

出國報告（出國類別：進修）

虛擬貨幣犯罪之法制及偵查實務研究

服務機關：桃園地方檢察署

姓名職稱：劉昱吟檢察官

派赴國家/地區：德國

出國期間：109年10月27日至110年10月26日

報告日期：111年1月25日

摘要

比特幣，第一個加密貨幣從 2008 年出現以來，帶動了金融科技及加密產業的蓬勃發展，同時也衝擊的傳統的金融機構與交易方式。因為虛擬貨幣的新穎性以及精密數學演算法等各項深奧技術，讓虛擬貨幣一直自帶神秘的色彩。虛擬貨幣的設計，允許使用者在幾分鐘內完成任何規模的價值交易，其中無需金融機構的中介或協助，也免去了政府的干預。加密貨幣模型依賴系統中以電腦維護的分散式帳本技術，以保持其最新狀態，並以此防止詐欺，並用代碼替換了使用者的個人姓名，而以使用者假名參與交易。人們對於加密貨幣有限的認識，以及使用者以假名進行交易所提供的匿名程度，疊加去中心化、無地域性、電子化快速性等特質，被不法分子視為一個進行洗錢的理想機會。這些不法分子或犯罪集團，可以通過去中心化及匿名性的加密貨幣系統，隱藏和掩飾其犯罪所得來源及去向。儘管隨著時間推演，人們對虛擬貨幣的認識不斷增加，但目前世界各國對虛擬貨幣的理解、使用和監管，仍然是相當有限的。隨著時間，虛擬貨幣也從原本法外之地，到低度的監管，再逐步增加監理的密度。然而，虛擬貨幣如何監管，如何在防弊及興利中取得平衡，一直都是難解的課題。本文先

從虛擬貨幣之特性、加密技術、加密貨幣參與者的說明開始，接著介紹歐盟各個洗錢防制指令，主要著重於歐盟第 4 個及第 5 個洗錢防制指令。另外說明第 6 個洗錢防制指令以及尚未完成立法程序的加密資產市場規則。再來，介紹我國目前對加密貨幣及交易平台之監理情形，將從探討加密貨幣的合法性開始，隨後介紹加密貨幣的定性上主管機關的態度以及司法實務的看法，繼而提出目前我國最新的洗錢防制及打擊資助恐怖主義規範，另輔以司法實務上虛擬貨幣所涉犯罪的統計，最後提出結論。

目錄

壹、前言

貳、虛擬貨幣之特性

一、法定貨幣、虛擬貨幣、加密貨幣

二、加密技術

三、加密貨幣的參與者

四、加密貨幣與洗錢防制的關係

參、歐盟對虛擬貨幣之監理-以洗錢防制為核心

一、防制洗錢金融行動工作組織 (Financial Action Task Force)

二、歐盟洗錢防制指令的建立

三、第 4 號及第 5 號洗錢防制指令 (the 4th and 5th Anti-Money Laundering Directive)

四、第五個洗錢防制指令未解決的問題

五、歐盟未來的發展

肆、我國目前對加密貨幣及交易平台之監理情形

一、加密貨幣的合法性

二、加密貨幣的定性

三、洗錢防制及打擊資助恐怖主義規範

四、我國虛擬貨幣所涉犯罪之統計

伍、結論

壹、前言

2008年10月，化名為「中本聰」(Satoshi Nakamoto)之人，發表了一篇名為「比特幣：一種點對點數位現金系統」(Bitcoin: A Peer-to-Peer Electronic Cash System)的研究報告¹。在這篇報告中，使用區塊鏈(Blockchain)作為加密技術的比特幣，自此橫空出世，開啟了虛擬貨幣的濫觴。之後，以相同於比特幣所使用的區塊鏈加密技術，出現以太幣(Ethereum)、泰達幣(Tether、USDT)萊特幣(Litecoin)、門羅幣(Monero)等各式各樣的加密虛擬貨幣。虛擬貨幣的特質強調去「中心化」(decentralized)，其出現與2008年金融海嘯後對於傳統金融機構的不信任也有關。比特幣(Bitcoin)，是第一個、也是目前最廣為人知也最廣受歡迎的加密貨幣。

雖然，至少到目前為止的態勢，加密貨幣尚不太可能取代傳統的法定貨幣，但加密貨幣卻已顛覆長期以來的傳統金融支付系統，尤其

¹ Nakamoto S., Bitcoin: A Peer-To-Peer Electronic Cash System, 2008, <https://bitcoin.org/bitcoin.pdf>。
(最後瀏覽時間 2021 年 12 月 4 日)

是在全球性的金融支付交易。加密貨幣可以規避各國貨幣相關規範之障礙，並且在匯率上取得優勢，在交易市場上形成一個一個免費又快速流動的交易系統。

由於虛擬貨幣具有去「中心化」及「匿名性」之特質，使各國司法機關及警調單位不易追查其來源、去向，因此從事不法犯罪行為者，濫用虛擬貨幣作為犯罪支付工具，或將其作為將犯罪所得轉出之洗錢工具。再者，又因為新興技術所帶來的神秘感，以及各類虛擬貨幣具有總數定量之特性，容易成為投機客的炒作客體。也因為定量特性，虛擬貨幣在市場上的價格波動極大，往來常為詐欺犯罪、不法吸金者所青睞的主題。

筆者於任職於臺灣桃園地方檢察署企業犯罪組檢察官期間，當時所處理與虛擬貨幣有關的案件，絕大多數是作為詐欺或吸金手法，也就是單純以虛擬貨幣的神秘性與價格大幅波動的投機性質來吸引投資的詐欺或吸金案件。也有不少是不肖份子，透過架設平台或軟體收受存取虛擬貨幣，在其等取得虛擬貨幣的私鑰後，即惡意使平台無法登入等詐欺取財案件。另外，在 2021 年「代購虛擬貨幣」案件類型

呈現急速增加的狀態（行為人請被害人購買比特幣等虛擬貨幣的案件）。例如，某詐欺集團成員假冒為在阿富汗或以色列等戰地工作的美國軍醫等專業人士，向被害人誣稱因在戰地受傷或退休想要到臺灣定居等幌子，向被害人表示需要一筆保證金或隔離費用等理由，委請被害人代其購買 USDT 或比特幣，並指示被害人透過中介第三人向貨幣交易所代買 USDT 或比特幣的詐欺案件。類似案件多半僅能追查至透過被害人匯款所至的代買手的新臺幣金融帳戶即止步。此類詐欺案件的金流，不再如以往傳統詐欺案件的金流最終流向一個有真實姓名年籍資料的本國金融帳戶，因此增加了追查資金流向的難度，也就更難破獲這類的詐欺集團。

目前加密貨幣在我國並非貨幣，亦非金融監督管理委員會（下稱金管會）核准發行的金融商品，目前較常作為「類金融投資商品」，在我國銀行並無法兌換、收受虛擬貨幣。也就是說在我國目前的法制狀態，加密貨幣並非支付工具，但斟酌加密貨幣在國際間亦得做為支付工具，因此考量虛擬貨幣潛在作為洗錢工具之風險，洗錢防制法已將「虛擬通貨平台及交易業務事業」納入洗錢防制範疇，並指定金管會擔任此事業的防制洗錢主管機關，但僅為洗錢防制目的，並不涉及

其產業治理、業務經營、消費者保護等議題。而藉由加密貨幣進行詐騙或洗錢等犯罪行為，因涉及刑事責任，則由司法機關認定具體事實依法處理。

本文擬先介紹虛擬貨幣、加密貨幣等概念，將聚焦在加密貨幣的洗錢防制為核心，探討目前在歐盟法下之監理情形，另試著提出建議代結論。

貳、 虛擬貨幣之特性

一、 法定貨幣、虛擬貨幣、加密貨幣

定義法定貨幣 (Legal Tender, Fiat Money, Flat Money) 並不困難，一般來說就是由「政府」所發行，法律上賦予其強制流通力，得以做為「法定清償工具」之貨幣。依據我國中央銀行法第 13 條第 2 項規定「本行發行之貨幣為國幣，對於中華民國境內之一切支付，具有法償效力」。因此，我國的法定貨幣是由中央銀行發行，而具有法償之效力。

虛擬貨幣 (Virtual Currency) 的概念亦不難理解，並且在生活

中遠比吾人想像中還常見。所謂虛擬貨幣是指非由政府發行，而以數位貨幣形式存在的貨幣²。因此廣泛來說，虛擬貨幣包括了任何遊戲裡面的貨幣、線上交易的代碼等等。歐洲中央銀行（European Central Bank，簡稱 ECB）在 2015 年提出「虛擬貨幣是一種以數位形式儲存價值，不是由中央銀行、銀行等金融機構或電子貨幣機構所發行的，在某些情況下，可以用作貨幣的替代品³」。由歐洲中央銀行此一定義可以知道，歐洲中央銀行並不承認虛擬貨幣是貨幣。防制洗錢金融行動工作組織（Financial Action Task Force，簡稱 FATF）根據歐洲中央銀行在 2012 年對虛擬貨幣提出定義，將虛擬貨幣定義為「……一種以數位形式呈現的價值，可以數位方式交易，並且在功能上是(1) 交易媒介；和/或 (2) 記帳單位；和/或 (3) 可用來儲存價值，但在任何司法管轄區不具有法定貨幣地位（也就是不具法定清償效

² 劉少軍，金融法學，頁 71，第一版。

³ “virtual currency is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.”參 European Central Bank, Virtual currency schemes—a further analysis, February 2015, 頁 4, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>, (最後瀏覽時間 2021 年 12 月 4 日)

力) ……⁴」。因此，根據防制洗錢金融行動工作組織的定義，也不承認虛擬貨幣是貨幣，而同歐洲中央銀行所定義的「一種以數位化方式儲存價值的工具」。

虛擬貨幣是數位貨幣 (Digital Currency) 的子項，加密貨幣 (Cryptocurrency) 又是虛擬貨幣下的子項。目前狹義上，吾人在談及虛擬貨幣的監理問題，大多是指所謂的「加密貨幣」，而本文之後的探討，亦只會討論虛擬貨幣的「加密貨幣」。加密貨幣利用加密技術和加密金鑰 (Encryption Keys) 來確保加密貨幣的價值和交易訊息是以安全的形式儲存及傳輸。通過使用特定的數學演算法產出數據結構，將其加密為不可讀的模式，或者稱為「加密文本」的格式，因而只能由擁有加密金鑰的另一個人「解密」⁵，藉由這樣方式來確保只

⁴ “...a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction...” 參 FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, June 2014, <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, 頁 4。(最後瀏覽時間 2021 年 12 月 4 日)

⁵ 參 Faulkner J., Getting started with Cryptography in NET, February 2016, 頁 5。

有擁有加密金鑰的個人或企業才能接收、讀取和處理數據或交易，也藉此機制確保交易和參與者的真實性。這種跨多個儲存資料庫的共享資料庫用的技術即為「分散式帳本技術」(distributed ledger technology)⁶。在2008年「中本聰」加密貨幣的研究報告中，首次提出使用「區塊鏈」作為加密技術的比特幣，即比特幣所使用的分散式帳本技術為「區塊鏈」。

二、 加密技術

要開始談到加密貨幣的交易前，必須先講到「加密技術」。在前一個段落已經提到，加密技術最簡化來說就是「分散式帳本技術」。透過精密的數學演算法產出的資料庫來存取、傳輸價值與交易，其中並沒有如銀行等其他中介或權威機關的介入，而是一種密碼學原理，透過加密的點對點網絡 (Peer-to-Peer Network) 技術，進行數位的

⁶ 參 World Bank Group, Distributed Ledger Technology (DLT) and Blockchain, FinTech Note No. January 2017, <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>. 頁 1-28。(最後瀏覽時間 2021 年 12 月 5 日)

交易、移轉、儲存，藉著高深的數學演算法驗證、擔保交易信息的真實性。隨著新交易的進行，信息塊不斷上傳到「鏈」上，特定的驗證和共識機制目的在於確保區塊鏈中包含的信息在添加的那一刻和之後的時刻都不能被篡改。因此，區塊鏈簡化了各種交易的執行，這些交易傳統上由銀行、金融機構等中介機構來做驗證與執行，然而應用區塊鏈的技術，這種「點對點」系統變得可行，消除了金融中介，同時降低交易成本。簡單來說，區塊鏈是一種「去中心化」的方式。因此，吾人談及加密貨幣便會直覺想到：加密貨幣就是一種去「中心化」。「去中心化」是虛擬貨幣最強的優勢之一，同時卻也是目前在管理上最棘手的部分之一。

區塊鏈技術除了用在支付和金融交易的傳輸與驗證以外，還可以應用在不同的領域，例如可以用於醫學的領域來保存紀錄與防止追蹤。然而，這樣去中心化的結果，同時也減少了對政府授權的監督。此外，保密性雖然增強了對使用者的保護，同時卻難以避免地使非法活動的交易變得更加隱蔽。

三、 加密貨幣的參與者

加密貨幣的使用者可以是自然人也可以是法人。使用者取得加密貨幣是出於商業目的，或者在現今大多數情況是作為一種投資目的，遠大於將加密貨幣作為一種支付方式。使用者可以通過多種方式獲取加密貨幣，以下是主要的四類取得方式：

1. 用法定貨幣或其他虛擬貨幣購買加密貨幣。
2. 挖礦。
3. 接受加密貨幣作為工作、禮物、獎勵、捐贈或付款。
4. 自發行者的初次發行或販售而取得。

(一) 加密貨幣的初次發行人 (Initiators of Cryptocurrencies)

加密貨幣的發起人可以是個人或群體⁷。例如，比特幣的發起者可

⁷ Haffke L., Fromberger M., and Zimmermann P., Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, *Journal of Banking Regulation*, 2020, 頁 127。

以建立一個新的區塊鏈並免費贈送⁸。發起人可以通過「初始代幣發行」(Initial Coin Offering, ICO) 出售新創建的代幣。

(二) 挖礦(Miners)

從最字面的意思來看，「礦工」就是在區塊鏈上運用計算能力驗證交易，報酬即是可以無償獲得新開採的加密貨幣。挖礦而無需花錢的參與者。「礦工」通常不會單打獨鬥，而是群體工作，這個群體運用電腦計算機去驗證一組稱為「區塊」的交易，並添加到稱為區塊鏈的支付賬本中。獎勵將通過自動新發行或發行人轉帳而創建。

虛擬貨幣目前未被廣泛接受的其中一個原因，就是挖礦過程中相當「耗電」，估計大約是瑞士全國用電量。這個耗能的結果，與貨幣演進過程目的在避免資源浪費、降低成本的發展，完全背道而馳⁹。

⁸ 同前註，頁 127。

⁹ Krugman, Paul (2018), "Transaction Costs and Tethers: Why I'm a Crypto Skeptic," The New York Times, Jul 31。參楊金龍，虛擬貨幣與數位經濟：央行在數位時代的角色，國立政治大學「金融科技生態系」高峰論壇演講稿，2018年8月。
<https://ws.www.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvMjk1L3J1bGZpbGUvNzcyMi8yODQ2N>

(三) 加密貨幣交易所及其平台 (Cryptocurrency Exchanges (and) Platforms)

加密貨幣交易所為加密貨幣使用者提供兌換服務，通常會從中收取服務費或佣金。加密貨幣使用者透過加密貨幣交易使用法定貨幣出售或購買加密貨幣。加密貨幣交易所的概念很類似股票交易所。加密貨幣交易收取費用的方式，通常可以接受現金、匯款、或加密貨幣。

目前在 Coinmarketcap 上的交易所共有 454 家¹⁰，全球交易量最大、評分最高亦是最眾所皆知的就是幣安 (Binance)，台灣本土的交易所共有 Max Exchange、幣託 (Bitopro、Bitoex)、ACE 交易所等。

論及買賣股票時集中交易的機構：臺灣證券交易所及證券櫃臺買

[jIvYjk2ZmMzMTQtMmUwYS00MzRkLT1hNzAtM2Q0ODM0NzFmZDA5LnBkZg%3D%3D&n=MjAxODA4MDfmpYrnuL3oo4HmvJTorJvoqZ4ucGRm&ico%20=.pdf](https://coinmarketcap.com/zh-tw/rankings/exchanges/)。(最後瀏覽日期：2022 年 1 月 25 日)

¹⁰ 「CoinMarketCap」是目前全球最常被引用的加密貨幣幣價追蹤網站，由 Brandon Chez 於 2013 年 5 月創立，在該網站中針對流量、流通性、交易量以及對所回報之交易量真實性的信心程度，對各加密貨幣交易所進行排名和評分，供加密貨幣使用者使用時參考。
<https://coinmarketcap.com/zh-tw/rankings/exchanges/>。(最後瀏覽時間 2022 年 1 月 8 日)

賣中心，加密貨幣交易所、交易平台的概念很類似與在次級市場上集中買賣股票的台灣證券交易所、證券櫃臺買賣中心。加密貨幣交易所、交易平台的功能，就是讓加密貨幣買賣雙方直接在平台上進行交易的市場。而因為加密貨幣去中心化的特質，所以在加密貨幣交易所的交易，並沒有由第三方或實體監管或處理交易的需要，而幾乎只憑藉著軟體來維護。也就是說，交易平台本身並不從事加密貨幣的交易，也不是由監督、執行交易的機構或公司所運營，交易平台只是作為一種媒介，僅僅只是將買賣雙方聯繫起來進行交易而已。

（四）加密貨幣錢包供應商（Wallet providers）

從望文生義的方式可以得知，加密貨幣電子錢包供應商即為那些為加密貨幣使用者提供儲存、發送、接收加密貨幣的虛擬錢包的供應商，有點類似於銀行帳戶與貨幣間的關係。實際的運作上，加密貨幣的交易是以「假名」來交易，加密貨幣錢包會以公鑰（Public key，可以理解成是「公開的鑰匙」）與私鑰（Private key，可以理解成是一把「私人鑰匙」）的方式來運行。因為在加密貨幣的交易中需要一對加密金鑰，加密貨幣錢包也可以作為加密金鑰的儲存及安全保護。

加密金鑰的公鑰類似於銀行帳號的概念，代表著錢包地址，就像加密貨幣的帳號，網絡使用者都看得到公鑰，可以接收特定類型的加密貨幣，例如接收比特幣就需要一個比特幣地址，錢包能查看與地址關聯的餘額，只要使用者是地址的所有者，就可以在區塊鏈上移動價值。當加密貨幣使用者想要互相移轉加密貨幣時，則需要私鑰來簽署相對應的交易。私鑰則是一種隨機生成的密碼數據，類似於實體交易上銀行帳戶交易密碼的作用，用來證明對加密貨幣的所有權及控制權，進行支付時必須使用私鑰來驗證是加密貨幣的持有者以進行交易。

加密貨幣錢包主要有以下三種分類：

1. 冷錢包 (Cold Wallet、Hardware Wallet)：

冷錢包也被稱為離線錢包或硬體錢包，是指加密貨幣使用者以數位方式持有加密金鑰的物理設備，例如 USB 裝置。冷錢包目前被認為是最安全的儲存方式之一，因為冷錢包沒有連接到網路的加密貨幣錢包，因此駭客相對難以滲透，這個特質讓冷錢包被認為是最安全的提供商。要交易時必須插入實體裝置才能交易，有點類似股票交易上交易憑證的概念。除了要有實體裝置外，通常亦同時設置有對應的軟體，

方便使用者檢視錢包裡即時的資產情況，不會將私鑰至於危險之中。

2. 熱錢包 (Hot Wallet、Soft Wallet)

熱錢包 (或稱軟件錢包) 是利用應用程式連接到加密貨幣使用者所儲存的加密密鑰。與冷錢包相比，連接熱錢包來執行交易會更快更容易，也可以讓使用者快速地檢視或使用持有的加密貨幣。只要在電腦、行動電話等能夠連接上網路設備運行裝置，例如只要下載 App 就可以使用了。因此，不難理解熱錢包比較容易會被犯罪分子所滲透，因為熱錢包是在容易被駭的連接網路的設備生成加密貨幣的私鑰，正因如此相較缺乏安全性，有比較高的駭客入侵風險。

3. 託管錢包供應商 (Custodian Wallet Provider)

託管錢包供應商被定義為「代表其客戶提供服務以保護私鑰、持有、儲存和移轉虛擬貨幣的實體」¹¹。因此，託管錢包供應商不同於

¹¹ “an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.” 參歐盟第 5 個洗錢防制指令 Article 3(d)。

冷、熱錢包，託管錢包供應商的角色反而與金融機構的功能雷同。在本文接下來的段落會繼續討論在歐盟洗錢防制指令，託管錢包供應商與虛擬貨幣交易所，均被認為與金融機構一般應受到監管，而為有遵循洗錢防制相關規範的義務主體。所以，無論是託管錢包供應商或虛擬貨幣交易所，都有義務進行「客戶盡職調查」(Customer Due Diligence)，並在必要時通報「可疑活動報告」(Suspicious Activity Reports)。除此之外，託管錢包供應商和虛擬貨幣交易所都必須在各自的國家或地區註冊。

四、 加密貨幣與洗錢防制的關係

加密貨幣的出現劇烈改變了傳統金融交易的方式，而傳統的洗錢手段也有相應發展和轉變。加密貨幣的性質使得很容易被犯罪分子濫用進行洗錢。首先，使用加密貨幣進行的價值轉移可以是匿名的（加密貨幣的交易部是匿名，但因為是假名交易而有匿名的結果），因此有機會製造金流斷點，使檢調部門難以追查資金的來源、去向或真正的所有者。再者，由於加密貨幣的去中心化性質，缺乏第三方或權威單位來監督交易中的非法活動。最後，加密貨幣交易的快速性，而且

沒有國界，加密貨幣交易相對不受監管或受到較少的監管，不管交易金額的大小，可以在很短的實踐就完成價值的移轉。結合上述加密貨幣交易的特徵，也就是匿名性、去中心化、快速、無國界以及沒有或較低密度的監管，加密貨幣交易被視為洗錢份子的理想機會。

參、歐盟對虛擬貨幣之監理-以洗錢防制為核心

一、防制洗錢金融行動工作組織（Financial Action Task Force，FATF）

早期為了解決利用金融系統將販毒所得等非法資產合法化此日益嚴重的洗錢問題，1989年7月在巴黎舉行的G7高峰會，成立了防制洗錢金融行動工作組織（以下簡稱為FATF）。FATF是一個跨政府的國際組織，職司建立各種標準，防制洗錢、打擊資助恐怖分子及大規模毀滅武器擴散資金的募集，以及其他對國際金融體系健全性的有關的威脅，制定國際標準，並促進、協調有關法律、監管及運作措施的有效執行。從1990年4月到2004年10月，FATF推出了一系列被稱為40+9建議的指導方針，以確保採取一致的全球應對標準來預防組織犯罪、貪腐和恐怖主義。2012年2月，FATF完成了對其標準和建議

的全面審查¹²。此次修訂已擴大因應新的威脅，例如資助大規模毀滅武器的擴散¹³。因為 FATF 與歐盟在今日國際洗錢防制上佔有重要的位置，所以本文主要以 FATF 與歐盟對加密貨幣洗錢威脅的因應措施為重心。

二、歐盟洗錢防制指令的建立

最一開始洗錢問題受到注意是因為國際注目的大型的販毒集團，如哥倫比亞麥德林和卡利集團（Columbian Medellin and Cali cartels），利用銀行等金融系統或其他中介機構（如服務提供商和空殼公司）來轉移、掩蓋因非法活動所得的經濟利益。而根據 FATF 對於洗錢的定義，洗錢是處理犯罪所得以掩蓋其非法來源¹⁴。洗錢本質

¹² FATF Recommendations, <https://www.fatf-gafi.org/about/historyofthefatf/#d.en.3157>, (最後瀏覽時間 2021 年 12 月 10 日)

¹³ FATF (2012-2020), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. <https://www.fatf-gafi.org/recommendations.html>, (最後瀏覽時間 2021 年 12 月 10 日)

¹⁴ Money laundering - Financial Action Task Force(FATF) 2020, <https://www.fatf-gafi.org/faq/moneylaundering/>, (最後瀏覽時間 2021 年 12 月 13 日)

上的概念並不難理解，就是「對犯罪活動所得進行偽裝、隱瞞其非法來源的過程¹⁵」。

FATF 是國際上洗錢防制的先驅，但當時利用合法金融系統或經濟循環將毒品交易非法所得合法化的問題在歐洲同樣亦日益嚴重，因此建立一個歐盟層級的洗錢防制架構，作為協調成員國之間的標準以穩定金融系統亦刻不容緩。歐盟於 1991 年 6 月 10 日通過了第一個洗錢防制指令 (Directive 91/308/EEC，以下簡稱 AMLD1)¹⁶。AMLD1 深受 FATF 建議的影響，不過當時只是單純要改善利用金融系統匿名洗錢的現象，因此要求金融機構與銀行在律所規定的狀況下，必須要確認客戶的身份 (Know Your Customer，簡稱 KYC，或是翻譯為「瞭解您的客戶」)。「瞭解您的客戶」，一言以蔽之就是一個驗證客戶真實身份的過程，完成 KYC 程序後，每個客戶就必須提供使用公司服務的

¹⁵ Schott. P. A., Reference Guide to Anti-Money Laundering and Combating the Finance of Terrorism, 2006, 頁 1。

¹⁶ Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, Official Journal L 166, 28/06/1991, p77 – 83。

身份證明文件。金融機構被要求再開始與客戶合作以前、在提供金融服務前，必須按照洗錢防制的規則驗證客戶的真實身份，這些是確保合法經營的必要措施，其實也一直就是洗錢防制規範的核心手段。

隨後又在 2001 年發布了第二個洗錢防制指令¹⁷ (Directive 2001/97/EC，以下簡稱 AMLD2)，此指令對修改了 AMLD1，納入非金融業的職業，由其是「法律顧問業」也有確認客戶身份等義務。後來在 2005 年 10 月，也就是在 FATF 於 2003 年 6 月發布建議修訂後，第三個洗錢防制指令¹⁸ (Directive 2005/60/EC，以下簡稱 AMLD3) 推出並取代了 AMLD2，再次擴大洗錢防制指令的適用範圍，同時 AMLD3 也引入 2003 年修訂的 FATF 建議，更嚴格規範注意義務，也納入了打擊資助恐怖主義的相關內容。洗錢與資助恐怖主義是兩個不同的現象，

¹⁷ Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering - Commission Declaration.

¹⁸ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25 November 2005, 15.

只是通常兩者或有緊密關連，而且通常是跨越不同司法管轄區的活動。FATF 於 2012 年 2 月發布了一套修訂後的建議後，歐盟對 AMLD3 進行了全面地檢視，並意識到歐盟有必要與 2012 年 FATF 建議保持同調。2015 年 5 月 20 日，透過第四個洗錢防制指令¹⁹(Directive (EU) 2015/849，以下簡稱 AMLD4) 與歐盟資金轉移條例 (EU Funds Transfer Regulation)，大幅改變了歐盟原有的洗錢防制與打擊資助恐怖主義的法律架構，與國際層級（主要是 FATF 規定的新標準）的法規整合。而隨著金融創新日新月異，出現許多新型支付工具或系統顛覆傳統支付方式，由其是虛擬貨幣從 2009 年出世後持續穩定發展，因此成為 2018 年第五個洗錢防制指令所要規範的核心議題。

三、第 4 個及第 5 個洗錢防制指令 (the 4th and 5th Anti-Money Laundering Directive)

¹⁹ Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5 juni 2015, 73

（一）第 4 個洗錢防制指令

在 AMLD3 公布近十年後，歐盟於 2015 年 5 月 20 日發布 AMLD4，基本上是沿襲 AMLD3 的規定，在洗錢防制執行一般注意義務的要件上，並未特別修改。重要的新修訂內容包括有通報義務者範圍的擴大、客戶盡職調查（Customer Due Diligence，CDD）的相關規定、規範受益所有人範圍及提高透明度。在客戶盡職調查的部分，在第 13 條第 1 項²⁰增訂要求銀行或其他相關單位對客戶盡職調查時，應根據可

²⁰ Article 13 1. Customer due diligence measures shall comprise: (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source; (b) identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer; (c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; (d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

When performing the measures referred to in points (a) and (b) of the first subparagraph, obliged entities shall also verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

靠的來源確認、驗證客戶的身份；確認受益人是誰，採取適當程序了瞭解客戶的所有權及其控制結構；審查以客戶名義進行交易的代理權等，以便認識自己的客戶與瞭解客戶業務的性質。本號新指令明確地擴大有義務與金融機構一樣尊本指令主體的範圍，在第 2 條²¹中新增「指定非金融事業與專業人士 / 指定申報主體」(Designated Non-Financial Business and Professions, 簡稱 DNBP) 的類別，被要求遵循指令中所規定的瞭解您的客戶、客戶盡職調查、通報義務等義務。

另外，AMLD3 已經有以風險為基礎 (Risk-Based Approach) 來區

²¹ Article 2 1. (3) the following natural or legal persons acting in the exercise of their professional activities: (a) auditors, external accountants and tax advisors; (b) notaries and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the: (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts; (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies, foundations, or similar structures; (c) trust or company service providers not already covered under point (a) or (b); (d) estate agents; (e) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; (f) providers of gambling services

分注意義務的相關規定，而本號指令擴大使用以風險為基礎的分析方式，用來區分注意義務的分級判斷義務，各會員國進行風險評估，並以風險為基礎的方式進行監督等。也就是說 AMLD4 的規定，在本號指令附件一至附件三列舉了規定要素與標準的目錄，以便進行判斷風險的高、低，不僅只考慮公司與其有業務的客戶風險類型，也納入了「地理區域、特定產品、服務、交易或交付的渠道(delivery channels)」等。各會員國應遵守以風險基礎分析的方式調查與評價洗錢及資助恐怖主義的風險，以連結適當的保護措施，風險基礎也會影響注意義務、通報義務等。

最值得注意的是，AMLD4 注意到了新的支付方式，而成為第一個規範「電子錢」(E-money) 的指令。雖然，AMLD4 第 12 條²²看起來只

²² Article 12 1. By way of derogation from points (a), (b) and (c) of the first subparagraph of Article 13(1) and Article 14, and based on an appropriate risk assessment which demonstrates a low risk, a Member State may allow obliged entities not to apply certain customer due diligence measures with respect to electronic money, where all of the following risk-mitigating conditions are met:

(a) the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 250 which can be used only in that Member State; (b) the maximum amount stored electronically does not exceed EUR 250; (c) the payment instrument is used exclusively to purchase goods or services; (d) the payment instrument cannot be funded with anonymous electronic money; (e) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or

是在規範經會員國以風險為基礎的分析方式評定為低風險時，會員國可以允許有遵循指令規範義務主體，可以不對電子錢進行客戶盡職調查措施，也就是說本條是對於電子錢客戶盡職調查的豁免規定。舉例來說，該條第 1 項(b)是當以電子方式儲存的最高金額不超過 250 歐元時，可以不履行特定的注意義務。即便如此，此指令等於是認同了當時電子錢正日益風行，成為銀行帳戶的替代品，因此自然應該規範在洗錢防制以及打擊資助恐怖主義架構下。不過，更準確地來說，AMLD4 中所規定的「電子貨幣」與「加密貨幣」不能相互混淆²³。尤其是在 AMLD4 第 2 條中已新增「指定非金融事業與專業人士 / 指定申報主體」此類應與金融機構同樣負有本號指令義務的主體，在已納入貨物商大額現金交易、買賣、租賃不動產仲介、賭場經營者，卻沒有提到任何關於加密貨幣市場參與者，是否就意味著 AMLD4 並未將加

suspicious transactions.

For the purposes of point (b) of the first subparagraph, a Member State may increase the maximum amount to EUR 500 for payment instruments that can be used only in that Member State.

²³ 參 Lin C.S., Cryptocurrencies And Its Regulations Within The Anti-money Laundering Directives, Institute for Law and Finance of Goethe-Universität Frankfurt am Main, March 2021。

密貨幣市場參與者納入本號指令遵循義務主體。即使，有論者基於本指令第 3 條第 2 款定義金融機構中(a)²⁴「貨幣兌換處」(the activities of currency exchange offices)的文字，認為加密貨幣交易所及提供虛擬貨幣兌換服務的平台也同樣是「貨幣兌換處」而為金融機構²⁵，而認為加密貨幣交易所或平台，也同樣是受 AMLD4 規範，需遵循該指令規範的相關義務，但是由於所謂的貨幣兌換處是指「法定貨幣」間的兌換，因此此見解將以法定貨幣兌換虛擬貨幣的業務平台也認為是「虛擬貨幣兌換平台」的論點，並未得到廣泛認可。

因此，為了因應由加密貨幣引發的洗錢和資助恐怖主義的問題，

²⁴ Article 3 (2) ‘financial institution’ means:

(a) an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex I to Directive 2013/36/EU of the European Parliament and of the Council (23), including the activities of currency exchange offices (bureaux de change);

²⁵ C. Hauben, “Bitcoin en EU-recht: de virtuele vreemde eend in de bijt” in *M. E. Storme and F. Helsen* (eds.), *Innovatie en disruptie in het economisch recht*, Antwerpen, Intersentia, 2017, 87, cited according to TAX3 Committee, *Crypto Currencies*, 頁 62。參考，Lin C.S., *Cryptocurrencies And Its Regulations Within The Anti-money Laundering Directives*, Institute for Law and Finance of Goethe-Universität Frankfurt am Main, March 2021。

催生了第 5 個洗錢防制指令的出現。

（二）第 5 個洗錢防制指令

在 AMLD4 頒布後的一年內，歐盟執行委員會（European Commission）開始提案修訂 AMLD4。由於加密貨幣的匿名性及交易迅速等特點，加密貨幣和虛擬貨幣的誕生，毋寧是提供犯罪集團一種額外的收集和洗錢的方式。因此歐盟執行委員會決定將加密貨幣納入規範，以終止這種不穩定的局面，因此有了第 5 個洗錢防制指令²⁶（the 5th Anti-Money Laundering Directive, Directive (EU) 2018/843, 以下簡稱 AMLD5）。無庸置疑地，此為監管加密貨幣的第一步。歐盟執行委員會於 2018 年 4 月 19 日宣布通過，並於同年 6 月 19 日公布確定案文內容，其中第 4 條要求各歐盟成員國必須在 18 個月內完成轉換立法納入國內法律中的程序。2015 年巴黎查理周刊遭到恐怖攻擊（Charlie Hebdo attacks），以及在 2017 年倫敦橋攻擊（London

²⁶ Directives (EU) 2018/843 of the European parliament and of the council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

Bridge attacks)，以及之後的巴拿馬文件之後，新指令的修訂目標著重在限制及拒絕恐怖主義的財務選擇，確保高層級防衛從高風險第三國之資金流入、加強金融情報中心的合作及獲取資訊、連結虛擬貨幣與預付卡以利追蹤資助恐怖主義者，聚焦於新金流的管道及不法匯款方式到合法的經濟循環，因此注意到了虛擬貨幣及其交換平台，以期可以達到有效防制洗錢及打擊資助恐怖主義²⁷濫用金融系統的現象。另外，包括減少預付卡限額，以及更新 AMLD4 已經規定的高價值商品和法律實體的最終受益人資訊 (the Ultimate Beneficial Ownership, UBO) 應在中央登記簿儲存資訊。綜合來說，有關「第五洗錢防制指令」主要新增及修訂，包含了將「託管錢包供應商」和「虛擬貨幣交換平台」視為新的義務主體，而納入指令規範範圍；各成員國須建立國家的銀行帳戶登記系統，以便執法機關查閱在成員國內的所有銀行帳戶資訊，並且該登記系統須與其他成員國相互連線，執法機關得要求義務主體提供資料；明確定義「重要政治人士」；針對高風險第三

²⁷ 參陳麗娟，歐盟洗錢防制法規發展現況之研究，萬國法律第 234 期，2020 年 12 月，頁 104。

國有更嚴格的管制；提高公司、信託實質受益人的透明度；禁止匿名保險箱；調整預付工具(Prepaid Instruments)需履行盡職調查的門檻，例如禮品卡、旅遊卡的門檻從 250 歐元調整至 150 歐元²⁸。但本文的主要重點是加密貨幣法規被納入洗錢防制指令的領域，因此會著重在加密貨幣規範的部分。

本號指令針對資助恐怖主義組織的財政及運作方式，觀察出一些新的趨勢，指出某些替代金融的新技術服務愈來愈受歡迎的現象，但這些新的金融科技服務，卻還不在規範的範圍內，或是被豁免於相關法律的適用等不合理的情形。AMLD5 毫無疑問的是在關於加密貨幣相關的洗錢防制指令上最重要的一個指令，因為 AMDL5 是第一個提供加密市場定義的歐盟洗錢防制指令，並且試著界定加密貨幣市場參與者。

在 AMLD5 第 3 條(d)中，虛擬貨幣被定義為「不是由中央銀行或公共機構發行或擔保，以數位化方式呈現經濟價值，不一定附屬於合

²⁸ 莊貫勤，歐盟「第五洗錢防制指令」將新科技於金融體系的應用納入管制，資訊工業策進會科技法律研究所，2019 年 1 月 20 日，<https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8183>。
(最後瀏覽日期：2022 年 11 月 5 日)

法發行的貨幣，不具貨幣或金錢的法律地位，但被自然人或法人接受為一種支付方式，可以透過電子方式轉移、儲存及交易²⁹」。在此指令中，同時明確指出虛擬貨幣（Virtual Currencies）及加密貨幣（Cryptocurrencies）都不應與電子錢（Electronic Money）或「遊戲幣」（In-game Money）混淆，遊戲幣只能在特定的遊戲環境下使用。這些貨幣最明顯的差別在於它們除了作為支付方式之外，虛擬貨幣還可以用於投資或價值儲存³⁰。由於加密貨幣的發行總額限定，以及價值波動性高，目前加密貨幣通常是作為投資商品，作為支付工具的比

²⁹ “virtual currencies” means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically;

³⁰ 參考 AMLD 5 的 Consideration (10) 。” Virtual currencies should not to be confused with electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council (5), with the larger concept of ‘funds’ as defined in point (25) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council (6), nor with monetary value stored on instruments exempted as specified in points (k) and (l) of Article 3 of Directive (EU) 2015/2366, nor with in-games currencies, that can be used exclusively within a specific game environment. Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies.”

例較低。

AMLD5 另將加密貨幣市場的兩個主要參與者，納為有遵循該指令的義務主體。這兩個受規範的義務主體³¹，包括前面所提到的「虛擬貨幣交易平台」以及「託管錢包供應商」。要求加密貨幣交易所亦需執行瞭解您的客戶、客戶盡職調查和可疑交易回報等義務。此外，這些加密貨幣服務供應商，必須在當地相關金融監理機關進行註冊，以提高交易的透明度和落實遵循指令的責任，希冀藉此可以大幅減少洗錢以及資助恐怖主義的風險。如前所述，錢包供應商存在多種選擇，包括冷錢包供應商、暖錢包供應商及託管錢包供應商。該指令針對託管錢包供應商進行監管的主要原因是因為託管錢包供應商「擁有另一個使用者的公鑰和私鑰」。與暖錢包供應商相比，暖錢包供應商只是利用與硬碟連結的應用程序儲存每個使用者的私鑰的一種單純技術服務供應商。從理論來看，託管錢包供應商的業務內容類似於金融機

³¹ Article 47 1. Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated.

構為客戶持有帳戶，並且執行該帳戶進、出帳等行為此一特徵。正因如此，監管政策上傾向認為託管錢包供應商也應該要像金融機構一樣受到監管。

AMLD5除了前開所述將加密貨幣交易所和託管錢包供應商納為應義務主體外，為因應加密貨幣所具有的匿名風險，另外增加了一項額外的安全措施。AMLD5 規定每個國家的金融情報中心（Financial Intelligence Units，簡稱 FIUs）將被授權接收加密貨幣持有者地址等資訊，以資識別虛擬貨幣的所有人³²。AMLD5 也引進「使用者自願登記」制度的概念，作為防制加密貨幣匿名性的一種方式，但由於仍需要更進一步評估，因此尚未正式通過。且前開金融情報中心被授權可

³² 參考 AMLD5 Consideration (9) : The anonymity of virtual currencies allows their potential misuse for criminal purposes. The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers. To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed.

以取得加密貨幣持有者地址等功能的實行狀況也尚待觀察。不過可以確認的事實是，這些新增的指令規範內容，已逐步將加密貨幣合法化，建立制度來區別一般正當的投資者與那些試圖透過加密貨幣洗錢或資助恐怖主義而濫用金融系統之人。

（三）小結：第 4 個及第 5 個洗錢防制指令的影響

自 1990 年推出 AMLD1 以來，隨著洗錢行為態樣及架構日趨複雜多元，歷經多次修訂，各歐盟會員國在將歐盟指令納入本國法律方面，本享有一定的自由度。早在 2017 年 6 月就已生效的 AMLD4，有些國家卻至今都尚未落實。而 AMLD5 的第 4 條³³規定，要求各歐盟會員國，至遲必須於 2020 年 1 月 10 日前，將該指令轉化為國內法。截至 2021 年 11 月 30 日，27 個成員國中已有 25 個成員國已完成該指令轉換³⁴。

³³ Article 4 1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 10 January 2020. They shall immediately communicate the text of those provisions to the Commission.

³⁴ 參考 EU Commission Anti-money laundering directive V (AMLD V) - transportation status,

無庸置疑地，AMLD5 是在如何監管加密貨幣並同時維持市場發展上的一大步，其中最顯而易見的難題是如何在隱私權保護、新興金融科技發展以及監理之間取得平衡。然而，加密貨幣交換平台和託管錢包供應商在被作為有義務實體後，將有相關的法令遵循成本的產生。上開業者必須因應指令所規範的新的義務內容，重新建構其等法令遵循的程序，甚至包括它們目前所使用之技術。而這些都會成為各別加密貨幣業者的成本，這些業者可能會也可能不會承擔這些變更程序的成本以遵守指令規範的義務。

總部位於英國的比特幣託管錢包供應商 Bottle Pay，因為新一波法規對從事加密貨幣行業的公司提出更嚴格的要求，而於 2019 年 12 月 13 日宣布退出市場，儘管該公司在兩個月前籌集了 200 萬美金。在該公司的公告中，還特別引用了來自 AMLD5 的措施。根據 Bottle Pay 表示：「要求蒐集客戶額外資料的數量及類型，將徹底改變目前使

https://ec.europa.eu/info/publications/anti-money-laundering-directive-5-transposition-status_en, (最後瀏覽日期 2022 年 1 月 15 日)

用者的經驗，而我們不願意將其強加給我們的社區³⁵」，而且這也將對加密貨幣市場造成高度負面影響³⁶。此外，僅處理比特幣交易的知名加密貨幣交易所之一的 Deribit，為了規避新的歐洲洗錢防制法令，於 2020 年 1 月 9 日在公司的部落格公布，將把其業務從荷蘭總部 (Deribit B.V) 移轉到由荷蘭總部百分百持股的巴拿馬 (DRB Panama Inc.) 公司營運，所有交易相關資料其他系統設置將從荷蘭總部轉移到巴拿馬公司，平台的伺服器則將如之前已宣布的計畫移至倫敦，並且發布新的 KYC 政策的細節³⁷。Deribit 也表示，做出此一決定的理由是因為 AMLD5 的實施，Deribit 不清楚將會對公司造成怎樣的影響。Deribit 認為荷蘭很可能會非常嚴格地實施 AMLD5。而如果 Deribit

³⁵ “The amount and type of extra personal information we would be required to collect from our users would alter the current user experience so radically, and so negatively, that we are not willing to force this onto our community.”，參 Qader-A. A., Finance Magnates, Bottle Pay Shuts Down as EU Regulations chase out Crypto Firms, 13 December 2019, <https://www.financemagnates.com/cryptocurrency/regulation/bottle-pay-shuts-down-as-eu-regulations-chase-out-crypto-firms/>, (最後瀏覽日期 2022 年 1 月 15 日)

³⁶ 同前註。

³⁷ 參 Deribit moving to Panama + KYC, February 2020, <https://insights.deribit.com/exchange-updates/deribit-moving-to-panama-kyc-february-2020/>。(最後瀏覽日期 2022 年 1 月 15 日)

要遵循相關的新規定，這意味著公司必須要求客戶提供大量訊息，這樣一來就違反了 Deribit 認為加密市場應該是對大多數人免費開放的原則，而且新的法令遵循將對大多數交易設置過高的例如監管成本上的障礙，將劇烈影響交易所及使用者³⁸。儘管有些公司選擇遷移至別的司法管轄區繼續提供服務，或者也有公司選擇完全退出市場，但也有些大型交易所和供應商，例如 Chainalysis、Coinfirm、CEX.IO、CoinBase 選擇繼續留在歐盟或英國。從長遠來看，這些留下來的公司因為加密貨幣規定相關法令的遵循，已經熟悉瞭解您的客戶、客戶盡職調查規則，對比其他同性質的公司，這些合法合規的公司，在市場上將可能更具有競爭優勢。也許，AMLD5 對加密貨幣交易市場產生劇烈的影響，但樂觀角度來看，就加密貨幣的相關監理有助於穩定金融系統，也將為新的金融創新開創更廣闊可行的道路。

由於歐盟洗錢防制規範是以指令 (Directive) 形式公布，依據
歐盟運作條約 (Treaty on the Functioning of the European

³⁸ 同前註。

Union，簡稱 TFEU)規定，各歐盟會員國必須轉換指令內容為內國法。身為歐盟成員國活躍成員，德國一直以身作則地將歐盟指令轉化為其內國法律。德國轉換歐盟洗錢防制指令為 Geldwäschegesetz (德國反洗錢法，以下簡稱 GWG)。而因應 AMLD5 的發布，德國金融監管局(Bundesanstalt für Finanzdienstleistungsaufsicht，以下簡稱 BaFin)於 2019 年 5 月 20 日公佈了其實施第 5 號反洗錢指令的法律草案 (Regierungsentwurf)，該法案修改了 GWG 的某些條款，而 Kreditwesengesetz (德國銀行法，以下簡稱 KWG)則是將指令中新納入的監管義務主體的職責規範在內³⁹。KWG 將加密資產 (Kryptowerte) 的定義為「以數位方式呈現的價值，未經由任何中央銀行或公共機構發行或擔保，不具有貨幣或金錢的法律地位，但被自然人或法人根據約定或實務上作為支付或交換工具，或用於

³⁹ 參 Referentenentwurf des Bundesministeriums der Finanzen Entwurf eines Gesetzes zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie [Richtlinie (EU) 2018/843], https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2019-12-19-Gesetz-4-EU-Geldwaescherichtlinie/1-Referentenentwurf.pdf?__blob=publicationFile&v=4, 20 May 2019。(最後瀏覽日期：2022 年 1 月 15 日)參考，Lin C.S., Cryptocurrencies And Its Regulations Within The Anti-money Laundering Directives, Institute for Law and Finance of Goethe-Universität Frankfurt am Main, March 2021。

投資目的，而且可以被電子方式傳輸、儲存或交易。」⁴⁰ 這樣的法律架構，即等同將加密貨幣服務供應商置於與金融工具(Financial Instruments) 相同的監理框架下。也就是根據 GWG 第 2 條第 2 款規定的義務主體⁴¹。另外，加密貨幣託管機構需要取得主管機關的許可，才能在德國從事加密貨幣託管服務，而已經在該國無許可證的加密貨幣託管平台，則必須在 2020 年 11 月底之前申請。已經在其他歐盟國家註冊的加密貨幣託管公司，不能直接移轉他們的許可證到德國，而是必須重新在德國提出申請，才能在德國提供加密貨幣託管服務。BaFin 對於虛擬貨幣的新分類，不僅只是回應 AMLD5，

⁴⁰ Section 1 para. 11 sentence 1 no. 10 German Banking Act Kreditwesengesetz - KWG: “Kryptowerte im Sinne dieses Gesetzes sind digitale Darstellungen eines Wertes, der von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen aufgrund einer Vereinbarung oder tatsächlichen Übung als Tausch- oder Zahlungsmittel akzeptiert wird oder Anlagezwecken dient und der auf elektronischem Wege übertragen...” 參考，Lin C.S., Cryptocurrencies And Its Regulations Within The Anti-money Laundering Directives, Institute for Law and Finance of Goethe-Universität Frankfurt am Main, March 2021。

⁴¹ Section 2 para. 1 no. 2 German Anti-Laundering Act *Geldwäschegesetz* - GWG: “Finanzdienstleistungsinstitute nach § 1 Absatz 1a des Kreditwesengesetzes...”

同時也是呼應防制 FATF 的建議。

四、第五個洗錢防制指令未解決的問題

AMLD5 大刀闊斧地將加密貨幣交易平台及託管錢包供應商二者加密貨幣參與者納入洗錢防制的監理架構下，固然值得肯定，但是就僅將此二者納入義務主體，是否足以打擊與加密貨幣相關的匿名性？如同本文前面相關段落中提及加密貨幣市場上仍有一些重要的參與者，而這些參與者並未同時被 AMLD5 納作義務主體，這樣是否為立法者當初有意識下的刻意安排？這樣的安排，是否足以涵蓋監理機關最初計畫所要監管的所有平台？

根據 AMLD5 發布前歐盟執行委員會所做的影響評估報告⁴²，利益相關者有從選項 A 到選項 F 可供選擇受監理的使用者，也就是加密貨

⁴² COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document “Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC”, SWD(2016) 223 final, 5 July 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN>, (最後瀏覽日期：2022 年 1 月 15 日)

幣交易平台及託管錢包供應商，所有選項的宗旨都是為了提高透明度並發現可疑交易⁴³。立法者本也有意將「礦工」納入監管範圍，但決定將「礦工」納入監管範圍，將會引起相關執行的問題，因為大多數礦工居住在中國。另一個可以解決加密貨幣匿名性的想法是「在歐盟區內全面禁止其使用」，但這個想法很顯然將不利於數位創新的發展而遭到揚棄⁴⁴。選項 A、B 是藉由規範加密貨幣使用者的強制或自願註冊；選項 C、D 則是針對加密貨幣交易平台，將其納入 AMLD5 或第 2 項支付服務指令（2nd Payment Services Directive）的監管範圍；選項 E、F 是將託管錢包供應商標記為具有與選項 C 和 D 相同的選項。最後選擇結果是選擇了選項 B、C、E。選項 B 的自願註冊已包含在 AMLD5 的第 9 條中，但如同本文前面段落所述，尚必須有進一步的評估才能實施。選項 D 和 F 未受到歡迎，因為雖然將加密貨幣交易平台和託管錢包供應商納入第二支付服務指令會自動將有義務的主體置於洗錢防制指令的監管架構之下，但會有對有義務的主體遵守必要的

⁴³ 同前註，頁 29-32。

⁴⁴ 同前註，頁 73。

許可、消費者保護和保障要求等要求。此外，將加密貨幣納入第二支付服務指令，有可能因為對加密貨幣提供合法性，而誤導消費者認為加密貨幣是經認定的安全可靠的產品⁴⁵。這個評估結論，後來被納入 AMLD5 中。

吾人得以從上述的影響評估報告中知悉立法者為什麼只選擇規範加密貨幣交易平台及託管錢包供應商。但關於只規範這兩個義務主體是否足夠的問題，確實可能存在著犯罪集團得以利用的漏洞。例如透過冷錢包或暖錢包，加密貨幣使用者仍然可以保持匿名的狀態，或是其他任何不在 AMLD5 第 1 條 (C) 定義的交易，都將不受該指令的監管。因此，僅將加密貨幣交易平台及託管錢包供應商納為義務主體，並不足以打擊加密貨幣的匿名性。但如同本文前面段落曾提及關於加密貨幣監理的困境：隱私與加密貨幣市場發展間的和諧，隨著監理法規施行時間的推移，密切關注加密貨幣交易匿名性問題的嚴重程度，以及相關監理法規對加密貨幣市場創新發展的影響程度，主管機關可

⁴⁵ 同前註，頁 31。

以適時地調整，試著而找到最佳的平衡。關於這個問題，本文在後面的段落也將繼續討論。

再者，關於歐盟使用者註冊的問題上，根據 AMLD 5 第 47 條規定⁴⁶，加密貨幣交易所和託管錢包供應商有義務進行註冊，具體如何由每個成員國決定。而這個註冊程序上如何進行，尚未有定論，可能需要好些時間才能夠建立一個平衡隱私與創新發展的系統。即使建立了自願註冊制度，但因為透過加密貨幣參與洗錢或資助恐怖主義的使者不太可能乖乖註冊他們的身份。而且還有歐盟各成員國協調的問題。因為如果每個歐盟成員國都以不同的方法和標準進行註冊，成員國之間的合作將會發生問題。

五、歐盟未來的發展

（一）第 6 個洗錢防制指令（the 6th Anti-Money Laundering

⁴⁶ Article 47 Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered, that currency exchange and cheque cashing offices, and trust or company service providers are licensed or registered, and that providers of gambling services are regulated.

Directive)

歐洲執行委員會於 2021 年 7 月 20 日發布一系列野心勃勃的立法提案包裹⁴⁷，宣示繼續加強洗錢防制及打擊資助恐怖主義不容懷疑的決心，並加強金融情報機構 (FIUs) 之間的合作。其中包括了成立新的監管機構 AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism)；發布新機構 AML/CFT 的草案，尤其包含客戶盡職調查和受益所有人的相關內容；還有第 6 條洗錢防制指令 (the 6th Anti-Money Laundering Directive，下稱 AMLD6) 草稿⁴⁸，生效後將取代 AMLD5；發布 2015 年資金轉移條例 (Regulation 2015/847/EU) 部分修正草稿，新增了對加密貨幣錢包轉帳的追蹤監

⁴⁷ 歐洲議會發布新文稿 European Commission press release, Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690 (最後瀏覽日期：2022 年 1 月 15 日)。

⁴⁸ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0423>。(最後瀏覽日期：2022 年 1 月 15 日)

管要求，以追蹤加密資產的轉移，增加了對大額現金支付的限制要求。

AMLD6 與本文最相關的部分在於，也就是如歐洲執行委員會所公告的內容，歐盟 AML/CFT 規範將全面應用於加密貨幣領域。在 AMLD6 之前，只有特定類別的加密資產服務供應商被納入歐盟 AML/CFT 監理的範圍內。新的規定將擴展到整個加密貨幣產業⁴⁹，要求所有服務供應商都必須對其客戶進行盡職調查。也就是說，所有比特幣和其他加密資產服務供應商，將都有義務對其客戶進行盡職調查，參與加密資產交易的所有服務提供商，都有義務收集及提供有關其經營的虛擬或加密資產交易的傳送者和接收者的各種個人資料，包括姓名、身份證件號碼、帳號、帳戶的建立和存在地點以及處理交易的確切地點。另外，為了確保加密資產轉移的完全可追溯性（traceability

⁴⁹ Article 5 1. Member States may require electronic money issuers as defined in Article 2(3) of Directive 2009/110/EC 44 , payment service providers as defined in Article 4(11) of Directive (EU) 2015/2366 and crypto-assets service providers operating through agents located in the host Member State and operating under either the right of establishment or the freedom to provide services, and whose head office is situated in another Member State, to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the entity operating on a cross-border basis, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.

requirements to crypto-assets)，將禁止匿名加密資產錢包，將歐盟 AML/CFT 規則全面適用於加密市場領域。歐洲執行委員會還特別指出，這些建議的目的，是在因應洗錢防制上的威脅及遵守國際標準之間找到適當的平衡，同時又不會給行業帶來過度的監管負擔，相反地這些提議將使加密貨幣受益於整個歐盟更新、一致的法律架構，因此將有利於整個加密產業的蓬勃發展⁵⁰。但對於個人數據、隱私、加密貨幣整體發展及洗錢防制、打擊資助恐怖主義防制上的影響，在實際操作上究竟會是怎樣的結果，尚需要等待這些相關配套法令預計施行的 2024 年施行後一段時間，才會比較客觀知道究竟是有如歐盟議會所主張的樂觀結論，或者是如同前面所提到因此遷移業務總部或乾脆退出市場的加密貨幣業者的悲觀結論。至少可以確定的是，各國的趨勢是正面認定加密貨幣的合法性，並且納入相關的法律框架，同時試著追求各個司法管轄下的統一標準。如果是從這一個觀點出發，再

⁵⁰ European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing, the Commission's Action Plan and other recent developments (2020/2686(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204_EN.html)。(最後瀏覽日期：2022 年 1 月 15 日)

考慮加密貨幣的無國界的特徵來看，就現階段而言，本文會比較傾向歐盟積極建立對加密貨幣的規範整體上是具有正面效益，雖然短期間可能使得加密貨幣的交易快速性減低，也將造成執行面上未決的困難，也無庸置疑地必定會增加加密貨幣業者或使用者的成本，但從遠程來看，很有可能有助於加密貨幣的制度性發展，讓加密貨幣規範更具一致性，並有利於加密貨幣的流通與方便性。

(二) 加密資產市場規則 (Markets in Crypto-assets Regulation)

歐盟執行委員會於 2020 年 9 月 24 日推出了新的數位金融套裝提案 (Digital Finance Package)，強調預計在 4 年內建立一套健全法律框架的必要性，目的在於提高提供更迅速、便宜的跨境支付系統，提升歐洲金融科技競爭力，同時降低風險並確保歐洲金融的穩定性。其中包括有關加密資產 (Crypto-Assets)、數位營運的彈性 (Digital Operational Resilience) 和零售支付戰略 (Retail Payments Strategy) 的法規提案。在加密資產部分，加密資產市場規則 (Markets in Crypto-assets regulation, MiCA，以下稱 MiCA) 此 168 頁的提案，是預計建立一個法律框架，允許加密資產繼續創新，同時保護金

融穩定及投資者⁵¹。正如同歐盟執行委員會金融服務專員 Mairead McGuinness 表示的：「歐盟是世界上最早尋求監管加密資產和穩定幣的地方之一。我們在 MICA 提案（加密資產市場監管）方面取得了良好進展。我們的目標是在支持創新的同時保護最終用戶、維護金融穩定和維護貨幣主權。」⁵²。MiCA 正在為以前未受監管的加密資產引入一個制度，監管框架中的擬議立法，將有利於加密貨幣公司透過許可制度在歐盟擴張，也就是在這該制度下，允許在一個成員國受監管的公司可以在其他國家運作⁵³。

⁵¹ EU Commission, Digital Finance Package, 24 September 2020, https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en。（最後瀏覽日期：2022 年 1 月 15 日）

⁵² “The EU is one of the first places in the world to look to regulate crypto-assets and stablecoins. We are making good progress with the MICA proposal, the regulation on markets in crypto-assets. Our goal is to protect end users, maintain financial stability and uphold monetary sovereignty whilst supporting innovation.”，參 Keynote speech at European Payment Institutions Federation Annual Conference，https://ec.europa.eu/commission/commissioners/2019-2024/mcguinness/announcements/keynote-speech-european-payment-institutions-federation-annual-conference_en。（最後瀏覽日期：2022 年 1 月 15 日）

⁵³ https://finance.yahoo.com/news/european-commission-urges-member-states-194015182.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2x1LmNvbS8&guce_referrer_sig=AQAAAC-TgKbC4IAIBWzhX-rOC8_0oOSIPvrTF0RY9UyQYM6wJL_F6PY5XXmN-

MiCA 主要是規範「可以使用分散式帳本技術或類似技術以電子化方式轉移和儲存的價值或權利的數位表現」的加密資產。另外提供與符合前開定義加密資產相關的任何服務的公司，包括但不限於託管服務、交易及貨幣兌換（加密資產和法定貨幣之間），必須取得歐盟成員國監理主管機構的許可，經歐盟成員國主管機關根據歐盟法規許可的公司，即可以將業務擴展到其他歐盟成員國，而不需另外取得他成員國的許可。

目前，加密資產市場監管仍處於歐洲議會的一讀程序⁵⁴，預計在未來四年內實施。該法規旨在為歐盟成員國提供單一市場內所有使用者和供應商一致的規則，目的是規範所有數位形式呈現的價值與權利（Digital Representation of Value and Rights），都可以藉由分

[ZfWEtnbA6vS87xDIRWSjISu-c82zjp2SNoVXYQDDc4BlqRrI8_BADyWCgMaAy2UaqCnqXwG4g9P423ORUYUmpYa_n4zoXE8MsmHkoVHRmVjeAZrfA0](https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52020PC0593&sortOrder=asc)。（最後瀏覽日期：2022 年 1 月 15 日）

⁵⁴ 參考 EUR-Lex, Procedure 2020/0265/COD, <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52020PC0593&sortOrder=asc>。（最後瀏覽日期：2022 年 1 月 15 日）

散式帳本技術 (Distributed Ledger Technology) 移轉或保留。

MiCA 還有望進一步涵蓋尚未規範在第二個金融工具市場和歐盟電子錢指令 (2nd Markets in Financial Instruments Directive and the Electronic Money Directive) 中的加密資產⁵⁵。

與本文前面所提到的洗錢防制指令相比，MiCA 更專注於在建立加密資產的法律框架，並沒有特別著重洗錢防制或者是打擊資助恐怖主義。因此，從監理的角度來看，這將是穩定歐盟金融市場上加密貨幣發展及其他加密資產使用者消費者保護上的新希望，相反的，是否會對透過加密貨幣來打擊洗錢及資助恐怖主義上產生重大影響仍有待評估。不過，在 4 年內，加密貨幣市場的發展日新月異，可能將與現在立法的考量完全不同，尚須密切注意觀察加密貨幣與洗錢及資助恐怖主義的發展。

⁵⁵ Cummings C., MiCA: A Guide to the EU's Proposed Markets in Crypto-Assets Regulation, Merkle Science, 23 November 2020, <https://medium.com/merkle-science/mica-a-guide-to-the-eus-proposed-markets-in-crypto-assets-regulation-c9098be039cf>。(最後瀏覽日期：2022 年 1 月 15 日)

肆、我國目前對虛擬貨幣及交易平台之監理情形

一、加密貨幣的合法性

2008 年 10 月，「中本聰」使用區塊鏈作為加密技術的比特幣開啟了虛擬貨幣的濫觴之後，陸續出現以太幣、泰達幣萊特幣、門羅幣等各類加密貨幣，目前世界上已經有 16000 多餘種的加密貨幣，在 coinmarketcap 上所陳列的加密貨幣就有 9112 種⁵⁶，根據該網站的統計資料，加密貨幣總市值曾在 2022 年 1 月 4 日達到 2.2 餘兆美金的一個高點，相比於 2020 年全球經濟產值約 84.705 萬億美元，也許目前還沒有佔全球市值很重的比重，但是加密貨幣持續不斷成長中，前景不容小覷。即使目前短期內加密貨幣也不太可能取代傳統的法定貨幣，但加密貨幣此新型態支付方式，卻已足以顛覆長期以來的傳統金融支付系統，尤其是在全球性的金融支付交易，加密貨幣可以規避各國貨幣的相關規範之障礙，並且有取得匯率上的優勢，在交易市場上形成一個一個免費又快速流動的交易系統。另外，在大量的去中心

⁵⁶ 參考 <https://coinmarketcap.com/>。(最後瀏覽日期：2022 年 1 月 17 日)

化金融服務(Decentralized Finance, 簡稱 Defi)出現後，加密貨幣開始與傳統金融出現整合關係是現在的趨勢。Defi 與傳統金融服務的整合下，提供加密貨幣的儲存、借貸、槓桿操作、期權交易、保險等各種交易型態，因其新型的金融服務和商業模式，甚至可以提供遠高於一般金融商品的殖利率。

由於虛擬貨幣具有去「中心化」及「匿名性」之特質，使各國司法機關及警調單位不易追查其來源、去向，因此從事不法犯罪行為者利用虛擬貨幣作為犯罪支付工具，或將其作為將犯罪所得轉出後，利用正常的經濟循環合法化的洗錢工具。再者，又因為各類虛擬貨幣的供給量是依循事先決定的協定 (Protocol)，不會依市場需求彈性調整供給，而具有總數定量之特性，又有新興技術所帶來的神祕感加乘，極容易成為投機者的炒作客體，也因為虛擬貨幣在市場上之價格波動極大，往往常是詐欺犯罪、不法吸金者青睞之主題。

虛擬貨幣從其出現在市場上以後，曾經有些國家不承認其合法性，或禁止發行或交易。日本率先於 2017 年 4 月承認虛擬貨幣為合法之支付工具，交易商視為特定事業，並由日本內閣授權金融廳

(Financial Services Agency , FSA) 為主管機關。英國以「加密貨幣指導方針」肯定虛擬貨幣可能作為一種金融工具，惟逐漸加強審查之密度；中國大陸曾為虛擬貨幣重要的市場參與者，然於 2017 年 9 月下令停頓各虛擬貨幣交易所，目前民眾仍可持有虛擬貨幣，但尚難經由銀行系統作為支付工具；德國聯邦議院於 2019 年發表聲明，認為虛擬貨幣並非真正貨幣，然仍積極立法加強對虛擬貨幣之控管；荷蘭中央銀行呼籲相關虛擬貨幣公司，向中央銀行進行註冊，而欲加強對於虛擬貨幣監管。

早於 1976，諾貝爾經濟學獎得主 Friedrich Hayek 教授發表《去國家化的貨幣》(The Denationalization of Money) 一書中，即已提議貨幣發行應由市場決定，以避免中央銀行因政治力掣肘，無法解決高通膨問題，且建議廢止政府的貨幣發行獨占權；主要因私人通貨 (private currency) 在面臨市場競爭下，將會讓銀行有誘因提供穩定的交易媒介⁵⁷。儘管這樣的論述可能會被認為太過天馬行空、不切

⁵⁷ Fry, Maxwell J., Isaack Kilato, Sandra Roger, Krzysztof Senderowicz, David Sheppard, Francisco Solis and John Trundle (1999), Payment Systems in Global Perspective, Bank of England, May 5. 參楊金龍，虛擬貨幣與數位經濟：央行在數位時代的角色，國立政治大學「金融科技生態系」

實際，然而觀察近年來加密貨幣由私人發行、去中心化等特質，其實在某程度上，就是實現Friedrich Hayek教授當年的構想，雖然加密貨幣的興起，並不是由政府有計畫的推動，而是由市場力量所促成。

就目前現況及世界各國監理趨勢，是傾向不禁止加密貨幣，禁止加密貨幣發展者為少數。相反的，基於在加密貨幣交易無國界的特質，本文對於是否在現實中能夠在特定司法管轄區達到全面禁止加密貨幣的況態，抱持著相當程度的懷疑。比較客觀實際的途徑，並不是掩耳盜鈴地否定加密貨幣的合法性，反而應該要持續審慎、密切地關注加密貨幣的創新與發展，而建立對應的監管系統。因為加密貨幣至今已行之多年，無法期待加密貨幣可能消失在市場上，加密貨幣的使用已經是一個不可逆的現象。又由於加密貨幣移轉不受地域限制的特質，即便某交易所在某司法管轄區遭到管制，在利之所趨下，也能迅速找

高 峰 論 壇 演 講 稿 ， 2018 年 8 月 。

<https://ws.www.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvMjk1L3J1bGZpbGUvNzcyMi8yODQ2NjIvYjk2ZmZMTQtMmUwYS00MzRkLT1hNzAtM2Q0ODM0NzFmZDA5LnBkZg%3D%3D&n=MjAxODA4MDfmpYrnuL3oo4HmvJTorJvoqZ4ucGRm&ico%20=.pdf>。(最後瀏覽日期：2022年1月25日)

到替代去路⁵⁸。也就是說，即使部分司法管轄區禁止其使用與交易，只是讓大多數交易轉為場外交易，或是轉往政策對加密貨幣業者或使用者較友善的國家發展。因此，本文認為應該要建立一個安全且有效率的加密貨幣法制框架，不僅有助於經濟活動的順暢，提升相關產業之生產力，甚至有助於擴大一國經濟規模與全球化發展。立法者或主管機關應該要更積極歸納出加密貨幣的特質，不僅讓消費者正面認識加密貨幣，也試著與相同特質或類似的金融工具、商品做相同強度的管理，並且建立對等的法制、監理架構，以便管理加密產業，同時也避免加密貨幣被污名化，或遭到犯罪集團濫用而用於洗錢，或者更嚴重地危及世界金融系統的秩序及穩定性。

我國目前對於加密貨幣並未有禁止之規定，但除了最近將加密貨幣納入洗錢防制規範範圍內外（此部分將在後面敘述），並未有相關的立法。立法院自 2018 年，三讀通過金融監理沙盒法案鼓勵金融科技發展與創新外，亦有研議推動區塊鏈與加密貨幣相關立法。又於

⁵⁸ 參郭秋榮，我國因應數位貨幣發展之對策與政策建議，經濟研究第 19 期，2019 年 3 月，頁 14。

2018年9月11日的「虛擬通貨交易所會員自律公約」公聽會主席結論，希望盡快確定虛擬貨幣的主管機關，即便尚未確定，虛擬通貨交易所會員自律公約可以先推動，並請金管會支持自律組織⁵⁹。面對加密貨幣的興起，如何平衡金融創新發展及金融監理密度，是監理上的一大挑戰。目前政府的態度上看似是由市場機制決定，國內幣圈界業者多認為應循序朝向立法方向前進⁶⁰，而歐洲當局監理上趨嚴或明朗化，並且同步強化洗錢防制、打擊資助恐怖主義以及消費者保護等相關機制。

二、虛擬貨幣的定性

（一）中央銀行及金融監督管理委員會的立場

同前面所提及在歐洲中央銀行、FATF、德國銀行法以及尚未通過立法的 MiCA 對於虛擬資產的定義，吾人得以歸結出歐洲對於虛擬貨

⁵⁹ 同前註，頁 33。

⁶⁰ 同前註，頁 34。

幣的態度。虛擬貨幣充其量只是加密資產、金融工具，而非貨幣，雖然可以用作支付工具，但是無法取代法定貨幣，在管理趨勢上有以成立專法，並類似於金融工具(Financial Instruments)的管理方式，由政府建立相關的法律制度，指定主管機關，扶植加密貨幣的發展。

回到我國來看，因為虛擬貨幣非國家貨幣當局發行，不具法償效力，也沒有發行準備或對償保證，並不具備著貨幣的三大核心功能，故我國中央銀行會同金融監督管理委員會（下稱金管會）在 2013 共同年發布新聞稿，將虛擬通貨定義為「虛擬商品」，而非貨幣，將比特幣定性為具有高度投機性的數位虛擬商品，又其尚不得作為社會大眾遍接受之支付工具，故銀行等金融機構不得收受、兌換比特幣，亦不得於銀行 ATM 提供比特幣相關服務；又於 106 年 12 月 19 日公開表示：比特幣為具有高度投機性的數位「虛擬商品」，價格波動極大，且具有高度的投機性，提醒社會大眾務必要審慎評估投資風險，並重申金融機構不得參與或提供虛擬貨幣相關服務或交易。也因此，在實務界⁶¹或學界是稱虛擬貨幣為「虛擬通貨」。而由於將虛擬貨幣視為商

⁶¹ 參楊金龍，虛擬貨幣與數位經濟：央行在數位時代的角色，國立政治大學「金融科技生態

品，因此在 2018 年 3 月，當時的財政部長曾在立法院回應比特幣議題時表示，虛擬貨幣買賣視同商品交易應該課稅⁶²。

隨後，金管會復於 2019 年 4 月召開「研商證券型代幣發行監理規範座談會」，擬將虛擬貨幣函定為證券交易法第 6 條之「有價證券」。金管會復於 2019 年 7 月 3 日發布(108)年金管證發字第 1080321164 號函令，依據證券交易法第 6 條 2 第 1 項規定，核定證券性質之虛擬通貨為證券交易法所稱之有價證券。該函令並參考美國關於投資契約之定義，將具證券性質之虛擬通貨，定義為「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，且具流通性及下列投資性質者：(1) 出資人出資；(2) 出資於一共同事業或計畫；(3) 出資人有獲取利潤之期待；(4) 利潤主要取決於發

系」高峰論壇演講稿，2018 年 8 月。中央銀行楊金龍總裁在演講稿中，均稱「虛擬貨幣」為「虛擬通貨」。
<https://ws.www.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvMjk1L3JlbGZpbGUvNzcyMi8yODQ2NjIvYjk2ZmZMTQtMmUwYS00MzRkLT1hNzAtM2Q0ODM0NzFmZDA5LnBkZg%3D%3D&n=MjAxODA4MDFmpYrnuL3oo4HmvJTorJvoqZ4ucGRm&ico%20=.pdf>。(最後瀏覽日期：2022 年 1 月 25 日)

⁶² 同前註，頁 29。

行人獲第三人之努力。金管會再於 2020 年 1 月 15 日發布 (108) 年金管證發字第 10803620609 號函令，規定募集發行金額新台幣 3 千萬以下具證券性質之虛擬通貨，且依財團法人中華民國證券櫃臺買賣中心證券商經營經營自行買賣具證券性質之虛擬通貨業務管理辦法者，為依據證券交易法第 22 條第 1 項規定經主管機關核定之其他有價證券，得豁免於該條項之申報義務。

目前加密貨幣在我國「並非貨幣」，亦非金管會核准發行的金融商品，目前較常作為「類金融投資商品」，在我國銀行並無法兌換、收受虛擬貨幣。

(二) 司法實務的立場

近年我國虛擬貨幣犯罪頻繁，「My Coin 比特幣交易網站」(臺灣臺北地方檢察署)、「法尼新創科技公司乙太幣」(臺灣桃園地方檢察署案件)、「MFC CLUB 虛擬貨幣」(臺灣臺中地方檢察署)等銀行法案件，為不法吸金的銀行法案件之標的。然而，因為目前中央銀行及金管會均認為虛擬貨幣是「虛擬商品」，因此以加密貨幣吸金標的之案件，是否能論以銀行法第 125 條第 1 項之違法經營收受存款業務罪，即有

適用上的問題。

目前司法實務上中關於虛擬貨幣定性的判決尚屬少見。臺灣新北地方法院 106 年度金訴字第 8 號刑事判決⁶³理由中，以文義解釋、歷史解釋、體系與目的解釋等方法論來認定比特幣的性質為虛擬商品，因此非屬銀行法第 29 條、第 29 條之 1 規定之「存款」、「款項」、「資金」，且由於銀行於現行制度下亦不可經營虛擬商品之收受、兌換、交易，因此也不會有非從事銀行的特許業務的違法問題，進而認為檢察官以比特幣為具有市場經濟價值之虛擬物，可視為貨幣之變形為由，起訴論以違反銀行法第 29 條、第 29 條之 1 擅自經營收受存款業務乙節，容有違罪刑法定原則。該判決先從文義解釋上認定銀行法第 29 條、第 29 條之 1 定有明文，係禁止非銀行不可收受「存款」、「款項」、「資金」，從社會一般認知及專業定義來看，「存款」係指放入金融機構存放之款項，「款項」、「資金」則應係指可為支付工具之貨幣，也就是法律認可在銀行交易兌換之貨幣，始為此處規範之「存款」、「款

⁶³ 臺灣新北地方法院 106 年度金訴字第 8 號判決，<https://law.judicial.gov.tw/FJUD/default.aspx>。

項」、「資金」。而經金管會 107 年 5 月 15 日金管銀法字第 10701094250 號函覆內容表示「比特幣並非貨幣，而係高度投機之虛擬商品」，認定則比特幣性質上並非貨幣，而係虛擬商品，顯然無法存入銀行成為存款，亦無法作為銀行認可之支付工具，自不該當銀行法所定「存款」、「款項」、「資金」之要件。復以歷史解釋論來審酌銀行法第 29 條之 1 之立法理由，認為該條立法原意是鑒於行為人為「非銀行」，不受金融主管機關特許而成立，營運行為不受監督，卻對外向不特定人吸收資金或存款，將使出資大眾的付出處於無法透過行政監理機制管控的風險，該法所表彰社會法益即遭有侵害之可能，即有適用本法予以規範之必要。因此上開條文是要禁止非銀行身分之人，從事與銀行類似的收受存款業務，然比特幣並非貨幣，無法存入銀行，顯然不在該立法者當初認定「收受存款」範圍之內，因此比特幣收受自不為銀行法第 29 條、第 29 條之 1 規範範圍內。最後以體系與目的解釋論認為，銀行法第 3 條有關銀行可經營業務之例舉規定中，並沒有可買賣、收受虛擬商品或比特幣之規定，而依照上揭金管會的回函，銀行也不能收受、兌換比特幣，可見主管機關並沒有准許銀行經營兌換、收受比特幣業務，這些並不是銀行可經營的業務範圍。該判決認定被害人

購買比特幣，是透過幣託公司或其他比特幣平台所購買，行為人收受大眾投入比特幣至平台，並非從事銀行之特許業務，自非銀行法所欲管制範圍內。且比特幣在現實交易上，雖可透過幣託公司轉賣為現金，然此並非透過銀行機構交易，比特幣在金融機構間，亦無強制流通性，因此行為人經手投資者投入之比特幣，再自行將該性質屬虛擬商品之比特幣變現牟利，並非以銀行自居，從事銀行才可以做的收受投資者「現金」存款業務，而不在現行銀行法第 29 條、第 29 條之 1 管制範圍之內。

該案上訴至臺灣高等法院，臺灣高等法院 107 年度金上訴字第 83 號刑事判決⁶⁴為目前對加密貨幣定性上最重要的實務判決。該判決理由亦是承前發行貨幣之主管機關即中央銀行、銀行法主管機關即金管會意見，而認為比特幣目前並非銀行等金融機構「收受款項」或「吸收資金」之客體，因此縱使「非銀行」之人（自然人或法人）以比特

⁶⁴ 臺灣高等法院 107 年度金上訴字第 83 號刑事判決，https://law.judicial.gov.tw/FJUD/default_AD.aspx。該判決目前上訴至最高法院，尚未確定。（最後瀏覽日期：2022 年 1 月 18 日）

幣作為投資契約之標的，非但未違反銀行專業經營原則，更與銀行法第 5 條之 1、第 29 條之 1 之收受款項或吸收資金等應由銀行專業經營之業務內容有別。且比特幣在現實交易上，雖可透過幣託公司轉賣為現金，然此並非透過銀行等金融機構交易，比特幣在銀行等金融機構間亦無強制流通性，不具有清算最終性。不同於一審判決的部分，此判決另外從銀行法第 122 條規定看來：「外國銀行收付款項，除經中央銀行許可收受外國貨幣存款者外，以中華民國國幣為限。」所謂的款項，應該是指通行貨幣，也就是法定貨幣或外國貨幣；資金是指可供使用或運用之金錢，通常以貨幣方式表現，用來進行周轉，滿足創造社會物質財富需要的流通價值。又依照銀行法第 10 條規定：本法稱信託「資金」，謂銀行以受託人地位，收受信託「款項」，依照信託契約約定之條件，為信託人指定之受益人之、利益而經營之「資金」。所以，銀行法講的款項或資金，只是觀察的角度不同，並不是截然不同的概念。「收受款項」或「吸收資金」通常僅係「收受」或「吸收」之被動、主動之地位不同而已。銀行所可以吸收的資金，並不以通行貨幣為限，但還是要以銀行法列舉、主管機關核准辦理的業務有關為限。

該判決指出中央銀行及金管會基於以下三點理由均否定比特幣具有貨幣性質：(1)比特幣目前非為社會大眾遍接受之交易媒介，且其價值不穩定，難以具有記帳單位及價值儲存之功能，不具真正通貨（real currency）特性；(2)比特幣非由任何國家貨幣當局所發行，不具法償效力，亦無發行準備及兌償保證，持有者須承擔可能無法兌償或流通之風險；(3)依據中央銀行法規定，該行發行之貨幣為國幣，對於國內之一切支付，方具有法償效力。該判決因此認定，被害人購買比特幣多為透過幣託公司或其他比特幣平台所購買，即使行為人是以投資、互助為名，收受大眾投入比特幣至平台，再將被害人投入之部分比特幣以上揭方式變現牟利，實際上並未經營銀行特許業務，僅係以比特幣作為投資契約之標的，作為資本市場之金融工具，而與銀行收受存款之貨幣市場存貸行為迥異，自非銀行法所欲管制或處罰之範圍。最後，該判決認為數位虛擬商品之比特幣，與「加密資產」之定性較為接近，目前並非銀行法第 5 條之 1、第 29 條之 1 所稱之「款項」或「資金」，且我國銀行等金融機構於現行制度下亦不可經營比特幣之收受、兌換或交易等業務，依罪刑法定原則，不該當銀行法第 125 條第 1 項前段之違法經營收受存款業務罪。

從上述法院見解脈絡可以得知，司法實務上的意見實係尊重專業單位如中央銀行與金管會對虛擬貨幣所為的專業判斷，同將虛擬貨幣作為「虛擬商品」，以及專業單位對虛擬商品採取低度的監管的態度。這樣的見解其實與前面所引述歐洲中央銀行對虛擬貨幣的看法是一致的。就目前偵查實務上，在尚未將虛擬貨幣納入銀行法條文或新增專法規範的情況下，對於收受比特幣的平台等吸金案件，除非行為人的行為足以該當刑法上的詐欺罪或證券交易法上相關規範等構成要件，否則依照罪刑法定原則，實際上是無法可處，偵查並也沒有太多的著力點。但是這類案件的被害人所暴露的風險，其實與銀行法案件所承受的風險相當，在對於消費者保護及社會法益維持上，檢察官所承受的其實是非戰之罪。

三、洗錢防制及打擊資助恐怖主義規範

加密貨幣也具有支付的功能，但是多是作為交易平台的投機或投資工具。就比特幣應用場景統計⁶⁵，全球支付商家僅約 1%，87%是應用

⁶⁵ Chainalysis (2020), "The 2020 Geography of Cryptocurrency Report," Sep. 2020. <https://ag-pssg-sharedservices-ex.objectstore.gov.bc.ca/ag-pssg-cc-exh-prod-bkt-ex/258%20->

再交易平台。另外，英國金融行為監理局(Financial Conduct Authority, 簡稱 FCA)於 2021 年公布購買虛擬通貨之原因調查⁶⁶，38% 是投機或投資，30%為多元投資組合，作為支付使用者則為 0。並且，虛擬通貨近年多以商品或證券代幣化形式朝向 Futures(類似期貨操作)、ETF(類似股票指數 ETF)或 ICO(類似 IPO)、STO(類似群眾募資)或 Stablecoin(穩定幣，類似電子支付儲值工具或電子貨幣)等類金融商品發展。目前主要國家多傾向採取國際結算銀行(Bank for International Settlements, 簡稱 BIS)總裁 Agustin Carstens 所建議的「相同風險、相同監理」(same risk, same regulation)原則⁶⁷，參照期貨或證券交易法等相關法規為監理；至於穩定幣，國際組

[%20002%20Appendix%20B%20-%202020-Geography-of-Crypto%201.pdf](#)。(最後瀏覽日期：2022 年 1 月 18 日)

⁶⁶ Financial Conduct Authority (2021), “Research Note: Cryptoasset Consumer Research 2021,” Jun. 17. <https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021>。(最後瀏覽日期：2022 年 1 月 19 日)

⁶⁷ Carstens, Agustín, “Money in the Digital Age: What Role for Central Banks?” Speech at the House of Finance, Goethe University, Frankfurt, Feb. 6 2018. 參「中央銀行數位貨幣(CBDC)整備狀況、以及如何因應加密貨幣跨入金融市場」專題報告，頁 10，立法院第 10 屆第 4 會期財政委員會第 8 次全體委員會議。<https://www.cbc.gov.tw/tw/dl-178284-f4f6c762503e41a2a1a2fd6ba7184cd3.html>。

織正在研擬相關監理準則⁶⁸。

目前台灣的虛擬通貨交易量占全球比重甚小，與實體經濟的連結度低，對支付系統、金融穩定及中央銀行貨幣政策實無顯著影響。惟我國曾於 2007 年被亞太防制洗錢組織列為一般追蹤名單，後於 2011 年被列為加強追蹤名單，而於 2018 年進行第三次評鑑，如未能通過，將嚴重影響我國金融機構海外活動。因此，我國於 2016 年 12 月 28 日修正公布洗錢防制法，並於 2017 年 6 月 28 日施行。新修正之洗錢防制法擴大所適用之犯罪類型及範圍，強調我國打擊洗錢犯罪之決心。幸亞太洗錢防制組織(APG) 於 2018 年 11 月完成對我國之第三次評鑑，並於 2019 年 6 月發布初步報告，我國達最佳的「一般追蹤」等級，已脫離加強追蹤名單。因此，不得不審慎評估及重視虛擬貨幣在我國可能造成洗錢防制規範漏洞的問題。

(最後瀏覽日期：2022 年 1 月 19 日)

⁶⁸ 「中央銀行數位貨幣(CBDC)整備狀況、以及如何因應加密貨幣跨入金融市場」專題報告，頁 10，立法院第 10 屆第 4 會期財政委員會第 8 次全體委員會議，頁 8。<https://www.cbc.gov.tw/tw/dl-178284-f4f6c762503e41a2a1a2fd6ba7184cd3.html>。(最後瀏覽日期：2022 年 1 月 19 日)

目前加密貨幣在我國「並非貨幣」，非金管會核准發行的金融商品，目前較常作為「類金融投資商品」，在我國銀行並無法兌換、收受虛擬貨幣，而且現階段台灣的虛擬貨幣交易量占全球比重小，與實體經濟的連結度低，對支付系統、金融穩定及央行貨幣政策無顯著影響⁶⁹。但考量加密貨幣在國際間亦得做為支付工具，而且虛擬貨幣潛在作為洗錢工具之風險，洗錢防制法已率先將「虛擬通貨平台及交易業務事業」納入洗錢防制範疇，並指定「金管會」擔任此事業的防制洗錢主管機關，但「僅為洗錢防制目的」，並不涉及其產業治理、業務經營、消費者保護等議題，並於今年4月7日指定本事業的範圍。行政院於2021年6月30日通過「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法⁷⁰」，除了該辦法中的第7條由金融監督管理委員會另定施行日期以外，其餘條文於2021年7月1日開始施行⁷¹。此辦

⁶⁹ 同前註，頁8至9。

⁷⁰ 虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法，<https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=G0380268>。(最後瀏覽日期：2022年1月21日)

⁷¹ 第18條：本辦法除第七條由本會另定施行日期外，自中華民國一百一十年七月一日施行。

法是洗錢防制法第 5 條第 2 項適用同法第 6 條第 3 項、第 7 條第 4 項前段、第 8 條第 3 項、第 9 條第 3 項、第 10 條第 3 項及資恐防制法第 7 條第 5 項規定訂定，並依據「洗錢防制法」第 5 條第 4 項指定「虛擬通貨平台及交易業務事業之範圍」。

上開辦法在第 2 條第 1 項第 2 款定義虛擬通貨為「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」。該辦法第 2 條第 1 項第 1 款⁷²的平台須如金融機構般負起瞭解您的客戶與客戶盡職調查義務。因此，金管會 110 年 9 月 30 日金管銀法字第 11002729181 號函釋⁷³，要求在國內設立登記之

⁷² 一、虛擬通貨平台及交易業務事業（以下簡稱本事業）：指為他人從事下列活動為業者（一）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。（二）虛擬通貨間之交換。（三）進行虛擬通貨之移轉。（四）保管、管理虛擬通貨或提供相關管理工具。（五）參與及提供虛擬通貨發行或銷售之相關金融服務。

⁷³ 參金管會 110 年 9 月 30 日金管銀法字第 11002729181 號函釋：
https://www.banking.gov.tw/ch/home.jsp?id=190&parentpath=0,3&mcustomize=lawnew_view.jsp&d

虛擬通貨平台及交易業務事業出具洗錢防制法令遵循聲明文件與資料，如聲明書、聲明人資料表以及經會計師複核之防制洗錢及打擊資恐內部控制與稽核制度檢查表等。另外依據該辦法第 3 條至第 6 條、第 9 條建立確認客戶身分及持續審查機制，其中規定包括不得接受客戶以匿名或使用假名建立或維持業務關係、以可靠、獨立來源之文件、資料或資訊，辨識及驗證客戶及代理人身分、辨識客戶實質受益人、應瞭解客戶業務關係之目的及性質、確認客戶身分措施及持續審查機制應以風險基礎方法⁷⁴決定其執行強度、應運用風險管理系統確認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等。第 13 條則規定進行資恐防制法第 7 條第 3 項之通報義務。

上開辦法，對於虛擬通貨、平台以及事業範圍有明確的定義，具

[ataserno=202109300009](#)。(最後瀏覽日期：2022 年 1 月 21 日)

⁷⁴ 參辦法第 2 條第 1 項第 6 款：「風險基礎方法：指本事業應確認、評估及瞭解其暴露之洗錢及資恐風險，並採取適當防制洗錢及打擊資恐措施，以有效降低此類風險。依該方法，對較高風險情形應採取加強措施，對較低風險情形，則可採取相對簡化措施，以有效分配資源，並以最適當且有效之方法，降低經其確認之洗錢及資恐風險。」

體的政策執行上包括客戶盡職調查與持續監控、風險基礎方法、通報義務等相關規定，可以見得與本文前述的 AMLD5 規定一致。不過此辦法有僅就是虛擬貨幣洗錢防制的法規架構而已，就我國虛擬貨幣的法規架構，例如消費者保護、產業管理的制度建置上的發展，仍有待發展。

四、我國虛擬貨幣所涉犯罪之統計

根據「新興金融科技遭濫用於犯罪之研究⁷⁵」一文研究團隊所做的統計數據，自 2016 年起至 2021 年 9 月 27 日止，於司法院法學資料庫上判決檢索結果，扣除判決內容雖提及虛擬通貨、虛擬貨幣、加密貨幣但與案情無實質關連性的判決，實際分析有 819 筆判決。而該文中將此 819 篇判決歸納為交易標的型、交付個人資料型、交付虛擬通貨帳戶型、支付對價型、不法所得洗錢型、挖礦竊電型等六大類型。其中，以將虛擬貨幣作為投資或買賣標的的詐欺或侵占案件的「交易

⁷⁵ 林繼恆、楊岳平、李鎰如，新興金融科技遭濫用於犯罪之研究，刑事政策與犯罪防治研究，第 30 期，2021 年 12 月。

標的型」為大宗，總計有 432 件，佔所有案件總數之 53%⁷⁶。而以提供金融帳戶、行動電話門號等個人資料的「交付個人資料型」共有 222 件，佔總數之 27%，但是這類案件於 2020 年的 41 件，至 2021 年 9 月大幅增加至 145 件⁷⁷。前者與性質雷同的「交付虛擬通貨帳戶型」所佔總數 8%⁷⁸相加總，是第二大宗的犯罪型態。而做為「支付對價」型的案件，只有 72 件，占案件數量之 9%⁷⁹。將詐欺等前不法行為所得，兌換為虛擬貨幣或是轉入非實名制之虛擬貨幣錢包形成金流斷點，亦即將虛擬貨幣作為不法所得之洗錢所用的「不法所得洗錢型」，總計占案件總數 15 件，佔比只有 2%⁸⁰。然而，值得注意的是，因為前揭文章所依據的數據是「判決」檢索結果，因此只有經檢察官提起公诉、聲請簡易判決處刑，或是經法院裁定交付審判案件才會前文研究

⁷⁶ 同前註，頁 186。

⁷⁷ 同前註，頁 187。

⁷⁸ 同前註，頁 188。

⁷⁹ 同前註，頁 189。

⁸⁰ 同前註，頁 190。

的基數。但就筆者在偵查的經驗，「不法所得洗錢型」在偵查階段的「被告」與「被害人」，通常同時是被詐欺的對象，正因如此，在偵查中此類型的被告，常常因為主觀上欠缺洗錢或詐欺之犯意，因而經檢察官為不起訴處分，實際上與「不法所得洗錢型」相關的犯罪數，應該遠比 15 件還多。因此，雖然金管會認為虛擬貨幣用於支付功能的情形上不普及，因此分析目前我國虛擬貨幣洗錢風險尚低，但實則虛擬貨幣能在生活中自由買賣、移轉或交換，可以透過平台以法定貨幣交換，亦可與不同種類的虛擬貨幣相互交換，虛擬貨幣的流通性可能就與現實貨幣相近，再加上區塊鏈技術平台的匿名性⁸¹，筆者認為近年來不法分子運用虛擬貨幣的匿名性及跨國性查緝不易來製造金流斷點，躲避追緝的情形，遠比吾人意識到的程度還更氾濫。

⁸¹ 吳婕華，區塊鏈與虛擬貨幣法律專題（二十一）虛擬通貨平台的監管—以防制洗錢及打擊資恐為中，
<https://zhongyinlawyer.com.tw/%E5%8D%80%E5%A1%8A%E9%8F%88%E8%88%87%E8%99%9B%E6%93%AC%E8%B2%A8%E5%B9%A3%E6%B3%95%E5%BE%8B%E5%B0%88%E9%A1%8C-%E4%BA%8C%E5%8D%81-%E8%99%9B%E6%93%AC%E9%80%9A%E8%B2%A8%E5%B9%B3%E5%8F%B0%E7%9A%84/>。
（最後瀏覽日期：2022 年 1 月 22 日）

伍、結論

著名投資者股神巴菲特（Warren Buffet）曾表示比特幣是「老鼠藥的平方」⁸²（Rat Poison Squared），並表示它們不是持久的交換手段或價值儲存手段。鴻海科技集團創辦人郭台銘針對近來最熱門的元宇宙及虛擬貨幣議題也表示：「貨幣永遠都不可能去中心化，虛擬貨幣是假議題，只有地下經濟會用虛擬貨幣⁸³。」無論對虛擬貨幣的觀感是正面或負面，虛擬貨幣持續穩定發展已經是趨勢。加密貨幣的優點是如此顯而易見的，加密貨幣在交易上，在轉移價值方面，比紙面等傳統價值移轉方式更有效率。儘管加密貨幣存在著價值來源或假名交易等缺點，但就因此將其完全認定會被用於現代洗錢或資助恐怖主義的用途，似乎也略顯不夠公允。加密貨幣的本質，尤其是其匿名性及便利性，確實是受犯罪分子青睞而用其進行非法活動媒介的原因。但是，任何司法管轄區全面禁止加密貨幣將不利於技術及金融的創新，

⁸² Warren Buffet Archive, <https://buffett.cnbc.com/2018/06/26/buffett-a-z-bitcoinand-cryptocurrencies.html>。（最後瀏覽日期：2022年1月18日）

⁸³ 參 <https://www.gvm.com.tw/article/84913>。（最後瀏覽日期：2022年1月22日）

實際上要全面禁止也窒礙難行。立委李貴敏在邀請中央銀行、金管會、財政部等財金部會首長赴立院財政委員會就「中央銀行數位貨幣 CBDC 整備狀況，以及如何因應加密貨幣跨入金融市場」案進行報告前曾表示：「虛擬貨幣逐步跨入金融市場已是不爭事實，堵不如疏，為了讓業者從以往的無規範野蠻生長步入監管範疇，財金部門實應重新審視是否在金融商品範疇上部分鬆綁加密貨幣及其衍生商品的限制。國人如果能以較便利地在合法管道購得金管會核准的加密貨幣衍生或投資商品，詐騙案件應該也可以減少，而可未雨綢繆防堵投資詐騙案件⁸⁴」。

歐盟經過 30 多年洗錢防制及打擊資助恐怖主義的立法，已經發布五個洗錢防制指令，最新的洗錢防制指令也已有基本的樣貌。隨著其歐盟成員國的實施，這些指令對於減輕洗錢和資助恐怖主義對世界造成的負面影響至關重要，也影響了我國對虛擬貨幣洗錢的法律規範。然而，加密貨幣的發展日新月異，以及法規實行的時間還不夠久，仍

⁸⁴ 參 <https://www.mypeoplevol.com/Article/8950>。(最後瀏覽日期：2022 年 1 月 21 日)

有實際執行面的問題尚待調整，必須定期進行深入及審慎的審查，以便在不嚴重損害行業利益的情況，更健全相關的法律規範密度。

從本文前面所提出的歐盟相關指令及我國目前現有對於加密貨幣所有的法律規範，主要是在主管機關監管上，於行政層面課予義務主體「瞭解您的客戶」、「客戶盡職調查」，另外在特定的情形下進行通報。以上的義務內容，雖然一直都是洗錢防制相關規範的核心規定事項，但整個歐盟似乎距離所有成員國都達到歐盟指定所要求的嚴格標準，還有很長的路要走，而歐盟範圍內的全面合規將大幅增強監控透過加密貨幣洗錢或資助恐怖主義的影響。歐盟實際面上的實行結果，也將做為我國的借鏡。

另外 AMLD5 有關金融情報中心的規範，尚未明確全面落實在我國加密貨幣相關法律架構下。虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法目前規定需實名制，在第 10 條有保存記錄憑證的規定，第 11 條要求對新臺幣 50 萬元以上之現金交易，應依法務部調查局所定之申報格式及方式，向法務部調查局申報。第 12 條規定對客戶交易的持續監控義務。然本文認為，應積極建置同金融情報中心相等概

念的金融科技犯罪共享資料庫。目前法務部調查局雖有洗錢防制處此金融情報中心，惟目前其工作項目⁸⁵係以洗錢防制相關為核心，例如洗錢防制策略之研究及法規之協商訂定；金融機構申報疑似洗錢交易資料之受理、分析、處理及運用；金融機構申報大額通貨交易資料與海關通報旅客或隨交通工具服務之人員攜帶大額外幣現鈔或有價證券入出國境資料之受理、分析、處理及運用；國內其他機關洗錢案件之協查及有關洗錢防制業務之協調、聯繫；與國外洗錢防制有關機構之資訊交換、跨國洗錢案件合作調查之聯繫、規劃及執行；洗錢防制工作年報、工作手冊之編修與資料之建檔及管理；其他有關洗錢防制事項。但就 AMLD5 的國家金融情報中心，是被授權可以取得加密貨幣持有者地址等功能。就偵查實務來說，這是最有效打擊透過虛擬貨幣製造金流斷點的方式。這其實跟尚未定施行時間的虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法第 7 條「旅行規則」(Travel Rule)，及要求虛擬貨幣之轉出方及接收方應落實實名制及虛擬貨幣

⁸⁵ 參 <https://www.mjib.gov.tw/EditPage/?PageID=cb9c3a93-6c70-4b68-bedd-4b2537dcbd27>。(最後瀏覽日期：2022 年 1 月 21 日)

金流資訊保留有關。這樣一來，可以有效解決檢調機關難以追查虛擬貨幣流向之問題，也有助於追回不法所得之落實。