國立臺灣大學法律學院科際整合法律學研究所

碩士論文

Graduate Institute of Interdisciplinary Legal Studies

College of Law

National Taiwan University

Master's Thesis

比特幣之搜索及扣押

Search and Seizure of Bitcoin

李星逸

Sing-Yi Li

指導教授：蘇凱平 博士

Advisor: Kai-Ping Su, J.S.D.

中華民國 113 年 1 月

Jan, 2024

doi:10.6342/NTU202400684

摘要

隨著比特幣衍生的一連串金融詐欺或犯罪情事日益氾濫，其應被妥善處理的重要性愈發顯著。尤其執法人員如何完成搜索及扣押比特幣的任務，往往是此類刑案能否取得供法院審理時調查的證據資料之關鍵。有鑑於此，本文選擇「對比特幣實施搜索、扣押時，如何妥善適用我國現行刑事訴訟法之規範？」以及「對比特幣實施搜索、扣押時，相應的具體流程與思惟為何？」兩層次探討。

就「對比特幣實施搜索、扣押時，如何妥善適用我國現行刑事訴訟法之規範？」此層面而言，首先針對特定明確原則，本文指出因著比特幣與一般電磁紀錄不同的技術內涵，亦即比特幣位址與私鑰皆無法隨使用者或他人的意志為任何更動的特性。在偵查資訊充足的狀況下，應將搜索票上的搜索客體分依冷錢包、熱錢包記載成「比特幣位址、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的筆記型電腦」與「比特幣位址、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的熱錢包程式、筆記型電腦」，以降低執法人員誤判搜索或扣押客體的風險，避免過度侵害受搜索人的隱私。

接下來針對一目瞭然法則，倘執法人員為搜索、扣押比特幣，在現場接觸受搜索人的電子載體，檢視受搜索人使用的比特幣位址係位於其中何處時，發現搜索票上未記載之本案應扣押電磁紀錄，或者另案應扣押之電磁紀錄。本文參酌 United States v. Carey 案，提出透過執法人員係出於惡意搜索令狀記載以外的電磁紀錄與否，作為是否適用一目瞭然法則的審查標準。

至於執法人員對交易所錢包實施搜索、扣押時，本文基於財產權社會義務與加密技術或驗證機制不盡相同的理由，嘗試透過虛擬資產平台及交易業務事業（VASP）公會訂定的自律規範，建構虛擬資產平台配合執法人員的協力義務，不僅得避免洗錢防制法第 13 條第 1 項或虛擬通貨事業洗防辦法第 7 條規定之下，虛擬資產平台執行上遭遇的技術困難，亦可滿足執法人員實務上的執法需求，降低其執法成本。

就「對比特幣實施搜索、扣押時，相應的具體流程與思惟為何？」此層面而言，在我國實務工作者發展出的若干搜索、扣押比特幣作法之基礎上，本文嘗試從私鑰控制權限者的角度，分別形塑數個搜索、扣押比特幣時，在執行面可供執法人員參考的思路與流程。

關鍵詞：比特幣、搜索及扣押、特定明確原則、一目瞭然法則、協力義務

。

doi:10.6342/NTU202400684

ABSTRACT

As a series of financial fraud or crimes derived from Bitcoin become more common, the importance of properly handling it becomes obvious. In particular, how law enforcement officials complete the task of searching for and seizing Bitcoin is often the key to whether obtain evidence for investigation in court trials. In view of this, this article chooses two levels: "When searching for and seizing Bitcoin, how do we properly apply the current criminal procedure law?" and "When searching for and seizing Bitcoin, what are the corresponding specific procedures and thoughts?" to discuss.

Regarding "When searching for and seizing Bitcoin, how do we properly apply the current criminal procedure law?", this article mentions The Particularity Requirement at fist. Then, this article points out that Bitcoin has different technical features from general electronic records, that is, the Bitcoin address and private key cannot be changed by the user's or other people's will. When the investigation information is sufficient, the searching for objects on the search warrant should be recorded as "the Bitcoin address, the private key required to transfer the target Bitcoin, and the laptop that can store the private key" (the cold wallet) and "Bitcoin address, private key required to transfer the target Bitcoin, and hot wallet program that may store the private key, and the laptop that can store the private key" (the hot wallet). In this way, we could anticipate reducing the risk of law enforcement officials' misjudgment of searching for or seizing objects and avoiding excessive infringement on the privacy of the person being searched.

Next, in order to search and seize Bitcoin, law enforcement officials search the electronic carrier of the person being searched, and the Bitcoin address used by the person being searched. They find that there is the electronic records should be seized in this case, or the electronic records should be seized in another case, but they are not recorded on the search warrant. This article refers to the case of United States v. Carey, and proposes whether law enforcement officials search electronic records other than those recorded in the search warrant with malicious intent as the standard of the Plain View Doctrine.

When law enforcement officials search and seize exchange wallets, this article attempts to use the self-regulatory regulations set by the Virtual Asset Services Providers (VASP) Association to construct the obligation of VASP to assist law enforcement

doi:10.6342/NTU202400684

officials. That is based on the social obligation of property rights and encryption technology or verification mechanisms. Constructing the obligation of VASP to assist law enforcement officials not only avoids the technical difficulties encountered in the execution of the VASP under Article 13, Paragraph 1 of the Money Laundering Prevention Act or Article 7 of Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction, but also meets the needs of law enforcement and reduces the costs of law enforcement.

In terms of "When searching for and seizing Bitcoin, what are the corresponding specific procedures and thoughts?", this article organizes several methods of searching for and seizing Bitcoin developed by practitioners in Taiwan at first. Then, this article attempts to shapes several ideas and processes that can be used as a reference for law enforcement officials when searching for and seizing Bitcoin.

Key Words: Bitcoin, Search and Seizure, The Particularity Requirement, The Plain View Doctrine, the obligation of VASP to assist law enforcement officials

doi:10.6342/NTU202400684

目次

doi:10.6342/NTU202400684

doi:10.6342/NTU202400684

第一章 緒論

自 1946 年以真空管設計出第一部通用型電腦，直到如今身處萬物皆可聯網的數位化時代，人們已習慣將大量的資訊儲存於消費性電子產品，並利用網際網路的廣泛連結，從事商務、娛樂或日常聯絡等人際互動，包括電子郵件、線上遊戲與各種電子支付工具[1]。這些資訊科技日新月異的演進，除了大幅改變現代社會的生活樣貌，連帶地，也影響植基於社會文化的法律秩序——較常見的，例如這些數位資訊一旦涉及刑事案件，執法人員對其施以強制處分，成為供法院審理時調查的證據資料。

縱然數位證據在司法程序中被使用的情形並不罕見，但我國傳統意義的搜索、扣押，一般係指以身體、物件、住宅或者其他有體物為目標，進行搜查檢索、或取得其占有之強制處分，在文義上得搜索、扣押的客體，其實不包含數位資訊[2]。直至 2001 年，立法者方於刑事訴訟法第 122 條、第 128 條第 2 項增列「電磁紀錄」為得受搜索之客體，然未見其修訂相關的具體執法方法[3]。

尤其近十餘年來，虛擬通貨打著金融創新的大旗，其種類與市值皆已茁壯至

[1] 施威銘、吳文立、李亮生、陳源宏（2010），《資訊科技概論》，頁 11，臺北：旗立資訊。

[2] 於 1967 年 1 月 28 日公布後施行的舊刑事訴訟法，第 122 條：「（第一項）對於被告之身體、物件及住宅或其他處所，必要時得搜索之。（第二項）對於第三人之身體、物件及住宅或其他處所，以有相當理由可信為被告或應扣押之物存在時為限，得搜索之。」、第 128 條第 2 項：「搜索票，應記載左列事項：一、應搜索之被告或應扣押之物。二、應加搜索之處所、身體或物件。」

[3] 於 2001 年 1 月 12 日公布、同年 7 月 1 日後施行的現行刑事訴訟法，第 122 條：「（第一項）對於被告或犯罪嫌疑人之身體、物件、**電磁紀錄**及住宅或其他處所，必要時得搜索之。（第二項）對於第三人之身體、物件、**電磁紀錄**及住宅或其他處所，以有相當理由可信為被告或犯罪嫌疑人或應扣押之物或**電磁紀錄**存在時為限，得搜索之。」、第 128 條第 2 項：「搜索票，應記載下列事項：一、案由。二、應搜索之被告、犯罪嫌疑人或應扣押之物。但被告或犯罪嫌疑人不明時，得不予記載。三、應加搜索之處所、身體、物件或**電磁紀錄**。四、有效期間，逾期不得執行搜索及搜索後應將搜索票交還之意旨。」

doi:10.6342/NTU202400684

令人無法忽視的程度[4]。隨之而來的，除了各種運用虛擬通貨的新興商業型態，便是涉及虛擬通貨的刑事案件。面對這類型的數位資訊，我國現行法制、以及目前實務上執行搜索、扣押電磁紀錄的方式，能否滿足執法人員對其施以搜索、扣押的執法需求，實有待商榷。

而這些眾多種類的虛擬通貨當中，又以比特幣（Bitcoin）在絕大多數時期為市值占比最高、流通量最多的虛擬通貨，相較其他幣別，更容易為不法份子利用於隱匿犯罪所得等不法情事[5]。基於上述，本文選擇此幣種作為研究對象實具有一定程度的研究價值。

本文的問題意識聚焦於「執法人員搜索、扣押比特幣時，如何妥善適用現行刑事訴訟法的規定？」、「執法人員搜索、扣押比特幣的執行方法，是否得與搜扣有體物、或搜扣一般數位資訊的方法相同？」。這些問題隨著虛擬通貨衍生的一連串金融詐欺或犯罪情事日益氾濫，其應被妥善處理的重要性愈發顯著，尤在偵查實務與適用規範這兩方面特別具有價值[6]。在偵查實務上，比特幣儲存於載體的樣態相較一般數位資訊來得複雜，故執法人員如何因應此種新穎技術，順利地執行搜索、扣押比特幣的任務，是道迫切需要被解決的難題[7]。另在適用規範上，即使執法人員可排除一切技術障礙，完成搜索、扣押比特幣的任務，但於現行刑事訴訟法的框架之下，執行過程中可能出現若干適用規定的爭議，亦有待

[4] 截至 2020 年年底，全球的虛擬通貨多達 8,800 種，總市值約 1.6 兆美元，其中比特幣約占 6 成居首。請參見：中央銀行（2021），〈虛擬通貨近期發展及國際監管概況〉，《存款保險資訊季刊》，34 卷 2 期，頁 14。

[5] 中央銀行，前揭註 4，頁 14；楊岳平（2023），〈虛擬通貨監管的比較法發展與我國監管架構芻議〉，《月旦法學雜誌》，335 期，頁 41。

[6] 王志誠、何雨柔（2020），〈論虛擬貨幣之發展與監理趨勢〉，《財稅研究》，49 卷 3 期，頁 88。

[7] 以比特幣錢包為例，實際上其未儲存比特幣，而僅是存放移轉或交易比特幣的工具：公、私鑰與比特幣位址，一般係儲存於比特幣錢包內，並視錢包種類而可能是線上平台、瀏覽器、電腦、行動裝置或紙張等載體。相關介紹請參見本文後述「第二章、第一節、區塊鏈、比特幣位址與錢包」的說明。

doi:10.6342/NTU202400684

本文於後續章節分析釐清。

於本章中，本文將會在第一節提出研究動機，在第二節具體說明問題意識、確認研究範圍，第三節則針對問題意識進行初步的文獻爬梳，並在第四節論述本文的研究方法，最後在第五節說明本研究的架構。

doi:10.6342/NTU202400684

第一節、研究動機

如前文所述，我國傳統意義上的搜索、扣押，其對象侷限於身體、物件、住宅或者其他有體物，尚不包括數位資訊。2001 年立法者方於刑事訴訟法第 122 條、第 128 條第 2 項增列「電磁紀錄」為得受搜索之客體後，執法人員搜索、扣押數位資訊方有明文依據。比特幣之本質固屬電磁紀錄，但其性質卻與一般常見的數位資訊（如文字檔、圖像檔或影音檔）差異甚多[8]。當執法人員對這些比特幣實施搜索、扣押時，如何妥善適用現行刑事訴訟法的規範，令本文產生好奇。

區塊鏈（blockchain）作為一種「分散式帳本技術」（Distributed Ledger Technology）的應用，廣泛被使用於比特幣、以太幣（Ether）等類似性質的虛擬通貨[9]。這些以區塊鏈為基礎的虛擬通貨，由於尚處金融監理政策的灰色地帶，因此也成為不法份子規避查緝、從事犯罪的新興科技工具。諸如惡名昭彰的 Silk Road 網站，即係創辦人 Ross William Ulbricht 於 2011 年透過 Tor 架構的暗網，且採取支付虛擬通貨的方式，提供買賣雙方可從中匿名進行毒品、槍枝或兒少情色作品等不法交易之線上平台。多國的檢警機關當時苦於未有因應虛擬通貨犯罪的偵查方法，縱能順利逮捕嫌疑人，亦時常無法順利扣押所有涉案的虛擬通貨、追回不法金流[10]。

---

[8] 關於比特幣的技術內涵，請參見本文後述「第二章、第一節、第二項、區塊鏈的本質與技術」的說明。

[9] 關於本文探討的虛擬通貨，係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；較詳細的定義論述請參見本章後述「第二節、研究問題」的說明。

[10] *See* U.S. Department of Justice, *United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars*, THE UNITED STATES DEPARTMENT of JUSTICE (NOV. 5, 2020), https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us (last visited Fed. 20, 2022); Federal Bureau of Investigation, *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*, THE FEDERAL BUREAU OF INVESTIGATION (OCT. 25, 2013), https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (last visited Fed. 21, 2022).

doi:10.6342/NTU202400684

近年來，國際組織、各國政府間已多有針對虛擬通貨犯罪著手草擬、制定新的監管政策或反洗錢、反資恐指引[11]。我國雖亦有隨之調整相關的監管政策或指引，但在偵查實務與刑事程序法領域仍對包括比特幣在內的虛擬通貨相對陌生。如何針對比特幣去中心化、不可竄改的特性提出相應的偵查方法，以供執法人員進行搜索、扣押時參考？在執法人員搜索、扣押比特幣的過程中，如何妥善適用現行刑事訴訟法的規定，以供司法機關據以審查該些強制處分的合法性？這些影響追訴比特幣犯罪成敗之重點，引發本文的好奇心。尤其經初步的文獻回顧後，發現針對上述議題提出正面回應的論述並不多見，促使本文欲進一步研究、釐清相關問題。

第二節、研究問題

比特幣係當前市值最大的虛擬通貨，其在公有鏈的架構上具有去中心化、匿名或不可竄改等特性，具有與有體物、一般數位資訊不同的技術內涵[12]。因此本文便選擇從「執法人員搜索、扣押比特幣的執行方法，是否得與搜扣一般數位資訊的方法相同？」、「執法人員搜索、扣押比特幣時，如何妥善適用現行刑事訴訟法的規定？」這兩個問題意識出發，深入探討相關執行方法與現行規範，以作為執法人員對虛擬通貨實施強制處分的參考建議。

[11] *See* FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (2021).

[12] 當前虛擬通貨的總市值約當為 1.18 兆美元，其中比特幣佔約 48.1%、以太幣佔約 19.1%。請參見：Global Cryptocurrency Charts: Total Cryptocurrency Market Cap，COINMARKETCAP，https://coinmarketcap.com/charts/ (last visited Jul. 29, 2023).

doi:10.6342/NTU202400684

而本文所稱的「虛擬通貨」，係我國金融監督管理委員會於 2021 年發布之《虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法》中，第 2 條第 2 款本文所稱：「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」。比特幣係於比特幣區塊鏈上運作的幣種，符合前揭定義下的虛擬通貨。

綜上，本文將研究問題設定為「對比特幣實施搜索、扣押時，如何妥善適用我國現行刑事訴訟法之規範？」以及「對比特幣實施搜索、扣押時，相應的具體流程與思惟為何？」兩層次進行探討。

第三節、文獻回顧

針對上開研究問題，本文於第三節將先回顧文獻資料，整理現有論述處理到的面向後，再闡明本文希望進一步研究的議題。

第一項、既有文獻資料整理 [13]

關於比特幣、虛擬通貨等議題在學術上的討論，國內既有的期刊文獻多集中金融監管或產業發展方面 [14]。就前一節提出的研究問題，本文在刪除重複列舉以

[13] 根據國家圖書館期刊文獻資料庫（https://tpl.ncl.edu.tw/NclService/）收錄的文獻資料，於 2023 年 07 月 29 日在查詢條件分別輸入 9 組關鍵字組別如下：「比特幣 AND 搜索」、「比特幣 AND 扣押」、「比特幣 AND 犯罪」、「虛擬通貨 AND 搜索」、「虛擬通貨 AND 扣押」、「虛擬通貨 AND 犯罪」、「虛擬貨幣 AND 搜索」、「虛擬貨幣 AND 扣押」、「虛擬貨幣 AND 犯罪」，總共可得 18 筆文獻。

[14] 根據國家圖書館期刊文獻資料庫（https://tpl.ncl.edu.tw/NclService/）收錄的文獻資料，於 2023 年 07 月 29 日在查詢條件分別輸入 3 組關鍵字組別如下：「比特幣」、「虛擬通貨」、「虛擬貨

doi:10.6342/NTU202400684

及與研究問題較無關的文獻後，僅餘 4 筆文獻[15]。

一、搜索、扣押比特幣或虛擬通貨於現行刑事訴訟法遭遇的爭議

關於搜索、扣押比特幣或虛擬通貨於現行刑事訴訟法遭遇的爭議，直接就此討論的我國文獻僅有數篇。有先從虛擬通貨是否為適格的扣押客體檢討，認為其本質既非物、亦不是權利，得否按刑事訴訟法第 133 條第 1 項、第 3 項、第 4 項作為保全沒收扣押之標的，不無疑義[16]。惟有文獻對前揭見解持相反意見：承認虛擬通貨屬同法第 122 條、第 129 條第 2 項第 3 款的電磁紀錄。一般虛擬通貨交易所需的錢包位址、存取虛擬通貨之私鑰皆非有體物，一般儲存於電腦硬碟、行動裝置或網路伺服器等有體物。若欲取得這些有體物的占有支配，可依循同法搜索、扣押的相關規定進行[17]。

另有文獻則從如何對新興金融科技造成的網路犯罪為刑事訴追出發，直接將虛擬通貨視為對電磁紀錄搜索、扣押的其中一環。除了釐清電腦或者行動裝置之鑑識屬於實質意義的搜索，並透過權衡發見真實以及隱私權與財產權的保護，分析對電磁紀錄實施搜索、扣押時發生的若干法律問題。例如是否需對扣押載體儲存

幣」，總共可得 152 筆文獻，但多與本文的研究問題無直接關聯，相關文獻請參見如：臧正運（2020），〈論密碼資產的興起與金融監理機關之職能變革〉，《月旦法學雜誌》，301 期，頁 64-85；曾宛如（2023），〈金融科技對金融市場、證券規範及公司治理之衝擊與影響〉，《月旦法學雜誌》，332 期，頁 89-117。

[15] 僅餘的 4 筆國內文獻分別是：施志鴻（2018），〈比特幣相關犯罪類型與因應作為之探討〉，《資訊、科技與社會學報》，18 卷 26 期，頁 64-79。鄭文中（2020），〈犯罪沒收與虛擬貨幣之保全扣押初探〉，《商業法律與財金期刊》，3 卷 1 期，頁 93-113。恆業法律事務所（2021），《新興金融科技遭濫用於犯罪之研究成果報告書》。羅韋淵（2023），〈偵辦虛擬貨幣相關犯罪之戰略思考—美國司法部史上最大查扣案之借鏡〉，《檢察新論》，32 期，頁 23-43。

[16] 鄭文中，前揭註 15，頁 105。惟注意此文未論及虛擬通貨是否為適格的「搜索」客體。

[17] 恆 業法律事務所，前揭註 15，頁 142-143。

doi:10.6342/NTU202400684

的所有檔案製作扣押物細目清單等爭議[18]。

二、搜索、扣押比特幣或虛擬通貨的偵查方法

在搜索、扣押比特幣或虛擬通貨的偵查方法上，學者、實務工作者為因應此種新穎科技的技術特性，諸如比特幣位址（Bitcoin Address）及錢包（Wallet）等特徵，皆有對以比特幣為例的搜索、扣押方法提出若干建議[19]。具體而言，包括：

1.從被搜索或被扣押人處尋獲並移轉「私鑰」（private key）—其可能儲存於各不同種類的錢包，或以「助記詞」（Mnemonic Phrase）的樣態出現[20]。

2.利用演算法將蒐集到的比特幣位址資訊交叉比對，進一步轉化成使用者層次的資料，發展比特幣交易的追蹤技術[21]。

3.整合線上偵查所獲的比特幣交易資訊、以及一般偵查所得的相關線下資訊（off-network information），藉以建構出嫌疑人的行為與樣態[22]。

---

[18] 恆業法律事務所，前揭註 15，頁 144-145。

[19] 法務部調查局（2018），《中華民國 106 年洗錢防制工作年報》，頁 68-78；施志鴻，前揭註 15，頁 75-76；黃柏翔（2019），〈新興電腦犯罪偵辦手法之研究—以虛擬貨幣犯罪為中心—〉，頁 24-47；羅韋淵，前揭註 15，頁 23-43；Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, 3 SECURITY & PRIVACY IN SOC. NETWORKS 1, 1-28 (2011)；Dorit Ron & Adi Shamir, *Quantitative Analysis of the Full Bitcoin Transaction Graph*, IN FINANCIAL CRYPTOGRAPHY AND DATA SECURITY:17TH INTERNATIONAL CONFERENCE, FC 2013, OKINAWA, JAPAN, APRIL 1-5, 2013, REVISED SELECTED PAPERS 6-24 (Ahmad-Reza Sadeghi ed., 2013)；Angela S.M. Irwin & Adam B. Turner, *Illicit Bitcoin transactions: challenges in getting to the who, what, when and where*, 21(3) J. MONEY LAUNDERING CONTROL 297, 297-313 (2018).

[20] 扼要地說，私鑰係由特定演算法生成、一般運用於公開金鑰加密技術的工具；助記詞在本質上則為私鑰的另種表現形式，旨在減少使用者儲存或記憶私鑰的負擔。關於上述兩者的詳細介紹，請參見本文後述「第二章、第一節、區塊鏈、比特幣位址與錢包」的說明。

[21] 施志鴻，前揭註 15，頁 75-76；羅韋淵，前揭註 15，頁 35；Ron & Shamir, *supra* note 19, at 10-20.

[22] Reid & Harrigan, *supra* note 19, at 15-17.

doi:10.6342/NTU202400684

第二項、本文希望進一步討論的議題

論及比特幣或虛擬通貨時，本節第一項「一、搜索、扣押比特幣或虛擬通貨於現行刑事訴訟法遭遇的爭議」提及的文獻，有針對其去中心化、不可竄改的特性為描述，並提出「於需要扣押電磁紀錄時應特別釋明之，法院同意後方可搜索、扣押」的意見，以取得追訴犯罪與保障人民基本權二者間的衡平[23]。然而，執法人員為扣押比特幣，在搜索票聲請書聲請書上究應如何記載或釋明，方得謂有「特別釋明之」？易言之，執法人員在前揭聲請書應具體記載或釋明至何種程度，法院審查後所核發的搜索票，方不至於成為執法人員濫行搜索或扣押的工具？故針對搜索、扣押比特幣，執法人員應如何就包括上述爭議在內的問題，妥善適用我國現行刑事訴訟法，本文認為實有必要再行深入探討。

另一方面，本節第一項「二、搜索、扣押比特幣或虛擬通貨的偵查方法」提及的文獻，多係針對比特幣提出的相關偵查方法建議，偏重技術、如何順利扣押比特幣，固對發見真實之目的有所裨益。惟在法治國原則的誡命之下，對比特幣實施強制處分亦應顧及人民財產權、隱私權的保障。於搜索、扣押比特幣的過程中，執法人員蒐集比特幣位址資訊、取得私鑰等動作，是否已然侵害財產權或隱私權存在些許爭議，值得本文對此加以著墨討論。

[23] 恆業法律事務所，前揭註 15，頁 145-146。

doi:10.6342/NTU202400684

第四節、研究方法

為了適切回應研究問題，本文選擇文獻分析法與功能比較法作為研究方法，本節即是就這兩者的扼要介紹，以及如何使用於處理研究問題。

第一項、文獻分析法

文獻分析法（Document Analysis）係指透過蒐集相關文獻資料，從而全面且精準地掌握研究問題的方法。首先，應廣泛地利用關鍵字蒐集文獻，包括但不限於專書、期刊論文、統計數據、新聞報導等資訊。接下來，歸納、統整蒐集到的文獻後，再圍繞著研究問題進行分析。經由文獻分析，可幫助研究者釐清研究的背景事實、理論的發展脈絡，認識、瞭解前人的研究內容與貢獻，藉以避免重複勞動[24]。

在實際操作上，本文將先針對研究問題，利用關鍵字搜尋、蒐集國內外相關的文獻資料，諸如專書、期刊論文、研究報告、政府出版品、新聞報導等資訊，接著再從事歸納、統整，以及更進一步的分析。關於搜索、扣押電磁紀錄的相關議題，國內外已累積不少的專書或期刊論文。相較之下，虛擬通貨、比特幣在法學上的討論多集中於金融監管政策[25]。故本文選擇先從搜索、扣押電磁紀錄的文獻蒐集資料。

[24] 葉至誠、葉立誠（2011），《研究方法與論文寫作》，3 版，頁 142-145，新北：商鼎數位。

[25] 相關中文文獻請參見如：楊岳平（2019），〈區塊鏈時代下的證券監管思維挑戰：評金管會最新證券型虛擬通貨監管方案〉，《國立臺灣大學法學論叢》，48 卷特刊，頁 1279-1374；楊岳平（2020），〈金融科技時代下的金融監管挑戰：論虛擬通貨交易平台的監管架構〉，《國立臺灣大學法學論叢》，49 卷特刊，頁 1309-1396；許永欽（2022），〈從 FATF 規範論虛擬資產防制洗錢之監理〉，《月旦律評》，1 期，頁 22-39。

doi:10.6342/NTU202400684

第二項、功能比較法

比較法作為法學方法，其重點在於深入探究不同法秩序之間，雷同與差異形成的原因或背景究竟為何，並據此進一步協助國內法秩序問題的深入理解與解決[26]。一般認為比較法進行的三個主要階段，依序為：1.尋求對於作為比較對象之外國法秩序與相關制度的認識（法的認識）[27]；2.進行對外國法與本國法相關制度或概念差異的澄清與對照；3.根據此等研究所得，檢視外國法與本國法秩序面對共同問題時，發展出不同因應管道的原因，並進而回過頭探討外國相關模式或制度引進本國、或適度供作本國法秩序參考的可能性與限制，藉以協助澄清並解決本國法的問題[28]。

其中，當前較主流的比較方法之一為「功能比較法」（亦稱為「功能方法」，functional method），係立基於「法律的功能在於回應社會問題」、「所有社會本質上都面對相同或大致類似的問題」兩項基礎假設上[29]。在瞭解外國與本國法制為何出現差異後，希冀透過參考外國法域中某項滿足該社會需求、解決社會問題的法規，釐清外國相關法制引進本國、或者供作本國參考的可能性與限制何在[30]。

不法份子相中虛擬通貨匿名、去中心化等特性，利用其所受監管薄弱、乃至無監管的現況，將犯罪金流以虛擬通貨的形式傳輸或匯兌，藉此規避金融機構與主管機關之審查，從事洗錢或資助恐怖主義等違法行徑[31]，係我國與美國共同面

[26] 黃舒芃（2005），〈比較法作為法學方法：以憲法領域之法比較為例〉，《月旦法學雜誌》，120 期，頁 185。
[27] 李建良（2018），〈法學方法與基本權解釋方法導論〉，《人文及社會科學集刊》，30 卷 2 期，頁 242-243；蘇凱平（2022），〈制定司法政策時如何參考外國法－以「蒐集法」與「功能比較法」為中心〉，《台灣法律人》，12 期，頁 110。
[28] 黃舒芃，前揭註 26，頁 190。
[29] 蘇凱平，前揭註 27，頁 101。
[30] 黃舒芃，前揭註 26，頁 190。
[31] 相關中文文獻請參見：吳盈德（2017），〈創新金融科技與洗錢防制趨勢〉，《月旦法學雜誌》，

doi:10.6342/NTU202400684

對的險峻挑戰[32]。然而，目前我國與美國皆無針對搜索、扣押虛擬通貨另行制定規範[33]。因此，本文選擇從與研究問題討論範疇重疊度高的搜索、扣押電磁紀錄之相關規定切入。

以本文將於第二章探討的問題為例，其涉及的主要是刑事訴訟法關於搜索票上的應扣押之物應如何記載，以及附帶扣押、另案扣押的規定。這些條文各自的法理基礎，與美國法上的「特定明確原則」（the requirement of particularity）或「一目瞭然法則」（the Plain View Doctrine）幾乎相同[34]。以一目瞭然法則為例，美國法對其的要件較我國法嚴謹清楚，得適用的範圍亦較我國廣泛，且美國法上數十年來累積的判決中，部分有處理搜索、扣押電磁紀錄與一目瞭然法則間的適用問題[35]。故值得我國借鏡美國法的思路或論述，驗證前揭判決所發揮的功能，是否亦得於我國現行刑事訴訟法對搜索、扣押比特幣在規範上如何妥善適用發揮作用。

267 期，頁 19-29；徐珮菱（2019），〈洗錢防制法制之研究—以區塊鏈及加密數位貨幣為中心〉，《月旦法學雜誌》，288 期，頁 73-99；吳俊志（2021），〈虛擬通貨平台之反洗錢規範〉，《財稅法令半月刊》，44 卷 14 期，頁 9-10。相關英文文獻請參見：Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015). Lissa L. Broome, *Banking on Blockchain*, 21 N.C. J.L. & TECH. 169 (2019).

[32] 我國案例請參見如：聯合新聞網（01/31/2023），〈泰達幣已成詐團洗錢工具 警方依詐欺案追辦〉，https://udn.com/news/story/7320/6939369（最後瀏覽日：02/12/2023）；美國案例請參見如：US Department of Justice, *TWO ARRESTED FOR ALLEGED CONSPIRACY TO LAUNDER $4.5 BILLION IN STOLEN CRYPTOCURRENCY*, THE UNITED STATES DEPARTMENT of JUSTICE (Fed. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency (last visited Feb. 20, 2022).

[33] 我國目前提及虛擬通貨的成文法規定，諸如洗錢防制法第 5 條第 2 項、同條第 4 項以及虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法，皆係以虛擬通貨之定義與監管方式為重心，其等規範內容不涉及如何對虛擬通貨為搜索、扣押。

[34] 扼要地說，「特定明確原則」係指法院核發搜索票時，必須特定明確、清楚記載應搜索之處所及應搜索（拘捕）之被告及應扣押之物；「一目瞭然法則」則係指當執法人員在合法搜索或逮捕時，落入目視範圍內之證據或得沒收物，得無令狀扣押之。關於上述二者的詳細介紹，請參見本文後述「第二章、第二節、搜索扣押比特幣之程序問題」。

[35] 王兆鵬（2001），〈附帶扣押、另案扣押與一目瞭然法則〉，氏著，《路檢、盤查與人權》，頁 34-35，臺北：元照。

doi:10.6342/NTU202400684

第五節、研究架構

第二章探討執法人員對比特幣實施搜索、扣押時，如何妥善適用我國現行刑事訴訟法。本章將先釐清執法人員對比特幣實施搜索、扣押時，可能侵害財產權、隱私權的若干情況，譬如搜索硬體錢包或軟體錢包的過程當中，若由執法人員匯出受搜索人持有硬體錢包或軟體錢包內的私鑰後，原儲存位置的私鑰並不會隨之移除，如此一來受搜索人的財產權是否受有侵害[36]。接著在現行刑事訴訟法的框架下，討論執法人員搜索、扣押比特幣時應如何妥善適用法規，尤將分析重點圍繞在：

1.為了取得儲存於比特幣錢包內的私鑰或助記詞，法院於其核發的搜索票上應為如何之記載？

2.執法人員在搜索現場接觸受搜索人持有的電子載體，檢視其內儲存的電磁紀錄時，倘發現本案應扣押但搜索票未記載，或者另案應扣押的文件檔、影像等電磁紀錄，得否一併扣押之？

就上述第二點的爭議而言，美國法上的 United States v. Carey 案同樣針對執法人員於搜索電子載體時，得否一併扣押令狀上未記載之本案或另案應扣押的電磁紀錄提出看法，值得借鏡其思路或論述以理清問題的全貌。

[36] 硬體錢包是種比特幣錢包，係將私鑰儲存於行動硬碟、專為虛擬通貨設計的隨身碟等硬體設備內。軟體錢包係使用者可下載於電腦、行動電話等電子載體，再利用其為虛擬通貨交易的應用程式。關於硬體錢包、軟體錢包、冷錢包、比特幣位址等專有名詞的詳細介紹，請參見本文後述「第二章、第一節、第五項、比特幣錢包」的說明。

doi:10.6342/NTU202400684

在深入探討研究問題前，本文亦將於第二章介紹區塊鏈、比特幣位址及比特幣錢包這三者的本質與技術。特別於本章第一節介紹這三者的原因，便係比特幣涉及的技術內涵實難在註解處以三言兩語簡單帶過，為便利讀者進入研究問題的討論脈絡，故選擇於本章扼要介紹這三者。第一步首先釐清「區塊鏈」此用語的意義，其本質究指涉何種技術內涵，並解釋區塊鏈具有的功能與作用，是如何在共識機制創造一個去中心化網絡。再者，著重觀察人們如何利用「比特幣位址」、「比特幣錢包」參與比特幣系統的運作——此處關係著執法人員對虛擬通貨實施強制處分時，其事前應為的準備工作，以及搜索、扣押的目標應鎖定何者[37]。

第三章聚焦對交易所錢包實施搜索、扣押時，如何就虛擬資產平台業者配合執法人員之協力義務，如凍結管理特定比特幣位址的交易所錢包，或提供犯罪嫌疑人於交易所登錄的資料與交易紀錄等事，選擇所憑的依據。本章將於第一節依序分析洗錢防制法第 13 條第 1 項、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，以及虛擬資產平台及交易業務事業（VASP）公會自律規範，何者較適合作為前揭協力義務之依據。

在第四章，本文則就我國執法人員如何搜索、扣押比特幣，提出若干想法與建議。本章將先於第一節介紹我國實務發展出對電磁紀錄為搜索、扣押之流程。再就現行電磁紀錄的搜扣流程而言，進一步討論是否適用於搜索、扣押比特幣。於第二節則針對如何順利完成搜索、扣押比特幣，本文選擇從私鑰控制權限者的角度，依託管錢包（Custodial wallet）與非託管錢包（Non-Custodial wallet）這兩種不同類型的比特幣錢包，提出若干可供執法人員參考的操作流程，包括利用幣流

[37] 比特幣位址，功能上近似現實生活中的銀行帳號，可利用它支付或收受比特幣。比特幣錢包係比特幣系統中的一個前端工具，其主要功能係發起轉帳交易、查看交易紀錄，以及管理一組或多組的公、私鑰與比特幣位址。

doi:10.6342/NTU202400684

分析工具追蹤涉有犯罪嫌疑的比特幣位址等建議[38]。最後就上述搜索、扣押比特幣的具體流程，現況可能存在一些執行面上的困難或配套措施欠缺之處，進行說明並反饋若干建議。

最後在第五章，針對研究問題，本章將統整第二章至第四章論述的內容後，再提出相對完整的回覆，以作為本文的結論。

[38] 冷錢包係未連接至網路的錢包，以離線、實體的方式儲存私鑰。熱錢包則係有連接至網路的錢包。

doi:10.6342/NTU202400684

第二章 搜索扣押比特幣於刑事訴訟法上之適用問題

進入研究問題之討論前，為使讀者更能融入後文的說明與分析，本章選擇先於第一節釐清區塊鏈的本質，亦即其具體上究係由何種內容物組成。接續介紹區塊鏈技術的三大特徵：「哈希值」、「公開金鑰加密技術」與「共識協議」，使讀者除了明白區塊鏈網路如何運作，亦能從中瞭解支撐其運作的技術。此外，本文亦進一步說明區塊鏈技術的應用：比特幣，尤著重介紹如何透過比特幣位址、比特幣錢包參與比特幣系統的運作。

本章第二節則主要處理執法人員對比特幣實施搜索、扣押時，如何妥善適用我國現行刑事訴訟法。首先，釐清搜索、扣押比特幣時可能對人民的財產權造成侵害的情況，特別是因著比特幣與一般數位資訊的技術內涵不同，而可能發生爭議的地方。接下來，本文將指出現行刑事訴訟法就比特幣之搜索、扣押而言，在適用上可能產生疑義之處，尤其係在有體物的搜索、扣押程序中較少遭遇的問題，包括如：

1.為取得儲存於比特幣錢包內的私鑰或助記詞，法院於其核發的搜索票上應為如何之記載，方與「特定明確原則」（the requirement of particularity）無違？此部分將針對應記載於搜索票上的應扣押之物與搜索客體兩者為探討[39]。

2.執法人員在搜索現場接觸受搜索人持有的電子載體，檢視受搜索人使用的比特幣位址係位於其中何處時，倘發現應扣押但搜索票未記載，或者另案應扣押的

[39] 按刑事訴訟法第 128 條第 2 項，搜索票的應記載事項包括案由；應搜索之被告、犯罪嫌疑人或應扣押之物；應加搜索之處所、身體、物件或電磁紀錄；有效期間。在案由、應搜索之被告、犯罪嫌疑人與有效期間這三部分，比特幣之搜索、扣押與實體物並無顯著差異，故本文僅就應扣押之物、搜索客體為探討。

doi:10.6342/NTU202400684

文件檔、影像等電磁紀錄，得否一併將其扣押之？此時如何妥善適用「一目瞭然法則」（the Plain View Doctrine）？

針對上述問題，本文將利用功能比較法，比較我國法院與美國法院相關判決對搜索、扣押電磁紀錄的看法，藉以挖掘其中值得我國現行法調整參考的思路或解決方案[40]。緣在本質上，前揭搜索、扣押比特幣時遭遇的問題，於執法人員搜索、扣押一般電磁紀錄時亦可能發生，而得依對電磁紀錄實施搜索、扣押的一般性規範處理。惟觀諸涉及上述問題的我國法院判決，卻也未能提供精準或穩定的答覆。在此前提下，由於我國與美國皆共同面臨上述問題，且上述問題所涉的法理基礎，在我國法與美國法上相當類似。因此，援引美國法院對搜索、扣押電磁紀錄的相關見解，諸如 United States v. Riccardi 案[41]以及 United States v. Carey 案[42]，作為處理上述問題的借鏡與參考，係具有一定程度的可比性。

[40] 關於功能取向比較法路徑，係為解決本國法秩序下的具體法律問題，基於比較法的問題導向、目的取向與功能性的考量，預設一套運用方法上的體系架構，藉以容納各種不同的比較需求。進一步的細緻論述，請參見：黃舒芃，前揭註 26，頁 189-190。

[41] United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005).

[42] United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

doi:10.6342/NTU202400684

第一節、區塊鏈、比特幣位址與錢包[43]

在開始探討本文的研究問題前，為充分說明對研究問題的分析，本章選擇先於第一節扼要介紹區塊鏈、比特幣位址與錢包等觀念的內涵後，再於下一節回歸研究問題討論。

第一項、區塊鏈的源起

區塊鏈的雛形係於 1990 年代現蹤，當時便有學者發表利用鏈型結構、數位時間戳記（digital time-stamp）來解決數位檔案遭竄改的問題[44]。2005 年電腦學家 Ian Grigg 在上開觀念的基礎上，進一步提出「三式簿記」（triple-entry bookkeeping）試驗系統，即在每筆交易被同時記載於借方與貸方的「複式簿記」（double-entry bookkeeping）系統上，加入加密的獨立開放帳本[45]。透過數位時間戳記與數位公證（digital notary）的功能，亦即在數位資料創造、移轉或消滅的當下，以密碼學技術為每項資料生成或變動的狀態，自動打上一個時間或公正的簽章，確定某一項數位資料在某個特定的時點，具有某些特定內容、或處於特定狀態[46]。但直至比特幣等虛擬通貨問世前，前揭技術發展普遍不被社會大眾所重視。

---

[43] 關於區塊鏈的技術原理，本文主要參考的中、英文文獻係：中文文獻包括蘇凱平（2021），〈當證據「上鏈」：論區塊鏈科技應用於法庭證據〉，《國立臺灣大學法學論叢》，50 卷 3 期，頁 1001-1013；Primavera De Filippi & Aaron Wright（著）、王延川（譯）（2019），《區塊鏈與法律：程式碼之治》，臺北：元照；杨保华、陈昌（2017），《区块链原理、设计与应用》，北京：机械工业出版社；William Mougayer（著）、徐瑞珠（譯）（2016），《區塊鏈商業應用｜次時代網路技術的前景、實踐與應用》，頁 15-32，臺北：碁峰資訊；李鈞、長鋏、李耀東、喻峰、蔡卓斯、宋歡平、袁維（2014），《比特幣：過去・現在與未來》，臺北：遠流。英文文獻則為 Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers*, 25 RICH. J.L. & TECH. 1, 1-106 (2018); Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies* 104, 104-121 (2015 IEEE Symposium on Security and Privacy, 2015), *available at* https://ieeexplore.ieee.org/document/7163021.

[44] Stuart Haber & W. Scott Stornetta, How to Time-Stamp a Digital Document, 3 J. CRYPTOLOGY 99, 99-111 (1991).

[45] Michael J. Casey & Paul Vigna（著）、林奕伶（譯）（2019），《真理機器：區塊鏈與數位時代的新憲法》，頁 47-48，新北：大牌出版。

[46] 蘇凱平，前揭註 43，頁 1002。

doi:10.6342/NTU202400684

第二項、區塊鏈的本質與技術

扼要地說，區塊鏈是種儲存數位資料的技術，由諸多包含各類資訊的「區塊」（blocks）首尾相接而形成的鏈條。每一個區塊皆包含以下三部分的內容：儲存的數位資訊、此區塊的哈希值（hash value，亦可意譯為「雜湊值」）以及上個區塊的哈希值[47]。其中，區塊鏈所儲存的數位資料，僅代表當鏈上因交易、支付或他原因發生變化時，某個時刻上某項事物的狀態被鏈上區塊記載下來。按照數位資料的屬性不同，區塊鏈可在不同的應用場域中被利用，例如比特幣即係記錄在鏈上發生的交易。

接續前段對區塊鏈本質的介紹，以下將圍繞哈希值、公開金鑰加密技術以及共識協定探討，便於後文提及區塊鏈的特性與應用時，可清楚地說明其原理為何。

第一款、哈希值（Hash Value）

哈希值（Hash Value）係藉由美國國家安全局（National Security Agency）發明的標準加密雜湊函數（Hash Function）而生成，主要應用於密碼學領域[48]。易言之，將區塊中發生的一系列交易，透過與該區塊交易唯一關聯的一串符號與數字表達，其位元數量是固定的[49]。目前較廣泛被使用的雜湊函數演算法包括 Message Digest（MD）系列與 Secure Hash Algorithm（SHA）系列。本文以虛擬通貨較常應用的

---

[47] 蘇凱平，前揭註 43，頁 1001。

[48] Primavera De Filippi & Aaron Wright（著）、王延川（譯），前揭註 43，頁 29。關於標準加密雜湊函數背後的數學原理，*See* J. Lawrence Carter & Mark N. Wegman, Universal Classes of Hash Functions, 18 J. COMPUTER & SYSTEM SCI. 143, 143-154 (1979).

[49] Bacon et al., *supra* note 4343, at 9.

doi:10.6342/NTU202400684

SHA-256 為例：輸入欲加密的資訊（可能是文字、符號、圖片或影像），經 SHA-256 演算法運算後，得出一個 256 位元長度的數值結果，即為哈希值。

如此單向加密的運算方式，使產出的哈希值具有兩種特性：「逆向困難」、「無法重複」[50]。前者係指難以從雜湊函數運算所得的哈希值（output），逆推得知原先輸入的資訊（input）為何；後者則係將不同型態的數位資訊投入上開函數運算後，其得出的哈希值係獨特、唯一的存在，確保每個哈希值都能與他區塊的哈希值相區辨，故被廣泛利用於密碼領域的加密與驗證[51]。

第二款、公開金鑰加密技術（Public Key Cryptography）

在傳送數位資訊的過程中，傳遞方如何利用加密技術避免第三者知悉內容，並同時使接收方得以解密技術閱覽訊息，是現代密碼學發展上的核心議題。早期多半採用「對稱加密技術」（Symmetric Cryptography），加密與解密的過程雙方共享相同的金鑰（key），因此具有運算效率快、加密強度較高的優勢。但在傳遞方寄送金鑰給接收方時，難保其過程不會遭他人竊聽、攔截或損毀，致使雙方必須承擔金鑰因此洩漏的風險[52]。

直至 1976 年，首度有密碼學家提出了「公開金鑰加密技術」（Public Key Cryptography）的概念，解決上述金鑰分配的困擾[53]。這樣的想法很快便被落實：1978

[50] Bacon et al., *supra* note 43, at 9-10；李鈞、長鋏、李耀東、喻峰、蔡卓斯、宋歡平、袁維，前揭註 43，頁 129-130。
[51] 蘇凱平，前揭註 43，頁 1006。
[52] 李鈞、長鋏、李耀東、喻峰、蔡卓斯、宋歡平、袁維，前揭註 43，頁 129-130。
[53] 此亦可稱為「非對稱加密（Asymmetric Cryptography）」或「公開金鑰基礎架構（Public Key Infrastructure）」。前者請參見：Whitfield Diffie & Martin Hellman, New Directions in Cryptography, 22:6 IEEE TRANSACTIONS ON INFO. THEORY 644, 644-654 (1976); Microsoft｜Learn, https://learn.microsoft.com/zh-tw/dotnet/standard/security/encrypting-data#asymmetric-encryption

doi:10.6342/NTU202400684

年麻省理工學院密碼學學者們開發出「RSA 演算法」（RSA algorithm）[54]：利用對龐大數字為質因數分解（prime factorization）困難的特性，生成具有數學關聯的公鑰（public key）與私鑰（private key）。由於 RSA 演算法係將一組金鑰拆分成公鑰與私鑰兩部分分別，故其處理速度、加密強度普遍較對稱加密技術差，但卻可大幅降低金鑰外流的擔憂[55]。

區塊鏈運用公開金鑰加密技術在傳遞方與接收方間進行加、解密，以確認雙方的身分為真。其中，私鑰作為區塊鏈使用者的身分表徵，一經生成便無法隨使用者或他人的意志更改。持有私鑰便能控制區塊鏈上儲存的資訊，其角色如同銀行帳戶的密碼，應當妥善保管，不可輕易使他人得知。相對地，公鑰係公開，可為不特定第三人知悉，作為解密資訊的「鑰匙」[56]。在區塊鏈的具體操作上，傳送方與接收方各自擁有一組公鑰以及私鑰，在彼此連線後，雙方便先交換彼此的公鑰。接下來，傳送方運用接收方的公鑰將目標資訊加密後，再將其傳送至接收方，由接收方運用己方持有的私鑰解密目標資訊[57]。如此一來，傳輸雙方便毋庸如對稱加密技術，提前共享可直接使用於解密、但不得為人所知的金鑰，一定程度確保了資訊傳輸過程的機密性。此時，公鑰如同具有在訊息上簽章的功能，實現數位簽章（Digital Signature）的效果[58]。

(last visited Jan. 3, 2023)；後者請參見：Michael J. Casey & Paul Vigna（著）、林奕伶（譯），前揭註 45，頁 87。

[54] Ronald L. Rivest, Adi Shamir & Leonard Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, 21:2 COMM. ACM 120, 120-126 (1978).

[55] 李鈞、長鋏、李耀東、喻峰、蔡卓斯、宋歡平、袁維，前揭註 43，頁 74-75。

[56] 蘇凱平，前揭註 43，頁 1007；William Mougayer（著）、徐瑞珠（譯），前揭註 43，頁 25。

[57] 李鈞、長鋏、李耀東、喻峰、蔡卓斯、宋歡平、袁維，前揭註 43，頁 72-73；魯特（2018），《比特幣精粹》，頁 59-62，臺北：白象文化；Primavera De Filippi & Aaron Wright（著）、王延川（譯），前揭註 43，頁 16-17。

[58] *See* Bacon et al., *supra* note 43, at 15.

doi:10.6342/NTU202400684

第三款、共識協議（Consensus Protocol）

相較於中心化管理的複式簿記，分散式帳本技術的出現使帳本不再由單一實體控制，而係由各個節點儲存相同的帳本，藉以降低數據遺失、或遭人任意竄改的風險[59]。然而，其發展之初卻無法妥善解決「拜占庭將軍問題」（Byzantine Generals Problem）[60]。此問題最早發軔於資訊工程學者們提出的一篇論文，描述資訊系統當中的節點（nodes）之間在傳遞訊息時，可能會因某些節點發出錯誤訊號，以致整個系統無法達成共識的困境[61]。因此，在不同區塊之間，如何確保其等記載的資訊皆為一致，藉以連結多個區塊成為一條「鏈」，滿足區塊鏈網路中的「共識協議」（Consensus Protocol），過往便不斷困擾著資訊領域的專家學者。直至 2008 年，化名為 Satoshi Nakamoto 的作者，在「比特幣：一種點到點的電子現金系統」（Bitcoin: A Peer-to-Peer Electronic Cash System）密碼學白皮書中提出「工作量證明鏈」（proof-of-work chain）的概念後，方有效地解決前揭問題[62]。

所謂的工作量證明鏈，係由 Satoshi Nakamoto 設計一個「試錯遊戲」性質的數學難題，讓節點上的各方計算、探尋有效哈希值之後，方能在鏈上添加新的資訊[63]。一旦該哈希值被發現，建立新生的區塊並新增至鏈上後，便會由其他節點確認其是

---

[59] 中文文獻亦有稱之為「分散式帳簿技術」或「分散式資料庫」，請參見：鄭婷嫻（2019），〈區塊鏈技術應用於我國公司治理法制之研究〉，《東吳法律學報》，30 卷 3 期，頁 2。

[60] 徐明星、刘勇、段新星、郭大治（2016），《区块链：重塑经济与世界》，頁 4-10，北京：中信出版社。

[61] Leslie Lamport, Robert Shostak & Marshall Pease, *The Byzantine Generals Problem*, 4(3) ACM TRANSACTIONS ON PROGRAMMING LANGUAGES & SYS. 382, 382-401 (1982).

[62] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), https://bitcoin.org/bitcoin.pdf. 目前共識協議運作的機制除了工作量證明鏈，另一主流機制便是「權益證明」（proof of stake），其目前多為以太坊（Ethereum）2.0 採用，係指由在區塊鏈上質押虛擬通貨的節點，負責驗證新生成的區塊是否合法。惟由於權益證明非本文重點，關於其更多介紹請參見：BINANCE—ACADEMY（12/06/2018），〈權益證明介紹〉，https://academy.binance.com/zt/articles/proof-of-stake-explained（最後瀏覽日：01/08/2023）。

[63] Paul Vigna & Michael J. Casey（著）、林奕伶（譯）（2017），《虛擬貨幣革命：區塊鏈科技，物聯網經濟，去中心化金融系統挑戰全球經濟秩序》，2 版，頁 170-171，新北：大牌出版；Primavera De Filippi & Aaron Wright（著）、王延川（譯），前揭註 43，頁 30-33。

doi:10.6342/NTU202400684

否符合共識協議的規格、檢驗其合法性；待其共識認可後，再向整個比特幣網路發布消息。在穩定的共識協議環境當中，任何中心化的實體幾乎不可能操縱區塊鏈網路[64]：所有節點原則上皆享有對等的權力，以共同維護鏈上數據[65]。

第三項、區塊鏈網路的類型

依參與者的不同、去中心化程度的高低，區塊鏈網路尚可區分為公有鏈（Public Chain）、私有鏈（Private Chain）與聯盟鏈（Consortium Chain）[66]。上述區分決定了區塊鏈的節點驗證機能如何運行，與區塊鏈不可竄改、去中心化等特徵息息相關[67]。就各類型區塊鏈網路之運作與異同處，本文將在以下段落與表一說明。

所謂公有鏈、亦稱為「非許可鏈」（permissionless blockchain），開放任何人皆得下載開源軟體加入、參與使用與維護，毋庸揭露其真實身分或取得彼此的信任，亦不必事先取得監管方的許可。在交易過程中，需要整條鏈上的節點從事驗證工作，故其速度較慢、交易成本相對高；但也因此具備最高的去中心化程度，難以被單獨一方擅自竄改，是最常被應用於虛擬通貨的區塊鏈類型，諸如以太坊。

---

64 在工作量證明鏈中，礦工能否得出有效的哈希值，通常取決於其擁有的「運算能力」（亦稱為「算力」）。因此，理論上若單一實體可掌握鏈上超過 50%的算力，其便有能力修改或逆轉交易過程，此又稱之為「51%攻擊（51% attack）」、或稱為「多數人攻擊」。但隨著鏈上區塊的增加與其規模的擴大，交易實務上罕有出現 51%攻擊的情形。請參考：Bacon et al., *supra* note 43, at 26-27; BINANCE—ACADEMY（11/28/2018），〈什麼是 51%攻擊？〉，https://academy.binance.com/zt/articles/what-is-a-51-percent-attack（最後瀏覽日：01/08/2023）。

65 Kevin Werbach, *Trustless Trust*, SSRN ELECTRONIC J. (2016), *at* https://www.researchgate.net/publication/318001398_Trustless_Trust.

66 以下主要參考：楊岳平，前揭註 25，頁 1289-1290；Primavera De Filippi & Aaron Wright（著）、王延川（譯），前揭註 43，頁 42-45；BINANCE─ACADEMY（01/06/2020），〈私有鏈、公有鏈和聯盟鏈有何區別？〉，https://academy.binance.com/zt/articles/private-public-and-consortium-blockchains-whats-the-difference（最後瀏覽日：01/08/2023）。

67 蘇凱平，前揭註 43，頁 1011。

doi:10.6342/NTU202400684

相反地，私有鏈、亦稱為「許可鏈（permissioned blockchain）」，並不允許自由參與使用，而須通過鏈上監管方的核准方可加入，其控制與驗證的權力集中單一節點。也因此，鏈上的節點數量不多，彼此間相互信任，不一定都參與每次交易的驗證過程，故其運行速度能較公有鏈來得快，交易成本相對低。私有鏈去中心化的色彩淡薄，監管方可輕易修改或刪除儲存於鏈上的資訊，故較常被使用者間在現實生活有聯繫的團體或組織應用，諸如我國集中保管結算所債券與票券商品交易的保管平台[68]。

聯盟鏈則可被視為公有鏈與私有鏈之間、偏向後者的折衷型，使用者雖亦須經鏈上監管方核准才能加入，但鏈上控制與驗證的權力不限單一節點、而擴張至多方實體，故交易的驗證過程較私有鏈耗時，但理論上應較公有鏈快。我國的行政與司法部門即是相中這些特性，於 2022 年建置司法聯盟鏈平台，期能發揮保護數位資料的功能[69]。

表一、各類型區塊鏈網路之異同

※資料來源：本圖為作者擷取自 BINANCE—ACADEMY（01/06/2020），〈私有鏈、公有鏈和聯盟鏈有何區別？〉，https://academy.binance.com/zt/articles/private-public-and-consortium-blockchains-whats-the-difference

	區塊鏈型別		
	公有鏈	私有鏈	聯盟鏈
准入限制	無	有	有
讀取者	任何人	僅限受邀使用者	相關聯使用者
寫入者	任何人	獲批參與者	獲批參與者
所屬者	無	單一實體	多方實體
瞭解參與者	否	是	是
交易速度	慢	快	快

[68] 中時新聞網（09/08/2020），〈金融創新再添一樁，固定收益商品服務將上「鏈」〉，https://www.chinatimes.com/realtimenews/20200908003700-260410?chdtv（最後瀏覽日：01/10/2023）。

[69] 法務部（07/13/2022），〈數位驗證，信任透明 本部舉辦「司法聯盟鏈建置及標章發表會」〉，https://www.moj.gov.tw/2204/2795/2796/150118/post（最後瀏覽日：02/19/2023）。

doi:10.6342/NTU202400684

第四項、比特幣位址（Bitcoin Address）

比特幣作為架構在公有鏈的支付系統，透過不依賴任何中介機構的方式，確保系統內的流通貨幣數量固定、避免未經授權的資金使貨幣貶值，並以不可竄改、不可逆的紀錄保障交易安全[70]。而凡是個體欲參與比特幣系統的運作、在節點間移轉比特幣，一般須透過比特幣錢包內建立的「比特幣位址」，方得為之[71]。

比特幣位址，其本質係經一系列雜湊運算的公鑰，無法隨使用者或他人的意志更改；其功能上近似現實生活中的銀行帳號，可利用它支付或收受比特幣[72]。此部分對研究問題的重要性在於，執法人員欲扣押比特幣時，須瞭解如何將被扣押人比特幣位址持有的比特幣，移轉至執法人員方的比特幣位址，避免被扣押人或第三人再行移轉之。

第五項、比特幣錢包（Bitcoin Wallet）

所謂比特幣錢包，係比特幣系統中的一個前端工具[73]。與人們的普遍認知不同，比特幣錢包實際上未儲存任何比特幣或虛擬通貨，其主要功能係發起轉帳交易或查看交易紀錄，以及管理一組或多組的公、私鑰與比特幣位址[74]。一般按比特幣錢包

---

[70] Primavera De Filippi & Aaron Wright（著）、王延川（譯），前揭註 43，頁 24。

[71] 蔣勇、文延、嘉文（2018），《白話區塊鏈》，頁 50，臺北：碁峰。

[72] 王毅丞（2018），《實戰區塊鏈技術｜加密貨幣與密碼學》，頁 65，臺北：碁峰；魯特，前揭註 57，頁 158。關於比特幣位址生成的過程，以現行交易實務最常見的 P2PKH（Pay-To-Public-Key-Hash）單一簽名位址為例：將公鑰先後透過 SHA-256、RIPEMD-160 演算法為數次雜湊運算後，連接位址版本號、4 位元組（Byte）驗證值，再經 BASE58 編碼、轉換成 34 個由數字或字母轉換的比特幣位址；此部分請參見：蔣勇、文延、嘉文，前揭註 71，頁 51-52；魯特，前揭註 57，頁 159-160。

[73] 魯特，前揭註 57，頁 194。

[74] 蔣勇、文延、嘉文，前揭註 71，頁 50。

doi:10.6342/NTU202400684

的運作機制是否有連接網際網路，可大別區分為「冷錢包」與「熱錢包」兩種類型，以下將分別介紹之[75]。

第一款、冷錢包（Cold Wallet）

冷錢包係指未連接至網路的錢包，以離線、實體的方式儲存私鑰，較常見的種類包括硬體錢包以及紙錢包：前者係將私鑰儲存於如行動硬碟、專為虛擬通貨設計的隨身碟等未連接至網路的硬體設備內；後者則係將私鑰存放於紙張之上[76]。

冷錢包既未連接至網路，幾乎不可能遭受駭客等網路攻擊，但其應如何完成比特幣交易的驗證？以硬體錢包為例，首先可透過隨身碟存取電腦上的接收交易，再以硬體錢包驗證交易，並將驗證後的交易紀錄回傳電腦、以廣播方式輸出至比特幣網路[77]。如此一來，這些冷錢包便能在私鑰不暴露於網路的狀態之下，完成比特幣交易的驗證程序。

我國執法人員在偵辦涉及冷錢包的虛擬通貨刑案時，通常會先將受搜索人拘提或當場逮捕後，再行扣押受搜索人用以存放私鑰的冷錢包[78]。

---

[75]「熱錢包」、「冷錢包」亦可分別稱之為「熱儲存」、「冷儲存」，請參見：魯特，前揭註 57，頁 198。

[76] 法務部調查局，前揭註 19，頁 65-67。

[77] 羅韋淵，前揭註 15，頁 27；法務部調查局，前揭註 19，頁 67。

[78] 內政部警政署刑事警察局（06/06/2022），〈台美合作緝獲強盜加密貨幣犯〉，https://www.cib.npa.gov.tw/ch/app/news/view?module=news&id=1885&serno=9763f014-97bd-4a0f-9259-e2fcb256ad10（最後瀏覽日：04/09/2023）；臺灣臺中地方檢察署（12/15/2022），〈加密貨幣場外交易詐騙陷阱多　臺中地檢署起訴投資詐騙假幣商詐欺洗錢案件〉，https://www.tcc.moj.gov.tw/295804/295830/657577/1024245/post（最後瀏覽日：04/09/2023）。

doi:10.6342/NTU202400684

第二款、熱錢包（Hot Wallet）

所謂熱錢包，係指有連接至網路的錢包，較常見的種類包括軟體錢包以及交易所錢包[79]。因為熱錢包不必附著於某一特定的實體載體，可藉由網路連線至個人帳戶，使用者在操作上相較冷錢包便利許多。但在另一方面，選擇使用熱錢包亦必須承擔遭駭客盜取私鑰、交易所倒閉或日蝕攻擊（Eclipse Attack）的風險[80]。

當前市面上的軟體錢包種類眾多，包括 Bitcoin Core、Electrum、Coinbase 等錢包，其多能與常見的電腦、行動裝置作業系統相容，並視儲存載具的類型，而亦可稱為桌面錢包或行動錢包[81]；其通常將未加密或加密的私鑰儲存在名為「Wallet.dat」的檔案內[82]。在這些軟體錢包當中，使用頻率最高的莫過輕錢包程式（light clients），緣其毋庸下載整個區塊鏈、只需下載與使用者有關聯的部分區塊鏈，即得為確認結算、接收或傳送款項之功能[83]。

交易所錢包（亦稱為網頁錢包、線上錢包）係各大虛擬通貨服務供應商提供的服務，諸如幣安（Binance）、幣託（BitoEX）等交易所。使用者通常在交易所將帳號註冊完成後，於交易所錢包內會產生一組比特幣位址，用以接收或傳送款項[84]。交易所錢包因著私鑰是否由交易所保管，又可細分為託管錢包（Custodial wallet，亦

---

[79] 法務部調查局，前揭註 19，頁 63-67；魯特，前揭註 57，頁 198-201；王毅丞，前揭註 72，頁 2-26。

[80] 日蝕攻擊係指駭客對目標位址發動 DDoS 攻擊，使其與比特幣系統脫節，從而大幅提升雙重支付發生的風險。詳細的介紹請參見：BINANCE─ACADEMY（01/19/2020），〈什麼是日蝕攻擊（Eclipse Attack）？〉，https://academy.binance.com/zt/articles/what-is-an-eclipse-attack（最後瀏覽日：03/02/2023）；Ethan Heilman & Alison Kendler, Eclipse Attacks on Bitcoin's Peer-to-Peer Network (24th USENIX Security Symposium, 2015), https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman.

[81] BINANCE─ACADEMY（06/18/2019），〈什麼是加密貨幣錢包？〉，https://academy.binance.com/zt/articles/crypto-wallet-types-explained（最後瀏覽日：03/05/2023）

[82] 法務部調查局，前揭註 19，頁 63-64。

[83] 王毅丞，前揭註 72，頁 28。

[84] 魯特，前揭註 57，頁 204。

doi:10.6342/NTU202400684

可稱為 Hosted wallet）與非託管錢包（Non-Custodial wallet，亦可稱為 Unhosted wallet）。前者係指下載至使用者端的交易所錢包，其私鑰實由交易所業者管理，使用者本身未擁有私鑰；與之相反，後者使用的交易所錢包，則係由使用者自行管理私鑰[85]。

我國執法人員偵辦涉及熱錢包的虛擬通貨刑案時，其方法之一，係先藉由相關情資交叉比對出嫌疑人持有的熱錢包，包括於何交易所註冊開立、交易紀錄與管理的虛擬通幣位址；掌握前揭資訊後，再進一步追蹤犯罪金流的後續去向，並要求虛擬通貨交易所凍結可疑帳戶，藉以及時地扣押虛擬通貨[86]。另一種方法則是，執法人員在搜索、逮捕受搜索人後，便將受搜索人於其交易所錢包內涉案的比特幣額度，在現場即時地移轉至事先備妥的冷錢包，藉以完成扣押犯罪所得之目的[87]。

第三款、助記詞（Mnemonic Phrase）

一般而言，私鑰乃由數十個大小寫英文字母與數字隨機組合而成的字串。以比特幣之私鑰為例，其便係在符合一定密碼學原理的運算下，隨機生成的 16 進位、64 位元字串[88]。為減少使用者儲存或記憶私鑰的負擔，「助記詞」（亦可稱為助記種子、萬能錢包）便是將私鑰經由特定演算法運算後，轉化而成的 12 至 24 個常見英文詞彙，例如「rose rocket invest real refuse margin festival danger anger border id le brown」。如同私鑰，助記詞一經生成便無法隨使用者或他人的意志為更改[89]。

當使用者欲移轉比特幣時，便可利用特定方法將助記詞還原成其持有的私鑰，

---

85 羅韋淵，前揭註 15，頁 28。
86 法務部調查局（2019），《107 年毒品犯罪防制工作年報》，頁 96-97。
87 TVBS 新聞網（12/13/2021），〈詐騙所得買比特幣！　警方用「冷錢包」查扣〉，https://news.tvbs.com.tw/local/1659339（最後瀏覽日：04/05/2023）。
88 羅韋淵，前揭註 15，頁 27。
89 法務部調查局，前揭註 19，頁 66；BINANCE─ACADEMY, *Seed Phrase*, *at* https://academy.binance.com/en/glossary/seed-phrase (last visited March 5, 2023).

doi:10.6342/NTU202400684

故助記詞本質上可視為私鑰的另一種表現形式。助記詞得藉由熱錢包或者冷錢包的方式儲存，亦即其可能儲存在電腦、行動裝置或紙張等載體，乃至人類大腦。

第二節、搜索扣押比特幣之程序問題

刑事訴訟上發動強制處分之目的絕不僅止於發見真實，不允許執法人員為發見真實，便可訴諸任何方法以及手段[90]。同等重要之目標，乃在於保護人權，避免人民的基本權利遭國家機器以偵查犯罪為名，行濫權侵害之實[91]。在權衡發見真實與保護人權前，勢必要先分辨執法人員實施的偵查究竟有無侵害人民的基本權利。因此，在進入研究問題的討論前，本文將先釐清搜索、扣押比特幣時，可能侵害人民財產權的爭議，藉以在本節第二項確認其是否可於現行刑事訴訟法的框架下妥適處理。

第一項、搜索扣押比特幣造成的財產權侵害

本項著重討論執法人員實施對比特幣的搜索、扣押時，發生與有體物的搜索、扣押程序不同，而可能對嫌疑人的財產權造成影響之處：執法人員取得扣得硬體錢包或軟體錢包內儲存的私鑰，但未隨之移除原儲存裝置或其他位置的私鑰或助記詞，得否構成我國刑事訴訟法上的「扣押」[92]？

---

[90] 司法院釋字第 392 號解釋理由書；林鈺雄（2022），《刑事訴訟法上冊》，11 版，頁 12，臺北：新學林。

[91] 王兆鵬、張明偉、李榮耕（2022），《刑事訴訟法（上）》，頁 6，臺北：新學林；林俊益（2022），《刑事訴訟法概論（上冊）》，22 版，頁 18，臺北：新學林。

[92] 倘執法人員此時將原儲存裝置或其他位置的私鑰或助記詞盡皆移除，由其壟斷該些私鑰與助記詞之支配，則此時執法人員取得私鑰或助記詞的行動，便構成我國刑事訴訟法上的扣押。此情形於我國法上之適用並無疑義，故不納入本款以下的的討論範圍。

doi:10.6342/NTU202400684

我國憲法上財產權的保障範圍，包括公、私法上的一切財產權，諸如債權、物權、無體財產權以及具有經濟價值的公法上權利[93]。在古典意義上，財產權係以所有權絕對、神聖不可侵犯的姿態出現，具有抗拒國家干預的消極性格，正如司法院釋字第 400 號解釋所揭示：「財產權作為一種制度性保障的權利，旨在確保個人依財產存續狀態行使其自由使用、收益以及處分之權能，並免於遭受公權力或第三人侵害[94]。」當國家欲對人民的財產權為一定程度之干預或限制時，形式上應以明文的法律規範訂定之，以符法律保留原則的要求，手段亦應通過比例原則之檢驗[95]。

其中，主要規範在我國刑事訴訟法第一編第十一章的「扣押」，便屬國家基於保全證據、得沒收之物以及追徵之目的，於判決確定前，干預嫌疑人財產權的強制處分[96]。執法人員實施扣押的具體手段，便是將可為證據及得沒收之物，暫時置於國家實力支配之下，取得其等物的占有[97]；亦即排除被扣押人對目標物的事實上管領力，由執法人員壟斷對目標物的支配。面對如電磁紀錄的情形，執法人員倘將硬碟內的特定檔案複製至另一硬碟內，僅係取得該檔案的複本，未排除原持有人對該檔案的占有，故此時不構成前揭意義下之扣押[98]。國內有學者對此認為，現行刑事訴訟法第 133 條第 1 項應修正成：「可為證據或得沒收之物，得扣押之；電磁紀錄物

---

93 許志雄、陳銘祥、蔡茂寅、周志宏、蔡宗珍（2008），《現代憲法論》，4 版，頁 180；吳庚、陳淳文（2013），《憲法理論與政府體制》，頁 224-226，臺北：三民。

94 節錄自司法院釋字第 400 號解釋解釋文。

95 李惠宗（2012），《憲法要義》，6 版，頁 116-119，臺北：元照；許育典（2011），《憲法》，5 版，頁 57-59，臺北：元照；張麗卿（2018），《刑事訴訟法理論與運用》，14 版，頁 224、226，臺北：五南。

96 林俊益，前揭註 91，頁 243；林鈺雄，前揭註 90，頁 312-313；林鈺雄（2001），《搜索扣押註釋書》，頁 197，臺北：元照。

97 蔡墩銘（2003），《刑事訴訟法概要》，修訂 6 版，頁 113，臺北：三民；黃東熊、吳景芳（2005），《刑事訴訟法論(上)》，修訂 6 版，頁 194，臺北：三民；林俊益，前揭註 91，頁 389；林鈺雄，前揭註 90，頁 453。

98 在現行刑事訴訟法的規範框架對電磁紀錄搜索、扣押之執行方法，我國實務係採「二階段搜索模式」。扼要言之，係由執法人員於搜索現場扣押儲存目標電磁紀錄的電子載體後，再將該載體攜至搜索現場以外之處，利用檢警機關的設備，依電腦鑑識程序搜尋載體內有無所需之電磁紀錄；本文將於「第四章、第一節、搜索扣押電磁紀錄之流程與比特幣」對此為進一步的說明。

doi:10.6342/NTU202400684

儲存有得作為證據之用之電磁紀錄者，亦同。」以符我國實務目前對電磁紀錄為扣押時，將目標電磁紀錄與儲存其的電子載體一併扣押的操作[99]。

比特幣固屬電磁紀錄之一環，然因著其與一般數位資訊的技術內涵不同，諸如分散式帳本、工作量證明鏈之設計，是否亦可得出同前段面對電磁紀錄的結論？申言之，偵辦涉及硬體錢包或軟體錢包的比特幣刑案時，執法人員實際上需要將扣押對象聚焦於儲存在前揭錢包的私鑰或助記詞，藉以完成扣押比特幣之目的[100]。而由執法人員匯出嫌疑人持有錢包內的私鑰後，原儲存位置的私鑰倘未隨之移除，或者在嫌疑人或第三人持有的另個比特幣錢包內，同樣存有得移轉目標比特幣的私鑰或助記詞。此時，執法人員與嫌疑人雙方皆持有得移轉目標比特幣的私鑰或助記詞，則執法人員上開匯出私鑰的動作，能否構成對私鑰之占有，進而宣稱完成扣押私鑰？此時有無干預嫌疑人的財產權？

本文認為，扣押比特幣的過程中，執法人員取得嫌疑人硬體錢包或軟體錢包內儲存的私鑰，不構成我國現行刑事訴訟法上的「扣押」，亦未干預嫌疑人的財產權[101]。緣對執法人員而言，欲扣押的對象係目標比特幣，私鑰或助記詞不過僅是其取得比特幣之工具。易言之，在扣押比特幣的過程中，私鑰或助記詞僅係移轉目標比特幣至檢警機關比特幣位址此一扣押動作時，必須擁有的媒介。故單純取得嫌疑人硬體錢包或軟體錢包內儲存的私鑰，此動作未使這些私鑰持有者可支配的比特幣數

[99] 李榮耕（2012），〈電磁紀錄的搜索及扣押〉，《國立臺灣大學法學論叢》，41 卷 3 期，頁 1076。

[100] 法務部調查局，前揭註 19，頁 68。在本段所述情況中，利用私鑰或助記詞移轉目標比特幣至檢警機關專用的比特幣位址，由執法人員壟斷對該些比特幣之支配，並導致嫌疑人比特幣位址持有的比特幣額度相對應減少，侵害嫌疑人的財產權，已然構成現行刑事訟法上的「扣押」，並無疑義；故本文將討論重心置於執法人員取得私鑰或助記詞的動作。

[101] 此動作雖不構成扣押，然以合理隱私期待的標準審視之，主觀上嫌疑人對該些私鑰或助記詞具有隱私期待，客觀上一般大眾認為其隱私期待係屬合理，故嫌疑人對該些私鑰或助記詞的合理隱私期待係合法且值得保護。今執法人員取得對該些私鑰或助記詞的控制權，已然侵犯嫌疑人的隱私權，構成我國刑事訴訟法上的「搜索」。

doi:10.6342/NTU202400684

目縮減，對其等的財產權並無影響[102]。何況在取得私鑰或助記詞時，其尚可能為嫌疑人或第三人持有，且亦難以使其他具有相同功能的私鑰或助記詞，喪失移轉目標比特幣之作用，而由執法人員壟斷對前揭私鑰之支配。

綜上所述，本文認為在扣押比特幣的過程中，執法人員取得嫌疑人硬體錢包或軟體錢包內儲存的私鑰，並無侵害人民的財產權，不構成我國現行刑事訴訟法上的「扣押」。

第二項、現行刑事訴訟法之適用問題

如前所述，有體物的搜索、扣押規範上適格之客體，於 2001 年前僅係指身體、物件、住宅或其他有體物，並不包括無形的數位資訊[103]。直至 2001 年，立法者於刑事訴訟法第 122 條、第 128 條第 2 項增列「電磁紀錄」為得受搜索之客體後，執法人員對電磁紀錄實施搜索、扣押方有明文依據[104]。故原則上但凡以電磁紀錄形式呈現的數位資料，包括文件檔、圖片檔、影音檔等執法人員皆得根據上述條文對其實施搜索、扣押。

比特幣係屬區塊鏈技術之應用，而區塊鏈是種儲存數位資料的技術，因此比特幣本質上仍為電磁紀錄。只是在面對某些如牽涉特定明確原則或一目瞭然法則的問題時，因著比特幣與一般電磁紀錄部分不同的技術特徵，諸如分散式帳本、工作量

---

[102] 私鑰或助記詞具有移轉目標比特幣的功能，對受搜索人而言固存在一定經濟價值，而為財產權保護的一環。然在扣押目標比特幣的過程中，私鑰或助記詞之取得並非此次扣押的最終目的，故本文不另討論此部分對受搜索人的影響。

[103] 於 1967 年 1 月 28 日公布後施行的舊刑事訴訟法第 122 條，請參見前揭註 2。

[104] 另有學者就現行刑事訴訟法的文字內容觀察，有令狀的搜索得以對電磁紀錄為之，但其餘無票搜索、有令狀或無令狀的扣押規定，皆是規定物件、物或標的。如此一來，容易造成除了有令狀的搜索之外，其餘干預行為一概不得對載體內數位證據取證的印象。惟此點並非本文欲討論的重心，有興趣的讀者煩請參見：施育傑（2017），〈數位證據的載體、雲端與線上取證──搜索扣押與類型化的觀點〉，《裁判時報》，64 卷，頁 68。

doi:10.6342/NTU202400684

證明鏈等設計，而有可能在現行刑事訴訟法的實際操作上稍加調整。

就影響搜索、扣押比特幣的成敗關鍵，能否順利取得涉案的私鑰或助記詞而言，我國實務工作者亦有因著比特幣的技術特徵，比如分散式帳本、得立即移轉而不可於公有鏈上竄改交易紀錄等性質，提出不同於一般搜索、扣押電磁紀錄的作法，包括利用演算法分析比特幣交易在全球帳本上的相關資訊，或要求執法人員應在獲悉得移轉目標比特幣所需的私鑰後，立即使用其將目標比特幣匯入檢警機關專用的比特幣位址等方法[105]。然觀察我國實務工作者就搜索、扣押比特幣所提出的種種建議或作法，適用上皆未超出現行刑事訴訟法關於搜索、扣押的規範架構。故本文認為，比特幣之搜索及扣押可置於現行刑事訴訟法的框架中處理，而無必要另行訂定專法或增修現行刑事訴訟法的條文。

執法人員若欲搜索、扣押嫌疑人的比特幣，非基於急迫情事或實際的執法需求，原則上應遵循要式搜索之程序[106]。首先，以書面記載第 128 條第 2 項各款事項後，再按第 128 條之 1 第 1 項、第 2 項向該管法院聲請核發搜索票[107]。於受理案件後，該管法院應就搜索票聲請書所敘述之理由及其釋明，審查有無符合第 122 條規定的「必要時」或「有相當理由」之要件，亦即是否有合理之根據認定被告或犯罪嫌疑人之身體、物件、電磁紀錄及住宅或其他處所可能藏有得作為犯罪或與之相關的

[105] 羅韋淵，前揭註 15，頁 35；法務部調查局，前揭註 19，頁 68、73；黃柏翔，前揭註 19，頁 33；洪敏超（2023），〈以 USDT 經營賭博網站之刑法管制與刑事偵查〉，《檢察新論》，32 期，頁 14。關於搜索、扣押比特幣在執行面上的可行作法，基於架構安排的原因，本文將於下述「第四章、第二節、搜索扣押比特幣之流程」再為詳盡說明。

[106] 要式搜索，亦可稱為「有票搜索」、「令狀搜索」，係執法人員事先取得法院核發的搜索票後，方發動的搜索行動。

[107] 第 128 條第 2 項：「搜索票，應記載下列事項：一、案由。二、應搜索之被告、犯罪嫌疑人或應扣押之物。但被告或犯罪嫌疑人不明時，得不予記載。三、應加搜索之處所、身體、物件或電磁紀錄。四、有效期間，逾期不得執行搜索及搜索後應將搜索票交還之意旨。」、刑事訴訟法第 128 條之 1：「（第一項）偵查中檢察官認有搜索之必要者，除第一百三十一條第二項所定情形外，應以書面記載前條第二項各款之事項，並敘述理由，聲請該管法院核發搜索票。（第二項）司法警察官因調查犯罪嫌疑人犯罪情形及蒐集證據，認有搜索之必要時，得依前項規定，報請檢察官許可後，向該管法院聲請核發搜索票。（第三項）前二項之聲請經法院駁回者，不得聲明不服。」

doi:10.6342/NTU202400684

證據存在，藉以決定是否核發搜索票[108]。

第一款、特定明確原則於搜索、扣押比特幣時之適用

第一目、問題提出

此刻應注意的是，如何記載搜索票上的應記載事項方得謂妥適，尤其是第 128 條第 2 項規定中所列的應扣押之物及搜索客體？就應扣押之物與搜索客體而言，學理上有所謂「特定明確原則」（the requirement of particularity），即由法院核發的搜索票上，必須特定明確、清楚記載應搜索之處所及應搜索（拘捕）之被告及應扣押之物[109]。我國實務則多以「概括搜索票禁止原則」稱之，亦要求搜索票上的應記載事項，必須事先加以合理的具體特定與明示[110]。上述原則之目的係在合理限制搜索的範圍，避免執法人員進行無節制地搜索、扣押行動，造成人民不必要與錯誤的權利侵害，使令狀節制強制處分的作用喪失[111]。

倘執法人員欲搜索、扣押的對象係比特幣，法院於其核發的搜索票上就搜索客體應為如何之記載，方與特定明確原則無違？析言之，就一般電磁紀錄搜索之搜索票，我國現行實務多半僅在搜索範圍的電磁紀錄欄內，記載可能儲存目標電磁紀錄的電子載體，諸如電腦、行動電話等消費性電子產品。惟對此國內有學者認為，搜索票上除了記載電子載體，亦應具體載明於電子載體內執法人員欲搜索的數位資訊

---

108 林俊益，前揭註 91，頁 355。

109 李榮耕（2012），〈特定明確原則與機動性通訊監察〉，《政大法學評論》，126 期，頁 113-122；王兆鵬、張明偉、李榮耕，前揭註 91，頁 238-239；李榮耕（2022），〈犯罪偵查中通訊內容的調取〉，《國立臺灣大學法學論叢》，51 卷 3 期，頁 814。我國部分實務亦有採納此原則，請參見如：臺灣高等法院臺南分院 106 年度重上更(三)字第 22 號刑事判決。

110 請參見如：最高法院 110 年度台上字第 396 號刑事判決、最高法院 100 年度台上字第 5065 號刑事判決。

111 王兆鵬、張明偉、李榮耕，前揭註 91，頁 239。

doi:10.6342/NTU202400684

為何，否則除了無法完整說明搜索、扣押時應具備的相當理由，更可能使執法人員於搜索過程中，得隨意瀏覽電子載體內的所有檔案[112]。本文認為以學者見解為當。緣倘依實務操作，恐造成執法人員無論係偵辦重大刑案或一般刑案，皆得持票搜索特定電子載體內儲存的所有數位資訊。而學者見解可適度限制執法人員搜索電磁紀錄時的範圍，避免受搜索人的隱私權與財產權蒙受不必要且錯誤之侵擾。

比特幣屬電磁紀錄的其中一環，故執法人員若欲對比特幣實施搜索、扣押，似得依前揭見解，於搜索票上關於搜索範圍的電磁紀錄欄內，僅記載目標比特幣以及執法人員認為可能儲存該私鑰或助記詞的比特幣錢包，比如以電磁紀錄樣態儲存在硬體錢包或軟體錢包，便可符合特定明確原則之要求[113]。

惟相較一般電磁紀錄，比特幣在技術內涵獨有的兩個特徵，使本文認為以比特幣為搜索客體的搜索票，記載上似可要求更加細緻化之程度[114]。其一，相較可由使用者或他人更改檔案名稱的一般電磁紀錄，使用於支付或收受比特幣的比特幣位址，無法隨使用者或他人的意志為任何更動。其二，以一般電磁紀錄形式呈現的密碼可由使用者或他人為更改，然包括移轉比特幣所需的私鑰，以及按一定密碼學原理運算而得出的助記詞，皆無法隨使用者或他人的意志為任何更動[115]。

此時，搜索票上須記載的應扣押物是否包含儲存私鑰或助記詞的載體？又比特幣位址、私鑰及助記詞同為移轉目標比特幣時所需的工具，是否需將三者一同具體

---

[112] 王銘勇（2003），〈網路犯罪之搜索與扣押〉，《法學叢刊》，48 卷 3 期，頁 51；李榮耕，前揭註 99，頁 1092-1093；林育賢（2020），〈數位證據之取證及證據能力〉，《司法新聲》，135 期，頁 35。

[113] 倘若執法人員認為可能儲存私鑰或助記詞的比特幣錢包係紙錢包，則應依其性質將之記載於物件欄內，併予敘明。

[114] 以比特幣為搜索客體的搜索票，具體上應如何記載方符特定明確原則之要求，本款將留待「第三目、現行刑事訴訟法之適用建議」當中說明。

[115] 此處涉及的相關技術內涵，請參見本章前述「第一節、第二項與第四項」的說明。

doi:10.6342/NTU202400684

記載，方與特定明確原則的要求無違？這些皆是本文認為就搜索、扣押比特幣而言，現行刑事訴訟法在適用上可能需面對的問題。

對此，我國刑事訴訟法第 128 條第 2 項僅規定，搜索票應記載案由、搜索對象、搜索客體與有效期間等事項，未特別敘明搜索、扣押的客體應記載至何種程度方與特定明確原則無違。而涉及搜索、扣押電磁紀錄的數個案件中，我國實務則多著墨概括搜索票禁止原則本身應如何詮釋。諸如最高法院 97 年度台上字第 1509 號刑事判決（節錄）：「……搜索票上之『應扣押物』以及『應搜索處所等』之任何一項，必須事先加以合理的具體特定與明示，方符明確界定搜索之對象與範圍之要求，以避免搜索扣押被濫用，而違反一般性搜索之禁止原則。所謂應扣押之物，……，不以於『有事實足認其存有者』為限，尚包括『一般經驗法則、邏輯演繹或歸納可得推衍其存有者』」[116]；智慧財產法院 106 年度刑智抗字第 3 號刑事裁定（節錄）：「……原審裁定據此聲請於扣押物一欄記載：違反著作權等之侵權物品、電腦電磁紀錄、行動電話所儲存之通訊記錄、帳冊或進出貨單、供犯罪所用工具及本案相關事證……。準此，依一般經驗法則或邏輯推理，應認藉由著作權人所指派之鑑定人員，其於搜索扣押執行時，協助確認是否屬本件之侵權物品，即可特定是否屬應扣押物，符合合理明確性之要求。職是，原裁定之記載未違反概括搜索禁止原則，應屬適法適當。」[117]；智慧財產及商業法院 110 年度刑智上易字第 49 號刑事判決（節錄）：「……如已記載依現有事證、經驗法則或邏輯推理上可認為存有之物，縱同時搭配概括之應扣押物記載，仍得依所例示物件之性質、種類、存在方式等，配合本案據以搜索之犯罪嫌疑，推知概括記載之應扣押物所指涉之範圍，當已足適當節制執行機關之權力行使，以兼顧偵查效率並保障受處分人之權利，依此等搜索票所為之搜索、扣押，即無違法之虞。」[118]除了第二則判決稍有提及儲存通訊紀錄的載體，

[116] 本判決以違反著作權法案件之光碟燒錄重製為例，執法人員在其所持搜索票上的應扣押之物，可記載為「與侵害著作權有關之光碟片、燒錄機、電腦、標籤、說明書、包裝等證物」。
[117] 本裁定係以違反著作權法案件之光碟為主題。
[118] 本判決係以違反商標法案件之設計圖形著作為主題。

doi:10.6342/NTU202400684

其餘部分多僅就應記載事項的特定程度為說明。迄今雖未見我國實務完善處理是否應將電磁紀錄連同儲存其的載體一併記載之論述，然面臨同樣問題的美國，美國法上的 United States v. Riccardi 案就此議題則有所回應[119]。故在未尋獲針對比特幣搜索及扣押的美國法判決之狀況下，本文選擇參考國內學者的路徑，借鏡 United States v. Riccardi 案處理搜索、扣押電子紀錄時，搜索票上的應扣押之物與搜索客體應如何記載，方符特定明確原則之要求[120]。

第二目、美國法院相關判決之借鏡

具體言之，針對第一個問題涉及的特定明確原則（the requirement of particularity），基於美國聯邦憲法增修條文第四條（the Fourth Amendment of the United States Constitution）之要求，亦即發動搜索或扣押前，除了必須事先向法院聲請令狀外，法院在其核發的令狀上，還必須明確記載應搜索之處所、應扣押之物品或應逮捕之人[121]。數件美國法院判決皆強調為防止空白搜索票及概括搜索之發生，應透過搜索令狀上特定明確記載之要求，藉以合理限縮搜索的範圍，以避免錯誤或不必要的搜索[122]。此些判決與上述我國實務提及的概括搜索票禁止原則相當類似，兩者在法理上具有可比性的基礎。

關於 United States v. Riccardi 案中執法人員對被告住處的搜索過程，本文扼要

---

[119] 根據司法院裁判書系統（https://judgment.judicial.gov.tw/FJUD/default.aspx）收錄的裁判資料，於 2023 年 12 月 20 日在查詢條件分別輸入 2 組關鍵字組別如下：「概括搜索票禁止原則」、「特定明確原則」，總共可得 35 筆不重複的裁判，但絕大多數並無提及是否應將電磁紀錄連同儲存其的載體一併記載之問題。

[120] 李榮耕，前揭註 99，頁 1093；United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005).

[121] U.S. CONST. amend IV. : "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." 關於此條文的中譯版本，本文係參考：李榮耕，前揭註 109，頁 113。

[122] *See* United States v. Hinton, 219 F.2d 324 (7th Cir. 1955); Maryland v. Garrison, 480 U.S. 79 (1987); Groh v. Ramirez, 540 U.S. 551 (2004).

doi:10.6342/NTU202400684

敘述如下：獲悉被告涉嫌違反妨害性自主的相關消息後，警方先後兩次向管轄法院聲請對被告住處的搜索令狀[123]。管轄法院在第二次搜索令狀上，授權執法人員得扣押被告住處的電腦，並搜索「一切儲存於該裝置內的電子與磁性介質」（all electronic and magnetic media stored within such devices）。接下來，警方便憑藉此搜索令狀，在被告住處扣押被告的電腦；並於後續的電腦鑑識過程中，順利發現被告電腦內儲存的青少年情色影像檔案，以及被告與多位青少年的網路聊天紀錄[124]。

本件其中一個爭點，便是執法人員於第二次搜索時扣押的青少年情色影像檔案，是否違反美國聯邦憲法增修條文第四條？對此，被告抗辯本次警方所憑搜索令狀上就搜索客體的記載，並不符合美國聯邦憲法增修條文第四條關於特定明確之要求[125]。

法院首先闡述，搜索令狀上的記載應使搜索人員可合理地確定並辨識何等品項應被搜索、扣押，方得被認定為足夠特定明確。政府機關必須盡可能在其掌握的情資範圍內，在搜索令狀上記載得足夠詳盡。倘搜索令狀上應被扣押的品項描述得較一般化，只要在執法人員搜查時可被特定，搜索令狀上的記載仍得被認定為合法。反之，若搜索令狀上記載的品項已無法使執法人員分辨其特徵，則該令狀很有可能被認定為違法[126]。系爭搜索令狀授權執法人員得搜索的範圍，係被告住處的電腦內建或外接裝置儲存之所有電磁紀錄，未限制任何特定的檔案，已不當侵害受搜索人的隱私，與美國聯邦憲法增修條文第四條的誡命有違[127]。

123 United States v. Riccardi, 405 F.3d 857-58 (10th Cir. 2005).
124 *Id.* at 858.
125 *Id.* at 861.
126 *Id.* at 862.
127 *Id.* at 862-63.

doi:10.6342/NTU202400684

第三目、現行刑事訴訟法之適用建議

如前文所述，我國現行制度遵循的特定明確原則，其目的係在合理限制搜索的範圍，避免執法人員無限制的搜索、扣押，造成人民不必要與錯誤的權利侵害。執法人員實施對比特幣之搜索、扣押亦不得違反此原則，固無疑義；然此時在適用特定明確原則上，卻產生以下難處：是否以及應如何記載比特幣位址、私鑰與儲存私鑰之載體。

移轉目標比特幣的關鍵除了掌握受搜索人的比特幣位址，便係取得移轉目標比特幣所需的私鑰之控制權。而比特幣之私鑰僅係大小寫英文字母與數字隨機組合而成的 64 位元字串，其除了得以電磁紀錄的樣態儲存於軟體錢包、硬體錢包或交易所錢包，亦得以紙本的樣態呈現於紙錢包 [128]。執法人員若欲搜索、扣押比特幣，其所持的搜索票關於搜索或扣押客體之記載，將面對前揭諸多比特幣錢包之可能。此時應當如何記載，方得在不過度壓縮第一線執法空間與避免執法人員濫行搜索之間取得平衡？能否僅記載應扣押物為比特幣 N 顆，藉以規避記載載體的問題？

針對上述，本文認為搜索票應同時記載比特幣位址、私鑰與可能儲存私鑰之載體，其必要性在於適度限縮執法人員的搜索範圍。緣數位資訊應與儲存其的載體分開檢視，合法控制載體不代表即可探查其儲存的數位資訊。在審視此搜索、扣押載體的合法性時，不可因數位資訊與儲存其的載體之緊密結合關係，便將兩者一同綑綁看待 [129]。另外，相較以一般電磁紀錄形式呈現的檔案名稱、密碼，比特幣位址與私鑰皆無法依使用者或他人的意志為任何更動，否則將使其喪失原具有的效用。故在偵查資訊充分的狀況下，要求執法人員具體記載欲搜索的比特幣位址，係在

[128] 請參見本章前述「第一節、第二項及第五項」的說明。
[129] 施育傑，前揭註 104，頁 60。

doi:10.6342/NTU202400684

特定具體原則下更細緻化的要求，藉以縮短執法人員搜索電子載體的時間與範圍，減少強制處分對受搜索人基本權造成的影響[130]。然私鑰無法為同等具體程度的要求，僅在搜索票上載明「私鑰」即可。緣執法人員若可於搜索行動前知曉移轉目標比特幣所需的私鑰為何，便得即時利用其將目標比特幣移轉至專供檢警機關使用的比特幣位址，無疑使發動當次搜索的相當理由消失。

倘若僅記載私鑰或比特幣，則執法人員恐藉此遍尋受搜索人處所有可能存放私鑰的載體，包括其持有的電腦、行動電話、行動硬碟等裝置，造成受搜索人不成比例的隱私權侵害。或若僅記載可能儲存私鑰的載體（例如：一臺受搜索人持有的 A 品牌筆記型電腦），除了目標私鑰，似亦允許執法人員得就載體內儲存的其他檔案或電磁紀錄為搜索；惟此時參考前揭 United States v. Riccardi 案的意旨，搜索令狀未特定載體內的檔案或電磁紀錄，不能使執法人員確定並辨識何等品項應被搜索、扣押，亦有不當侵害受搜索人的隱私之虞，而與特定明確原則的要求不符。

另法院或執法人員原則上應盡可能在發動搜索行動前，嘗試釐清、確認嫌疑人儲存私鑰的載體為何，比如透過蒐集嫌疑人進行比特幣交易之相關資訊，分析其較習慣使用的載體，藉以更具體記載成例如「比特幣位址 1f52FsR526Gqwx904GF30Dxca930Qws52D、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的 A 品牌筆記型電腦、B 品牌桌上型電腦」[131]。惟要求法院或執法人員事先精準地預測所有需搜索或應扣押之載體，無疑係緣木求魚。制度上應准許法院在令狀為較彈性的記載，使警察官員得以在搜索現場隨機應變，以滿足實際執行

[130] 此處特別強調「在偵查資訊充分的狀況下」，係因著部分執法人員對比特幣技術的不熟悉，或基於其他技術原因而無法獲取比特幣位址的資訊時，實難要求執法人員在搜索票上記載欲搜索的比特幣位址。

[131] 執法人員不一定可確切知曉移轉目標比特幣所需的私鑰，係儲存於嫌疑人持有的何項載體當中。但可透過本段提及的偵查活動所蒐集到之資訊或情報，盡可能將載體的範圍具體載明，而避免僅記載「儲存私鑰的載體」。

doi:10.6342/NTU202400684

上的需要[132]。

然嫌疑人儲存私鑰的錢包若係熱錢包，則因著此時儲存私鑰的載體不等於比特幣錢包，而係載體內部的熱錢包程式，故此時搜索客體應記載成例如「比特幣位址 1f52FsR526Gqwx904GF30Dxca930Qws52D、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的熱錢包程式、A 品牌筆記型電腦、B 品牌桌上型電腦」，併予敘明。

綜上，若按前揭方式記載私鑰或助記詞，或甚以更精確的方式描述，不僅可說明法院授權之搜索確係具有相當理由，亦使執法人員經合理查證後，得據搜索票上的記載執行，降低其誤判搜索或扣押客體的風險，避免過度侵害受搜索人的隱私，以符特定明確原則之要求[133]。

第二款、一目瞭然法則於搜索電子載體時之適用

第一目、問題提出

如前文所述，在令狀主義的要求下，非基於急迫情事或實際的執法需要，執法人員僅得就搜索票或扣押裁定上記載的事項為搜索、扣押，限制其可搜索、扣押的範圍，藉以確保強制處分之發動確實存有相當理由，避免法院事後判斷的偏頗，並透過聲請程序篩檢不必要的搜索、扣押[134]。然而，倘執法人員執行搜索、扣押的

[132] 李榮耕，前揭註 109，頁 124。以本段所舉的例子而言，在執法人員提供的偵查資訊可能不夠充沛，如無法判斷儲存私鑰的電腦究竟是筆記型電腦或桌上型電腦時，法院在搜索票上記載「可能儲存私鑰的電腦」即可，執行時再交由警察官員在搜索現場判斷。

[133] 李榮耕，前揭註 109，頁 815。

[134] 王兆鵬、張明偉、李榮耕，前揭註 91，頁 181-189。

doi:10.6342/NTU202400684

過程中，無意間發現搜索票或扣押裁定上未記載之本案應扣押物，或者另案應扣押之物，要求其就此聲請並等待法官另行簽發搜索票或為扣押裁定後方得行動，恐顯得緩不濟急且與國民法感情不符[135]。就此，第 137 條、第 152 條關於附帶扣押、另案扣押的規定，便允許執法人員在當次搜索、扣押係合法的前提下，倘依相當理由之標準認定，發現之物乃搜索票或扣押裁定上未記載之本案應扣押物，或另案應扣押之物，執法人員得在無令狀的情況下扣押之[136]。

針對前揭規定，國內有學者認為，為避免使搜索票或扣押裁定控制搜索、扣押之意旨流於形式，導致執法人員濫行搜索、扣押的情況發生，第 137 條、第 152 條應限縮解釋為「於發見搜索票所記載之物以前，所發見的本案應扣押之物，或另案應扣押之物，始得扣押」[137]。另有學者不認同上開見解，認為此說法未必能防範執法人員之濫權，對執法人員亦有失公允[138]。如此一來，第 137 條、第 152 條究竟應如何適用？

本文認為，應以「一目瞭然法則」（the Plain View Doctrine）作為前揭規定的適用標準，方得同時兼顧發現真實、程序正義與人權保障。緣所謂的「一目瞭然法則」源自美國法，係指當執法人員在合法搜索或逮捕時，落入目視範圍內之證據或得沒收物，得無令狀扣押之[139]。此法則一方面基於公益與犯罪訴追，無法期待執法人員對違法事證視而不見，任由證據或應沒收之物滅失，或危及自身與公眾安全；一方

135 林俊益，前揭註 91，頁 401。

136 林俊益，前揭註 91，頁 402-408；林鈺雄，前揭註 90，頁 455-456。刑事訴訟法第 137 條：「（第一項）檢察官、檢察事務官、司法警察官或司法警察執行搜索或扣押時，發現本案應扣押之物為搜索票或扣押裁定所未記載者，亦得扣押之。（第二項）第一百三十一條第三項之規定，於前項情形準用之。」刑事訴訟法第 152 條：「實施搜索或扣押時，發見另案應扣押之物亦得扣押之，分別送交該管法院或檢察官。」

137 黃東熊、吳景芳，前揭註 97，頁 206-207。

138 王兆鵬、張明偉、李榮耕，前揭註 91，頁 322。

139 王兆鵬、張明偉、李榮耕，前揭註 91，頁 322-323；張麗卿，前揭註 95，頁 298-299；Coolidge v. New Hampshire, 403 U.S. 443 (1971).

doi:10.6342/NTU202400684

面為避免執法人員濫行擴權，故將此種得無令狀搜索的狀況，侷限於以目視方式發現證據之情形[140]；另方面執法人員知曉應扣押之物係透過目視方式，並未使用其他工具或設備，為原先對物強制處分之通常延伸，無造成受搜索人基本權更進一步的侵害，與先前合法強制處分之正當性相去不遠。就一目瞭然法則而言，除了國內有學者認為，此即附帶扣押與另案扣押規定的理論基礎，故在適用相關規定時，應參酌此法則之意旨[141]；我國實務亦有援引此法則，作為詮釋第 137 條第 1 項中的「發現」與第 152 條中的「發見」之內涵[142]。綜上所述，以一目瞭然法則作為適用第 137 條、第 152 條的標準，應屬妥當。

今為確認得移轉目標比特幣的私鑰或助記詞之所在，執法人員因而檢視嫌疑人持有的電腦、行動裝置等電子載體內儲存資訊之動作，勢必將瀏覽到與本案無關的檔案、程式或網頁。此時，倘於該些電子載體內發現應扣押但搜索票或扣押裁定未記載，或者另案應扣押的文件檔、影像等電磁紀錄，則執法人員得否按第 137 條附帶扣押，或按第 152 條另案扣押？此問題的重要性在於，受搜索人持有的電子載體通常能儲存許多個人隱私資訊，尤其係可透過網路連結至雲端伺服器的現況[143]。

具體言之，倘法官簽發的搜索票上，記載的應扣押之物僅有涉案的目標比特幣；惟執法人員因而在現場接觸受搜索人持有的電腦，瀏覽該電腦主機內儲存的數位資訊後，倘發現搜索票上未記載之本案應扣押電磁紀錄，或者另案應

[140] 林文村（2022），〈附帶搜索「立即控制範圍延伸」之理論與適用分析—比較法的觀察〉，《軍法專刊》，68 卷 3 期，頁 122。

[141] 王兆鵬，前揭註 35，頁 34-35。

[142] 請參見如：最高法院 101 年度台上字第 763 號刑事判決、最高法院 103 年度台上字第 448 號刑事判決、臺灣高等法院 96 年度上訴字第 2935 號刑事判決。

[143] 徐仕瑋（2013），〈數位證據與現行搜索、扣押法制間之適用問題〉，《檢察新論》，13 期，頁 37；吳景欽（04/07/2022），〈電磁紀錄怎麼刑事扣押〉，《ETtoday 新聞雲》，https://www.ettoday.net/news/20220407/2223595.htm?fbclid=IwAR2Rpt-JAodl_b4r0OTUEqxXdvE8Dti_kB_cAXhYWFEWfO1zMgatB74AeB7c（最後瀏覽日：10/05/2023）。

doi:10.6342/NTU202400684

扣押之電磁紀錄，得否基於一目瞭然法則，按第 137 條或第 152 條扣押之[144]？就此，本文認為這些是搜索、扣押比特幣時，現行刑事訴訟法在適用上亦可能需面對的課題。

涉及搜索、扣押電磁紀錄的案件中，我國實務目前尚未就上述課題形成穩定見解，僅在零星判決當中提及。舉例來說，於 2020 年國內發生的一件涉及個人資料保護法之本案，調查處人員合法搜索他案被告持有的手機，檢視其安裝的通訊軟體內與本案被告的對話紀錄（此非他案搜索票上記載的搜索客體）並扣押之，此時得否依一目瞭然法則，認定對本案被告對話紀錄的扣押係合法，上開對話紀錄於本案具有證據能力[145]？

就此，一審法院於本案判決書中認為，「……被告與證人張簡宏斌之 LINE 通訊軟體之對話紀錄及數位採證之對話紀錄，確實是調查處人員在執行本院核發搜索票之合法搜索下，查扣證人張簡宏斌之手機，然查扣證人張簡宏斌之手機後，除非進一步點選手機內的 APP，進一步查閱相關通訊內容，否則是無法看到本件被告與張簡宏斌的 LINE 對話內容」，故認為「……無法簡單的一望即得被告與張簡宏斌之對話內容，在在都需要進一步點選查找，或是翻閱查找，即與上揭最高法院裁判意旨揭露之『另案扣押』之要件之一：『一目瞭然』法則不合。[146]」自上述內容可推知，本案法院嘗試以執法人員是否進一步點選 APP、查閱內容

[144] 以執法人員搜索熱錢包為例，就前一項本文建議搜索票上的應記載事項（比特幣位址 1f52FsR526Gqwx904GF30Dxca930Qws52D、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的 A 品牌筆記型電腦、B 品牌桌上型電腦）而言，倘若開啟受搜索人持有載體內的熱錢包後，發現其頁面上不僅顯示目標比特幣位址，亦有其他受搜索人創建的比特幣位址。此時執法人員基於相當理由認為，其他的比特幣位址亦有可能被受搜索人利用於本案或他案的犯罪情事，即有適用一目瞭然法則的空間。

[145] 關於本件的相關報導，請參見：自由時報（08/06/2023），〈獨家》罕見！「手機內」違法搜索？被告律師獲判無罪〉，https://news.ltn.com.tw/news/society/breakingnews/4387484（最後瀏覽日：10/03/2023）。

[146] 請參見：臺灣臺南地方法院 112 年度訴字第 111 號刑事判決。

doi:10.6342/NTU202400684

等舉動，判斷執法人員扣押搜索令狀以外的電磁紀錄時，其客觀上有無更加侵害受搜索人的隱私，藉以決定有無一目瞭然法則之適用。

然本案的二審法院未接受前段一審法院的看法，而係因著電磁紀錄並無固定實體，而須儲存於電子載體等與實體物不同的技術特性，否定搜索、扣押電磁紀錄有一目瞭然法則之適用。二審法院闡述：「……數位證據之儲存及取得有其特殊性，傳統搜索、扣押物理性之實體物方式，無法完全套用於數位證據之搜查及取得，傳統搜索扣押，可以藉由搜索票記載明確控制搜索範圍，數位證據之搜索、扣押，令狀無法發揮類似功能，且偵查階段嫌疑人之涉嫌事實仍具浮動性，令狀僅在審查行為人嫌疑是否達到發動搜索、扣押之門檻，並核准偵查機關發動對嫌疑人之進一步偵查行為，在尚未實際搜索、扣押預定取得作為證據之物品前，令狀無法事先指定有關數位證據第二階段搜索、扣押之具體鑑識方法，在開啟電腦設備後，資訊以檔案方式儲存，偵查人員無法以視線所及方式，發現某檔案內所儲存之資訊是否即為嫌疑人涉案之相關證據，因此一目瞭然原則明顯無法適用於數位證據之搜索、扣押採證上」[147]。

根據上述兩個來自我國實務的看法，本文認為，本案一審法院以執法人員搜索電子載體時，其舉動是否已逾越搜索令狀允許侵害受搜索人隱私的範圍，作為得否適用一目瞭然法則的看法，無疑要求執法人員聲請搜索令狀時，便準確劃定欲在電子載體內搜索的範圍；然誠如本案二審法院所言，偵查階段的事實仍處於浮動階段，執法人員如何根據事實準確記載將形成不小的挑戰。

本案二審法院則基於電磁紀錄與實體物不同的技術特性及搜索、扣押模式，

[147] 請參見：臺灣高等法院臺南分院 112 年度上訴字第 1355 號刑事判決。

doi:10.6342/NTU202400684

導致搜索令狀無法發揮明確控制搜索範圍及指定數位證據鑑識方法等理由，否定搜索、扣押電磁紀錄有一目瞭然法則之適用。然如此詮釋不僅易使人誤解搜索、扣押電磁紀錄時，特定明確原則對搜索令狀的要求可較為下降；亦未說明倘搜索、扣押電磁紀錄時不適用一目瞭然法則，則執法人員應當如何處理該些應扣押但搜索票或扣押裁定未記載，或另案應扣押的電磁紀錄。

就本目涉及一目瞭然法則的課題而言，上述見解提出的判準各自有其不足之處。又誠如前文所述，我國刑事訴訟法第 137 條關於附帶扣押及第 152 條關於另案扣押的規定，其法理基礎與美國法上的一目瞭然法則相同。綜合分析後，本文認兩國法制在此部分具有可比性，故美國法上關於一目瞭然法則的相關案例，值得我國借鏡其論述。故本文選擇借鏡美國法上的 United States v. Carey 案，觀察此類型案例中，美國實務係如何適用一目瞭然法則。

第二目、美國法院相關判決之借鏡

關於 United States v. Carey 案中執法人員對涉案電腦的搜索過程，本文扼要敘述如下[148]：執法人員持搜索令狀對被告住處發動搜索，除了扣押涉案的古柯鹼、大麻等毒品，亦將被告住處內可能供作毒品交易證據的兩臺電腦一併扣押。隨後，警方便開始對這兩臺電腦為電腦鑑識。在鑑識過程中，執法人員雖屢以如錢、帳戶、人等關鍵字試圖找尋涉案的數位資訊，但卻一無所獲。於此同時，執法人員發現眾多標記「JPG」的檔案，其部分內容係兒童的情色影像。惟管轄法院就警方為搜索上開電腦而聲請的搜索令狀上，記載得搜索的檔案範圍，僅包括涉及販賣與散布管制物質的姓名、電話號碼、收據、住址及其他文件證據[149]。

[148] United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).
[149] *Id.* at 1270-71.

doi:10.6342/NTU202400684

本件中，執法人員於鑑識過程中發現的兒童情色影像檔，是否有一目瞭然法則之適用？警方主張，執法人員無意間發現第一張兒童情色影像檔時，其便足以產生相當理由認為，被告電腦內儲存的其他檔案亦可能含有相似的內容，因而可搜索之。如同持搜索令狀去搜索裝有許多抽屜的檔案櫃（file cabinets），儘管每個抽屜皆已標明名稱，但執法人員仍須逐一開啟檢視，確認抽屜內是否存有目標物，避免遭抽屜外標記的名稱混淆。被告則辯駁，執法人員後續對兒童情色影像檔所為之搜索，已使其持有的搜索令狀成為「概括令狀」（general warrant）。基於美國聯邦憲法增修條文第四條對應扣押物的描述必須具有充分特定性之要求，執法人員對兒童情色影像檔的搜索係屬違法[150]。

針對本件爭議，法院參酌聯邦最高法院的見解認為，一目瞭然法則並非讓執法人員得任意擴張搜索的範圍，亦不允許其在尋獲最後一個應扣押之物前，可任意為搜索[151]。執法人員固然較難單從檔名判斷此檔案是否與本案有關，通常須開啟檔案後，方能確認其內容是否涉及本件毒品交易。然一旦執法人員得知其中一個 JPG 檔的內容係兒童情色影像後，倘基於其他 JPG 檔亦是相似情慾內容的相當理由，開始逐個檔案搜索確認，法院認為，此時執法人員的動作並不構成無意發現，而無一目瞭然法則之適用[152]。

另一方面，法院亦不認同警方將搜索被告的電腦檔案，類比為對檔案櫃抽屜進行搜索之形容。緣相較過往的儲存方法，電磁儲存空間得存放更多數量、更多種類的資訊，封閉容器或檔案櫃之類比恐過度簡化美國聯邦憲法增修條文第四條揭示的令狀主義，且忽略現代電腦大量儲存空間的事實（ignore the realities of massive

[150] *Id.* at 1272.
[151] Coolidge v. New Hampshire, 403 U.S. 443 (1971).
[152] United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999).

doi:10.6342/NTU202400684

modern computer storage）[153]。法院認為，此時可將電腦儲存空間類比成混雜大量檔案的搜索現場，執法人員應即時向法官敘明現場狀況，並得其就搜索行動之指示與允許後，方得為進一步的搜索[154]。

第三目、現行刑事訴訟法之適用建議

本款提到的問題，係探討執法人員接觸受搜索人的電子載體時，倘在檢視比特幣位址是在其中何處的過程中，發現搜索票或扣押裁定上未予記載之本案應扣押電磁紀錄，或者另案應扣押之電磁紀錄，則執法人員得否按刑事訴訟法第 137 條附帶扣押，或按第 152 條另案扣押[155]？

借鏡 United States v. Carey 案的意旨，倘執法人員於搜索電子載體的過程中，明知搜索的電磁紀錄已逾當次搜索令狀記載的範圍，卻仍恣意為之時，並無一目瞭然法則之適用。此判決揭示的審查標準，較接近我國實務以執法人員是否惡意違反令狀記載，判斷發現及扣押的本案其他證據或另案證據有無證據能力。倘若搜索、扣押比特幣時援用此標準，我國法院在操作上自是較為熟悉；法院將執法人員惡意違反令狀記載所取得的本案其他證據或另案證據，認定為違反法定程序而取得的證據，不得予以扣押。

另參考國內學者援引外國學者的說法認為，基於對受搜索人隱私權的保護，以及使執法人員於搜索電子載體時不必有所顧忌，得利用一切技術、應用程式與程序在目標載體上為地毯式搜索，藉以取得可證明本案或他案犯罪之證據。執法

[153] United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir.1982).
[154] United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).
[155] 具體案例請參見本文前揭註 144 的說明。

doi:10.6342/NTU202400684

人員搜索電子載體時，若發現其他可供本案或另案證據之用的電磁紀錄，無論其主觀上是否出於惡意，或其尋獲的電磁紀錄涉及重罪或輕罪，應完全排除一目瞭然法則之適用；搜索過程中尋獲的其他本案證據或另案證據，均不得予以扣押[156]。

在現行刑事訴訟法的規範框架下，上述兩種見解皆係處理執法人員於搜索電子載體時，如何適用一目瞭然法則的爭議。審酌對人民隱私權侵害的程度以及偵查犯罪的效率，本文認為宜借鏡 United States v. Carey 案的意旨處理此課題；採納此見解與不採取另一者的理由，如下所述：

就排除一目瞭然法則於搜索電子載體時適用之見解而言，本文肯認其為了保護受搜索人的隱私，因而對執法人員取得的其他本案證據或另案證據採一律排除之立意。不過如此一來，亦可能導致執法人員更肆無忌憚地探知電子載體內所有可得的資訊，人民的隱私將完全暴露於偵查權限之下。基於上述理由，本文認為不宜採納此見解[157]。

解讀 United States v. Carey 案的意旨，主要以執法人員係出於惡意搜索令狀記載以外的電磁紀錄與否，作為是否適用一目瞭然法則的審查標準。執法人員扣得目標比特幣前，勢必於搜索令狀劃定的範圍內，遍尋得移轉目標比特幣的私鑰或註記詞；此時，於過程中倘尋獲其他本案證據或他案證據，可推斷執法人員並非蓄意為之，而得適用一目瞭然法則。反之，若執法人員扣得目標比特幣後，仍持續其搜查行動，找尋搜索令狀未記載的其他本案證據或他案證據，可認定執法人員此時的搜索係基於惡意，而無一目瞭然法則之適用。緣執法人員扣得搜索

156 李榮耕，前揭註 99，頁 1106-1107。

157 國內亦有學者對此認為，一律排除所有另案證據的證據能力之作法，將侵蝕國家追訴重大犯罪的利益，我國在個案權衡適用或立法政策選擇上，是否願意接受如此嚴苛的方式，不無疑義。請參見：李榮耕，前揭註 99，頁 1107。

doi:10.6342/NTU202400684

令狀上記載的目標比特幣後，若欲再次開啟對同個受搜索人的身體、物件、電磁紀錄或住宅處所之強制處分，原則上應本於令狀主義之要求向法院提出聲請，否則即喪失搜索令狀節制執法人員搜索行動的作用。倘執法人員忽略此程序上的要求，而持續對同個受搜索人為搜索，可認其係基於惡意為之，實無以一目瞭然法則保護此時搜索發現的證據之必要。

針對此見解，有學者提出兩點評論[158]。其一，執法人員取得可作為另案證據之用的電磁紀錄時，其是否出於惡意的主觀層面判斷，恐存在極高的審查難度。其二，有鑑於電磁紀錄的特性，倘執法人員遵循機關的內部規則，從而鉅細靡遺地檢視電子載體內儲存的檔案或電磁紀錄，以確保是否與本件相關。在檢視過程中，執法人員因此發現可作為另案證據使用的電磁紀錄，實難認定其是出於惡意違反搜索令狀上的記載。

惟就前段兩點評論而言，本文認為有待商榷，並提出以下兩點淺見：

其一，現階段固難期待每位法官皆曾審理涉及搜索、扣押比特幣的案件，而對此作出判決或裁定，但因著我國檢警機關查獲不法分子利用比特幣從事犯罪的案件量逐年增加之趨勢，司法實務可逐漸累積出具體的審查判準，比如前文提及的臺灣臺南地方法院 112 年度訴字第 111 號刑事判決。

其二，關於以機關的內部規則要求執法人員須詳盡檢視電子載體內儲存之檔案，致使無從判斷其搜索令狀記載以外的電磁紀錄之主觀意圖，進而否定 United States

[158] 李榮耕，前揭註 99，頁 1104-1105。此文雖是針對電腦鑑識為評論，然鑑識人員在操作時實際上亦係對電子載體為搜索，故適用於本文尚無明顯矛盾；惟執行電腦鑑識時遵循的步驟與程序，勢必較一般執法人員於現場搜索電子載體的狀況複雜。

doi:10.6342/NTU202400684

v. Carey 案提出的審查標準之說法[159]。此見解有待商榷的原因在於，一目瞭然法則與機關的內部規則彼此所處的法令位階不同，不得以後者間接限制前者的適用範圍。按司法院釋字第 443 號理由書揭示之意旨，對人民的隱私權或財產權為限制者，應以法律、或法律授權主管機關所發布的法規命令為之[160]。上開規則僅係偵查機關對所屬人員業務處理方式的一般性規定，在我國法上的性質屬行政規則，不得以其限制人民的隱私權或財產權[161]。倘執法人員於搜索時遵循上開規則，詳盡地檢視電子載體內儲存的檔案，除了可能擴大受搜索人隱私的侵害，此時亦恐導致一目瞭然法則得適用的空間極其狹小，間接限制立基於一目瞭然法則的刑事訴訟法 137 條、152 條之適用範圍，似有違法律保留原則之虞。

綜上所述，排除一目瞭然法則於搜索電子載體時適用之見解固然立意良善，但操作後可能發生的狀況反而無法妥適保護人民的隱私，且嚴重侵蝕國家追訴重大犯罪的利益。在現行法的規範框架下，本文認為前揭見解不可採，而應以 United States v. Carey 案提出執法人員係出於惡意搜索令狀記載以外的電磁紀錄與否，作為是否適用一目瞭然法則的審查標準。

159 李榮耕，前揭註 99，頁 1104-1105。

160 司法院釋字第 443 號解釋理由書（節錄）:「…至何種事項應以法律直接規範或得委由命令予以規定，與所謂規範密度有關，應視規範對象、內容或法益本身及其所受限制之輕重而容許合理之差異：諸如剝奪人民生命或限制人民身體自由者，必須遵守罪刑法定主義，以制定法律之方式為之；涉及人民其他自由權利之限制者，亦應由法律加以規定，如以法律授權主管機關發布命令為補充規定時，其授權應符合具體明確之原則；若僅屬與執行法律之細節性、技術性次要事項，則得由主管機關發布命令為必要之規範，雖因而對人民產生不便或輕微影響，尚非憲法所不許。」

161 行政程序法第 159 條：「（第一項）本法所稱行政規則，係指上級機關對下級機關，或長官對屬官，依其權限或職權為規範機關內部秩序及運作，所為非直接對外發生法規範效力之一般、抽象之規定。（第二項）行政規則包括下列各款之規定：一、關於機關內部之組織、事務之分配、業務處理方式、人事管理等一般性規定。二、為協助下級機關或屬官統一解釋法令、認定事實、及行使裁量權，而訂頒之解釋性規定及裁量基準。」

doi:10.6342/NTU202400684

第三章 虛擬資產平台協力義務之依據

執法人員對交易所錢包實施搜索、扣押，其行動最終成功與否的關鍵之一，在於虛擬資產平台業者須負有配合強制處分的協力義務，比如凍結管理特定比特幣位址的交易所錢包，或者提供犯罪嫌疑人於交易所登錄的資料與交易紀錄等。

理論上，面對虛擬資產平台業者管理交易所錢包使用的加密技術或驗證機制，只要擁有足夠的設備、資源及時間，執法人員非不得對交易所錢包實施搜索、扣押之直接強制處分[162]。易言之，虛擬資產平台業者若不願配合執法人員的強制處分時，執法人員得逕行對其所管理的交易所錢包實施搜索、扣押。然之所以課予虛擬資產平台業者負有前揭協力義務之間接強制處分，本文認為係基於兩點理由，以下分述之：

其一，如第二章所述，在古典意義上，財產權作為社會經濟生活的基礎，係以所有權絕對、神聖不可侵犯的姿態出現，屬於排除公權力侵害或干預的消極防禦性權利。然而，隨著 19 世紀共產主義對資本主義過度擴張後的反動，當代憲法多已不再將財產權視為所有者得絕對支配的權利，而是附隨於所有權發生的社會義務，此即財產權的社會義務性[163]。亦即基於增進公共利益之必要，就人民合法取得的財產權而言，國家非不得以法律為合理之限制；此項限制究至何種程度始逾人民財產權所應忍受之範圍，則應就行為之目的與限制手段及其所造成之結果予以衡量[164]。

---

[162] 李榮耕（2018），《通訊保障及監察法》，頁 249，臺北：新學林。虛擬資產平台業者管理交易所錢包可能使用的加密技術，比如將比特幣交易雙方欲傳送的資訊予以重新編碼，確保只有傳送者及接收者方得知悉資訊的內容。

[163] 李惠宗，前揭註 95，頁 284-285；許育典，前揭註 95，頁 296-297；法治斌、董保城（2012），《憲法新論》，5 版，頁 273-275，臺北：元照。財產權的社會義務性亦為我國憲法實務所承認，請參見司法院釋字第 577 號解釋解釋文。

[164] 節錄自司法院釋字第 564 號解釋理由書。

doi:10.6342/NTU202400684

沿著財產權社會義務性的脈絡，虛擬資產平台管理的交易所錢包固屬私人財產，執法人員原則上不得動用公權力干涉或限制之。然本文認為，為追求發見真實及遏阻犯罪的重要公益，當執法人員搜索、扣押交易所錢包時，要求虛擬資產平台負有凍結管理特定比特幣位址的交易所錢包，或者提供犯罪嫌疑人在交易所登錄的資料與交易紀錄之協力義務。不僅有助於搜索、扣押任務之完成，且衡量前揭重要公益之追求與虛擬資產平台對其交易所錢包之使用、收益，虛擬資產平台就其財產之利用，應一定程度容忍相關協力義務加諸的限制，落實財產權社會義務性的面向。

其二，因著各虛擬資產平台業者管理交易所錢包使用的加密技術或驗證機制不盡相同，比如幣安使用的兩階段驗證（Two-Factor Authentication）或 HitBTC 交易所支援的實體金鑰設定。即便不考慮突破這些加密技術或驗證機制需耗費的時間與人力，執法人員亦有必要先透過虛擬資產平台業者瞭解其使用的加密技術或驗證機制。故基於加密技術或驗證機制之特性，為使執法人員順利完成搜索、扣押交易所錢包的任務，此時虛擬資產平台業者須負有配合強制處分的協力義務。

然同樣是配合執法人員的偵辦行動，於現行法下，我國虛擬資產平台並無如電信事業或郵政事業，須按通訊保障及監察法第 14 條第 2 項、第 4 項負有協助執行通訊監察的義務之規定 [165]；或者如銀行須遵循存款帳戶及其疑似不法或顯屬異常交易管理辦法第 5 條，暫停警示帳戶的全部交易功能 [166]。因此，當執法人員搜索、

[165] 通訊保障及監察法第 14 條（節錄）:「（第 2 項）電信事業及郵政事業有協助執行通訊監察之義務；其協助內容為執行機關得使用該事業之通訊監察相關設施與其人員之協助。（第 4 項）電信事業之通訊系統應具有配合執行監察之功能，並負有協助建置機關建置、維持通訊監察系統之義務。但以符合建置時之科技及經濟上合理性為限，並不得逾越期待可能性。」

[166] 存款帳戶及其疑似不法或顯屬異常交易管理辦法第 5 條：「存款帳戶依前條之分類標準認定為疑似不法或顯屬異常交易者，銀行應採取下列處理措施：一、第一類：（一）存款帳戶如屬偽冒開戶者，應即通知司法警察機關、法務部調查局洗錢防制處及財團法人金融聯合徵信中心，銀行並應即結清該帳戶，其剩餘款項則俟依法可領取者申請給付時處理。（二）存款帳戶經通報為警示帳戶者，應即通知財團法人金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入

doi:10.6342/NTU202400684

扣押交易所錢包時，要求我國虛擬資產平台負有協力義務之依據何在，自是必須充分回應的問題。

本章主要探討執法人員倘要求我國虛擬資產平台負有配合強制處分之協力義務時，其可能的依據為何。對此，本文依序分析洗錢防制法第 13 條第 1 項、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，以及虛擬資產平台及交易業務事業（VASP）公會自律規範，何者較適合作為前揭協力義務之依據。

值得特別說明的是，本文以下選擇使用「虛擬資產平台」，指稱從事包括比特幣、以太幣等虛擬通貨之交換、移轉或保管等營業活動的業者，與我國現行條文當中亦出現的「虛擬通貨平台」在概念上並無差異。對此，下述兩點理由說明之：

其一，如洗錢防制法、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：虛擬通貨事業洗防辦法）採用的「虛擬通貨」，係源自防制洗錢金融行動工作組織（Financial Action Task Force，以下簡稱 FATF）於 2014 年發布的研究報告中 Virtual Currency 的中譯[167]。惟鑑於虛擬資產的新產品、服務與商業模式之發展，維持使用 Virtual Currency 恐不足以涵蓋 FATF 欲監管的範圍。FATF 遂自 2018 年起在其發布的 FATF 建議、指引等正式文件，改採 Virtual Asset 此一詞彙取代 Virtual Currency；而 Virtual Asset 於我國官方的中譯便係「虛擬資產」[168]。

款項逕以退匯方式退回匯款行。（三）存款帳戶屬衍生管制帳戶者，應即暫停該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付功能，匯入款項逕以退匯方式退回匯款行。（四）依其他法令規定之處理措施。二、第二類：（一）對該等帳戶進行查證及持續進行監控，如經查證有不法情事者，除通知司法警察機關外，並得採行前款之部分或全部措施。（二）依洗錢防制法等相關法令規定之處理措施。」

[167] FATF, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS, at 4 (2014).

[168] FATF 在洗錢防制及打擊資恐領域係國際間公認最具影響力的組織。而我國身為亞太防制洗錢組織（Asia/Pacific Group on Money Laundering）的成員國，負有遵守 FATF 建議（The FATF Recommendations）之義務。就 FATF 監管虛擬資產的歷程之相關介紹，請參見

doi:10.6342/NTU202400684

其二，按我國金融監督管理委員會於 2023 年 9 月新頒布的「管理虛擬資產平台及交易業務事業（VASP）指導原則」，其對虛擬資產平台的定義，便係完全沿襲自虛擬通貨事業洗防辦法第 2 條第 1 項第 1 款中對虛擬通貨平台的定義[169]。由此推論之，我國主管機關於將來的立法程序中，亦有意以虛擬資產平台替代虛擬通貨平台，指稱受其監管的平台業者。

本章後述「第一節、第二項、虛擬通貨事業洗防辦法第 7 條」的說明。

[169] 管理虛擬資產平台及交易業務事業（VASP）指導原則，頁 2。此原則中明確指出：「參考洗錢防制法第 5 條第 2 項及『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 2 條所定『虛擬通貨平台及交易業務事業』規定，敘明本指導原則規範對象，即國內虛擬資產平台及交易業務事業之定義。」

doi:10.6342/NTU202400684

第一節、虛擬資產平台之協力義務

本節主要探討執法人員搜索、扣押交易所錢包時，要求虛擬資產平台負有配合強制處分的協力義務，比如凍結管理特定比特幣位址的交易所錢包，或提供犯罪嫌疑人於交易所登錄的資料與交易紀錄等，其所憑依據為何。

對此，本節以下將依序分析現行法中意旨較接近的規定，以及虛擬資產平台及交易業務事業（Virtual Asset Service Providers, VASP）公會自律規範。之所以選擇不同層次的規範探討，係因著在財產權社會義務性的脈絡建構之虛擬資產平台協力義務，我國就其訂定的依據，係散落在法律、法規命令，以及透過發布指導原則將公權力滲入公會自律規範等層次。

第一項、洗錢防制法第 13 條第 1 項

針對凍結管理特定比特幣位址的交易所錢包，洗錢防制法第 13 條第 1 項提供了一個回應[170]。虛擬資產平台之所以適用本條，係因同法第 5 條第 2 項將虛擬資產平台認定為適用洗錢防制法關於金融機構的規定之主體[171]。如此一來，倘檢察官於偵查中，認被告涉有利用帳戶、匯款、通貨或其他支付工具犯洗錢防制法第十四條及第十五條之罪時，得在取得該管法院核發對該筆目標比特幣為禁止提款、轉帳、

[170] 洗錢防制法第 13 條第 1 項：「檢察官於偵查中，有事實足認被告利用帳戶、匯款、通貨或其他支付工具犯第十四條及第十五條之罪者，得聲請該管法院指定六個月以內之期間，對該筆交易之財產為禁止提款、轉帳、付款、交付、轉讓或其他必要處分之命令。其情況急迫，有相當理由足認非立即為上開命令，不能保全得沒收之財產或證據者，檢察官得逕命執行之。但應於執行後三日內，聲請法院補發命令。法院如不於三日內補發或檢察官未於執行後三日內聲請法院補發命令者，應即停止執行。」本項規定雖未明文受規範的客體，然參酌同是對特定債權為禁止向債務人收取或為其他處分，並禁止向被告或第三人清償的刑事訴訟法第 133 條第 5 項，以及其於 2016 年 06 月 22 日增修時的立法理由，本文認為本段情境當中受禁止命令規範的客體，應係被告與受被告所託管理該筆比特幣的虛擬資產平台業者。

[171] 洗錢防制法第 5 條第 2 項：「辦理融資性租賃、虛擬通貨平台及交易業務之事業，適用本法關於金融機構之規定。」

doi:10.6342/NTU202400684

付款、交付、轉讓或其他必要處分之命令後，要求虛擬資產平台負有凍結特定交易所錢包之義務。甚至在情況急迫，不即時行動恐不得保全得沒收或得為證據之目標比特幣時，檢察官亦得逕命執行，要求虛擬資產平台負擔上開義務。

就本項規定而言，其立法目的固在藉由對人民的金融交易工具為禁止、限制付款、轉帳、提款或交付等強制處分權之行使，避免匯款或其他通貨以外之支付工具，遭不法分子利用作為從事洗錢之工具[172]。惟本文認為在執行面可能遭遇的問題，恐使執法人員依本項要求虛擬資產平台負有凍結交易所錢包的協力義務時，其過程將面臨諸多困難與挑戰。以下析述之：

按本項文義，對交易所錢包為禁止與限制之方式，原則上係檢察官就該筆目標比特幣，向該管法院聲請核發凍結之命令。惟隨著比特幣交易匿名性技術之發展，提供不法分子得利用如混幣器（mixers and tumblers）的技術，將目標比特幣與其他虛擬通貨混合後，再與交易對象進行比特幣之交易，使原先即不易識別實際交易對象的虛擬資產平台與檢察官，在分辨是否為該筆應予聲請凍結的目標比特幣時，增加更多技術上的障礙[173]。

---

[172] 於 2003 年 02 月 06 日公布、同年 08 月 06 日施行的舊洗錢防制法，第 8 條之一的立法理由（節錄）：「二、**匯款或其他通貨以外之支付工具亦有被不法分子利用作為從事洗錢之工具，爰明列於得禁止或限制金融交易之範圍**。三、**對於人民之金融交易工具為禁止、限制付款、轉帳、提款或交付等強制處分權之行使，應採令狀主義，以符合憲法保障人民財產權之本旨，爰明定上開權限由法院行使，並為避免影響當事人權益**，其禁止或限制金融交易之期限為六個月之內，至於檢察官於情況急迫時，為保全證據亦得為上開禁止或限制交易之命令，並於三日內報請法院補發命令，法院如不於三日內補發時，應即停止執行，以維護人民之權利。法院為上開禁止或限制金融交易之命令，應以書面為之，並準用刑事訴訟法第一百二十八條之規定。」之所以援引上述立法理由，係因洗錢防制法在 2007 年 07 月 11 日、2009 年 06 月 10 日及 2016 年 12 月 28 日酌為文字修正與條次變更的數次增修中，將本條規範為條次變更至現行法的第 13 條；但單就規範意旨而言，現行法第 13 條與 2003 年舊法第 8 條之一的旨趣幾乎完全相同。故本文援引 2003 年舊法第 8 條之一的立法理由，作為適用現行法第 13 條時得參考的立法意旨。

[173] 混幣器係使不同來源與不同種類的虛擬通貨混合之軟體服務，其得將原本可被追蹤的目標虛擬通貨與其他虛擬通貨混合後，再移轉至使用者指定的位址，藉以隱匿虛擬通貨交易之流向。關於混幣器的進一步說明，請參見：羅韋淵，前揭註 15，頁 33。

doi:10.6342/NTU202400684

且為遵循本項對人民的金融交易工具為干預時，檢察官於偵查中僅得就「該筆目標比特幣」，而不得就「被告持有的比特幣錢包」向該管法院聲請凍結之命令。倘面臨該筆目標比特幣在同個比特幣錢包拆分成多筆交易先後出現，乃至散布在不同比特幣錢包的狀況時，檢察官勢必就目標比特幣之交易為逐筆確認後，方能同時或先後向該管法院聲請凍結之命令。與目前國內偵查實務得對銀行的警示帳戶採暫停全部交易功能之作法相比，上述操作為遵循令狀主義的要求，大幅增加執法人員搜索、扣押比特幣時需耗費的人力與時間，恐已過度犧牲執法效率，導致執法人員在實務操作時的困難。

另檢察官亦不得就目標比特幣價額為整體記載（例如：約當價值新臺幣十萬元的比特幣），而必須個別記載欲扣押的目標比特幣，其主要原因在於，在我國現行法制下比特幣非屬法定貨幣之債，而係特定的給付[174]。申言之，比特幣並非由我國中央銀行發行的貨幣，且個別比特幣獨有的技術特徵，包括公有鏈上的交易紀錄、私鑰及助記詞，是可藉此與其他比特幣相區辨。檢察官搜索、扣押比特幣的令狀上，不得如扣押我國國幣的記載方式，不重視個別貨幣之本身而僅就整體數額為記載[175]；相反地，個別記載欲扣押的目標比特幣，對後續如沒收、發還被害人等程序，在財產歸屬的釐清上亦有裨益。

綜上所述，倘該當洗錢防制法第 13 條第 1 項前段的情形，檢察官固得依此向該管法院就該筆目標比特幣之凍結聲請核發命令；或在情況急迫，不即時行動恐不得保全得沒收或得為證據之目標比特幣時，由檢察官逕命凍結該筆目標比特幣。然

[174] 劉春堂（2011），《民法債編通則（一）契約法總論》，增修版，頁 189-198，臺北：自版。所謂貨幣之債，又可稱為金錢之債，係指給付一定數額的貨幣為標的之債。其中以具有強制通用效力的貨幣為給付者，稱之為法定貨幣之債。

[175] 中央銀行法第 13 條第 2 項：「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。」

doi:10.6342/NTU202400684

因著比特幣交易匿名性技術之發展，使虛擬資產平台不易配合執行凍結該筆目標比特幣之命令，以及在執法效率與遵循令狀主義之間的權衡，過度偏重後者而造成執法人員實務操作時的困難。考量偵查實務上可能遭遇的技術障礙與低落的執法效率，本文認為執法人員搜索、扣押交易所錢包時，本項不宜作為要求虛擬資產平台負有凍結特定交易所錢包，或查詢犯罪嫌疑人於交易所登錄的資料與交易紀錄等協力義務之明文依據[176]。

第二項、虛擬通貨事業洗防辦法第 7 條

就要求虛擬資產平台負有配合強制處分的協力義務而言，虛擬通貨事業洗防辦法第 7 條第 1 項、第 2 項的規範內容，亦提供一個回應[177]。自前揭規範的字面觀察，本規定係在執法人員要求時，僅為轉出人處理交易的虛擬資產平台業者負有提供虛擬資產移轉相關資訊的義務，課予其協助執法人員搜索或扣押特定交易所錢包的責任。

惟若欲以本規定建構上述虛擬資產平台的協力義務，停留在字面上的觀察並不足夠，而有必要結合其規範脈絡與政策背景瞭解。因此，本文接下來將以虛擬資產

[176] 與本文採相同結論者，請參見：羅韋淵，前揭註 15，頁 40。

[177] 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：「（第一項）本事業如擔任虛擬通貨移轉之轉出方，應依下列規定辦理：一、應取得必要且正確之轉出虛擬通貨之客戶（以下簡稱轉出人）資訊及必要之接收虛擬通貨之客戶（以下簡稱接收人）資訊，且依第十條規定保存所取得之前開資訊，並應將前開資訊立即且安全地提供予擔任接收方之事業。檢察機關及司法警察機關要求立即提供時，應配合辦理。二、前款轉出人及接收人之必要資訊應包括：（一）轉出人資訊應包括：轉出人姓名、轉出虛擬通貨之錢包資訊及下列轉出人各項資訊之一：1.官方身分證明文件號碼。2.地址。3.出生日期及出生地。（二）接收人資訊應包括：接收人姓名、接收虛擬通貨之錢包資訊。三、本事業未能依前二款規定辦理時，不得執行虛擬通貨之移轉。（第二項）本事業如擔任虛擬通貨移轉之接收方，應依下列規定辦理：一、應採取適當措施，以辨識出缺少前項第二款必要資訊之虛擬通貨移轉。二、應具備以風險為基礎之政策及程序，以判斷何時執行、拒絕或暫停缺少前項第二款必要資訊之虛擬通貨移轉，及適當之後續追蹤行動。三、應依第十條規定，保存所取得之轉出人及接收人資訊。（第三項）本事業執行虛擬通貨之移轉時，應確認交易對手（接收方或轉出方）之事業所受監理規範與防制洗錢金融行動工作組織（FATF）所定防制洗錢及打擊資恐標準一致。」

doi:10.6342/NTU202400684

平台的協力義務為核心，簡要爬梳包括 FATF 所制定的相關規範或者指引、洗錢防制法、虛擬通貨事業洗防辦法以及我國金融監督管理委員會（以下簡稱：金管會）於 2023 年 9 月頒布的《管理虛擬資產平台及交易業務事業（VASP）指導原則》（以下簡稱：VASP 指導原則）後，嘗試在現行法制與政策之框架下進行答覆。

之所以將 FATF 制定的相關規範或指引納入此問題之討論範圍，是因為此組織在 1989 年舉行的七國高峰會議（Group of Seven Summit）成立後，便致力於檢視各種洗錢犯罪的手段，以建立防制洗錢及打擊資恐的標準，並持續敦促、監督各國政府透過立法與監理改革相關措施[178]；迄今加入的成員國已近四十個，在洗錢防制及打擊資恐領域係國際間公認最具影響力的組織[179]。而且我國身為亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，以下簡稱 APG）的成員國，負有遵守 FATF 建議（The FATF Recommendations）之義務[180]；近年在洗錢防制法、資恐防制法、虛擬通貨事業洗防辦法增修的部分，其立法理由多半有提及參考 FATF 制定的相關規範或指引[181]。故處理我國虛擬資產平台究無負有協助執法人員搜索、扣押行動的法定義務時，本文認為有必要將 FATF 制定的相關規範或指引列入討論，併予敘明。

---

178 FATF, *History of the FATF*, https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html (last visited: 10/22/2023).

179 台灣金融研訓院編輯委員會（2021），《防制洗錢與打擊資恐政策及法令解析》，頁 28-29，臺北：財團法人台灣金融研訓院。

180 請參見 2016 年 12 月 28 日公布的洗錢防制法第 1 條之立法理由（節錄）：「……二、我國為亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，以下稱 APG）之會員國，有遵守防制洗錢金融行動工作組織（Financial Action Task Force，以下簡稱 FATF）於二O一二年發布之防制洗錢及打擊資助恐怖主義與武器擴散國際標準四十項建議（以下簡稱 FATF 四十項建議）規範之義務，.....。」

181 請參見如：2016 年 07 月 27 日公布的資恐防制法第 3 條至第 5 條、2016 年 12 月 28 日公布的洗錢防制法第 2 條至第 4 條之立法理由，以及 2021 年 06 月 30 日公布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之立法總說明。

doi:10.6342/NTU202400684

第一款、FATF 監管虛擬資產與虛擬資產服務提供業者之脈絡

面對包括比特幣在內的虛擬通貨潛在之犯罪風險，FATF 最早於 2014 年發布的研究報告，提出虛擬通貨（Virtual Currencies, VC）的定義與其相關的洗錢、資助恐怖主義之風險[182]。翌年，則首次針對虛擬通貨發布風險基礎方法指引，著重與傳統金融體系連結的虛擬通貨支付商品與服務（Virtual Currency payment products and services, VCPPS）[183]。概括而言，此時期 FATF 尚在研究虛擬通貨將造成何等洗錢防制、資助恐怖主義風險之階段，其所制定的相關規範或指引，主要係關注具有支付工具性質的虛擬通貨，以及提供虛擬通貨與法幣交換服務的金融機構或交易所，並未提及更廣泛意義的虛擬資產與虛擬資產平台[184]。

惟隨著各種關於虛擬資產的新產品、服務與商業模式之發展，諸如匿名程度增強（anonymity-enhanced）的虛擬通貨、混幣器、去中心化交易平台或匿名錢包（privacy wallets）等興起，不僅降低虛擬通貨交易的透明性，亦增加虛擬通貨被利用於洗錢等刑事犯罪的風險[185]。

有鑑於此，FATF 監管虛擬通貨的立場便轉趨嚴格。自 2018 年起先在 FATF 建議詞彙表內，以新增的「虛擬資產」（Virtual Asset, VA）取代先前指引使用的 VC，其定義包括支付或投資目的的數位價值表彰，但排除已受 FATF 建議規範涵蓋的數位法幣、證券或其他金融資產；以新增的「虛擬資產服務提供業者」（Virtual Asset Service Providers, VASP）取代 VCPPS，其定義不僅包括提供法幣、虛擬資產間以及

182 FATF, *supra* note 167, at 3-12.
183 FATF, GUIDANCE FOR A RISK-BASED APPROACH: VIRTUAL CURRENCIES 3 (2015).
184 楊岳平（2022），〈虛擬通貨的洗錢防制監管疆域與國際標準－評我國「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」〉，《法律扶助與社會》，9 期，頁 108-109。
185 FATF, UPDATED GUIDANCE: A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS 7 (2021).

doi:10.6342/NTU202400684

虛擬資產、虛擬資產間之交易，亦擴及其他關於虛擬資產服務如經紀、移轉、託管或承銷[186]。

2019 年間則修正 FATF 建議第 15 項建議的注釋，明確規定各國應針對虛擬資產服務提供業者設有許可或登記制度，要求其採行 FATF 建議下的相關措施[187]。爾後，於 2020 年、2021 年就每 12 個月檢視虛擬資產洗錢防制議題發布的兩份審查報告，則分別指明 FATF 的 2019 年指引當中哪些部分有必要加強說明，以及指出各國對於虛擬資產洗錢風險存在的若干缺陷，比如全球仍欠缺一套統一的虛擬資產洗錢防制機制、若干國家尚未實施轉帳規則（Travel Rule）等問題[188]。

第二款、轉帳規則與虛擬通貨事業洗防辦法第 7 條

目前 FATF 對虛擬資產的監理方向，除了擴大對於虛擬資產的監管範圍，亦將其管制的對象鎖定為虛擬資產服務提供業者，視其係虛擬資產領域的中介機構，課予其須遵守 FATF 建議第 10 項建議至第 21 項建議的義務[189]。其中，牽涉虛擬資產平台是否負有協助執法人員搜索、扣押行動的法定義務之規範，便係所謂的轉帳規則。

轉帳規則，係指依 FATF 建議第 15 項建議，當虛擬資產服務提供業者為客戶從事的交易逾 1,000 美元時，亦須履行 FATF 建議第 16 項建議關於電匯之規範。詳言

186 FATF, *supra* note 11, at 130.
187 FATF, *supra* note 11, at 76.
188 楊岳平，前揭註 184，頁 13-14。所謂的轉帳規則，國內中文文獻亦有稱為「旅行規則」，係指依 FATF 建議第 15 項建議，要求當虛擬資產服務提供業者為客戶移轉虛擬資產的價值逾 1,000 美元時，亦須履行 FATF 建議第 16 項建議關於電匯之規範。本文將於本項第二款對轉帳規則為詳細介紹。
189 FATF, *supra* note 11, at 77.

doi:10.6342/NTU202400684

之，此時虛擬資產服務提供業者除了須對交易對手方（counterparty VASP）進行盡職調查（due diligence），負責轉出的虛擬資產服務提供業者及負責接受的虛擬資產服務提供業者皆必須取得、驗證及保存客戶資訊[190]。前揭資訊應包括客戶姓名、錢包位址、客戶的地址、身分證字號或生日其中之一[191]。

FATF 課予虛擬資產服務提供業者前揭義務之目的，在於透明化虛擬資產之轉換路徑[192]。如此一來，除了可避免不法分子透過虛擬資產移轉或藏匿犯罪金流，亦裨益各國政府部門查緝稅捐或追訴刑事犯罪時，得在短時間內發現虛擬通貨金流的最終受益人。

為因應 2018 年 APG 的第三輪評鑑，我國於 2017 年 6 月施行大幅度翻修後的洗錢防制法條文，便多係參考 FATF 建議的標準而制定[193]。前文提及的轉帳規則在我國法上具體落實的條文，即係依洗錢防制法第 5 條第 2 項適用同法第 6 條第 3 項訂定的虛擬通貨事業洗防辦法第 7 條[194]。則我國執法人員得否據本條規定，課予虛擬資產平台負有協助執法人員凍結交易所錢包，或提供犯罪嫌疑人於交易所登錄的資料與交易紀錄之協力義務？以下將先後從規範面以及執行面的角度分析。

在規範面上，本條課予虛擬資產平台的轉出方應取得必要且正確（accurate）轉

190 FATF, *supra* note 11, at 77; 許永欽，前揭註 25，頁 28-29。

191 FATF, *supra* note 185, at 59.

192 蔡佩玲（2022），〈虛擬貨幣與洗錢防制──未知之金流世界交易規則〉，《月旦法學雜誌》，324 期，頁 139。

193 行政院，〈洗錢防制新制上路〉，https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/c935e972-67f5-4625-80b6-0e775a846cad（最後瀏覽日：10/26/2023）。

194 洗錢防制法第 5 條第 2 項：「辦理融資性租賃、虛擬通貨平台及交易業務之事業，適用本法關於金融機構之規定。」、洗錢防制法第 6 條第 3 項：「第一項制度之實施內容、作業程序、執行措施，前項查核之方式、受委託之資格條件及其他應遵行事項之辦法，由中央目的事業主管機關會商法務部及相關機關定之；於訂定前應徵詢相關公會之意見。」、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 條的立法理由：「參酌 FATF 評鑑方法論第十五項建議之評鑑準則第九點(b)，明定本事業進行虛擬通貨之移轉時應遵循之事項。」

doi:10.6342/NTU202400684

出人資訊之義務，而擔任接收方的虛擬資產平台僅需辨識轉出人與接收人必要資訊是否短缺，未負有取得必要且正確接收人資訊之義務[195]。如此規範不僅較 FATF 要求擔任轉出方、接收方的虛擬資產平台應分別取得正確之轉出客戶資訊、接收客戶資訊為寬鬆，恐增加執法人員確認相關資訊是否屬實的成本[196]。亦難想像執法人員得據虛擬通貨事業洗防辦法第 7 條規定，請求虛擬資產平台業者配合凍結管理特定比特幣位址的交易所錢包，蓋無法從本條文義得出虛擬資產平台就此負有協力義務。基於上述，就建構虛擬資產平台於執法人員搜索、扣押交易所錢包時的協力義務而言，本文認為虛擬通貨事業洗防辦法第 7 條可發揮的功能相對有限。

在執行面上，依虛擬通貨事業洗防辦法第 18 條，同辦法第 7 條非如其他條文自中華民國 110 年 7 月 1 日起施行，而係由金管會另定施行日期[197]。然截至 2023 年年底，金管會仍未訂定虛擬通貨事業洗防辦法第 7 條的施行日期，故本條迄今仍未被實際執行。 為何金管會遲遲不訂定本條的施行日期，以提升對虛擬資產平台的監管力道，並降低不法分子利用虛擬通貨從事犯罪的風險？

---

[195] 許永欽，前揭註 25，頁 32-33。此處的「正確」係指上述資訊經驗證（verify）確立為真。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：「（第一項）**本事業如擔任虛擬通貨移轉之轉出方，應依下列規定辦理：一、應取得必要且正確之轉出虛擬通貨之客戶（以下簡稱轉出人）資訊及必要之接收虛擬通貨之客戶（以下簡稱接收人）資訊，且依第十條規定保存所取得之前開資訊，並應將前開資訊立即且安全地提供予擔任接收方之事業。檢察機關及司法警察機關要求立即提供時，應配合辦理。**二、前款轉出人及接收人之必要資訊應包括：（一）轉出人資訊應包括：轉出人姓名、轉出虛擬通貨之錢包資訊及下列轉出人各項資訊之一：1.官方身分證明文件號碼。2.地址。3.出生日期及出生地。（二）接收人資訊應包括：接收人姓名、接收虛擬通貨之錢包資訊。三、本事業未能依前二款規定辦理時，不得執行虛擬通貨之移轉。（第二項）**本事業如擔任虛擬通貨移轉之接收方，應依下列規定辦理：一、應採取適當措施，以辨識出缺少前項第二款必要資訊之虛擬通貨移轉。**二、應具備以風險為基礎之政策及程序，以判斷何時執行、拒絕或暫停缺少前項第二款必要資訊之虛擬通貨移轉，及適當之後續追蹤行動。三、應依第十條規定，保存所取得之轉出人及接收人資訊。（第三項）本事業執行虛擬通貨之移轉時，應確認交易對手（接收方或轉出方）之事業所受監理規範與防制洗錢金融行動工作組織（FATF）所定防制洗錢及打擊資恐標準一致。」

[196] FATF, METHODOLOGY FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS (Updated Nov. 2022), at 55.

[197] 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 18 條：「本辦法除第七條由本會另定施行日期外，自中華民國一百十年七月一日施行。」

doi:10.6342/NTU202400684

整理相關文獻的說法後，本文認為金管會迄今仍不願貿然施行本條的緣由，係因目前尚待解決的困境如下：

其一，虛擬資產平台業者彼此間欠缺如傳統銀行體系中的 SWIFT 系統，在客戶資訊傳輸上目前無統一的標準格式，難以達成轉帳規則的要求[198]。其二，轉帳規則課予虛擬資產平台取得客戶資訊之義務，從根本上破壞比特幣等虛擬通貨去中心化、匿名性的特性，引發虛擬資產平台業者們不小的反彈與輿論壓力[199]。

面對虛擬通貨事業洗防辦法第 7 條執行面上的困境，金管會並未動搖其推動本條施行的立場。近期頒布的 VASP 指導原則中，金管會表示將與受規範的虛擬資產平台及交易業務事業研商，漸進推動實施虛擬資產移轉之資訊取得及傳遞規定。規劃先以受規範對象間辦理特定虛擬資產類別且達一定金額以上之移轉交易納入施行範圍，再漸進擴大實施至不限金額及虛擬資產類別之移轉交易[200]。

就前段金管會期望的進程而言，本文的淺見如下：其一，固然我國金管會與 FATF 皆對轉帳規則之推行站在積極肯定的立場，惟 FATF 各成員國並非皆採相同的態度[201]。倘國際間未能對此形成共識，合作建立如統一的交易資訊傳輸規格、彼此的聯絡渠道，轉帳規則在實際運作上恐難克竟全功。其二，依虛擬通貨事業洗防辦法第 2 條第 1 項、第 2 項，我國對虛擬資產平台及交易業務事業的監理範圍，僅限於在國內設立登記者[202]。如此一來，為規避執法人員的查緝行動，

198 許永欽，前揭註 25，頁 29。所謂的 SWIFT 系統，係指由環球銀行金融電信協會（Society for Worldwide Interbank Financial Telecommunication）營運的全球性金融訊息網路，目前為銀行間進行資訊交換的主流管道。關於 SWIFT 系統的進一步說明，請參見：游士弘、郭閔裕（2013），〈「外幣結算平台」之架構設計及系統建置〉，《財金資訊季刊》，75 期，頁 7。

199 蔡佩玲，前揭註 192，頁 138-139。

200 管理虛擬資產平台及交易業務事業（VASP）指導原則，頁 14-15。

201 蔡佩玲，前揭註 192，頁 139。

202 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 2 條（節錄）：「（第一項）本辦法

doi:10.6342/NTU202400684

不法分子勢必多轉向使用未在前揭監理範圍內的虛擬資產平台提供之服務[203]。

綜上所述，在規範面上，虛擬通貨事業洗防辦法第 7 條的規範密度不如 FATF 建議要求的程度；另在執行面上，縱使我國金管會與 FATF 對轉帳規則之施行皆採肯定的立場，惟面對當前技術水準有待突破、國際間就此尚未凝聚具體共識等現階段無法解決之難題，恐使執法人員在實際操作時窒礙難行。故執法人員於搜索、扣押交易所錢包時，得否依本條請求虛擬資產平台負有如凍結管理特定比特幣位址的交易所錢包，或提供犯罪嫌疑人於交易所登錄的資料與交易紀錄之協力義務，本文皆持否定的立場看待。

第三項、虛擬資產平台及交易業務事業（VASP）公會自律規範

第一款、我國虛擬資產平台業者訂定自律規範之優勢與必要性

所謂的自律規範，一般係指由某行業內的自律組織（Self-Regulatory Organization）透過章程、規則或簽署公約之方式，制定約束、管理其會員之規範。由於自律組織係對特定行業或職業團體執行一定程度監督、管理的機構，其權力來源可能係法規、主管機關授權或產業慣例，故除了參與自律組織的會員，該行業的業者亦負有遵循自律規範之義務[204]。以金融產業為例，除了國際間知名的美國金融業監理局（Financial Industry Regulatory Authority）、日本證券業協會（日本証券業協会）或者加拿大投資交易商協會（Investment Dealers Association of Canada）皆有建立相關的

用詞，定義如下：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。……（第二項）前項第一款所稱本事業，係以在國內設立登記者為限。」

[203] 許永欽，前揭註 25，頁 32。

[204] 中國科技大學商學院（2009），《我國證券相關公會自律機制之強化與整合》，頁 1-3。

doi:10.6342/NTU202400684

自律規範，我國的證券商、期貨商或投資信託及投資顧問業，亦有依法成立相應的同業公會並訂定自律規範[205]。

於國家機關制定的法令基礎上，透過自律組織訂定自律規範，藉以管理並監督行業內從業業者之優勢，本文整理相關文獻後歸結出兩點，以下說明：

其一，具體化監管規範，並可及時彈性調整。國家機關若欲推動對某行業的監管政策，通常係透過制定相關監管規範為之，比如我國的銀行法、保險法第五章之內容。但在實際執行時的作業程序、配套措施或技術問題，恐無法鉅細靡遺地於條文或施行細則中呈現。此時便得透過自律規範的要求，將國家制定的監管政策或規範進一步地具體落實。而且民主國家的法令增修從草案形成、議會討論與表決到正式施行，其過程多半十分耗時，恐無法及時因應充滿變數的產業局勢。相較之下，自律規範便得對各種產業面變化，更加彈性地回應與調整[206]。

其二，增加監理資源的質與量，優化監管效率。具有一定代表性的自律組織得擔任產業界與主管機關間的溝通橋樑，除了可扮演主管機關的傳聲筒與協力者之角色，透過自律規範的發布協助推動相關政策，亦得即時向主管機關反映產業內面臨的法遵問題。同時，由於自律組織團隊多由行業內的資深從業人員組成，主管機關可將年度法遵檢查、監測報告分析或證照測驗命題等仰賴從業經驗的任務，部分交

[205] 以我國的投資信託及投資顧問業為例，請參見證券投資信託及顧問法第 88 條第 1 項：「同業公會之任務，除依商業團體法第五條規定辦理外，包括下列事項：**一、訂定自律規範，並督促會員自律。**二、辦理主管機關授權處理之事項。三、對違反法令或自律規範之會員予以停權、課予違約金、警告、命其限期改善等處置；或要求會員對其從業人員予以暫停執行業務一個月至六個月之處置。四、檢查會員是否遵守法令及自律規範。五、對於業務經營顯然不善，重大損害投資人權益之會員，協調其他會員協助處理該會員之業務，或報請主管機關為適當之處分。六、對於破產會員之財產進行管理。七、對於違反本法規定之會員為撤銷或暫停會員資格之處置。」

[206] 恆業法律事務所，前揭註 15，頁 186-187；婁天威（2013），〈新興市場國家採行證券自律組織之分析〉，《證交資料》，619 期，頁 49-50。

doi:10.6342/NTU202400684

由自律組織執行並訂定相關細則，藉以減少監管成本、優化監管效率[207]。

綜上，自律組織訂定的自律規範可在國家立法機關制定法規的基礎之上，除了可彈性地因著複雜多變的產業局勢進行調整，亦得充實監理能量，確保行業內絕大部分業者能在合法合規的狀況下營業。

回歸本節主題，本文認為我國虛擬資產平台業者組成自律組織，並訂定相關自律規範，除了可享有上述優勢，亦得藉此建構關於虛擬資產平台的協力義務。以下說明：

如本節前兩項所述，我國現行法對於執法人員搜索、扣押交易所錢包，虛擬資產平台是否負有協力義務固非完全無規範。然根據本文前述的剖析，可知執法人員若按洗錢防制法第 13 條第 1 項，或虛擬通貨事業洗防辦法第 7 條搜索、扣押交易所錢包，恐因著虛擬資產平台執行上遭遇的技術困難，使執法人員於搜索、扣押交易所錢包的過程中窒礙難行。

鑒於我國立法者的修法時程無法期待，現階段可先透過金管會對虛擬資產平台業者們軟性的行政指導，期以虛擬資產平台業者間的自我約束，經由自律組織訂定如為配合執法人員的執法行動，本平台可凍結涉嫌犯罪的交易所錢包，或者提供涉案者於平台登錄的個人資料以及交易紀錄等相關自律規範[208]。如此一來，不僅得避免洗錢防制法第 13 條第 1 項或虛擬通貨事業洗防辦法第 7 條規定之下，虛擬資產

[207] 婁天威、駱武昌、喬中玨（2014），〈金融海嘯後證券業自律組織發展趨勢之分析〉，《證券服務》，63 期，頁 34。

[208] 區塊客（09/07/2023），〈虛擬資產正式納管！台灣金管會：料 9 月前出台指導原則〉，https://blockcast.it/2023/03/30/fsc-confirms-to-take-control-of-virtual-currency/（最後瀏覽日：01/03/2024）。

doi:10.6342/NTU202400684

平台執行上遭遇的技術困難，亦可滿足執法人員實務上的執法需求，降低其執法成本。

而且透過虛擬資產平台及交易業務事業的自律規範，藉以補充及執行既有規範之細節，或配合政府機關的執法行動，在國際上亦非罕見。目前舉凡日本、英國、新加坡與瑞士等國，皆由各該國的虛擬資產平台業者為核心，組成虛擬資產產業的自律組織，包括如日本密碼資產交易業者協會（Japan Virtual and Crypto assets Exchange Association）、CryptoUK、新加坡加密貨幣企業與初創企業協會（Association of Crypto Currency Enterprises and Start-ups Singapore）以及英國金融服務標準協會（The Financial Services Standards Association）；其等成立的主要目的之一，便是制定得約束業界自律規範。而自律規範的內容除了入會資格、年度預算等行政庶務，重點便是在指導、監督會員遵循法規，在涉有不法情事時配合執法人員的偵辦行動。若有違反自律規範或政府法規的情況發生，將經由一定的調查與懲戒程序後，視涉案規模、不法所得等情節輕重，給予違反者警告、罰款、停權或除名等不利益處分[209]。

基於上述，藉由訂定虛擬資產平台及交易業務事業（VASP）公會自律規範，以建構執法人員搜索、扣押交易所錢包時，虛擬資產平台負有如凍結特定交易所錢包，或提供犯罪嫌疑人於交易所登錄的資料與交易紀錄等協力義務，本文認為係現階段較可行的作法。

至於自律規範中關於虛擬資產平台協力義務的具體內容，可參照我國數家較知名的虛擬資產平台與其使用者間訂定之定型化契約中，就配合執法人員的執法行動，

[209] 恆業法律事務所，前揭註 15，頁 187-196。

doi:10.6342/NTU202400684

虛擬資產平台負有相關協力義務之條款[210]。前揭條款中多有直接敘明，為協助、配合執法人員的執法行動，虛擬資產平台不僅得將使用者註冊時輸入的個人資料與相關交易紀錄提供予執法人員，亦得於使用者持有的錢包涉及洗錢、資助恐怖主義等不法情事時，禁止其就持有的交易所錢包進行出金、移轉比特幣等行為。除此之外，也可參考同受金管會監管，且由自律組織訂定關於協力義務自律規範的證券投資信託及顧問法第 88 條第 3 項、同法第 92 條。

第二款、我國虛擬資產平台業者訂定自律規則之發展與現況

既已肯認由我國虛擬資產平台業者組成自律組織，並訂定相關自律規範以建構虛擬資產平台協力義務之優勢與必要性，則近年來我國虛擬資產平台自律組織發展的狀況何如？

早於 2018 年 5 月，由金融科技協會發起的區塊鏈與加密代幣自律組織，便與數家虛擬資產平台、區塊鏈相關業者共同宣示推動業界自律，以期建立更具有公信力的平台與可持續性的區塊鏈生態系[211]。其後續更於同年 9 月公開簽署「交易所

[210] 對此，本文列舉其中三家虛擬資產平台為例，請參見如：BitoPro 數位貨幣交易平台使用條款第二章第 4 條：「本公司將依法協助、配合司法機關與行政執法等機關防範洗錢行為，亦依法協助相關機關查詢、並禁止用戶提款、轉帳、付款、交付、轉讓等行為。」、ACE Exchange 使用者條款第六節第 11 條：「當您的 ACE Exchange 帳戶於 ACE Exchange 提供服務之期間，涉及任何疑似違反本條款、禁止行為、涉嫌違反反詐欺、反洗錢和反恐怖主義規定等不法情事或消費糾紛，ACE Exchange 有權立即暫停、取消和／或終止您的 ACE Exchange 帳戶和／或禁止交易或凍結資金，而無須另行通知您和／或您的關聯人，並依檢警調單位、金融機構辦理警示帳戶聯防機制通報之文件，暫時凍結系爭交易款項，日後需依上述單位通知之文件，作為返還或支付系爭交易款項之依據；如發生上述疑似不法之行為，ACE Exchange 亦有權將您於 ACE Exchange 註冊時提交之個人資料與所進行的交易資料主動提交予檢警調單位。」、MAX Exchange 使用條款第 8.4 條：「關於您使用 MAX Exchange 服務和本網站、您與其他用戶和第三方的互動及您同意或代表的第三方的行為，不得涉及任何第 8.3 條和第 9.1 條所規定的任何行為或活動（以下合稱「禁止行為」）。MAX Exchange 有權隨時監控、審查、保留和揭露任何資訊，以滿足或主動配合相關法律、法規、制裁計畫、法律程序或政府要求。」

[211] 數位時代（05/22/2018），〈台灣區塊鏈產業自律聯盟成立，業者：盼政府低度監管〉，https://www.bnext.com.tw/article/49204/taiwan-blockchain-sro（最後瀏覽日：11/14/2023）。

doi:10.6342/NTU202400684

自律行為準則」之自律規範，聚焦守法、公開透明、善良管理、作業風險管理、市場、流動資產及信用風險管理這五個面向，望能開啟與我國政府溝通協商的大門[212]。惟可能因著虛擬資產產業在國內發展初期，虛擬資產平台業者仍在捉摸自律規範訂定的方向與力道，使前揭自律規範的內容相對空泛；且我國當時遲未決定虛擬資產產業的主管機關，虛擬資產平台業者未有可參考的政策方向以及與公部門間明確的溝通窗口，導致前揭自律組織的相關作為後續便不了了之[213]。

直至 2023 年 3 月，我國金管會奉行政院指定為擔任具金融投資或支付性質之虛擬資產平台的主管機關後，宣示將洽請虛擬資產平台及交易業務事業的業者推動業界自律。由虛擬資產平台及交易業務事業業者組織相關協會後，再依 VASP 指導原則訂定自律規範。期待由國內經營規模較大的業者帶動較小型的業者強化內部控制，循序漸進地強化虛擬資產平台對其客戶權益之保護[214]。

對此，我國虛擬資產平台業者們亦有採取相對應的具體行動。同年 9 月國內九家虛擬資產平台共同組織臺灣虛擬資產平台及交易業務事業公會籌備小組（Taiwan Virtual Asset Service Provider Preparatory Office），盼能在經濟部修正商業團體分業標準（增訂「虛擬通貨商業」團體業別及業務範圍）後，順利成立公會並訂定相關的自律規範[215]。

---

[212] BLOCKTEMPO（09/23/2018），〈提倡產業自律，台灣 15 家交易所業者共同簽署「交易所自律行為準則」，希望與政府良性溝通〉，https://www.blocktempo.com/sro-taiwan-15-exchange-sign-1/（最後瀏覽日：11/20/2023）。

[213] 中時新聞網（05/20/2021），〈陳冲呼籲政府對虛擬貨幣儘早擇定主管機關〉，https://www.chinatimes.com/realtimenews/20210520004186-260410?chdtv。（最後瀏覽日：01/03/2024）

[214] 金融監督管理委員會，金管會擔任具金融投資或支付性質之虛擬資產平台主管機關之推動規劃，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202303300001&toolsflag=Y&dtable=News（最後瀏覽日：11/14/2023）。

[215] 臺灣虛擬資產平台及交易業務事業公會籌備小組，〈臺灣三大交易所攜手籌備公會！整合加密貨幣產業鏈，積極與監管單位對話〉，https://www.twvasp-po.org.tw/tai-wan-xu-ni-zi-chan-ping-tai-ji-jiao-yi-ye-wu-shi-ye-gong-hui-chou-bei-xiao-zu-taiwan-virtual-asse/xin-wen-gao/2023-nian-9-

doi:10.6342/NTU202400684

自上述觀之，與其等待我國立法者增修相關法令，透過國內虛擬資產平台業者成立的公會訂定之自律規範，似是短期內建構虛擬資產平台協力義務較實際的解方。然國內有學者質疑，此方法在憲政體制上恐存在民主正當性的疑慮。緣我國之所以監管虛擬資產產業，不光是為了謀求上述業者的利益，尚需平衡兼顧消費者、投資人的權益[216]。申言之，今自律規範係由上述業者組成的自律組織自行訂定，可能因涉及切身的利害關係而故意通融放寬。如此一來不僅無法滿足主管機關的監管需求，對廣大消費者、投資人之保障亦屬不周。

惟本文認為，隨著 VASP 指導原則之頒布，在一定程度上可緩解前揭自律規範欠缺民主正當性之疑慮。緣 VASP 指導原則當中明定：「本事業應推動成立同業公會與訂定自律規範，並遵守本指導原則及自律規範[217]。」在虛擬資產平台須同時遵守 VASP 指導原則及自律規範的狀況下，可預見將來由虛擬資產平台自律組織訂定的自律規範，將貼合 VASP 指導原則指引的監管方向，使上述自律規範或多或少將帶有公權力色彩；乃至於在金管會的督導下，以自律規範的形式頒布若干指引。

就此推論，相較 2018 年時全然由虛擬資產平台業者訂定的自律規範，未來將訂定的自律規範形式上固為私法自治，但其內容將不可避免地滲入相關監管政策的意旨。考量我國金管會的權力係由民主選舉間接賦予，且制定對虛擬資產平台的監管政策時，亦經由正當程序蒐集各方意見與觀點，在一定程度上緩解自律規範欠缺民主正當性之擔憂。

---

yue-26-ri-xin-wen-gao（最後瀏覽日：11/19/2023）。

[216] 鏈新聞（10/14/2023），〈「加密專法」是為了保護業者或消費者？楊岳平教授解讀台灣監管之路〉，https://abmedia.io/prof-alex-yang-taiwan-crypto-law-draft（最後瀏覽日：11/19/2023）。

[217] 管理虛擬資產平台及交易業務事業（VASP）指導原則，頁 13。

doi:10.6342/NTU202400684

退步言之，縱無 VASP 指導原則等政策指引，虛擬資產平台業者們自行籌組公會後訂定的自律規範中，倘要求公會成員負有配合執法人員強制處分的協力義務，否則將課予懲戒等不利處分，亦無必要擔憂民主正當性或法律保留原則的問題。

緣按司法院釋字第 479 號解釋保障結社自由之意旨，具體言之，包括設立、加入、內部運作、退出、社團合併與解散等自由[218]。尤其，內部運作係指社團內部應設置何種組織單位、社團內部意見形成之程序以及如何推動社務；甚至在不違法的前提下，對於社員之紀律罰（懲戒罰），社團均享有自主權[219]。虛擬資產平台業者們籌組公會後，自行訂定的自律規範亦屬內部運作之一環。除非違反我國法對結社自由的若干限制，該自律規範課予公會成員協力義務否則將招致懲戒的內容，自屬結社自由保障的範疇，毋庸過於擔憂欠缺民主正當性，或與法律保留原則有違的問題[220]。

[218] 司法院釋字第 479 號解釋解釋文（節錄）:「憲法第十四條規定人民有結社自由，旨在保障人民為特定目的，以共同之意思組成團體並參與其活動之自由。」

[219] 法治斌、董保城，前揭註 163，頁 255-259。李惠宗，前揭註 95，頁 233-236。許育典，前揭註 95，頁 280-283。

[220] 我國現行法對結社自由的限制，包括如中華民國刑法第 154 條參與犯罪結社罪、工會法第 4 條第 2 項禁止現役軍人與國防部所屬及依法監督之軍火工業員工組織工會。

doi:10.6342/NTU202400684

第四章 搜索扣押比特幣之流程與建議：以私鑰控制權限者的角度切入

搜索、扣押屬我國法明文規範的強制處分，通常係執法人員為保全證據實施之行動[221]。按現行搜索、扣押電磁紀錄的執行流程，係執法人員進入特定處所，當場找尋儲存目標電磁紀錄的載體；在尋獲後排除受搜索人對該載體之持有，進而由執法人員占有之。再於搜索現場以外之處，由鑑識人員利用偵查機關的設備，透過電腦鑑識搜尋該載體內有無儲存目標電磁紀錄[222]。

比特幣固屬電磁紀錄之一環，似得依前揭搜索、扣押電磁紀錄的流程處理。然如前所述，就影響搜索、扣押比特幣的成敗關鍵，在於能否順利取得涉案的私鑰或助記詞而言，我國實務工作者亦有因著比特幣的技術特徵，發展出若干不同於一般搜索、扣押電磁紀錄的作法。惟鑒於這些涉及搜索、扣押比特幣的作法相對破碎，目前尚未形成具體的流程；且為使執法人員得於確定私鑰控制權限者後，預先準備並利用更精準的打擊手段取得私鑰。在我國實務工作者發展出的若干搜索、扣押比特幣作法之基礎上，本文嘗試從私鑰控制權限者的角度，分別形塑數個搜索、扣押比特幣時，在執行面可供執法人員參考的思路與流程。同時，針對執法人員在此些流程可能遭遇的執法困難提出建議。

在第一節，本文將先說明於現行刑事訴訟法的框架下，執法人員對電磁紀錄實施搜索、扣押時採行的「二階段搜索模式」係如何進行。接下來，著重討論對一般電磁紀錄以及對比特幣發動強制處分時，其各自側重之目的其實不盡相同。

---

221 林鈺雄，前揭註 90，頁 311；張麗卿，前揭註 95，頁 278。
222 李榮耕，前揭註 99，頁 1060-1061。

doi:10.6342/NTU202400684

在第二節，則先從私鑰控制權限者的角度，亦即比特幣錢包內的私鑰究係由使用者或虛擬資產平台業者管理，分別提出執法人員於搜索、扣押比特幣時，在執行面可參考的思路與具體流程。接下來，描述我國執法人員若按上述流程搜索、扣押比特幣時，在執行面上可能遭遇到的困難，包括如基層警員普遍對虛擬通貨的技術內涵不夠熟悉，欠缺合適的虛擬通貨流向分析工具等問題。對此，本文除了即時更新我國檢警機關近期提出的政策與具體作為，亦提出若干淺見供權責機關參考。

doi:10.6342/NTU202400684

第一節、搜索扣押電磁紀錄之流程與比特幣

電磁紀錄係無體物，其無法脫離載體而單獨存在。對電磁紀錄搜索、扣押的流程，我國實務發展出所謂的「二階段搜索模式」，以下析述之：

一般而言，執法人員進入應搜索的處所後，須先按第 145 條將搜索票示第 148 條在場之人，再開始找尋可能儲存電磁紀錄的載體[223]。若有尋獲，則應排除受搜索人對該載體的占有，將其移入公權力之支配。離開搜索現場前，執法人員除了應在現場制作扣押物品收據，將其付與所有人、持有人或保管人，亦應將執行結果與搜索、扣押筆錄，陳報核發搜索票之法院[224]。惟法院僅得將此陳報作為爾後是否核發搜索票的參考，無權予以撤銷該次執行結果[225]（第一階段）。

後續再於搜索現場以外之處，利用檢警機關的設備，依電腦鑑識（computer forensics）程序搜尋載體內有無所需之電磁紀錄（第二階段）[226]。在執法人員發動二階段搜索模式之前，通常會依所屬人員具備的技能或專長，分配其等不同的任務[227]。同時，備妥多重開機片、檔案管理軟體與側錄軟體等工具，以利現場偵查作業之進行[228]。

---

[223] 刑事訴訟法第 145 條：「法官、檢察官、檢察事務官、司法警察官或司法警察執行搜索及扣押，除依法得不用搜索票或扣押裁定之情形外，應以搜索票或扣押裁定示第一百四十八條在場之人。」刑事訴訟法第 148 條：「在有人住居或看守之住宅或其他處所內行搜索或扣押者，應命住居人、看守人或可為其代表之人在場；如無此等人在場時，得命鄰居之人或就近自治團體之職員在場。」

[224] 刑事訴訟法第 132 條之 1：「檢察官或司法警察官於聲請核發之搜索票執行後，應將執行結果陳報核發搜索票之法院，如未能執行者，應敘明其事由。」刑事訴訟法第 139 條第 1 項：「扣押，應制作收據，詳記扣押物之名目，付與所有人、持有人或保管人。」

[225] 林鈺雄，前揭註 90，頁 192。

[226] 李榮耕，前揭註 99，頁 1060-1061。電腦鑑識（computer forensics）亦可稱為「數位鑑識」（digital forensics）。

[227] 內政部警政署（2019），《警察偵查犯罪手冊》，頁 74。

[228] 王旭正、柯永瀚、ICCL 資訊密碼暨建構實驗室（2007），《電腦鑑識與數位證據—資安技術、科技犯罪的預防、鑑定與重建現場》，頁 117-122，新北：博碩文化。

doi:10.6342/NTU202400684

其中所謂的「電腦鑑識」，最初於 1991 年的國際電腦調查專家協會（International Association of Computer Investigation Specialists）被提出，係針對電子設備上的數位資訊，以經驗證的科學方法對數位資訊進行保存、擷取、驗證、識別、分析、解讀、紀錄與呈現，藉以還原事件全貌、協助重建整個犯罪過程[229]。具體而言，扣押電腦、行動裝置等載體時應符合比例原則，並須謹慎拆裝搬運，以免因扣押物受損、而影響其證據能力[230]。

鑑識人員取得被扣押的載體後，便開始採集、記錄的工作[231]：通常先以位元流（bitstream）的方式，將扣押載體的第一個位元一直複製至最後一個位元，最終製作出一個映像檔（mirror image）[232]。鑑識人員會在映像檔上搜尋所需的檔案，接續進行分類、比較、辨識個體與現場重建等工作，而非直接在扣得的載體上作業[233]。

比特幣係屬電磁紀錄之一環，故我國偵查實務目前依前揭搜索、扣押電磁紀錄的流程處理。以一件近期警方搜索虛擬通貨交易所的實際案件為例，根據相關報導，執法人員係進入特定處所搜索，並當場拘束受搜索人的人身自由後，扣押受搜索人使用的硬體錢包。接下來，再將這些被扣押的硬體錢包攜回檢警機關，依電腦鑑識程序搜尋硬體錢包管理的私鑰[234]。

---

229 陳詰昌（2016），〈數位鑑識「原件不可變動原則」之適用－由行動裝置鑑識與電腦鑑識差異探討〉，《司法新聲》，119 期，頁 44。

230 內政部警政署，前揭註 227，頁 75。

231 林宜隆（2012），〈建構數位證據鑑識標準作業程序（DEFSOP）與案例實證之研究〉，《司法新聲》，101 期，頁 52。

232 李榮耕，前揭註 99，頁 1060。

233 王旭正、柯永瀚、ICCL 資訊密碼暨建構實驗室，前揭註 228，頁 41。

234 本件的相關報導，請參見：鏡週刊（06/08/2022），〈虛擬貨幣交易所遭搜索 負責人轟警不專業〉，https://www.mirrormedia.mg/story/20220608soc006/（最後瀏覽日：10/11/2023）。

doi:10.6342/NTU202400684

惟本文認為，上述作法忽略對一般電磁紀錄與比特幣發動強制處分側重之目的其實不盡相同。蓋執法人員扣押載體，並透過電腦鑑識搜尋如文件檔、圖片檔等一般電磁紀錄，其主要目的通常係將這些電磁紀錄作為數位證據如實呈現在法庭，以供法院於審判程序中還原、釐清並認定犯罪事實[235]。若在搜索現場扣押所有涉案的載體後，被扣押人或第三人仍持有與這些電磁紀錄一模一樣的檔案，除非於審判時發生數位證據原件與複製品是否同一的爭執，否則不影響所涉案件的進行[236]。

相對地，執法人員藉由搜索比特幣位址、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的載體之方式，達成扣押比特幣之任務，更偏重保全將來沒收之執行，以澈底剝奪受搜索人的不法利得。若執法人員搜索前揭客體時，係採取二階段搜索模式，只要被搜索人或第三人在執法人員扣押比特幣前，利用其所有且同樣得移轉目標比特幣的私鑰或助記詞，透過公有鏈上其他節點驗證這些比特幣轉入其他比特幣位址的交易，再向整個比特幣網路發布消息[237]。如此一來，縱執法人員後續利用電腦鑑識尋獲相同的私鑰，此次為扣押目標比特幣發動的強制處分仍是徒勞無功。

綜上所述，執法人員若逕以二階段搜索模式的流程與思惟，執行扣押比特幣之任務，恐需承擔更大的失敗風險。而就搜索、扣押比特幣之流程，觀察我國刑事訴訟法、通訊保障及監察法等現行的刑事程序法規，皆無對此為明文規範[238]。本文將在下一節，嘗試從私鑰控制權限者的角度，提出若干執行面上的建議與思惟，以供

---

[235] 王旭正、柯永瀚、ICCL 資訊密碼暨建構實驗室，前揭註 228，頁 38-39；陳詰昌，前揭註 229，頁 45。

[236] 關於數位證據原件與複製品是否同一的細緻論述，請參見：蘇凱平（2022），〈論數位證據之原件、複製品與最佳證據法則——最高法院 107 年度台上字第 3724 號等 8 則刑事判決評析〉，氏著，《數位科技與證據法則》，頁 17-56，臺北：元照。

[237] 黃柏翔，前揭註 19，頁 33。

[238] 法務部調查局宣稱：其下轄單位已於 2019 年 4 月下旬，正式發表國內首套的「搜扣虛擬通貨比特幣的 SOP 標準作業規範」。惟根據寫作期間屢次搜尋的結果，均未見前揭規範的具體內容或進一步說明。請參見：法務部調查局（07/25/2019），〈虛擬通貨易淪為吸金詐騙工具，調查局邀集學者專家及主管機關代表探討成因協力防制犯罪，並呼籲民眾應審慎投資〉，https://www.mjib.gov.tw/news/Details/1/487（最後瀏覽日：04/08/2023）。

doi:10.6342/NTU202400684

執法人員與其所屬人員參考。

第二節、搜索扣押比特幣之流程

比特幣在本質上固屬電磁紀錄，然執法人員若逕以搜索、扣押一般電磁紀錄的流程與思惟，執行扣押比特幣之任務，恐需承擔更大的失敗風險。因此，本節以下將進入研究問題的另一重心：就比特幣之搜索、扣押，其相應的執行流程與思惟為何。

之所以選擇從私鑰控制權限者的角度，分別提出搜索、扣押比特幣時不同的流程，係因執法人員得於確定移轉目標比特幣所需的私鑰控制權限，係使用者或虛擬資產平台後，預先準備並利用更精準的打擊手段取得私鑰。以下將執法人員搜索、扣押比特幣的流程軸，切分成事前準備、事中進行兩階段為論述；並針對由使用者或虛擬資產平台業者管理私鑰的比特幣錢包，分別闡述得如何因應其特性為搜索、扣押行動。

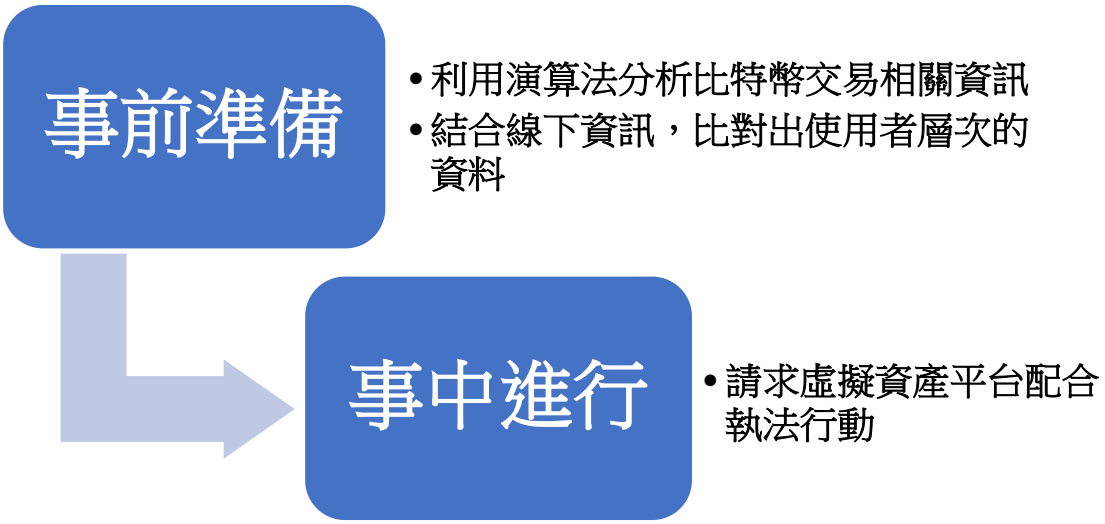
以私鑰控制權限者的判準區分比特幣錢包類型，其概念係源自 FATF 就託管錢包與非託管錢包之分類，亦即以使用者下載至手機或電腦端使用的錢包程式中，私鑰由使用者或虛擬資產平台業者管理區分之[239]。

[239] *See* FATF, *supra* note 185, at 39.

doi:10.6342/NTU202400684

由使用者管理私鑰的錢包類型，包括熱錢包當中的軟體錢包以及冷錢包；由虛擬資產平台業者管理私鑰的錢包類型，則僅有熱錢包中的交易所錢包[240]。另在搜索、扣押比特幣的過程中，可透過特定演算法運算轉換成私鑰的助記詞，亦為移轉目標比特幣之關鍵；但因可儲存其的態樣與私鑰相同，亦即得透過冷錢包或熱錢包儲存，並無另行論述的必要性，故本節以下不就助記詞分析之，併予敘明。

第一項、由虛擬資產平台管理私鑰的錢包類型



圖一、搜索扣押比特幣之流程：由虛擬資產平台管理私鑰的錢包類型
※資料來源：本圖為作者自製

第一款、事前準備：利用演算法分析比特幣交易相關資訊

比特幣作為分散式帳本技術的應用之一，每當利用錢包交易、移轉比特幣時，公有鏈上的其他節點便需驗證付款方、收款方兩者比特幣位址提供的資訊，可稱之

[240] 關於冷錢包、熱錢包、軟體錢包、交易所錢包的意義，請參見本文前述「第二章、第一節、第五項」的說明。

doi:10.6342/NTU202400684

為「鏈上交易」（on-chain transactions）[241]。這些資訊包括鎖定腳本（scriptPubkey）、解鎖腳本（scriptSig），藉以確認此筆交易的語法與數據結構是否正確[242]。

此類匿名的比特幣位址相互移轉、交易比特幣之資訊於比特幣網路公開，且原則上無法被單一實體任意竄改，而可在區塊鏈上的全球帳本檢視[243]。執法人員有機會利用如 Chainalysis、TRM Lab、CipherTrace 或坤侑科技等公司開發的虛擬通貨數據分析平台或偵測軟體（請參見圖一），在設定範圍內的交易紀錄檔案，交叉比對這些交易紀錄，並且標註比特幣位址與不同的使用者，使虛擬通貨的金流圖形化[244]。如此一來，便得過濾與清查涉案的各層比特幣位址，鎖定哪些交易係由嫌疑人的比特幣位址進行。

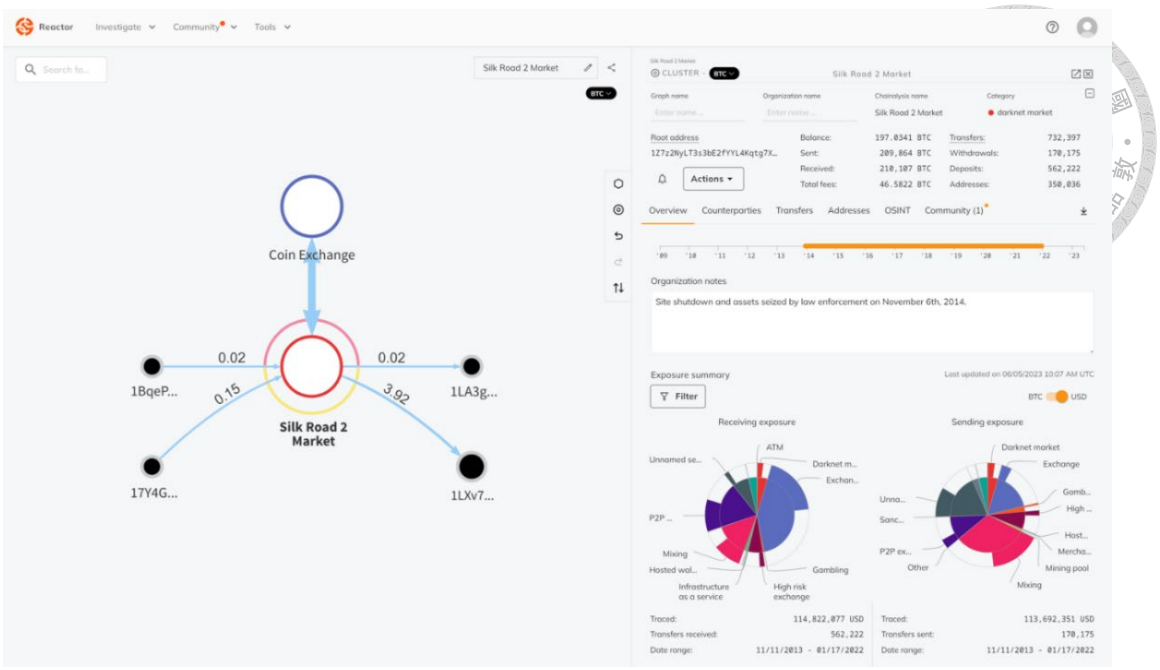
[241] 王毅丞，前揭註 72，頁 39-40。

[242] 扼要地說，「鎖定腳本」係由付款方設置的交易權限，用以控制當筆款項的輸出對象為何者；「解鎖腳本」係由收款方設置的交易權限，用以證明己方為當筆款項的合法接收者；關於二者的詳細介紹請參見：魯特，前揭註 57，頁 175-180；Joseph Bonneau et al., *supra* note 43, at 105-106.

[243] 黃柏翔，前揭註 19，頁 29；法務部調查局，前揭註 86，頁 95。

[244] 羅韋淵，前揭註 15，頁 35；施志鴻，前揭註 19，頁 75；洪敏超，前揭註 105，頁 14；Ron & Shamir, *supra* note 19, at 10-20；三立新聞網（02/07/2024），〈執法新利器「虛擬貨幣數據分析平台」 防範虛擬貨幣洗錢及詐欺犯罪〉，https://www.setn.com/News.aspx?NewsID=1424314&fbclid=IwAR3t38SaucW4uT1Vgyr-cYM25Z5pw2_vF47d29aAJXcKSC1kR-c7kPGHj57M（最後瀏覽日：02/07/2024）。

doi:10.6342/NTU202400684



圖二、Chainalysis 公司開發的虛擬通貨交易偵測軟體「Chainalysis Reactor」
※資料來源：本圖為作者截取自 Chainalysis 公司的官方網站：
https://www.chainalysis.com/chainalysis-reactor/

第二款、事前準備：結合線下資訊，比對出使用者層次的資料

初步匡列嫌疑人可能持有的比特幣位址與其相關的交易紀錄後，為了提升偵查行動的精準度，執法人員應結合線下偵蒐時獲得的資訊，包括嫌疑人的住所地、其金融機構帳戶與信用卡的交易細節等資料，以及其他可得的公開情報綜合分析、建構出嫌疑人的交易內容以及特徵，盡可能拼湊出所有犯罪金流的動向，將各比特幣位址連結至現實生活中的使用者身分[245]。譬如嫌疑人持有的比特幣位址若在一段期間內，收到多筆來自不同比特幣位址的小額款項後，再將約當價值款項以多筆小額的方式，迅速轉出至多個不同的比特幣位址時，則可合理懷疑嫌疑人係透過比特幣金流從事洗錢活動，得藉此追蹤其他經手的比特幣位址是否為嫌疑人的黨羽或白手套所持有。

[245] 羅韋淵，前揭註 15，頁 24；Reid & Harrigan, *supra* note 19, at 15-17.

doi:10.6342/NTU202400684

值得注意的是，在機器學習技術的基礎之上，有論者認為政府部門可進一步建立具有預測功能的運算架構[246]。自動蒐集、偵測比特幣網路上的交易資訊與其外部的相關資料後，執法人員再結合線下偵辦時取得的情資，綜合比對出若干可疑的比特幣交易[247]。

第三款、事中進行：請求虛擬資產平台配合執法行動

結合線上分析取得嫌疑人可能持有的比特幣位址與交易紀錄，以及線下由執法人員偵蒐時獲得的相關資訊後，執法人員應可掌握較精準的涉案比特幣位址清單。據此，執法人員得再向各該比特幣位址所在的虛擬資產平台，請求配合搜索、扣押交易所錢包等執法行動[248]。諸如提供犯罪嫌疑人與其黨羽於交易所註冊登錄的資料、歷年交易紀錄等資訊，或者凍結其等持有的交易所錢包，包括禁止出金與比特幣轉出、轉入等功能，近似我國法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將特定存款帳戶列為警示的作法[249]。

如此一來，檢警機關便毋庸再派遣人力至搜索現場，執法人員可在遠端透過網際網路直接扣押涉案的交易所錢包，將其持有的比特幣移轉至專供檢警機關搜索、扣押比特幣的比特幣位址。

---

246 Irwin & Turner, *supra* note 19, at 297.

247 施志鴻，前揭註 19，頁 76。

248 具體個案如幣安（BINANCE）交易所建置的「政府執法機構資訊查詢協助系統」，執法人員可通過本系統提交資訊查詢申請，於幣安交易所核對相關資訊後，就個案情況配合提交的資訊查詢要求。請參見如：BINANCE，https://www.binance.com/zh-TC/support/law-enforcement（最後瀏覽日：11/18/2023）。

249 所謂「出金」，原為期貨交易上的專業詞彙，在虛擬通貨領域則常係指使用者將其交易所錢包內存放的虛擬通貨，按市價或約定價格轉換為現實世界中等值的金額。

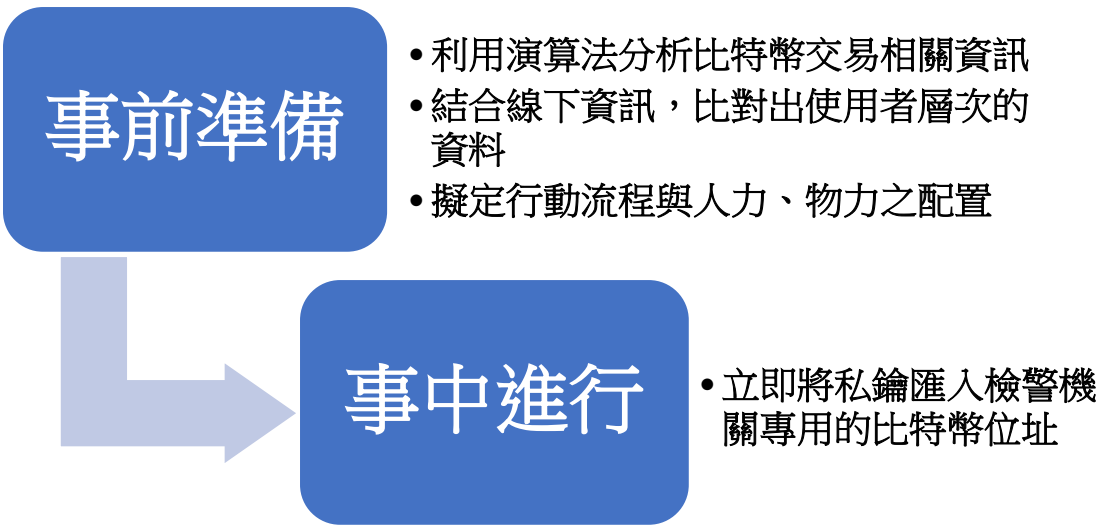
doi:10.6342/NTU202400684

第四款、附論：鏈下交易

倘嫌疑人與其往來對象係利用在同一虛擬資產平台業者註冊的交易所錢包交易、移轉比特幣，此時是由虛擬資產平台業者負責驗證付款方、收款方兩者的資訊，而不是公有鏈上的其他節點[250]。這種實質上係由單一中心化業者控制，非在區塊鏈上進行的「鏈下交易」（off-chain transactions），其相關的交易紀錄以及資訊便無法在區塊鏈的全球帳本上檢視。

面對鏈下交易的情形，執法人員較難直接透過前述利用演算法分析比特幣交易紀錄與資訊的方法，鎖定嫌疑人的比特幣位址，此時可多藉由蒐集、分析線下資訊，比對出使用者層次的資料後，再向各該比特幣位址所在的虛擬資產平台，請求配合搜索、扣押交易所錢包等執法行動。

第二項、由使用者管理私鑰的錢包類型



[250] 黃柏翔，前揭註 19，頁 30。

doi:10.6342/NTU202400684

圖三、搜索扣押比特幣之流程：由使用者管理私鑰的錢包類型
※資料來源：本圖為作者自製

第一款、事前準備：擬定行動流程與人力、物力之配置

就此類型的錢包而言，在發動強制處分前，執法人員除了可按前項提供的偵查技巧，利用演算法分析比特幣交易相關資訊後，結合線下資訊，比對出使用者層次的資料。同時，亦盡可能先確認「移轉目標比特幣所必要的私鑰或助記詞」係儲存於受搜索人持有的何種載體中，其類型包括硬體錢包、各品牌廠製作的冷錢包。

接下來，視此次搜索任務的難易度、出勤人員的數量，擬定行動流程與人力、物力之配置，尤其備妥專供搜索、扣押比特幣使用的數個硬體錢包，並且確保其中儲存檢警機關專用的比特幣位址已完成初始化作業，以便在執法人員搜獲涉案錢包的當下，可對目標比特幣為立即無遲延之移轉[251]。另外，目前在我國偵查實務上，執法人員尚有利用可嗅聞化學塗料的電子產品偵測犬，作為搜尋電子載體的方法之一[252]。

惟當處在如刑事訴訟法第 131 條第 2 項、第 133 條之 2 第 3 項提及有相當理由發動搜索或扣押的急迫情況時，要求執法人員隨身攜帶前揭硬體錢包、乃至返回任職單位領取後再行動，皆顯得不切實際[253]。此際，執法人員可以利用手邊可能攜帶的行動裝置、筆電，即時在現場建立專供扣押使用的比特幣錢包。

---

[251] 法務部調查局，前揭註 19，頁 68。

[252] 三立新聞網，〈台灣第一隻電子產品偵測犬從美國返台　「虛擬貨幣冷錢包」也能找到〉，https://www.setn.com/News.aspx?NewsID=1346792&from=y（最後瀏覽日：10/15/2023）。

[253] 刑事訴訟法第 131 條第 2 項：「檢察官於偵查中確有相當理由認為情況急迫，非迅速搜索，二十四小時內證據有偽造、變造、湮滅或隱匿之虞者，得逕行搜索，或指揮檢察事務官、司法警察官或司法警察執行搜索，並層報檢察長。」同法第 133 條之 2 第 3 項：「檢察官、檢察事務官、司法警察官或司法警察於偵查中有相當理由認為情況急迫，有立即扣押之必要時，得逕行扣押；檢察官亦得指揮檢察事務官、司法警察官或司法警察執行。」

doi:10.6342/NTU202400684

第二款、事中進行：立即將私鑰匯入檢警機關專用的比特幣位址

為避免執法人員扣押冷錢包或軟體錢包後，受搜索人或第三人仍以其他形式持有目標比特幣的私鑰或助記詞，並利用其將比特幣轉入其他比特幣位址。凡於搜索現場尋獲一個或多個由受搜索人持有，且可能儲存私鑰的電子載體，在利用各種方法突破這些載體內設計的加密技術後，執法人員便可「立即」將移轉目標比特幣所需的私鑰，匯入檢警機關專用的比特幣位址；其移轉全程宜使用攝影器材錄影[254]。而相應的規範安排，則可透過刑事訴訟法第 128 條第 3 項後段或法院辦理刑事訴訟案件應行注意事項 64 點的規定，由核發本件搜索票的法官將前揭指示記載於其核發的搜索票上，藉以避免執法人員遲誤取得私鑰的時機，以致發動當次強制處分的目的落空[255]。

執法人員在搜索現場若僅是複製並另存這些私鑰，恐使受搜索人或其同夥仍以其他形式持有目標比特幣的私鑰或助記詞，並搶在執法人員移轉前，將目標比特幣移至其他比特幣位址[256]。

此處之所以將關注重點放在如何取得私鑰或助記詞，係因支撐比特幣網路運作的公開金鑰加密技術中，私鑰具備的功能便是控制在區塊鏈上特定區塊儲存的資訊，

---

[254] 法務部調查局，前揭註 19，頁 68、73；黃柏翔，前揭註 19，頁 33。若執法人員於現場尋獲的是儲存私鑰之紙錢包，此時操作的動作並無不同。

[255] 刑事訴訟法第 128 條第 3 項：「搜索票，由法官簽名。法官並得於搜索票上，對執行人員為適當之指示。」法院辦理刑事訴訟案件應行注意事項 64 點：「搜索票務須填載刑訴法第一二八條第二項各款法定必要記載之事項，不得遺漏，尤其第四款『有效期間』，應審酌聲請人之請求及實際需要，慎重決定。為確保人權不受公權力過度侵害，法官得視個案具體狀況，於搜索票上對執行人員為適當之指示，例如指示應會同相關人員或採隱密方式等。對於偵查中聲請核發搜索票之程序，包括受理、訊問、補正、審核、分案、執行後陳報、事後審查、撤銷、抗告、抗告法院裁定等程序，各相關人員於本案起訴前均應依法保守秘密，不得公開。」

[256] 法務部調查局，前揭註 19，頁 69。

doi:10.6342/NTU202400684

私鑰的持有者得依其意志將這些資訊新增或移除[257]。由此觀之，執法人員取得嫌疑人冷錢包或軟體錢包內儲存的私鑰或助記詞，其主要目的實非占有這些私鑰或助記詞，而係利用這些私鑰或助記詞移轉目標比特幣至檢警機關專用的比特幣位址。待此動作完成後，即便嫌疑人持有的硬體錢包或軟體錢包內仍儲存這些私鑰，乃至第三人持有的比特幣錢包內儲存同樣得移轉目標比特幣的私鑰或助記詞，而未由執法人員壟斷這些私鑰的占有，亦不影響本次強制處分發動之目的。

待公有鏈上的多數節點驗證此筆交易完成，執法人員便可確認其錢包內的交易紀錄與餘額是否已同步化。此時，公有鏈儲存的交易資訊已經由共識驗證，原則上不會被任何中心化的實體更改[258]。接下來，執法人員將扣得錢包內所有比特幣位址記載的交易紀錄一併匯出，以列有「日期、數額、標籤與交易識別碼」形式的檔案呈現，作為執法人員後續分析犯罪金流的材料[259]。

離開搜索現場之前，執法人員將其扣得的私鑰、助記詞、相關交易紀錄及移轉的比特幣額度，詳細記載於「扣押物品目錄表」後，再將此表付與被扣押人[260]。警察機關在移送扣得的比特幣額度予地方檢察署時，僅將其錢包內比特幣位址的私鑰或助記詞，移轉至後者專用的比特幣位址即可。

第三項、其他注意事項與對上述流程之質疑

上述段落係本文認為搜索、扣押涉及錢包的比特幣刑案時，可供執法人員利用

[257] 黃柏翔，前揭註 19，頁 34。另請參見本章前述「第一節、第二項、第二款、公開金鑰加密技術」的說明。
[258] 極少數例外遭公有鏈上單一實體修改或逆轉交易過程的情形，請參見前揭註 64 的說明。
[259] 法務部調查局，前揭註 19，頁 70。
[260] 刑事訴訟法第 139 條第 1 項：「扣押，應制作收據，詳記扣押物之名目，付與所有人、持有人或保管人。」

doi:10.6342/NTU202400684

的流程與思惟，但仍宜視個案情形調整執行細節。倘若基於種種原因無法在搜索現場完成移轉比特幣的扣押工作時，執法人員或可考慮改採二階段搜索模式。

值得特別注意的是，執法人員順利搜索、扣押比特幣後，其使用的硬體錢包有必要妥善地保管、收藏，避免因溫度、濕度、磁場、靜電、油汙或灰塵等環境背景因素，變動、毀損硬體錢包內儲存的電磁紀錄[261]。而執法人員若未能於現場順利移轉目標比特幣，而由鑑識人員對電子載體為鑑識程序時，視其技術特性之不同（例如：電腦、行動裝置），謹慎操作破解密碼鎖、取證軟體內容以及製作映像檔等動作[262]。如此一來，這些被扣押的電磁紀錄方得在被證明為證據相同、情況相同的狀況下，成為刑事審判程序中的證據；亦即，證明這些被扣押的電磁紀錄其保管鏈（chain of custody）並未斷裂。

或有實務工作者對前揭方法提出質疑：要求執法人員攜帶硬體錢包實施對比特幣之搜索、扣押，不僅在執行過程中徒增管理硬體錢包的成本，採購與維護數量龐大的硬體錢包亦是所費不貲。其認為改採「一案一錢包」的方案，即於搜索現場只需要求受搜索人將持有錢包內涉案的比特幣，移轉至檢警機關專用的比特幣位址，便毋庸承擔前揭方法在運作上較高的執法成本[263]。

前段質疑固非無據，但本文認為，一來採購、管理硬體錢包的成本非不能忍受，且可透過檢警機關內部的教育訓練與偵辦經驗分享，盡可能降低硬體錢包遺失或毀損的風險；二來觀察所謂「一案一錢包」方案，執法人員僅透過要求受搜索人移轉

[261] 法思齊（2011），〈美國法上數位證據之取得與保存〉，《東吳法律學報》，22 卷 3 期，頁 138-140；李承龍、蔡佩芬（2023），〈數位取證與區塊鏈保存物證之探討〉，《萬國法律》，249 期，頁 5。在我國實務上，甚至還出現調查局人員於搜索現場誘導被告竄改比特幣交易紀錄的情形，請參見：臺北地方法院 107 年度訴字第 272 號刑事判決。

[262] 就此部分更進一步的說明，請參見：陳詰昌，前揭註 229，頁 49-52。

[263] 法務部調查局，前揭註 19，頁 76。

doi:10.6342/NTU202400684

涉案的比特幣，便可達成其發動此次強制處分之目的，卻未見受搜索人為何願意配合執法人員行動的說明，無疑是過於樂觀的解決方案。

第四項、搜索扣押比特幣可能遭遇的困難與建議

追緝涉及比特幣的刑案時，執法人員能否順利完成搜索、扣押比特幣的任務，將受搜索人持有的比特幣移轉由執法人員支配，往往關係到這些刑案能否被偵破。有鑑於此，前文已提出若干執行面上搜索、扣押比特幣的具體作法與思路。惟前揭作法在我國現行法上多無明文規定，未來若欲落實於偵查實務，現況可能存在一些執行面上的困難或配套措施欠缺之處，因此在本項詳加闡述與回應。

如前文所述，哈希值、區塊鏈等諸多與虛擬通貨相關的概念，本身即具備一定的技術門檻。尤其於搜索、扣押比特幣的過程中，無論目標係儲存於熱錢包或冷錢包的私鑰或助記詞，第一線的執法人員對比特幣錢包、比特幣位址等工具如何操作，皆有必要存在一定程度的認識，方有能力理解搜索票上的指示，以完成當次搜扣任務。

然而，面對此類偵辦技術難度較高的刑案，不僅我國執法人員在其培育階段大多無學習比特幣或虛擬通貨領域的知識，故普遍對此感到陌生，目前基層執法單位亦幾乎未備妥搜索、扣押虛擬通貨所需的科技工具[264]。以兩件近年警方搜索搜索、扣押比特幣的實際案件為例：其中一件，根據相關報導，執法人員雖持有該管法院核發的搜索票，但因著對虛擬通貨技術的不熟悉，在現場需先詢問受

[264] 時任臺北市警察局刑警大隊科技偵查隊鄭國隆隊長的發言，收錄於：中華警政研究學會（2023），〈第 54 場警政與警察法相關圓桌論壇論壇紀錄〉，頁 10；天下雜誌（10/05/2023），〈加密幣不再是完美犯罪天堂　熱血警察自費 15 萬，追到詐騙金流〉，https://www.cw.com.tw/article/5127639?fbclid=IwAR11TGS_KnbkQ0bMjuL-FqzCgC1fECJbhjG-a8sB731yd-ssvtuGed8mxPI（最後瀏覽日：02/07/2024）。

doi:10.6342/NTU202400684

搜索人後，方能決定扣押的範圍為何，且未依法給予被搜索人扣押物品清單[265]。另一件，根據相關報導，執法人員在受搜索人住處欲扣押價值逾新臺幣一億元的虛擬通貨時，其事先準備供作扣押虛擬通貨的冷錢包，竟未支援某常見幣種的規格，導致執法人員需緊急調派人力購買合乎規格的冷錢包後，方順利完成此次強制處分[266]。

如此推論，前述提出搜索、扣押比特幣的執行建議，在理論面縱能成功運作，但於實際實施時，因著前揭困境而可能只收得事倍功半之效。而就執法人員對搜索、扣押比特幣的認識與準備普遍不足之困境，我國檢警機關與實務工作者已有所察覺，並在這幾年積極提出若干對策，本文整理成五點如下[267]：

其一，透過交流、分享偵處涉及虛擬通貨的刑案之相關經驗，持續開設對基層執法人員的教育訓練與培訓課程，並期待可將若干執行重點與偵辦策略統整成一本教戰手冊。

其二，將添購的幣流分析工具 Chainalysis Reactor、TRM Forensics，陸續導入臺灣高等檢察署、刑事警察局等機關，以便執法人員在偵辦涉及虛擬通貨的刑案時，可迅速調閱特定比特幣位址的上下游交易紀錄，明瞭犯罪金流的分布網路與流向，鎖定金流受益人之身分。

---

[265] 本件的相關事實，請參見：鏡週刊（06/08/2022），〈虛擬貨幣交易所遭搜索 負責人轟警不專業〉，https://www.mirrormedia.mg/story/20220608soc006/（最後瀏覽日：02/17/2023）。

[266] 本件的相關事實，請參見：聯合報（01/19/2024），〈辦案工具兩光贓款無處放 打詐國家隊如何「精進」作為？〉，https://vip.udn.com/vip/story/122366/7720380（最後瀏覽日：01/25/2024）。

[267] 羅韋淵，前揭註 15，頁 40-41；施志鴻，前揭註 19，頁 75；時任臺北市警察局刑警大隊科技偵查隊鄭國隆隊長的發言，收錄於：中華警政研究學會，前揭註 264，頁 10；黃立維，〈檢察機關科技偵查運用實務現況介紹〉，《檢察新論》，32 期，頁 47-50。

doi:10.6342/NTU202400684

其三，可參考美國司法部或日本最高檢察廳的經驗，成立一批由資工領域專家、具備資訊科技或電腦專長的檢察官組合而成的專業團隊，處理涉案金額達一定程度以上或犯罪情節嚴重的虛擬通貨刑案。

其四，鑒於組成比特幣位址、私鑰的字串甚長而不易記憶，執法人員偶爾於登記時發生誤寫或漏寫的情形，建議可透過 QR Code 的方式呈現，並設定一定的防錯機制。

其五，刑事警察局未來亦有計畫建立「國家級司法查扣專用電子錢包」、「黑名單錢包追蹤資料庫」等數位工具，藉以優化執法人員偵辦涉及虛擬通貨的刑案之品質[268]。

前述由我國檢警機關提出的相關對策，本文對其政策方向與態度敬表贊同，亦觀察到其正逐步落實當中，並無淪為口號，包括如邀請虛擬通貨領域的專家至科技偵查教育訓練班授課[269]；訂定「受理涉及虛擬貨幣詐騙案件登錄『警察電信金融聯防平臺（165 反詐騙系統平臺）』作業程序」，以利偵辦人員驗證比特幣錢包位址與交易資訊[270]；成立加密貨幣金流分析小組，其成員係取得原廠認證分析證照的電子組檢察事務官[271]。

[268] 鏡週刊（02/14/2021），〈【隨身碟值 600 萬 3】防犯罪溫床 台警建黑名單錢包追蹤資料庫〉，https://www.mirrormedia.mg/story/20210208soc030/（最後瀏覽日：05/15/2023）。根據此篇報導，所謂「國家級司法查扣專用電子錢包」，係執法人員於搜索現場執行搜索時，可即時將虛擬通貨轉入此錢包，藉以確保犯罪事證扣押之完成；所謂「黑名單錢包追蹤資料庫」，則係將特定錢包設定交易監控，以便在其發生異常交易時即時通知負責的執法人員。

[269] 請參見如：中央社（06/28/2023），〈新北警強化科偵能力 邀請虛擬貨幣調查專家蔡孟凌授課〉，https://www.cna.com.tw/postwrite/chi/345015（最後瀏覽日：10/18/2023）。

[270] 時任內政部警政署刑事警察局預防科林書立科長的發言，收錄於：中華警政研究學會，前揭註 264，頁 9。

[271] 黃立維，前揭註 267，頁 48。

doi:10.6342/NTU202400684

惟關於搜索、扣押比特幣的具體執行，我國檢警機關迄今仍未因著此類型案件的技術特性，訂定一套相對完整的通用偵辦指引或標準作業流程。對此，本文建議我國檢警機關在既有對策的基礎上，儘速蒐集相關偵查經驗、國內外專家學者們的意見，訂定前揭指引或作業流程，並建立可與國內、外主要虛擬資產平台聯繫、合作的窗口（請參見表二）[272]。其必要性除了在於為處理數量日益增加且技術難度更高的虛擬通貨刑案，亦恐執法人員忌憚若逕自使用新型態的偵查方法，往往被迫承受較大的違法風險，因此次行動而背負刑事處罰[273]。

表二、本文對我國實務既有對策的建議

※資料來源：作者自製

我國實務現行對策	本文建議
交流、分享偵處涉及虛擬通貨的刑案之相關經驗，持續開設對基層執法人員的教育訓練與培訓課程。	在持續精進對虛擬通貨的偵查技術之基礎上，本文認為，為便利基層執法人員得按圖索驥學習，亦使其於偵辦時得溝通進程，檢警機關實應儘速蒐集相關偵查經驗、國內外專家學者們的意見，訂定一套相對完整的通用偵辦指引或標準作業流程。
將幣流分析工具 Chainalysis Reactor、TRM Forensics 導入臺灣高等檢察署、刑事警察局等機關。	
透過 QR Code 的方式呈現私鑰或者助記詞，並設定一定的防錯機制。	

[272] 時任內政部警政署刑事警察局科技研發科莊明雄代理科長的發言，收錄於：中華警政研究學會，前揭註 264，頁 5。

[273] 李榮耕（2020），〈初探遠端電腦搜索〉，氏著，《數位時代中的搜索扣押》，頁 336，臺北：元照。

doi:10.6342/NTU202400684

成立一批由資工領域專家、具備資訊科技或電腦專長的檢察官組合而成的專業團隊，處理涉案金額達一定程度以上或犯罪情節嚴重的虛擬通貨刑案。	檢警機關組建專門處理重大虛擬通貨刑案的團隊與科技工具時，亦可建立得與國內、外主要虛擬資產平台聯繫、合作的窗口，更有利於即時監測不法金流的動向。
計畫建立「國家級司法查扣專用電子錢包」、「黑名單錢包追蹤資料庫」等數位工具。	

doi:10.6342/NTU202400684

第五章 結論

面對不法分子利用比特幣從事犯罪的情況，執法人員對比特幣實施搜索、扣押時，在規範面上，如何妥善適用我國現行刑事訴訟法之規範；在執行面上，相應的具體流程與思惟為何。這些影響追訴比特幣犯罪成敗之重點，本文接下來將綜合第二章至第四章的內容扼要回應。

就「對比特幣實施搜索、扣押時，如何妥善適用我國現行刑事訴訟法之規範？」此層面而言，先從財產權侵害的角度，釐清私鑰僅是扣押比特幣之工具，故執法人員取得嫌疑人硬體錢包或軟體錢包內儲存的私鑰，並無侵害人民的財產權後，便進入特定明確原則的討論。

因著比特幣與一般電磁紀錄不同的技術內涵，亦即比特幣位址與私鑰皆無法隨使用者或他人的意志為任何更動的特性。在偵查資訊充足的狀況下，本文於發見真實與保障人民財產權、隱私權的權衡上偏向後者，認為應將搜索票上的搜索客體，分依冷錢包、熱錢包記載成「比特幣位址、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的 A 品牌筆記型電腦」與「比特幣位址、移轉目標比特幣所需之私鑰，以及可能儲存私鑰的熱錢包程式、A 品牌筆記型電腦」，以降低執法人員誤判搜索或扣押客體的風險。

接下來針對一目瞭然法則，倘執法人員為搜索、扣押比特幣，在現場接觸受搜索人的電子載體，檢視受搜索人使用的比特幣位址係位於其中何處時，發現搜索票上未記載之本案應扣押電磁紀錄，或者另案應扣押之電磁紀錄，得否一併將其扣押之？在依序介紹並討論 United States v. Carey 案的意旨，以及完全排除一目瞭然

doi:10.6342/NTU202400684

法則適用之學說後，本文選擇參酌 United States v. Carey 案，提出透過執法人員係出於惡意搜索令狀記載以外的電磁紀錄與否，作為是否適用一目瞭然法則的審查標準。

至於執法人員對交易所錢包實施搜索、扣押時，固然得直接對管理該些交易所錢包的虛擬資產平台為直接強制處分，但本文基於財產權社會義務與加密技術或驗證機制不盡相同的理由，建構虛擬資產平台配合執法人員的協力義務。在我國現行法的框架下，依序討論包括洗錢防制法第 13 條第 1 項、虛擬通貨事業洗防辦法第 7 條以及虛擬資產平台及交易業務事業（VASP）公會訂定的自律規範等選項後，藉由論證得避免虛擬資產平台執行上遭遇的技術困難，亦可滿足執法人員實務上的執法需求，降低其執法成本，本文選擇末者作為虛擬資產平台協力義務之依據。

另就「對比特幣實施搜索、扣押時，相應的具體流程與思惟為何？」此層次而言，本文先論證，若以現行實務對一般電磁紀錄實施搜索、扣押時採取的二階段搜索模式處理比特幣，恐因著對二者實施強制處分側重之目的不同，而使扣押目標比特幣之目的落空。故在我國實務工作者發展出的若干搜索、扣押比特幣作法之基礎上，為使執法人員得於確定私鑰控制權限者後，預先準備並利用更精準的打擊手段取得私鑰，本文從私鑰控制權限者的角度，分別提出由虛擬資產平台管理私鑰的錢包類型、由使用者管理私鑰的錢包類型，在事前準備與事中進行兩階段的流程下，執行面可供執法人員參考的作法。同時，針對執法人員操作此些流程時可能遭遇的執法困難，本文除了即時更新我國檢警機關近期提出的政策與具體作為，亦建議權責機關因著此類型案件的技術特性，盡速訂定一套相對完整的偵辦指引或標準作業流程，並建立可與國內、外主要虛擬資產平台聯繫的窗口。

就本文研究成果的預期貢獻而言，除了供作執法人員搜索、扣押比特幣時一套

doi:10.6342/NTU202400684

可操作的參考流程，同等重要地，在於一方面使司法者認識如何審查這些被扣押比特幣的證據能力，另方面亦可為立法者在未來相關立法計畫的研議上，得納入考量的想法與建議。

doi:10.6342/NTU202400684

參考文獻

一、中文部分

Michael J. Casey & Paul Vigna（著）、林奕伶（譯）（2019），《真理機器：區塊鏈與數位時代的新憲法》，新北：大牌出版。

Paul Vigna & Michael J. Casey（著）、林奕伶（譯）（2017），《虛擬貨幣革命：區塊鏈科技，物聯網經濟，去中心化金融系統挑戰全球經濟秩序》，2版，新北：大牌出版。

Primavera De Filippi & Aaron Wright（著）、王延川（譯）（2019），《區塊鏈與法律：程式碼之治》，臺北：元照。

William Mougayer（著）、徐瑞珠（譯）（2016），《區塊鏈商業應用｜次時代網路技術的前景、實踐與應用》，臺北：碁峰資訊。

中央銀行（2021），〈虛擬通貨近期發展及國際監管概況〉，《存款保險資訊季刊》，34 卷 2 期，頁 14-25。

中國科技大學商學院（2009），《我國證券相關公會自律機制之強化與整合》，載於：chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.twsa.org.tw/B01/doc/%E6%88%91%E5%9C%8B%E8%AD%89%E5%88%B8%E7%9B%B8%E9%97%9C%E5%85%AC%E6%9C%83%E8%87%AA%E5%BE%8B%E6%A9%9F%E5%88%B6%E4%B9%8B%E5%BC%B7%E5%8C%96%E8%88%87%E6%95%B4%E5%90%88.pdf。

中華警政研究學會（2023），〈第 54 場警政與警察法相關圓桌論壇論壇紀錄〉，頁 1-14。

王旭正、柯永瀚、ICCL 資訊密碼暨建構實驗室（2007），《電腦鑑識與數位證據─資安技術、科技犯罪的預防、鑑定與重建現場》，新北：博碩文化。

王兆鵬（2001），〈附帶扣押、另案扣押與一目瞭然法則〉，氏著，《路檢、盤查與人權》，頁 33-52，臺北：元照。

王兆鵬、張明偉、李榮耕（2022），《刑事訴訟法（上）》，6 版，臺北：新學林。

王志誠、何雨柔（2020），〈論虛擬貨幣之發展與監理趨勢〉，《財稅研究》，49 卷 3 期，頁 80-108。

王銘勇（2003），〈網路犯罪之搜索與扣押〉，《法學叢刊》，48 卷 3 期，頁 45-62。

王毅丞（2018），《實戰區塊鏈技術｜加密貨幣與密碼學》，臺北：碁峰。

台灣金融研訓院編輯委員會（2021），《防制洗錢與打擊資恐政策及法令解析》，臺北：財團法人台灣金融研訓院。

doi:10.6342/NTU202400684

吳庚、陳淳文（2013），《憲法理論與政府體制》，臺北：三民。
李承龍、蔡佩芬（2023），〈數位取證與區塊鏈保存物證之探討〉，《萬國法律》，249 期，頁 2-23。
李建良（2018），〈法學方法與基本權解釋方法導論〉，《人文及社會科學集刊》，30 卷 2 期，頁 237-277。
吳俊志（2021），〈虛擬通貨平台之反洗錢規範〉，《財稅法令半月刊》，44 卷 14 期，頁 9-10。
吳盈德（2017），〈創新金融科技與洗錢防制趨勢〉，《月旦法學雜誌》，267 期，頁 19-29。
李鈞、長銨、李耀東、喻峰、蔡卓斯、宋歡平、袁維（2014），《比特幣：過去・現在與未來》，臺北：遠流。
李惠宗（2012），《憲法要義》，6 版。
李榮耕（2012），〈特定明確原則與機動性通訊監察〉，《政大法學評論》，126 期，頁 105-153。
--------（2012），〈電磁紀錄的搜索及扣押〉，《國立臺灣大學法學論叢》，41 卷 3 期，頁 1055-1116。
--------（2018），《通訊保障及監察法》，臺北：新學林。
--------（2020），〈初探遠端電腦搜索〉，氏著，《數位時代中的搜索扣押》，頁 335-383，臺北：元照。
--------（2022），〈犯罪偵查中通訊內容的調取〉，《國立臺灣大學法學論叢》，51 卷 3 期，頁 757-831。
林文村（2022），〈附帶搜索「立即控制範圍延伸」之理論與適用分析─必較法的觀察〉，《軍法專刊》，68 卷 3 期，頁 93-126。
林育賢（2020），〈數位證據之取證及證據能力〉，《司法新聲》，135 期，頁 18-51。
林宜隆（2012），〈建構數位證據鑑識標準作業程序（DEFSOP）與案例實證之研究〉，《司法新聲》，101 期，頁 50-74。
林俊益（2022），《刑事訴訟法概論（上冊）》，22 版，臺北：新學林。
法治斌、董保城（2012），《憲法新論》，5 版，臺北：元照。
法思齊（2011），〈美國法上數位證據之取得與保存〉，《東吳法律學報》，22 卷 3 期，頁 95-147。
法務部調查局（2018），《中華民國 106 年洗錢防制工作年報》，臺北：法務部。
--------（2019），《107 年毒品犯罪防治工作年報》，臺北：法務部。
林鈺雄（2001），《搜索扣押註釋書》，臺北：元照。
--------（2022），《刑事訴訟法上冊》，11 版，臺北：新學林。
施育傑（2017），〈數位證據的載體、雲端與線上取證──搜索扣押與類型化的觀點〉，《裁判時報》，64 卷，頁 55-71。

doi:10.6342/NTU202400684

施志鴻（2018），〈比特幣相關犯罪類型與因應作為之探討〉，《資訊、科技與社會學報》，18 卷 26 期，頁 64-79。
施威銘、吳文立、李亮生、陳源宏（2010），《資訊科技概論》，臺北：旗立資訊。
洪敏超（2023），〈以 USDT 經營賭博網站之刑法管制與刑事偵查〉，《檢察新論》，32 期，頁 2-22。
恆業法律事務所（2021），《新興金融科技遭濫用於犯罪之研究成果報告書》，載於：https://www.cprc.moj.gov.tw/1563/1595/1601/1607/34933/post。
徐仕瑋（2013），〈數位證據與現行搜索、扣押法制間之適用問題〉，《檢察新論》，13 期，頁 29-46。
徐明星、刘勇、段新星、郭大治（2016），《区块链：重塑经济与世界》，北京：中信出版社。
徐珮菱（2019），〈洗錢防制法制之研究—以區塊鏈及加密數位貨幣為中心〉，《月旦法學雜誌》，288 期，頁 73-99。
陳詰昌（2016），〈數位鑑識「原件不可變動原則」之適用－由行動裝置鑑識與電腦鑑識差異探討〉，《司法新聲》，119 期，頁 42-55。
婁天威（2013），〈新興市場國家採行證券自律組織之分析〉，《證交資料》，619 期，頁 48-58。
婁天威、駱武昌、喬中珏（2014），〈金融海嘯後證券業自律組織發展趨勢之分析〉，《證券服務》，63 期，頁 30-37。
許永欽（2022），〈從 FATF 規範論虛擬資產防制洗錢之監理〉，《月旦律評》，1 期，頁 22-39。
許育典（2011），《憲法》，5 版，臺北：元照。
--------（2012），《憲法要義》，6 版，臺北：元照。
許志雄、陳銘祥、蔡茂寅、周志宏、蔡宗珍（2008），《現代憲法論》，4 版。
張麗卿（2018），《刑事訴訟法理論與運用》，14 版，臺北：五南。
游士弘、郭閔裕（2013），〈「外幣結算平台」之架構設計及系統建置〉，《財金資訊季刊》，75 期，頁 7-12。
黃立維，〈檢察機關科技偵查運用實務現況介紹〉，《檢察新論》，32 期，頁 44-62。
黃東熊、吳景芳（2005），《刑事訴訟法論(上)》，修訂 6 版。
黃柏翔（2019），〈新興電腦犯罪偵辦手法之研究─以虛擬貨幣犯罪為中心─〉。
黃舒芃（2005），〈比較法作為法學方法：以憲法領域之法比較為例〉，《月旦法學雜誌》，120 期，頁 183-198。
葉至誠、葉立誠（2011），《研究方法與論文寫作》，3 版，新北：商鼎數位。

doi:10.6342/NTU202400684

楊岳平（2019），〈區塊鏈時代下的證券監管思維挑戰：評金管會最新證券型虛擬通貨監管方案〉，《國立臺灣大學法學論叢》，48 卷特刊，頁 1279-1374。
--------（2020），〈金融科技時代下的金融監管挑戰：論虛擬通貨交易平台的監管架構〉，《國立臺灣大學法學論叢》，49 卷特刊，頁 1309-1396。
--------（2022），〈虛擬通貨的洗錢防制監管疆域與國際標準－評我國「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」〉，《法律扶助與社會》，9 期，頁 93-140。
杨保华、陈昌（2017），《区块链原理、设计与应用》，北京：机械工业出版社。
鄭文中（2020），〈犯罪沒收與虛擬貨幣之保全扣押初探〉，《商業法律與財金期刊》，3 卷 1 期，頁 93-113。
鄭婷嫻（2019），〈區塊鏈技術應用於我國公司治理法制之研究〉，《東吳法律學報》，30 卷 3 期，頁 1-43。
劉春堂（2011），《民法債編通則（一）契約法總論》，增修版，臺北：自版。
魯特（2018），《比特幣精粹》，臺北：白象文化。
蔣勇、文延、嘉文（2018），《白話區塊鏈》，臺北：碁峰。
蔡佩玲（2022），〈虛擬貨幣與洗錢防制──未知之金流世界交易規則〉，《月旦法學雜誌》，324 期，頁 132-142。
蔡墩銘（2003），《刑事訴訟法概要》，修訂 6 版，臺北：三民。
羅韋淵（2023），〈偵辦虛擬貨幣相關犯罪之戰略思考─美國司法部史上最大查扣案之借鏡〉，《檢察新論》，32 期，頁 23-43。
蘇凱平（2021），〈當證據「上鏈」：論區塊鏈科技應用於法庭證據〉，《國立臺灣大學法學論叢》，50 卷 3 期，頁 993-1071。
--------（2022），〈制定司法政策時如何參考外國法－以「蒐集法」與「功能比較法」為中心〉，《台灣法律人》，12 期，頁 97-116。
--------（2022），〈論數位證據之原件、複製品與最佳證據法則──最高法院 107 年度台上字第 3724 號等 8 則刑事判決評析〉，氏著，《數位科技與證據法則》，頁 71-96，臺北：元照。

doi:10.6342/NTU202400684

二、英文部分

Bacon, J., Michels, J. D., Millard, C., Singh, J. (2018). Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers, *Richmond Journal of Law and Technology* 25, 1-106.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. & Felton, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, In *2015 IEEE Symposium on Security and Privacy* (pp. 104-121). DOI: 10.1109/SP.2015.14.

Broome, L. L. (2019). Banking on Blockchain, *North Carolina Journal of Law & Technology 21*, 169-195.

Carter, J. L. & Wegman, M. N. (1979). Universal Classes of Hash Functions, *Journal of Computer and System Science 18*, 143-154.

Diffie, W. & Hellman, M. (1976). New Directions in Cryptography, *IEEE Transactions on Information Theory 22*(6), 644-654. DOI: 10.1109/TIT.1976.1055638.

Financial Action Task Force on Money Laundering. (2014). Virtual Currencies: Key Definitions and Potential AML/CFT Risks.

-------- (2015). Guidance for a Risk-Based Approach: Virtual Currencies.

-------- (2020). Methodology For Assessing Technical Compliance With The FATF Recommendations and The Effectiveness of AML/CFT Systems.

-------- (2021). Updated Guidance: A Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

Haber, S. & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document, *Journal of Cryptology 3*, 99-111.

Heilman, E. & Kendler, A. (2015). Eclipse Attacks on Bitcoin's Peer-to-Peer Network, In 24th USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/heilman.

Irwin, A. S.M. & Turner, A. B. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where, *Journal of Money Laundering Control 21*(3), 297-313.

Kiviat, T. I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions, *Duke Law Journal 65*, 569-608.

Lamport, L., Shostak, R. & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems 4*(3), 382-401.

Nakamoto, S. (2008). A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Reid, F. & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. *Security & Privacy in Social Networks, 3*, 1-28.

doi:10.6342/NTU202400684

Rivest, R. L., Shamir, A. & Adleman, A. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communication of the ACM 21*(2), 120-126.

Ron, D. & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. In Sadeghi, Ahmad-Reza (Eds.), *Financial Cryptography and Data Security:17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers* (pp. 6-24). Berlin, Germany: Springer.

Werbach, K. (2016). Trustless Trust, SSRN Electronic Journal. DOI: 10.2139/ssrn.2844409.

doi:10.6342/NTU202400684