

14. Since adoption, we have had informal feedback on the recognition approach with concerns being raised about the process, in particular, uncertainty around the time it would take for an application to be considered, and concerns about the application fee of USD 10,000 being viewed as high, especially if a firm wanted to get several Crypto Tokens recognised and could not be certain that they would be recognised.

15. This feedback has prompted us to review the approach we have adopted, as well as looking at what other regulators with similar approaches have done, to see if any adjustments should be made.

(ii) The process

16. We know that some view the recognition process as an unnecessary burden (much of the feedback to CP143 focused on this point), and that some were concerned about the operational side of this process, for example, how it would work and how long it would take for the DFSA to consider an application for recognition.

17. As we set out in our Feedback Statement[6] to CP143, our expectation is that all Authorised Firms and AMIs should understand their products and perform a comprehensive risk assessment before offering any service related to a Crypto Token to their Clients. Therefore, we do not think that Authorised Firms, AMIs or other applicants, with the right compliance culture, should struggle to obtain the information required for a recognition application.

18. We do, however, appreciate concerns about the operational side of the recognition process. We currently are not in a position to provide timeframes for recognition applications. However, we intend to closely engage with firms applying for recognition so that they are kept fully informed both as to the progress of that application and if we need any further information.

(iii) Fees

19. The current application fee for recognition is USD 10,000. In light of the experience we have now gained, we are proposing to lower the fee to USD 5,000.

(iv) Fiat Crypto Token recognition criteria

20. In addition to the standard recognition criteria for all Crypto Tokens set out in GEN 3A.3.4, where we will look at, for example, the regulatory status, transparency, market depth, technological resilience, and other risks related to a Crypto Token, we also have additional criteria for so called “stablecoins,” i.e., what we call a Fiat Crypto Token. Fiat Crypto Tokens are typically pegged to a fiat currency and backed by reserve assets denominated in the peg currency.

21. The additional criteria we have in place for Fiat Crypto Tokens[7] includes the composition of the reserves where we specifically require 80% of the reserves to be held in cash.

---

4 https://www.dfsa.ae/news/notice-amendments-legislation-october-2022-2
5 https://www.dfsa.ae/news/notice-crypto-token-recognition
6 https://www.dfsa.ae/download_file/3249/0
7 See GEN 3A.3.4(4).

22. As our regime increasingly needs to accommodate Fiat Crypto Tokens that are issued in other jurisdictions under various detailed regulatory requirements, we consider that we should provide some more flexibility and not prescribe hard requirements on the proportion of reserve assets, e.g., how much of the reserves should be held in cash. We are, therefore, proposing to change our recognition criteria in relation to Fiat Crypto Tokens to:

    a) remove specific requirements on the proportion of assets held in reserves, and instead require that reserves must be held in assets that are likely to maintain their value, (including during periods of stress), are highly liquid, are appropriately diversified and carry minimal credit risk; and

    b) require daily valuation.

23. We emphasise that our proposal does not mean we are relaxing our approach, rather it is meant to provide the DFSA with the flexibility to recognise Fiat Crypto Tokens issued in other jurisdictions with comparable regulation. It also means that we do not need to update our approach as market dynamics change.

24. Lastly, we are proposing changes to the definition of a Fiat Crypto Token. This involves removing the reference to a combination of fiat currencies so that a Fiat Crypto Token is referenced/pegged to a single fiat currency only. Market and regulatory experience demonstrated the increased risks related to maintaining a peg against two or more fiat currencies. Tokens pegged to a basket of currencies will however still fall within the definition of a Crypto Token.

Proposal 1 – Crypto Token Recognition

25. We propose to:

    a) reduce the application fee for recognition from USD 10,000 to USD 5,000;

    b) amend the recognition criteria for a Fiat Crypto Token as per paragraph 22; and

    c) amend the definition of a Fiat Crypto Token as per paragraph 24.

Please see draft GEN 3A.3.4 and App2.5.5, and FER 2.9A.

Question 1:

a) Do you agree with our proposals in paragraph 25? If not, why not?

b) Do you think our proposals in respect of the Fiat Crypto Token reserves are sufficiently stringent to address the risks associated with stablecoins?

B. Financial Services Activities

Collective Investment Funds

26. When we set out our proposals in CP143 for Collective Investment Funds, we limited the fund activities which could be undertaken in respect of Crypto Tokens. Since then, we have had both Fund and Asset Managers approach us wishing to expand their activities to include Crypto Tokens. They expressed the view that the current regulatory approach was too stringent, especially the limitations on External Funds and Foreign Funds investing in Crypto Tokens and, for some, the restriction on investing in

Recognised Crypto Tokens only. We have considered their requests, benchmarked our regime against other jurisdictions, and put forward the following proposals.

(i) External and Foreign Funds

27. We are proposing to allow External Funds to invest in Crypto Tokens, and the offer of Foreign Funds that invest in Crypto Tokens, provided all the following requirements are met:

    a) the total investment in Crypto Tokens is limited to Recognised Crypto Tokens and does not exceed 10% of the gross asset value (GAV) of the Fund;

    b) daily valuations are conducted on the investment in Crypto Tokens;

    c) the units in the Fund are offered to Professional Clients only by way of a Private Placement;

    d) the minimum subscription is USD 50,000; and

    e) an Eligible Custodian has been appointed to safeguard and administer the Fund's investment in Crypto Tokens.

28. In respect of the proposal in paragraph 27(e), we recognise that the existing definition of an Eligible Custodian in CIR 8.2.4 is not appropriate for Crypto Token custody. On that basis, we propose to expand the definition of an Eligible Custodian for a Fund Manager of an External Fund, or Authorised Firm offering the Units of Foreign Fund that invests in Crypto Tokens. In such cases, an Eligible Custodian may either be an Authorised Firm who is licenced to Provide Custody of Crypto Tokens or a Person whom the relevant Fund Manager or Authorised Firm has, after performing due diligence, assessed as having adequate custody arrangements. In performing the required due diligence, we propose that firms consider a range of factors, including:

    a) the regulatory status of the custodian, e.g., whether the Person is authorised and supervised by another Financial Services Regulator when providing custody of Crypto Tokens;

    b) whether the Person's systems and controls ensure safety and segregation of Crypto Tokens;

    c) the adequacy of the Person's policies and procedures for the storage of private keys;

    d) the robustness of the Person's technology governance;

    e) the independence and management of conflicts of interest, and;

    f) appropriate Client disclosures and periodic reporting.

Fund Managers of External Funds

29. Considering the novelty of the asset class and a general lack of global (comprehensive) regulation in this area, in addition to the requirements in paragraph 27 and 28, we propose to require Fund Managers of External Funds that invest in Crypto Tokens to:

a) provide Unitholders with relevant and up-to-date information about the performance and management of the Fund's Crypto Token investments (upon request);

b) include relevant disclosures in the Prospectus, including information on the rights and obligations conferred by Crypto Tokens, the Distributed Ledger Technology (DLT) used, cybersecurity risks and other relevant information; and

c) maintain records, including daily valuations of the Fund's investments in Crypto Tokens as well as other information to demonstrate compliance with the additional requirements.

30. We propose, by way of Guidance, to remind Fund Managers of External Funds that they remain subject to overarching obligations applicable to Authorised Firms[8]. In particular, Fund Managers must observe high standards of integrity and fair dealing, and apply due skill, care and diligence, in managing an External Fund. Similarly, a Fund Manager must have adequate systems and controls to ensure that the affairs of the Fund are effectively managed, having regard to the nature, scale and complexity of the Fund's operations and investment objectives and needs of its investors.

Authorised Firms offering Foreign Funds

31. As we are conscious that Foreign Funds are not managed by DFSA authorised Fund Managers and Authorised Firms offering Units of those Foreign Funds are not likely to be able to exercise control over the Fund's systems, controls or investment strategy, we propose to limit the offering of Foreign Funds to those that conduct daily valuations of their investments in Crypto Tokens and whose exposure to Crypto Tokens does not exceed 10% of GAV of the Fund.

32. In CP143 we stated that we did not have the risk tolerance to allow Representative Offices to "market" activities related to Crypto Tokens in or from the DIFC. In this CP we reiterate this position and - as such - marketing of Foreign Funds investing in Crypto Tokens will not be available to Representative Offices.

(ii) Domestic Funds

33. Domestic Funds are permitted to invest in Crypto Tokens provided they are Recognised Crypto Tokens. Since the introduction of the regime the DFSA has recognised five Crypto Tokens, covering nearly 80% of the total crypto market capitalisation.

34. While we believe that the recognition process of Crypto Tokens is important (as discussed in paragraph 12), we have considered whether we could accommodate limited investment by Domestic Funds in unrecognised Crypto Tokens.[9]

35. We are proposing to allow Domestic Funds to make limited investments in unrecognised Crypto Tokens, provided:

a) the total exposure to unrecognised Crypto Token does not exceed 10% of the GAV of the Fund; and

[8] Including in Article 22, Article 38 of the Collective Investment Law, GEN Chapter 5 (Systems and Controls requirements) and GEN section 4.2 (The Principles for Authorised Firms).

[9] To note, this does not include any Prohibited Tokens such as Privacy Tokens or Algorithmic Tokens.

b) the Domestic Fund is a Qualified Investor Fund (QIF) (i.e., a Fund the Units of which are offered only to Professional Clients via Private Placement with a minimum subscription of USD 500,000).

36. We propose to require Fund Managers of such QIFs to provide Unitholders with information on unrecognised Crypto Token investments, including information on the rights and obligations conferred by the Crypto Token, its trading history, technology characteristics and associated cybersecurity risks. We also highlight that while a Fund Manager of a QIF is exempt from many detailed requirements applicable to Public Funds and Exempt Funds, it will continue to be subject to the overarching obligations of a Fund Manager.

37. Having arrived at a proposal for the funds industry, we are seeking information on the degree of interest in unrecognised Crypto Tokens from other types of firms, such as private banks, or discretionary portfolio managers. We invite comments on what type of limits there should be on the type of Clients involved, or the consent required, for example.

Proposal 2 – Collective Investment Funds

38. We propose to:

a) allow External Funds to invest up to 10% of their GAV in Crypto Tokens provided the conditions in paragraph 27-30 are met;

b) allow Foreign Funds with investments of up to 10% of GAV in Crypto Tokens to be offered in the DIFC, provided the conditions in paragraphs 27, 28, 31 and 32 are met;

c) introduce additional requirements for Authorised Firms offering Units of Foreign Funds that invest in Crypto Tokens (as set out in paragraph 31); and

d) allow certain Domestic Funds to invest in unrecognised Crypto Tokens, provided the investment does not exceed 10% of GAV and the Fund is a QIF so its Units are only offered to Professional Clients via Private Placement at a minimum subscription of USD 500,000.

Please see draft amendments to GEN 2.26.1(4); 3A.2.1; CIR 3.1.16; 6.2.2; 6.2.4; 8.2.4, 8.2.6 13.13.2; 14.2.6; and 15.1.9.

Question 2:

a) Do you agree with the proposals set out in paragraph 38? If not, why not?

b) Is there interest from firms to invest in unrecognised Crypto Tokens? If so, please provide details of the business model and what type of Client limits should be applied.

Custody of Crypto Tokens

(i) Introduction

39. Custody of Crypto Tokens[10] is a vital component in terms of providing access to, and the safe storage of, the Crypto Tokens. In order to address this key role, we require an Authorised Firm which Provides Custody of Crypto Tokens to comply with the DFSA's Client Asset requirements[11] including COB 6.13 (Client Investments and Client Crypto Tokens), COB 6.14 (Record Keeping), COB 15.4 (Requirements for Providing Custody of Crypto Tokens) with references to COB 14.3 (Requirements for Providing Custody of Investment Tokens), COB App2.1.8 (Additional Information for Providing Custody of Crypto Tokens) and COB App6 (Safe Custody).

40. Other key obligations include (but are not limited to):

a) having systems and controls to ensure there is proper safeguarding of those Client Crypto Tokens and proper segregation of Client Crypto Tokens;

b) developing policies and procedures regarding the storage of a Client's private keys including the type of storage chosen, safety of the keys, and measures to protect the keys from a hack, theft or fraud;

c) proper disclosure to Clients regarding transfers, what happens if transfers are incorrectly executed and details of what the firm will do if there has been suspect or actual hacking, theft or fraud;

d) placing responsibility for any unauthorised or incorrectly transferred Crypto Tokens (i.e., to put the Client back into the position it would have been) on the firm providing the custody; and

e) technology governance requirements, for example, maintenance and development of relevant systems used, security measures, procedures to deal with outages, decision making protocols, and audits to check compliance with the governance requirements.

41. Where an Authorised Firm holds or controls Client Crypto Tokens, it must comply with COB 6.13 (Client Investments and Client Crypto Tokens), COB 6.14 (Record Keeping) and COB App 6 (Safe Custody). Lastly, where a Third Party Agent (TPA) is selected, the obligations are on the Authorised Firm to undertake an assessment of that TPA and ensure that they are suitable to hold those Crypto Tokens.

(ii) Private keys and digital wallets

42. Custody providers generally hold private keys,[12] that allow access to, and use of, a Crypto Token. Typically, this service is referred to as digital wallet provision, where a digital wallet (a device or programme) stores the private keys.

43. There are two types of wallets available. The first – custodial – is where a custodian (or centralised third party) holds the private keys, and reliance is placed on their

[10] GEN 3A.2.1(2) allows a DIFC licenced custodian to safeguard and administer Crypto Tokens (Recognised, unrecognised, and Excluded Tokens), except for Prohibited Tokens.
[11] These require segregation of Clients Assets from a firm's own assets.
[12] A private key is a string of alphanumeric characters (similar to a password) which is used to perform certain functions such as authorising a Crypto Token transaction.

technological expertise and security measures to protect those keys. The other type is known as non-custodial or unhosted, where the owner of the Crypto Tokens is fully responsible for managing the private keys. The type of wallet provided (e.g., hot, cold or warm[13]) varies in terms of the level of security provided, the ease of use and the immediacy of access desired.

44. Safety and security of wallets is essential, as Crypto Tokens are often targets for hackers. Due to this risk, there has been discussion by regulators about the type of wallet provided and whether regulators should mandate a proportion of Crypto Tokens that should be held in cold wallets, with no immediate online access. We have not taken this position, which is in line with the recently finalised IOSCO Crypto and Digital Asset (CDA) Recommendations, where IOSCO has not recommended specific thresholds in relation to the storage of the private keys and what type of wallet they should be held in.

45. However, in the CDA Recommendations, IOSCO has said that sufficient, reliable and clear information should be made available to Clients to enable them to understand the rights to any Client Crypto Tokens, including the ability for a Client to receive their Crypto Tokens back, should they suffer losses, in the event of insolvency.

Proposal 3 – Private keys and digital wallets

46. Considering the above, we propose to align further with the CDA Recommendations in this area and to require Authorised Firms Providing Custody to disclose their policies on the chosen storage arrangements for Client Crypto Tokens, why they have chosen that storage option, the risks associated with the option, how they will address the risks, and the mechanism for transfer between wallets.

Please see draft COB App 6.7.1(2)(c).

Question 3:

Do you agree with our proposal in paragraph 46? If not, why not?

(iii) Segregation of Client Crypto Tokens

47. Market events continue to underscore the importance of firms having effective and robust arrangements in place for the identification and segregation of Crypto Tokens. We already require that firm assets and Client Crypto Tokens should always be recorded, registered, and held separately. However, we have not yet commented on whether we expect all Client Crypto Tokens to be held in individual segregated wallets, as we have seen some regulators do.

48. While we see merit in the creation of a separate Crypto Token wallet for each Client as a means of clearly identifying the Crypto Tokens belonging to each Client and to facilitate the return of Client Crypto Tokens in the event of insolvency, there would be significant costs involved with that segregation, which might typically be passed onto the Client. We believe the most proportionate position to take, without diminishing the level of security, is to allow an Authorised Firm to hold a Client's Crypto Tokens in a wallet solely for that Client. Alternatively, an Authorised Firm may choose to pool a Client's Crypto

[13] A hot wallet is one that is connected to the internet; a warm wallet is one where the private keys are held offline but transactions online can be created automatically; and a cold wallet is one that is completely offline and is not connected to the internet.

Tokens in a wallet containing Crypto Tokens of more than one Client. This is aligned with the position we take for Client Investments.

49. However, we do believe that information should be provided to Clients about the service provided, and we are proposing that Authorised Firms Providing Custody disclose the approach taken, why they have taken that approach (e.g., to reflect Client demands), and any risks involved with the approach.

Proposal 4 – Segregation

50. We propose to allow Authorised Firms Providing Custody to segregate a Client's Crypto Tokens or pool them with those of other Clients provided they disclose the approach taken, why they have taken it and any risks involved with the approach taken.

Please see draft COB App6.4 and App 6.7.1(2)(h).

Question 4:

Do you agree with our proposals in paragraph 50? If not, why not?

(iv) Unauthorised or incorrectly executed transfers

Arrangements for unauthorised or incorrectly transferred Crypto Tokens

51. We require an Authorised Firm that Provides Custody of Crypto Tokens to be responsible for any unauthorised or incorrectly executed transfers of Client Crypto Tokens, and we require that firm to address the situation promptly and within three business days put the Client's account back in the position it would have been in if the transfer had not taken place or had been executed correctly (as applicable).[14] However, we have not provided any further direction about the type of rectification that would be acceptable and how this might be administered.

52. We believe further clarity would be helpful for the market and propose to require an Authorised Firm Providing Custody of Crypto Tokens to:

a) have in place appropriate policies and procedures to enable it to identify and rectify any unauthorised or incorrectly executed transfers of Client Crypto Tokens;

b) have in place appropriate compensation arrangements to cover the potential losses in the case of any unauthorised or incorrectly executed transfers of Client Crypto Tokens;

c) disclose to its Clients the compensation arrangements selected; and

d) review (at least annually) the measures and arrangements it has selected to comply with this obligation.

Reporting of unauthorised or incorrectly transferred Crypto Tokens

53. We are also proposing to require Authorised Firms Providing Custody to report to the DFSA, on a quarterly basis:

[14] See COB 15.4.5(1).

a) the numbers of unauthorised or incorrectly transferred Client Crypto Tokens;

b) the numbers of unauthorised or incorrectly transferred Client Crypto Tokens that were reversed and the time it took to reverse the transfer;

c) the total number and value of those unauthorised or incorrectly transferred Client Crypto Tokens; and

d) the total amount of compensation paid to Clients for any unauthorised or incorrectly executed transfers of Client Crypto Tokens.

54. This information will assist the DFSA in identifying any vulnerabilities in a firm's ability to safeguard and control a Client's Crypto Tokens and enable the DFSA to focus on higher risk firms in line with its risk-based approach to supervision.

Proposal 5 – Unauthorised or incorrectly executed transfers

55. We propose to require firms Providing Custody of Crypto Tokens to have in place the measures set out in paragraph 52, and to report to the DFSA on a quarterly basis the information set out in in paragraph 53.

Please see draft COB 15.4.5 – 15.4.8 and App 6.7.1(2)(d).

Question 5:

Do you agree with the proposals set out in paragraph 55? If not, why not?

(v) Third Party Agents

56. Before an Authorised Firm appoints a TPA it must carry out an assessment of that TPA and conclude that they are suitable to hold those Crypto Tokens.[15] We currently have guidance that lists the type of factors an Authorised Firm should have regard to when assessing the suitability of that TPA, but we believe that the guidance could be more detailed where Client Crypto Tokens are held by a TPA.

57. We propose, where a TPA is used, that an Authorised Firm should have regard to whether that TPA is authorised and supervised to provide custody of Crypto Tokens and the adequacy of their arrangements. This would involve looking at the suitability of the TPA's systems and controls to ensure proper safeguarding and segregation of Crypto Tokens; the extent of the policies and procedures regarding the storage of Client Crypto Tokens including the type of storage chosen, safety of the keys, and the measures in place to protect the keys from a hack, theft or fraud; and the robustness of technology governance requirements.

[15] COB App 5.6.

Proposal 6 – Third Party Agents

58. We propose to add further guidance about the assessment of suitability of a TPA as per paragraph 57.

Please see draft COB App 6.5.2 Guidance 2.

Question 6:

Do you agree with our proposal in paragraph 58? If not, why not?

(vi) Records

59. We require Authorised Firms to maintain records under COB 6.14. The records should enable the Authorised Firm to demonstrate and explain all the entries related to Client Crypto Tokens. However, there is currently little guidance or direction about what we want to see specifically in relation to Crypto Tokens.

60. In the CDA Recommendations, IOSCO has said that custody of a Client's Crypto Tokens is reliant on the strength of a firm's systems, policies, procedures, and records. This is especially true due to the nature of Crypto Token custody and the protection of the private keys. They have also set out their expectations in terms of the records a firm is expected to maintain.

61. We have considered what type of information we would expect in firm records and would propose, at a minimum, that Authorised Firms maintain records which:

a) are accurate, and up to date;

b) establish a separate entry for each Client;

c) set out the type of Crypto Token held, the amount, location, transfer history and ownership status of those Crypto Tokens; and

d) record the type of storage (if it is hot, cold or warm storage) and if it is commingled with the tokens of other Clients or individually segregated.

62. Given the importance of records, we also propose that these records are maintained in such a manner that they are readily available to the DFSA, if requested.

Proposal 7 – Records

63. We propose to add further requirements regarding records for Crypto Token custody as per paragraphs 61 and 62.

Please see draft COB 6.14.1.

Question 7:

Do you agree with our proposal in paragraph 63? If not, why not?

(vii) Reconciliation

64. As part of our Client Asset requirements, we currently require an Authorised Firm:

a) at least every 25 days, to reconcile its records of Client Accounts held with Third Party Agents with monthly statements received from those Third Party Agents;

b) at least every six months, to count all Safe Custody Crypto Tokens physically held by the Authorised Firm, or its Nominee Company, and reconcile the results of that count with the records of the Authorised Firm; and

c) at least every six months, to reconcile individual Client ledger balances with the Authorised Firm's records of Safe Custody Crypto Token balances held in Client Accounts.[16]

65. We do not think these current requirements are sufficient due to the risks of fraud and misappropriation associated with Crypto Token custody and therefore propose to require daily reconciliation of Client Crypto Tokens.[17] This is in line with the CDA Recommendations that set out that regular and frequent reconciliations should be carried out. This would also include situations where Client Crypto Tokens are held with TPAs. Given the construction of crypto business around technology, we do not believe that this will prove to be an onerous requirement.

Proposal 8 – Reconciliation

66. We propose to require Authorised Firms that Provide Custody or hold or control Crypto Tokens to carry out daily reconciliation of Client Crypto Tokens.

Please see draft COB App 6.9.1.

Question 8:

Do you agree with our proposals in paragraph 66? If not, why not?

(viii) Safe Custody Auditor's Report

67. Custody of a Client's Crypto Tokens is reliant, as we have set out in this section, on the firm's policies, procedures and controls, including means of access and type of storage of a Client's private keys. While we mandate an Authorised Firm which is Providing Custody or holding or controlling a Client's Crypto Tokens to produce a Safe Custody Auditor Report,[18] we refer only to the requirements in COB App6.

68. Given the additional requirements we have put in place for custody of Crypto Tokens, we believe that additional parts of COB need to be considered as part of the Safe Custody Auditors Report. This would include the requirements proposed in COB 15.4, such as auditing the systems and controls in place to store a Client's private keys to protect those keys against hacking, theft or fraud.

[16] See COB App6.8.
[17] To note, this would include any unrecognised Client Crypto Tokens held by DIFC licenced custodians.
[18] AUD A4.

Proposal 9 – Safe Custody Auditor's Report

69. We propose to require the production of a Safe Custody Auditor's Report to include an audit on the systems and controls in place to store a Client's Crypto Tokens to ensure they are adequate to protect them against hacking, theft or fraud.

Please see draft AUD App4.1.1.

Question 9:

Do you agree with our proposal in paragraph 69? If not, why?

C. Financial Crime

70. As part of the proposals consulted on in CP143, we reminded Relevant Persons engaging in Crypto Business that they are subject to all Federal AML/CFT Laws and Regulations, that they should follow FATF standards and guidance, and that they also must comply with the DFSA's AML Module. We did not, at that time, provide any specific details regarding our expectations around AML/CFT compliance but flagged an intention to look further at this in our next set of proposals.

71. We have now considered the areas where we think Authorised Persons would benefit from further guidance and propose to focus on "Travel Rule" compliance and transaction monitoring and blockchain analysis.

The "Travel Rule"

(i) What is the Travel Rule?

72. The Travel Rule- (though not a defined DFSA term) is commonly used to refer to FATF Recommendation 16, which requires financial institutions engaged in Crypto Token transfers to obtain originator information and beneficiary information and share it with counterparties before or during the transaction. Due to the information about the transacting parties 'travelling' with their transfers, the requirement was dubbed the "Travel Rule". Since 2019, the FATF has advocated the importance of applying these requirements and has reiterated that jurisdictions should implement the Travel Rule as soon as possible.

73. Under the Travel Rule, firms must collect:

a) the Originator's name;

b) the Originator's account number for the account used to process the transaction (e.g., wallet address);

c) the Originator's physical (geographical) address; national identity number; customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution or date and place of birth;

d) the Beneficiary's name; and

e) the Beneficiary's account number for the account used to process the transaction (e.g., wallet address).

74. This information must be sent securely between firms before or alongside the transfer. It cannot be sent after the transfer has been made. Originating firms must also conduct due diligence on the beneficiary firm, which must be done prior to the transfer.

(ii) Proposed approach

75. The UAE has implemented the Travel Rule as part of its updated Federal AML legislation and has also published guidance. Additionally, given the importance placed on the Travel Rule, we propose to:

a) require Authorised Persons to have policies and procedures in place to deal with the money laundering risks arising from the transfer of Crypto Tokens (this would include transfers to or from an unhosted wallet), including how the Authorised Person will deal with situations where a transfer of a Crypto Token is received without the relevant information;

b) where Crypto Token transfers are USD 1,000 or more, Authorised Persons are required to conduct due diligence on any counterparty Virtual Asset Service Provider (VASP) and identify the money laundering risks associated with a transfer, applying appropriate risk-based measures; and

c) specify additional requirements that would apply to Non-Fungible Token and Utility Token transfers carried out by a Designated Non-Financial Business or Profession (DNFBP).

Transaction and blockchain analysis

76. We have so far not mandated any automatic transaction monitoring by Authorised Persons. Rather, we leave it up to them to decide what monitoring (automatic or manual) is appropriate considering the size and nature of the business, the customer base, and the complexity and volume of customer transactions.[19] However, in the Crypto Token context, we do not think it is possible to comply with AML/CFT requirements without adopting some type of automatic transaction monitoring and blockchain analysis solution. This is especially true if firms are to comply with the Travel Rule, for example, check wallet addresses (which can go into the thousands) and carry out sanctions screening.

77. There are currently a range of transaction monitoring and blockchain analysis providers on the market. They carry out screening of customers, wallet screening, transaction monitoring, screening for counterparty Crypto Token firms, and crypto investigations. Given the range of providers and the products and services they offer, we are proposing that where an Authorised Person uses a solution (or solutions), they should demonstrate to us (at the licensing stage or during a risk assessment) the effectiveness of that transaction monitoring and blockchain analysis in relation to the firm's size, customer base and complexity. In doing so, they should look at the quality and effectiveness of the tracking, screening, and tracing provided (e.g., the breadth of the searches conducted across different Crypto Tokens and Crypto Token businesses).

[19] See AML 7.6.1 Guidance 4.

Proposal 10 – Financial Crime

78. We propose to:

a) include requirements relating to Crypto Token transfers in the AML module;

b) require Authorised Persons to develop policies and procedures for how they will comply with the Travel Rule as per paragraph 75; and

c) require an Authorised Person to have adequate transaction monitoring procedures to detect the origin, any intermediate transaction, and destination of Crypto Tokens transferred from or to its customer so that it can identify and report any suspicious transactions.

Please see draft AML 9.1, 9.3A and 9.3B.

Question 10:

Do you agree with our proposal in paragraph 78? If not, why not?

Part III – Decentralised Finance

A. Staking

(i) Introduction

79. We currently allow an Authorised Firm to facilitate or arrange for its Clients to participate in Proof of Stake (PoS) consensus mechanisms – for the purposes of this CP we will refer to this activity as "staking" – but have limited the offer of these services to Professional Clients and Market Counterparties.[20] In our Feedback Statement to CP143, we said that we would need to do more work to consider what additional requirements and/or guidance might be needed to clarify our expectations in this area. As part of this work, we have looked more into the risks associated with staking which include, but are not limited to the following:

a) *Validator risk*: As validators are typically not regulated, there are risks that they might act dishonestly, and/or not fulfil their validator role, which could result in the staked Crypto Tokens being slashed[21] partially, or completely;

b) *Liquidity risk*: As staked Crypto Tokens can be locked up for periods of time, which can vary from a few days to several months, there is a risk that staked Crypto Tokens will not be easily available and could prevent a holder from being able to react to market conditions if, for example, there was a large drop in the market price of that Crypto Token;

c) *Losses*: There is a risk that the Crypto Tokens staked may be reduced or lost if, for example, the validator acts dishonestly. Depending on the severity of the violation, the amount taken for the validator's actions can range from a partial reduction in Tokens to the complete confiscation of the Tokens. This loss would

[20] See COB 15.6.5.

[21] Slashing is the process of a validator losing some or all their staked ETH for failure to meeting their expected requirements as a validator, for example, if they process a fraudulent or malicious transaction or do not participate on the network as expected.

be on top of the fee[22] charged by the validator to stake the Tokens, and the potential fee charged by a third party (if custodial staking is involved), which could result in the staker losing more than they had started with.

d) *Misleading information*: Staking has often involved the advertising of potential high returns, attracting users who perceive the risks to be low. For example, often the advertised yields are much higher than those offered in the traditional financial system, but the sources of these revenue streams are unclear, unsustainable, or in some cases fraudulent. Additionally, many of the arrangements put in place are unclear, as are the rights and responsibilities of the validator.

(ii) Financial Services permissions

80. We have carefully considered the risks involved in staking (as set out above) and are proposing to limit staking to be offered only by Authorised Firms who Provide Custody of Crypto Tokens.[23] As we see more developments in the market, and more regulation of those providing staking services, we may consider expanding the ability to offer staking to other Authorised Firms.

(iii) Diligence

81. Given the risks associated with choosing a validator, we propose that a Custodian must undertake a full assessment of the validator and satisfy itself on reasonable grounds that they are suitable to provide staking services. We propose that a Custodian should have regard to the following:

a) the borrower's governance and internal controls;

b) the borrower's financial status;

c) the borrower's compliance with applicable laws;

d) the infrastructure used and the security measures in place; and

e) the number of Crypto Tokens staked by the borrower on its nodes.

(iv) Risk disclosure

82. While staking services are currently restricted to Professional Clients or Market Counterparties, the risks associated with staking are not always understood. So, while we would not typically apply additional requirements to these types of Clients, in this area we believe it is justified and would propose that the following risk disclosure is made available to Clients before they stake their Tokens:

a) details of the staking service and the role of any third parties;

b) due diligence performed;

c) risks related to staking, such as risk of loss due to technical errors or bugs in the protocol; hacks or theft of the Crypto Tokens, and how losses will be dealt with;

---

[22] The fees charged by a validator are in relation to running a node (which involves hardware and electricity costs). They can also charge fees to stake and unstake the Crypto Tokens.

[23] To note, staking can only be offered in relation to Recognised Crypto Tokens.

d) potential for losses;

e) bonding and unbonding periods and what this might mean if a Client cannot withdraw their staked tokens;

f) fees and charges; and

g) how rewards are calculated, and how they are paid out to Clients.

(v) Changes to the information provided

83. Given the potential for developments in the market, we are also proposing that if there are any changes in the information provided to Clients as set out in paragraph 82, an Authorised Firm must inform their Clients of any of these changes (in a reasonable time) e.g., information about changes in rewards, fees or about slashing incidents that may have occurred.

(vi) Consent

84. Given the risks involved, prior to staking a Crypto Token a Client's explicit consent must be obtained for that staking service.

(vii) Authorised Market Institutions

85. Currently, we take the same approach on lending and staking for both Authorised Firms and AMIs. However, as set out above, we propose to limit staking to firms who are Licensed to Provide Custody of Crypto Tokens. Therefore, as AMIs are not eligible to provide this Financial Service, we propose to no longer allow AMIs to provide any facility or service in relation to staking.

Proposal 11 – Staking

86. We propose the following:

a) to limit staking to be arranged only by Authorised Firms who Provide Custody of Crypto Tokens;

b) for Authorised Firms arranging staking to carry out diligence when choosing a validator as per paragraph 81;

c) for Authorised Firms arranging staking to disclose the information as per paragraph 82, and to update that disclosure if there has been a change in the information provided;

d) for Authorised Firms arranging staking to obtain a Client's explicit consent for that staking service; and

e) to remove an exception for staking in respect of AMIs.

Please see draft COB 15.6.5.

Question 11:

Do you agree with our proposals in paragraph 86? If not, why not?

Part IV – Other discussion points

A. Proprietary Trading

87. We have had inquiries about whether Proprietary Trading in the DIFC involving Crypto Tokens is inside or outside the scope of DFSA regulation. It would generally be considered a regulated activity if a Person carries on that activity by way of business, that is, if they do any one or more of the following:

    a) they engage in the activity in a manner which constitutes the carrying on of a business,

    b) they hold themselves out as willing and able to engage in that activity; or

    c) they regularly solicit other Persons to engage with them in transactions that constitute that activity.

88. We believe this test (set out in GEN 2.3.1) to be clear and see no need to amend or update the provision.

B. Insurance

89. We have seen Crypto Tokens being discussed in the context of insurance in the following areas:

    a) the use of DLT in traditional insurance to create efficiencies in underwriting and claim management;

    b) the use of Crypto Tokens in insurance business (denominating policies, receiving premiums, and paying out claims); and

    c) underwriting specific risks in the crypto market.

90. Where DLT or other similar technology is used by Authorised Firms to facilitate business processes or support back-office operations (either in Insurance or other Financial Services), we would not typically need to regulate this use if Clients are not exposed to the risks arising from that use and the Firm is following other applicable regulations (e.g., in respect of outsourcing requirements).

91. However, more recently, we have seen interest from firms wanting to use Crypto Tokens in their insurance business, e.g., denominating policies in Crypto Tokens and/or paying out claims in Crypto Tokens or to underwrite Crypto Token and blockchain specific risks. To inform our work, and to understand the demand and direction of development in this market, we seek feedback on the following:

    a) the market trends regarding underwriting Crypto Token specific risks and associated regulatory risks;

b) the regulatory risks of using Crypto Tokens as a medium of exchange in insurance and how volatility would be addressed; and

c) the prudential treatment of crypto exposures where Insurers receive premiums and pay out claims in Crypto Tokens.

Question 12:

a) Do you have any comments in respect of proprietary trading and our position set in paragraph 87?

b) What are the factors driving interest in insurance in blockchain and Crypto Token specific risk coverage?

c) Considering the volatility of Crypto Tokens, would the function of insurance as a risk management tool be significantly diminished if Crypto Tokens are used as a medium of exchange between insurers and Clients? Please provide your arguments and explanation of how any issues could be addressed.

d) Do you have any considerations in respect of prudential treatment of Crypto Token exposures of Insurers?

e) What other regulatory risks or market opportunities do you see in relation to the usage of Crypto Tokens in insurance?

Annex 1: Questions in this Consultation Paper

Question 1:

a) Do you agree with our proposal in paragraph 25? If not, why not?

b) Do you think our proposals in respect of the Fiat Crypto Token reserves are sufficiently stringent to address the risks associated with stablecoins?

Question 2:

a) Do you agree with our proposal in paragraph 38? If not, why not?

b) Is there interest from firms to invest in unrecognised Crypto Tokens? If so, please provide details of the business model and what type of Client limits should be applied.

Question 3: Do you agree with our proposal in paragraph 46? If not, why not?

Question 4: Do you agree with our proposal in paragraph 50? If not, why not?

Question 5: Do you agree with our proposal in paragraph 55? If not, why not?

Question 6: Do you agree with our proposal in paragraph 58? If not, why not?

Question 7: Do you agree with our proposal in paragraph 63? If not, why not?

Question 8: Do you agree with our proposal in paragraph 66? If not, why not?

Question 9: Do you agree with our proposal in paragraph 69? If not, why not?

Question 10: Do you agree with our proposal in paragraph 78? If not, why not?

Question 11: Do you agree with our proposal in paragraph 86? If not, why not?

Question 12:

a) Do you have any comments in respect of proprietary trading and our position set in paragraph 87?

b) What are the factors driving interest in insurance in blockchain and Crypto Token specific risk coverage?

c) Considering the volatility of Crypto Tokens, would the function of insurance as a risk management tool be significantly diminished, if Crypto Tokens are used as a medium of exchange between insurers and Clients? Please provide your arguments and explanation of how any issues could be addressed.

d) Do you have any considerations in respect of prudential treatment of Crypto Token exposures of Insurers?

e) What other regulatory risks or market opportunities do you see in relation to the usage of Crypto Tokens in insurance?

Appendix 4

In this Appendix underlining indicates new text and striking through indicates deleted text.

Some text that is not being amended is included for information only.

The DFSA Rulebook

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module

(AML)

...

1.3 Application table

Guidance

Relevant Person	Applicable Chapters	
Authorised Person	**1 - 14**	
Representative Office	**1 - 5***	**10- 14**
Registered Auditor	**1 -8**	**10 - 14**
~~**DNFBP**~~	~~**1 - 8**~~	~~**10 – 15**~~
DNFBP	**1 - 15**	

* Chapters 6 – 9 are unlikely to apply to a Representative Office as such an office is only permitted to carry on limited activities in the DIFC and therefore must not have Customers.

2 OVERVIEW AND PURPOSE OF THE MODULE

Guidance

1. In this module, for simplicity, a reference to "money laundering" also includes terrorist financing, the financing of illegal organisations and proliferation financing (see Rule 3.1.1).

…

10. Chapter 9 sets out certain obligations in relation to correspondent banking, wire transfers, the transfer of Crypto Tokens and other matters which (except for section 9.3B) apply to Authorised Persons, and, in particular, to banks. Section 9.3B applies to DNFBPs which send or receive NFTs or Utility Tokens.

…

3.2.1 In this module, the terms and abbreviations listed in the table below have the following meanings:

…	
Unhosted Wallet	Means software or hardware that enables a person to store and transfer Crypto Tokens on their own behalf, and in relation to which the private key is controlled or held by that person.
…	

…

9 CORRESPONDENT BANKING, ELECTRONIC FUND TRANSFERS AND AUDIT

9.1 Application

9.1.1 This chapter applies only to an Authorised Person, except section 9.3B which applies only to a DNFBP.

…

9.3A Additional requirements for Crypto Token transfers

9.3A.1 This section applies to an Authorised Person that sends or receives Crypto Tokens.

9.3A.2 (1) An Authorised Person must have adequate policies and procedures in place to mitigate the money laundering risks arising from the transfer of Crypto Tokens.

(2) The policies and procedures in (1) must without limitation address the situation where a transfer of Crypto Tokens is received without relevant information and under what circumstances such transfer should be rejected, reversed (if technically possible), delayed or permitted.

9.3A.3 (1) An Authorised Person must have in place adequate transaction monitoring procedures to detect the origin, any intermediate transaction, and destination of Crypto Tokens transferred from or to its customer so that it is able to identify and report any suspicious transaction.

(2) The procedures in (1) must allow for the:

(a) tracking of the transaction history of Crypto Tokens to accurately identify their source and destination; and

(b) identification of transactions involving Digital Wallet addresses that are associated with illicit or suspicious activities.

9.3A.4 (1) Before effecting a Crypto Token transfer ("CTT") with a total value of $1,000 or more, an Authorised Person must conduct due diligence on any VASP counterparty involved in the CTT to identify and assess the money laundering risks associated with the transfer and apply appropriate risk-based measures.

(2) For the purpose of conducting the due diligence under (1), an Authorised Person must at least:

(a) identify the VASP counterparty;

(b) collect sufficient information about the VASP to understand:

(i) the nature of its business;

(ii) its reputation; and

(iii) the quality and effectiveness of the money laundering regulation and supervision over the VASP in the jurisdictions in which it operates;

(c) determine the nature and expected volume and value of the CTT; and

(d) assess the money laundering controls of the VASP counterparty and be satisfied that those controls are adequate and effective.

Guidance

1. When an Authorised Person transfers Crypto Tokens it will be exposed to money laundering risks which may vary depending on a number of factors, including: (a) the types of products and services offered; (b) the types of customers to which the counterparty provides services; (c) geographical exposures of the counterparty and its customers; (d) the anti-money laundering regime in the jurisdictions in which the counterparty operates and/or is incorporated; and (e) the adequacy and effectiveness of the money laundering controls of the counterparty. The purpose of this section is to ensure that an Authorised Person avoids sending or receiving (where possible) Crypto Tokens to or from an illicit actor or a person that had not been subjected to appropriate due diligence measures.

2. An Authorised Person that sends or receives Crypto Tokens on behalf of a customer should be aware of its obligations under Article 33 bis 3 of Cabinet Decision No 10 of 2019. These obligations include the requirement to obtain and keep accurate information on the sender and beneficiary of the transfer and to provide that information to the VASP immediately and securely.

9.3B Additional requirements for NFT and Utility Token transfers

9.3B.1 A DNFBP that sends or receives one or more NFTs or Utility Tokens must comply with the requirements that would apply to an Authorised Person under section 9.3A and for that purpose a reference to a Crypto Token is taken to be a reference to a NFT or Utility Token (as the case may be).

…