BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6)

Exposure Draft

This exposure draft outlines the proposed requirements and standards that a digital currency exchanger as defined under the First Schedule of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) must carry out as reporting institutions. This is to ensure effective and robust Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) control measures are in place to safeguard the safety and integrity of the financial system as well as to promote greater transparency in the conduct of digital currencies transactions.

The Bank invites written feedback and comments on this exposure draft. Please support each comment with a clear rationale and accompanying evidence or illustration, as appropriate.

Responses must be submitted by **14 January 2018** to:

Pengarah
Jabatan Perisikan Kewangan dan Penguatkuasaan
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
Email: amlpolicy@bnm.gov.my

Electronic submission is encouraged. Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

Any queries may be directed to:
Nantini Kaneson - nantini@bnm.gov.my or 03 2698 8044 (ext.7478)
Farez Mohd Latip - farez@bnm.gov.my or 03 2698 8044 (ext.8615)

Table of Contents

PART A OVERVIEW

1. Introduction

1.1 Due to the rapid development in the field of digital currencies, increasing functionality of its use, growing adoption and its global nature, governments around the world have adopted various approaches and regulatory measures to address the risks associated with and posed by digital currencies.

1.2 In June 2014, the Financial Action Task Force (FATF) released the report entitled "Virtual Currencies – Key Definitions and Potential AML/CFT Risks" and subsequently in June 2015, a Guidance for a Risk-Based Approach for Virtual Currencies was issued to explain the application of the risk-based approach (RBA) to anti-money laundering/counter financing of terrorism (AML/CFT) measures in the digital currencies context, identify the entities involved in digital currencies and clarify the application of relevant FATF recommendations to convertible digital currency exchangers, which are more likely to present money laundering and terrorism financing (ML/TF) risks.

1.3 Governments around the world have adopted various measures to address the risks associated with digital currencies. These measures have also factored in recent rapid developments including the global nature of its usage and the diverse multiple functions these digital currencies are being used for.

1.4 Promoting greater transparency in the use of digital currencies serves to protect the integrity of the financial system and strengthen incentives to prevent their abuse for illegal activities. With this in view, "any person offering services to exchange digital currencies either to fiat money or to another digital currency and vice versa" will be subject to obligations

under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) as reporting institutions pursuant to First Schedule of the AMLA.

1.5 This document sets out the minimum requirements and standards that digital currency exchangers must observe as reporting institutions to increase the transparency of activities relating to digital currencies and ensure effective and robust AML/CFT control measures are in place to mitigate risks that digital currency exchangers may be used as conduits for illegal activities. The requirements and standards will also support law enforcement activities.

1.6 The Bank reiterates that digital currencies are not recognised as legal tender in Malaysia. Members of the public are therefore advised to undertake the necessary due diligence and assessment of the risks involved in dealing in digital currencies or with entities providing services associated with digital currencies.

1.7 Nothing in this document shall be taken to indicate the Bank's licensing, authorisation, endorsement or validation of digital currencies or any entities involved in the provision of digital currencies exchange services. Accordingly, dealings in digital currencies are not covered by prudential and market conduct requirements applicable to licensed and authorised activities, or by established avenues for redress in the event of complaints or losses and damages incurred by parties dealing in digital currencies.

2. Scope

2.1 Pursuant to the AMLA, digital currency exchangers must comply with requirements in this document relating to:

(a) the identification and verification of customers and beneficial

owners, on-going monitoring of customers' transactions, sanction screening, suspicious transaction reporting and record keeping;

(b) transparency obligations; and

(c) requirements for the submission of data and statistics to the Bank for the purpose of managing ML/TF risks.

3. Legal Provisions

3.1 This document is issued pursuant to sections 13, 14, 14A, 15, 16, 17, 18, 19, 20, 66E and 83 of the AMLA.

4. Applicability

4.1 This document is applicable to reporting institutions carrying on the following activities listed in Paragraph 25 of the First Schedule to the AMLA:

(a) activities carried out by any person who provides any or any combination of the following services:

(i) exchanging digital currency for money;

(ii) exchanging money for digital currency; or

(iii) exchanging one digital currency for another digital currency,

whether in the course of carrying on a digital currency exchange business or otherwise.

4.2 For avoidance of doubt, a reporting institution covered by this document includes any person carrying on the activities listed in Paragraph 4.1 in Malaysia, regardless that the person is not domiciled in Malaysia.

4.3 Where the reporting institutions are subject to more than one AML/CFT policy issued pursuant to section 83 of the AMLA, the more stringent requirements shall apply.

5. Effective Date

5.1 This document shall come into effect on a date specified by the Bank through a Government of Malaysia gazette.

5.2 The Bank is committed to ensure that its policies remain relevant and continue to meet the intended objective. Accordingly, the Bank will review this policy document within five years from the date of issuance or the Bank's last review, and where necessary, amend or replace this policy document.

6. Definition and Interpretation

6.1 The terms and expressions used in this document shall have the same meanings assigned to them in the AMLA, unless otherwise defined in this document.

6.2 For the purpose of this document:

"Bank"	Refers to Bank Negara Malaysia.
"beneficial owner"	Refers to any natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or control" or "ultimate effective control" refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.
"business relationship"	Refers to any dealings between the reporting institution

	and any other persons in relation to the activities prescribed under Paragraph 4 of this document.
"customer"	The term also refers to a client.
"customer due diligence"	Refers to any measures undertaken pursuant to section 16 of the AMLA.
"digital currency"	For the purposes of this document, "digital currency" means a digital representation of value that – (a) functions as a medium of exchange; and (b) is interchangeable with any money (including through the crediting or debiting of an account) but excluding electronic money, as defined under the Financial Services Act 2013 [*Act 758*] and the Islamic Financial Services Act 2013 [*Act 759*], issued by an approved issuer of electronic money under those Acts.
"Government-linked company"	Refers to a corporate entity that may be private or public (listed on a stock exchange) where the government owns an effective controlling interest, or is owned by any corporate entity where the government is a shareholder.
"G"	Denotes "Guidance" which may consist of such information, advice or recommendation intended to promote common understanding and sound industry practices which are encouraged to be adopted.
"higher risk"	Refers to circumstances where the reporting institutions assess the ML/TF risks as higher, taking into consideration, and not limited to the following factors: (a) Customer risk factors:

	• customers with transactions conducted in unusual circumstances (e.g. without a valid economic purpose); • customers from locations known for high rates of crime (e.g. drug producing, trafficking, smuggling); • customers with occupation, businesses or activities identified by the FATF or other international bodies as having higher risk for ML/TF; and • persons who match the red flag criteria of the reporting institutions. (b) Country or geographic risk factors: • countries having inadequate AML/CFT systems; • countries identified by the FATF or other international bodies as having higher risk for ML/TF; • countries that may be linked to sanctions, embargos or similar measures issued by, for example, the United Nations; • countries having significant levels of corruption or other criminal activities; and • countries or geographic areas identified as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country. In identifying countries and geographic risk factors, reporting institutions may refer to credible sources such

	as mutual evaluation reports, detailed assessment reports, follow up reports and other relevant reports published by international organisations such as the FATF, United Nations or other reputable organisations. (c) Product, service, transaction or delivery channel risk factors (as offered by the digital currency exchangers): • anonymous transactions (which may include cash); • non face-to-face business relationships or transactions; • payment received from multiple persons and/or countries that do not fit into the person's nature of business and risk profile; and • payment received from unknown or un-associated third parties.
"higher risk countries"	Refers to countries that are listed by FATF or other FATF-styled regional bodies on its Public Statement or the Government of Malaysia, with either on-going or substantial ML/TF risks or strategic AML/CFT deficiencies that pose a risk to the international financial system.
"international organisations"	Refers to entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as residential institutional units of the countries in which they are located. Examples of international organisations include the following: (a) United Nations and its affiliated international

	organisations; (b) regional international organisations such as the Association of Southeast Asian Nations, the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organization of American States; (c) military international organisations such as the North Atlantic Treaty Organization; and (d) economic organisations such as the World Trade Organization.
"legal person"	Refers to any entities other than natural persons that can establish a permanent customer relationship with a reporting institution or otherwise own property. This includes companies, bodies corporate, foundations, partnerships, or associations and other similar entities.
"politically exposed persons (PEPs)"	Refers to: (a) foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials; (b) domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government, judiciary or military officials, senior executives of state

	owned corporations and important political party officials; or (c) persons who are members of senior management or have been entrusted with a prominent function by an international organisation. For example, directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
"S"	Denotes a "Standard", requirement or specification that must be complied with. Failure to comply may result in one or more enforcement actions.
"satisfied"	Where reference is made to a reporting institution being "satisfied" as to a matter, the reporting institution must be able to justify its assessment to the supervisory authority.

PART B AML/CFT REQUIREMENTS

7. Declaration to the Bank

S 7.1 Reporting institutions covered under Paragraph 4.1 of this policy document shall declare its details to the Bank.

S 7.2 A declaration under Paragraph 7.1 shall be made to the Bank in the manner specified in **Annex 1** of this policy document.

S 7.3 A reporting institution shall not represent itself as an entity authorised / licensed by the Bank, or in any way create a legitimate expectation that its activities are regulated by the Bank.

S 7.4 A reporting institution that has ceased its operation or provision of service shall declare such cessation of operation to the Bank.

8. Risk-Based Application

8.1 **Risk Assessment**

S 8.1.1 Reporting institutions must take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customers, countries or geographical areas and products, services, transactions or delivery channels.

S 8.1.2 In assessing ML/TF risks, reporting institutions are required to have the following processes in place:

(a) documenting their risk assessments and findings;

(b) considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) keeping the assessment up-to-date through a periodic review; and

(d) having appropriate and clearly defined mechanisms to provide risk assessment information to the supervisory authority.

S 8.1.3 Reporting institutions must comply with any requirements of the Bank or relevant supervisory authorities to conduct additional risk assessments, which may include expanding relevant risk factors or increasing the frequency of reviews.

G 8.1.4 Reporting institutions may be guided by, take into consideration and integrate the results of the National Risk Assessment issued by the National Co-ordination Committee to Counter Money Laundering in conducting their own risk assessments.

8.2 Risk Control and Mitigation

S 8.2.1 Reporting institutions must:

(a) have policies, controls and procedures to manage and mitigate ML/TF risks that have been identified;

(b) monitor the implementation of those policies, controls, procedures and enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

8.3 Risk Profiling

S 8.3.1 Reporting institutions must conduct risk profiling on their customers.

S 8.3.2 In profiling the risk of its customers, reporting institutions must consider the following factors:

(a) customer risk (e.g. resident or non-resident, type of

customers, occasional or one-off, legal person structure, status as PEP, occupation);

(b) geographical location of business or country of origin of customers;

(c) the products, services, transactions or delivery channels (e.g. cash-based, face-to-face, non face-to-face, domestic or cross-border); and

(d) any other information suggesting that the customer is of higher risk.

S 8.3.3 The risk control and mitigation measures implemented by reporting institutions shall be commensurate with the risk profile of a particular customer or type of customer.

S 8.3.4 Upon the initial acceptance of the customer, reporting institutions are required to regularly review and update the customer's risk profile based on their level of ML/TF risks.

9. Customer Due Diligence (CDD)

9.1 When CDD is required

S 9.1.1 Reporting institutions are required to conduct CDD on all customers and the persons conducting the transaction in the circumstances set out below:

(a) when the reporting institution establishes business relationship with customer; and

(b) when the reporting institutions have any suspicion of ML/TF.

S 9.1.2 Reporting institutions are also required to comply with other specific CDD measures as may be specified by the Bank.

9.2 **What is required**

S 9.2.1 Reporting institutions are required to:

(a) identify the customer and verify that customer's identity using reliable, independent source documents, data or information;

(b) verify that any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source, such that the reporting institution is satisfied that it knows who the beneficial owner is; and

(d) understand and, where relevant, obtain information on, the purpose of the business relationship.

S 9.2.2 In relation to Paragraph 9.2.1, reporting institutions must be able to demonstrate on a continuing basis that appropriate measures are in place.

G 9.2.3 Reporting institutions may use the following measures to verify the identity of non face-to-face customer such as:

(a) requesting additional documents to complement those in Paragraph 9.3;

(b) developing independent contact with the customer; or

(c) verifying customer information against any database maintained by the authorities.

S 9.2.4 In conducting CDD, reporting institutions must comply with the requirements on combating the financing of terrorism under Paragraph 19.

9.3 **CDD Requirements**

On Individual Customer and Beneficial Owner

S 9.3.1 In conducting CDD on an individual customer and beneficial owner, the reporting institution is required to obtain at least the following information:

(a) full name;

(b) National Registration Identity Card (NRIC) number or passport number or reference number of any other official documents bearing the photograph of the customer or beneficial owner;

(c) residential or mailing address;

(d) date of birth;

(e) nationality; and

(f) purpose of transaction

Non Face-to-Face Business Relationship

9.3.2 Reporting institutions must be vigilant in establishing and conducting non face-to-face business relationships via information communication technology.

9.3.3 Reporting institutions are required to establish appropriate measures for identification and verification of a customer's identity that shall be as effective as that for face-to-face customer and implement monitoring and reporting mechanisms to identify potential ML/TF activities.

S 9.3.4 Reporting institutions can accept any other official documents bearing the photograph of the customer or beneficial owner, as the case may be, under Paragraph 9.3.1(b) provided that the reporting institution can be satisfied with the authenticity of the documents which

contain the necessary required information.

S 9.3.5 Reporting institutions shall verify the documents referred to under Paragraph 9.3.1(b) by requiring the customer or beneficial owner, as the case may be, to furnish the original document and make a copy of the said document. However, where biometric identification method is used, verification is deemed to be satisfied.

S 9.3.6 Where there is any doubt, reporting institutions are required to request the customer and beneficial owner, as the case may be, to produce other supporting official identification documents bearing their photographs, issued by an official authority or an international organisation, to enable their identity to be ascertained and verified.

On Legal Persons

S 9.3.7 For customers that are legal persons, reporting institutions are required to understand the nature of the customer's business, its ownership and control structure.

S 9.3.8 Reporting institutions are required to identify the customer and verify its identity through the following information:

(a) name, legal form and proof of existence, such as Memorandum/Article/Certificate of Incorporation/ Partnership or any other reliable references to verify the identity of the customer;

(b) the powers that regulate and bind the customer such as directors' resolution, as well as the names of relevant persons having a senior management position; and

(c) the address of the registered office and, if different, a

principal place of business.

S 9.3.9 Reporting institutions are required to identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person. At a minimum, reporting institution must obtain the following:

(i) identification document of Directors/ Shareholders with equity interest of more than twenty five percent/Partners;

(ii) authorisation for any person to represent the company or business either by means of a letter of authority or directors' resolution; and

(iii) relevant documents such as NRIC for Malaysian/permanent resident or passport for foreigner, to identify the identity of the person authorised to represent the company or business in its dealings with the reporting institution;

(b) to the extent that there is doubt as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) referred to in Paragraph 9.3.9(a) or where no natural person(s) exert control through ownership interests, the identity of the natural person exercising control of the legal person through other means; and

(c) where no natural person is identified under Paragraphs 9.3.9(a) or (b) above, the identity of the relevant natural person who holds the position of senior management.

S 9.3.10 Where there is any doubt as to the identity of persons referred to under Paragraphs 9.3.8 and 9.3.9, the reporting institution shall:

(a) conduct a basic search or enquiry on the background of such person to ensure that the person has not been or is not in the process of being dissolved or liquidated, or is a bankrupt; and

(b) verify the authenticity of the information provided by such person with the Companies Commission of Malaysia, Labuan Financial Services Authority or any other relevant agencies.

S 9.3.11 Reporting institutions are exempted from obtaining a copy of the Memorandum and Articles of Association or certificate of incorporation of the legal person which fall under the following categories:

(a) public listed companies or corporations listed in Bursa Malaysia;

(b) foreign public listed companies:
- listed in recognised exchanges; and
- not listed in higher risk countries;

(c) foreign financial institutions that are not from higher risk countries;

(d) government-linked companies in Malaysia;

(e) state-owned corporations and companies in Malaysia;

(f) an authorised person, an operator of a designated payment system, a registered person, as the case may be, under the Financial Services Act 2013 and the Islamic Financial Services Act 2013;

(g) persons licensed or registered under the Capital Markets and Services Act 2007;

(h) licensed entities under the Labuan Financial Services and Securities Act 2010 and Labuan Islamic Financial Services and Securities Act 2010; or

(i) prescribed institutions under the Development Financial Institutions Act 2002.

G 9.3.12 Reporting institutions may refer to the Directives in relation to Recognised Stock Exchanges (R/R6 of 2012) issued by Bursa Malaysia in determining foreign exchanges that are recognised.

9.4 Enhanced CDD

S 9.4.1 Reporting institutions are required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, shall include at least, the following:

(a) obtaining CDD information under Paragraph 9.3;

(b) obtaining additional information on the customer and beneficial owner (e.g. volume of assets and other information from public database);

(c) inquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and

(d) obtaining approval from the Senior Management of the reporting institution before establishing (or continuing, for existing customers) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management at the head office.

G 9.4.2 In addition to Paragraph 9.4.1, reporting institutions may also consider the following enhanced CDD measures in line with the ML/TF risks identified:

(a) obtaining additional information on the intended level and nature of the business relationship with the reporting institutions;

(b) updating more regularly the identification data of customer and beneficial owner; and

(c) inquiring on the reasons for intended or performed transactions.

9.5 On-Going Due Diligence

S 9.5.1 Reporting institutions are required to conduct on-going due diligence on the business relationship with its customers. Such measures shall include:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

G 9.5.2 In conducting on-going due diligence, reporting institutions may take into consideration the economic circumstances and purpose of any transaction or business relationship which:

(a) appears unusual; or

(b) casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customers.

S 9.5.3 The frequency of the on-going due diligence or enhanced on-going due diligence, as the case may be, shall be commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

S 9.5.4 When a customer is assessed as higher risk, reporting institutions must conduct enhanced on-going due-diligence on that customer.

S 9.5.5 Reporting institutions are required to increase the number and frequency of controls applied, and to select patterns of transactions that need further examination, when conducting enhanced on-going due diligence.

9.6 Existing Customer – Materiality and Risk

S 9.6.1 Reporting institutions are required to apply CDD requirements to existing customers on the basis of materiality and risk.

S 9.6.2 Reporting institutions are required to conduct CDD on such existing relationships, taking into account whether and when CDD measures have previously been undertaken and the adequacy of information obtained.

G 9.6.3 In assessing materiality and risk of an existing customer under Paragraph 9.6.1, reporting institutions may consider

the following circumstances:

(a) the nature and circumstances surrounding the transaction including the significance of the transaction;

(b) any material change in the way the account, transaction or business relationship is operated; or

(c) insufficient information held on the customer or change in customer's information.

10. Politically Exposed Persons (PEPs)

10.1 General

S 10.1.1 The requirements set out under this Paragraph are applicable to family members or close associates of all types of PEPs.

10.2 Foreign PEPs

S 10.2.1 Reporting institutions must take reasonable measures to determine whether a customer or a beneficial owner is a foreign PEP.

S 10.2.2 Upon determination that a customer or a beneficial owner is a foreign PEP, the requirements of enhanced CDD as set out under Paragraph 9.4 and enhanced on-going due diligence as set out under Paragraph 9.5.4 must be conducted on the foreign PEP.

10.3 Domestic PEPs or Person entrusted with a prominent function by an international organisation

S 10.3.1 Reporting institutions must take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person entrusted with a prominent function by an international organisation.

S 10.3.2 If the customer or beneficial owner is determined to be a domestic PEP or a person entrusted with a prominent function by an international organisation, reporting institutions are required to assess the level of ML/TF risks posed by the business relationship with the domestic PEP or person entrusted with a prominent function by an international organisation.

S 10.3.3 The assessment of the ML/TF risks, as specified under Paragraph 10.3.2, shall take into account the profile of the customer under Paragraph 8.3.2 on Risk Profiling.

S 10.3.4 The requirements of enhanced CDD as set out under Paragraph 9.4 and enhanced on-going due diligence as set out under Paragraph 9.5.4 must be conducted in respect of domestic PEPs or person entrusted with a prominent function by an international organisation who are assessed as higher risk.

G 10.3.5 Reporting institutions may apply CDD measures similar to other customers for domestic PEPs or persons entrusted with a prominent function by an international organisation if the reporting institution is satisfied that the domestic PEPs or persons entrusted with a prominent function by an international organisation are not assessed as higher risk.

11. New Digital Currencies, Products and Business Practices

S 11.1 Reporting institutions are required to identify and assess the ML/TF risks that may arise in relation to the development of new digital currencies, products, services and business practices, including new delivery mechanisms, and the use of new or developing technologies

whether for new or existing solutions.

S 11.2 Reporting institutions are required to:

(a) undertake the risk assessment prior to the launch or adoption of such new digital currencies, products, services, business practices and technologies;

(b) take appropriate measures to manage and mitigate the risks; and

(c) document the risk assessment in writing.

12. Reliance on Third Parties

Definition

12.1 "Third Party" refers to reporting institutions that are supervised by a relevant competent authority and that meet the requirements under this Paragraph, namely persons or businesses who are relied upon by the reporting institution to conduct the customer due diligence process.

This definition does not include outsourcing or agency relationships because the outsourced service provider or agent is regarded as synonymous with the reporting institution.

Customer Due Diligence

G 12.2 Reporting institutions may rely on third parties to conduct CDD or to introduce business.

S 12.3 The ultimate responsibility and accountability for CDD measures shall remain with the reporting institution relying on the third parties.

S 12.4 Reporting institutions shall have in place internal policies and procedures to mitigate the risks when relying on third parties. The

internal policies and procedures shall appropriately reflect the higher risk of reliance on third parties from jurisdictions that have been identified as having strategic AML/CFT deficiencies that pose a ML/TF risk to the international financial system.

S 12.5 Reporting institutions are prohibited from relying on third parties located in the higher risk countries that have been identified as having on-going or substantial ML/TF risks.

S 12.6 In placing reliance on the third party, the reporting institution, at a minimum:

(a) must be able to obtain immediately the necessary information concerning CDD as required under Paragraph 9.3.1; and

(b) must be reasonably satisfied that the third party:

(i) is properly regulated and supervised by the respective authorities;

(ii) has an adequate CDD process;

(iii) has measures in place for record keeping requirements; and

(iv) can provide the CDD information and provide copies of the relevant documentation immediately upon request;

G 12.7 Reporting institutions may obtain an attestation from the third party to satisfy itself that the requirements in Paragraph 12.6 have been met, provided there is no evidence or indications to the contrary. Reporting institutions should take additional measures to satisfy itself of the requirements if such contrary evidence or indications exist.

G 12.8 Reporting institutions may obtain written confirmation from the third party that it has conducted CDD on customers or beneficial owners, in accordance with Paragraph 9.

On-going Due Diligence

S 12.9 Reporting institutions shall not rely on third parties to conduct on-going due diligence of its customers.

13. Higher Risk Countries

S 13.1 Reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF, other FATF-styled regional bodies or the Government of Malaysia as having on-going or substantial ML/TF risks.

S 13.2 Where ML/TF risks are assessed as higher risk, reporting institutions are required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies and have not made sufficient progress in addressing those deficiencies.

S 13.3 In addition to the enhanced CDD requirement under Paragraph 9.4, reporting institutions that are domiciled in Malaysia are required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks, as follows:

(a) limiting business relationships or financial transactions with identified countries or persons located in the country concerned;

(b) conducting enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the reporting

institution or financial group, located in the country concerned; and

(c) conduct any other measures as may be specified by the Bank.

14. Failure to Satisfactorily Complete CDD

S 14.1 Reporting institutions shall not commence business relations or perform any transaction in relation to a potential customer, or shall terminate business relations in the case of an existing customer, if the reporting institution is unable to comply with the CDD requirements.

S 14.2 In the event of failure to comply with the CDD requirements, reporting institutions must consider lodging a suspicious transaction report under Paragraph 18.

15. Management Information Systems

S 15.1 Reporting institutions must have in place an adequate management information system (MIS), to complement and support its CDD process. The MIS is required to provide the reporting institution with timely information on a regular basis to enable the reporting institution to detect irregularity and/or any suspicious activity.

S 15.2 The MIS shall be commensurate with the nature, scale and complexity of the reporting institution's activities and ML/TF risk profile.

S 15.3 The MIS must be able to capture, at a minimum, information on multiple transactions over a certain period, large transactions, anomalies in transaction patterns, customers' risk profiles and transactions exceeding any internally specified threshold.

S 15.4 The MIS shall be able to aggregate customer transactions from multiple accounts and/or from different systems.

G 15.5 The MIS may leverage on and be integrated with the reporting institution's existing information systems that support its business operations to the extent that customer information captured in such systems is accurate, up-to-date and reliable.

16. Record Keeping

S 16.1 Reporting institutions must keep relevant records including any accounts, files, business correspondence and documents relating to transactions, including those obtained during the CDD process to verify the identity of customers and beneficial owners, and results of any analysis undertaken. The records maintained must remain up-to-date.

S 16.2 Reporting institutions must keep the records for at least six years following the date of completion of the transaction or the date of termination of the business relationship.

S 16.3 In situations where the records are subjected to on-going investigation or prosecution in court, they shall be retained beyond the stipulated retention period until such time reporting institutions are informed by the relevant law enforcement agency that such records are no longer required.

17. Appointment of Compliance Officer

S 17.1 The reporting institutions must appoint a Compliance Officer.

S 17.2 The Compliance Officer shall act as the reference point for AML/CFT matters within the reporting institutions.

S 17.3 The Compliance Officer must have sufficient stature, authority and seniority within the reporting institutions to participate in and be able to effectively influence decisions relating to AML/CFT.

S 17.4 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT responsibilities effectively.

G 17.5 "Fit and proper" assessments may include considerations of a person's:

(a) probity, personal integrity and reputation; and

(b) competency and capability.

S 17.6 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF methods and counter measures to mitigate ML/TF risks.

G 17.7 Reporting institutions may encourage the Compliance Officer to pursue professional qualifications in AML/CFT so that he is able to carry out his obligations effectively.

S 17.8 Reporting institutions are required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

S 17.9 The Compliance Officer has a duty to ensure the following:

(a) the reporting institution has put in place adequate AML/CFT policies and procedures;

(b) the reporting institution's compliance with the AML/CFT requirements to facilitate proper implementation of the AML/CFT policies;

(c) the appropriate AML/CFT procedures, including CDD, record-keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism, are implemented effectively;

(d) the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;

(e) the channel of communication from the respective employees of the reporting institutions on submission of internally generated suspicious transaction reports to the Compliance Officer is secured and that information is kept confidential;

(f) all employees are aware of the reporting institution's AML/CFT measures, including policies, control mechanisms and the channel of reporting;

(g) internally generated suspicious transaction reports are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and

(h) the identification of ML/TF risks associated with new products or services or arising from the reporting institution's operational changes, including the adoption of new technology and processes.

S 17.10 Reporting institutions are required to inform, in writing, the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, within ten working days, of the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as may be required.

18. Suspicious Transaction Report

18.1 General

S 18.1.1 Reporting institutions must promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia whenever the reporting institutions suspect or have reason to suspect that the transaction (including attempted or proposed transaction), regardless of the amount, appears:

(a) unusual;

(b) illegal;

(c) to have no clear economic purpose;

(d) to involve proceeds from an unlawful activity and instrumentalities of an offence; or

(e) to indicate that the customer could be involved in ML/TF.

S 18.1.2 Reporting institutions must provide the required and relevant information that gives rise to doubt in the suspicious transaction report form. This includes but is not limited to a description of the nature and circumstances surrounding the transaction and business background of the person conducting the transaction that appears to be connected to the unlawful activity.

S 18.1.3 Reporting institutions must establish a reporting system for the submission of suspicious transaction reports to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.

G 18.1.4 Reporting institutions may refer to **Annex 2** of this policy document which provides examples of transactions that may trigger an obligation to report suspicious transactions.

18.2 **Reporting Mechanism**

S 18.2.1 Reporting institutions that are domiciled in Malaysia are required to ensure that the designated branch or subsidiary compliance officer is responsible for channelling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer at the head office. In the case of employees at the head office, such internal suspicious transaction reports shall be channelled directly to the Compliance Officer.

S 18.2.2 Reporting institutions are required to have in place policies on the reasonable duration upon which internally generated suspicious transaction reports must be reviewed by the Compliance Officer, including the circumstances when the timeframe can be exceeded, to enable submission of suspicious transaction report promptly if required.

S 18.2.3 Upon receiving any internal suspicious transaction report, the Compliance Officer must evaluate the grounds for suspicion. Once the suspicion is established, the Compliance Officer must promptly submit the suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and retain records of the decision, supported by the relevant documents.

S 18.2.4 The Compliance Officer must submit the suspicious transaction report in the specified suspicious transaction report form (attached in **Annex 3**) through any of the following modes:

Mail : Director
Financial Intelligence and Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)

Fax : +603-2693 3625

E-mail : str@bnm.gov.my

S 18.2.5 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the Compliance Officer of a reporting institution must submit its suspicious transaction reports on-line:

Website : https://bnmapp.bnm.gov.my/fins2

S 18.2.6 The Compliance Officer must ensure that the suspicious transaction report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion.

S 18.2.7 Reporting institutions must ensure that in the course of submitting the suspicious transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer shall have the sole discretion and independence to report suspicious transactions.

S 18.2.8 Reporting institutions must provide additional information and documentation as may be requested by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to respond promptly to any further enquiries with

regard to any report received under section 14 of the AMLA.

S 18.2.9 Reporting institutions must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preserve secrecy.

S 18.2.10 Where a suspicious transaction report has been lodged, reporting institutions are not precluded from making a fresh suspicious transaction report as and when a new suspicion arises.

18.3 Tipping Off

S 18.3.1 In cases where the reporting institution forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the customer, the reporting institution is permitted not to pursue the CDD process. In such circumstances, the reporting institution may proceed with the transaction and immediately file a suspicious transaction report.

S 18.3.2 Reporting institutions shall observe the prohibition of tipping-off as stipulated under section 14A of AMLA. Disclosure of any report or related information referred to in section 14 is only allowed when any of the exemptions under subsection 14A(3) of AMLA apply.

18.4 Triggers for Submission of Suspicious Transaction Report

S 18.4.1 Reporting institutions are required to establish internal criteria ("red flags") to detect suspicious transactions.

G 18.4.2 Reporting institutions may be guided by examples of suspicious transactions provided by the Bank or other

corresponding competent authorities, supervisory authorities and international organisations.

S 18.4.3 Reporting institutions must consider submitting a suspicious transaction report when any of its customer's transactions or attempted transactions fits the reporting institution's list of "red flags".

18.5 **Internally Generated Suspicious Transaction Reports**

S 18.5.1 Reporting institutions must ensure that the Compliance Officer maintains complete records on all internally generated suspicious transaction reports and any supporting documentary evidence regardless of whether such reports have been submitted. The internally generated reports and the relevant supporting documentary evidence must be made available to the relevant supervisory authorities upon request.

19. Combating the Financing of Terrorism

S 19.1 Where relevant, references to a customer in this Paragraph include a beneficial owner and beneficiary.

19.2 *Maintenance of List*

S 19.2.1 Reporting institutions are required to keep updated with the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures, in particular the UNSC Resolutions 1267 (1999) / 1989 (2011), 1988 (2011), and subsequent resolutions which require sanctions against individuals and entities belonging or related to terrorism.

S 19.2.2 Reporting institutions are required to maintain a list of

individuals and entities for this purpose. The updated UN List can be obtained at the relevant Sanctions Committees page at: https://www.un.org/sc/suborg/en/sanctions/

S 19.2.3 Reporting institutions are required to maintain a database of names and particulars of listed persons in the UN List and such orders as may be issued under sections 66B and 66C of the AMLA by the Minister of Home Affairs.

S 19.2.4 Database of names and particulars of listed persons based on the orders issued under sections 66B and 66C of the AMLA by the Minister of Home Affairs may be obtained at: http://www.moha.gov.my/index.php/en/

S 19.2.5 Reporting institutions shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees.

G 19.2.6 Reporting institutions may also include in their database the other recognised lists of designated persons or entities issued by other jurisdictions.

S 19.2.7 Reporting institutions are required to conduct checks on the names of new customers, as well as regular checks on the names of existing customers, and potential customers, against the names in the database. If there is any name match, reporting institutions must take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, reporting institutions must immediately:

(a) freeze the customer's funds or block the transaction

(where applicable), if it is an existing customer;

(b) reject the potential customer, if the transaction has not commenced;

(c) submit a suspicious transaction report; and

(d) inform the relevant supervisory authorities.

S 19.2.8 In addition to Paragraph 19.2.7, reporting institutions are also required to identify any transaction or account that may be indirectly controlled by individual listed in the database.

S 19.2.9 Reporting institutions are required to submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the UN List or orders made by the Minister of Home Affairs under sections 66B or 66C of the AMLA.

S **19.2.10** Reporting institutions are required to ascertain potential matches with the database to confirm whether they are true matches to eliminate "false positives". The reporting institutions may make further inquiries of the customer to assist in determining whether the match is a true match.

20. Reporting and Transparency Requirements

S *General*

20.1 A reporting institution shall comply with requirements specified by the Bank in **Annex 4** to submit data and statistics to the Bank for the purpose of the Bank's assessment, monitoring and management of ML/TF risks.

S 20.2 Reporting institutions shall submit reports required under Paragraph 20.1 to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia.

S 20.3 Reporting institutions shall additionally comply with any ad-hoc requirements to submit information as may be specified by the Bank for the purpose stated in Paragraph 20.1.

S 20.4 Reporting institutions must publish the prices of the digital currencies exchanged, including the pricing methodology used in determining the prices for the exchange of digital currencies.

S 20.5 The Bank may publish any non-proprietary information submitted under Paragraph 20 to promote transparency of digital currencies activities by reporting institutions and to inform assessments by the public of the risks associated with digital currencies activities.

21. Non-Compliance

S 21.1 Enforcement actions can be taken against the reporting institutions including its directors, officers and employees for any non-compliance with any provision marked as “S” in this document in accordance with the provisions in sections 22, 66E, 86, 86A, 87, 88, 92 and 93 of the AMLA.

RAHSIA **Annex 1**

Please send completed form to:
Financial Intelligence & Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn, 50480 Kuala Lumpur
Fax : 03-2693 3625 E-mail : str@bnm.gov.my

DECLARATION FORM

DIGITAL CURRENCY EXCHANGERS

a This report is made pursuant to the requirement in section 8 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) - Digital Currency (Sector 6).

b This declaration shall be submitted under oath.

c Under section 24 of the AMLA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith.

d By submitting this form, you hereby agree that Bank Negara Malaysia (BNM) may utilise and disclose your personal data provided in this form, for ensuring transparency of digital currency business and provision of service under the AMLA.

e The information in this declaration form shall be updated by the reporting institutions, when necessary.

PART A: INFORMATION ON REPORTING INSTITUTION

Name of reporting institution			
Reporting institution type *(tick where applicable)*	Individuals ☐	Businesses ☐	LLP* ☐ **Limited Liability Partnership*

Individuals and LLP

Identification type		
Identification number	NRIC ☐	Passport ☐

Business only

Business registration no.	
Shareholder name	

All reporting institutions

Business address		
Contact number		
Email address		
Entity is offshore	Yes ☐	No ☐
Business platform	Web ☐	Please specify URL:
	Social media ☐	*Tick and specify group name (where applicable)*
		Telegram ☐
		Whatsapp ☐
		Others ☐ *(please specify)*

Key responsible person

Name of key responsible person	
Identification number	
Nationality	
Address	

Please append photo of key responsible person

Compliance Officer

Name of key responsible person	
Identification number	
Nationality	

PART B : INFORMATION ON BUSINESS

Business activities	Exchanging digital currency for money	☐			
(Tick where applicable)	Exchanging money for digital currency	☐			
	Exchanging one digital currency for another digital currency	☐			
Digital currencies transacted	Bitcoin	☐	Ether	☐	Ripple ☐
(Tick where applicable)	DASH	☐	Zcash	☐	Bitcoin Cash ☐
	Others ☐ *(please specify)*				
Wallet address					
Other services provided	Wallet	☐	Others	☐	*(please specify)*
Commencement of operations in Malaysia	since *(yyyy)*				

Annex 2

Examples of Transactions That May Trigger Suspicion

1. Transactions that appear inconsistent with a customer's known profile or unusual deviations from normal transaction or relationship.

2. Transactions that require the use of complex and opaque legal entities and arrangements.

3. Transaction with entity established in jurisdictions with weak or absent AML/CFT laws and/or secrecy laws.

4. A customer who is reluctant to provide evidence of his identity or where the customer is a corporate entity, evidence of its place of incorporation and the identity of its major shareholders and its director(s) or relevant officer(s).

5. Any situation where the identity of the customer is difficult to determine.

RAHSIA

Annex 3

Please send completed form to:
Financial Intelligence & Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn, 50480 Kuala Lumpur
Fax : 03-2693 3625 E-mail : str@bnm.gov.my

Reference no :_____

SUSPICIOUS TRANSACTION REPORT

DIGITAL CURRENCY EXCHANGERS

a. This report is made pursuant to the requirement to report suspicious transaction under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA)

b. Under section 24 of the AMLA, no civil, criminal or disciplinary proceedings shall be brought against a person who makes a report unless it was made in bad faith

PART A: INFORMATION ON CUSTOMER

Customer

1) Individual

Nationality			
Name			
Other/previous name	(1)		
	(2)		
	(3)		
New NRIC no		Old NRIC no	
Other identification		Other identification	
Gender			

Contact information

Residential/business address	Correspondence address
Other address	**Previous address**

RAHSIA

Reference no :

Email address	
Contact no	- (Off) - (Res) - (Mob)
Fax no	

Employment information

Business/ employment type	
Occupation	
Occupation description	
Employer name	
Employment area	
Other known employment	

Marital information

Marital status	
Spouse name	

Spouse identification

New NRIC no		Old NRIC no	
Other identification		Other identification type	
Passport no		Place/country of issue	

Person conducted the transaction

1 Individual

Nationality			
Name			
Other/previous name	(1)		
	(2)		
	(3)		
New NRIC no		Old NRIC no	
Other identification		Other identification	
Gender			

RAHSIA

Reference no :

Contact information

Residential/business address	Correspondence address

Other address	Previous address

Email address	
Contact no	- (Off) - (Res) - (Mob)
Fax no	

Employment information

Business/ employment type	
Occupation	
Occupation description	
Employer name	
Employment area	
Other known employment	

Marital information

Marital status	
Spouse name	

Spouse identification

New NRIC no		Old NRIC no	
Other identification		Other identification	
Passport no		Place/country of	

PART B: TRANSACTION DETAILS

Attempted but not completed: No

Transaction reference		Transaction type	
Date account opened		Status of relationship	
Transaction date	- to -		
Transaction amount (MYR)	0.00	Equivalent digital currency amount	0.00
Type of digital currency			

RAHSIA

Reference no :

PART C: DESCRIPTION OF SUSPICIOUS TRANSACTION	
Grounds for suspicion	Reactivated dormant account
	Large/unusual cash deposit/withdrawal
	Activity inconsistent with customer profile
	Payment is credited into a customer's account by a third party with no apparent relation to the customer
	Unwillingness of customer/third party to disclose identity
	Others (Please specify)
Others (please specify)	
Description of suspected criminal activity	
Details of the nature and circumstances surrounding it	
Date of reporting	

RAHSIA

Please send completed form to:
Financial Intelligence & Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn, 50480 Kuala Lumpur
Fax: 03-2693 3625 Email: xxx@bnm.gov.my

Annex 4

MONTHLY REPORT ON DIGITAL CURRENCY ACTIVITY STATISTICS AND FINANCIAL INFORMATION

Instructions:
(a) This reporting requirement is applicable to any reporting institution offering services to exchange digital currency either to fiat money or another digital currency, and vice versa, pursuant to Paragraph 20.1 of the Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) - Digital Currency (Sector 6) document
(b) Statistics reported should only capture all transactions involving the provision of services stipulated in part (a) to any user in Malaysia.
(c) The report must be completed on a monthly basis and submitted to Bank Negara Malaysia by the 10th after the end of the reporting month. Should the submission deadline fall on a weekend or public holiday, the deadline will be moved to the next working day.
(d) For daily average calculations, please use the number of days in the reporting month.

PART A: REPORTING INSTITUTION INFORMATION

Name of reporting institution		**Business address** *(entities)*	
Reporting period *(Month/Year)*		**Residential address** *(natural persons)*	
Details of Person Reporting:			
Name		**Contact email**	
Designation		**Contact number**	

PART B: DIGITAL CURRENCY (DC) TRANSACTION DATA

I. TRANSACTION DATA BY TYPE OF DIGITAL CURRENCY

Reporting digital currency:
(If more than one digital currency is offered by your entity, please fill in a separate table for each reporting digital currency. See Appendix to Annex 2 for illustration)

NUMBER OF TRANSACTIONS

		Fiat currency	Month total	Daily average
Conversions involving fiat currency	Fiat currency to reporting DC	*RM*		
		USD		
		Other currencies		
	Reporting DC to fiat currency	*RM*		
		USD		
		Other currencies		
Conversions involving other digital currencies	Other DC to reporting DC			
	Reporting DC to other DC			

VALUE OF TRANSACTIONS

		Fiat currency	Month total	Daily average *(up to two decimal places)*	Daily average conversion price per digital currency unit
Denominated in reporting digital currency value					
Conversions involving fiat currency	Fiat currency to reporting DC	*RM*			
		USD			
		Other currencies			
	Reporting DC to fiat currency	*RM*			
		USD			
		Other currencies			
Conversions involving other digital currencies	Other DC to reporting DC				
	Reporting DC to other DC				
Denominated in respective fiat currency* value					
Conversions involving fiat currency	Fiat currency to reporting DC	*RM*			
		USD			
		Other currencies (in USD equivalent)			
	Reporting DC to fiat currency	*RM*			
		USD			
		Other currencies (in USD equivalent)			

** Average price quoted on entity's platform as at the last day of the reporting period*

II. NET BUY/SELL POSITIONS (ORDER-BOOK)

Data reported for this section reflects the average number of customer bids for buy and sell positions in queue per day. This is calculated by adding the number of positions in queue recorded at the end of each day, divided by the number of days during the reporting month. See Appendix to Annex 2 for illustration.

Type of digital currency	Daily average of number of positions in order-book		Daily average of total transaction value* in order-book	
	Buy	*Sell*	*Buy*	*Sell*

**Denominated in digital currency value*

III. PURPOSE OF TRANSACTIONS

Please specify the purpose of transactions identified as a percentage of: i) total number of transactions; and ii) total transaction value, made through services you have offered during the month:

Purpose of transaction	Number of transactions (%)	Total transaction value	
		Value (USD)*	Percentage (%)
Investment			
Remittances			
a. Out of Malaysia			
b. Into Malaysia			
Payments in Malaysia			
Others *(please specify below)*			

**To provide in USD equivalent. For conversion rates, please use exchange rates quoted on the last day of the reporting month published on Bank Negara Malaysia's website.*

IV. PAYMENT METHOD

For digital currency transactions involving fiat currency conversions, please specify the method of payment used by your customers as a percentage of: i) total number of transactions; and ii) total transaction value, made through services you have offered during the month:

Payment method	Number of transactions (%)	Total transaction value	
		Value (USD)*	Percentage (%)
Bank transfers			
Cash			
Credit/debit card			
Online accounts *(e.g. Paypal, Unionpay, etc)*			
Others *(please specify below)*			

**To provide in USD equivalent. For conversion rates, please use exchange rates quoted on the last day of the reporting month published on Bank Negara Malaysia's website.*

PART C: CUSTOMER ACCOUNT DATA

I. NUMBER OF CUSTOMER ACCOUNTS

Type of customer		Total number of accounts at month-end *(Existing & new accounts)*	New accounts within month	Accounts terminated within the month
Natural persons	Malaysian			
	Non-Malaysian			
Entities	Incorporated in Malaysia			
	Incorporated outside of Malaysia			

II. ACCOUNTS AND OUTSTANDING VALUE

	Number of accounts	Outstanding value in account as at end reporting period		
		Digital currency value		Value in RM
Active accounts (At least 1 transaction in reporting month)		*E.g. BTC**		
		ETH		
Inactive accounts (No transactions made in reporting month)		*E.g. BTC*		
		ETH		

**Additional rows to be inserted for each type of reporting digital currency*

PART D: FINANCIAL INFORMATION OF ENTITY

Reporting institutions are required to submit the following:

1) Monthly balance sheet statement by the 10th after the end of each reporting month; and
2) Annual consolidated financial statement no later than 3 months after the end of the entity's financial year end period.

Appendix to Annex 4

Reporting Illustration for Part B, Sections I & II of the Monthly Report on Digital Currency Activity Statistics and Financial Information

The purpose of this section is to provide a simplified illustrative example of mathematical calculations for Part B, Sections I & II of the report.

Scenario
Reporting period: March 2018

PART B: DIGITAL CURRENCY (DC) TRANSACTION DATA

I. TRANSACTION DATA BY TYPE OF DIGITAL CURRENCY

Reporting digital currency: *Bitcoin (BTC)*

NUMBER OF TRANSACTIONS

		Fiat currency	Month total	Daily average
Conversions involving fiat currency	Fiat currency to reporting DC	*RM*	*5000*	*= 5000/31 = 161*
		USD	*3000*	*97*
		Other currencies	*600*	*19*
	Reporting DC to fiat currency	*RM*	*4000*	*13*
		USD	*2000*	*65*
		Other currencies	*400*	*13*
Conversions involving other digital currencies	Other DC to reporting DC		*250*	*8*
	Reporting DC to other DC		*150*	*5*

VALUE OF TRANSACTIONS

		Fiat currency	Month total	Daily average *(up to two decimal places)*	Daily average conversion price per digital currency unit
Denominated in reporting digital currency value					
Conversions involving fiat currency	Fiat currency to reporting DC	*RM*	*120 BTC*	*3.87 BTC*	
		USD	*50 BTC*	*1.61 BTC*	
		Other currencies	*30 BTC*	*0.97 BTC*	
	Reporting DC to fiat currency	*RM*	*110 BTC*	*3.55 BTC*	
		USD	*45 BTC*	*1.45 BTC*	
		Other currencies	*20 BTC*	*0.65 BTC*	
Conversions involving other digital currencies	Other DC to reporting DC		*10 BTC*	*0.32 BTC*	
	Reporting DC to other DC		*5 BTC*	*0.16 BTC*	
Denominated in respective fiat currency* value					
Conversions involving fiat currency	Fiat currency to reporting DC	*RM*	*RM8,280,000*	*RM267,097*	*RM69,000*
		USD	*USD800,000*	*USD25,806*	*USD16,000*
		Other currencies (in USD equivalent)	*USD481,500*	*USD 15,532*	*USD16,050*
	Reporting DC to fiat currency	*RM*	*RM7,480,000*	*RM241,290*	*RM68,000*
		USD	*USD675,000*	*USD21,774*	*USD15,000*
		Other currencies (in USD equivalent)	*USD 316,000*	*USD10,194*	*USD15,800*

** Average price quoted on entity's platform as at the last day of the reporting period*

Reporting digital currency: *Ether (ETH)*

NUMBER OF TRANSACTIONS

		Fiat currency	Month total	Daily average
Conversions involving fiat currency	Fiat currency to DC	*RM*	*10000*	*= 10000/31 = 323*
		USD	*6000*	*194*
		Other currencies	*1500*	*48*
	DC to fiat currency	*RM*	*8000*	*258*
		USD	*4000*	*129*
		Other currencies	*800*	*26*
Conversions involving other digital currencies	Other DC to reporting DC		*500*	*16*
	Reporting DC to other DC		*300*	*10*

VALUE OF TRANSACTIONS

		Fiat currency	Month total	Daily average *(up to two decimal places)*	Daily average conversion price per digital currency unit
Denominated in reporting digital currency value					
Conversions involving fiat currency	Fiat currency to DC	*RM*	*2000 ETH*	*64.52 ETH*	
		USD	*500 ETH*	*16.13 ETH*	
		Other currencies	*200 ETH*	*6.45 ETH*	
	DC to fiat currency	*RM*	*1000 ETH*	*32.26 ETH*	
		USD	*300 ETH*	*9.68 ETH*	
		Other currencies	*80 ETH*	*2.58 ETH*	
Conversions involving other digital currencies	Other DC to reporting DC		*50 ETH*	*1.61 ETH*	
	Reporting DC to other DC		*100 ETH*	*3.23 ETH*	
Denominated in respective fiat currency* value					
Conversions involving fiat currency	Fiat currency to DC	*RM*	*RM3,800,000*	*RM122,581*	*RM1,900*
		USD	*USD235,000*	*USD7,581*	*USD470*
		Other currencies (in USD equivalent)	*USD 97,000*	*USD 3,129*	*USD 485*
	DC to fiat currency	*RM*	*RM1,800,000*	*RM58,065*	*RM1,800*
		USD	*USD138,000*	*USD4,452*	*USD460*
		Other currencies (in USD equivalent)	*USD 37,200*	*USD 1,200*	*USD 465*

** Average price quoted on entity's platform as at the last day of the reporting period*

II. NET BUY/SELL POSITIONS (ORDER-BOOK)

Data reported for this section reflects the average number of customer bids for buy and sell positions in queue per day. This is calculated by adding the number of positions in queue recorded at the end of each day, divided by the number of days during the reporting month.

Type of digital currency	Daily average of number of positions in order-book		Daily average of total transaction value* in order-book	
	Buy	*Sell*	*Buy*	*Sell*
Bitcoin	*8,000*	*6,000*	*350 BTC*	*200 BTC*
Ether	*20,000*	*13,000*	*4000 ETH*	*2900 ETH*

**Denominated in digital currency value*