This exposure draft presented by Labuan FSA is to provide an overview of the proposed requirements on digital currencies that are admissible for trading by the Labuan financial institutions (LFIs) undertaking digital financial services. This includes the requirements for LFIs to institute adequate control measures through prudent governance oversight in line with the varying level of risk profiles of the digital currencies.

Labuan FSA welcomes and values feedback on the requirements of the exposure draft. The comments or inputs may encompass suggestions, recommendations and alternatives, which should be supported with clear rationale, practicality and relevance for Labuan FSA's consideration.

Feedback shall be submitted electronically to Labuan FSA using the response template by **14 October 2024** to ppu@labuanfsa.gov.my. Should you require any clarification on the exposure draft, please contact the following officers:

i) Carmelitta Liaw (carmelitta@labuanfsa.gov.my) (03-8873-2036)
ii) Jennifer Voon Mei Ying (jennifer@labuanfsa.gov.my) (03-8873-2034)
iii) Billy Gumbang (billy@labuanfsa.gov.my) (03-8873-2035)

ADMISSIBILITY FRAMEWORK FOR DIGITAL CURRENCIES

1.0 Introduction

1.1 Digital currencies have emerged as a new investment class that offers both substantial opportunities and considerable risks for investors.

1.2 Since 2018, there has been significant growth in the digital currency transactions undertaken within Labuan International Business and Financial Centre (IBFC). While digital currencies have yet to pose a material risk to financial stability, general consensus among regulatory authorities is that they could compromise investor interests. As such, there is a need to set requirements to govern the trading of digital currencies and regulatory stance on privacy coins.

1.3 The *Admissibility Framework for Digital Currencies* (referred to as "the Guidelines") provides the regulatory expectation on the trading of digital currencies. This includes the identification of the inherent risks for various types of digital currencies as well as the corresponding risk control measures that need to be instituted by the Labuan financial institutions (LFIs). For the purpose of the Guidelines, digital currencies do not include digital tokens such as securities and non-securities tokens.

2.0 Applicability

2.1 The Guidelines are applicable to LFIs which provide financial services related to the trading and exchanging of digital currencies as permitted under the applicable law, as follows:

(i) Labuan banks and Labuan investment banks licensed under Part VI of the Labuan Financial Services and Securities Act 2010 (LFSSA);

(ii) Labuan Islamic banks and Labuan Islamic investment banks licensed under Part VI of the Labuan Islamic Financial Services and Securities Act 2010 (LIFSSA); and

(iii) Labuan money-broking business and Labuan Islamic money-broking business licensed under Part VI of the LFSSA and Part VI of the LIFSSA, respectively.

2.2 Notwithstanding paragraph 2.1, Labuan FSA reserves the right to modify the scope to include other LFIs to observe the requirements of the Guidelines which may be specified from time to time.

2.3 The Guidelines are to be read together with the requirements under relevant guidelines issued by Labuan FSA as set out in **Appendix I**.

3.0 Legal Provision

3.1 The Guidelines are issued pursuant to Section 4A of the Labuan Financial Services Authority Act 1996 (LFSAA) for the purpose of specifying the requirements to be implemented by LFIs.

3.2 Any person who fails to comply with the Guidelines may be imposed with an administrative penalty under Section 36G of the LFSAA and/or other enforcement actions provided under the LFSAA.

4.0 Effective Date

4.1 The Guidelines shall come into effect on **1 July 2025** and would remain effective and applicable unless amended or revoked. Notwithstanding this, LFIs are highly encouraged to early adopt the requirements of the Guidelines prior to the effective date.

Question 1:

Do you anticipate challenges in complying with the Guidelines by the proposed effective date? If so, please suggest a more suitable effective date and provide justification for the proposed timeline.

5.0 Definitions

Central Bank Digital Currency	A digital representation of fiat currency issued by a sovereign government or central bank. A central bank digital currency is considered as a new form of central bank money.
Digital Currency	Means a digital representation which is issued/transferred using a distributed ledger technology (DLT) or blockchain technology. It can be digitally traded and functions as medium of exchange, unit of account or store of value.
Hard Fork	A hard fork is a major update to a blockchain's protocol that is incompatible with the previous version, resulting in a permanent split into two separate networks. This creates a new blockchain and cryptocurrency, requiring all nodes to upgrade to the new software and typically grants holders of the original tokens equivalent tokens on the new chain.
Privacy Coin	Digital currency that preserves the anonymity and obscure the flow of transaction details across the networks.
Pseudonymous	The transaction details are public, but user identities are concealed. Having said that, the information about the sender or recipient of digital currencies can be inferred from analysing transaction data and patterns.
Stablecoin	Digital currency issued by private entity that aims to maintain stable value relative to a specified financial asset or a basket of financial assets.
Traditional Cryptocurrency	Digital currency that is neither central bank digital currency nor stablecoin. It is issued by private entity and has no formal backing or underlying asset.

6.0 Type of Digital Currencies

6.1 The Guidelines cover the following categories of digital currencies:

(i) Central bank digital currency (CBDC);

(ii) Stablecoin;

(iii) Traditional cryptocurrency; and

(iv) Privacy coin.

Central Bank Digital Currency

6.2 The value of CBDC is backed by a sovereign government or central bank. This includes CBDCs with regional usability features similar to the Euro for European Union member countries.

6.3 In view that CBDC may function as digital equivalent of fiat currency, it may be exchanged and traded similarly as foreign exchange of fiat currencies.

Stablecoin

6.4 A stablecoin has value stabilisation mechanism and may be less volatile as compared to traditional or unbacked cryptocurrencies. Notwithstanding this, its stability would depend on the way in which it is pegged, the type and volatility of reserve assets (if any) as well as the governance structure that underpins the backing and redemption mechanism.

6.5 For the purpose of the Guidelines, the relevant models of stablecoins include:

(i) **Fiat-backed stablecoin**

The value is backed by one or more fiat currencies such as US Dollar, Euro, etc. which is held by regulated financial institution typically in a 1: 1 ratio to the reserve fiat currency e.g. Tether USD (USDT), USD Coin (USDC).

(ii) **Crypto-backed stablecoin**

The value is backed by another digital currency or a portfolio of digital currencies e.g. Dai (DAI), Wrapped Bitcoin (WBTC). This type of stablecoin functions similarly to fiat-backed stablecoin, but the peg is executed on-chain through smart contracts. Given the high volatility of the underlying digital currencies, these stablecoins usually require over-collateralisation to mitigate the associated risks.

(iii) **Algorithmic stablecoin**

The value is controlled by protocols or algorithms that dynamically adjust the stablecoin's supply in response to changes in demand e.g. TerraUSD (UST).

Traditional Cryptocurrency

6.6 The value is subject to market forces and speculation, resulting in significant price volatility e.g. Bitcoin (BTC), Ethereum (ETH).

Privacy Coin

6.7 A digital currency with anonymous features would be deemed as privacy coin e.g. Monero (XMR), Zcash (ZEC) and Dash (DASH).

6.8 A privacy coin employs advanced privacy technologies such as ring signatures, stealth addresses, or zero knowledge proofs to hide transaction information which include the amount, identities of transaction parties, etc.

Question 2:

Do you agree with the type of digital currencies and the descriptions provided above? Are there any areas that require further clarification or modification? Please provide your suggestion and justification.

7.0 Digital Currencies Risk Profiles

7.1 The relative riskiness of various types of digital currency from least to most risky is as follows:

(i) CBDC;

(ii) Stablecoin;

(iii) Traditional cryptocurrency; and

(iv) Privacy coin.

7.2 A CBDC is considered the least risky as it represents a direct claim on a sovereign government or central bank, which provides a high level of safety.

7.3 A stablecoin is generally less risky than a traditional cryptocurrency provided that its value stabilisation mechanism such as the financial assets backing it functions effectively.

7.4 Based on the categories of stablecoins, the relative level of riskiness is ranked as below:

(i) Fiat-backed stablecoin is the least risky as it is supported by fiat currencies held in regulated financial institutions.

(ii) Crypto-backed stablecoin is riskier than fiat-backed stablecoin as it is subject to the volatility of the underlying digital currency.

(iii) Algorithmic stablecoin is the riskiest due to concerns on its algorithms' transparency and effectiveness especially during high-stress periods.

7.5 Privacy coin poses the highest risks related to money laundering (ML), terrorism financing (TF) and proliferation financing (PF). Its advanced privacy features can complicate efforts to detect and prevent illicit financial activities. As such, it is highly probable that such features would not be able to meet the requirements of the *Guidelines on Travel Rule for Labuan Digital Financial Services*.

7.6 The risk metrics used to assess the risk profiles of varying types of digital currencies are provided under **Appendix II**.

7.7 As the digital landscape is evolving rapidly, the risk profile of digital currencies outlined in the Guidelines reflects the current risk environment. These risks may change as the digital currency ecosystem continues to develop and mature.

Question 3:

Do you agree with the risk profiling of the digital currencies? Please provide your suggestion and justification if there are areas that require modification.

8.0 Risk Control Measures

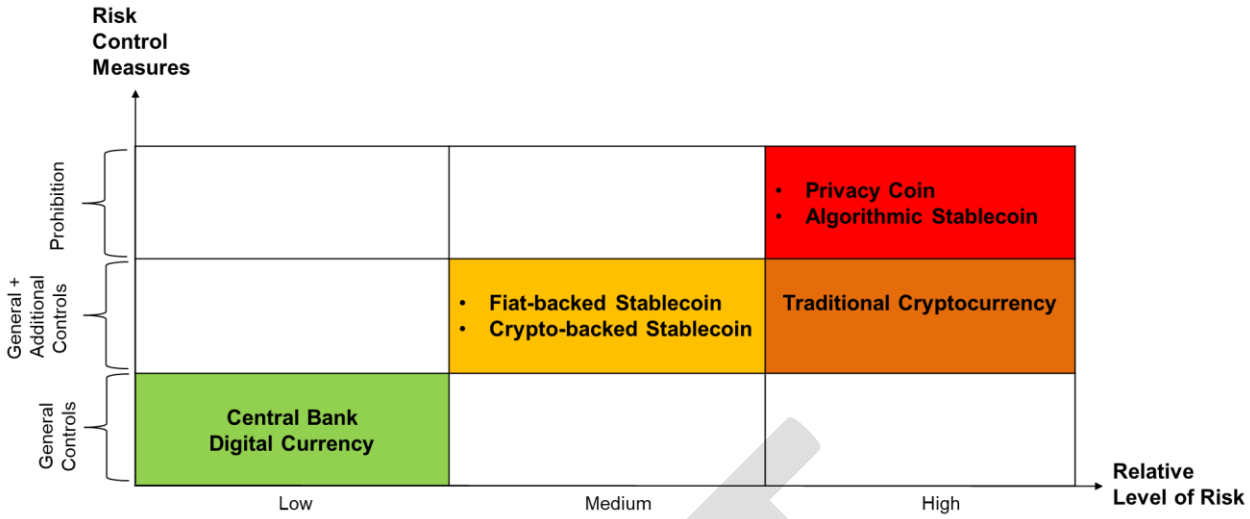
8.1 Based on the risk-profiling of digital currencies under paragraph 7.0, LFIs are required to adopt an appropriate approach in assessing the treatment for the different types of digital currencies. The nature and extent of control measures imposed will be commensurate with the risks posed by each digital currency category.

8.2 Depending on the categories of digital currencies, LFIs are required to employ three-level controls as follows:

(i) **General controls**: Standard controls apply to all categories of admissible digital currencies i.e. CBDCs, stablecoins and traditional cryptocurrencies.

(ii) **Additional controls**: Enhanced controls apply to categories of admissible digital currencies with relatively higher risks i.e. stablecoins and traditional cryptocurrencies, to supplement the general controls.

(iii) **Prohibition:** Privacy coins and algorithmic stablecoins are not admissible.



Question 4:

Do you agree on the prohibition of algorithmic stablecoin? Please provide justification on your view.

Question 5:

Do you agree with the relative level of risk for digital currencies and the corresponding control measures imposed? If not, please provide your suggestions and justification for any areas that may require modification.

8.3 In relation to paragraph 8.1, the control measures that need to be adopted by LFIs include following key areas:

(i) Governance and Monitoring Overview;

(ii) Admissibility of Digital Currencies for Trading;

(iii) Policy Review and Implementation;

(iv) Internal Audit;

(v) Removal of Digital Currencies from Trading;

(vi) Risk Warning and Disclosure; and

(vii) Regulatory Reporting.

A. Governance and Monitoring Overview

8.4 The LFI shall ensure that the overall governance oversight on the risk control measures under paragraph 8.0 is in line with the regulatory expectation of the *Guidelines on Digital Governance Framework*.

Board of Directors

8.5 The Board of Directors of the LFI is expected to:

(i) approve the internal policies and procedures relating to the admission, monitoring and removal of digital currencies for clients to trade;

(ii) ensure that the trading of digital currencies is managed in a prudent and sound manner;

(iii) receive timely updates on the details of digital currencies for trading and any notable issues; and

(iv) promptly notify Labuan FSA upon becoming aware of any matter that adversely affects, or is likely to adversely affect the LFI's ability to meet its obligations or to fulfil its responsibilities under the Guidelines.

Digital Currency Oversight Committee

8.6 An LFI is required to set up a Digital Currency Oversight Committee (DCOC) to manage the trading of digital currencies.

8.7 The DCOC comprises at least two senior management members with relevant expertise and experience in managing digital currency business or internal control functions within the LFI.

8.8 The roles and responsibilities of the DCOC include:

(i) Establishing and reviewing criteria and process for the admission and removal of digital currencies for client trading to ensure they remain appropriate and relevant;

(ii) Deciding whether to admit and remove a digital currency for client trading based on policies and procedures approved by the board of directors;

(iii) Developing and reviewing policies and procedures to ensure effective identification, assessment, and mitigation of risks associated with digital currencies;

(iv) Maintaining record of digital currencies held personally by DCOC members, board of directors and other internal stakeholders who may influence admission or removal decisions. This record should be used to implement information barriers to prevent conflict of interest, market manipulation or insider trading;

(v) Ensuring that internal policies, decisions, reports and the record of digital currencies are properly documented, kept and readily accessible to Supervision Department of Labuan FSA at all times; and

(vi) Reporting to the board of directors at least quarterly covering details of digital currencies available for trading and any notable issues. However, if there are any critical matters such as the removal of digital currencies by DCOC, adverse news with regard to the banning of digital currencies by other regulatory authorities or digital exchanges, DCOC must escalate this to the board of directors immediately.

B. Admissibility of Digital Currencies for Trading

8.9 An LFI must perform a comprehensive due diligence process to assess all digital currencies prior to offering them for trading and ensure that these digital currencies continue to satisfy the admissibility criteria. The details of the admissibility criteria are as specified under paragraphs 8.10 to 8.12.

8.10 As part of general controls, the minimum admissibility criteria which apply to all admissible digital currencies must include the assessment on the sovereign risk e.g. whether the issuer is being sanctioned/from a sanctioned country.

8.11 For stablecoins and traditional cryptocurrencies, additional controls would be required in addition to general controls. In this regard, the admissibility criteria must include the following:

(i) Regulatory status of the digital currency in other jurisdictions e.g. whether it has been approved or banned by another regulator.

(ii) Information of the digital currency e.g. nature, purpose, protocols, consensus mechanism, etc.

(iii) Governance arrangement e.g. information about the founder, issuer, management team, key persons, miners, significant holders, etc. including audited financial statement of issuer.

(iv) Amount in circulation, liquidity, trading history on volumes and prices of digital currency.

(v) Market risk e.g. ownership concentration of the digital currency by a small number of individuals or entities, price manipulation, etc.

(vi) Adequacy and suitability of the technology associated with the digital currency, cybersecurity risk, cyberattack history as well as operational risk.

(vii) Mitigation of risks associated with the digital currency including risks relating to governance, legal, regulatory, cybersecurity, ML, TF, PF, other illicit finance, etc.

(viii) Traceability of the digital currency.

8.12 To manage the pecuniary risk in relation to the underlying reserve of stablecoins, the admissibility criteria would need to further include the following:

(i) Existence of public information on the value and composition of the reserves of the fiat-backed or crypto-backed stablecoin and the information is published at least quarterly by the issuer of the stablecoin.

(ii) Independent third-party verification of published information under paragraph 8.12 (i) by a suitably qualified professional at least annually.

(iii) Ability of the stablecoin to maintain a stable value relative to the fiat currency or digital currency it references.

(iv) Existence of party clearly responsible and liable to investors for the stablecoin.

(v) Existence of redemption policy that enable stablecoin holders to redeem stablecoin in a timely fashion.

(vi) For fiat-backed stablecoin, an LFI must ensure that the issuer of the stablecoin maintain reserve that is:

(a) at least equal to the notional value of all outstanding units of the stablecoin in circulation i.e. the value is calculated as the product of the number of stablecoins in circulation and the purported pegged fiat currency value;

(b) denominated in the reference fiat currency;

(c) held in segregated accounts with regulated banks or custodians supervised by a recognised and competent regulatory authority; and

(d) consist of high-quality liquid assets.

(vii) For crypto-backed stablecoin, an LFI must ensure that the issuer of the stablecoin maintain reserve that is:

(a) meeting the predefined amount i.e. typically more than the notional value of all outstanding units of the stablecoin in circulation i.e. the value is calculated as the product of the number of stablecoins in circulation and the purported pegged digital currency value; and

(b) denominated in the reference digital currency.

Question 6:

Do you agree with the minimum admission criteria for digital currencies to be traded? If not, please provide any changes required and the justification.

C. Policy Review and Implementation

8.13 An LFI must undertake an annual review of its internal policies and procedures on digital currencies. This covers:

(i) reviewing the criteria and process for the admission and removal of digital currencies to ensure they remain appropriate as well as reflective of current market conditions and regulatory requirements;

(ii) re-evaluating each digital currency at least annually to verify whether it continues to meet the admission criteria and to determine if its removal from trading is warranted. The re-evaluation of digital currencies may occur on more frequent basis in response to material changes or developments such as hard forks, significant technological advancements, or changes in the legal or regulatory environment that may affect the digital currency's suitability for trading, etc.; and

(iii) monitoring the implementation of control measures to manage risks associated with the digital currency on an ongoing basis. These risks include but are not limited to cyber security, ML, TF, PF, sanction, etc.

8.14 Regular review reports detailing the findings from ongoing monitoring and the actions taken or planned to address identified issues must be promptly submitted to the DCOC by the LFI.

D. Internal Audit

8.15 The LFI is required to ensure that its internal audit oversight includes planned assessments on internal controls relating to the trading of digital currencies.

8.16 The scope, frequency and intensity of the internal audit must be in line with the LFI's annual audit plan as well as its own risk assessment and appetite. For clarity, the requirement under paragraph 8.15 shall be an independent exercise which is distinctive from the annual review expected out of the DCOC under paragraph 8.13 of the Guidelines.

E. Removal of Digital Currencies from Trading

8.17 Once a decision to remove a digital currency is made by the DCOC, LFI must implement a detailed rollout plan to ensure that the removal is executed in an orderly manner. The roll out plan, at a minimum includes the following:

(i) **Communication with Clients**: The LFI must use all reasonable efforts to communicate clearly and in advance with clients to minimise potential harm. In particular, the LFI must ensure the following:

(a) **Advance Notification Period**: Provide at least 30 calendar days' notice before the removal of the digital currency. If immediate action is necessary due to factors beyond its control, the LFI must provide as much advance notice to clients as practicable;

Question 7:

Do you agree with the proposed 30 calendar days advance notice to client before removing digital currency from trading? If not, please suggest an alternative timeline that may be more feasible or is commonly practiced by other platform operators.

(b) **Content**: Include details on the timing of the removal of the digital currency, the justification for the removal decision and the options available to affected clients such as selling or transferring the digital currency off the platform, if permitted; and

(c) **Communication Method**: Use written notice via email, publication or alert notice at the LFI's website/platform or any other public communication channels.

Question 8:

Do you agree with the specified communication methods? If not, please suggest alternative communication means and provide justification for their suitability.

(ii) **Client Support**: LFI must offer dedicated support by:

(a) responding to phone, email, or chat inquiries from affected clients;

(b) assisting clients with selling or transferring the impacted digital currency if permitted; and

(c) providing tailored FAQs to address common questions and concerns.

Question 9:

In situation where clients do not respond i.e. sell or transfer the impacted digital currency after the notification period, what would LFI normally do on such clients' digital currency?

(iii) **Ongoing Monitoring of Removal Process**: The LFI must monitor the removal process to ensure it is conducted safely and soundly. This includes rendering expertise to identify financial health issues, potential cybersecurity vulnerabilities, illicit finance risk and other challenges affecting client experience.

(iv) **Impact Analysis**: The LFI must undertake an impact analysis to evaluate the effects of the removal decision on clients, internal business operations, counterparties and third-party service providers involved with the digital currency.

8.18 An LFI must document all key aspects of the digital currency removal decision. This includes:

(i) Outcome of monitoring that led to the removal decision;

(ii) Approval of the removal decision e.g. meeting minutes;

(iii) Data on the estimated impact on LFI's customer base;

(iv) Communications shared with clients; and

(v) Documentation responsive to customer support issues.

8.19 If the LFI reverses a removal decision or re-admits a digital currency, it must issue a public notice on its website/platform to announce the decision.

8.20 Labuan FSA may direct the LFI to remove certain digital currencies from client trading when deemed necessary for investor protection, prevention of ML, TF and PF or for the proper functioning of digital business.

F. Risk Warning and Disclosure

8.21 An LFI must prominently display risk warnings related to Digital Currencies on its website and platform. These risk warnings must be clearly visible to clients to ensure they are adequately informed of the potential risks and volatility associated with Digital Currencies. The details of the risk warnings are as specified under paragraphs 8.22 and 8.23.

8.22 As part of general controls, the risk warning shall at a minimum incorporate the following:

(i) Digital currencies are vulnerable to cyber-attacks, which may result in theft. Recovering lost or stolen digital currency is often limited or impossible.

(ii) Risks associated with digital currencies include anonymity, the irreversibility of transactions, accidental transactions, issues with transaction recording, and settlement challenges.

(iii) Technological difficulties experienced by the LFI may hinder access to or use of a client's digital currencies.

(iv) There is no recognised compensation scheme available for providing redress to aggrieved participants.

8.23 For stablecoins and traditional cryptocurrencies, additional controls are required and the risk warning should further include the following:

(i) Digital currencies are not legal tender and not backed by any government.

(ii) Digital currencies are highly volatile and their value can fall quickly (including stablecoins, if they lose their stability peg).

(iii) Investors may lose some or all of their investment.

(iv) Digital currencies may lack liquidity or transferability.

(v) Investing in digital currencies differs from investing in traditional investments such as securities.

8.24 An LFI is required to disclose the following information on its website/platform to ensure transparency:

(i) Admission criteria of digital currency for trading;

(ii) Ongoing monitoring policies and procedures; and

(iii) Execution process for removal of digital currency.

8.25 An LFI is required to publish a Key Features document on its website/platform for each digital currency. The details of the Key Features document are as specified under paragraphs 8.26 and 8.27.

8.26 As part of general controls, the Key Features document needs to include the following information:

(i) Name of the digital currency;

(ii) Country of origin of the issuer; and

(iii) Access details specifying whether client can access the platform directly for trading of the digital currency or only through the LFI and outlining the process for accessing the platform. If the platform is not owned by the LFI, to provide details of the platform operator.

8.27 For stablecoins and traditional cryptocurrencies, additional controls are required and the Key Features document must further include the following:

(i) Issuer details of the digital currency;

(ii) Essential characteristics of the digital currency;

(iii) Information about the underlying DLT or similar technology used for the digital currency;

(iv) Risks associated with the digital currency including price volatility, cybersecurity threats, fraud, hacking and financial crime; and

(v) For fiat-backed and crypto-backed stablecoin, information on the backing reserves, stabilisation mechanism and redemption process.

G. Regulatory Reporting

8.28 An LFI is required to submit regulatory reporting on the digital currency transactions to Labuan FSA on half-yearly basis.

APPENDIX I LIST OF POLICY DOCUMENTS TO BE READ TOGETHER WITH THE GUIDELINES

1. The Guidelines are to be read together with the following guidelines:

   (i) Guidelines on Travel Rule for Labuan Digital Financial Services

   (ii) Guidelines on Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Labuan Key Reporting Institutions

   (iii) Guidelines on Market Conduct for Labuan Digital Financial Intermediaries

   (iv) Guidelines on Technology Management

   (v) Guidelines on Technology and Cyber Risk Management for Labuan Banking and Insurance Business

   (vi) Guidelines on Digital Governance Framework

   (vii) Guidelines on Minimum Audit Standards for Internal Auditors of Labuan Banks

   (viii) Directive on Accounts and Record-Keeping Requirement for Labuan Entities

   (ix) Guidelines on the Establishment of Money Broking Business in Labuan IBFC

APPENDIX II RISK METRIC FOR ASSESSING THE DIGITAL CURRENCIES RISK PROFILES

The table below shows a summary of the characteristics and risks of digital currencies that are considered in deriving their overall risk profiling:

Category	CBDC	Stablecoin	Traditional Cryptocurrency
Issued by	Sovereign government or central bank	Private entity	Private entity
Underlying Rights of Digital Currencies' Owners	Direct claim on central bank	• Depends on the design of stablecoins. • There may be no direct claim against an issuer or redemption right against the reserve asset.	No direct claim against an issuer
Price Volatility	Low	Less volatile than traditional cryptocurrency	High
Elements of anonymity	• Transactions can be designed to be completely anonymous, pseudonymous or protected via authentication process. • However, identity of issuing government is clear.	Majority are pseudonymous by default while some are anonymous i.e. privacy coins.	Majority are pseudonymous by default while some are anonymous i.e. privacy coins.
Sovereign Risk	A country may face bankruptcy or sanction resulting in loss of public confidence on the CBDC.	The issuer may be originating from a sanctioned country.	The issuer may be originating from a sanctioned country.
Legal, Regulatory and Governance Risks	Yes	Yes	Yes

Category	CBDC	Stablecoin	Traditional Cryptocurrency
Liquidity Risk	No	Yes	Yes
Credit Risk	No	Yes	Yes
Market Risk	Similar to fiat currency the CBDC represents	• Concentration risk • Digital run risk which may be triggered by confidence shock	• Speculation • Concentration risk • Digital run risk which may be triggered by confidence shock
Technological and Cybersecurity Risks	Yes	Yes	Yes
Potential Illicit Finance Risks	Yes, greater ML, TF and PF risks than cash	Yes, including ML, TF and PF risks	Yes, including ML, TF and PF risks
Overall Risk Profiling	**Low Risk**	**Medium to High Risk**	**High Risk**

Question 10:

Do you agree with the characteristics and risk profiling of the digital currencies? Please provide your suggestion and justification if there are areas that require modification.

Question 11:

Labuan FSA seeks comments on the ED's overall requirement, including the following areas:

(i) Challenges in implementing the ED's requirements; and

(ii) Any suggestions for enhancement to the ED.

Labuan Financial Services Authority
XX XX 2024