POLICY AND PROCEDURE FOR SEIZING CRYPTOCURRENCIES

DISCLAIMER

The purpose of this document is to provide generic guidance and suggested process on seizing cryptocurrencies. It was developed based on input from the relevant agencies, compilation of best available information, knowledge and field experience to provide guidance to Malaysian law enforcement officers so that activities are performed in a consistent and standardized manner.

This document should be used as a reference. However, differences may exist between the procedures referenced in this document and what is appropriate under field-specific conditions. For the avoidance of doubt, the use of this document shall not in any way create, or be relied upon to give rise to, any right in the user which may be enforceable at law in any matter whether civil or criminal.

Any products, manufacturers or organisations referenced in this document are presented for informational purposes only and do not in any way constitute approval or endorsement by National Anti-Financial Crime Center(NFCC) and CyberSecurity Malaysia(CSM).

COPYRIGHT AND CONFIDENTIALITY STATEMENT

FOREWORD
NATIONAL ANTI-FINANCIAL CRIME CENTER

Virtual assets including cryptocurrencies, have been identified in Malaysia's National Risk Assessment on Money Laundering and Terrorism Financing 2020 as posing a growing threat to the money laundering and terrorism financing landscape in Malaysia. Globally, there have been numerous cases in which cryptocurrency has been used to launder money such as Silk Road and BTC-e, as well as in illicit transactions in Darknet online marketplaces. A more concerted and collaborative efforts are needed to effectively address this new emerging threats, particularly from the angle of investigation.

In Malaysia, NFCC has forged solid collaboration with CyberSecurity Malaysia via MoU signed in August 2021, where one of key areas is on cryptocurrency. In November 2021, CyberSecurity Malaysia and NFCC have jointly organized a seminar on Cryptocurrencies in Digital Economy during the Malaysia Financial Crime Prevention Conference 2021(MFCPC'21) for law enforcement agencies. The seminar attended by 80 officers from 24 agencies in Malaysia aimed to enhance knowledge on cryptocurrency investigations, especially on the use of cryptocurrencies in criminal world, the impact to the digital economy, and ways to mitigate the crime.

Since then, CyberSecurity Malaysia and NFCC made joint efforts to prepare draft model policy and standard operating procedures of investigation and seizure of cryptocurrency. The aim of the document is to ensure all law enforcement agencies have right capabilities, adhere to sound policy and standard operating procedures to manage risk associated with investigation and seizure of cryptocurrencies. This is to also ensure that in doing so, the rights of all related parties are adequately protected. The document covers all key aspects of pre and post seizure to reduce and manage risk associated with cryptocurrencies seizure.

We wish to thank all members of our Executive Committee especially Royal Malaysia Police, Securities Commission, Bank Negara Malaysia, Attorney General's Office and Labuan Financial Services Authority for the feedbacks on the draft document. We also wish to thank our international partners particularly the United States of America and Australia, who shared their valuable knowledge and experience as well as provided inputs to improve our draft document.

We trust that this final document, once adopted and implemented as the policy and standard operating procedures applicable to the law enforcement agencies, will serve to facilitate the investigation related to cryptocurrency, and will eventually result in greater amount of cryptocurrencies seizure in the future.

Lastly, I wish to convey my special thanks to our partner, CyberSecurity Malaysia especially **Dato' Ts. Dr. Haji Amirudin Bin Abdul Wahab** and **Ts. Sarah Khadijah Taylor,** who have steadfastly worked with us on this project.

DATO' SERI HAJI MUSTAFAR BIN HAJI ALI
Director General,
National Anti-Financial Crime Center

FOREWORD
CYBERSECURITY MALAYSIA

Cryptocurrencies are often associated with financial and cybercrime activities. Despite the fact that cryptocurrencies offer their consumers convenience, they also possess characteristics that make them attractive to criminals. Among them are volatile prices, difficult tracking of funds and challenges in the seizure of cryptocurrencies.

However, I believe that despite the challenges in combating financial crimes involving cryptocurrencies, there are ways and strategies that we can do to tackle the issues and risks it brings. Apart from empowering the knowledge and technical skills of Malaysian Law Enforcement Agencies (LEA), a concerted effort involving enforcement, regulatory and technical agencies are needed to counter measure the criminal activities.

As such, CyberSecurity Malaysia, in collaboration with National Anti-Financial Crime Center (NFCC) have spearheaded the development of Policy and Procedure of Seizing Cryptocurrencies. These documents will serve as guidelines for high level management from the Malaysian LEA and Relevant Regulatory and Supervisory Authority (RRSA) as well as for the First Responder to follow during crime scene investigation.

I would like to take this opportunity to highlight that the development of these policy and procedure are only possible through the commitment and contribution of some Malaysian LEAs and RRSA such as Cryptocurrencies Unit of Commercial Crime Investigation Department, Police Diraja Malaysia (PDRM), Securities Commission (SC), Bank Negara Malaysia (BNM), Attorney General Chambers (AGC), Labuan Financial Services Authority (LFSA) and Suruhanjaya Pencegahan Rasuah Malaysia (SPRM). These policy and procedure are also developed based on inputs and interactions gathered from international counterparts such as, Australian Federal Police (AFP), and the International Criminal Police Organization (INTERPOL).

It is through cooperation and initiative such as this that we can continue to drive efforts to ensure that the issues and risks brought by cryptocurrencies can be dealt with effectively and impactfully. This in turn can ensure the safety and prosperity of the digital economy in Malaysia, and hence, benefitted the Rakyat in long terms.

DATO' Ts. DR HAJI AMIRUDIN ABDUL WAHAB FASc
Chief Executive Officer,
CyberSecurity Malaysia

DOCUMENT OVERVIEW

The nature of cryptocurrencies where it is intangible, high volatility, fast settlement, cross borders transactions and pseudonymous entities pose unique challenge to investigation and prosecution. However the manner of investigating cryptocurrencies case is largely similar to traditional method. The criminal schemes are not necessarily new schemes, but are traditional criminal schemes accomplished using the latest technology.

This document contains two(2) section; Policy and Procedure. Policy is high level statement whereas Procedure contains the details process on executing the statement. This document provides guidance to agency and its First Responder in seizing cryptocurrencies at field site.

DOCUMENT PURPOSE

The purpose of this document is to provide guidance to the Malaysian Law Enforcement Agency (LEA) and Relevant Regulatory and Supervisory Authority (RRSA) in seizing cryptocurrencies.

This document is applicable to LEA and RRSA operating under different operational frameworks. The statements in this document are made in general so that it can be adopted by various LEA and RRSA. As each agency may have own process, agency may need to elaborate further of each statement.

ACKNOWLEDGEMENT

This document was jointly developed by National Anti-Financial Crime Centre (NFCC) and CyberSecurity Malaysia (CSM) in collaboration with Cryptocurrencies Unit of Commercial Crime Investigation Department, Polis Diraja Malaysia (PDRM), Securities Commission Malaysia (SC), Bank Negara Malaysia (BNM), Labuan Financial Services Authority (LFSA) and Suruhanjaya Pencegahan Rasuah Malaysia (SPRM) to address challenges in investigating cryptocurrencies cases.

TABLE OF CONTENT

LIST OF TERMINOLOGIES

Term	Definition
Authorized Officer	Officer that has been appointed by the agency's higher authorities to hold and secure the seed phrase of the Controlled Cryptowallet.
Controlled Cryptowallet	A wallet that is under the control of the law enforcement agency whose role is to handle seized criminal proceeds[1].
Controlled Address	An official and secured address, controlled only by the seizing agency[2]. It is and where the corresponding private key is stored offline[3]. Controlled Addresses are generated from a Controlled Cryptowallet.
Cryptocurrencies	Cryptocurrency is a digital representation of value which is recorded on a distributed digital ledger whether cryptographically-secured or otherwise, that functions as a medium of exchange and is interchangeable with any money, including through the crediting or debiting of an account. It has the same meaning of assigned to it in accordance with definition of Digital Currency under the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019[4]. It is also known as a subset of virtual asset under the FATF[5].
Cryptowallet	A device or program that is used to send and receive cryptocurrencies.
Desktop wallet	A type of cryptowallet that requires user to download and install an application on a computer. It allows user to generate address to receive cryptocurrencies without the Internet, however Internet is needed to send out cryptocurrencies. To update the transaction records on the wallet, the wallet needs to connect to the Internet[6]. Examples of such wallet are Jaxx Liberty and MultibitHD.
First Responder	Officer who is authorized, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence[7].
Hardware wallet	A type of cryptowallet that comes in a hardware device[6]. To use the hardware, user needs to first install the hardware apps on user's device. It allows user to generate address to receive cryptocurrencies without the Internet, however Internet is needed to send out cryptocurrencies. To update the transaction records on the wallet, the wallet needs to connect to the Internet. Examples of such wallet are KeepKey, Ledger Nano, Trezor and Digital Bitbox.

1 'Guidelines for the Seizure and Sale of Virtual Assets' (Singapore: INTERPOL Innovation Centre, 2020), pp. 1–29.

2 'Guidelines on The Darknet and Cryptocurrencies' (Singapore: INTERPOL, 2020).

3 'Virtual Asset Seizure Best Practices' (Federal Bureau Investigation(FBI), 2020), pp. 1–45.

4 Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (Securities Commission Malaysia, 2019).

5 'Virtual Assets and Virtual Asset Service Providers (Updated October)' (Financial Action Task Force(FATF), 2021) <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>.

6 Sarah Taylor, K.Akram Z.Ariffin, and others, 'Cryptocurrencies Investigation : A Methodology for the Collection and Preservation of Cryptowallets', in 3rd International Cyber Resilience Conference (CRC) (IEEE, 2021), pp. 1–5 <https://doi.org/doi: 10.1109/CRC50527.2021.9392446>.

7 INCITS/ISO/IEC 27037:2012 (R2019) Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, 2019.

Term	Definition
Hosted wallet	A cryptowallet hosted by a third-party financial institution, known as the cryptocurrencies exchanger, or third party custodian services company[8]. The term unhosted wallet could also interchange with non-custodial wallet.
Mobile wallet	A type of cryptowallet installed on a smartphone. Examples are such as Hedera Wallet, Binance, Xapo, Luno Bitpay, MyCelium and Bitcoin Wallet.
OSINT	Open Source Intelligence Tool
Paper wallet	A piece of paper that contains a private key and an address. A paper wallet can be printed from the provider's website or a cryptocurrencies Automated Teller Machine (ATM)[6].
Private key	A cryptographic equivalent of a Personal Identification Number(PIN) or password. The private key is generated by the cryptowallet and it can be copied or stored in myriad locations[9].
Seed Phrase	A set of 12, 18 or 24 words used to regenerate the private keys[2]. The seed functions as a wallet backup and can recover and re-create all the private keys in the same or another compatible, deterministic wallet application[10].
Stablecoin	A type of cryptocurrencies designed to have a stable value as compared with other types of cryptocurrencies, which frequently experience significant volatility[11].
Sweep Procedure	A method of adding the value of an imported private keys to a new wallet. The process involves transferring the value associated with an address to a brand new address generated by—and backed up with a recovery key of—the new wallet[9].
Target Cryptowallet	A cryptowallet that is owned by the suspect.
Unhosted Wallet	A type of cryptowallet where owner has sole access to the private keys[12]. The term unhosted wallet could also interchange with non-custodial wallet.
Web Wallet	A type of cryptowallet hosted by the exchange, such as Coinbase, Binance and Luno. User needs to go the exchanger website and login to get access to wallet.

8 Sarah Taylor, Steve Ho-yong Kim, and others, 'A Comprehensive Forensic Preservation Methodology for Crypto Wallets', Forensic Science International : Digital Investigation, 42 (2022), 301477 <https://doi.org/10.1016/j.fsidi.2022.301477>.

9 Asset Forfeiture Policy Manual, U.S. Department of Justice, 2021 <https://www.justice.gov/criminal-afmls/file/839521/download>.

10 'Guidance on Financial Investigations Involving Virtual Assets' (Financial Action Task Force(FATF), 2019).

11 'Cryptocurrencies Enforcement Framework', U.S. Department of Justice (Washington, D.C, 2020) <https://www.justice.gov/ag/page/file/1326061/download>.

12 'Guidance on Financial Investigations Involving Virtual Assets'.

SECTION A
POLICY STATEMENT

1 POLICY STATEMENT

1.1 POWER TO INVESTIGATE

1.1.1 The investigation of an offence involving cryptocurrencies shall be conducted under the law of the relevant agency.

1.1.2 Upon investigation of the offence (serious offence), if there is an element of money laundering, terrorism financing or proliferation financing, another investigation is recommended to be opened under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001(AMLATFPUAA) [Act 613] and to be investigated in parallel with the said investigation.

1.1.3 Notification on the seizing and freezing under the AMLATFPUAA shall be in parallel with Section 44(9) and 50(1A) of the Guidance to Enforcement Agencies on Notification under Section 44(9) and Section 50(1A) of the AMLATFPUAA.

1.2 CONTROLLED CRYPTOWALLET AND CONTROLLED ADDRESS

1.2.1 Agency shall generate Controlled Cryptowallets for the management of the proceeds of crime before going to a crime scene. These wallets shall be used to store the seized cryptocurrencies.

1.2.2 Controlled Cryptowallet shall be generated using unhosted wallet, preferably a hardware wallet for a better guarantee of wallet security.

1.2.3 Controlled Cryptowallet shall be setup in a secure manner. The integrity and the chain of custody of this wallet shall be well-maintained.

1.2.4 The Controlled Address shall be well-managed so as to ensure the recovery and the forfeiture of the crypto asset in future can be executed in orderly and effective way.

1.2.5 Agency shall appoint and authorize a Cryptowallet Managing Officer (CMO) to generate and manage the Controlled Cryptowallet.

1.2.6 The CMO shall have sufficient training and demonstrate understanding of how cryptocurrencies work. The CMO shall be explained on the associated risks and his/her responsibility on managing and securing the crypto wallet.

1.2.7 For joint task force activity, the Controlled Cryptowallet shall be generated and managed by the Lead Agency.

1.2.8 The Controlled Cryptowallet and the Controlled Addresses shall be reviewed at a planned schedule by authorized officer (such as Internal Auditor) to verify that the integrity of the seized cryptocurrencies and the seed phrase are intact.

1.3 GENERAL PROCEDURE OF SEIZURE

1.3.1 Depending on under which law a search and seizure to be conducted, if required, search warrant to be obtained from the court. The application for the said search warrant shall contain the required information, inter alia -

a. nature of the offence that has been committed;
b. nature of evidence or thing which is necessary to the conduct of the investigation of the said offence;
c. description of the house or place, or part thereof, to which the search to be confined; and
d. name(s) of the First Responder(s) to execute the warrant.

1.3.2 The evidence or thing, in particular the cryptocurrencies, seized at the search location or crime scene shall be immediately preserved by the First Responder. The preservation is conducted by transferring the cryptocurrencies to the Controlled Address.

1.3.3 The process of transferring the cryptocurrencies shall be witnessed by the suspect or other person present at the premise.

1.3.4 The cryptocurrencies shall be retained in its original form when transfer is made. This is to preserve the integrity of the evidence.

1.3.5 The process of transferring cryptocurrencies to the Controlled Address requires some transaction fee. This fee is imposed by the cryptocurrencies network from the target's cryptowallet in order to allow the transaction to take place. Suspect shall bear the cost for the fees associated with this transaction.

1.3.6 Some wallets offer choices for transaction fee. In this case, First Responder shall choose transaction fee that facilitate fast processing to minimize any potential risks that may jeopardize the investigation. Risks are such as the safety of the First Responder and the safety of the carried tools at the crime scene.

1.3.7 There are a lot of emerging cryptocurrencies in the market. Some of these cryptocurrencies may lose value over time. When it is foreseen that the value will significantly reduce, First Responder may opt for converting the cryptocurrencies to stablecoin or to fiat currency to retain its value. This shall be done in accordance with law and with the consent of higher authority within the LEA.

1.3.8 All process conducted during search and seizure shall be properly documented in relevant forms.

1.3.9 The detailed process of seizing cryptocurrencies is explained in section 2 *Procedure* of this document.

1.4 FORFEITURE AND RECOVERY

1.4.1 The seized cryptocurrencies shall be forfeited or recovered in accordance with law, including if required with the order of the court.

1.5 TRAINING

1.5.1 Officers involved in with cryptocurrencies investigation and prosecution shall have sufficient training before conducting the tasks. The knowledge and skill shall be adequately tested prior to the tasks.

1.5.2 Continuous training program shall also be created to ensure officers keep updated with new cryptocurrencies technology.

1.5.3 Training program and training materials shall be updated to reflect the latest development of technology. Collaboration from external parties such as technology developer and industry player can be incorporated into the training program in order to get latest updates on the technology.

1.5.4 Awareness program shall also be conducted to other officers not dealing directly with investigation and prosecution.

1.6 WORKING WITH EXTERNAL PARTIES

1.6.1 The trustworthiness of an external party and potential conflict of interest must be considered when cooperation is required from private sectors. Confidentiality of an investigation must be maintained at all times.

1.6.2 For communication and networking purposes, it is advisable to identify the person in charge of the said cooperation i.e liaison officers.

1.7 BREACH OF CONTROLLED CRYPTOWALLET

1.7.1 Should there be evidence or suspicion showing that the Controlled Cryptowallet has been compromised, the officer holding the information shall report this matter to the relevant authorities in his or her organization.

1.7.2 The relevant authorities shall investigate this matter by following the agency's internal inquiry procedure.

1.7.3 The relevant authorities shall form a solution to mitigate the Controlled Cryptowallet security issue by gathering technical inputs from the experts. Experts may come from internal or external parties.

SECTION B
PROCEDURE STATEMENT

2 PROCEDURE STATEMENT

2.1 PREPARING FOR THE SEIZURE

2.1.1 Seizure of cryptocurrency largely requires First Responder to transfer tainted cryptocurrencies discovered at field site into a Controlled Cryptowallet owned by the Law Enforcement Agency(LEA).

2.1.2 A Cryptowallet Managing Officer (CMO) should be appointed to manage the Controlled Cryptowallet. Refer to *Form for Appointment of CMO* as a guide.

2.1.3 First Authorized Officer, Second Authorized Officer and Third Authorized Officer should also be appointed as the custodian for the Controlled Cryptowallet's seed phrase. Refer to *Form for Appointment of Authorized Officer* as a guide.

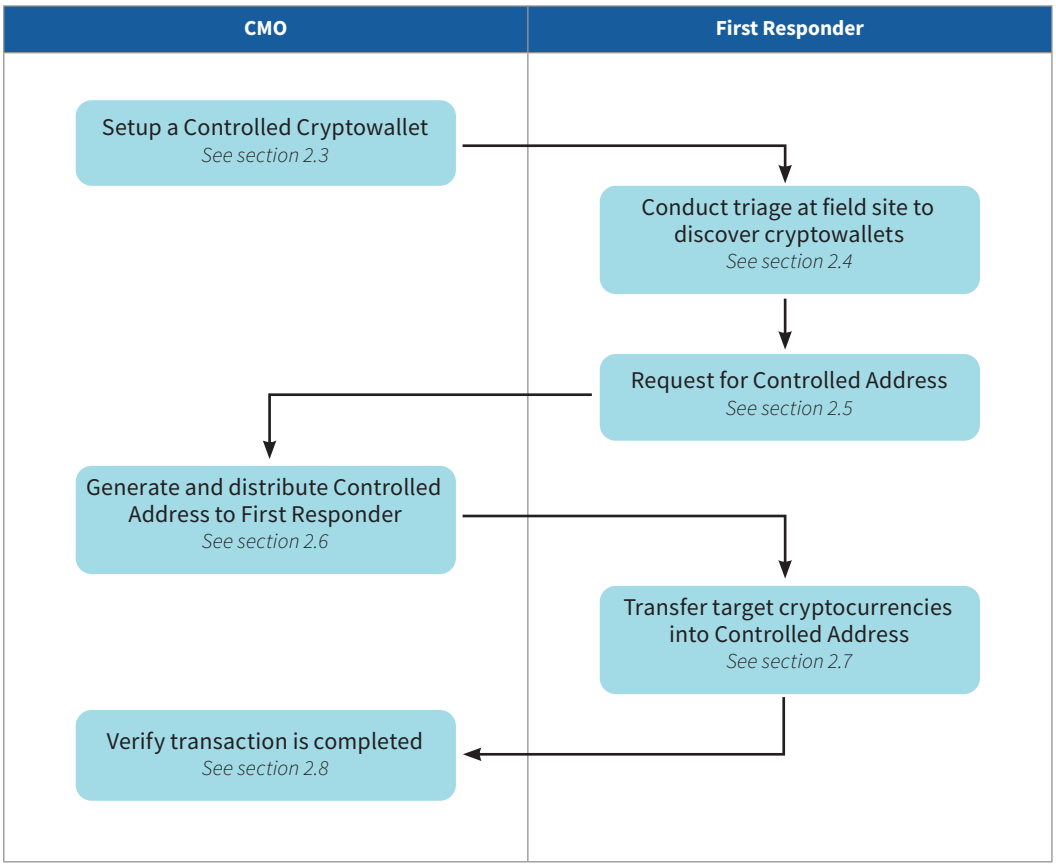
2.1.4 CMO and the exhibit vault keeper must not be the same officer. In other word, they must be different officers.

2.1.5 All necessary forms used for cryptocurrency seizure must be prepared before hands. The following are the list of suggested forms:

a. Form to document the creation of Controlled Cryptowallet. See *Form of Generate Controlled Cryptowallet* as a guide.
b. Form to document the seized cryptocurrencies. See *Form of Seizing Cryptocurrencies* as a guide.
c. Form to register all generated Controlled Cryptowallet. See *Form of Controlled Cryptowallet List* as a guide.
d. *Chain of Custody Form* to log movement of the Controlled Cryptowallet.

2.2 SEIZING CRYPTOCURRENCIES

2.2.1 The general procedure of seizing cryptocurrencies is illustrated in the following *Process Flow 1*.



Process Flow 1. Overall cryptocurrencies seizing process

2.2.2 Prior to the seizing activity, a Controlled Cryptowallet need to be generated by the CMO. This process is further explained in section 2.3.

2.2.3 At the field site, First Responder conducts triage on digital evidence to locate cryptowallets belong to suspect(target wallet). This process is further explained in section 2.4.

2.2.4 Upon discovering the target wallet, First Responder requests for Controlled Address from the CMO. This process is further explained in section 2.5.

2.2.5 CMO then generates Controlled Address and distribute it to the First Responder. This process is further explained in section 2.6.

2.2.6 First Responder transfers the cryptocurrencies from the target wallet to the Controlled Address, which is explained further in section 2.7.

2.2.7 CMO verifies that the transaction is completed, and the process is described in section 2.8.

2.3 SETTING UP A CONTROLLED CRYPTOWALLET

2.3.1 A Controlled Cryptowallet is setup by using a hardware wallet. Hardware wallets provide higher security as opposed to desktop, mobile, web or paper wallet. This wallet usually comes with an application to allow user to generate addresses and to view account balance.

2.3.2 The process of setting up a Controlled Cryptowallet is illustrated in the *Process Flow 2*.

2.3.3 First, uniquely label the Controlled Wallet and register it. Refer to *Form of Controlled Cryptowallet List* as a guide.

2.3.4 Next, download the cryptowallet application from its official website and consider to verify that the hash of the application from the website is matched with the hash of the downloaded file. Next install it on agency's computer, then disconnect the computer from the Internet after installation is completed. It is strongly suggested that the computer is secured with anti-virus in place.

2.3.5 Generate the cryptowallet's PIN code. Document the PIN code and keep the completed form in a dedicated folder. Refer to *Form of Generate Controlled Cryptowallet (1 of 4)* as a guide.

2.3.6 Next, generate the cryptowallet seed phrase and write words 1 to 16 in hardcopy format. Refer to *Form of Generate Controlled Cryptowallet (2 of 4)* as a guide. Fold this paper according to its instructions, put it in an envelope, seal it and distribute it to the agency's First Authorized Officer.

2.3.7 Write words 8 to 24 of the seed phrase in dedicated form. Refer to *Form of Generate Controlled Cryptowallet (3 of 4)* as a guide. Fold this paper according to its instructions, put it in an envelope, seal it and distribute it to the agency's Second Authorized Officer.

2.3.8 Then, write words 1 to 8 and 16 to 24 of the seed phrase in dedicated form. Refer to *Form of Generate Controlled Cryptowallet (4 of 4)* as a guide. Fold this paper, put it in an envelope, seal it and distribute it to the agency's Third Authorized Officer.

2.3.9 Authorized Officer receives the sealed envelope and keep the envelope securely in a locked cabinet.

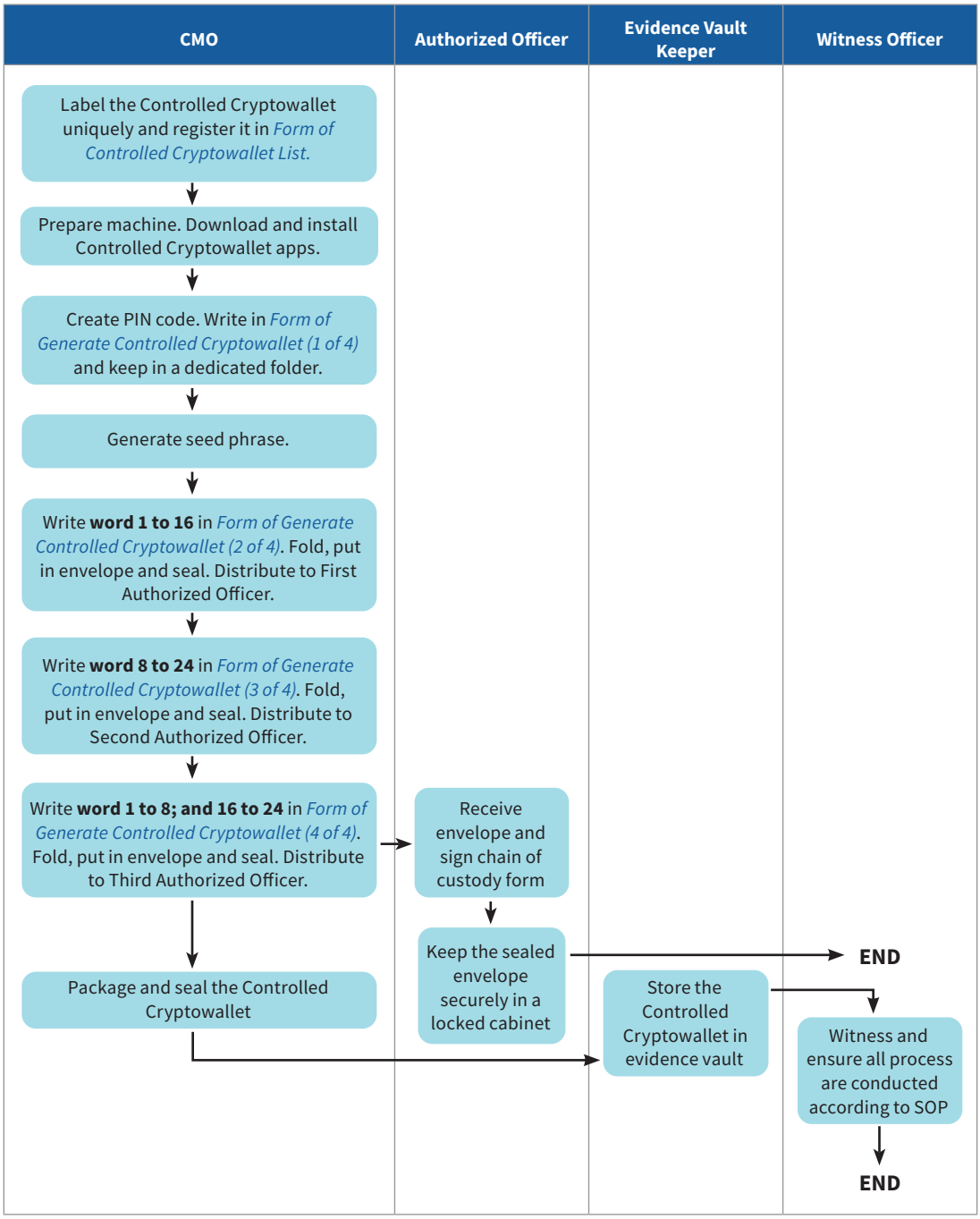
2.3.10 Package, seal and hand over the Controlled Cryptowallet (the hardware) to the Evidence Vault Keeper.

2.3.11 Evidence Vault Keeper stores the Controlled Cryptowallet in the evidence vault according to agency's procedure.

2.3.12 Ensure all process are witnessed by another officer.

2.3.13 When setting up the Controlled Cryptowallet, ensure that the following process is adhered to:

a. No camera is recording the PIN code and the seed phrase, including CCTV.
b. Seed phrase is not written intentionally or unintentionally anywhere, ie. on another paper or on the table surface and treated as confidential information
c. *Form of Generate Controlled Cryptowallet* are immediately distributed to the Authorized Officers.



Process Flow 2. Setting up a Controlled Cryptowallet

2.4 CONDUCT TRIAGE TO LOCATE TARGET WALLET

2.4.1 At the field site, conduct triage on digital evidence to find existence of a cryptowallet. To do this, First Responder must access the digital evidence and depending on relevant law, suspect's cooperation must be sought in order to gain access to the evidence (mobile phone, computer, tablet, etc).

2.4.2 DO NOT turn off the Internet connection of the target device before transfer is made. This is because the transfer process requires Internet. In addition, some cryptowallet that has multifactor authentication may send SMS or Google Authenticator message to that device. In doing so, ensure that the device is secure from remote access with malicious intent.

2.4.3 Access target device and locate cryptocurrencies artifacts. This can be cryptowallet application installed, online account, emails, Google Authenticator, SMS or any data showing the use of cryptocurrencies.

2.4.4 Extend the search to physical premise to locate hardware wallet, paper wallet or written seed phrase on piece of paper, engraved surfaces or other medium.

2.4.5 When target wallet is discovered, video record the wallet details such as user profile, list of transactions, list of saved addresses and bank accounts. Alternatively, First Responder can look for the seed phrase and document it in the *Form of Seizing Cryptocurrencies*. Digital Forensics Analyst can then recover and extract addresses of the target cryptowallet by using the seed phrase at later stage.

2.4.6 If the target wallet contains cryptocurrencies values, transfer need to be made from suspect's wallet to Controlled Cryptowallet without delay. Proceed to next process.

2.5 REQUEST CONTROLLED ADDRESSES AT FIELD SITE

2.5.1 First Responder requests for Controlled Addresses from the CMO. Request can be made in a form of email or instant messaging.

2.5.2 When request is made, the following data, among others, need to be supplied to the CMO (as *Figure 1*):

a. Exhibit number
b. Wallet application, ie. Binance, Luno, Jaxx Liberty
c. Cryptocurrencies type, ie. BTC, ETH, USDT
d. Blockchain network; ie. TRC-20, BEP-20 or ERC-20

2.5.3 The above information, except the Exhibit Number, need to be obtained from the target wallet.

2.5.4 First Responder must ensure that the accurate cryptocurrencies and blockchain information is being supplied to the CMO. Mistake in supplying these informations could cause the failure of cryptocurrencies retrieval. For example, Tether(USDT) is available on ERC-20, TRC-20 and BEP-20; if it is run on ERC-20, then the generated Controlled Address must also compatible with ERC-20.

Figure 1. Example of an instant message sent by the First Responder to the CMO requesting for a Controlled Address

2.6 GENERATE A CONTROLLED ADDRESS

2.6.1 The CMO, who can be at the field site or at the command center, generates a new, fresh Controlled Address for each of the request.

2.6.2 **DO NOT** use the same Controlled Address as it may lead to conflict during asset recovery or forfeiture at later stage.

2.6.3 The Controlled Address must be labelled properly so that it can be traced to the case number and the seized digital evidence. See *Figure 2* for reference.

2.6.4 When CMO is responding to the First Responder, the following data, among others, need to be supplied to the officer (as *Figure 3*):

a. Exhibit number
b. Controlled Address tagging (refer *Figure 2*)
c. Wallet application, ie. Binance, Luno, Jaxx Liberty
d. Cryptocurrencies type
e. Controlled Address in QR code and in text format

2.6.5 Upon receive of the Controlled Address, First Responder ensures that it is valid and has no transaction by checking the address on blockchain explorer. Refer to *Appendix A* for sample of invalid address and *Appendix B* for sample of address without transaction.

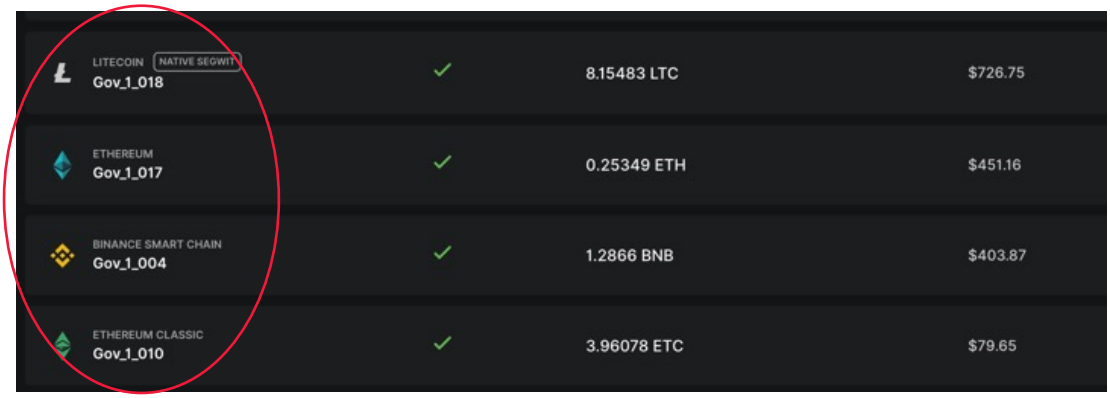
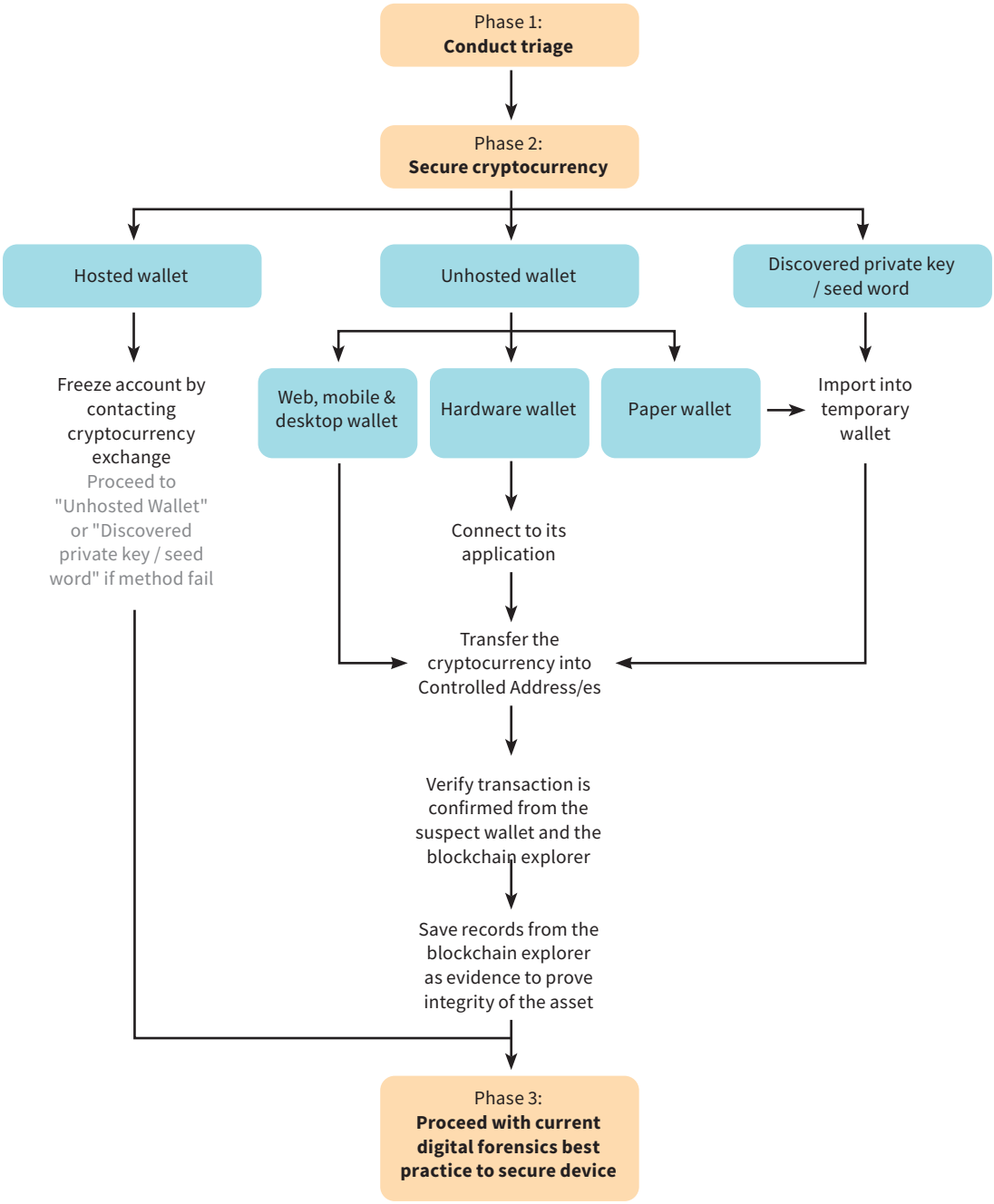


Figure 2. A display of Ledger Live, a software application for hardware wallet Ledger Nano. The first column shows unique taggings have been used for each of the generated Controlled Address.

Figure 3. Example of response in instant messaging received from CMO.

2.7 TRANSFER CRYPTOCURRENCIES TO CONTROLLED ADDRESS

2.7.1 The process of transferring crytocurrencies from target wallet to the Controlled Address depends on type of the target wallet, as illustrated in *Process Flow 3*.



Process Flow 3. Process of transferring cryptocurrencies depending on types of the target wallet.

2.7.2 The following process to be followed depending on types of target wallet discovered at field site (refer to *Appendix C* for samples of wallets):

A. HOSTED WALLET

i. Hosted wallet is operated by an exchanger, hence, First Responder can contact the exchanger and request for account freeze. Information such as email address, phone number or account name need to be supplied to the exchanger for account freeze.

ii. Foreign exchanger may involve and legal procedures need to be considered, such as Mutual Legal Assistance(MLA), warrants and subpoenas.

iii. If the account could not be frozen due to uncontactable third-party, unregulated business operation, or failure to comply within the desired time frame, then proceed to follow steps *B Web, Mobile or Desktop Wallet*.

B. WEB, MOBILE OR DESKTOP WALLET

i. Perform a direct transfer from the target cryptowallet into the Controlled Address.

ii. Scan the QR code of Controlled Address or type it into the target cryptowallet, then press submit button. Proceed to *section 2.8*.

C. HARDWARE WALLET

i. If seed phrase of the target hardware wallet is available, restore the target wallet into agency's hardware wallet. The restoration must be conducted on agency's device (laptop or tablet).

ii. Then perform transfer from the restored wallet into the Controlled Address. Proceed to *section 2.8*.

iii. If seed phrase is not available, then request PIN code of the target hardware wallet from suspect.

iv. Download the cryptowallet apps from its official website and consider to verify that the hash of the apps from the website is matched with the hash of the downloaded file. Install it on the agency's device.

v. Connect the target hardware wallet to the agency's device. Enter the PIN code. Be caution that some hardware wallet will lock after three times of wrong PIN guess. If this happens, the data on the hardware will be wiped. The cryptocurrencies, however, can still be accessible if seed phrase is available.

vi. Then perform transfer from the target wallet into the Controlled Address. Proceed to *section 2.8*.

D. PAPER WALLET

i. Identify the compatible cryptowallet with the paper wallet and the right blockchain network. This information can be sought from the suspect or via OSINT.

ii. Install the identified cryptowallet to hold the target cryptocurrencies temporarily on the agency's device. Always choose unhosted wallet downloaded from official website.

iii. Import the public address into the temporary cryptowallet by scanning the QR code or typing the address in. Press submit.

iv. After completion, follow steps *B Web, Mobile or Desktop Wallet* to transfer the target cryptocurrencies into Controlled Address.

E. SEED PHRASE IS DISCOVERED

i. Identify the compatible cryptowallet with the paper wallet and the right blockchain network. This information can be sought from the suspect or via OSINT.

ii. Create a temporary cryptowallet to hold the target cryptocurrencies temporarily on the agency's device. Always choose unhosted wallet downloaded from official website. This wallet must be installed on a device owned by the agency.

iii. On the temporary cryptowallet apps, choose restore wallet, then type in the seed phrase.

iv. After completion, follow steps *B Web, Mobile or Desktop Wallet* to transfer the target cryptocurrencies into Controlled Address.

2.8 VERIFY THE TRANSACTION

2.8.1 Verify that the transaction is completed by observing the balance from target wallet; and from the blockchain explorer. Ensure minimum confirmation blocks have been reached before exiting the premise; ie. Bitcoin is 6 confirmations while Ethereum is 15 confirmations.

2.8.2 Save the URL of the blockchain explorer as well as PDF format of the blockchain explorer into case file. This will serve as a receipt for the transaction, like the ATM slip.

2.8.3 Document the transfer process in dedicated form. Refer to *Form of Seizing Cryptocurrencies* as guide. Due to the long characters and numbers of the addresses and transaction hashes, this form must be written in softcopy format and saved into PDF format.

2.8.4 After cryptocurrencies have been transferred, proceed with digital evidence best practice to secure device.

2.8.5 If the device is a mobile phone, then follow current best practice to secure phones, and if the device is a computer, follow the computer best practice.

2.9 CONSIDERATIONS WHEN SEIZING TARGET CRYPTOCURRENCIES

2.9.1 All process must be meticulously documented, preferably in softcopy format to prevent error.

2.9.2 Addresses from where the target wallet receives its cryptocurrencies must be documented, by browsing through each transaction and video record it.

2.9.3 Alternatively, First Responder can look for the seed phrase and document it in the *Form of Seizing Cryptocurrencies*. The Digital Forensics Analyst can then recover and extract addresses of the target cryptowallet by using the seed phrase in the laboratory at later stage.

2.9.4 Some wallets offer choices for transaction fee. Always choose highest fee or default fee provided by the cryptowallet. Choosing low fee will result in delay in confirmation of the transaction to the Controlled Address.

2.9.5 When target cryptowallet has various kinds of cryptocurrencies, always conduct transfer of Ethereum at the last stage. This is because some cryptocurrencies require fee in Ethereum, and hence, a balance of Ethereum is required.

2.9.6 Ensure process conducted at the field site is witnessed by another officer.

2.10 SEIZING CRYPTOCURRENCIES UNSUPPORTED BY CONTROLLED CRYPTOWALLET

2.10.1 In the event that the cryptocurrencies type is not supported by the Controlled Cryptowallet or any unhosted wallet, then First Responder may conduct the following options:

a. Option a: Leave the cryptocurrencies as it is (no transfer is conducted). Video-record all details of the target wallet including user profile and transaction records, and then seize the digital evidence;

b. Option b: Liquidate the cryptocurrencies into fiat currency or convert the currency into stablecoin (USDC or USDT). This step however may tamper with the evidence integrity as the original condition is no longer retained, hence proper legal documentation is required. This process requires agency to follow own SOP on liquidation of proceeds of crime.

2.10.2 Document clearly all process in the dedicated form. Refer to *Form of Seizing Cryptocurrencies* as guide.

2.11 REVIEW ON CONTROLLED ADDRESS AND CONTROLLED CRYPTOWALLET

2.11.1 The Controlled Address that contains seized cryptocurrencies must be reviewed and checked by CMO once in every three (3) months. This is to ensure the seized cryptocurrencies is still intact. Any discrepancy must be reported to supervisor immediately.

2.11.2 The Controlled Cryptowallets PIN codes kept in a dedicated folder must be checked by the CMO at least once a year to ensure the paper is still in good condition and the handwriting is legible.

2.11.3 The Controlled Cryptowallets seed phrase kept by the Authorized Officers must also be checked by the CMO at least once a year to ensure the paper is still in good condition and the handwriting is legible.

3 LIST OF CONTACTS

For crime scene investigation and technical advise:
Head of Digital Forensics Department, CyberSecurity Malaysia
Phone: +603 - 8800 7999
Email: dfd@cybersecurity.my
www.cybersecurity.my

For coordination of money laundering investigation involving multi enforcement agencies:
Director of Integrated Operation (DIO),
National Anti-Financial Crime Center
Phone: (general extension)
Email: dio_nfcc@jpm.gov.my
https://nfcc.jpm.gov.my

Form1.Crypto

FORM FOR APPOINTMENT OF CRYPTOWALLET MANAGING OFFICER(CMO)

Dear <Name>,

ETTER OF APPOINTMENT AS CRYPTOWALLET MANAGEMENT OFFICER(CMO)

This letter is to inform that you have been appointed as CMO for <agency name>. This is effective from date of today, until further notice.

2. The duties and responsibilities of CMO are to:
   a. Manage Controlled Cryptowallets as described in Policy and Procedure for Seizing Cryptocurrencies
   b. Conduct regular review on Controlled Address and Controlled Cryptowallet to ensure its integrity is intact
   c. Report any irregularities related to cryptocurrencies seizing process to higher management *(to be defined by agency)*
   d. Conduct regular awareness program to First Responder for technology and procedure updates
3. You are required to perform activities of CMO in addition to your existing duties.

Thank you.

Yours faithfully,

NAME
DESIGNATION
<Higher authority>

Acknowledgement

I, _____, staff ID: _____ hereby acknowledge and accept the above appointment.

Sign:
Designation:
Date:

Form2.Crypto

FORM FOR APPOINTMENT OF AUTHORIZED OFFICER

Dear <Name>,

LETTER OF APPOINTMENT AS FIRST/SECOND/THIRD AUTHORIZED OFFICER

This letter is to inform that you have been appointed as First Authorized Officer for <agency name>. This is effective from date of today, until further notice.

2. The duties and responsibilities of Authorized Officer are as follows:
   a. Safekeep the seed phrase sealed in an envelope as described in Policy and Procedure for Seizing Cryptocurrencies
   b. Maintain secrecy of seed phrase at all times
   c. Cooperate with Cryptowallet Management Officer(CMO) during review and check process of the seed phrase.
3. You are required to perform activities of Authorized Officer in addition to your existing duties.

Thank you.

Yours faithfully,

NAME
DESIGNATION
<Higher authority>

Acknowledgement

I, _____, staff ID: _____ hereby acknowledge and accept the above appointment.

Sign:
Designation:
Date:

Form3.Crypto

FORM OF GENERATE CONTROLLED CRYPTOWALLET (1 OF 4)

Instructions:

1. CMO shall setup the Controlled Cryptowallet using a dedicated laptop used ONLY for wallet setup.
2. The setup process shall be witnessed by another officer.
3. Once done, keep this page in dedicated crypto case file.

SECTION A: WALLET DETAILS

1.	Wallet ID	:	
2.	Wallet Brand	:	
3	Wallet PIN code	:	
3.	Generated by	Sign here	:
		Name	:
		Staff ID	:
		Date & Time	:
4.	Witnessed by	Sign here	:
		Name	:
		Staff ID	:
		Date & Time	:

SECTION B: CHAIN OF CUSTODY

Date & Time	From	To	Purpose
	Sign here Name:	Sign here Name:	
	Sign here Name:	Sign here Name:	
	Sign here Name:	Sign here Name:	
	Sign here Name:	Sign here Name:	

Form3.Crypto

FORM OF GENERATE CONTROLLED CRYPTOWALLET (2 OF 4)

Instructions:

1. CMO generates the Controlled Wallet seed phrase, and fill in this form.
2. Fold this form, put in an envelop and seal it.
3. Handover this form to the **FIRST AUTHORIZED OFFICER.**
4. Document the movement of sealed envelop in Chain of Custody form.
5. Keep the Chain of Custody form in case file.
6. Ensure all process is witnessed by another officer.

Warning:

Fill all the fields CAUTIOUSLY. Failure to fill these in correctly will result in the LOSS OF THE CRYPTOCURRENCY FOREVER.

1.	Wallet ID	:			
2.	Wallet Brand	:			
3.	Generated by	Sign here	:		
		Name	:		
		Staff ID	:		
		Date & Time	:		
4.	Witnessed by	Sign here	:		
		Name	:		
		Staff ID	:		
		Date & Time	:		
5.	The first 16 seed words	Word 1	:	Word 9	:
		Word 2	:	Word 10	:
		Word 3	:	Word 11	:
		Word 4	:	Word 12	:
		Word 5	:	Word 13	:
		Word 6	:	Word 14	:
		Word 7	:	Word 15	:
		Word 8	:	Word 16	:
6.	PIN code of the Controlled Cryptowallet	:			

Form3.Crypto

FORM OF GENERATE CONTROLLED CRYPTOWALLET (3 OF 4)

Instructions:

1. CMO generates the Controlled Wallet seed phrase, and fill in this form.
2. Fold this form, put in an envelop and seal it.
3. Handover this form to the **SECOND AUTHORIZED OFFICER.**
4. Document the movement of sealed envelop in Chain of Custody form.
5. Keep the Chain of Custody form in case file.
6. Ensure all process is witnessed by another officer.

Warning:

Fill all the fields CAUTIOUSLY. Failure to fill these in correctly will result in the LOSS OF THE CRYPTOCURRENCY FOREVER.

1.	Wallet ID	:			
2.	Wallet Brand	:			
3.	Generated by	Sign here	:		
		Name	:		
		Staff ID	:		
		Date & Time	:		
4.	Witnessed by	Sign here	:		
		Name	:		
		Staff ID	:		
		Date & Time	:		
5.	The 8 to 24 seed words	Word 8	:	Word 17	:
		Word 9	:	Word 18	:
		Word 10	:	Word 19	:
		Word 11	:	Word 20	:
		Word 12	:	Word 21	:
		Word 13	:	Word 22	:
		Word 14	:	Word 23	:
		Word 15	:	Word 24	:
		Word 16	:		
6.	PIN code of the Controlled Cryptowallet	:			

Form3.Crypto

FORM OF GENERATE CONTROLLED CRYPTOWALLET (4 OF 4)

Instructions:

1. CMO generates the Controlled Wallet seed phrase, and fill in this form.
2. Fold this form, put in an envelop and seal it.
3. Handover this form to the **THIRD AUTHORIZED OFFICER.**
4. Document the movement of sealed envelop in Chain of Custody form.
5. Keep the Chain of Custody form in case file.
6. Ensure all process is witnessed by another officer.

Warning:

Fill all the fields CAUTIOUSLY. Failure to fill these in correctly will result in the LOSS OF THE CRYPTOCURRENCY FOREVER.

1.	Wallet ID	:			
2.	Wallet Brand	:			
3.	Generated by	Sign here	:		
		Name	:		
		Staff ID	:		
		Date & Time	:		
4.	Witnessed by	Sign here	:		
		Name	:		
		Staff ID	:		
		Date & Time	:		
5.	The 1 – 8 and 16 - 24 seed words:	Word 1	:	Word 16	:
		Word 2	:	Word 17	:
		Word 3	:	Word 18	:
		Word 4	:	Word 19	:
		Word 5	:	Word 20	:
		Word 6	:	Word 21	:
		Word 7	:	Word 22	:
		Word 8	:	Word 23	:
				Word 24	:
6.	PIN code of the Controlled Cryptowallet	:			

Form4.Crypto

FORM OF SEIZING CRYPTOCURRENCIES (1 OF 3)

SECTION A: TARGET CRYPTOCURRENCY DETAILS

Instructions:

1. Fill in all the fields in this form in softcopy format.
2. Use copy and paste method for Transaction ID, Controlled Address and URL blockchain explorer; never write them down.
3. After completed, save this file into PDF with appropriate filename.

Case No:				**Exhibit No:**					
No	**Apps Name** Binance, Huobi,..	**Coin Type** USDT, BTC, LTC	**Total Coin** 0.3411	**Current MYR Value**	**Successful transfer?** Y | N	**Transaction ID**	**Controlled Address**	**URL Blockchain Explorer** Must copy and paste from DF workstation	**Controlled Wallet ID**
		Total:							

Form4.Crypto

FORM OF SEIZING CRYPTOCURRENCIES (2 OF 3)

SECTION B: CONVERSION DETAILS

No	Coin Type	Reference for MYR Value (the URL & Screenshots)

SECTION C: TARGET WALLET DETAILS

Conducted By:

Sign here

Name :
IC Number :
Date & Time :

Witnessed By:

Sign here

Name :
IC Number :
Date & Time :

Form4.Crypto

FORM OF SEIZING CRYPTOCURRENCIES (3 OF 3)

SECTION D: WALLET RECOVERY DETAILS

This section is to document the target cryptowallet's seed phrase. Let this blank if the seed phrase is not available.

---------- 2. FOLD THIS SECTION AND ENSURE THE WORDS ARE NOT VISIBLE FROM OUTSIDE. SEAL THIS PAGE. ----------

---------- 1. FOLD THIS SECTION FIRST AND ENSURE THE WORDS ARE NOT VISIBLE FROM OUTSIDE. ----------

No	Apps Name	Seed Phrase/Recovery Seed/Recovery Phrase

Form5.Crypto

FORM OF CONTROLLED CRYPTOWALLET LIST

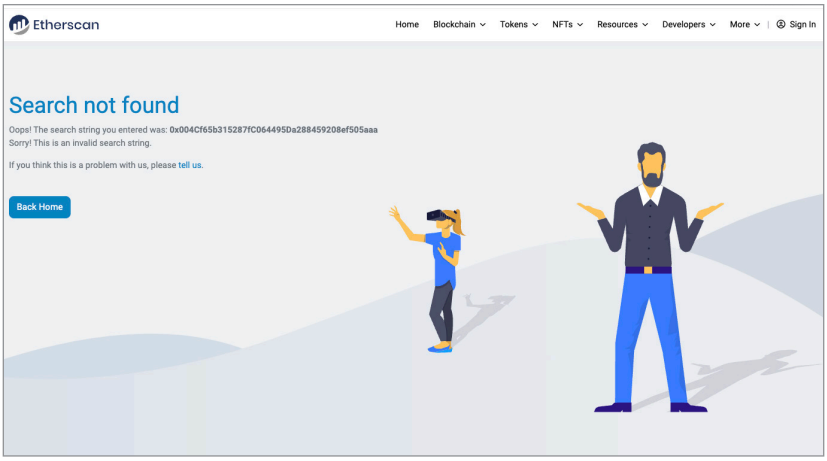
Instruction:

This form is to list all generated Controlled Cryptowallet. This form needs to be filled in by the Cryptowallet Managing Officer(CMO).

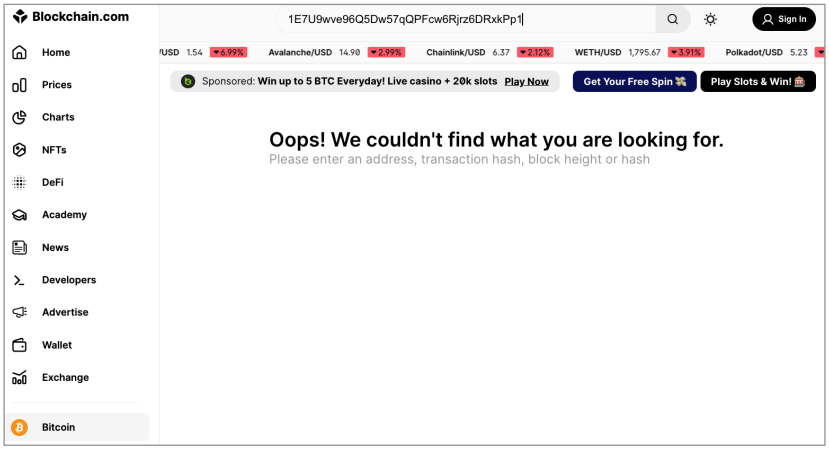
No	Wallet ID	Wallet Brand	Generated By	Generated Date

APPENDIX A
SAMPLE OF INVALID CRYPTOCURRENCY ADDRESSES

Ether Address: 0x004Cf65b315287fC064495Da288459208ef505aaa

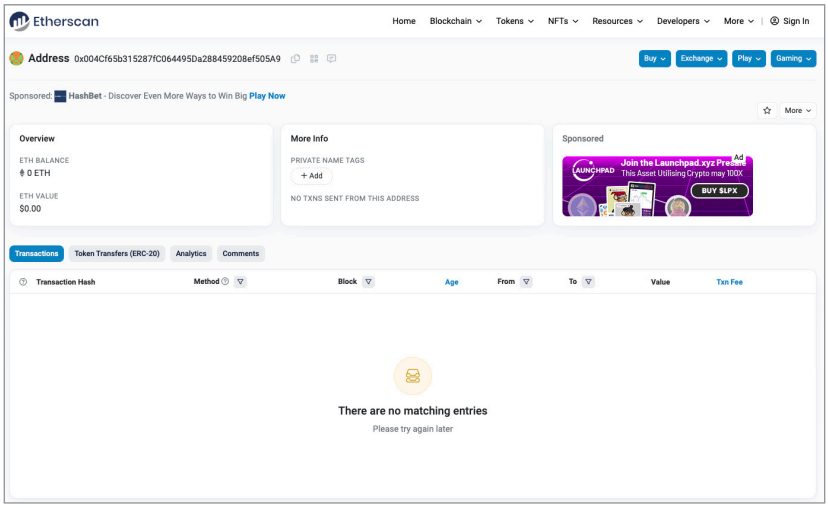


Bitcoin Address: 1E7U9wve96Q5Dw57qQPFcw6Rjrz6DRxkPp

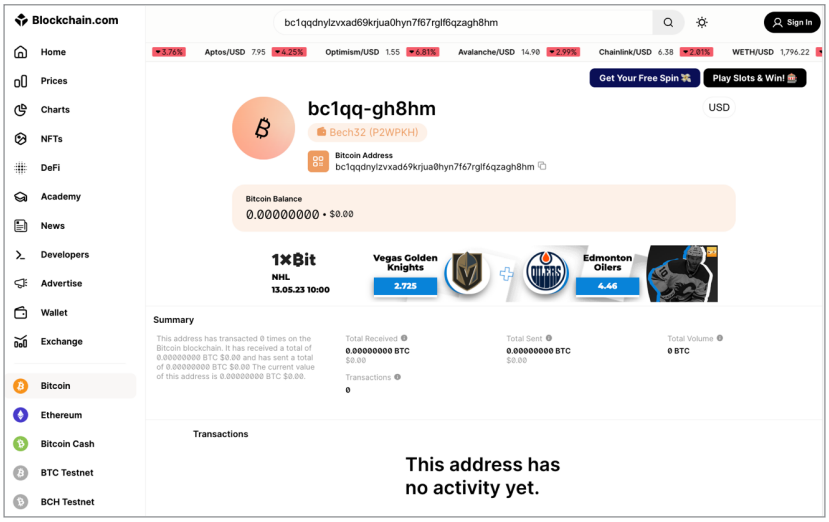


APPENDIX B
SAMPLE OF CRYPTOCURRENCY ADDRESSES WITHOUT TRANSACTION

Ether Address: 0x004Cf65b315287fC064495Da288459208ef505A9



Bitcoin Address: 1E7U9wve96Q5Dw57qQPFcw6Rjrz6DRxkPp



APPENDIX C
VARIOUS SAMPLES OF CRYPTOWALLET

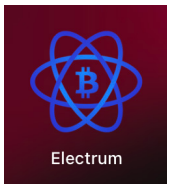
A. Hardware Wallet

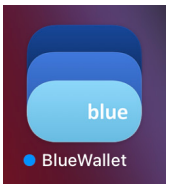
Ledger Nano

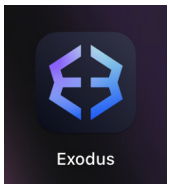
Trezor

KeepKey

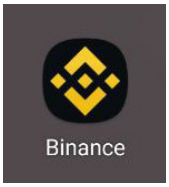
B. Desktop Wallet

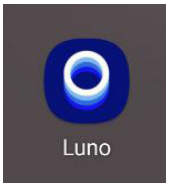




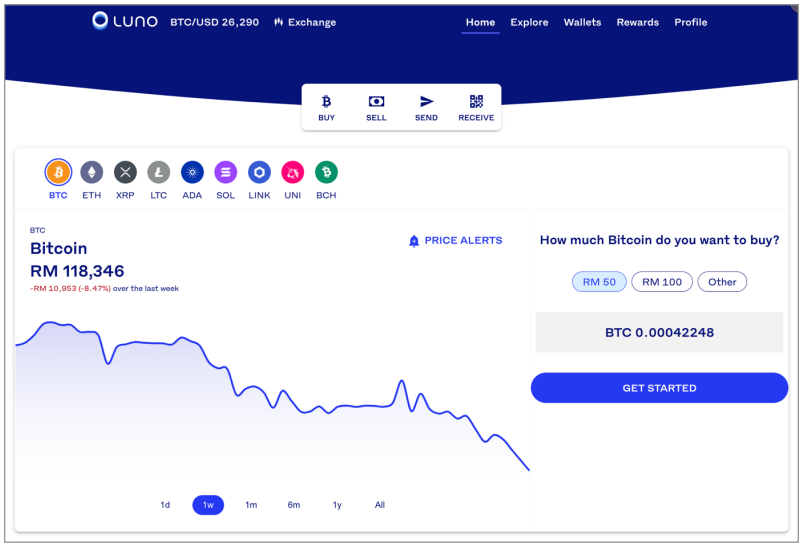


C. Mobile Wallet





D. Web Wallet



E. Paper Wallet

CyberSecurity
MALAYSIA