虛擬資產反洗錢白皮書
2022

ACAMS

台灣虛擬通貨反洗錢協會
Taiwan Virtual Asset Anti-money laundering Association

聲明

本白皮書所提供之信息僅供參考，無任何形式的保證或擔保。內容均不作為商業建議或正式法律意見，發起單位與聯合發布單位對本白皮書所含信息的準確性與完整性不承擔任何法律責任。

編撰團隊

臺灣虛擬通貨反洗錢協會

理事長 簡書永

副理事長 曹維傑律師

副理事長 彭少甫

理事 黃亞森律師

秘書長 蔣可元

秘書 蔡馥聰

特邀專家

林介山

Goethe-Universität Frankfurt am Main ILF LL.M.

特邀專家

公認反洗錢師協會(ACAMS)專家課題組

特別感謝

William Scott Grob, Director of Research & Analysis, ACAMS

序

自2008年中本聰（Satoshi Nakamoto）所發布論文《比特幣：一種對等式的電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System），並於隔年發布首個比特幣軟體，比特幣問世以來，從首次用於支付購買「披薩」，其後被用於「絲綢之路」、「AlphaBay」等暗網，作為不法犯罪的對價支付工具，從而國際間對於使用虛擬資產之相關犯罪偵測及降低風險措施，亦越加重視。

而對於虛擬資產的中英文名詞也數度更迭，從虛擬貨幣、加密貨幣、數字（位）貨幣，各式各樣不同的名詞，多方紛呈。直到臺灣於2018年11月7號修正《洗錢防制法》時，將其正式定名為「虛擬通貨」，然而近期《洗錢防制法草案》為順應防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering, FATF）之相關指引之用詞，故將虛擬資產（Virtual Asset）作為未來法規之正式用語，「虛擬通貨」也將更名為「虛擬資產」，從名詞上的更正，也令人十分期待接下來的法規調整與制定，想必是能更加完善且符合國際趨勢。

關於「虛擬資產究竟確實是有高度的洗錢風險？抑或僅係被外界扭曲之妖魔化？」一問，可以用近日喧囂塵上的烏俄戰爭作為一個例子，虛擬資產可用於資助烏克蘭政府對抗俄國的善款，但同時亦被俄國之制裁名單人士用以移轉資產，據此可知水能載舟亦能覆舟，**「虛擬資產就是一個中性的工具，端看使用者如何應用」**。

臺灣虛擬通貨反洗錢協會很榮幸在全球最大的反金融犯罪會員組織ACAMS公認反洗錢師協會[1]的邀請下，召集臺灣同時專精反洗錢及虛擬資產專業知識的專業人士，共譜臺灣虛擬通貨反洗錢白皮書，期待透過粗淺的虛擬資產反洗錢相關資訊分享，能收拋磚引玉之效，並為臺灣過往較付之闕如的虛擬資產反洗錢文獻增添一份色彩。同時能對於臺灣的虛擬資產服務提供者及相關法遵工作者作為具有參考價值的入門手冊，則本協會便已幸不辱命，達成成立之宗旨。

臺灣虛擬通貨反洗錢協會理事長　簡書永

2022年3月21日

1. ACAMS是全球最大的反金融犯罪會員組織，在180多個國家/地區擁有超過89,000名會員。CAMS被世界各地的監管機構、公共部門、私營部門認定為反洗錢能力認證的黃金標準，您可以訪問ACAMS網站acams.org瞭解更多關於我們的資訊。

目錄

第一章 前言暨虛擬資產服務提供者行業現況

自 2008 年中本聰（Satoshi Nakamoto）發布《比特幣：一種對等式的電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）一文以來，虛擬資產（Virtual Asset）以新興價值載體的面貌逐漸普及全球，對既有產業產生不小的衝擊。特別是對傳統金融監理體系的挑戰，使各國監理機構無不展開研究，並試圖作出規範控制，以調和新興科技發展之風險，其中就洗錢防制及打擊資恐的監理最為關鍵及迫切。

本文將先以防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering，以下簡稱FATF）對於虛擬資產服務提供者（Virtual Asset Service Providers, VASPs）之定義範疇來介紹虛擬資產服務提供者的行業現況；其次將分析利用虛擬資產施行洗錢前置犯罪的樣態與手法；接著會概覽虛擬資產的國際規範，並鳥瞰各國的監管趨勢；而後將以臺灣地區的虛擬資產反洗錢為核心，梳理現行法規的脈絡；隨後本文將提出虛擬資產產業之合規管理框架分析；最後也會對於虛擬資產的反洗錢為總結與未來展望。

FATF於2018年修改其建議書（The FATF Recommendations），將「虛擬資產」及「對於虛擬資產服務提供者」，納入洗錢防制範疇，該定義為各國所廣泛採用，其中「虛擬資產服務提供者」包含了從事下列活動為業者：虛擬資產與法定貨幣間之交換（exchange between virtual assets and fiat currencies）；虛擬資產間之交換（exchange between one or more forms of virtual assets）；進行虛擬資產之移轉（transfer of virtual assets）；保管、管理虛擬資產或提供相關管理工具（safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets）；以及參與及提供虛擬資產發行或銷售之相關金融服務（participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset）。

一、虛擬資產與法定貨幣間之交換

如於 2021年 4 月成為虛擬資產產業在美國首家上市的 Coinbase 交易所，提供美國用戶以美元購買比特幣等虛擬資產；又如臺灣的ACE王牌虛擬貨幣交易所（ACE Exchange），提供用戶新台幣與諸多虛擬資產之交易對，MaiCoin數位資產買賣平台提供新台幣對虛擬資產的代買代售服務，即為虛擬資產與法定貨幣間之交換業務。

二、虛擬資產間之交換

如被認為是全球最大的虛擬資產交易所，幣安交易所（Binance Exchange），提供了超過三百個幣種及一千對以上的交易對，且除了現貨交易，亦包含了合約及槓桿交易；又如交易量在全球前幾位的去中心化交易平台（Decentralized Exchange, DEX） Uniswap，不具有紀錄訂單的委託簿或中間人撮合買賣方的交易，而是利用自動做市商（Automated Market-Makers, AMM）的機制實現虛擬資產間之交換。

三、進行虛擬資產之移轉

如場外交易（Over-the-Counter, OTC）中相當著名的火幣全球平台（Huobi Global），於其平台提供用戶間點對點的虛擬資產交易，交易雙方將交易標的都轉入平台，由平台負責移轉給對方；又如隨著虛擬資產逐漸普及後，民間諸多自然人或法人協助客戶透過交易平台將虛擬資產移轉給另一客戶並賺取價差或佣金者，亦屬於進行虛擬資產之移轉。

四、保管、管理虛擬資產或提供相關管理工具

如歐洲加密資產管理公司CoinShares透過風險投資、股票投資、虛擬資產及借貸等方式滿足用戶的各種投資目標及策略，如比特幣對沖基金，以及以太幣計價的私募基金；又如鎖定東南亞和臺灣的虛擬資產投資平台Coinomo，由對傳統金融及虛擬資產都熟悉之團隊利用基於虛擬資產的期貨合約交易等策略為高資產、機構客戶及家族辦公室提供各類資產管理服務。

五、參與及提供虛擬資產發行或銷售之相關金融服務

如交易所FTX具有廣為人知的首次交易所發行（Initial Exchange Offering, 以下簡稱IEO）業務，FTX與虛擬資產發行方有代為發行承銷之約定，用戶於該平台上質押特定數量之平台幣FTT，即可依規則獲取參與抽籤及中籤後的分配資格；又如Templum Markets公司為證券型虛擬資產做代幣化資產發行（Tokenized Asset Offering, TAO），曾經承銷著名的渡假酒店The St. Regis Aspen Resort之普通股代幣化專案等。

第二章 虛擬資產洗錢及資恐之犯罪態樣

一、犯罪類型

(一) 詐欺

依據臺灣行政院洗錢防制辦公室出版的《2021年國家洗錢資恐及資武擴風險評估報告》指出，分析臺灣執法機關內政部刑事警察局近年偵辦案件，可辨識出五大虛擬資產犯罪態樣，其中以「詐欺」最為常見。

據前揭執法機關統計，自2020年1月起至2021年9月止，虛擬資產投資詐騙（包含假借虛擬資產名義之投資詐騙）案件數達5,281件，詐騙金額達新臺幣28億6,949萬2,365元。

1. 投資詐騙
   近年由於區塊鏈、Web3.0之興起，詐騙集團看準一般民眾不熟悉新興科技之專業名詞，往往假借「虛擬資產投資」，以龐氏騙局[2]手法利用「後金補前金」之方式吸金投資客購買虛擬資產後，旋即將其移轉到國外交易所，致使投資客血本無歸且求償無門。
2. 詐騙集團不法資金
   虛擬資產詐欺不僅限於投資詐騙（龐氏騙局），也可能藉由各種不同的手法（例如情感詐欺[3]）騙取受害人財產後，再將不法資金轉換為虛擬資產後，藉以混淆金流。

(二) 非法跨境匯兌

因各種理由，當無法經由正常金融體系匯款時，為閃避臺灣銀行法第29條非銀行不得辦理國內外匯兌業務之規範，肇因於虛擬資產可作為價值媒介之特性、其可輕易跨境移轉之特性，便成為犯罪集團作為跨境洗錢的工具，特別是泰達幣（Tether, USDT）此種美元穩定幣，大量被使用於臺灣或他國之移轉上。

(三) 博弈網站

博弈集團通常採取分工模式，會將總公司設於境外，而將客服、資管和電銷等據點設於臺灣，除了博弈網站會接受以虛擬資產的方式下注外，也會透過與幣商或非法虛擬資產交易所合作，將虛擬資產兌換為法償貨幣，將博弈公司的不法金流，傳至國外或是反向由國外至國內，達成實質上跨境匯兌的效果。

(四) 購買毒品、槍枝等違禁品

比特幣（Bitcoin, BTC）早期應用場景為暗網絲綢之路（Silk Road）[4]的支付工具，因此需求者便會透由暗網或國外網站上用比特幣或隱私幣（匿名幣），購買毒品、槍枝或其他違禁品（如假造之Covid 19疫苗護照或遭竊疫苗）[5]。

(五) 逃稅

為避免被國家課徵贈與稅、遺產稅或其他稅賦時，逃稅者就會選擇將資金轉換為虛擬資產後進行移轉，以躲避國稅局的追查。

2. 「龐氏騙局」稱謂源自美國一名義大利移民查爾斯·龐氏，他於1919年開始策劃一個陰謀，成立一空殼公司騙人向這個事實上子虛烏有的企業投資，許諾投資者將在三個月內得到40%的利潤回報，然後龐氏把新投資者的錢作為快速盈利付給最初投資的人，以誘使更多的人上當。由於前期投資的人回報豐厚，龐氏成功地在七個月內吸引了三萬名投資者，這場陰謀持續了一年之久才被戳破。龐氏騙局，載於**https://zh.wikipedia.org/wiki/%E9%BE%90%E6%B0%8F%E9%A8%99%E5%B1%80**（最後閱覽日：2022年02月26日）
3. 情感詐欺較為常見的手法是詐欺犯透由交友軟體認識受害者後，透由各種故事，說服受害者自願交付財物。
4. 絲路（Silk Road）是一個利用Tor的隱密服務來運作的黑市購物網站，Tor的服務保證了網站用戶的匿名性。
5. INVESTIGATION INSIGHT (2021, July 01). Fraudulent Covid Vaccination Certificates and Stolen Vaccines on Darknet Markets. Coinfirm. **https://www.coinfirm.com/blog/covid-vaccine-darknet-markets/**

（六）盜幣

多數常見的盜幣事件為駭客利用漏洞或其他方式入侵虛擬資產交易所盜取虛擬資產或該交易所員工監守自盜，之後將所竊得之虛擬資產，經由去中心化交易所或混幣商模糊幣流或形成幣流斷點，藉此達成清洗不法所得。

（七）資助恐怖份子

虛擬資產除了遭犯罪份子用於洗錢外，反極端主義項目（Counter Extremism Project, CEP）亦指出比特幣被惡名昭彰的伊斯蘭國（the Islamic State of Iraq and Syria, ISIS）透由社群媒體，以小額募資之方式，用於募集資金。

美國區塊鏈分析機構Chainalysis於其2022年虛擬資產犯罪報告分析指出[6]，北韓（朝鮮）政府因試射彈道飛彈而遭聯合國安理會等實施經濟制裁，為了籌措金源持續發展武力，不惜動用隸屬於偵查總局的駭客組織部隊「Lazarus Group」透過網路釣魚、惡意軟體（例如WannaCry）等駭取價值近4億美元規模的虛擬資產，存進北韓可動用的帳戶。

另依據臺灣行政院洗錢防制辦公室出版的2021年國家洗錢資恐及資武擴風險評估報告指出，聯合國安理會第1718號決議制裁委員會專家小組報告（S/2019/6）91觀察到，北韓廣泛且日益複雜地利用網路手段從世界各地的金融機構及虛擬資產交易所竊取資金、洗淨偷竊所得並產生收入，同時藉以規避金融制裁。類此手法的案例自2008年起在數量、複雜性及範圍上皆有增加，包括於2016年起明顯轉為以創造收入為重點，而對網路／虛擬資產服務提供者發動相關攻擊。此一轉變使北韓得以創造通常較難以追蹤且比傳統銀行部門受到較少監理之收入，據聯合國安理會專家小組2021年報告（S/2021/211） 80指出，自2019年至2020年11月，北韓行竊的虛擬資產總值已高達3.164億美元。

二、洗錢角色

（一）場外交易商

除一般市面上廣為人熟知的，可兌換法幣的虛擬資產交易所外，支撐起虛擬資產洗錢犯罪活動的重要角色就是場外交易商（Over-the-Counter，以下簡稱OTC商）。雖然目前並沒有任何一個針對OTC商的正式定義，但普遍對於其認知為，並非透由線上系統下單，即可自動買賣或搓合虛擬資產，而需透由線下面交的方式完成交易，即為OTC商。

有個常見的誤區是OTC商並不完全等同於「個人幣商」或「水商」，OTC商亦有成立公司以法人方式，進行正派經營者，並且進行一定程度的反洗錢措施。當然目前臺灣OTC商的組成最大宗的還是屬個人幣商，其往往與水商僅有一線之隔[7]，個人幣商在交易時向客戶所做的身分識別確認程序（Know Your Customer，以下簡稱KYC）往往只是為了避免後續因詐騙金流進入帳戶而發生警示帳戶、衍生性管制帳戶的問題，從而留存客戶資料，不僅沒有使用姓名檢核資料庫進行姓名檢核，更遑論交易監控或是進一步申報可疑交易。

（二）非法虛擬資產交易所

幣商通常會在可兌換法幣之虛擬資產交易所開戶來調節需求水位，因此往往會有配合的非法虛擬資產交易所與其合作。

（三）虛擬資產交易所人頭帳戶

詐騙集團騙取受害者資金後，會透過在虛擬資產交易所完成開戶之人頭帳戶購買虛擬資產後轉出到國外之虛擬資產交易所。

6. CHAINALYSIS TEAM (2022, January, 13). North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High. Chainalysis. https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/
7. 個人幣商並不會特別過問，也不知悉買賣幣背後的資金來源，對個人幣商而言就是單純的賣買虛擬資產予客戶；惟水商則是清楚知道買賣幣的來源係不法資金，而故意配合犯罪份子透由買賣虛擬資產來達到隱匿或模糊不法資金的效果。

（四）比特幣自動販賣機

犯罪份子將不法資金透過比特幣自動販賣機（Bitcoin ATM，以下簡稱BTM）轉為虛擬資產後轉至國外或未進行KYC之無法辨識的錢包地址。

（五）混幣商

因各類前置犯罪所生之虛擬資產，意欲移轉並模糊虛擬資產流向者，可透過混幣商（Mixer）造成區塊鏈上之幣流斷點，以逃避幣流追蹤系統的追查及識別。

（六）不法礦場

竊電之礦場或不法資金所投資之礦場[8]，所挖出之虛擬資產（俗稱挖礦[9]），因全新生成之虛擬資產，故無法透過幣流系統追查或標註之方式辨識其來源係不法資金。

（七）去中心化金融及非同質化代幣平台

去中心化金融（Decentralized Finance, 以下簡稱DeFi）或非同質化代幣（Non–Fungible Token，以下簡稱NFT）[10]平台如Uniswap、Compound或OpenSea，因所連結之未託管錢包，如常見的狐狸錢包（MetaMask），欠缺身分識別程序（非實名制錢包），因此極為容易成為洗錢的管道。

美國區塊鏈分析機構Chainalysis於其2022年虛擬資產犯罪報告分析指出，不法份子利用NFT平台未實名制之特性，除了以刷交易（Wash Trading）之方式，左手換右手墊高NFT價格，或以購入NFT作為移轉不法資金（諸如詐欺、制裁名單之資金）之洗錢手法。

8. 早年挖礦尚未普及時，便有不法份子透由投資礦場，將手上的不法資金轉換為虛擬資產。
9. 挖礦係指在驗證分散式帳本過程中完成驗算，進而獲得虛擬資產作為獎勵的過程。礦工（驗算者）必須加強自身的算力，才能與其他礦工搶奪「記帳權」獲得獎勵。
10. NFT是區塊鏈上的其中一種加密資產，具有唯一的標識碼和將它們彼此區分開來的元數據。與同質化代幣（例如比特幣、以太幣）不同之處在於，它們不能進行交易或等價交換。同質化代幣則因具有相同價值，因此十分容易作為商業交易（價值流通）的媒介。

第三章 虛擬資產之國際規範概述及各國監管趨勢

一、虛擬資產及服務提供者監管指引重點概述

(一) 前言

早於2018年10月FATF就首次變更其第十五項建議，並納入且定義虛擬資產及虛擬資產服務提供者的概念，要求VASPs均應遵循洗錢防制及打擊資恐之相關義務，直至2021年10月FATF更新2019年首次發布之虛擬資產及服務提供者監管指引予公、私部門參考。

(二) 重點摘要

1. 虛擬資產及虛擬資產服務提供者之定義

(1) 何謂虛擬資產？

FATF認為虛擬資產必須是數位化且能基於支付或投資之目的以數位化交易或傳輸[11]，其定義所涵蓋之範圍雖看似頗為廣泛，然而FATF也同時表示虛擬資產不能為僅係數位化之法幣、證券或其他金融資產，此種已為既有FATF準則中已涵蓋者。

此外FATF不打算令資產同時具有虛擬資產及金融資產之地位，如涉及可能同時符合之爭議時，權責機關應依其舊有管理金融資產之體系或虛擬資產體系採取適切地定位該數位資產。

其中關於NFT究係是否屬虛擬資產？一般來說依據NFT的特徵而言，此並非屬FATF定義下所稱之虛擬資產，然而重要的是必須考量該NFT之本質及其實際功能，不能僅依其用詞或行銷用字判斷。縱或表面上該NFT並非屬虛擬資產，然而系爭NFT被用於支付或投資目的時，仍應認其符合虛擬資產之定義。

(2) 何謂虛擬資產服務提供者

依據FATF詞彙表對虛擬資產服務提供者之定義係指任何未受FATF既有建議所涵蓋之自然人或法人，且作為業務執行下述一種或多種活動，抑或代表自然人或法人經營者亦屬之：

A. 虛擬資產與法償貨幣之間對交換。

B. 一種或多種虛擬資產之間交換。

C. 傳輸虛擬資產。

D. 保管且／或管理虛擬資產，或是得控制虛擬資產之工具。

E. 參與及提供，與發行人提供且／或銷售虛擬資產有關之金融服務。

此外FATF表示各國應依上述定義區辨究否屬虛擬資產服務提供者，不可僅依據企業自行採用的詞彙作為判斷依據。

其中DeFi是否為VASPs？雖然DeFi公司本身不是VASPs，惟在具控制權的情形下，縱似以去中心化之方式運行協議，其運營商、所有者和創建者仍可被定義為 VASPs，應遵循FATF準則。

2. FATF準則如何適用於所謂穩定幣（so-called stablecoins）

FATF認為穩定幣一詞並非一個明確的法律或科技類別，而主要為擁護此種幣別的人，所使用的一種市場用語。基此FATF於其G20的報告中，以「所謂穩定幣（so-called stablecoins）」作為用詞。而為符合一般用詞，本指引暫稱其為穩定幣（stablecoins），但並不表示支持其主張。

11. FATF對虛擬資產定義可參考2021年10月28號所發佈之FATF虛擬資產及監管指引詞彙表，原文如下：A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.
FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

穩定幣的發行者得為一個中心發行者或治理主體所組成，該主體可由一個或多個自然人或法人組成，從而設置相關的穩定幣協議規則。一般而言，此種中心化主體往往存在於穩定幣協議中，而認應屬FATF規範準則下的金融機構或VASPs，系爭主體應於開業或使用前執行全面風險評估以降低洗錢風險。

然而並非所有的穩定幣都會逕自被視為中心化主體，從而被認定為金融機構或VASPs，然而當無法輕易識別時，國家應考量其風險，並予以降低其風險的手段。

3. 提供指引予P2P交易洗錢及資恐之風險和工具

國家應透過下述方式，瞭解P2P交易（Peer-to-Peer Transaction）之風險，例如聯繫私部門（VASPs及P2P之代表）、訓練主管機關、金融情報機構（Financial Intelligence Unit, FIU）及執法部門、鼓勵發展發方法論或工具（如區塊鏈分析工具）藉此分析P2P市場及辨識可疑交易。

又降低P2P之降低手段風險，列舉如下：

(1) 促進P2P交易的可見度，例如制定P2P交易紀錄保存之相關規範。

(2) 提升VASPs業者對於未辨識之錢包交易之風險意識。

(3) 敦促VASPs僅與基於基礎風險方法論（Risk-Based Approach, RBA）考量下，可被接受者進行交易。

(4) 規範VASPs僅得與VASPs或合規企業交易，如欲與非合規業者進行交易，需加諸其他防制洗錢及打擊資恐（AML/CFT）之義務。

4. 提供更新指引予註冊及登記之VASPs

FATF建議國家應採取行動，針對從事虛擬資產活動卻未註冊或未取得執照的自然人或法人，進行識別並採取適當的制裁，且國家應指定有權之機關負責此事。縱然是選擇全面禁止虛擬資產及服務提供者的國家，亦應具備設置工具及有權機關負責進行辨識。

為能識別，現存尚未註冊或取得執照之虛擬資產服務提供者，FATF提供若干資訊來源及工具，臚列如下：

(1) 利用區塊鏈或其他相類似之分散式帳本分析工具進行調查。

(2) 由未註冊或未取得執照之企業所提供的瀏覽網頁或其他公開資訊（如宣傳廣告等社群媒體）。

(3) 由大眾或業界所提供之回饋目前市面上現存未註冊或未取得執照之企業。

(4) 由FIU或其他申報機構提供，例如從可疑交易申報（Suspicious Transaction Report, STR）中或調查過程中，可能透露出目前市面上現存未註冊或未取得執照之自然人或法人。

(5) 由非公開取得資訊，例如先前曾申請註冊或執照之企業，甚或是提出申請後撤回者。

(6) 由執法部門或情資報告，包含國際合作情報。

5. 提供指引予公私部門關於轉帳規則（以下簡稱Travel Rule）之施行

FATF認為應將虛擬資產傳輸視為電匯（Wire Transfers），因此國家應該將FATF第十六條轉帳規則建議，適用於虛擬服務提供商進行虛擬資產傳輸。此外，無論法幣或虛擬資產之交易都應適用之。惟交易手續費（Transaction Fees）並不在此適用範圍內，原因在於基於技術之理由虛擬資產服務提供者之傳輸方可能會匯出高於設定之數量，並於完成移轉後取得部分退款作為交易手續費，則於此情況下收到退款的虛擬資產服務提供者不會被認為是接收方，故不適用轉帳規則。[12]

6. VASPs之監管者間之資訊共享及合作原則

監管者於國際之間的合作應被鼓勵並應建立於互信之基礎關係之上，而資訊分享的協議應視給予個案彈性處理的空間。

12. 匯款手續費不適用於旅行規則的原因是匯款手續費退還給本人，則發送方與接收方均為同一人，因此無庸特別透過旅行規則辨識。

二、歐洲與日本虛擬資產反洗錢監管趨勢

（一）歐洲虛擬資產反洗錢監督趨勢

1. 歐洲政策制定者及其他國際組織對虛擬資產的態度

(1) 歐洲證券和市場管理局

2018年，歐洲證券和市場管理局（European Securities and Markets Authority, ESMA）與歐洲銀行管理局（European Banking Authority, EBA）和歐洲保險暨職業年金管理局（European Insurance and Occupational Pensions Authority, EIOPA）就虛擬資產向消費者發出警告。在他們發布的警告中，他們將虛擬資產定義為 「……一種既不由中央銀行或公共機構發行也不由其擔保且不具有貨幣或貨幣法律地位的價值的數字表示形式。」 它指出，虛擬資產之價格擁有高度波動，通常沒有任何有形資產支持，也沒有完全監管以致購買者受法律保護的程度。

(2) 歐洲銀行管理局

2014年，歐洲銀行管理局發布了關於虛擬資產的官方意見。該意見指出，「虛擬資產被定義為一種價值的數字表示，它既不是由中央銀行或機構發行，也不一定附屬於法定貨幣，但被自然人或法人用作交換手段，並且可以以電子方式傳輸、存儲或交易。」 它進一步解釋說，如果當局或銀行在背後支持虛擬資產，那麼應該被視為法定貨幣而不是虛擬資產。 此外，該意見亦警告了虛擬資產的洗錢和恐怖主義融資風險，強調了虛擬資產易於被犯罪分子或恐怖組織所利用，並不受國界或司法管轄地監管且具匿名轉移的能力。

(3) 世界銀行

世界銀行（World Bank）[13]在其觀點中獨樹一幟，將虛擬資產歸類為「依靠加密技術達成共識的數字貨幣的子集，例如比特幣和以太幣。」雖然在定義虛擬資產的特徵方面略有不同，但世界銀行依舊還是提醒用戶注意，要使虛擬資產和分散式帳本技術完全集成到金融系統中，完全的遵守「客戶盡職調查」規則的義務乃至關重要。

(4) 國際貨幣基金組織

2016年1月，國際貨幣基金組織（International Monetary Fund，以下簡稱IMF）[14]發布了一份工作人員討論筆記，其中將虛擬資產定義為「由私人開發商發行並以他們自己的記賬單位計價的數字價值表現形式」。與歐洲央行的觀點類似，它還補充說，由於還沒有對虛擬資產的通用定義，隨著系統的迅速變化，定義也將被修改以更好地建立完善的定義。它還意識到監管部門對全面監管業務的挑戰，表明由於虛擬資產特性的許多濫用，存在洗錢和恐怖主義資助風險。此份筆記更進一步表明，監管應超越傳統監管金融部門的「看門人」。隨著點對點交易的增加，有關虛擬資產的法規應包括更廣泛的市場參與者，以適應不斷發展的技術。

2. 第4號和第5號反洗錢指令對虛擬資產之規定

繼《第3號反洗錢指令》，經過近十年後，《第4號反洗錢指令》於2015年5月20日被引入歐盟，其主要重點是提高受監管實體的所有權之透明度。新指令對於擴大有義務實體與金融機構遵守法規的範圍方面具有決定性作用；添加的實體包含了「特定非金融事業與專業人士」（Designated Nonfinancial Business and Professions，以下簡稱 DNFBP） 的集合，它們將被要求遵守指令中規定的認識您的客戶、客戶盡職調查和其他各種義務。在擴大指令中義務實體的分類的同時，它還擴大了義務實體的「風險基礎方法」的概念，不僅考慮了公司與之開展業務的客戶類型，還考慮了「地理區域和特定產品、服務、交易或交付渠道」。

在對「增強盡職調查」和「重要政治性職務之人」等術語的許多其他修訂和修改中，最值得注意的是，《第4號反洗錢指令》是第一個引入有關電子貨幣法規的指令。 儘管對進行客戶盡職調查有免

13. 世界銀行（World Bank）為開發中國家資本項目提供貸款的聯合國系統國際金融機構。是世界銀行集團的組成機構之一，同時也是聯合國發展集團（United Nations Sustainable Development Group, UNDG）的成員。載於：https://zh.wikipedia.org/wiki/%E4%B8%96%E7%95%8C%E9%93%B6%E8%A1%8C（最後閱覽日：2022年02月26日）
14. 國際貨幣基金組織於1945年12月27日成立，屬於聯合國經濟及社會理事會（Economic and Social Council, ECOSOC）下屬的專門機構，與世界銀行同為世界兩大金融機構，由189個國家組成，致力於促進全球貨幣合作，確保金融穩定，促進國際貿易。載於：https://zh.wikipedia.org/wiki/%E5%9C%8B%E9%9A%9B%E8%B2%A8%E5%B9%A3%E5%9F%BA%E9%87%91%E7%B5%84%E7%B9%94（最後閱覽日：2022年02月26日）

除條件（以電子方式存儲的最大金額不超過250歐元），但該指令承認當時電子貨幣正日益成為銀行賬戶的替代品，因此應包括在內，以防止洗錢或恐怖主義資助風險。然而，準確來說，《第4號反洗錢指令》中包含的電子貨幣不應與虛擬資產相混淆。由於指令第3(2)(a)條規範將「貨幣兌換處」定義為應被視為義務實體的金融機構，一些專家認為這適用於虛擬資產交易所和提供虛擬資產兌換服務的平台。這一論點並未得到廣泛認可，僅僅是因為《第4號反洗錢指令》中規定的DNFBP不包括特定虛擬資產市場參與者，因此不應誤認為它將虛擬資產納入指令的範圍。因此，為了應對由虛擬資產導致的洗錢和恐怖主義資助問題，《第5號反洗錢指令》於2018年7月9日生效。

毫無疑問，《第5號反洗錢指令》是過去指令中針對虛擬資產最初與最重要的指令，它是同類中第一個提供虛擬資產的法律定義並收緊其市場參與者的繩索。在《第4號反洗錢指令》頒布後的一年內，歐盟委員會開始起草新指令作為其繼任者。在2015年巴黎恐怖攻擊事件和2017年倫敦橋襲擊事件之後，新指令的主要重點乃限制與杜絕恐怖分子所擁有的財務管道。這包括降低預付卡限額，以及擴大《第4號反洗錢指令》已規定之高價值商品和其受益所有權。 然而，這裡討論的主要焦點是《第5號反洗錢指令》將虛擬資產納入反洗錢指令規範的領域。

在《第5號反洗錢指令》第3(d)條規範中，虛擬資產被定義為「非中央銀行或公共機構發行或擔保價值的數字表示形式，不一定附屬於合法建立的貨幣，不具有貨幣或貨幣的法律地位，但被自然人或法人接受為一種交換手段，可以通過電子方式轉移、存儲和交易。」 該指令還明確指出，虛擬資產不應與電子貨幣或「電動遊戲貨幣」混淆，其用途僅限於其周圍環境，例如特定種類遊戲貨幣在某個遊戲世界中有辦法使用。最顯著的區別是，除了作為支付手段之外，虛擬資產還可以用於投資或價值儲存。在《第5號反洗錢指令》範圍內給虛擬資產一個法律定義顯然不足以對市場產生影響，因此該指令決定首先將虛擬資產市場的兩個主要參與者視為義務實體，須首當其中的遵守其所訂定之相關規定。這兩個實體包括「虛擬資產交易所」和「託管錢包供應商」。通過監管作為虛擬資產市場供應商和買賣雙方聯合體的虛擬資產交易所，這將大大降低洗錢和恐怖主義資助風險，並過約束他們執行認識您的客戶、客戶盡職調查和可疑活動報告。此外，這些虛擬資產服務提供者被要求在當地金融機構從事註冊，從而提高其交易的透明度和作為義務實體的責任。

如前所述，錢包提供商的存在包括多種選擇，包括熱錢包提供商、冷錢包提供商和託管錢包提供商。 該指令針對託管錢包提供商進行監管的主要原因是，冷件錢包提供商是利用與硬碟鏈接的軟體應用程序來存儲每個用戶的私鑰的技術服務提供商，而託管錢包提供商則是擁有用戶的公鑰和私鑰。理論而言，這一特徵類似於為其客戶持有支付和銀行賬戶的金融機構，因此應該更傾向於受到監管。

除了將虛擬資產交易所和託管錢包提供商作為《第5號反洗錢指令》下的義務實體外，亦增加了一項額外的措施，用以針對虛擬資產所具之匿名風險特性。該指令規定，每個會員國之FIU都應該要具備能夠準確取得虛擬資產交易地址來往之信息，用以識別虛擬資產交易雙方之身分。作為打擊虛擬資產匿名性的另一種方式，該指令更是提出用戶自願登記的概念，然由於需要進一步評估此項提案，至今尚未正式強制施行。這些新加入的法規進一步使虛擬資產邁向合法化，並對於區分一般投資者和那些試圖利用其進行洗錢或恐怖主義資助而濫用系統的人有一大步的前進。

3. 第5號反洗錢指令後對歐盟和德國虛擬資產市場的影響

《第5號反洗錢指令》的實施是在監管虛擬資產的同時努力維持市場協調的一大步。因此，顯而易見的困境是在隱私與監管之間是否能取得平衡。創新總是伴隨著相對的代價，在完全遵守指令的過程將意味著各義務實體必須針對其架構或是現在應用的技術有所調整，這一切將導致虛擬資產相關實體營運的成本上升。值得注意的是，單一處理比特幣交易的較知名虛擬資產服務提供者之一Deribit宣布將總部從荷蘭遷至巴拿馬。Deribit認為荷蘭將內國法化更嚴格版本的《第5號反洗錢指令》。這違背了Deribit對虛擬資產長期保有之看法，認為虛擬資產應該「免費」提供給每個客戶。若是通過遵守指令的監管標準，對於大部分用戶來說是無法接受之情形，且他們本身並不願意承擔此額外之成本。

身為歐盟的領頭羊，德國一直以身作則，將歷任歐盟指令迅速地內國法化。2019年5月20日，德國聯邦財政部（Bundesfinanzministerium）公佈了其實施《第5號反洗錢指令》的法案（Regierungsentwurf），該法案將修改Geldwäschegesetz（德國反洗錢法，簡稱GwG）中的一些

條文和Kreditwesengesetz（德國銀行法，簡稱KWG），將指令中確定之新監管義務實體的職責包括在內。KWG將虛擬資產（Kryptowerte）定義為「尚未發行且具價值的數字表示或由任何中央銀行或公共機構擔保，不具有貨幣或貨幣的法律地位，但被自然人或法人根據協議或實務上接受為交換或支付手段，或用於投資目的並且能以電子方式傳輸、存儲和交易。」這項改變使虛擬資產服務提供者與德國原有之金融商品受到相同之法律規範。

4. 第6號反洗錢指令和Markets in Crypto–Assets Regulation（MiCA）

《第6號反洗錢指令》的實施截止日期訂於2020年12月3日。繼《第5號反洗錢指令》之後，不僅擴大了對於「犯罪活動」的定義，且更是擴大了根據該指令可能受到懲罰的人員範圍。新指令列出了22項構成犯罪活動的罪行，最高刑責可判刑1至4年。此外，法人亦可被列為被告，對於法人所進行之制裁，包括從取消公共募資資格、司法監督、清盤令和勒令停業。 該指令確立的另一項重要調整乃將「協助和教唆、企圖、煽動」洗錢或恐怖主義資助納入刑事罪責。該指令亦呼籲成員國在橫跨多個司法管轄區的犯罪發生時彼此應主動合作，同時列出在決定何成員國具管轄權時可以參考之要件。

歐盟委員會於2020年9月24日推出了新的《金融包裹法案》（Digital Finance Package），其中包括有關虛擬資產、數位運營韌性和零售支付策略的法規提案。在虛擬資產領域，此法案對於虛擬資產市場監管預計將建立一個框架，允許虛擬資產繼續創新，同時保護金融穩定和其相關投資者。目前，Markets in Crypto–Assets Regulation（以下簡稱MiCA）仍處於歐洲議會的一讀階段，預計在未來四年內實施。該法規旨在為歐盟提供針對單一市場內所有用戶和提供商的系統性規則，旨在規範所有可以通過分散式帳本技術轉移或保留的價值和權利的數位表示。這有望進一步涵蓋尚未在第2號金融工具市場指令和歐盟電子貨幣指令中作為金融工具監管的虛擬資產。與反洗錢指令相比，MiCA並沒有準確地針對洗錢或恐怖主義資助訂定新法律，但在其Consideration (8)中特別提到，此立法在試圖涵蓋現有指令和法規中遺漏虛擬資產的同時，「也應有助於打擊洗錢和恐怖主義資助」。從監管機構的角度來看，這將是進一步穩定歐盟金融市場上虛擬資產的一個新指標。該法規是否會因全面性規範而有效遏止洗錢和恐怖主義資助而帶來重大影響仍有待評估。因為在四年內，虛擬資產市場可能與現在大為不同。因此，根據反洗錢指令，持續之監控和分析虛擬資產如何運用於洗錢和恐怖主義資助時的方式並快速有效地立法，才是實務上最具效率的方式。

（二）日本虛擬資產反洗錢監管趨勢

1. 前言

與其他國家經營虛擬通貨交易所不需要牌照，日本由於早期全球最大的比特幣交易所Mt.Gox於日本倒閉，引起一波日本社會輿論之討論，故日本政府於2016年即修改其支付法令[15]，並新增一「虛擬通貨交易所」章節並於2017年實施，從而經營虛擬通貨交易所必須要有持有一「虛擬通貨交易所」之牌照，並針對何謂虛擬通貨交換作出定義，說明該等業者有消費者保護義務及依據日本防制洗錢法規[16]，指定該等業者應遵守防制洗錢之義務。

而後有鑒於Initial Coin Offering（以下簡稱ICO）[17]之蓬勃發展下所產生涉及金融法令解釋疑義和詐欺、詐騙等情事發生，包含相關衍生性虛擬通貨商品之出現，日本政府更進一步要求有提供與虛擬通貨相關衍生性服務（槓桿交易、期貨等）應該要再額外申請衍生性之金融牌照，並配合產業變化修法並闡明錢包託管業者也屬於「虛擬通貨業」，並配合國際FATF反洗錢組織Crypto Asset之稱呼，改虛擬通貨（仮想通貨）為密碼資產（暗号資産）[18]（以下虛擬通貨將以密碼資產稱呼之）。

於日本經營密碼資產產業應先取得密碼資產交換業之牌照，除防制洗錢義務外，尚有相關之法規遵循義務，如包含消費者保護、用戶及交易所財產分別保管、廣告勸誘、系統穩定性、內稽內控、洗錢防制及資訊安全等相關要求，而為方便業者理解法條要求之內容及實際操作方便，日本金融廳則有針對該業者的內部經營和相關法遵釋出指引（事務ガイドライン第三分冊：金融会社関係）[19]，業者多會根據該指引去思考並建構相關制度。

15. 即日本的《資金結算法》（資金決済に関する法律），該法一般來說被理解為日本的支付法，相當於臺灣電子支付、第三方支付、禮券綜合的統整法規。
16. 日本的《犯罪收益移轉防止法》（犯罪による収益の移転防止に関する法律）。
17. 指2017年所出現大量之區塊鏈專案或是計畫項目，透過以群眾募資的方式，說明收受以太幣或是比特幣等流通性較高之密碼資產，而透過智能合約或是網站去販售或交換特定區塊鏈專案或計畫項目下所設計的代幣（token）或密碼資產。
18. 臺灣實務用語仍多以「虛擬通貨」稱呼之，但為配合日本政府之修正，故以下將以「密碼資產」之用語稱呼之。
19. 密碼資產相關業者指引，載於https://www.fsa.go.jp/policy/virtual_currency/index_2.html （最後閱覽日：2022年02月26日）

除此之外，日本亦有針對密碼資產下所衍生的交易，要求提供者應取得衍生性交易業者之金融牌照，並有針對因應ICO活動下產生具證券性質的Token進行規範，即證券型代幣發行（Securities Token Offering，以下簡稱STO）制訂出相關規範，並創設一「電子記錄移轉權利」作為STO之文字敘述納入規範，業者經營相關業務應取得金融牌照，從而納入金融法體制下，而有相應之防制洗錢義務 ，而本文主要則針對密碼資產交換業者之防制洗錢義務進行說明。

承前所述，由於法規監理要求，日本密碼資產交換業者應設立相關自律組織進行自我規範，業者們亦於2018年成立其自律組織並設立許多規範要求自律組織會員遵循，於防制洗錢之部分則針對「密碼資產交換業者」制訂出「密碼資產交換業者之反洗錢及資恐遵循指引 （暗号資産交換業に係るマネー・ローンダリング及びテロ資金供与対策に関する規則・ガイドライン）」[20]，反映法規要求其一些具體之說明，以利相關密碼資產交換業者遵循，最新一版為2021年12月1日更新。

故日本於判斷誰為密碼資產之防制洗錢之適用主體，則是先回歸到其支付法《資金結算法》下密碼資產交換業者之定義判斷，從而確定義務主體。除了外部法規規範外，尚能透過密碼資產交換業者自律組織之相關實務指引，作為理解日本密碼資產交換業者實務上係如何遵守密碼資產之防制洗錢義務：

2.「密碼資產」及「密碼資產交換業」之定義

(1) 密碼資產之定義

「密碼資產」之定義分為兩種層次之定義，一種為正面定義，另一種則為補充定義。

其中第一層之正面定義如下：「於收受商品或服務時，基於債務清償之目的，而能對不特定人使用，並且得從不特定人處買入或賣給不特定人，且其移轉主要是透過電子訊息處理組織之方式為移轉，而具備一定財產價值者而言（惟該財產價值限於以電子機器或相類似之形式進行紀錄，且非以法償貨幣為其計價單位或背後有一法償貨幣做擔保）」。

從日本的定義來看，可以發現日本法令上承認其得以作為一種獨立於法幣價值系統以外的支付工具地位，並嘗試針對使用範圍以及其流動性進行抽象文字之規範，而所謂的電子訊息處理組織之方式則是針對區塊鏈技術所作出之文字規範，不過考量到技術之日新月異，故不明言必須為區塊鏈技術，而以電子訊息處理組織之方式稱之[21]。

此外，為避免正面定義無法涵蓋部分其他密碼資產，故而針對說無法直接透過法幣買到之密碼資產，但能與前述第一層次的密碼資產交換，且亦能透過電子訊息處理組織之方式移轉者，亦為這邊所說之密碼資產交換業者。

(2) 密碼資產交換業

所謂的「密碼資產交換業」則是指進行以下行為的業者：

A. 協助密碼資產的買賣或與其他密碼資產交換。

B. 作為前項行為的媒合、行紀或代理之角色。

C. 基於前2項行為之關係，為使用者管理金錢者。

D. 為他人保管密碼資產者。

而其中就「為他人保管密碼資產」，依據金融廳之相關指引解釋[22]，其中最主要的判斷重點在於「是否可以不須用戶授權或同意，即得透過保管者自行發起交易移轉該密碼資產 」，縱然是採用所謂的私鑰分片或分散儲存，若還是可以不用透過用戶即可進行移轉，則縱然分片仍可能會若入此處「為他人保管」之定義範圍中。

因此，從上述之定義可以得之日本在定義上已能涵蓋FATF中的VASPs定義，而涉及參與及提供密碼資產之相關金融服務者，則落入既有金融業法中管理，從而也有相關防制洗錢之義務。

3. 密碼資產之防制洗錢義務遵循

依據日本密碼資產交換業者自律組織之相關指引，於防制洗錢規範上，可以發現其規範上較著重之

20. 密碼資產交換業者相關之洗錢暨資恐相應對策之規則，載於https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/B14_jvcea202112.pdf（最後閱覽日：2022年02月26日）
21. 如IOTA之Tangle技術即不一定必須存在區塊鏈，而為一無區塊鏈（Blockchainless）的技術系統，而為DAG（Directed Acyclic Graph，有向無環圖）。
22. 同註13。

部分，該規範分為以下幾個章節：

(1) 總則：目的、風險基礎方法、防制洗錢法令遵循。

(2) 風險管理：風險的確定、評價、利用者風險評價、風險控制。

(3) 使用者管理：使用者業務關係建立之政策、可信賴證明文件、使用者姓名及交易監控、使用者風險評級及管理、使用者資訊之持續更新、交易對象之管理、交易之拒絕。

(4) 交易之確認義務：一般及特別狀況下之處理措施、高風險下之處理措施、KYC確認時點。

(5) 身分及交易紀錄：記錄的作成和保存、其他資料之保存

(6) 可疑交易：可疑交易之判斷、通報、管理。

(7) 業務制度：內控制度之建立、被害者救濟、內規建立、資訊搜尋資料庫、IT系統活用、資料管理。

(8) 體制：經營階層、第1、2線之管理、內控的實施、PDCA、外部委託規範等。

日本前述的自律組織之指引，如同FATF要求一樣，要求洗錢防制之遵循應採用所謂的風險基礎方式，且必要時應採取相關之控制措施以降低風險的可能性。只是於該指引中另有特別針對業者該如何特定風險做出較詳細的要求，如應該依據處理的密碼資產本身進行評級，並包含交易型態、國家地區、使用者屬性進行判斷，並說明說若有新的密碼資產或是採用新的技術進行交易，這都應該先進行風險評估包含提供方、合作方、委託方等進行思考，並應嘗試做出定量之分析指標。於風險的評價上，亦要求說應定期檢視風險，並且依據交易型態、國家地區、使用者屬性等細分化風險，並再次整合風險，評估整體風險，使風險可視化等等。

此外，針對KYC之部分也有要求應該針對使用者的職業及內容、經歷、收入及居住地、買入的密碼資產、使用之服務及交易型態進行了解，且本人之確認及交易目的應有相關佐證。並且應該適當進行定期的監控和掃描，並且在KYC之時點上，除了建立業務關係時應該進行KYC外，於臨時性交易時，針對密碼資產之交換或是受使用者要求移轉密碼資產時，超過10萬日圓，則應該對其進行KYC，且相關KYC調查所取得之證據亦應保存一定期間，對於高風險者則應保存7年。

而於內部控制，則要求應該採用PDCA之原則（Plan–Do–Check–Act）設計，並且應對員工進行訓練及培養，且應該有第1及第2道防線之機制設立，並且應導入資訊搜索系統，協助監測各項交易、姓名及風險之檢測等等，並應該做成相關之SOP以因應防制洗錢之相關規範要求。

4. 結論

日本比起其他國家來說，經營其密碼資產交換業，實際上有更多的義務存在，主要是導因於其發展歷史上有多次交易所倒閉或消費者資產被竊之情形，故而其很早就有相關監理存在，並要求取得一定之牌照。而在防制洗錢義務上，於2018年即開始納入法規實施，除了透過日本的犯罪收益移轉防止法之防制洗錢法規規範外，也透過業者間之自律組織和針對不同涉及金融的交易型態設立清楚的定義劃分，將不同形態和業者納入防制洗錢之防護網內，透過外部法規和業者內部自律規則之要求，強化防制洗錢義務之落實。

自律組織於防制洗錢起到之效益，則如過去日本交易所早期有針對說是否要上架所謂的「匿名幣」[23]進行討論，所謂的匿名幣是可以隱藏鏈上的交易地址和交易發起地址，從而使得追蹤記錄更困難之密碼資產，不同於比特幣或是以太幣等區塊鏈網路上得以被追蹤交易紀錄之區塊鏈。日本密碼資產之業者，即透過自律組織協議，要求會員應詳細考慮不上架可能被用於犯罪高度關聯之密碼資產，若要上架該等幣別，應採取相關措施降低追查困難度，若無法解決或無相關措施存在，則不應上架該等密碼資產，以避免難以落實防制洗錢之相關義務[24]。

23. 如Zcash、Monero等。
24. 第4條（應審慎處理判斷的密碼資產），載於**https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/B03_jvcea20200925.pdf**（最後閱覽日：2022年02月26日）

第四章　臺灣虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法簡介及實務運作初探

一、前言

臺灣於2018年修正洗錢防制法，首將VASPs納入規範，要求該等事業建立洗錢防制以及打擊資助恐怖主義（以下簡稱防制洗錢及打擊資恐）制度，包含內部控制制度、稽核制度、客戶身分確認、紀錄保存、疑似洗錢或資恐交易申報等事項，並指定金融監督管理委員會（以下簡稱金管會）為VASPs之防制洗錢及打擊資恐之主管機關。據此，金管會依據上開法令之授權，於2021年6月30日發佈《虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法》（以下簡稱本辦法），規範VASPs建立防制洗錢及打擊資恐之各項制度及細節，並於同年9月30日要求在國內設立登記之VASPs出具洗錢防制法令遵循聲明文件，至遲於須在11月底完成；並且應於2022年6月底前完成「防制洗錢及打擊資恐內部控制與稽核制度檢查表」，並由會計師事務所查核，始可謂完成相關法令遵循。至此，臺灣正式將虛擬資產納入反洗錢及打擊恐資之一環，有其重要性。本文在此擬介紹上開辦法之相關內容，並初步說明各項制度之設立重點，如有實務上可能觸及之問題或模糊地帶，亦將併予說明。

二、臺灣防制洗錢及打擊資恐之制度建立

(一)　適用主體

欲探討各項制度之建立，首應確認者乃在於本辦法之適用範圍，釐清哪些主體應遵守本辦法之義務。依本辦法第2條第1項之規定訂了五種事業，會被金管會認定為虛擬通貨平台及交易業務事業，在此說明如下：

1. 虛擬通貨與新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣間之交換：

   此種類型之業者，多數是指提供法幣入金以及出金之VASPs，且此處之法幣，不限於新台幣，包含任何外國政府或區域所通行之法幣且用以交換虛擬資產，均屬之。

2. 虛擬通貨間之交換：

   此處即所謂之幣幣交易而言，即任何虛擬通貨間之互相交換均屬之。依目前各個VASPs內，所提供不同虛擬資產交易對之之交換，縱然該VASPs為提供法幣入出金服務，亦不能脫免此之義務，均須符合本辦法所賦予之各項義務，認識客戶、風險評估、交易監控等。

3. 進行虛擬通貨之移轉：

   此處所指乃是協助客戶進行虛擬通貨之移轉服務，包含在不同VASPs之間之轉移，或協助用戶將虛擬通貨移轉之冷錢包，或移轉予用戶所指定之人。

4. 保管、管理虛擬通貨或提供相關管理工具：

   此處之相關管理工具，乃是指提供託管技術工具之業者，且於立法理由中明確表示，此類業者同時也包含為客戶保管私鑰，換言之，如未保管私鑰者，例如冷錢包業者，即毋庸進行本辦法所賦予之防制洗錢及打擊資恐義務。

5. 參與及提供虛擬通貨發行或銷售之相關金融服務：

   此處於立法理由明示，所謂相關金融服務即虛擬通之承銷等行為，諸如常見的ICO、STO、IEO等業者，或協助進行造市之業者，均屬之。

以上本辦法所定之五大類別，其範疇實為廣泛，實已涵蓋諸多現行常見的產業活動，且產業常見哪些業者需要遵守反洗錢以及打擊資恐義務的適用爭議解決，諸如幣幣交易、ICO等，均須本辦法中加以規範，以杜爭議。惟因虛擬資產此一產業之變化迅速，即有新的適用疑義，說明如下：

1. NFT是否需要執行防制洗錢及打擊資恐義務？

有關於NFT，即所謂的「非同質化代幣」，是建立區塊鏈上程式碼，能用智能合約（Smart Contract）自動執行協議，具有不可替代、不可分割及獨一無二的特性。而於本辦法中其用語為「虛擬資產」，究竟NFT是否可為本辦法所稱之虛擬資產所涵蓋，即有疑義。

FATF於2021年10月28日發布之最新加密監管指南，即提到NFT原則上應不符合FATF對於虛擬資產之定義，但如果NFT在運作過程中用於支付或投資，則可能又落入該組織對於虛擬資產之定義，進而提供NFT應用之各種服務提供商，諸如服務提供者、發行方等均負有遵守防制洗錢及打擊資恐之義務，是以FATF 建議採用個案判斷之方式，加以定調個案中之NFT用於支付或投資。

而以目前實務上有關於NFT之運作，時常可以看到某些NFT之價值動輒數百萬台幣，並且在各大平台諸如OpenSea、Rarible、Nifty Gateway等均可見NFT交易，殊難想像NFT不具有投資價值，故多數提供這類交易之服務提供者，實應遵守防制洗錢及打擊資恐之各項義務。

臺灣法務部於2021年12月28日公告《洗錢防制法修正草案》（以下簡稱修法草案），草案將原有之「虛擬通貨」作為立法用語，調整為「虛擬資產以及虛擬資產服務提供者」，而使反洗錢義務可更精準涵蓋所有虛擬資產服務提供者，包含NFT業者，或許可據此將NFT交易亦納入防制洗錢及打擊資恐之義務中。惟如欲更加清楚，則或可於本辦法中明揭NFT亦應遵守相關防制洗錢及打擊資恐義務。

2. DeFi是否需要執行防制洗錢及打擊資恐義務？

有關於DeFi為Decentralized Finance之縮寫，即「去中心化金融」，相關於傳統應用上都是由中心化實體提出服務，監管上針對這些中心化業者進行管理較為直接方便。但在DeFi中，則無中心化業者之概念，是一種建立於將程式碼部署於區塊鏈上之金融，例如DEX、P2P借貸、期貨、槓桿交易等，不依賴任何中心化之券商、交易所或銀行等機構提供金融工具，而是利用區塊鏈上的智慧型合約（例如以太坊）進行，並以虛擬通貨進行金融活動。

由於DeFi形式上不若傳統中心化金融，由中介機構進行推出各項金融商品服務，而可賦予此等中介機構執行相關義務。DeFi等金融商品之智能合約一經部署於區塊鏈上後，即自行運作。使用者只要透過自身之加密錢包與智能合約互動即可開始進行各項投資，中間亦無任何中介機構進行任何防制洗錢及打擊資恐之作為。

實則，各項於區塊鏈上之DeFi智能合約，雖號稱去中心化未有人對之進行管理運作，惟其背後多數都有運營團隊對之進行維運，甚或是宣傳行銷，例如多數的DEX背後都有團隊在進行管理行銷等。然也因此，去中心化金融容易成為以去中心化之名義推出各項中心化之金融服務，卻可以規避中心化金融之監管義務，例如防制洗錢及打擊資恐，此即為漏洞。

於前所述2021年10月28日發布之最新加密監管指南亦有針對DeFi之運作明確表示，DeFi此一產業並未完全排除在防制洗錢及打擊資恐義務之外，並且在某些情況下，例如該DeFi之創造者、所有者、營運團隊或任何保持對DeFi有安排且有控制或足夠影響力之人，也可能被視為VASPs，藉此將DeFi亦納入防制洗錢及打擊資恐之義務中。

臺灣對此並未有明確之表示，是否本辦法第2條第1項所列之各種主體，即可涵蓋DeFi業者？然DeFi既然部署在區塊鏈上，究應尋求何人或者何機構、單位負擔相關義務，在實務運作上恐有模糊地帶。或許可參考前述FATF之認定標準，具體個案判斷究竟何人有影響力而為適用主體，較為妥適。

（二）各項管控

1. 內部控制制度之建立

(1) 規範內容及其目的

為強化臺灣防制洗錢與打擊資恐機制，並健全VASPs內部防制洗錢及打擊資恐之管控，臺灣於本辦法第15條規定，虛擬通貨業者之防制洗錢及打擊資恐風險控管機制，應包括建立辨識、衡量與監控洗錢及資恐風險之管理機制，及遵循防制洗錢及打擊資恐相關法令之政策以及標準作業程序，以降低其洗錢及資恐之風險。

(2) 建立重點

為建立虛擬通貨業者完善落實內部控制制度之建立，首應先行制定相關洗錢與資恐風險管理政策。政策之重要性，猶如國家憲法之位階相同，乃是屬於不可牴觸相違背，各公司內部之防制洗錢及打擊資恐政策為公司在反洗錢以及打擊資恐領域中最高位階之規範，公司內部之各項程序錯失，或其他輔助施行之表單等，均須架構在此一政策下，往下制定各個細節之規範，且不容違背此政策。

其次，建立起注意事項程序以及各項標準化作業流，同時輔以各個文件表單，以此協助公司內部人員在執行時，不至於於各個作業流程中有所遺漏。

最後，各項之內部規範，亦需經適當之管理階層核准，同時各項書面文件亦有每年經適當之管理階層定期檢視與確認其內容之妥適性等規範。縱然，於虛擬通貨產業中，均為新創產業，組織特色乃極為扁平，然仍應予公司之經營管理階層，諸如公司之代表人、執行長或其他具有管理權責之主管等，予以核准，且其過程中，應留下紀錄。此等文件經過公司內部一定程序核准除可彰顯公司管理階層之重視，同時亦可據此上行下效，全公司均應遵守與施行。

2. 洗錢及資恐風險之辨識、評估與管理

(1) 規範內容及其目的

依本辦法第14條之規定，VASPs應採取適當作為以辨識、評估及瞭解其洗錢及資恐風險，評估之面向至少涵蓋客戶、國家或地區、產品及服務、交易或支付管道等。之所以需要先瞭解評估前述風險，是因為現行對於防制洗錢及打擊資恐機制之建立，希望是以風險為基礎之方法進行相關管控機制之設置，瞭解哪些風險比較大後，VASPs投入較多資源在此已進行防堵，而非要求各VASPs以無限上綱、漫無目的全方位之方式進行管控。因此，VASPs防制洗錢及打擊資恐之作為上，即需辨識以及評估VASPs內洗錢及資恐之風險程度，瞭解這些面向在VASPs經營上，帶給VASPs多大的洗錢及資恐風險，進而發展出抵減這些風險之方法進行管理。

(2) 建立重點

為確保VASPs落實前述風險為基礎之方法，於建立各項機制時，應先行建立各項辨識、評估、管理洗錢以及資恐之相關方法論，並將之書面化，藉此確認相關機制設計之基本思維，後續並以此等方法論作為機制有效與否之基本依據。

再者，各項風險評估之內容以及其範圍應完整包含是否涵蓋客戶、地域、產品及服務、交易或支付管道等面向，並與各項業務種類、性質、營運規模等相對應，同時檢視細項規定分析風險因素與風險判斷方式等是否符合邏輯。例如，客戶層面，可以考量在VASPs內部中有多少來自於高風險國家之客戶、客戶有多少是從事高風險職業；產品以及服務層面，則考量VASPs中有多少產品是去中心化等。

3. 認識客戶身分

(1) 規範內容及其目的

誠如上所述，對於防制洗錢及打擊資恐機制之建立，乃是以風險為基礎之方法進行相關管控機制之設置。方法之一即是將客戶進行不同程度之風險評分，賦予不同客戶不同評分或等級，並依其評分進行不同程度之管控以及交易監控。而有效之風險評分，乃是建立在已經取得完整之客戶資訊，VASPs應建立妥適之客戶身分確認措施，並且有效認識客戶資訊，即所謂之客戶實名認證，故依本辦法第3條以及第4條規定，VASPs需建立確認客戶身分之流程，同時亦須有拒絕建立業務關係之機制，以確保客戶之資訊完整，其後始能據此作為後續風險評級之依據。

(2) 機制設立

有關於客戶身分確認之措施之建立，其流程應包含客戶身分確認之時點，於虛擬通貨產業常見之情形，例如新建立業務關係、發現疑似洗錢或資恐交易時、對於過往所取得客戶身分資料之真實性或妥適性有所懷疑時，均是確認客戶身分明確之時點。

其次，於取得客戶身分資訊後，亦須對於各項資訊進行驗證，故在進行KYC程序中，即需蒐集相關之佐證文件，包含自然人身分證明文件、可驗證地址之水電帳單、法人之設立登記文件等，以作為客戶身分確認及驗證之依歸。

另針對客戶屬於法人或信託之受託人時，尚需檢視確認是否取得必要資訊，包含法人客戶之章程、股東名冊，或信託契約等，以辨識客戶之實際受益人或信託關係中之信託人、受託人或受益人等，以判斷是否進行合理之驗證。尤其與法人建立業務關係時，對於法人之股權結構計算，應特別留意對於持股比例之計算是否正確。

(3) 常見之問題：

在實務中，有關於客戶身分證明文件之蒐集與確認，如客戶屬於臺灣本國之客戶，其身分證明文件可以臺灣發行之身分證作為依據，如有蒐集第二證件亦可以健保卡或駕照，但第一證件仍應以身分證為宜，蓋因取得身分證後，可透過內政部換補領系統確認該身分證是否有換補領，是否為客戶最新之資訊，而健保卡或駕照則無法進行確認其上所顯示資訊為最新以及是否換補領，故作法上仍應以身分證件作為第一證件為宜。然如VASPs有國外客戶，則須留意，世上部份國家並未核發身分證件，例如丹麥或冰島等國，此時，VASPs始可進一步考量，是否以當地政府所核發之證明文件進行身分驗證，例如護照、駕照進行驗證。再者，世界各國所核發之官方證明文件多有不同，究應蒐集何種證件，實應時時依據所申請建立業務關係之客戶國籍而逐一檢視各國政策，以避免有所疏漏或所蒐集之文件不切實；同時不論是此等國家，或其他境外客戶而以護照或其他官方身分證明文件，皆應留意其有效期限，不得以逾期文件進行身分驗證。

居住地址之蒐集，乃具有確認客戶之實際居住地址之目的，如客戶確實進行洗錢甚或詐騙等犯罪行為，亦有助於警察以及檢調等得以迅速定位嫌犯。而對於居住地址之驗證，多以水、電帳單或銀行對帳單進行驗證。實務上常見問題在於，如客戶為居住在外地，其銀行帳單或對帳單所列地址，未必屬於其所承租之地，或是水電帳單上之姓名為房東本人，此種情形，或可考量取得客戶與其房東之租賃契約，只要能確保該客戶確實為租賃契約上之承租人，即可確認其居住地。

4. 客戶風險分級

(1) 規範內容及其目的

對於客戶進行風險評估以及分級，其主要目的在於可使VASPs依客戶之風險等級不同，進行不同之管理，對於經識別出之高風險客戶，VASPs得以集中較多之資源進行管控，而對於中低風險客戶，則得以採取相對寬鬆彈性之管控，充分達到以風險為基礎之管理。

(2) 機制設立

對於客戶風險等級之建立，除建立VASPs內部規範或程序文件以建立起風險分級架構及其規則，且客戶風險等級至少劃分為兩等級，較為完整之方式為三等級，並對於各類風險之客戶制定有定期審查之機制。

另有關於客戶風險評估因子部分，其面向可涵蓋客戶本身、客戶之國籍或地區、客戶所使用之產品及服務、交易或支付管道等進行設計，在此或可評估：

A. 客戶：年齡（或公司成立期間）、所提交之身分證證明文件形式。

B. 國籍：出生國（公司註冊國家）、居住國籍（或公司主要營運國家）。

C. 產品及服務：現貨、代買代賣、槓桿、定投、流動性挖礦、期權或經由交易所參與Defi投資等。

D. 交易或支付管道：綁定信用卡、綁定銀行、超商、虛擬資產ATM過往是否有六層以內之交易無法追蹤其來源或去向等。

以上風險因子僅為初步提供參考，實際狀況須依照各個VASPs所提供之服務進行擇採，同時間各個風險級距也須因各個VASPs業務量或其他因素進行劃分。

5. 客戶及交易有關對象之姓名及名稱檢核

(1) 規範內容及其目的

依本辦法第4條第7款VASPs應辨識建立業務關係之對象是否屬於制裁名單人士，並婉拒與此等人士建立業務關係，並且依本辦法第9條之規定，VASPs應辨識客戶及其實質受益人是否為現任或曾任國內外政府或國際組織之重要政治性職務人士，並且透過風險評估賦予此類客戶不同風險分數後，採取不同之管控措施或進一步拒絕交易。因此各VASPs應建立起對於客戶、實質受益人及交易對象等姓名檢核之機制。

(2) 機制建立

首應建立VASPs對於客戶及交易有關對象之姓名及名稱檢核程序，確認VASPs依風險基礎方法建立書面化之姓名檢核之機制，同時亦可藉此訂定上開機制之比對與篩檢邏輯，以及制定比對及篩檢門檻，以確認有效篩選確實有疑義之名單人士。

上開比對以及篩選邏輯，應有其建立之方法，並考量VASPs內部資源以及人力（即所謂以風險為基礎之方式），進行門檻之選擇。最後，此種比對及篩選邏輯之建立，亦須經過一定之核可程序並留下軌跡記錄，如欲調整亦同，以避免恣意調整而使得姓名檢核系統流於無用。

在制定前述姓名檢核程序時，應留意該程序應包含如掃中名單時，後續之派案及調查程序，以及如應於一定期間內完成調查，如無法判斷客戶與名單上是否為同一人，應如何處理？如仍欲建立業務關係，後續應如何管控其風險？交易是否應另有監控措施？

同時VASPs對於姓名檢核程序亦須建立起定期掃描，因為客戶身分資訊會變動，例如本為低風險之一般客戶，但一段時間後客戶因為涉有犯罪而有負面新聞，且可能為洗錢前置犯罪之新聞，故可能須對客戶進行較為嚴格之管控。故建立掃瞄機制時，亦應有定期大量批次掃描之機制，其頻率至少每週，如能每日夜間批次掃描則更為妥適。

(3) 常見問題

實務上對於姓名掃描時，由於各國的命名系統不同，導致客戶在進行KYC以及姓名檢核時，難以透過其身分證明文件進行篩選。例如，有部分之印尼人其命名系統上，不會使用姓氏，因此可能出現僅單一名之可能，也有可能不帶姓氏的複名，或帶有姓氏的複名等情形。因此，如客戶為印尼人，其所提交之姓名資訊，很可能僅為一字，此時在姓名掃描篩選上，將因無法有完整資訊而有效篩選與外部名單系統上同名同姓之客戶。對於此類無法篩選之客戶，各VASPs可能須視實際情形，斟酌跟客戶額外徵提其他佐證文件可供篩選，或者對於此等客戶建立業務關係初期，將之列為高風險客戶，並且再限縮其交易額度，待觀察其交易模式，是否有符合異常交易情境，或建立業務關係後短期內其有大量交易，以判斷其是否確實有風險，如未有異常，待過一定期間後再調降其風險等級。

其次，如果客戶掃中負面新聞，是否一律均須劃分為高風險？例如客戶曾有酒駕、外遇等，是否即應視為高風險？就此，應以洗錢及打擊資恐有關之犯罪新聞為主，例如洗錢防制法第3條所列之前置犯罪，例如詐欺侵佔，蓋因這些前置犯罪往往僅跟隨後續之洗錢犯罪，故應著重在此類與洗錢或資恐有高度關聯之負面新聞。同時，亦可考量該犯罪新聞。

縱然客戶真的曾有類似詐欺侵占等前置犯罪行為，然如果此等犯罪之負面新聞已非常久遠，例如達十年以上，且期間亦未有其他犯罪新聞，則或許毋庸再將該客戶評價具有負面新聞而列為高風險，蓋因十年前之犯罪，其期間久遠洗錢風險或許已低，然仍應個案中輔以其他資料判斷，同時也需要兼顧VASPs中之資源，以風險為基礎判斷之。

6. 客戶身分持續審查

(1) 規範內容及其目的

對於客戶進行風險評分後，客戶之資訊極可能發生變動，例如客戶之居所地變更，可能搬遷至高風險國家地區，或客戶可能因其職業變更，可能變更為高風險職業如律師或會計師等，此時如未有對客戶身分資訊有效掌握以及更新，將可能因此使得客戶風險評估無法反應客戶真實身分，而無法有效評估，進而無法有效掌控風險以及設計抵減措施。是以，依本辦法第5條之規定，VASPs需依照不同等級之客戶，進行不同頻率以及程度之持續性調查，對於客戶資訊之有效且確實的掌握，並據此降低VASPs洗錢及資恐風險。因此，VASPs亦應建立起客戶盡職調查之機制，其內容應依客戶重要性及風險程度，並於考量前次執行審查之時點及所獲得資料之適足性後，決定審查之方式以及頻率，對已存在或新增業務往來關係之客戶進行審查，或依據客戶之重要性及風險程度或其身分背景有重大變動時執行審查程序。尤其對於高風險客戶，應至少每年檢視一次相關之客戶及實質受益人身分之資訊。

(2) 機制建立

VASPs首應先確立是否訂定確認客戶身分措施及持續審查之程序，檢視是否以風險基礎方法作為其執行強度之依據，甚而其內容對於高風險客戶是否採取更進一步之強化措施，並且能有效降低其風險。而於調查之內容上，可設計表單加以輔助，內容可包含瞭解客戶財富及資金來源，如資金來源為存款，則應進一步瞭解該存款之來源，並可由客戶進行細部說明。

以上各項資料之徵提，不能僅單純將盡職調查表單交由客戶填寫即為結束，而應就客戶所填寫之各項資料，徵提相關資料予以驗證。此外，由於虛擬通貨產業之交易上，基本上都是非面對面交易，然對於某些特殊高風險之客戶，在執行盡職調查過程中甚至可斟酌是否以視訊調查之方式，加以探詢客戶之實際狀況，並留下佐證紀錄。

7. 旅行規則（Travel Rule）

(1) 規範內容及其目的

本辦法在制訂時，特別於第7條訂定擔任虛擬通貨移轉交易轉出人之VASPs，於其用戶進行虛擬通貨交易時，需取得該用戶以及接收方必要且正確之資訊，並應將前述資訊立即且安全地提供予擔任接收方之VASPs。而相關資訊於轉出人應包括：轉出人姓名、轉出虛擬通貨之錢包資訊及官方身分證明文件號碼、地址、出生日期及出生地；於接收人其則應包括接收人姓名、接收虛擬資產之錢包資訊等。此一規則，猶如傳統金融在進行國際匯兌時，需要經由環球銀行金融電信協會（Society for Worldwide Interbank Financial Telecommunication, SWIFT）系統傳送有關銀行之間的交易內容以及客戶資訊等標準化訊息後，可以併同執行反洗錢或打擊資恐之檢核。

接收方另應採取適當措施，以辨識出缺少必要資訊之虛擬通貨移轉並透過風險為基礎之政策及程序，以判斷何時執行、拒絕或暫停缺少必要資訊之虛擬通貨移轉，及適當之後續追蹤行動。

於雙方VASPs接收到相關訊息時，應進一步確認交易對手接收方或轉出方之事業所受監理規範與FATF所定防制洗錢及打擊資恐標準一致，確認該VASPs未有其反洗錢與打擊資恐之相關作為達到FATF所定之標準。

應特別留意者在於，上開機制在立法前金管會邀集業者之討論會議上，業者提出因現行國際上各國並非全然施行Travel Rule，倘如本辦法第7條予以制定並施行，業者在國際虛擬通貨之交易上，將無法遵行恐有違法之虞，是以金管會特於第18條規定，須視國際間之執行情形，再由主管機關另訂施行日，故本條目前尚未有實際施行之案例。

(2) 機制建立

有關於Travel Rule 之實踐流程上，除相關程序應予以制定外，其發出方以及接收方之資訊相互拋傳應採取資訊先行之方式，亦即每次交易發動時，應先以將發出方之資訊拋傳予接收方之VASPs，並由接收方VASPs進行完相關法遵檢核後回傳確認無誤或無異狀之訊息後，始開始後

續之鍊上交易。此種資訊先行之方式，能在交易發出前即確定交易對手是否具有洗錢及資恐風險，並進而防堵之。

交易雙方VASPs依照Travel Rule所傳輸取得之資訊時，即可透過VASPs之姓名檢核系統進行掃描，判斷客戶是否屬於名單人士，此外，因錢包資訊亦會先行互相拋傳，此時亦可針對此等錢包進行掃描，確認是否經過制裁，並據此決定是否開啟後階段之交易。

8. 帳戶及交易持續監控及交易追蹤

(1) 規範內容及其目的

與客戶建立業務關係後，VASPs對於其客戶即須對於客戶之帳戶或其交易內容持續性監控，以確保客戶之交易未有疑似洗錢或資助恐怖主義之情形。而此種監控均同時應搭配虛擬通貨於區塊鏈上之交易追蹤系統，以辨識虛擬資產之交易活動。

(2) 機制設立

首先應依據以風險為基礎之方法，並且參考金管會於2021年7月所發布異常交易情境監控態樣，建立客戶帳戶及交易監控程序，內容應依據本辦法之規定以及客戶性質、業務規模及複雜度、洗錢與資恐之相關趨勢與資訊、內部風險評估結果等，設定疑似洗錢之監控態樣，並且包含交易態樣、交易金額門檻、交易頻率等參數，同時亦須有監控案件的檢視程序及申報標準等，以作為各項表徵之內容。

其次，對於上開機制亦同時訂有定期檢視以及更新交易監控態樣之機制，並且檢視其資訊系統是否整合全公司客戶之基本資料及交易資料，確認是否足以強化VASPs對於帳戶及交易監控能力。此外，亦可透過實際檢測系統之程式碼，確認前述各項表徵以及參數、金額門檻等，均有確實設定於系統上。

由於虛擬通貨之交易，均是透過虛擬通貨之錢包進行幣與幣之間之交易，而現行國際上已經開始有政府組織會將用於洗錢或資恐之錢包進行制裁並發布相關名單，實應於交易過程中，併同掃描錢包地址，確認此一地址是否來已受制裁？如有，亦應於交易當下予以拒絕交易。

交易追蹤部分，VASPs對於用戶之每筆交易應判斷並追蹤其後續之交易層級，盡可能追溯其交易後面一定層數以上，識別出交易是否曾經過暗網、或是否曾經由混幣器等此種人為刻意抹去其交易歷程或使得難以追蹤。且亦可另外訂定，例如客戶之過往交易曾有單筆交易五層內曾有經過暗網或混幣器等，賦予該筆交易較高之風險，如客戶短時間內有三筆或五筆此類高風險交易，即應回饋之客戶自身之風險評估，將客戶之風險列為高風險，並即採行嚴格之盡職調查。前述例子，僅供參考，實則，在交易監控上，不如是異常交易之監控或是虛擬通貨之交易追蹤上，均可將其風險回饋之客戶風險評估上，除可滾動式調整客戶風險達到現時的客戶風險樣貌，並且可及時採取後續之盡職調查作為，以減低VASPs之機構風險。

9. 紀錄保存

(1) 規範內容及其目的

在執行防制洗錢及打擊資恐之相關義務時，相關執行或調查之紀錄保存實屬管控重點之一，例如姓名檢核知調查結果、異常交易監控之調查報告等，主要因為VASPs須配合金融情報機構或金融監理單位甚或是合作往來之銀行單位之管理需要，適時提供相關交易紀錄或調查記錄，因此VASPs必須明訂相關紀錄保存與保護之機制，且相關紀錄資料是否保存至與客戶業務關係結束後或臨時性交易結束後，至少五年。

(2) 機制建立

VASPs面對記錄保存此義務，應明訂相關規範或作業方式，其應至少包含記錄保存內容之完整度、保存時間、保存位置、存取管控、調閱方式等議題。同時間，亦應針對何種資訊可能哪些層級之職員閱覽，而建立起不同之分層管理架構，以避免文件記錄不當外洩。

應特別留意，各項客戶之個人資訊、交易紀錄、風險評估等，均係在系統上完成，應留意此類資訊之變更、或如風險評估之因子設定或調整、異常交易情境等參數設定或調整，其系統背後之軌跡記錄亦應留存，凡有異動均須記錄下來，包含何人、何時、為何異動均須記錄，以避免私自竄改。

10. 可疑交易申報

(1) 規範內容及其目的

可疑交易申報作業乃屬於VASPs應盡義務之一，VASPs應依其作業特性、客戶交易往來狀況，適時將相關可疑交易資訊申報至金融情報機構，以收即時反應與打擊洗錢犯罪之效果。

(2) 機制建立

VASPs應確認當監控報告識別出異常交易時，VASPs有無適當的分析與調查政策、程序和派案流程，並確保案件不會積累過多。此外各項程序亦應明定細部調查判斷之方法，如：與客戶身分、收入或營業規模顯不相當、與客戶本身營業性質無關、不符合客戶商業模式、無合理經濟目的、無合理解釋、無合理用途、資金來源不明或交代不清等情事。如個案中專責人員核定確實為異常交易，應於核定後立即向法務部調查局通報，其期限不得逾二個營業日。

11. 指定防制洗錢及打擊資恐專責人員負責遵循事宜

(1) 規範內容及其目的

由於VASPs對於防制洗錢及打擊資恐之管控有其特殊性與必要性，因此透過配置一定之管理監督資源並設置專責角色，能夠確保相關管控能夠結合業務活動適當執行，以收防制洗錢及打擊資恐之效。

(2) 機制建立

VASPs在此應設置防制洗錢及打擊資恐合規之專責人員，並確認其權責分工與資源配置是否合宜。

一旦確立專責人員，該專責人員即需負責協調監督防制洗錢及打擊資恐事宜。並定期向董事會或高階管理階層進行報告公司防制洗錢及打擊資恐相關事宜，包含內部控制與稽核制度、備置並定期更新洗錢及資恐風險評估報告等。

12. 員工遴選及任用程序

(1) 規範內容及其目的

由於防制洗錢與打擊資恐之作業活動須有適當且專業之員工執行，因此如何遴選出具有廉正品格之員工，並協助其發展防制洗錢與打擊資恐之管理專業，亦是VASPs管理重點。是以，VASPs依第15條第1項第3款之規定建立高品質之員工遴選及任用程序。

(2) 機制建立

VASPs應建立書面化之員工遴選及任用程序，其內容應至少包含員工資格遴選方式、瞭解員工基本資訊與背景等，並應確認針對特定工作職務之資格任用，是否符合洗錢防制法暨相關法令或辦法規定之資格條件。

實務上可參考之作法，乃是於遴選中，將員工之姓名進行姓名檢核，已確認是否曾有負面新聞或是是否有其他名單上所示之資訊，以考量該名員工是否聘任？倘如聘任，後續應如何管控？或其職務是否需要進行一定阻隔？

13. 持續性員工訓練計畫

(1) 規範內容及其目的

由於虛擬通貨產業，因此如何有效嚇阻或偵測相關異常行為，亦須仰賴執行人員具備豐富之相關經驗與足夠認知，透過持續性地對相關員工展開適當之訓練計畫，能夠讓VASPs從業人員在面對可疑交易對象或活動時，保持足夠敏感度執行客戶審查或交易分析工作。

(2) 機制建立

VASPs應建立持續性之職前訓練與在職教育訓練計畫，且各項課程內容應涵蓋教育訓練紀錄以及教育訓練計畫之落實度。同時亦應包含針對未滿足該年度上課時數要求或缺席課程之補救或追蹤機制。

VASPs應針對不同對象執行適合該對象之教育訓練活動，例如第一線執行人員、法令遵循人員、內部稽核人員或高階主管等。同時亦應有如何衡量教育訓練成果，以確定教育訓練之有效性。

14. 測試防制洗錢及打擊資恐系統有效性之獨立稽核功能

(1) 規範內容及其目的

VASPs一旦建立起內部之反洗錢與打擊資恐管理機制運作，後續即需確認其機制有效性，此時VASPs必須結合內部稽核機制，或透過委由獨立第三方協助進行有效性測試活動，以便能夠掌握管理機制在設計面或是落實面，是否還有需要改善或優化之處。

(2) 機制建立

VASPs應建置防制洗錢及打擊資恐系統有效性之內部稽核作業計畫，並應評估該作業計畫內容之妥適性與完整度，確保其涵蓋面向足夠。

並應建立內部稽核報告和工作底稿內容，確認稽核方法或稽核之抽樣比例亦應合宜。

應建立防制洗錢及打擊資恐系統有效性之內部稽核報告，並依據其所提之查核意見或發現事項進行內容確認，並應審視高風險事項之改善計畫，期改善計畫內容應包含改善負責單位，預計完成時程，具體改善方式等資訊。

以上針對本辦法之初步介紹，內容亦有提及機制如何設立。然應留意者在於，各項機制設立或可能遇到的問題，乃是筆者過往服務之經驗累積，且乃是依筆者所待之交易所或其他VASPs內部情形，不一定能一體適用到其他VASPs。然此也體現出，防制洗錢及打擊資恐本就是以風險為基礎之方式進行設置，順應實際狀況進行調整。而臺灣在虛擬資產之管理上仍有好長一段路需要與時俱進，例如是否仿照如韓國、新加坡等發放牌照，透過牌照要求VASPs達到更多義務，例如消費者保護、資訊安全落實等；或是針對NFT、DeFi洗錢及資恐防制上，應如何作為，乃至於DeFi觸及傳統《期貨交易法》、衍生性金融商品之管理等，均須待主管機關釐清。希冀透過此種逐步且溫和調整之方式，讓業者仍在創新與監管之間取得平衡，共同促進產業之發展。

第五章 虛擬資產業之法令遵循

傳統金融機構歷經約600年的發展，期間發生過無數次金融危機及諸多非法行為。在巴塞爾銀行監理委員會（Basel Committee on Banking Supervision）於1988年公布並陸續更新的《巴塞爾協定》，確立了穩定金融市場的三大支柱即「最低資本要求」、「監理審查」以及「市場紀律」，其根本目的在於透過對金融機構的監督管理來確保金融市場的整體穩定性。這亦使法令遵循已成為全世界金融機構的顯學。與傳統金融機構相比，因應2009年比特幣白皮書而生的VASPs其從事的行為本質與傳統金融機構相似，隨著虛擬資產的規模日益壯大，各國政府也逐步實施各項監理措施。在區塊鏈應用更為普及與廣泛的前題下，可預期未來VASPs所受之監管措施亦會逐步仿照傳統金融機構之高度監管模式。

一、聘請內部法遵團隊

VASPs的法遵團隊除了須處理企業所在地主管機關之法令遵循要求，同時亦要實時注意國際組織或各國主管機關之監管措施或指引。VASPs聘請的內部法遵團隊除須具備傳統金融機構處理法令遵循事項外，需要具備對虛擬資產、區塊鏈的基礎知識。目前可藉由國際組織團體，如公認反洗錢師協會（Association of Certified Anti-Money Laundering Specialists, ACAMS）提供專門虛擬資產和區塊鏈專家級別認證證書，亦或可參與致力於教育培養區塊鏈人才的地域性組織，如臺灣虛擬通貨反洗錢協會，參與定期舉辦的論壇活動以累積虛擬資產、區塊鏈的相關知識。

此外，由於現在虛擬資產及區塊鏈的相關教育系統尚未發展成熟，且虛擬資產業在諸多國家尚未取得正式的承認，因此筆者觀察到鮮少有從事法令遵循的求職者會僅鎖定虛擬資產業作為其求職目標，並自費參與上述認證資格或課程，因此VASPs招募人才後仍需要花費資源與時間栽培法令遵循人員關於虛擬資產或區塊鏈的相關知識。是故，VASPs亦可考慮專注於虛擬資產法令遵循領域的顧問公司，利用派遣等方式，由顧問公司的專業顧問建立VASPs內部法令遵循制度並培訓VASPs內部法遵團隊，無非是有效之舉。

二、 使用防制洗錢技術服務和工具

VASP與傳統金融機構最大不同之處在於為客戶保管的虛擬資產與傳統金融產品有本質上的差異。虛擬資產在地址與地址之間轉移，僅是羅馬數字與英文字母的亂數，若不借助專門為虛擬資產分析的技術服務實難辨識交易資訊，更別說實施防制洗錢與打擊資恐的任務。

另一方面，虛擬資產的問世是在網際網路爆發性發展的時間，因此與傳統金融機構不同的是，絕大多數VASPs是以網際網路與客戶建立業務關係，並且由於虛擬資產的特性本無國界之分，當地法令無明文禁止的前期下，VASPs通常會以網路的方式收受來自世界各地的客戶的註冊要求，因此要如何有效地確認客戶身分亦是VASPs面臨的挑戰。

最後關於FATF要求VASPs實施Travel Rule的要求，目前全球尚未針對資訊交換的格式等細節有共識，目前有將近10種不同的協議，尚未具備統一共識而難以實行。VASPs的法遵團隊應實時關注當地政府是否針對轉帳規則設立日出條款，並關注虛擬資產業轉帳規則在如何資訊交換的議題有無重大突破。

三、 建立可信的身分識別體系

目前已有許多專注於提供電子化客戶盡職調查（Electronic Know Your Customer, e-KYC）的解決方案。其主要原理為利用機器學習、臉部基礎的生物辨識技術和活體偵測技術來快速準確地驗證遠端客戶的數位身分。具體而言，e-KYC會辨識客戶上傳的身分證明文件的真實性並執行相似性和活體偵測，以驗證持有身分證的人是否與身分證中顯示的人是否為同一個人，並且是否真實存在。同時可利用光學辨識技術提取身分證明文件上之資訊，供執行姓名檢核等其他洗錢防制措施使用。e-KYC能減低VASPs辨認外國身分證明文件真偽之成本，並可節省確認客戶身分之審查人力成本。

四、 部署虛擬資產流向追蹤工具

VASPs欲落實洗錢防制首要的任務即是辨識虛擬資產的交易資訊及其風險，目前已有諸多公司能提供虛擬資產風險分析與流向追蹤工具，其主要原理為，利用虛擬資產的移轉紀錄皆公示於區塊鏈上之特性，並綜合三種面向，一是利用搜集網路公開資源，如勒索軟體要求受害者須將虛擬資產移轉至指定的「地址」，二來是國際組織公布的制裁名單中與虛擬資產有關的情報資訊，最後是公司自行購買或自行調查的資訊，如向網路賭博網站註冊取得地址等。將搜集的情報資訊加以整理歸納，即可對地址施與風險分數。近期屢見有利用虛擬資產流向追蹤工具而協助執法機關調查的案例，此種工具筆者認為係VASPs不可或缺的工具之一。

第六章 總結與展望

防制洗錢及打擊資恐本即是以風險為基礎推展，因應實際狀況加以調整。承前對於國際監管趨勢之觀察，歐盟國家現以反洗錢指令為根據，持續監控及分析虛擬資產於洗錢及資恐上的運用方式，作為後續立法之基礎。日本則受國內虛擬資產服務提供者之發展歷史影響，很早即將之納入監管，透過外部法規和業者內部自律規則之要求，加強反洗錢義務之落實。在虛擬資產所使用的區塊鏈已成為金融科技發展的重要趨勢之現下，應用日趨深遠且廣泛，已可預期未來將會仿照傳統金融機構之監管強度發展。

在防制洗錢及打擊資恐監管漸獲重視的國際環境中，臺灣於2021年6月正式將虛擬通貨平台及交易業務事業納入反洗錢之一環，指定金管會為主管機關，然而，此並未涉及虛擬資產之產業治理、業務經營、消費者保護、資訊安全等議題，現階段係針對確認客戶身分、紀錄保存及可疑交易申報等三面向，加以監督。針對虛擬資產之管理，仍有許多議題尚待主管機關釐清，例如是否透過牌照促使VASPs履行更多義務，或是針對NFT、DeFi防制洗錢及資恐上之作為，乃至於DeFi觸及傳統期貨交易法、衍生性金融商品之管理等面向。

另外，在VASPs的法令遵循方面，應聘僱內部法遵團隊定期更新主管機關之相關法令，並留意國際組織或各國的監管措施或指引。法遵團隊應時時關注主管機關是否針對轉帳規則設立日出條款，並關注虛擬資產業轉帳規則在共識上有無重大突破、透過電子化客戶盡職調查建立可信的客戶身分識別系統、設立虛擬資產識別追蹤流向之工具以掌握虛擬資產的交易資訊並降低其風險。

期待虛擬資產服務提供者逐漸發展、監管資料數量累積具相當規模時，再進一步加強服務提供者的反洗錢義務，循序漸進在發展過程中尋求調適，共同促進科技金融產業的發展與健全。

V06062022