Amendments to CBB Rulebook Volume 4 for Crypto-Asset Rules

Amendments to AU Module:

AU-1.1.22D Investment firm licensees wishing to undertake the following regulated investment services involving crypto-assets that fall under the definition of financial instruments must notify the CBB prior to undertaking such activity:

(a) Dealing in financial instruments as agent;
(b) Arranging deals in financial instruments;
(c) Managing financial instruments;
(d) Safeguarding financial instruments (i.e. a custodian);
(e) Advising on financial instruments; and
(f) Operating a collective investment undertaking (i.e. an operator).

Investment firm licensees must not undertake the activity of dealing in crypto-assets as principal.

AU-1.1.22E Investment firm licensees offering the regulated investment services referred to in Paragraph AU-1.1.22D involving custody or transfers of crypto-assets (e.g. brokerage or trading platform) must comply with the requirements stipulated in Appendix AU-1. Such licensees must also provide confirmation from an independent third-party expert that it has established adequate policies, procedures, systems and controls to undertake such activities in compliance with the requirements of Chapter FC-11 and Appendix AU-1. Licensees that offer any regulated investment service referred to in Paragraph AU-1.1.22D involving crypto-assets must provide relevant disclosures and risk warnings to its clients (e.g. relevant disclosures listed under item 34 of Appendix AU-1). In addition, licensees must satisfy the CBB that they have sufficient competence and expertise to undertake the activities.

AU-1.1.22F For purpose of Paragraphs AU-1.1.22A and AU-1.1.22D, investment firm licensees must submit a board resolution to undertake the activity together with the following information:

(a) Description of the services/products;
(b) Changes to organisation structure and framework (if any);
(c) Experience of resources responsible for such services and their details;
(d) Enhancements to its risk management framework to capture, monitor, measure, control and report risks arising from the activity;
(e) Proposed fees and charges; and
(f) Relevant staff training plans.

Appendix AU-1: Requirements for Regulated Investment Services Involving Crypto Assets

Crypto-asset Listing Policy

1. Licensees must establish and adopt a board approved crypto-asset listing policy in accordance with the framework stipulated in this Section.

2. Prior to listing a crypto-asset, a licensee must notify the CBB of its intent to list the crypto-asset, provide the findings of the risk assessment undertaken along with the board resolution approving the crypto-asset. The licensee must confirm in its notification to CBB that the proposed new crypto-asset complies with the requirements of its crypto-asset listing policy.

3. Licensees must provide a list of all the crypto-assets listed on its platform no later than 10 days from the end of each quarter to the CBB.

4. Licensees must have necessary blockchain monitoring capability (e.g. via monitoring systems, internal monitoring control etc.) in place before listing of the crypto-asset on its platform.

5. Licensees must not list crypto-assets that facilitates or may facilitate the obfuscation or concealment of the identity of a customer or counterparty or crypto-assets that are designed to or substantially used to circumvent laws and regulations. Licensees must ensure that they only list crypto-assets to which they have in place the necessary AML monitoring capabilities.

6. Licensees must ensure that:
   (a) its board of directors reviews and independently makes decisions to approve or disapprove each new crypto-asset;
   (b) any actual or potential conflicts of interest in connection with the review and decision-making process have been assessed and effectively addressed, whether such actual or potential conflicts of interest are related to the licensee's board members, shareholders employees, their families, or any other party;
   (c) records are readily available for the CBB's review, of the crypto-asset listing policy's application to each crypto-asset. This includes minutes of the board of directors meeting held to approve a crypto-asset, the documents the board of directors reviewed including an assessment of all associated material risks in connection with each crypto-asset approval or disapproval, such as reviews and sign-offs by various departments of the licensee, such as the legal, compliance, cybersecurity, and operations department etc.;
   (d) its board of directors reviews, at least annually, the crypto-asset listing policy to ensure that it continues to properly identify, assess, and mitigate the relevant risks and to ensure the robustness of the governance, monitoring and oversight framework;
   (e) it informs the CBB immediately, at any time after the submission of its crypto-asset listing policy to CBB, if the said policy ceases to comply with the general framework laid out in this section; and
   (f) it does not make any changes or revisions to its crypto-asset listing policy without the prior written approval of its Board. A copy of the revised crypto-

asset listing policy along with the written Board approval must be submitted to the CBB.

7. Licensees must establish criteria and undertake a comprehensive risk assessment of the crypto-assets that it intends to list on its platform. The risks to be assessed must include, but are not limited to, the following:
   (a) Licensees must conduct a thorough due diligence process to ensure that the crypto-asset is created or issued by a legitimate entity or entities for lawful and legitimate purposes, and not for evading compliance with applicable laws and regulations (e.g., by facilitating money laundering or other illegal activities); and that the process is subject to a strong governance and control framework. Licensees must consider the following factors while undertaking the due diligence:
      (i) The technological experience, track record and reputation of the issuer and its development team;
      (ii) The availability of a reliable multi-signature hardware wallet solution;
      (iii) The protocol and the underlying infrastructure, including whether it is: (1) a separate blockchain with a new architecture system and network or it leverages an existing blockchain for synergies and network effects, (2) scalable, (3) new and/or innovative or (4) the crypto-asset has an innovative use or application;
      (iv) The relevant consensus protocol;
      (v) Developments in markets in which the issuer operates;
      (vi) The geographic distribution of the crypto-asset and the relevant trading pairs, if any;
      (vii) Whether the crypto-asset has any in-built anonymization functions;
      (viii) Crypto-asset exchanges on which the crypto-asset is traded.
   (b) Operational risks associated with a crypto-asset. This includes the resulting demands on the licensee's resources, infrastructure, and personnel, as well as its operational capacity for continued customer on-boarding and customer support based on reasonable forecasts considering the overall operations of the licensee;
   (c) Risks associated with any technology or systems enhancements or modification requirements necessary to ensure timely adoption or listing of any new crypto-asset;
   (d) Risks related to cybersecurity: Whether the crypto-asset shall be able to withstand, adapt, respond to, cyber security vulnerabilities, including size, testing, maturity, and ability to allow the appropriate safeguarding of secure private keys;
   (e) Traceability/Monitoring of the crypto-asset: Whether licensees are able to demonstrate the origin and destination of the specific crypto-asset, whether the crypto-asset enables the identification of counterparties to each trade, and whether transactions in the crypto-asset can be adequately monitored.
   (f) Market risks, including minimum market capitalisation, price volatility, concentration of crypto-asset holdings or control by a small number of individuals or entities, price manipulation, and fraud;
   (g) Risks relating to code defects and breaches and other threats concerning a crypto-asset and its supporting blockchain, or the practices and protocols that apply to them;
   (h) Risks relating to potential non-compliance with the requirements of the licensee's condition and regulatory obligations as a result of the listing of new crypto-asset;

(i) **Legal risks associated with the new crypto-asset, including any pending or potential civil, regulatory, criminal, or enforcement action relating to the issuance, distribution, or use of the new crypto-asset; and**

(j) **Type of distributed ledger: whether there are issues relating to the security and/or usability of a distributed ledger technology used for the purposes of the crypto-asset; whether the crypto-asset leverages an existing distributed ledger for network and other synergies; whether this is a new distributed ledger that has been demonstrably stress tested.**

8. **Licensees must have policies and procedures in place to monitor the listed crypto-assets to ensure that continued use of the crypto-asset remains prudent. This includes:**

   (a) **Periodic re-evaluation of crypto-assets, including whether material changes have occurred, with a frequency and level of scrutiny tailored to the risk level of individual crypto-assets, provided that the frequency of re-evaluation must not be less than annual;**

   (b) **Implementation of control measures to manage risks associated with individual crypto-assets; and**

   (c) **The existence of a process for de-listing of crypto-assets, including notice to affected customers and counterparties in the case of such de-listing.**

9. **Licensees must make adequate disclosures for each listed crypto-asset, containing at a minimum, the following information:**

   (a) **Details about the crypto-asset: the type of crypto-asset (payment token, asset token, utility token, stablecoin etc.), its function and detail about the asset(s) where a crypto-asset is backed by asset(s);**

   (b) **The risks related to the specific crypto-asset such as, but not limited to, price volatility and cyber-security; and**

   (c) **Any other information that would assist clients to make an informed investment decision.**

10. **Licensees must prominently display on their platform the following statement, "THE CENTRAL BANK OF BAHRAIN HAS NEITHER REVIEWED NOR APPROVED THE LISTED CRYPTO-ASSETS."**

Where the CBB determines that undertaking regulated services in a crypto-asset may be detrimental to the financial sector of Bahrain and/or it may affect the legitimate interest of investors, it may, at its sole discretion, instruct licensees to delist the crypto-asset. In such an event, licensees shall remain responsible for orderly settlement and any liability arising due to the delisting of the crypto-asset and obligations arising due to the delisting of the crypto-asset must be resolved by the licensee in a manner that addresses investors' concerns appropriately.

Crypto-asset Custody

11. **A licensee that maintains custody or control of crypto-assets on behalf of a client must store, at a minimum, 95% of client's crypto-assets in cold wallets to minimise exposure to losses arising from a compromise or hacking. The requirement to hold 95% of client's crypto-assets in cold wallet is to be calculated separately for each crypto-asset that is listed on the licensee's platform and not at aggregate level.**

12. **A licensee must have a documented policy detailing the mechanism for the transfer of crypto-assets between hot, cold and other storage. The scope of authority of each**

function designated to perform any non-automated processes in such transfers must be clearly specified in the policy document.

13. Licensees must have written procedures for dealing with events such as forks (hard, soft or temporary forks) or air drops from an operational and technical point of view.

14. Where the underlying protocol of an crypto-asset is changed, and the older version of the crypto-asset is no longer compatible with the new version and/or there is an entirely new and separate version of the crypto asset (hard fork), licensees must ensure that client balances on the old version are reconciled with the new version of the crypto asset. This includes availability of reverse compatibility for as long as required. Licensees maintain transparent lines of communication with their clients on how licensees are managing clients crypto-asset holdings in such a scenario.

15. In the case of a hard fork, licensees must proactively manage any discrepancy between the balances recorded on the previous version versus the new version by engaging with the entity which is responsible for updating and supporting the underlying protocol of the relevant crypto-asset. Additionally, licensees must ensure that, where they seek to offer services in relation to the crypto-asset associated with the new version of the underlying protocol, this new crypto-asset meets the requirements for a crypto-asset and that they notify the CBB well in advance of offering the new crypto-asset as part of its activities.

Licensees may implement the following three types of custodial arrangements or any other type of custodial arrangement that is acceptable to the CBB:

(a) The licensee is wholly responsible for custody of client's crypto-assets and provides this service "in-house" through its own crypto-assets wallet solution. Such an arrangement includes scenarios where a licensee provides its own in-house proprietary wallet for clients to store any crypto-assets bought through that licensee or transferred into the wallet from other sources.

(b) The licensee is wholly responsible for the custody of client's crypto-assets but outsources this service to a third party crypto-asset custodian. Such an arrangement includes the scenario where a licensee uses a third-party service provider to hold all its clients' crypto-assets (e.g., all or part of the clients' private keys).

(c) The licensee wholly allows clients to "self-custodise" their crypto-assets. Such an arrangement includes scenarios where licensees require clients to self-custodise their crypto-assets. Such licensees only provide the platform for clients to buy and sell crypto-assets; Clients are required to source and use their own third party crypto-asset custodians (which the licensee have no control over or responsibility for). This arrangement also includes the scenario where licensees provide an in-house wallet service for clients, but also allow clients to transfer their crypto-assets out of this wallet to another wallet from a third-party wallet provider chosen by the client (and which the licensee does not control).

16. Where a licensee provides a third-party crypto-asset custodian to a client it must undertake an appropriate risk assessment of that crypto-asset custodian. Licensees must also retain ultimate responsibility for safe custody of crypto-assets held on behalf of clients and ensure that they continue to meet all their regulatory obligations with respect to crypto-asset custody service and outsourced activities.

In undertaking an appropriate risk assessment of the third party crypto-asset custodian in accordance with Rule CRA-8.2.3, licensees should take into account any or all of the following:

(a) The expertise and market reputation of the third party crypto-asset custodian, and once a crypto-asset has been lodged by the firm with the third party crypto-asset custodian, the crypto-asset custodian's performance of its services to the licensee;
(b) The arrangements, including cyber security measures, for holding and safeguarding crypto-assets;
(c) An appropriate legal opinion as to the protection of crypto-assets in the event of insolvency of the custodian;
(d) Whether the third party crypto-asset custodian is regulated and by whom;
(e) The capital or financial resources of the third party crypto-asset custodian;
(f) The credit rating of the third party crypto-asset custodian; and
(g) Any other activities undertaken by the third party crypto-asset custodian and, if relevant, any affiliated company.

Licensees should consider, at the minimum, the following two types of crypto-asset wallets:

(a) Custodial Wallet: the custodial wallet provider holds crypto-assets (e.g., the private keys) as an agent on behalf of clients, and has at least some control over these crypto-assets. Licensees that holds crypto-assets on behalf of their clients should generally offer custodial wallets and may even offer multi-signature wallets. Clients using custodial wallets do not necessarily have full and sole control over their crypto-assets. In addition, there is a risk that should the custodial wallet provider cease operations or get hacked, clients may lose their crypto-assets.
(b) Non-Custodial (Self-Custody) Wallets: the non-custodial wallet provider, typically a third-party hardware add/or software company, offers the means for each client to hold their crypto-assets (and fully control private keys) themselves. The non-custodial wallet provider does not control client's crypto currencies – it is the client that has sole and full control over their crypto-assets. Hardware wallets, mobile wallets, desktop wallets and paper wallets are generally examples of non-custodial wallets. Clients using non-custodial wallets have full control of and sole responsibility for their crypto-assets, and the non-custodial wallet provider does not have the ability to effect unilateral transfers of clients' crypto-assets without clients' authorisation.

In addition to the two main crypto-asset wallet types described above, the CBB recognises that there may be alternative crypto-asset wallet models in existence, or which may emerge in future. Licensees seeking to provide such alternative types of crypto-asset wallets and who are unsure of the regulatory obligations they may attract are encouraged to contact the CBB.

Only entities providing the custodial wallets as described in above are considered to be carrying out the regulated activity of safeguarding, storing, holding, maintaining custody of or arranging custody on behalf of clients for crypto-assets. With respect to the non-custodial wallets as described above, the wallet provider is merely providing the technology; it is the wallet user himself who has full control of and responsibility for his crypto-assets.

17. Licensees must put in place necessary Rules and regulations for crypto-asset wallets. Licensees that outsource their crypto-asset wallets to a third party are considered as "arranging custody" and must comply with the requirements of this Chapter.

18. Licensees must have, or where the licensee uses the service of a third party crypto-asset custodian must ensure that the third party crypto-asset custodian has, adequate processes in place for handling deposit and withdrawal requests for crypto-asset to guard against loss arising from theft, fraud and other dishonest acts, professional misconduct or omissions. In this regard, a licensee and its appointed third party crypto-asset custodian, if any, must:

(a) continuously monitor major developments (such as technological changes or the evolution of security threats) relevant to all crypto-assets included for

trading. There should be clear processes in place to evaluate the potential impact and risks of these developments as well as for handling fraud attempts specific to distributed ledger technology (such as 51% attacks), and these processes should be proactively executed;

(b) ensure that client IP addresses as well as wallet addresses used for deposit and withdrawal are whitelisted, using appropriate confirmation methods;

(c) have clear processes in place to minimise the risks involved with handling deposits and withdrawals, including whether deposits and withdrawals are performed using hot or cold storage, whether withdrawals are processed on a real-time basis or only at certain cut-off times, and whether the withdrawal process is automatic or involves manual authorisation;

(d) ensure that any decision to suspend the withdrawal of crypto-assets is made on a transparent and fair basis, and is communicated without delay to all its clients; and

(e) ensure that the above processes include safeguards against fraudulent requests or requests made under duress as well as controls to prevent one or more officers or employees from transferring assets to wallet addresses other than the client's designated wallet address.

19. A licensee must at least every calendar month:

(a) perform reconciliation of its record of safe custody crypto-assets held with third party crypto-asset custodians with monthly statements received from those third party crypto-asset custodians;

(b) aggregate all safe custody crypto-assets held by the licensee, or its hird party custodian, and reconcile the result to the records of the licensee; and

(c) reconcile individual client balances with the licensee's records of safe custody crypto-assets balances held in client accounts.

(d) where the licensee discovers discrepancies after carrying out the above reconciliations, it must maintain a record of such discrepancies and the measures taken to remedy such differences.

Key Management and Wallet Storage

20. A licensee must establish and document keyman risk management measures that include arrangements in place should individuals holding encryption keys or passcodes to stored assets, including wallets, or information be unavailable unexpectedly due to death, disability or other unforeseen circumstances. Such measures must, among others, include keyman insurance or other similar cover.

21. A licensee must ensure that it maintains no encrypted accounts that cannot be retrieved in the future for any reason. It must also advise its clients who maintain wallets with firms outside Bahrain and not licensed by the CBB about any associated risks.

22. Licensees must implement robust procedures and protective measures to ensure the secure generation, storage, backup and destruction of both public and private keys.

In order to access crypto assets, the device on which the private key is held needs access to a network (which, in most cases is through the internet). A wallet where the private key is held on a network attached device is called a hot wallet. Hot wallets are vulnerable to hacking attempts and can be more easily compromised by viruses and malware.

23. **Crypto assets that do not need to be immediately available must be held off line, in a 'cold wallet'.**

24. **Both hot and cold wallets must be password protected and encrypted. The key storage file that is held on the online or offline device must be encrypted. The user is therefore protected against theft of the file (to the degree the password cannot be cracked). However, malware on the machine may still be able to gain access (e.g., a keystroke logger to capture the password).**

25. **Licensees must use multi-signature wallets (e.g., where multiple private keys are associated with a given public key and a subset of these private keys, held by different parties, are required to authorise transactions). Noting that there is no way to recover stolen or lost private keys unless a copy of that key has been made, multi-signature wallets ~~may~~ offer more security because a user can still gain access to its crypto-assets when two or more Private Keys remain available.**

To mitigate the risks associated with hot wallets, private keys can be stored in a cold wallet, which is not attached to a network. Licensees should implement cold wallet key storage where possible if they are offering wallet services to their Clients.

Wallets may also be stored on a secondary device that is never connected to a network. This device, referred to as an air-gapped device, is used to generate, sign, and export transactions. Care must be taken not to infect the air-gapped device with malware when, for example, inserting portable media to export the signed transactions. Hardware security modules emulate the properties of an air gap. A proper policy must be created to describe the responsibilities, methods, circumstances and time periods within which transactions can be initiated. Access and control of single private keys should be shared by multiple users to avoid transactions by a single user.

Some wallet solutions enable cryptographic keys to be derived from a user-chosen password (the "seed") in a "deterministic" wallet. The most basic version requires one password per key pair. A Hierarchical Deterministic wallet derives a set of keys from a given seed. The seed allows a user to restore a wallet without other inputs.

26. **Licensees offering deterministic wallet solutions must ensure that users are provided with clear instructions for situations where keys, seeds or hardware supporting such wallet solutions are lost.**

27. **A licensee must establish and implement strong internal controls and governance procedures for private key management to ensure all cryptographic seeds and private keys are securely generated, stored and backed up. A licensee using a third party crypto-asset custodian must ensure that the third-party custodian establishes and implements such controls and procedures. These include the following:**

    (a) **The generated seed and private key must be sufficiently resistant to speculation or collusion. The seed and private key should be generated in accordance with applicable international security standards and industry best practices so as to ensure that the seeds (where Hierarchical Deterministic Wallets, or similar processes, are used) or private key (if seed are not used) are generated in a non-deterministic manner which ensures randomness and thus are not reproducible. Where practicable, seed and private key should be generated offline and kept in a secure environment, such as a Hardware Security Module**

(HSM), with appropriate certification for the lifetime of the seeds or private keys;

(b) Detailed specifications for how access to cryptographic devices or applications is to be authorised, covering key generation, distribution, use and storage, as well as the immediate revocation of a signatory's access as required;

(c) Access to seed and private key relating to crypto-assets is tightly restricted among approved persons, no single approved person has possession of information on the entirety of the seed, private key or backup passphrases, and controls are implemented to mitigate the risk of collusion among authorised personnel; and

(d) Distributed backups of seed or private key is kept so as to mitigate any single point of failure. The backups need to be distributed in a manner such that an event affecting the primary location of the seed or private key does not affect the backups. The backups should be stored in a protected form on external media (preferably HSM with appropriate certification). Distributed backups should be stored in a manner that ensures seed and private key cannot be re-generated based solely on the backups stored in the same physical location. Access control to the backups needs to be as stringent as access control to the original seed and private key.

28. Licensees must establish, maintain and implement a private key storage policy to ensure effective and prudent safekeeping of the seed and private key at all times. In particular, such policy must address:

(a) the keyman risk associated with the storage of seed and private key is appropriately addressed;

(b) the seed and private key can be retrieved at a short notice without excessive reliance on one or more individuals who may be unavailable due to death, disability or other unforeseen circumstances; and

(c) where a licensee maintains a physical copy of the seed and private key, the physical copies of seed and private key must be maintained in Bahrain in a secure and indestructible manner and the same can be used to access the wallets if need arises.

29. The private key storage policy along with other documents and evidences confirming that the seed and private key are held securely must be made available to the CBB upon request.

Transaction with Counterparties

30. Licensees must use appropriate technology and wherever appropriate third-party services to identify the following situations, and other additional mitigating or preventive actions as necessary to mitigate the money laundering and terror financing risks involved:

(a) the use of proxies, any unverifiable or high-risk IP geographical locations, disposable email addresses or mobile numbers, or frequently changing the devices used to conduct transactions;

(b) transactions involving tainted wallet addresses such as "darknet" marketplace transactions and those involving tumblers; and

(c) where an applicant's IP address is masked (for example, where access is via a virtual private network), a licensee must take reasonable steps to unmask the IP address or decline to provide services to that applicant.

31. **Licensees must establish and maintain adequate and effective systems and processes, including suspicious transaction indicators to monitor transactions with a client or counterparty involving crypto- assets and conduct appropriate enquiry and evaluation of potentially suspicious transactions identified. In particular:**
    (a) **identify and prohibit transactions with wallet addresses or their equivalent which are compromised or tainted; and**
    (b) **employ technology solutions which enable the tracking of crypto-assets through multiple transactions to more accurately identify the source and destination of these crypto- assets.**

For the purposes of 3(b), a wallet address is compromised or tainted where there is reasonable suspicion that it is used for the purpose of conducting fraud, identity theft, extorting ransom or any other criminal activity.

32. **A licensee must avoid transactions with another crypto-asset entity, infrastructure or service provider where the counterparty is unknown or anonymous (e.g., via certain peer to peer or decentralised exchanges) at any stage of its business process.**

33. **Licensees are only allowed to undertake spot trading (spot market) in crypto-assets. Licensees must approach the CBB and seek a written approval prior to offering derivative products.**

The CBB may, at its sole discretion, allow a licensee to list and conduct trading activities in derivatives of crypto-assets such as, but not limited to, futures, options, indices, contract for difference (CFD's), swaps etc provided the CBB is satisfied that the licensee has a comprehensive derivative transactions risk management framework. The aforementioned risk management framework should provide appropriate measure to mitigate, amongst others, market risk, credit risk, liquidity risk, settlement risk, operational risk and legal risk. In addition, the derivative transaction risk management framework should also include guidelines for stress testing, back testing, settlement process, margin methodology, derivative product selection policy, client exposure limit and suitability and appropriateness policy.

Disclosure to Clients

34. **As part of establishing a relationship with a client, and prior to entering into an initial transaction with such client, licensee must disclose in clear, conspicuous, and legible writing in both Arabic and English languages, all material risks associated with crypto-asset products and services including at a minimum, the following:**
    (a) **A crypto-asset is not a legal tender and is not backed by the government;**
    (b) **legislative and regulatory changes or actions at national level or international level may adversely affect the use, transfer, exchange, and value of crypto-assets;**
    (c) **transactions in crypto-assets may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable;**
    (d) **some crypto-asset transactions may be deemed to be made when recorded on a public ledger, which is not necessarily the date or time that the client initiates the transaction;**
    (e) **the value of crypto-assets may be derived from the continued willingness of market participants to exchange fiat currency for crypto-asset, which may**

result in the potential for permanent and total loss of value of a particular crypto-asset should the market for that crypto-asset disappear;

(f) the volatility and unpredictability of the price of crypto-assets relative to fiat currency may result in significant loss over a short period of time;

(g) the nature of crypto-assets may lead to an increased risk of fraud or cyber-attacks;

(h) the nature of crypto-assets means that any technological difficulties experienced by the licensee may prevent the access or use of a client's crypto-assets;

(i) any investor protection mechanism;

(j) the rights and entitlements of a client when events such as, but not limited to, forks and airdrops occur;

(k) how they execute and route client's order and source liquidity (e.g. whether they pass or route orders to an exchange to execute). Where the licensee routes client orders to one or more crypto-asset exchanges for execution, it must disclose details of all the crypto-asset exchanges; and

(l) how it determines the prices of the crypto-assets it quotes to clients.

Prevention of Fraud

35. Licensees must take reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy. The anti-fraud policy must, at a minimum, include:
    (a) the identification and assessment of fraud-related risk areas;
    (b) procedures and controls to protect against identified risks;
    (c) allocation of responsibility for monitoring risks; and
    (d) procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

36. Licensees must, as a minimum, have in place systems and controls with respect to the following:
    (a) Crypto-asset Wallets: Procedures describing the creation, management and controls of crypto-asset wallets, including:
        (i) wallet setup/configuration/deployment/deletion/backup and recovery;
        (ii) wallet access privilege management;
        (iii) wallet user management;
        (iv) wallet Rules and limit determination, review and update; and
        (v) wallet audit and oversight.
    (b) Private keys: Procedures describing the creation, management and controls of private keys, including:
        (i) private key generation;
        (ii) private key exchange;
        (iii) private key storage;
        (iv) private key backup;
        (v) private key destruction; and
    (c) Origin and destination of crypto-asset funds: Systems and controls to mitigate the risk of misuse of crypto currencies, setting out how:
        (i) the origin of crypto-asset is determined, in case of an incoming transaction; and

(ii) the destination of crypto-asset is determined, in case of an outgoing transaction.

Additions to Glossary:

Financial Instruments:

Financial instruments are any of the following instruments: ~~, as further defined in Volume 4, Section AU-1.5, of the CBB Rulebook~~:
(a) Transferable securities;
(b) Islamic financial instruments;
(c) Money market instruments;
(d) Holdings in collective investment undertakings;
(e) Derivative contracts other than commodity derivatives;
(f) Derivative contracts relating to commodities settled in cash;
(g) Derivative contracts relating to commodities;
(h) Credit derivatives;
(i) Financial contracts for differences;
(j) Other derivative contracts;
(k) Interests in real estate property;
(l) Certificates representing certain securities; ~~and~~
(m) Rights or Interests in Financial Instruments; and
(n) crypto-assets which are fungible and transferable (having characteristics similar to a transferable security) or their derivatives.

Transferable securities

Those classes of securities which are freely negotiable, with the exception of instruments of payment. Transferable securities include:
(a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;
(b) bonds or other forms of securitized debt, including depositary receipts in respect of such securities;
(c) warrants;
(d) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.

Transferable securities shall be considered freely negotiable if they can be traded between the parties to a transaction, and subsequently transferred without restriction and if all securities within the same class as the security in question are fungible.

A security that is officially listed on a regulated market and the listing of which is not suspended, shall be deemed to be transferable security.

Securities

Means shares or bonds issued by shareholding companies, government debt instruments and the following financial instruments:

(a) Shares in companies and other securities equivalent to shares in companies or other entities, and depositary receipts in respect of shares;
(b) Bonds or other forms of debt, including depositary receipts in respect of such securities;
(c) Warrants;
(d) Units, rights or interests (however described) of the participants in a collective investment scheme;
(e) Options, futures and any other derivative contracts relating to commodities that must be settled in cash or may be settled in cash at the option of one of the parties (otherwise than by reason of a default or other termination event);
(f) Options, futures and any other derivative contract relating to commodities that can be physically settled;
(g) Units to Real Estate Investment Trusts (REITs);
(h) Index tracking products including Islamic indices;
(i) Any other financial instrument approved as a financial instrument by the CBB for the purpose of trading such instrument on an exchange;
(j) Islamic securities, being those financial instruments that are Shari'a compliant; and
(k) Crypto-assets which exhibit characteristics similar to securities such as:
  (i) a crypto-asset which gives right to a financial entitlement, either in form of a pre-determined cash flow (similar to bonds) or a share in profit (similar to equities);
  (ii) a crypto-asset which grants decision power in a project to its holders (similar to voting rights); or
  (iii) a crypto-asset which represents a monetary claim on the issuer.

Crypto-asset: Means a cryptographically secured digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology but does not include central bank issued digital currencies. Most common forms of crypto-asset are:

i. Payment tokens: Payment tokens are virtual tokens which can be digitally traded and be used for acquiring goods or services or for investment purposes. Payment tokens give rise to no claims on their issuer and are usually decentralised. The most prominent example is Bitcoin.

ii. Utility tokens: Utility tokens are tokens that are intended to provide access to a specific application or service.

iii. Asset tokens: Asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category.

iv. Hybrid Tokens: Hybrid tokens are those that have features of one or more of the other three types of tokens.