行政院及所屬各機關因公出國人員報告
（出國類別：進修）

韓國釜山虛擬資產調查訓練

報告

服務機關：法務部

姓名職稱：

劉怡君檢察官（臺灣高等檢察署智慧財產分署）

羅韋淵主任檢察官（臺灣士林地方檢察署）

周官緯檢察事務官（臺灣高等檢察署）

派赴國家：韓國

出國期間：113 年 10 月 27 日至 11 月 1 日

報告日期：114 年 1 月 3 日

摘要

世界銀行在加拿大政府反恐能力建設計畫的支持下，協助亞太地區國家打擊洗錢（ML）、恐怖主義融資（TF）和擴散融資（PF）。此類協助旨在增強預防、偵查和打擊非法資金流動及金融犯罪的能力。

透過與亞太反洗錢組織（APG）的合作，世界銀行瞭解到提高整個 APG 地區執法官員在調查洗錢、資產追回、詐欺及涉及加密貨幣金融犯罪方面的技能及知識的重要性。故而，世界銀行與 BlockTrace LLC[1]合作，取得日本政府及釜山 FATF 培訓學院支持，舉辦本次虛擬資產調查訓練課程。

本文除針對本次訓練課程內容進行說明外，另就課堂上各國的學員對於調查洗錢、資產追回、詐欺及涉及加密貨幣金融犯罪等相互交流進而提出心得與建議，期供相關政策擬定之參考。

[1] BlockTrace LLC 公司與政府和私人實體合作，其利用行業領導者的專業，克服加密貨幣調查相關的挑戰，並直接與美國的執法部門和稅務部門合作。

目次

一、 前言

隨著全球經濟的數位化，加密貨幣及虛擬資產的應用日益廣泛，但也帶來新的金融犯罪風險。為有效應對這些挑戰，提升執法機關及金融機構的能力即至關重要。本次虛擬資產調查訓練課程為此背景原因而舉辦，旨在提升學員對加密貨幣生態系統的理解和能力。

世界銀行在加拿大政府反恐能力建設計畫的支持下，協助亞太地區國家打擊洗錢（ML）、恐怖主義融資（TF）和擴散融資（PF）。這些協助旨在增強預防、偵查和打擊非法資金流動及金融犯罪的能力。透過與亞太反洗錢組織（APG）的合作，世界銀行認識到提高整個 APG 地區執法官員在調查洗錢、資產追回、詐欺及涉及加密貨幣金融犯罪方面的技能及知識的重要性。為滿足此一需求，世界銀行與 BlockTrace LLC 合作，取得日本政府及釜山 FATF 培訓學院支持，舉辦本次虛擬資產調查訓練課程。

本文除針對本次訓練課程內容進行說明報告外，透過與講師的經驗交流，並與來自亞洲各國的檢察官、執法人員、中央銀行人員互相交流，瞭解各國政府對於虛擬資產監管與執法之現況，末提出了受訓心得及建議，希望帶給我國打擊虛擬資產犯罪新的思考方向。

二、 訓練目的

（一） 本次訓練在提升學員對加密貨幣生態系統的理解及能力，介紹與虛擬資產及虛擬資產服務提供者(VASP)相關的反洗錢/打擊資助恐怖主義(AML/CFT，Anti-Money Laundering / Countering The Financing Of Terrorism)國際標準。學員在整個培訓過程中，將獲得虛擬資產知識及經驗，了解加密貨幣生態系統中的主要參與者，以及各種類型的加密貨幣及其應用案例。學員將學習如何識別可疑的加密貨幣地址、追蹤其來源和關連性，並採取最有效的策略來調查洗錢活動。訓練還將透過真實案例了解最新調查技術。

（二） 課表：

Time	DAY 1	DAY 2	DAY 3	DAY 4
0900-0930	Welcome and Opening Remarks	Human Rights / Diversity	FATF Best Practice and Guidance on Financial Investigations Involving Crypto	Recap
	Program Overview	Crypto Wallets		
0930 - 1000	FATF requirements relating to VA/VASP		Ethereum 101	Seizing Cryptocurrency
1000-1030		Private Keys & Seed Phrases		
	Break			
1030-1100	Binance: A VASP Case Study	Private Keys & Seed Phrases (Cont.)	Ethereum 101	Korean Experience
1100-1130		Live Crypto Transfers		
1130-1200	Binance Q&A	Restoring Wallets		Practical Exercises
	Break			
1200-1230	Cryptocurrency 101	Restoring Wallets Practical Exercise	Ethereum Explorer	Practical Exercises
1230-1300	Bitcoin 101		Money Laundering Trends	
1300-1330	Lunch			
1330-1400				
1400-1430	Bitcoin 101 (Cont.)	Tool 1 Presentation	Tool 2 Presentation	Dark Web Overview
1430-1500	Bitcoin Transactions			
1500-1530	Blockchain Explorers			Survey / Closing Remarks
	Break			
1530 -1600	Practical Exercise	Tool 1 Practical Exercise	Tool 2 Practical Exercise	
1600 - 1630				
1630-1700	Q & A	Q & A	Q & A	

三、 Introduction to Cryptocurrency（虛擬貨幣簡介）

本課程概述了加密貨幣的基本概念、優勢、挑戰及其未來的潛力。

(一)、 加密貨幣的定義及用語：虛擬貨幣（Virtual Currency[2]）或加密貨幣（Cryptocurrency[3]）一詞在我國法制上並非法定用語，其用語在各國亦非一致，有稱為「數位資產」（Digital Assets[4]）、虛擬資產（Virtual Assets）等不一而足。因虛擬貨幣依我國之法制並非「貨幣」，洗錢防制法第 5 條第 2 項於民國 113 年 7 月 31 日修正前之規範用語為「虛擬通貨」，修正後則以「虛擬資產」稱之，依修正理由提及：「FATF 於一百零七年十月將 虛擬資產(Virtual Asset)相關活動納入洗錢防制規範。FATF 修正四十項建議之建議第十五項及評鑑方法論，並於詞彙表新增「Virtual Asset（虛擬資產）」及「Virtual asset service provider, VASPs（虛擬資產服務提供者）」之定義。為使本法用語及規範範圍與 FATF 一致，考量使用「虛擬通貨」一詞仍易造成 外界誤解其屬於貨幣，爰將第二項及第四項「虛擬通貨平台及交易業務之事業」之文字修正為「提供虛擬資產服務之事業或人員」。」另虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法於 113 年 11 月 26 日亦隨之修正為「提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法」，該辦法第 2 條第 1 項第 2 款則定義：「虛擬資產：指運用密碼學及分散式帳本技術或其他類似技術，表彰得以數位方式儲存、交換或移轉之價值，且用於支付或投資目的者。但不包

---

[2] FATF 亦曾在正式出版之指引中使用虛擬貨幣（Virtual Currency）一詞，請參見：https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html

[3] 美國司法部（DOJ）於 2022 年 2 月 17 日宣布成立國家級加密貨幣執法小組（National Cryptocurrency Enforcement Team, NCET），其用語即為「Cryptocurrency」可參見：https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team 。此外，美國司法部位求增強其偵辦加密貨幣執法之能量，於 2023 年 7 月 20 宣布將 NCET 併入電腦犯罪與智慧財產部門（Computer Crime and Intellectual Property Section, CCIPS)，合刑事部門在打擊網路犯罪各個方面的專業知識，可參見：https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-center

[4] 例如：美國國稅局（Internal Revenue Service, IRS）以 Digital Assets 稱之，並認比特幣、穩定幣、NFT 均屬之。請參見：https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets

括數位型式之新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣、有價證券及其他依法令發行之金融資產。」而「密碼學[5]」、「分散式帳本」技術二者即為區塊鏈之核心特色，可知我國所指虛擬資產雖未言名係基於區塊鏈技術而發展，但所指即為包含目前國內偵查實務上遇到最多的比特幣、以太幣、由泰達公司（Tether）在諸多區款鏈上[6]部屬智能合約發行之USDT等基於區塊鏈技術而發展之虛擬資產，其利用加密技術來確保交易的安全性和防止偽造。加密貨幣通常基於區塊鏈技術，為一種分散式的資訊庫技術，能夠記錄所有交易。本文以下用語雖有使用虛擬資產、虛擬貨幣、加密貨幣等，惟所指均係基於區塊鏈技術而發展之虛擬資產。

(二)、 去中心化特性：加密貨幣不受任何中央機構（如政府或銀行）的控制。亦即用戶可以直接進行交易，不需透過中介機構，從而提高透明度及安全性。

(三)、 主要的加密貨幣：比特幣為第一種也是最知名的加密貨幣，主要用做數位資產和價值儲存。以太坊則不僅是一種貨幣，也是一個平台，允許開發者創建智能合約7和去中心化應用。萊特幣則是比特幣的衍生品，旨在提供更快的交易確認時間。

(四)、 交易的匿名性：加密貨幣交易通常不需要提供個人身份訊息，使用戶在進行交易時可保持匿名。這一特性雖然有其優勢，但也可能被不法分子利用。

(五)、 交易手續費低：加密貨幣的交易手續費8通常低於傳統金融系統，特別是在跨國交易時，使其成為一種更具成本效益的支付方式。

---

[5] 因為加密貨幣使用密碼學（Cryptography）之技術，這也是 Cryptocurrency 稱呼之由來。又依據筆者羅韋淵長期與國外檢察官及執法機關交流之經驗，在談及虛擬貨幣或加密貨幣時，亦常見口語上以「Crypto」稱之。

[6] Tether tokens exist as digital tokens built on various blockchains including Algorand, Avalanche, Celo, Cosmos, Ethereum, EOS, Liquid Network, Near, Polkadot, Solana, Tezos, Ton, and Tron. Therefore, issuance of Tether tokens is viable on various blockchains with varying capabilities depending on the transport protocol used. 請參見：https://tether.to/en/how-it-works

[7] 智能合約或智慧合約（Smart contract）是一種智慧型協定，在區塊鏈內制定合約時使用，當中內含了程式碼函式 (Function)，亦能與其他合約進行互動、做決策、儲存資料及傳送以太幣或其他虛擬資產等功能。智慧型合約主要提供驗證及執行合約內所訂立的條件。

[8] Gas Fee 是區塊鏈交易時需支付的費用，類似於我們在銀行轉帳時都要支付手續費，在區塊鏈交易時也需要支付 Gas Fee，用來支付網路上執行交易或智能合約所需的計算費用。通常來說，

(六)、 快速的交易速度：加密貨幣交易的確認時間通常在幾分鐘內，比傳統銀行轉帳所需的幾天時間快很多，在國際交易中此優勢尤其顯著。

(七)、 市場波動性：加密貨幣市場的價格波動性很大，意味價格可能在短時間內大幅上升或下降。此種波動性吸引許多投資者，同時也帶來高風險。

(八)、 法律和監管挑戰：由於加密貨幣的去中心化特性，各國對其的法律和監管框架尚不完善，可能導致法律風險和不確定性，影響加密貨幣廣泛採用的可行性。

(九)、 安全性問題：雖區塊鏈技術本身具安全性，但加密貨幣交易所和數位錢包可能成為駭客攻擊的目標[9]。用戶需要妥善保管自己的私鑰，以防止資金損失。

(十)、 未來的潛力：加密貨幣被認為有潛力改變全球金融系統，提供更便捷的支付方式，可能成為未來的主流貨幣。隨著技術的進步和接受度的提高，加密貨幣的應用範圍亦可能不斷擴大。

在各區塊鏈上用於支付手續費（國內或有稱礦工費或油費）的都是各區塊鏈上的原生代幣，例如在以太坊上是 ETH，在 TRON（波場鏈）上是使用 TRX。Gas Fee 會隨著網路、同時段中的交易需求之變動，以 USDT 為例，其在各區塊鏈上的 Gas Fee

[9] 2022 年，加密貨幣駭客攻擊在多個交易所總共竊走了 38 億美元的加密貨幣，高於 2021 年的 33 億美元。可參見：https://www.kaspersky.com.tw/resource-center/threats/crypto-exchange-hacks

四、The Rise of Bitcoin: A Decentralized Digital Currency（比特幣的崛起：去中心化電子貨幣）

本堂課提供對比特幣及其生態系統的深入理解，涵蓋運作原理、挑戰和未來的發展潛力。

(一)、 比特幣的定義：比特幣為一種數位貨幣，允許用戶之間進行直接的金融交易，而不需要銀行或其他金融機構作為中介。此種設計旨在提高交易的效率和降低成本。

(二)、 去中心化的特性：比特幣的去中心化意味著沒有單一的控制機構，所有交易和資訊都分散在全球的多個節點上[10]。此種設計使得比特幣不易受到政府或單一實體的干預或操控。

(三)、 區塊鏈技術：區塊鏈為一種分散式的資訊庫技術，所有的比特幣交易都被記錄在一個公共帳本上，稱為區塊鏈。此種技術確保交易的透明性及不可篡改性，因為每個區塊都包含前一個區塊的雜湊值。

(四)、 安全性：比特幣的安全性來自於其去中心化的網路和加密技術。每個交易都需要經過網路中多個節點的驗證，使任何單一實體都難以控制或篡改交易記錄。

(五)、 環境影響：比特幣的挖礦過程需要大量的計算能力，產生高能耗問題。隨著比特幣的普及，挖礦對環境影響的關注也日益增加，也促使人們尋求更具持續性的挖礦方法。

(六)、 私鑰的重要性：私鑰是用戶控管其比特幣資產的關鍵。如果用戶遺失私鑰，將無法再控管其比特幣，使得私鑰安全性至關重要。

(七)、 交易的匿名性：雖然比特幣交易不直接顯示用戶的身份，但每筆交易都可以在區塊鏈上被追蹤。這意味著通過分析交易資訊，可能會揭示用戶的身份，對於隱私而言是一個潛在風險。

[10] 目前全球大約有 20597 個比特幣節點（Node），可參見：https://bitnodes.io/

(八)、 未來的挑戰：比特幣的交易速度和手續費問題為普及性的一大挑戰。隨著用戶數量的增加，交易雍塞可能導致手續費上升，促使開發者尋求解決方案，諸如閃電網路[11]等方式，以提高交易效率。

(九)、 技術改進：比特幣的協議不斷進行升級，以提高其功能和效率，例如 Taproot 升級，旨在增強隱私性和交易靈活性，使複雜交易更高效。

(十)、 監管與政策：隨著比特幣的普及，各國政府開始制定監管政策，以應對金融穩定、消費者保護及潛在的非法活動等問題。這些政策可能會影響比特幣的發展方向，可能促進其合法化，也可能帶來限制。

[11] 閃電網路 (Lightning Network) 是位於比特幣之上的「第 2 層」支付協定。旨在實現參與節點之間的快速交易，並已被提議作為比特幣可擴展性問題的解決方案。

五、Crypto Wallets（加密貨幣錢包）

本課程概述加密貨幣錢包的基本概念、功能及安全管理的重要性。

(一)、 加密貨幣錢包的定義：加密貨幣錢包是一種專門設計的軟體工具，主要用於儲存用戶的私鑰（用於簽署交易的密碼）和比特幣地址[12]（用於接收比特幣的公共識別碼）。這些錢包不僅能夠安全地管理前揭關鍵資訊，且允許用戶進行加密貨幣的交易。

(二)、 錢包的類型：錢包分為兩大類：熱錢包和冷錢包。熱錢包是連接到網際網路的錢包，使用方便，適合日常交易，但因連結網路而面臨較高的安全風險。冷錢包則是離線儲存方式，安全性較高，適合長期保存資產，但使用上不如熱錢包便利。

(三)、 比特幣地址：比特幣地址係用於接收比特幣的公共密鑰，類似於銀行帳號。用戶可將地址分享給他人，以便他人向其發送比特幣。比特幣地址通常由一串字母和數字組成，具有唯一性。

(四)、 私鑰與公鑰：錢包生成的公鑰用於接收比特幣，而私鑰則是用戶用來控管其比特幣的關鍵，任何擁有私鑰的人，都可以控制相應的比特幣資產，因此私鑰的安全性至關重要。

(五)、 助記詞（Seed Phrase）：助記詞是一組隨機生成的單詞，通常由12到24個單詞組成，用於生成和恢復私鑰。此種設計使用戶於遺失設備或錢包時，可透過助記詞恢復其資產。

(六)、 紙錢包[13]：紙錢包是一種冷儲存方式，將私鑰和比特幣地址列印在紙上。此方法提供物理安全性，因為不連接到網際網路，適合長期保存比特幣，但需妥善保管，避免損壞或遺失。

---

[12] 關於私鑰、公鑰與錢包地址之關係及產生方式，可參見：https://www.bitira.com/public-key-vs-private-key-what-are-the-key-differences/

[13] 紙錢包 (Paper Wallet) 是一種離線儲存加密貨幣的方法，包含把加密貨幣地址的公鑰和私鑰列印在實體的紙張上。這通常包含了兩種密鑰的 QR Code，透過讓用戶掃描代碼，而不是手動輸入冗長的字母和數字字串以簡化交易。請參見：https://www.bitget.com/zh-TC/glossary/paper-wallet

(七)、 HD 錢包：分層確定性（HD）錢包[14]能夠生成和管理多個比特幣地址，使用戶可更方便管理資產。HD 錢包使用一個主私鑰來生成多個子私鑰，簡化密鑰管理的過程。

(八)、 安全性建議：為了保護資產，建議用戶定期備份錢包，使用高強度密碼保護錢包，並啟用雙重認證等安全措施，防止資產被盜或遺失。

(九)、 使用說明：錢包的使用說明提供生成比特幣地址的具體步驟和注意事項，並強調在生產環境中使用某些工具的風險，建議用戶謹慎操作。

[14] 分層確定（Hierarchical Deterministic，簡稱 HD）錢包是一種基於數學原理的錢包結構，它允許使用者生成無限多的私鑰和公鑰，並且可以有效地備份和恢復錢包資訊。與傳統的錢包不同，分層確定錢包使用一組種子（Seed），通常是一組 12、18 或 24 個單詞的助記詞，通過一個獨特的演算法生成所有的私鑰和公鑰。請參見：https://help.coolwallet.io/zh-TW/support/solutions/articles/151000024211-%E4%BB%80%E9%BA%BC%E6%98%AF%E5%88%86%E5%B1%A4%E7%A2%BA%E5%AE%9A%E6%80%A7-hd-wallet-%E9%8C%A2%E5%8C%85-

六、Cryptocurrency Wallets: The Importance of Private Keys and Seed Phrases （虛擬貨幣錢包：私鑰與助記詞之重要性）

本課程有助於深入理解私鑰和助記詞在加密貨幣管理中的重要性，以及如何有效保護及管理前揭關鍵資訊。

私鑰的重要性： 私鑰是用於控管特定加密貨幣地址的唯一密碼。每個加密貨幣地址都有一個對應的私鑰，可用於簽署交易，證明擁有者對該地址資產的所有權。如果私鑰遺失或被盜，則無法再控管該地址上的資金，也意味資產將永久無法恢復。

(一)、 助記詞的功能： 助記詞（通常由 12 到 24 個隨機單詞組成）是用來生成和恢復整個加密貨幣錢包的備份。當用戶首次設置錢包時，系統會生成一個助記詞，這個片語可以用來恢復所有與該錢包相關的私鑰和地址。這就像是虛擬資產的備用鑰匙，確保用戶在設備遺失或損壞時仍能訪問資產。

(二)、 行動錢包： 行動錢包是專為智慧型手機設計的加密貨幣錢包，允許用戶隨時隨地進行交易。此類錢包通常提供便捷的用戶界面，方便用戶快速發送和接收加密貨幣。然而，行動錢包的安全性相對較低，因為手機可能被盜或遭受惡意軟體攻擊。

(三)、 紙錢包： 紙錢包係將私鑰和公鑰以印刷或手寫的方式記錄下來的儲存方法。此方法提供一種離線的物理儲存選擇，能夠有效防止駭客攻擊。然而，紙錢包的缺點是如果紙張損壞或遺失，則無法恢復資產。

(四)、 無法恢復的損失： 如果用戶遺失私鑰或助記詞，將無法恢復其加密貨幣資產。這與現實生活中遺失現金的情況相似，將無法找回，故妥善保管前揭資訊非常重要。

(五)、 最佳實踐： 在執法行動中，確保有見證人在場是非常重要的，可以避免任何潛在的法律風險。此外，應該在執行前諮詢法律顧問，以確保所有執行動作的合法性，並需注意遵循相關法律及規定。

(六)、 保護助記詞： 助記詞應以防止篡改的方式存放，例如使用密封信封或安全儲存設備，以確保助記詞的完整性，防止未經授權者取得。

(七)、 區塊鏈交易歷史的保存： 在執法行動中，獲得所有相關區塊鏈交易的完整記錄是必要的，以建立清晰的證據鏈，確保資金的合法性及來源。

(八)、 資金轉移： 在法律允許情況下，應儘快將資金轉移到自己控制的錢包中，以確保資金安全，防止法律程序中發生任何風險。

(九)、 執法行動的步驟： 在執法行動中，應先進行初步評估，確保加密貨幣的安全，在適當的時候將資金轉移到受控地址，此有助於確保資金的安全及合法性。

七、《Ethereum 101》以太坊 101

本課程涵蓋以太坊的基本概念、技術架構及其在區塊鏈生態系統中的重要性。

(一)、 以太坊基礎知識：以太坊為開放的區塊鏈平台，於 2015 年由 Vitalik Buterin 創立，主要目的是支持智能合約[15]（Smart contract）及去中心化應用（DApps[16]）。以太坊的核心是以太坊虛擬機（(The Ethereum Virtual Machine, EVM），為一個去中心化的計算環境，允許開發者在其上編寫和執行代碼。EVM 能夠執行任何代碼，使以太坊成為一個靈活的開發平台。

(二)、 以太坊與比特幣的比較：以太坊和比特幣是兩種主要的加密貨幣，但目的及功能有所不同。比特幣主要旨在作為價值儲存和交易媒介。反之，以太坊不僅是一種加密貨幣（ETH），也是一個支持智能合約的平臺，可供執行更複雜的交易和應用程序。以太坊的區塊生成時間約為 12 秒，而比特幣則約為 10 分鐘，故以太坊在交易速度上更具優勢。

(三)、 以太坊的帳戶類型：以太坊有兩種主要的帳戶類型：

1. 外部帳戶（Externally Owned Account, EOA）：由用戶的私鑰控制，能發送交易和管理資產。每個 EOA 都有一個公鑰和私鑰，公鑰用於接收資金，私鑰則用於簽署交易。
2. 合約帳戶：由智能合約代碼控制，能執行合約邏輯並與其他帳戶互動。合約帳戶的代碼通常用 Solidity 或 Vyper 編寫，並編譯為 EVM 位元組碼。

(四)、 智能合約的運作：智能合約係自動執行的合約，當特定條件滿足時，合約中的代碼會自動執行，消除了中介的需求，提高了交易的透

[15]智能合約(Smart Contracts)是區塊鏈中制定合約所使用的特殊協議，這是一種自動執行的合約，將雙方的協議條款寫入代碼中。請參閱：https://rich01.com/what-is-smart-contract/

[16] Dapp 的全名是去中心化應用程式（Decentralized Application），相對於過往運行在中心化服務器的 App，Dapp 的程式部署在分佈式的網絡上，所有的數據皆公開透明且不可篡改。可參見：https://www.blocktempo.com/about-dapp-n-things-you-need-to-know/

明度和安全性。智能合約的代碼在以太坊區塊鏈上運行，任何人都可以檢查其邏輯，使合約的執行過程公開透明。

(五)、 以太坊的層級 2 解決方案：層級 2 解決方案是為了提高以太坊普及性及交易速度而設計的技術。這些解決方案在主鏈之外處理交易後，將結果提交回主鏈，從而減少交易費用及提高處理速度。常見的層級2解決方案包括Rollups（將多個交易打包在一起）和Plasma（創建子鏈以處理交易）。

(六)、 以太幣的單位和面額：以太幣（ETH）是以太坊的原生加密貨幣，並且有多種面額。以太幣最小的單位是 Wei，1 ETH 等於 10^18 Wei。這些不同的單位使進行小型交易時更加方便，並能夠支持各種規模的交易。

(七)、 以太坊上的代幣類型：以太坊支持多種代幣標準，主要有三種：

1. ERC-20：可替代代幣，所有代幣之間是相同的，通常用於發行新的加密貨幣。
2. ERC-721：非可替代代幣[17]，每個代幣都是獨特的，常用於數字藝術和收藏品。
3. ERC-1155：混合型代幣，允許在同一合約中定義可替代和非可替代代幣，這使得開發者能夠在一個合約中管理多種代幣。

(八)、 去中心化應用（DApps）：DApps 是運行在以太坊區塊鏈上的應用程式，利用智能合約實現去中心化的功能。這些應用程式可涵蓋各種領域，包括金融（DeFi）、遊戲、社交媒體等，並且通常具有開放原始碼的特性，使任何人都可以參與開發和改進。

(九)、 以太坊的共識機制：以太坊最初使用工作量證明（Proof-of-Work, PoW）作為共識機制，需要礦工進行計算以驗證交易。隨著以太坊 2.0 的推出，將轉向權益證明（Proof-of-Stake, PoS），此種機制更具持續性，並能夠提高網路的效率及安全性。PoS 允許用戶通過質押以太來幣參與網路的驗證過程，可減少能源消耗。

[17] 國內常稱之為非同質化代幣（Non-Fungible Token，簡稱：NFT）

(十)、 以太坊的未來發展：以太坊社區持續致力於改進及擴展平台，包含升級以太坊 2.0 以解決可擴展性和安全性問題。這些升級將使以太坊能處理更多交易，降低交易成本，進一步促進去中心化應用的發展。隨著技術進步及生態系統擴展，以太坊有潛力成為全球去中心化應用的主要平台。

八、 Money Laundering Typologies（洗錢類型）

本課程概述洗錢的基本概念及洗錢在加密貨幣環境中的具體情況，強調合規性和國際合作的重要性。

(一)、 洗錢定義： 洗錢是指將非法獲得的資金（如毒品販賣、詐騙等）轉化為看似合法的資金。這一過程通常分為三個階段：處置（Placement）、分層（Layering）及整合（Integration）。處置階段，犯罪者將現金或資產轉入金融系統；在分層階段，通過多次交易掩蓋資金來源；在整合階段，資金被重新引入經濟體系，而外觀看似合法。

(二)、 加密貨幣的角色： 加密貨幣如比特幣（Bitcoin）和以太坊（Ethereum）因具備去中心化和匿名性特性，成為洗錢活動的理想工具。加密貨幣允許用戶在無需中介機構情況下進行交易，從而降低被監管機構追蹤的風險。

(三)、 常見的洗錢方法：

1. 空殼公司：犯罪者設立虛假公司掩蓋資金流動，此類公司通常並無實際業務運作。
2. 離岸帳戶：利用低度監管或無監管的國家開設帳戶，將資金轉移到這些帳戶中隱藏資金來源。
3. 加密貨幣混合服務：此類服務將用戶的加密貨幣與其他用戶的資金混合，使得追蹤資金來源變得困難。

(四)、 加密貨幣交易所的合規要求： 許多國家要求加密貨幣交易所遵循「了解你的客戶」（KYC）和反洗錢（AML）法律規定。此類法律要求交易所於開設帳戶時驗證客戶身份，防止洗錢活動的發生。

(五)、 轉帳規則（Travel Rule[18]）： 要求在超過 1,000 美元的交易中，交易所必須共享客戶資訊，包含發送者和接收者的身分，有助增強交易透明度，減少洗錢發生的風險。

[18] FATF's Travel Rule (or Recommendation 16) requires VASPs to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers. This is a key AML/CFT measure that enables VASPs and financial institutions to carry out effective sanction

(六)、 國際合作： 鑑於洗錢活動往往跨越國界，各國間的情報共享機制變得十分重要。國際組織如金融行動特別工作組（FATF）均致力促進各國在打擊洗錢和資恐方面的合作。

(七)、 隱私幣（Privacy Coins）的風險： 隱私幣如 Monero 和 Zcash 提供更高的匿名性，使得追蹤交易變得更加困難[19]。此種貨幣的設計旨在保護用戶的隱私，但也因此被犯罪者用於進行洗錢活動。

(八)、 賭博網站合規性問題： 許多離岸賭博網站缺乏有效的合規控制，因而成為洗錢活動的高風險場所。犯罪者可透過網站將非法資金轉換為看似合法的盈利。

(九)、 技術手段的演變： 隨著技術的進步，洗錢手法也在不斷演變。犯罪者利用新技術（如智能合約和去中心化金融）掩蓋其活動，使得監管機構面臨更大的挑戰。

(十)、 防範措施： 政府和金融機構應加強監管，提升合規性要求，利用技術手段（如區塊鏈分析工具）追蹤及打擊洗錢活動，而提升公眾教育及意識亦為防範洗錢的重要措施。

---

screening and detect suspicious transactions. 可參：https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Targeted-Update-Implementation-FATF%20Standards-Virtual%20Assets-VASPs.pdf.coredownload.pdf 。在我國的情況，業已將轉帳規則訂入「提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法」第 7 條，然依照同辦法第 18 條：「本辦法除第七條由本會另定施行日期外，自中華民國一百十三年十一月三十日施行。」，可知轉帳規則在我國尚未施行。

[19] 可參見：https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/

九、 Seizing Cryptocurrency（扣押虛擬貨幣）

本課程係對加密貨幣扣押過程的全面理解，幫助執法機關在實務上可有效運作。

(一)、 組建專業團隊：進行加密貨幣扣押時，組建專業團隊具有關鍵重要性。團隊應包括資訊工程師、腳本語言（Scripting language[20]）工程師及人工智慧專家等技術專家，以便有效地篩選及分析大量資訊，確保所有相關訊息都能被充分利用。這些專家能幫助執法人員理解和及理複雜的資訊，提高扣押的成功率。

(二)、 加密貨幣錢包專家：團隊中應包括熟悉各種加密貨幣錢包、助記詞和私鑰的專家。因為了解不同類型的錢包及其運作方式對於成功扣押極為重要，這些專家能幫助執法人員識別和控管被扣押的數位資產，確保正確處理敏感的數位資訊。

(三)、 法律要求：進行數位資產扣押通常需要法院令狀或判決，而此類扣押通常與非法活動（如詐騙或洗錢）相牽連，執法機關必須遵循法律程序，獲得必要的授權，始能確保所有執法行為的適法性，避免未來遭遇法律挑戰。

(四)、 數位搜索令狀：執法機關需要獲得搜索令狀以取得第三方平台商（如亞馬遜、Google 和社交媒體平台）所持有的資訊，蓋令狀是確保合法性和證據能力的關鍵步驟，避免未經令狀授權而取得資訊產生證據被排除的法律效果。

(五)、 證據完整性：在扣押過程中，必須確保對加密貨幣資產、私鑰和相關數位證據的正確處理、文檔記錄和安全儲存，以維持證據鏈及法律程序為法律所允許，包括詳細記錄每一步的操作，以便在法庭上能證明證據的來源及完整性。

(六)、 區塊鏈取證專家：在複雜的加密貨幣扣押案件中，聘請區塊鏈取證及加密貨幣分析專家是最佳執法方式。這些專家能提供深入的技術

[20] 腳本語言(Scripting Language)又譯手稿語言，源自系統管理者將一些例行的管理工作編寫於一個文字檔，稱為手稿(Script)，執行這個 Script，就可將這一批工作一次完成。可參：https://www.cc.ntu.edu.tw/chinese/epaper/0050/20190920_5003.html

分析，幫助執法機關追蹤金流和交易歷史，對於理解犯罪活動的全貌十分重要。

(七)、 持續更新知識：隨著加密貨幣技術的快速發展，執法機關的專業人員必須不斷更新他們的知識和技能。參加培訓計劃、在線資源和行業論壇是保持競爭力的關鍵，這樣他們才能掌握最新的技術和法律發展。

(八)、 資訊科學家角色：資訊科學家在分析證據和產生新見解方面，具有重要作用。他們使用商業智慧軟體（如 Metabase 和 Jupyter Notebook）分析資訊，幫助執法機關做出正智決策，而分析內容亦可揭露潛在的犯罪模式及資金流動。

(九)、 K9 數位證據犬[21]：專門訓練的 K9 犬可以幫助檢測和找到電子設備，有助於扣押程序執行。特別是在大型或複雜執法環境下，K9 犬隻能在現場快速定位可能的數位證據，增強執法效率。

(十)、 案例研究：通過分析具體案例（如 Jimmy Zhong 的案例），執法機關可以學習如何有效進行加密貨幣扣押[22]。這些案例提供實際的經驗教訓，幫助改進未來的操作執行，提供給其他執法機關參考。

[21] Electronics Storage Device Detection K9，縮寫為 K9 ESD，這類警犬對於電子產品儲存裝置（Storage Device）上的化學物質「三苯基氧化膦」（Triphenylphosphine oxide ，TPPO）極度敏感，電子產品偵測犬能在犯罪現場搜尋藏匿之電子產品，像是 SD 卡、手機、硬碟、隨身碟、甚至是離線儲存虛擬貨幣的冷錢包（Cold Wallet）。目前亞洲僅 3 隻，臺灣有一隻名叫「Wafer」，是由美國非營利組織「地下鐵路行動（Operation Underground Railroad, O.U.R.）」捐贈我國警政署。可參見：
https://www.facebook.com/taiwaninla/posts/692445339596013?ref=embed_post

[22] 我國法務部委託臺灣高等檢察署建置「檢察機關查扣虛擬資產監管平台」已於 113 年 4 月 15 日正式上線，https://www.moj.gov.tw/2204/2795/2796/204533/post

十、FATF Standards for Virtual Assets and VASPs （FATF 對於虛擬資產及虛擬資產業者之標準）

重點強調虛擬資產在全球金融體系中的重要性，以及各國因應相關風險所需採取的措施。

(一)、 資產返還：國家必須建立法律框架，以便能追蹤、扣押和沒收虛擬資產，包括確保有機制管理扣押之虛擬資產，能在國際上協助其他國家進行資產的凍結和沒收（建議事項 4）。

(二)、 國內合作：各國應確保其 AML/CFT 策略包含虛擬資產的濫用考量，建立有效的國內訊息共享機制，促進各機構之間的合作，增強對虛擬資產相關風險的應對能力。

(三)、 國際合作：金融情報單位（FIUs）和執法機關（LEAs）應具備使用正式和非正式國際合作機制的權力，包括在涉及加密貨幣的案件中進行相互法律協助（MLA）和引渡（建議事項 37-40）。

(四)、 客戶盡職調查：虛擬資產服務提供商（VASPs）必須進行客戶盡職調查，包括識別客戶的身份、了解其業務性質及資金來源，以防止洗錢及資恐問題（建議事項 10）。

(五)、 政治公職人員：VASPs 需採取合理措施確認其客戶或受益人是否為政治公職人員（PEP），並根據風險評估採取相應的監控措施（建議事項 12）。

(六)、 新技術的要求：FATF 於 2019 年擴展了全球 AML/CFT 要求至虛擬資產，要求各國對 VASPs 進行監管，確保其遵守相關反洗錢和反資恐措施（建議事項 15）。

(七)、 內部控制：VASPs 必須建立內部控制系統，實施反洗錢/反資恐計劃，包括任命合規官員以確保遵守相關法規。

(八)、 可疑活動報告：VASPs 必須具備識別可疑活動的能力，向金融情報單位報告可疑交易（建議事項 20），以助於及早發現潛在的洗錢或資恐活動。

(九)、 合規性評估：截至 2024 年 10 月有 27 個亞太反洗錢組織（APG）成員已根據修訂的 R.15 要求進行合規性評估，顯示各國在實施 FATF 建議方面有具體進展。

(十)、 實施方法的多樣性：APG 成員在實施修訂的 R.15 要求上採取多種方法，包括禁止某些活動（如孟加拉國、柬埔寨等）、建立監管框架（如加拿大、印尼等），亦有未建立任何框架的國家（如不丹）。前揭不同國家所採取的不同方式，反映各國在應對虛擬資產風險的不同策略及挑戰。

十一、 Presentation on Non public FATF report on crypto investigation（FATF 對於虛擬資產調查之非公開報告）

本堂課提供加密貨幣調查的全面理解，強調當前金融環境中有效應對風險及犯罪的必要性。

(一)、 風險評估：風險評估是識別及分析加密貨幣交易中潛在風險的過程。評估不同類型的加密貨幣、交易平台和用戶行為，以了解加密貨幣可能被用於洗錢、詐騙或其他非法活動的風險。

(二)、 金融情報：金融情報是指收集和分析金融資訊以識別可疑活動的過程。金融情報在打擊金融犯罪中非常重要，可幫助執法機關及時發現及因應潛在的犯罪行為。

(三)、 調查技術：有效的調查技術包括使用資訊分析工具、區塊鏈分析軟體及其他技術手段，以追蹤可疑交易，幫助調查人員識別資金流向及來源，並揭示潛在的犯罪網路。

(四)、 資產返還：資產返還指從犯罪活動中追回被盜或非法獲得的資產。此部分通常涉及法律程序及國際合作，以確保資產能有效追蹤及返還。

(五)、 國內合作：國內合作指各國內部不同機構（如執法機關、金融監管機構和稅務機關）之間的協作，此種合作可促進訊息共享，提高打擊金融犯罪效率。

(六)、 國際合作：國際合作指不同國家之間在打擊跨國金融犯罪方面的協作，包括共享情報、協調調查及執行法律，以因應全球性金融犯罪的挑戰。

(七)、 法律框架：法律框架涉及現有法律及法規對加密貨幣的適用性，包括分析如何將現有的反洗錢和反資恐法律適用於加密貨幣交易，及哪些法律需要進行修改以適用於新興技術。

(八)、 監管挑戰：監管挑戰指監管機構在監管加密貨幣市場時所面臨的困難，包括技術快速變化、缺乏透明度及全球性特性，使監管更趨複雜。

(九)、 教育與培訓：教育與培訓指對執法機關和相關人員進行有關加密貨幣及其風險的教育，有助於提高前揭人員的識別和應對能力，更有效打擊金融犯罪。

(十)、 透明度與合規性：提高透明度和合規性指促進加密貨幣交易的透明度，確保所有交易都遵循反洗錢和反資恐的規定，有助於減少非法活動，增強公眾對加密貨幣市場的信任。

十二、　心得及建議

(一)、　區塊鏈上的虛擬資產應用發展日新月異，虛擬資產在發展之初，因各國尚不熟悉，故無規範須遵守 KYC、AML，可以完全匿名以及天文數字量的資訊等特性，為洗錢、詐欺及涉及加密貨幣金融犯罪提供一個接近完美的平台。因此，處理虛擬資產相關案件非常具有挑戰性的。在案件中，如何成功利用大數據分析讓犯罪者入獄，關鍵在於如何獲取大數據並將其轉化為檢察官、法官易於理解的故事，此種能力可能是案件得以成功的最重要因素之一。處理大數據的能力一定要有調查員、工程人員、程式設計師的團隊來建立解決方案。講者在課堂中亦分享其任職於 FBI 時，從 GOOGLE、AMAZON、APPLE、BINANCE 等大型企業取得原始大數據資料時，如何建立自己團隊，著手針對不同的企業撰寫程式，把不同格式電腦資料及天文數字般資訊進行整理，成為一般人可理解的文字，再轉化為檢察官、法官易於理解的故事。簡而言之，堅實及專職的資訊專業人員團隊，在虛擬資產調查案件上是不可缺的。對於檢察官的專業知能而言，理想上如果可以隨著日新月異的區塊鏈知識而持續學習精進，瞭解相關技術知識，才能夠面對、追查使用最新技術洗錢的犯罪集團。但是在目前實務上第一線偵查檢察官的工作負荷繁重下，實在很難期待檢察官可以隨時跟上最新的技術。不過，目前臺灣高等檢察署內業成立專責的幣流分析事務官小組[23]，並分配商用工具給部分地檢署使用，此外，警方及調查局也有對於幣流追蹤做教育訓練，故或許檢察官無須親自操作區塊鏈分析工具來追查幣流，而可委由專責的檢事官小組、警方、調查局分析，但檢察官仍然必須具備區塊鏈、虛擬貨幣之基礎知識，始能有效理解虛擬貨幣犯罪態樣、與檢事官、執法機關溝通，並在法庭上，以簡單的方式說明給法院理解。

[23] 虛擬貨幣運用區塊鏈的技術，具有去中心化及追查不易的特性，常淪為犯罪者隱匿不法金流的工具，臺灣高等檢察署在 110 年起購買國際執法單位使用的虛擬貨幣幣流分析工具 CA、TRM，成立虛擬貨幣金流分析小組，進行幣流分析。自 111 年 3 月 1 日起至 113 年 9 月 25 日止，高檢署協助地檢署幣流分析案件達 563 件，其中詐欺案件為 458 件，佔比達 81.3%，可參見：https://www.ftnn.com.tw/news/321382

(二)、 要培育檢察官具有區塊鏈、網路犯罪、數位科技的基礎知識實為當務之急，蓋現今的各種犯罪都可能使用最新的科技、通訊技術、網路等當作工具，檢察官如果不具備基礎知識，則無法跟上犯罪集團的腳步，遑論與之對抗。以荷蘭檢察官為例，就網路犯罪相關之教育訓練，就開設初、中、高階課程，供荷蘭檢察官教育訓練[24]。而我國就檢察官的數位犯罪偵查能力的教育訓練，宜多投入資源，才能培養臺灣的檢察官具備基礎的數位科技知能，用以對抗日新月異的犯罪集團。例如可以仿效法務部金融證照班，分為初、中、高階，給予檢察官進修數位、網路、科技相關知識之教育訓練機會。

(三)、 講者亦提及目前區塊鏈上的虛擬資產調查，以荷蘭之執行經驗最佳，建議各國若有機會，可與荷蘭團隊進行交流或合作，荷蘭團隊有先進資訊及網路團隊，可分析區塊鏈上混幣器之相關資訊。講者與荷蘭專家們共同研究區塊鏈上混幣器數據，荷蘭團隊在此部分取得許多重要進展，不僅提高對數據的理解，也學會將之應用於實際案例中的方式，在追蹤及分析數據時能更全面地了解其運作模式和相關活動，有助於在打擊金融犯罪方面獲得更大的成就。荷蘭團隊的經驗，應值得我國借鏡及參考。

[24] 此節是筆者之一羅韋淵於 2023 年 9 月赴英國倫敦，參加國際檢察官協會第 28 屆年會擔任報告人，與荷蘭檢察官之交流所得。

十三、　訓練課程照片與交流

(一)、　劉怡君檢察官於課程中，對於虛擬資產相關問題發言。

(二)、　羅韋淵主任檢察官向與會的各國檢察官、執法機關人員說明我國法務部所建置之「檢察機關查扣虛擬資產監管平台」之應用情形，及臺灣執法機關查扣虛擬貨幣之實務作法。

(三)、　周官緯檢察事務官在課堂中對於虛擬資產相關問題發言。

(四)、　劉怡君檢察官與課程講師合影。

(五)、　周官緯檢察事務官與課程講師合影。

(六)、　羅韋淵主任檢察官領取結訓證明

(七)、 筆者三人在 FATF Training Institute 前合影。

(八)、 FATF 的訓練及研究機構（FATF Training and Research Institute TREIN）於 2016 年 9 月開幕，位在釜山國際金融大樓（Busan International Finance Center）的 53 樓，教室內部及窗外風景


BUSAN
INTERNATIONAL
FINANCE CENTER


FAIF Standards Training Room