出國報告（出國類別：進修）

新興電腦犯罪偵辦手法之研究
—以虛擬貨幣犯罪為中心－

服務機關：臺灣臺北地方檢察署

姓名職稱：黃柏翔檢察官

派赴國家：美國

出國期間：民國 108 年 7 月 25 日

至　109 年 7 月 24 日

報告日期：民國 109 年 10 月 20 日

摘要

本文概分為三大部分，第一部分著重虛擬貨幣之基礎概念介紹，從其定性及運作方式談起，並說明區塊鏈技術在虛擬貨幣網絡中之應用與意義，以及區塊鏈技術何以既能使虛擬貨幣網絡使用者共同參與，卻又保有某種程度之匿名特性。第二部分則從虛擬貨幣之特性出發，說明與虛擬貨幣有關之各種犯罪態樣，主要可分為：以虛擬貨幣為媒介並加以濫用之犯罪、以虛擬貨幣為犯罪標的之犯罪、以虛擬貨幣之名作為包裝之犯罪等三大類型。第三部分則總結虛擬貨幣犯罪之偵查困境，並借鏡美國立法與司法實務，提出相應之偵查作為建議，其中尤為刻不容緩的，是犯罪嫌疑人身分與金流分析資料庫的建置、虛擬貨幣扣押專戶之設置、建立全國一致之虛擬貨幣變價準則、增加並強化雙邊司法互助的管道，期使偵查機關更能與國際接軌，共同有效打擊虛擬貨幣犯罪。

目錄

壹、 研究目的

近年來，隨著網路科技日新月異的發展與革新，新興網路犯罪亦不斷升級與進化，其中尤為棘手的是虛擬貨幣犯罪（cryptocurrency misconduct），不但所涉及的技術複雜，所使用的語彙亦令人費解，不只是一般民眾，甚至包含許多執法者在內，可能都難以理解其堂奧；此外，因為虛擬貨幣犯罪必然涉及網際網絡使用，再加上網路無國界的特性，使得虛擬貨幣犯罪行為多半具有跨國、跨境的特徵，這也導致行為人、被害人、證人、犯罪所得及其他相關證據可能散落世界各地，對於執法機關而言，無疑增添許多犯罪偵防上之困境。

自從西元 2009 年第一個以區塊鏈技術為基礎的虛擬貨幣——比特幣（Bitcoin）正式問世後，時至今日，虛擬貨幣之應用可以說是方興未艾，目前市面上除了始祖級的比特幣之外，還有以太幣（Ethereum）、瑞波幣(Ripple)、萊特幣(Litecoin)、達士幣(Dash)等數以百計的虛擬貨幣活躍在國際交易市場上。可以預見的是，虛擬貨幣在下個十年、二十年，必然會持續蓬勃發展，而與虛擬貨幣有關的犯罪行為亦來勢洶洶，如何有效率地針對虛擬貨幣犯罪進行偵查、追訴、審判與執行，已成為執法者難以迴避的課題。

有感於此，本文不惴淺陋，從虛擬貨幣之相關基礎概念談起，以簡單扼要之方式說明其運作模式以及可能之濫用行為，期使相關執法者對虛擬貨幣及其應用有所瞭解，並借鏡美國立法與司法實務的實踐，嘗試對司法工作者所可能遭遇之各種偵查困境，包含匿名性之突破、

不法金流之追蹤、資料庫之建置、扣押與沒收之執行、跨境合作等事項，提出相應之建議[1]。

貳、 研究經過

筆者於民國108年7月間獲法務部選赴美國哈佛大學法學院攻讀碩士學位，期間為能涉獵並精進新興電腦犯罪及虛擬貨幣之相關學識，特別選修了Andrew Crespo教授所開設之刑事訴訟法、Noah Feldman教授所開設之社群媒體法(Social Media and The Laws)、Seth Berman教授所開設之電腦犯罪實體與程序法（Cyber Crime Law and Procedure）等課程。Andrew Crespo教授早年致力於刑事案件辯護，累積了深厚的刑事司法實務經驗，尤其專精科技時代下的搜索、扣押等強制處分之法律議題，其在哈佛大學所開設之各項課程均深受學生推介，極為熱門。Noah Feldman 教授為美國著名憲法學者，長年關注言論自由議題，於西元2019年首次在哈佛大學開設社群媒體法課程，深度探討社群媒體平台之自律與他律、平台言論之審查與管制暨其界限、個人資料及隱私保護及平台責任等議題。Seth Berman教授曾經擔任麻薩諸薩州與紐約郡助理檢察官，並專責包含虛擬貨幣犯罪在內之新興電腦犯罪查緝，任職期間偵辦多起跨國妨害電腦使用、網路詐欺、竊取個人資料及駭客攻擊案件並提起公訴，深具跨境司法合作實務經驗，其於離開公職後，亦投身電腦犯罪之鑑識與顧問工作，

[1] 本文以下對於虛擬貨幣的討論，囿於篇幅且避免焦點過於發散，所使用的例子皆為比特幣，這是因為比特幣可說是虛擬貨幣之鼻祖與原型，在此一領域具有代表性，也最為世人所知曉，至於比特幣問世後所開發出的其他虛擬貨幣，多半是在比特幣的模型上發展、革新，甚至有將這些後續發展出的虛擬貨幣稱之為「山寨幣」的說法。需特別說明的是，本文所提及各項特性，並無法全盤適用在市面上的所有虛擬貨幣，不同的貨幣在運作上的設計或多或少有其異同之處，針對不同的虛擬貨幣，在具體個案中，將必須依據其差異來調整偵查作為。

致力於網路安全及個人資料隱私維護，不但熟稔偵查實務，更清楚了解新興電腦犯罪對於偵查機關所帶來的衝擊以及因應之道。

前開各項課程為筆者充實了美國立法與司法部門在新興網路犯罪議題上的實踐，有了這些基礎認識後，深感新興網路犯罪所涉領域繁雜，為了在有限的篇幅內盡可能聚焦討論，幾經考量，最後擇定筆者自身既感興趣但又全然陌生的虛擬貨幣犯罪作為研究主題，希望藉留學此行，充實自己不足之處；且美國學界與立法、司法機關在此一領域上已經累積為數眾多的專文與實務經驗，這些論述及經驗對於我國將來處理是類案例必能有所助益，筆者作為偵查機關之一員，自應善用地利之便，把握難得的機會加以引介。

擇定研究主題後，筆者邀請並獲 Christopher Bavitz 教授首肯擔任論文指導人，Christopher Bavitz 教授致力智慧財產權之相關研究，特別專精於數位化時代對法律、社會與人際所帶來之衝擊與應對，亦熟稔虛擬貨幣之技術建置與應用。在 Christopher Bavitz 教授悉心指導下，筆者得以化繁為簡，有效率地閱讀與吸收虛擬貨幣之相關基礎知識暨其法律議題，終於 109 年 5 月間完成哈佛大學法學碩士畢業論文《虛擬貨幣濫用之犯罪偵查》(Misuse and Investigation of Cryptocurrency Misconduct），順利結業取得學位。

有了前開論文及所引用之參考文獻作為基礎，本文更進一步考量臺灣特殊的國際現況，結合我國立法與司法在虛擬貨幣犯罪相關議題上已有之實踐，包含制度面向的討論及實際案例的引用，從偵查者的角度出發，具體說明本土性之偵查困境，並於文末嘗試提出解決辦法。

參、 虛擬貨幣概說

一、 什麼是虛擬貨幣？

掌握虛擬貨幣犯罪的第一步，必須先界定何為虛擬貨幣。這個問題目前並沒有一致的答案，不同國家甚至同個國家內的不同地區，對於虛擬貨幣可能有著寬嚴不一的定義[2]。總的來說，虛擬貨幣是一種可用於交易的數位序列（serial numbers），其有別於傳統貨幣的獨特之處在於，虛擬貨幣是「去中心化的」（decentralized），也就是說，虛擬貨幣不需要一個可信賴的、中心化的權威第三方（例如銀行或國家）存在，來為虛擬貨幣之發行及交易進行記錄、擔保、驗證或干涉[3]；這些傳統上向來由中心化第三方擔任的角色與功能，在虛擬貨幣的世界中，透過貨幣網之使用者以「共同參與」的方式取而代之[4]。

虛擬貨幣另一個有別於傳統貨幣之特點在於，它本質上是虛擬的數位序列組合，也正由於這樣的特性，虛擬貨幣究竟應該被定性為貨幣、商品或一種投資契約，其實至今仍存在有相當大的爭議[5]。從結論來說，依據不同的規範需求，虛擬貨幣其實可以有不同的定性，舉例言之，美國財政部與國稅局曾明白表示：雖然虛擬貨幣可以用於商

---

[2] 我國目前對於虛擬貨幣並無明確的立法定義，司法實務上也少有清楚的說明，多半是抽象概念及名詞的重複，例如：虛擬貨幣是一種基於去中心化，採用點對點網路與共識主動性，開放原始碼，以區塊鏈作為底層技術的數位資產。類似意見可參照臺灣高等法院 107 年度金上訴字第 83 號刑事判決。

[3] Nicholas Godlove, *Regulatory Overview of Virtual Currency*, 10 Okla. J.L. & Tech. 2 (2014).

[4] 更多關於「去中心化」的詳細討論，可參考 Vitalik Buterin, *The Meaning of Decentralization*, MEDIUM (Feb. 6, 2017), https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. (last visited Oct. 11, 2020)

[5] *Supra* note 3, at 24-31.

品交易，但其並不具有與法定貨幣相同之地位[6]；然而在某種程度上，虛擬貨幣就如同戰時的黃金或者牢獄等矯正機構裡的香菸一般，具有與法定貨幣相同之交易功能[7]，將之定性為「貨幣」，與其現實上之效用並無齟齬，且由於虛擬貨幣之使用並不受限於國界，其流通性甚至可以超越法定貨幣；另一方面，以虛擬貨幣作為一種募資方式早已不是新聞，美國法界亦有認為此種作為募資使用之虛擬貨幣具有有價證券之特性，並應受相關有價證券法制之規範[8]。

我國實務見解在虛擬貨幣之定性上亦曾有過不同的意見，其中有以比特幣為例，明白表示比特幣雖然具有市場經濟價值，但並非銀行法第 5 條之 1、第 29 條之 1 所稱之「款項」或「資金」，且我國銀行等金融機構於現行制度下亦不可經營比特幣之收受、兌換或交易等業務，從而認定被告等透過比特幣平台收受或吸收投資者投入比特幣之行為，不該當銀行法第 125 條第 1 項前段之違法經營收受存款業務罪，所持理由略為：所謂「收受存款」包含「收受款項」或「吸收資金」，其中「款項」係指通行貨幣（法定通行貨幣或外國貨幣），尚

---

[6] *See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FINANCIAL CRIMES ENFORCEMENT NETWORK (FIN-2013-G001, Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf; IRS Pub. IRS Notice 2014-21 (2014), INTERNAL REVENUE SERVICE, https://www.irs.gov/pub/irs-drop/n-14-21.pdf (both last visited Oct. 11, 2020)

[7] *Interview with Eric Posner*, TOP OF MIND, 21 Goldman Sachs Issue, https://www.dwt.com/files/paymentlawadvisor/2014/01/GoldmanSachs-Bit-Coin.pdf (last visited Oct. 11, 2020)

[8] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, U.S. SECURITIES AND EXCHANGE COMMISSION (81207, Jul. 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf (last visited Oct. 11, 2020)
有趣的是，美國 Cipher Technologies Bitcoin Fund 公司曾於西元 2019 年間，向美國證券交易委員會（SEC）申請成為一家投資銀行，並將大部分的資產投資於比特幣，該公司於申請文件中向 SEC 說明比特幣是一種證券，應受美國證券交易法管轄，然而 SEC 在與該公司的往來信件中，卻明白表示比特幣「不是證券」，在在顯示虛擬貨幣的定性具有流動性，於不同的脈絡下可能會獲致不同的結論。*See* Re: Cipher Technologies Bitcoin Fund, SECURITIES AND EXCHANGE COMMISSION (No. 811-3443, Oct. 11, 2020), https://www.sec.gov/Archives/edgar/data/1776589/999999999719007180/filename1.pdf (last visited Oct. 11, 2020)

無疑義，而「資金」是指可供使用或運用之金錢，通常以貨幣方式表現，用來進行周轉，滿足創造社會物質財富需要的流通價值，誠然，除收受存款外，銀行得吸收之「資金」非以通行貨幣為限，但仍應以銀行法第 3 條第 1 至 21 款所列舉者，或同條第 22 款經中央主管機關核准辦理之有關業務為限，各類實體物或無形權利，縱使得經市場交易而呈現貨幣價值，而有「資金」外觀，但收受或吸收該實體物或無形權利，如非屬銀行依法得辦理之上揭業務，當非銀行法規範、甚至處罰之對象。比特幣得在公開市場上交易，受市場供需影響而有價格波動，性質上類同投資工具，雖經市場交易而有一定貨幣價值，但我國發行貨幣及銀行法之主管機關均否定其貨幣性質，蓋因：（一）比特幣目前並非社會大眾普遍接受之交易媒介，且其價值不穩定，難以具有記帳單位及價值儲存之功能，不具真正通貨特性；（二）比特幣非由任何國家貨幣當局所發行，不具法償效力，亦無發行準備及兌償保證，持有者須承擔可能無法兌償或流通之風險；（三）依據中央銀行法規定，該行發行之貨幣為國幣，對於國內之一切支付，方具有法償效力；（四）此外，金融監督及管理委員會亦重申：比特幣並非貨幣，係屬「虛擬商品」性質，尚不得作為社會大眾普遍接受之支付工具，故銀行等金融機構不得收受、兌換比特幣，亦不得於銀行 ATM 提供比特幣相關服務等，可見比特幣目前在我國的法律定位上並非貨幣，而係數位虛擬商品，換言之，比特幣目前並非銀行等金融機構「收受款項」或「吸收資金」之客體，且比特幣在現實交易上，雖可透過幣託公司轉賣為現金，然此並非透過銀行等金融機構交易，比特幣在銀行等金融機構間亦無強制流通性，不具有清算最終性。本案被害人購

買比特幣，多係透過比特幣平台所購買，被告等人雖以投資、互助為名，收受大眾投入比特幣至平台，再將被害人投入之部分比特幣以上揭方式變現牟利，與銀行收受存款之貨幣市場存貸行為迥異，自非銀行法所欲管制或處罰之範圍[9]。

前開見解在立場上明白否定虛擬貨幣之法定貨幣性質，且以此作為排除銀行法違法經營收受存款業務罪適用的論據之一，但同一法院亦曾有過截然相反的意見，判決理由略謂：暗黑幣、香港寶石及霹克幣投資案，均係約定給付與本金顯不相當之紅利、獎金，而向不特定多數人吸收資金，業經審認如前，被告雖辯稱暗黑幣、霹克幣均為虛擬貨幣，每日交易行情有所變動，投資人能獲得之利益亦因此有高有低，難以斷論其等能取得與本金顯不相當之報酬云云，然觀諸暗黑幣、霹克幣投資案之方案內容，可知均係允諾投資人每月可領得固定之虛擬貨幣數量，暗黑幣、霹克幣投資案之文宣上，更均載明「月收益」、「年收益」之比例，復如前述，顯然在招攬投資之初，即係以約定給付與本金顯不相當利益之方式，吸引投資人交付款項，則縱使嗣後因幣值波動，或真有被告所宣稱之暗黑幣在大陸地區遭查禁，導致無法買賣等情事，亦均無解於被告確以上開投資案吸收資金之認定，成立銀行法第 125 條第 1 項前段之違法經營收受存款業務罪[10]。

---

[9] 臺灣高等法院 107 年度金上訴字第 83 號刑事判決參照。

[10] 臺灣高等法院 108 年度金上訴字第 7 號、109 年度台上字第 730 號刑事判決參照。惟此一爭議在銀行法第 125 條於 108 年 4 月 17 日修正公布後，已算是塵埃落定，此觀該次修正理由特別說明：「近年來，違法吸金案件層出不窮，犯罪手法亦推陳出新，例如透過民間互助會違法吸金，訴求高額獲利，或者控股公司以顧問費、老鼠會拉下線，虛擬遊戲代幣、虛擬貨幣『龐克幣』、『暗黑幣』等，或以高利息（龐氏騙局）與辦講座為名，或者以保本保息、保證獲利、投資穩賺不賠等話術，推銷受益契約，吸金規模動輒數十億，對於受害人損失慘重……」等語，顯然已明確將以虛擬貨幣作為投資資金或投資名義之存款收受行為，納入銀行法之規制範圍內。

除了刑事案件外，虛擬貨幣之定性在我國民事強制執行實務中亦有過不同之意見，有認為比特幣屬「金錢債權」者，亦有認為屬「物」者，其所持理由略謂：查比特幣因非為社會大眾普遍接受之交易媒介，且其價值不穩定，難以具有記帳單位及價值儲存之功能，不具真正通貨特性，且非由任何國家貨幣當局所發行，為我國中央銀行所認定在案，應認比特幣在我國不能認屬貨幣，而比特幣之性質，審酌其係為與特定政府組織發行之流通貨幣區隔，藉由比特幣本身表彰一定價值，使比特幣持有者得持以兌換等值之物或貨幣，可知比特幣為權利所依附之客體，其性質應屬「物」，且屬「代替物」，自應依交付代替物之執行方法為之，如債務人占有該代替物，則取交債權人，如未占有該代替物，債務人應依執行名義購買代替物交付債權人，債務人不為此行為，則依強制執行法第 127 條之規定，裁定命債務人支付採買代替物之費用，於債務人不支付時，以該裁定為執行名義，對債務人一切財產為執行；本件所涉確定判決之執行名義，其主文係命抗告人應給付相對人 5 顆比特幣，依前開說明，其執行程序自應依交付代替物之執行方法為之，惟原執行法院並非依此執行程序為之，而係依金錢債權之執行程序為之，逕為對抗告人之財產為查封之執行行為，此部分之執行程序已有可議[11]。

綜合以上國內外民刑事實務意見，可知虛擬貨幣既可能是貨幣、商品，也可能是有價證券，在強制執行之領域中，甚至可以被看作「物」，其定性端看所持觀點與規範目的而定，對於犯罪偵防人員而言，這也意味著蒐證方向與他日在法庭上之攻防重點，將會因為虛擬貨幣在個

[11] 臺灣高等法院臺南分院 108 年度抗字第 123 號民事裁定參照。

案當中的定性而有不同的偏重，進而影響偵查作為與辯論的策略擬定。

二、 虛擬貨幣如何運作？

虛擬貨幣本質上是透過演算法編碼加密的數位序列，每組編碼都具有獨特性而可與其他編碼代表之貨幣區別。以比特幣為例，透過演算法編碼後的資料，表面上就只是一組看似毫無意義的英文與數字亂碼組合[12]，需要配合特定的「鑰匙」來進行解碼，但一把鑰匙僅僅只能解鎖一組編碼，因為不同的原始資料經過編碼後都會得到相異的編碼結果，各自需要不同的鑰匙來進行解讀，這也意味編碼過程同時具有加密的作用，可使經過編碼的資料成為「密文」（cipher text）。經過加密的資料除了其對應之鑰匙外，以目前所知的科技範疇，在理論上無從破解，這也使得虛擬貨幣的「價值」得以被相信與確立[13]。

前開提到用以解碼之「鑰匙」，又區分為「公鑰」（public key）及「私鑰」（private key），兩者相應而生。公鑰顧名思義為該虛擬貨幣網絡中之所有使用者所周知，至於私鑰，則由虛擬貨幣之擁有者保管，也是所有權的證明。在進行虛擬貨幣交易時，首先由貨幣所有權人使用私鑰對所欲進行的交易「簽名」，證明其為貨幣之擁有者，從而得以對特定虛擬貨幣錢包地址中之貨幣進行處分，接著演算法會產出對應之公鑰，並公告周知於整個貨幣網絡，其他網絡使用者便可

[12] 唯一的規則可能僅僅是：比特幣的開頭多為 1 或 3，例如：3MieYo1wiBYWHRUnoe6vvhGVwndmVoBjDr（此為真實存在的比特幣位址），而以太幣的開頭則為 0x。另外，為了表達上的便利性，虛擬貨幣現在也可以用 QR Code 或二維條碼的形式來表示。

[13] Godlove, *supra* note 3, at 10.

透過公鑰來驗證該交易之有效性並完成交易，且整個交易過程都會留下公開的紀錄[14]。

所有之貨幣交易均留有公開紀錄，正是讓虛擬貨幣得以風行崛起的重要特徵。以比特幣為例，貨幣自創造之初迄今之所有歷史交易訊息皆為公開且依時序記錄，一筆交易訊息鏈著一筆，持續延長並相互連結，且新的交易紀錄一旦加入到區塊鏈中就不會再被移走，此即「區塊鏈」（Blockchain）技術之具體應用。如果用更易於理解的方式來說明，區塊鏈技術在比特幣中之運用，可以看作是一種「將資料寫錄」並且「全民皆可參與」的「公眾電子帳本」（ shared public ledger）[15]，這種去中心化的資料庫，透過使用者的集體維護，並依靠複雜的密碼學來加密資料，在不需要權威第三方介入的前提下讓使用者達成共識，解決了網路上信任與資料價值的難題[16]。

為什麼說虛擬貨幣交易資料庫，是由使用者來集體維護呢？這涉及區塊鏈的核心宗旨——去中心化。去中心化強調區塊鏈的共享性，其目標是讓使用者不用去依靠額外的管理機構、硬體設施和中心機制，而能彼此自我驗證、傳遞與管理。去中心化是區塊鏈最突出也是最核心的本質特色，其應用在虛擬貨幣上，便是所有的交易皆是透過貨幣網絡使用者的參與，以其各自的資源來運算並驗證交易，以實現多方共同維護[17]。此一驗證交易的過程，在比特幣的交易市場上稱之為「挖

[14] *Id.*
[15] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (2009), https://bitcoin.org/bitcoin.pdf (last visited Oct. 11, 2020)
[16] *How Does Bitcoin Work*, BITCOIN.ORG, https://bitcoin.org/en/how-it-works (last visited Oct. 11, 2020) *See also* Raina S. Haque, *Blockchain Development and Fiduciary Duty*, STANFORD JOURNAL OF BLOCKCHAIN LAW & POLICY (2019), https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty (last visited Oct. 11, 2020)
[17] *Id.*

礦」（mining），它是透過「工作量證明機制」（Proof of Work，POW）來進行，所謂「工作量證明機制」類似於一種運算競爭，因為「挖礦」需要超高速的電腦和大量的記憶體，而且必須能快速處理這些大量的記憶體，「礦工」通常需要使用專門用於「挖礦」的特殊處理晶片，透過自己的工作效率來與他人較勁，看誰能先證明運算結果，以將驗證、確認後的交易「打包」到區塊鏈中。這樣的技術競爭受到許多專業人士的熱愛，讓大家可以在眾多的公開平台上發掘不同硬體的計算能力，彼此較勁誰可以運用各自的運算資源，花費最少的時間算出答案並驗證交易，以獲得「報酬」（比特幣或者手續費）[18]。

整個驗證過程與結果，除了涉及被加密的部分（例如私鑰）外，所有的運算數據都是公開的，任何人都可以查詢區塊鏈中的數據，這使得區塊鏈的交易訊息非常透明。此外，區塊鏈的資料一旦經過驗證便永久寫入該區塊中，任何人皆無法篡改，這也去除掉了人為操控的可能，讓區塊鏈獨立且安全，藉以確保網絡不會受制於個人、團體或其他外力干預[19]。

需要特別說明的是，雖然虛擬貨幣的交易資訊是公開的，但所公開的內容並不及於交易者的身分識別資訊，該等資訊（至少在理論上）是無從被知曉的，因為所有的公開紀錄至多只會連結到網絡使用者所使用的電子位址（electronic addresses）或假名（pseudonyms）[20]，這意味著參與交易的雙方只要在確保假名或電子位址不會與他們的

[18] *Id.*
[19] *Id.*
[20] *Id.* 更多關於比特幣之匿名性可否被推翻、貨幣所有人的身分可否被追蹤的更多討論，*see* e.g., Fergal Reid & Martin, *An Analysis of Anonymity in The Bitcoin System* (2011), https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (last visited Oct. 11, 2020)。

身分識別資訊有進一步的連結，便得以保有真實身分與隱私的方式來進行交易，此即虛擬貨幣交易之匿名性（Anonymity）。

匿名性固然對虛擬貨幣網絡使用者提供了充足的隱私保護，但這也暗示有心人士得以藉著匿名的特性來規避法律（例如銀行法或稅法相關規定），或甚至利用虛擬貨幣從事不法行為[21]，這些不法行為中，有些是利用虛擬貨幣易於藏匿真實身分以製造金流斷點之特性為之，例如洗錢，或者透過洗錢所藏匿的犯罪，有些則是著重虛擬貨幣本身財產價值、以不法方式奪取虛擬貨幣處分權為目標，例如針對貨幣交易所所發動的駭客攻擊行為，另外也有表面上涉及虛擬貨幣，實質上與虛擬貨幣的技術應用無關的犯罪行為，各種以虛擬貨幣為名之違法吸金與詐欺案件屬之。以下分別詳述之。

肆、 虛擬貨幣之濫用：洗錢及藏匿於洗錢之下的犯罪

虛擬貨幣所應用之區塊鏈技術使得前所未見的跨境點對點（peer-to-peer）匿名交易成為可能，自西元 2009 年比特幣問世以來，已有無以數計的虛擬貨幣持有者利用區塊鏈「去中心化」的特性進行匿名交易，這也使得虛擬貨幣在國際市場蓬勃發展的同時，有心人士得以利用其特性隱匿犯罪跡證，藉此規避查緝[22]。

虛擬貨幣被濫用為洗錢工具一事，向來是司法機關對於這個新世代支付工具最大的擔憂。虛擬貨幣史上最有名的罪犯，要數著名網路

[21] *See* Simon Dyson et al., *The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime*, 1 JBBA 1 (2018).
[22] *See* Raina S. Haque, *Blockchain Development and Fiduciary Duty*, STANFORD JOURNAL OF BLOCKCHAIN LAW & POLICY (2019), https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty (last visited Oct. 11, 2020)

黑市（或稱「暗網」，darknet or black market）——「絲路」（Silk Road）的創辦人 Ross Ulbricht，他在「絲路」上使用「Dread Pirate Roberts」為其代號，對外宣稱創建「絲路」是為了要提供世上所有人一個可以販售、購買任何物品的自由市場，而 Ross Ulbricht 本人甚至也曾經透過該網路平台買兇殺人。案經美國聯邦調查局(Federal Bureau of Investigation，FBI）偵辦後，Ross Ulbricht 被控提供「絲路」作為交易毒品、武器、駭客軟體、毒害物質等違禁物的平台，而該平台上的交易的媒介即為比特幣[23]。據統計，有超過市值 200 萬美元的比特幣流通其上[24]。使用虛擬貨幣作為交易工具被認為是黑市「內建」的重要特徵[25]，賣家出售商品可以得到各種虛擬貨幣作為對價，這些貨幣往往可以在同一網站甚至其他交易平台上直接用於購買他種合法或非法的商品[26]，甚至也可以轉換為美元、歐元等各種流通性高的法定貨幣，這也使得違禁物品可藉此銷售、散佈、流通；此外，透過虛擬貨幣作為支付工具，犯罪活動所生之不法所得便可在商品、虛擬貨幣、法定貨幣間的轉換過程中「洗白」[27]。

---

[23] *See* United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014); *see also* United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017); *see also* Claire Nolasco Braaten & Michael S. Vaughn, *Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions*, DEVIANT BEHAVIOR (2019), https://doi.org/10.1080/01639625.2019.17060706 (last visited Oct. 11, 2020)

[24] 自有網路黑市開始，比特幣一直都是最受歡迎的交易貨幣，雖然早在絲路之前，就已經有所謂的暗網，但自從絲路問世，並結合了比特幣作為支付工具之後，暗網才算是真正發揮了它真正的影響力。*See* Martin Horton Eddison and Matteo Di Cristofaro, *Hard Interventions and Innovation in Crypto-Drug Markets: The Escrow Example*, 11 Policy Brief 3-4 (2017). *See also* World Drug Report, *Global Overview of Drug Demand and Supply*, UNITED NATIONS ON DRUGS AND CRIME (2018), https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf (last visited Oct. 11, 2020)

[25] EMCDDA and Europol, *Drugs and The Darknet* 55 (2017).

[26] *Id.*

[27] *Id.*

我國司法實務前於民國 104 年間，即有針對利用虛擬貨幣進行洗錢之犯罪行為進行偵查並提起公訴之案例[28]，其犯罪事實略為：被告等在臺灣設立轉帳詐騙機房，詐騙大陸地區人民所得超過 500 萬元，所騙得之款項先轉入大陸地區金融機構帳戶後，再集中轉入另一人頭帳戶，另由部分被告假冒大陸地區人民，偽造大陸地區居民身分證，持向比特幣交易所網站人員以視訊方式進行身分認證。嗣以假身分成功取得比特幣電子錢包後，被告等旋將前開不法所得轉入其所掌控之電子錢包中，接著再將比特幣轉入其他虛設之電子錢包中，共計至少使用 6 個虛設之彼特幣電子錢包進行洗錢，最後再將比特幣兌換為人民幣，並輾轉將人民幣再轉入其他大陸地區金融機構帳戶，以上開方式層層轉換及轉帳的方式，製造金流斷點以藏匿犯罪所得，取得詐騙款項。

至於藏匿於洗錢之下的犯罪行為，除了毒品、槍枝等違禁物之非法交易外，應該也包含了非銀行業經營匯兌業務[29]之「地下匯兌」行為。此類犯行在臺灣及大陸地區之間原本就屬常見，自從虛擬貨幣問世之後，地下匯兌業者所辦理的匯兌業務也就更為「多元」了，依照我國向來實務意見，資金、款項皆得為匯兌業務之客體，本無法定貨幣或外國貨幣等之限制[30]，根據這樣的看法，則地下匯兌業者收受新

[28] 臺灣新北地方檢察署 104 年度偵字第 32056 號、105 年度偵字第 1137 號至第 13518 號、第 13522 號至第 13524 號、第 18378 號、第 18392 號、第 19037 號起訴書參照。案經臺灣高等法院以 106 年度金上重訴字第 13 號刑事判決有罪，部分被告提起上訴，最高法院於 106 年 12 月 27 日以 106 年度台上字第 4184 號判決駁回上訴確定。

[29] 銀行法第 29 條第 1 項所謂匯兌業務，依最高法院之看法，係指行為人不經由現金之輸送，而藉與在他地之分支機構或特定人間之資金清算，經常為其客戶辦理異地間款項之收付，以清理客戶與第三人間債權債務關係或完成資金轉移之行為，凡從事異地間寄款、領款之行為，無論是否賺有匯差，亦不論於國內或國外為此行為，均符合銀行法該條項「匯兌業務」之規定。最高法院 97 年台上字第 6582 號、95 年度台上字第 5910 號、92 年度台上字第 2040 號判決意旨參照。

[30] 最高法院 99 年度台上字第 7380 號判決意旨參照。

臺幣後，為客戶代購虛擬貨幣並存入指定之虛擬貨幣錢包，再經客戶自行利用虛擬貨幣交易平台變現為人民幣，達到移轉資金功能，應認亦屬於匯兌業務之範疇無訛，我國偵查機關亦已有就此類案件提起公訴的案例[31]。

需特別強調的是，洗錢僅僅是虛擬貨幣犯罪中的一部分環節，因為所有可以產出金錢利益的犯罪活動，理論上都有藏匿其所得來源的動機，因此，若能有效打擊虛擬貨幣作為洗錢工具，同時也就能抑制其他犯罪活動，這也是美國司法機關自 Silk Road 上線以來，持續投入許多資源防杜虛擬貨幣洗錢犯罪的原因。然而，FBI 雖於西元 2013 年成功使 Silk Road 下架，但該網站的關閉並沒有成功根除黑市的存在，亦未遏止虛擬貨幣繼續被濫用為洗錢工具。

繼 Silk Road 關站之後，Agora 和 Evolution 分別於西元 2013 年、2014 年相繼問世，並成為熱門黑市[32]。根據歐洲毒品及成癮監控中心（Europe Monitoring Centre of Drugs and Drug Addiction，EMCDDA）所做的研究報告，西元 2011 年至 2017 年間，全球至少有 103 個網路黑市；熱門黑市的更迭非常頻繁——Silk Road 為西元 2011 年至 2013 年間的霸者，2014 年間，Agora 和 Evolution 為熱門首選，到了西元 2015 年至 2016 年間，則為 AlphaBay、Nucleus 和 Dream Market， 其中尤以 AlphaBay 最具支配地位，直至西元 2017 年 7 月

[31] 臺灣新北地方檢察署 108 年度偵字第 12477 號起訴書參照。該案被告等人即係以類似之手法，於收受客戶所交付之新臺幣後，將客戶之不法所得移轉至大陸地區，並為顧客代購商品或虛擬貨幣、代為充值支付工具或兌換為人民幣，藉以達到洗錢之目的，經該地方檢察署以違反組織犯罪條例、洗錢防制法及銀行法而提起公訴，現仍在法院審理中。

[32] Amanda Roxburgh, *A Short History of Darknet Markets and The Impact of Disruptions along The Way*, NATIONAL DRUG & ALCOHOL RESEARCH CENTER, https://ndarc.med.unsw.edu.au/blog/short-history-darknet-markets-and-impact-disruptions-along-way (last visited Oct. 11, 2020)

AlphaBay 關站後，才被 Dream Market 和 Valhalla、Silk Road 3.1、Darknet Heroes League、Apple Market 等網站取而代之[33]。

由於有這麼多的國際黑市接踵崛起，如何有效打擊洗錢犯罪、遏止虛擬貨幣成為洗錢工具，藉此防杜、查緝藏匿於洗錢外衣之下的犯罪活動，已經毫無疑問成為現代犯罪偵防機關極具挑戰性的重大任務。

伍、 以虛擬貨幣為犯罪標的之犯行

雖然虛擬貨幣最終該應該被定性貨幣、商品、有價證券或投資契約，仍存有相當大的爭議，但究其本質與特性，如同美國聯邦最高法院在對 Ross Ulbricht 的判決中所揭示的——比特幣的價值取決於它能夠作為支付工具以換取物品，它無法被放在書架上或蒐集放進箱子裡，它是數位的而不具有具體的外型，是由字節與位元組所組成的財物[34]，目前主流意見已經接受虛擬貨幣是具有經濟價值的財物，而正因為虛擬貨幣具有經濟價值，它也時常成為犯罪者攻擊的目標。

以虛擬貨幣為目標之犯罪活動中，最常見的是竊取「鑰匙」的行為。以比特幣為例，雖然經過編碼加密後，理論上他人無從破解，然而其運作機制上需要得以證明所有權並可加以解碼、處分的「私鑰」配合[35]，而所謂的私鑰，其實也不過就是一組可以儲存為文字檔（text

[33] *Supra* note 25; *see also Global Overview of Drug Demand and Supply*, UNITED NATIONS ON DRUGS AND CRIME, https://www.unodc.org/wdr2018/prelaunch/WDR18_Booklet_2_GLOBAL.pdf (last visited Oct. 11, 2020)

[34] 這段判決理由是美國聯邦最高法院對被告 Ross Ulbricht 被控洗錢犯罪所做無罪答辯的回應，被告認為比特幣交易並非財產交易，從而不適用美國法典中關於洗錢的規定（18 U.S.C. § 1956）。*See* United States v. Ulbricht, 31 F. Supp. 3d 540, 570 (S.D.N.Y. 2014).

[35] *Supra* note 3, at 19.

file）的字元[36]，貨幣持有者為了避免遺忘私鑰，多半會將之儲存在電腦硬碟、雲端空間或甚至是公眾網路平台上的儲存空間，一旦儲存私鑰的檔案遭到駭客入侵並加以複製，或被釣魚網站騙取（fake URL hijacking），或者遭到網路平台人員內神通外鬼而流出，則私鑰所表彰的虛擬貨幣即可能被盜用變賣[37]。

虛擬貨幣史上最著名的竊案之一發生於西元 2014 年，遭竊的虛擬貨幣交易所為 Mt. Gox，該交易所曾經是全球最大的比特幣交換中心，經手當時超過 70%的比特幣交易。然而在西元 2014 年 2 月，該交易所突然宣布破產，起因在於網站遭到駭客入侵，導致該網站的使用者都無法處分原本持有之比特幣，據估計損失約 7 萬 4,000 顆比特幣（佔當時流通比特幣總數的 6%），在當時市值約為 4 億 6,000 萬歐元[38]。雖然事件的全貌至今仍然有未明之處，但一般認為「私鑰」遭洩是導致此次竊案發生的主要原因[39]。

遺憾的是，Mt. Gox 並不是虛擬貨幣史上唯一遭駭的交易所，類似的駭客入侵事件也發生在其他交易所網站，例如 Flexcoin 交易所（西元 2014 年）[40]，以及 Binance 交易所（西元 2019 年）[41]，也同樣都造成鉅額的損失。在亞洲地區也有這類的案件發生，交易所網站雖架設在日本，但亦間接衝擊臺灣之虛擬貨幣所有人，此即西元 2019 年 7 月 11 日 BITpoint Japan 公司經營之虛擬貨幣交易平台遭駭客入

---

[36] *Id.*
[37] *Id.*
[38] Andrew Norry, *The History of the Mt Gox Hack: Bitcoin's Biggest Heist*, BLOCKONOMI (2019), https://blockonomi.com/mt-gox-hack/ (last visited Oct. 11, 2020)
[39] *Id.*
[40] Godlove, *supra* note 3, at 18-20.
[41] Anthony Xie, *Investigating the $40 million Binance Hack*, HODLBLOG, https://www.hodlbot.io/blog/binance-hack (last visited Oct. 11, 2020)

侵事件，該公司因此受有約 35 億日圓之損失，並旋即關閉交易系統，而臺灣之幣寶亞太科技資訊有限公司因使用同一伺服器建置了相同的交易系統，為配合日方調查該事件，於同年月 12 日起亦關閉加密貨幣之轉入及轉出服務，致虛擬貨幣之所有人無法加以處分[42]。

至於我國本土的案例則發生在「幣託」（BitoEX）網站，該網站係由泓科科技有限公司架設，以對外經營比特幣之交易為業，然於民國 105 年 6 月 30 日起，經被告以隱藏實際 IP 位址之技術，營造層層轉傳之連線路徑，而輾轉以境外 IP 位址連結網路至該公司主機，並冒用該公司網站工程人員之帳號名義，於破解密碼後入侵幣託網站之後台管理系統，繼以管理者權限，先將幣託網站內各該比特幣會員帳戶於轉出比特幣時所預設、用以接收簡訊認證碼之電話號碼，均竄改變更為被告前向國外不知名網站所匿名申請之免費國際電話號碼，進而恣意從幣託網站內之各該比特幣會員帳戶內轉出共計 2,292.85 顆比特幣（於案發時市值約新臺幣 5,000 萬元，至今未據扣案）至被告所管領之境外比特幣帳戶內[43]。

陸、 以虛擬貨幣為名之犯行

除了被利用為洗錢工具，或者本身就是犯罪行為的目標之外，虛擬貨幣也可能被濫用作為「幌子」，化身成為各式各樣的騙術。在某些案例中，不肖之徒可能唆使投資者購買跟虛擬貨幣有關的投資合約，

[42] 臺灣臺北地方檢察署 109 年度偵字第 6772 號、第 6773 號、第 9060 號、第 9890 號、第 12729 號、第 13883 號、第 14037 號不起訴處分書參照。

[43] 該案嗣於 106 年 8 月 21 日提起公訴，被告應為我國第一位盜取虛擬貨幣經起訴之駭客，而依起訴當時之市值計算，被告所盜取之比特幣價值約為 2 億 5,000 萬元，與犯罪當時相較，市值已增加近 2 億元。臺灣臺北地方檢察署 106 年度偵字第 17735 號、第 18963 號起訴書參照。

佯稱投資虛擬貨幣交易可以獲得可觀的報酬[44]，或者詐稱購買網站會員即可以透過網站獲得有關虛擬貨幣交易的投資顧問服務，但於隨即關閉網站而未提供任何原先應允的任何服務[45]，又或者未經向美國證券交易委員會（Securities & Exchange Commission，SEC）登記即以發行虛擬貨幣公開募資（亦有稱為首次代幣發售、虛擬貨幣首次公開募資，Initial Coin Offering，即 ICO）[46]等。

另外在美國商品期貨委員會（U.S. Commodity Futures Trading Commission，CFTF ）對 My Big Coin Pay 股份有限公司的案件中，被告公司販售了價值超過 600 萬美元的虛擬貨幣「My Big Coin」，宣稱其發行之虛擬貨幣價值有黃金期貨在背後撐腰，可以使用在任何接受萬事達信用卡的通路，並且在各大交易所中被活絡地買賣與使用。對此，美國商品期貨委員會認為該公司涉嫌以販賣商品為詐欺行為，已違反《商品交易法》（Commodity Exchange Act）授權[47]該委員會訂定之相關行政規定[48]而提起訴訟[49]。

在美國證券交易委員會對 Sharma 的案件中，被告二人為提供財務金融服務的創投公司——CentraTech 股份有限公司的創立者，他們以發行虛擬貨幣公開募資，有數千投資者響應，總計募集金額超過 3,200 萬美元;該公司宣稱其所提供之虛擬借記卡(crypto debit card)可用於接受 Visa 及萬事達信用卡的通路，使用者亦可輕易將虛擬貨

44 CFTC v. My Big Coin Pay, Inc., 334 F. Supp. 3d 492 (D. Mass. 2018).

45 CFTC v. McDonnel, 287 F.Supp.3d 213 (E.D.N.Y. 2018).

46 SEC v. Sharma, 1:18-cv-02909 (S.D.N.Y. April 4, 2018).

47 7 U.S.C. § 9 (1).

48 17 C.F.R. § 180.1(a).

49 *Supra* note 44; *see also* Claire Nolasco Braaten & Michael S. Vaughn, *Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions*, DEVIANT BEHAVIOR (2019), https://doi.org/10.1080/01639625.2019.17060706 (last visited Oct. 11, 2020)

幣轉換成美元或其他法定貨幣加以使用，然而實際上該公司與 Visa 及萬事達信用卡根本沒有任何合作關係，嗣經美國證券交易委員會認為涉嫌以詐術發行虛擬貨幣公開募資而提起訴訟[50]。

在臺灣，相類似的案件也十分常見，例如：被告等共同基於非法經營收受準存款業務之犯意聯絡，透過 LINE 通訊軟體邀約不特定人投資之訊息，佯稱是「台北最大挖礦場聚力礦場」營業部協理，專長經營挖比特幣與乙太幣，可以「天天返利 5%」、「15 期計畫：日日返利 3%，15 天總收益 145%」、「30 天期計畫：日日返利 5%，30 天總收益 250%」等，表示募集資金用於參與投資虛擬貨幣，允以 15 日或 30 日為 1 期，每日返還投資現金 3%或 5%之利潤，期滿返還本金，致被害人等陷於錯誤而交付財物[51]；被告等對外宣稱開發虛擬貨幣「以太幣」之挖礦機，以區塊鏈技術為基礎提供智慧合約服務，且預計未來於大陸九華山地區建設發展「以太世界」渡假村，投資者可使用 「以太世界」APP 軟體進行開戶及操作各項投資配套方案，獲利可高達 200%至 300%，部分可提領現金或轉換成以太幣，嗣被告等逕將以太世界投資方案官方網站及 APP 系統關閉，致使投資人已無法依投資方案所述，將持有之「以太黃金幣」轉換為美元或新臺幣而取回實質獲利[52]；被告等明知 Unicoin 為自行創設之虛擬貨幣，實際上並無法在任何虛擬貨幣交易所或其他平臺交易流通，以及 IBCoin 之發行者、來源、交易價格及功能均不明，難以流通變現等情，竟利用

---

[50] *Supra* note 45; *see also SEC Halts Fraudulent Scheme Involving Unregistered ICO*, U.S. SECURITY AND EXCHANGE COMMISSION (Immediate Release 2018-53), https://www.sec.gov/news/press-release/2018-53 (last visited Oct. 11, 2020)

[51] 臺灣臺北地方檢察署 109 年度偵字第 2573 號、第 2574 號不起訴處分書參照。

[52] 臺灣臺北地方檢察署 108 年度偵字第 759 號、第 8555 號、第 10176 號、第 15384 號、第 17714 號起訴書參照。

一般人對虛擬貨幣之原理、價值及交易方式均欠缺充分之認識及理解，佯稱「IBCoin、Unicoin係與比特幣、以太幣具有相同投資價值之虛擬貨幣」、「IBCoin會灌入資金炒幣」、「IBCoin會有基金投入及灌入資金」、「IBCoin已有公司團隊在操盤」、「IBCoin於2至3個月會上交易所」、「IBCoin會上前三大交易所」、「IBCoin可用在成人娛樂產業」、「菲律賓蓋了賭場未來可用IBcoin」、「IBCoin、Unicoin兩虛擬貨幣是獨家販售」云云，致被害人等陷於錯誤，以1顆新臺幣50元以上顯不相當之價格,向被告等購買未具市場流通性，且無投資價值之IBCoin、UNicoin虛擬貨幣，被告等則藉此詐得款項共計達新臺幣1,341萬1,500元[53]。

這類以虛擬貨幣之名行詐術之實的犯行近年來已經成為執法機關以及網路使用者共同的夢魘。根據跨國之非營利組織商業改進局（Better Business Bureau）於西元2019年所做的調查報告，前十大最具風險的商業騙術中，包含了求職陷阱、網路購物詐騙、空頭支票等，其中虛擬貨幣詐欺排名第二，僅次於求職陷阱，網路購物詐騙則名列第三，據統計，共有32%的騙術涉及了虛擬貨幣的交易（包含商品、服務或其他法定貨幣的交換）[54]。

與前述利用虛擬貨幣洗錢或以虛擬貨幣為犯罪目標的犯罪行為不同的是,前開兩類的犯罪行為多半是濫用或規避虛擬貨幣本身的系統技術與設置，相對的，以虛擬貨幣為名的犯行則往往不涉及虛擬貨

[53] 臺灣臺北地方檢察署108年度偵字第2540號、第3280號、第3452號、第20536號、第21008號、第22474號起訴書參照。

[54] *New Risks and Emerging Technologies*, BBB SCAM TRACKER RISK REPROT (2019), https://www.bbb.org/globalassets/local-bbbs/council-113/media/bbb-institute/riskreport2019/2019-scamtracker-riskreport-digital.pdf (last visited Oct. 11, 2020)

幣技術的本體，而是看準潛在被害者對於虛擬資產欠缺必要的認識並加以利用，藉虛擬貨幣之名，讓要約顯得獲利可期，進一步誤導被害者，讓他們相信投資可以獲得可觀的報酬。對於偵查機關而言，這樣的區別往往也意味著調查重點與挑戰的不同：以虛擬貨幣為名的犯行，與其他詐騙行為並無本質上的不同，重點在犯罪嫌疑人於是否傳遞與事實不符的訊息，並使被害人陷於錯誤而交付財物；至於利用虛擬貨幣洗錢或以虛擬貨幣為犯罪目標的犯罪行為，偵查人員於具體個案中，對於行為人如何規避或濫用虛擬貨幣之運作設置與交易機制，務須精確掌握，才能有效查緝，這個部分也是偵查機關偵辦是類案件最感棘手之處，以下即就偵查機關所可能遭遇之困境，以及可資應對之偵查作為分別說明之。

柒、 虛擬貨幣犯罪之偵查

一、 偵查困境概說

對於偵查者而言，如何破解虛擬貨幣交易的匿名性，無疑是首當其衝的難題。虛擬貨幣犯罪行為人經常利用匿名性的特性隱匿其真實身分以規避查緝，更為棘手的是，這樣的匿名性往往是多重的：(一)首先，行為人可能利用「洋蔥路由器」（The Onion Router，TOR）或類似的匿名通信軟體，透過多層加密方式（故以洋蔥為喻）包裹通訊與交易內容，藉此隱匿 IP 位址或網路使用者身分，使網路使用者可以在不被得知 IP 位址的情況下，將原始資料發送至目標位址；(二)其次，不同的虛擬貨幣，其匿名性的程度也有差別，行為人可能會選

擇能夠最大限度允許持有者及交易對象隱匿真實身分的虛擬貨幣進行交易；（三）再者，即使許多的虛擬貨幣交易所為了配合洗錢防制政策，開始使用實名制的身分驗證機制作為開立帳戶及進行貨幣交易的條件，但行為人仍可能想辦法規避實名制的要求，創造假帳號為之[55]。層層交織的各種匿名機制使得犯罪行為人的身分確認愈加困難重重。

即使能夠成功追查到犯罪嫌疑人的真實身分，犯罪偵查機關依然面臨一個艱難的挑戰，那就是虛擬貨幣犯罪往往是跨越國界的，以至於個案中的關鍵證據與犯罪嫌疑人可能四散多國，甚至完全不在我國境內，而且證據或嫌疑人所在國家與我國之間也未必有司法互助的協定，抑或者根本是敵對狀態，這使得偵查進度可能因為管轄權的因素大受阻礙，進而影響犯罪訴追。

以近年來備受矚目的 Mt. Gox 交易所遭駭事件為例，該案發生於西元 2014 年，犯罪嫌疑人的真實身分屢有爭議，據稱是由一名俄國籍的男子 Alexander Vinnik 所為，他於西元 2017 年在希臘被逮捕，此後二年都被拘禁在希臘，接著又被引渡至法國受審[56]；雖然其逮捕是依據美國政府所核發的拘捕令，且美國政府也一直爭取將

---

[55] Claire Nolasco Braaten & Michael S. Vaughn, *Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions*, DEVIANT BEHAVIOR (2019), https://doi.org/10.1080/01639625.2019.17060706 (last visited Oct. 11, 2020)

[56] *See* Gaspard Sebag, *Russian Bitcoin Suspect Charged in France After Greek Extradition*, BLOOMBERG.ORG, https://www.bloomberg.com/news/articles/2020-01-28/russian-cyber-suspect-charged-in-france-after-greek-extradition; Mathew Hrones, ***The Man Behind the BTC-e Exchange***, BITCOINIST.COM, https://bitcoinist.com/russian-national-arrested-in-greece-with-ties-to-money-laundering-btc-e-mt-gox-theft/; *Greek Courts Supports Extradition of Former BTC-E Operator Alexander Vinnik*, NEWS.BITCOIN.COM, https://news.bitcoin.com/greek-court-supports-extradition-former-btc-e-operator-alexander-vinnik/ (all last visited Oct. 11, 2020)

Alexander Vinnik 引渡回國受審，但 Alexander Vinnik 至今仍未在美國境內經歷過任何一天的司法訴追程序，其在該案件中的角色為何、是否確須為該案負責等犯罪事實，也一直無法獲得釐清。

可以想見的是，如何確認犯罪嫌疑人的真實身分、如何有效蒐集、保全與扣押證據、如何確保犯罪嫌疑人可以在臺灣接受調查、受審與執行刑罰、如何查扣並沒收犯罪所得等，在虛擬貨幣犯罪的案件中，必然會對司法機關帶來很大的衝擊與挑戰，再加上臺灣在國際間的處境特殊，在在都將使得執法人員所面臨的困境更為險峻。

二、 偵查作為倡議

（一） 打破匿名性的迷思

虛擬貨幣世界的匿名性究竟是不是如此堅不可破呢？其實，比特幣社群中的技術人員曾向幣圈的成員提出警告，說明無堅不摧的匿名性從來不是原初規劃與設計比特幣網絡的目標[57]，這似乎已經暗示著虛擬貨幣的匿名性或許只是種迷思，犯罪偵防人員若能掌握關鍵的拼圖，應該能夠成功拼湊出犯罪嫌疑人的真實身分。

首先，可用以追查犯罪嫌疑人真實身分的相關資訊，其實可能早已被公開揭露於網際網路，這是因為並非所有的網路使用者都充分認知到妥善保管敏感資訊的必要性，這些敏感資訊包含郵寄地址、電子郵件、IP 位址、虛擬貨幣及電子錢包位址等，甚至包含可以處分虛擬貨幣所需的私鑰，都可能由於資訊持有者缺乏保護意識而自行揭露

[57] *See* Fergal Reid & Martin, *An Analysis of Anonymity in The Bitcoin System* (2011), https://users.encs.concordia.ca/~clark/biblio/bitcoin/Reid%202011.pdf (last visited Oct. 11, 2020)

於網路世界中。若是能搭配適當的網路工具，例如強力的搜尋引擎及分析工具，執法人員便可加以蒐集、分析、比對這些公開的資料，進而查知所欲追捕的犯罪嫌疑人身分。

其次，雖然虛擬貨幣本身具有去中心化的特性，但經手虛擬貨幣的組織或機構則不盡然，換句話說，這些組織或機構為了提供與管理其服務所需，往往具有集中管理與驗證的機制，這也成為犯罪偵防人員得以突入的破口。舉例言之，接受虛擬貨幣作為支付工具的網路商店、虛擬貨幣交換中心、提供虛擬貨幣電子錢包的平台等，為了提供相關服務，可能會有徵信、與銀行金融往來、身分認證或者貨品遞送之需求，也因此往往持有得以辨識使用者身分的相關資訊，例如信用卡卡號與持有者、銀行帳號、電子郵件、IP 位址、寄送地址等，以及使用者在該網站的歷史活動紀錄；此外，由於洗錢防制基本上已為全球潮流，為了配合各國政府打擊洗錢犯罪的政策，許多經手虛擬貨幣的平台都已具有身分驗證的實名機制，使用者必須註冊並通過實名身分驗證，方能於該平台上進行虛擬貨幣交易[58]，這也意味著虛擬貨幣的匿名性並非絕對，如果偵查機關能依法取得是類資訊，勢必有助於清查特定虛擬貨幣交易所涉及的相關人員真實身分[59]。

上開為完成服務而由管理機構持有的資訊，根據服務條款的內容，使用者可能於使用服務之初，即已同意服務平台於必要時得提供執法機關使用，這將非常有利於犯罪偵防機關之查緝行動。因此，每遇有

[58] 至於現實上這種實名驗證機制能發揮多少把關的功能，是另一個層次的問題。在一些對虛擬貨幣管制政策比較寬鬆或甚至欠缺管制敏感度的國家，這種驗證機制也可能只是徒具形式。例如最高法院 106 年度台上字第 4184 號刑事判決中之被告，即係以電腦及印表機合成「中華人民共和國居民身分證」，並持偽造之身分證向比特幣網站人員進行視訊認證，以此方式虛設比特幣人頭帳戶，以利遂行其等洗錢之犯罪行為。

[59] *Supra* note 57.

需向管理機構調取清查犯罪嫌疑人真實身分所需的資訊時，首要之務即在確認服務條款中是否已經有此類同意使用之約定。

至於服務條款沒有同意提供執法機關使用的相關約定時則相對棘手，但並非沒有對應之道。美國立法部門依據資訊種類與服務提供者的不同、是否曾經政府機構的事前通知等，制定了相應的規範，各有寬嚴不一的實體及程序要件，執法機關須視情形取得法院核發的令狀（warrant）或法院命令（court order）以調取所需資料，亦可能經法律授權而自行開立傳票（subpoena）命資訊持有者提供，茲將相關規定擇要說明如下，以資對照借鏡。

依據美國聯邦刑法典第 2701 條至第 2712 條(即儲存通訊紀錄法，Stored Communication Act，SCA）之規範，執法機關如欲要求網路服務提供者（Remote Computing Service，RCS）[60]提出資訊時，不論是網路服務使用者於網路服務平台上「涉及通訊內容」之資訊，包含使用者的瀏覽歷史（searching histories）、在平台的紀錄檔案（logfile）等，或者網路服務使用者之姓名、地址、付款方式與來源（包含信用卡號及銀行帳號）等關於身分識別而「未涉及通訊內容」之資訊，原則上都需要取得法院核發的令狀(warrant)[61]；其中，針對通訊內容之調取，最多只能向前調取 180 天內之通訊紀錄[62]。此外，如果執法機關是依據法院核發之令狀調取通訊內容，則不必於調取前先行通知網路服務使用者[63]。

---

[60] *See* 18 U.S.C. § 2711(2). 依照該條款之定義，原則上所有提供虛擬貨幣服務的平台，都能為此處之所稱之「網路服務提供者」涵括。.
[61] 18 U.S.C. § 2703(a), 2703(b).
[62] 18 U.S.C. § 2703(a).
[63] 18 U.S.C. § 2703(b)(1)(A).

針對「未涉及通訊內容」之資訊，除了依據法院核發之令狀調取外，也允許執法機關依法院命令（court order）為之；如果所調取者為使用者之姓名、地址、通聯紀錄（號碼、發話與通話時間）、網路位址、身分證號碼、付款方式與來源等資訊，執法機可以僅憑法律授權之行政傳票（subpoena）命網路服務提供者提出。原則上，調取「未涉及通訊內容」之資訊前，執法機關均毋庸先行通知網路服務使用者[64]。

有別於向法院聲請令狀(warrant)需要符合較為嚴格的要件(例如相當理由、犯罪事實之與罪名之特定等)，聲請法院核發調取命令（court order）則相對容易，惟執法機關仍須向法院釋明特定的關聯事實（specific and articulable facts），以說明犯罪偵防機關確實有合理的根據（reasonable grounds）相信欲調取的資訊是犯罪調查得以持續進行的相關素材（relevant and material）[65]。

以上說明係針對美國執法機關向網路服務提供者調取資訊時所需符合之相關實體及程序要件，但美國聯邦刑法典儲存通訊紀錄法同時也規定，在特定情況下，網路服務提供者可「主動」、「自願」向執法機關提供相關資訊。基於保護個人資料之需，網路服務提供者原則上禁止提供資訊予包含執法機關在內之第三人，然而，當通訊內容為網路服務提供者善意取得（inadvertently obtained），且其內容顯示與犯罪相關時，則不在禁止之列[66]，這對執法機關來說可以省去許多向法院周旋以取得令狀的精力與時間，因此，如何與網路服務提

[64] 18 U.S.C. § 2703(c)(3).
[65] 18 U.S.C. § 2703(d).
[66] 18 U.S.C. § 2702(b)(7).

供者建立共識並促其善盡守門人之責，亦是執法機關需要善加耕耘之處。

相較於美國立法部門所為細膩甚至可說是繁雜的規範，臺灣立法實務目前對此一領域之規定尚屬單純，原則上，如屬通訊保障及監察法所保護之通訊內容或通信紀錄，偵查機關須依該法規定向法院聲請調取，或於符合例外的情況下不待法院核可而職權調取[67]；如果偵查機關所需之資訊非屬通訊保障及監察法所保護之內容，在符合個人資料保護法對於個人資料之蒐集、處理及利用所定要件[68]下，當可逕向虛擬貨幣交易所等網路服務提供者發函調取。

至於未來修法方向為何、是否仿照美國立法實務針對資訊種類之不同訂定寬嚴不一之調取要件，國內目前尚乏相關之討論與共識。在此部分立法尚屬真空的情形下，偵查機關似宜先期沙盤推演各種可能之偵查困境、所需之偵查手段與相應之法律授權，積極擬具法案並參與法制形成，避免立法結果過度悖離與箝制偵查實務，尤其可考慮引入美國法制關於網路服務提供者於特定條件下可主動提供與犯罪相關之資訊予偵查機關之規定，以利偵查作為之開展。

（二） 跟著金流走

雖然行為人違犯虛擬貨幣犯罪的動機難以數計，但幾乎所有的虛擬貨幣犯罪，不論是利用虛擬貨幣買賣毒品或是買兇殺人，其犯罪階

[67] 通訊保障及監察法第 3 條、第 3-1 條、第 11-1 條規定參照。
[68] 個人資料保護法第 15 條至第 18 條規定參照。

段原則上都會涉及虛擬貨幣的交易與轉換[69]，這是因為虛擬貨幣表彰了相當的交易價值[70]，且虛擬貨幣最初被創造的目的之一，就是意欲作為交易工具使用，也因此，不論行為人利用虛擬貨幣的交易與轉換遂行了什麼樣的犯罪行為，都必定有虛擬貨幣的金流藏匿於其後。既然所有的金流理論上都有其始點與終點，若能有效追蹤虛擬貨幣的金流，應能帶領偵查機關掌握關鍵證據。

該如何追蹤虛擬貨幣的金流呢？事實上，偵查機關若要掌握金流，關鍵的拼圖之一即是虛擬貨幣在區塊鏈的實際運用。正如本文開頭所述，虛擬貨幣利用區塊鏈的技術，使每個貨幣自創造尹始迄今的所有歷史交易紀錄，全都按照發生時序被留存於區塊鏈帳本中，並持續不斷地被參與的「礦工」更新，而且一旦交易紀錄被加入帳本中，就不會再被移除，亦無從被竄改；更重要的是，這些紀錄都是「公開」的，也就是說，只要能充分掌握區塊鏈揭示的公開訊息，偵查機關甚至不需要搜索票或調取票，就形同握有了一份詳實記載虛擬貨幣移動軌跡的地圖，這份地圖包含了交易雙方的錢包地址、交易序號、時間、金額與手續費等交易細節。只要透過必要的技術與設備支援，例如利用所謂的區塊瀏覽器（Blockchain Browser，一種可用以查詢區塊鏈上所有交易資訊的瀏覽器），偵查機關即可蒐集與嫌疑人有關的各種交易細節。

需要加以說明的是，區塊鏈上固然能夠查得全部的歷史交易訊息，但這也僅僅限於「鏈上交易」（on-chain transactions），也就是

[69] 比較例外的情形應該是純以虛擬貨幣作為「幌子」的犯罪類型，由於此等犯行主要是利用潛在被害者卻乏虛擬資產的相關認識並使其陷於錯誤，然而現實上可能根本不存在行為人所稱之虛擬貨幣，自然也就沒有虛擬貨幣的金流可言。

[70] *Supra* note 34.

曾經透過區塊鏈驗證的交易才會被記錄於其中;如果交易是發生在中心化交易所，其用戶在該交易所內彼此進行交易，交易的驗證與記帳是由該中心化的交易所進行而未予以「上鏈」，這種「鏈下交易」（off-chain transactions）的交易資訊就不會出現在區塊鏈中。也就是說，如果僅僅侷限於追查區塊鏈的交易資訊，金流很可能出現斷點，畢竟有心利用虛擬貨幣交易機制掩飾真實身分以利遂其犯行的行為人，往往也熟知區塊鏈的特性，其等為了躲避追查而刻意製造斷點，要屬尋常之事，這也意味著偵查機關除了掌握區塊鏈訊息外，往往還需要輔以其他資訊以利分析、比對，才能拼湊完整的交易細節，進一步追查資金流向及犯罪嫌疑人真實身分。所謂的「其他資訊」，就是本文上個段落提到的「可用以追查犯罪嫌疑人真實身分而存在於各個中心化的交易所、網路商店等網路平台上的相關資訊」，透過取得這些中心化的機構所掌握的訊息，與區塊鏈上的交易訊息加以比對，偵查機關才有可能將一連串看似亂碼排列的錢包地址，連結至現實生活中的具體個人。

既然虛擬貨幣的犯罪偵防與整個貨幣鏈內鏈外的網絡息息相關，建置虛擬貨幣犯罪防制資料庫之必要性已不言可喻——利用類如毒品或人口販運資料庫之分析工具，將手上握有之交易細節及身分相關資訊與歷史資料進行分析、比對，並將比對結果與執行所得等偵查成果逐步累積、更新，藉此提升資料庫之完整性。此一虛擬貨幣犯罪資料庫，其規模應盡可能地朝國際合作與資料共享之方向建置，這是因為虛擬貨幣犯罪往往具有跨越國界的特性，如果資料庫的內容僅僅侷限於單一國家之內，甚至一切從零開始累積，則犯罪偵防之進展也

必定大受限制，相對的，若是能在其他國家所累積的成果上前進，勢必能夠事半功倍。

面對不斷升級進化的虛擬貨幣犯罪、不斷擴張的貨幣網絡，在可預見的未來，虛擬貨幣的金流追查勢必會碰上新的困境，偵查機關須為長期抗戰做好準備；如果不是透過跨國資料庫的建置，偵查成果將無法有效率地累積，使得所有案件都將從零開始，面對層出不窮的新挑戰，恐怕都將治絲益棼。

（三） 建立扣押與變價機制

除了用以追緝犯罪嫌疑人之外，追查虛擬貨幣金流最重要的目的之一，在於犯罪所得之扣押，以利沒收等後續執行事宜；如果僅僅是進行犯罪偵查與訴追，而不為犯罪所得之扣押與沒收，對於虛擬貨幣犯罪之遏止顯然無濟於事。

虛擬貨幣由於轉換容易，且易於藏匿交易軌跡，更為根本的是，其既名為「虛擬」，本質上只是一組數位序列的排列組合，存在於去中心化的、無實體的網路世界中，其在扣押與沒收程序之進行上，勢必與傳統犯罪所得之扣押與沒收有別，而須另為不同之處理。舉例言之，傳統金融犯罪之犯罪所得扣押，多半是以扣押被告名下或其所直接、間接控制之實體財產與金融帳戶作為手段，若扣押之標的為金融帳戶，金融機構依據司法機關之扣押命令凍結相關帳戶，即可達到避免被告脫產以及保全後續執行之目的，問題是，虛擬貨幣本身沒有中心化的管理機構，偵查機關即使核發或取得了扣押命令，也不知該向

何人或何機關送達以及執行，則偵查機關究竟應該如何才能有效扣押虛擬貨幣以防免嫌疑人脫產呢？

要有效進行虛擬貨幣之扣押，首先必須要瞭解「錢包」的概念。虛擬貨幣世界中所謂的錢包，相當於金融帳戶，是可以用於存取多個虛擬貨幣位址的檔案夾，也是擁有與處分虛擬貨幣的前提，它會持續地與區塊鏈進行「對帳」並更新錢包內之虛擬貨幣收支結餘，有些錢包也提供存放與保管「私鑰」的功能。錢包可以多種不同之形式存在，最常見的是所謂的「錢包程式」（software wallets）[71]，使用者可將程式下載應用程式至電腦或手機等裝置後進行虛擬貨幣交易；有些錢包則以「錢包網頁」（web-based wallets）或「線上錢包」（online wallets）[72]的形式存在，使用者須至網頁輸入帳號及密碼登入後，方得存取與處分虛擬貨幣；還有一種有別於線上錢包的「離線錢包」（offline wallets or cold storage wallets），也是目前被認為相對安全的虛擬貨幣錢包，通常是將虛擬貨幣位址以及用以處分貨幣之私鑰一起保存在離線之實體硬碟中[73]，以避免網路系統漏洞所可能導致的駭客入侵或私鑰遭竊。據此，在進行虛擬貨幣扣押時，首先必須要辨識嫌疑人所使用之錢包種類為何，如果是離線錢包，須留意嫌疑人所持用外觀看似隨身碟之存取裝置，特別是裝置上顯示若有 12 至 24 字元之亂碼英數組合，或是條碼、QR CODE 等，則該裝置即有可能為離線錢包，應扣押作為證物。若嫌疑人未使用離線錢包，可檢視其持用之電腦或手機桌面是否有錢包應用程式之捷徑，如果發現疑

[71] 常見之錢包程式有 Armory、Bitcoin Core、MultiBit-HD 等。
[72] 知名之線上錢包例如、Mycelium、Greenbits、Airbitz 、Coinbase、GDAX、Gemini、Kraken 等，其中具有 Coinbase 和 GDAX 具有身分驗證機制，且與美國執法部門曾有合作關係。
[73] 例如 Ledger 或 TREZOR，具有類似隨身碟的外型，也因此被稱作實體錢包。

似為錢包程式之圖樣，應將手機或電腦設備扣案。若嫌疑人未使用離線錢包或錢包程式，則應進一步查閱其網頁瀏覽歷史，確認是否曾造訪並使用線上錢包網站；值得注意的是，如果嫌疑人使用的是線上錢包，該提供錢包之網站往往也留有嫌疑人之註冊與登入資料，及該錢包之歷史交易紀錄，對於偵查機關而言，極具證據價值，宜併向該網站調取之；此外，如果該網站亦兼具虛擬貨幣交換所的角色，且嫌疑人亦曾在該交換所進行交易，通常也表示虛擬貨幣去中心化及匿名之特性在此有所緩和，交換所將可能協助凍結與扣押嫌疑人之虛擬貨幣錢包，以阻止嫌疑人進一步處分錢包內之虛擬貨幣。

成功扣押虛擬貨幣之關鍵在於速度，一旦決定了要進行扣押，就必須迅速而精確地將存放虛擬貨幣的錢包，以及處分貨幣所需之私鑰，併同扣案。另一個關鍵之處在於——建置由執法機關所管領專供扣押與執行沒收所用之虛擬貨幣錢包，於扣得嫌疑人錢包的當下，即刻將錢包內之虛擬貨幣移轉至執法機關所掌管的錢包中，這是因為僅僅只是扣押犯罪嫌疑人所持用電腦主機與手機等電子設備，甚至連犯罪嫌疑人都被羈押了，也依然不足以防免嫌疑人脫產，因為其所持有之虛擬貨幣，仍可能被遠端掌握虛擬錢幣位址及私鑰的第三人進行處分[74]，故唯有即刻將扣得之虛擬貨幣移轉至執法機關之錢包，並產生新的私鑰，才能確保所扣得之虛擬貨幣無法被執法機關以外之人所處分[75]。

[74] 唯一的例外可能就屬實體錢包，因為實體錢包為帶有私鑰之離線裝置，且獨一無二，扣押了實體錢包基本上即可確保虛擬貨幣不會被處分。

[75] 依筆者所瞭解，我國目前針對虛擬貨幣之扣押所使用之工具多為實體之硬錢包，藉以避免線上錢包可能遭駭之危險，此外，私鑰部分亦拆分由複數承辦人員分別保管，以求分散風險。

從上所述，可以想見「私鑰」在扣押程序中扮演的重要性，如果少了犯罪嫌疑人的私鑰，整個扣押程序恐怕功虧一簣。問題在於，現實狀況往往並不盡如人意，執法機關未必能於搜索、扣押之過程中順利發現所需之私鑰，此時，如果取得受搜索人之同意，經其主動告知或交付私鑰，固然是解決方式之一，但期待所有受搜索人都願意主動配合，顯然不切實際，當遇有搜索未果且受搜索人亦拒絕交付私鑰之情形時[76]，執法機關究竟有何手段以資因應？針對此一困境，美國司法實務是以向法院聲請調取命令之方式，命犯罪嫌疑人解鎖錢包及提出私鑰，而臺灣目前之立法與司法實務在此一議題上仍屬空白，現階段恐屬無解，未來或可考慮引進類似美國以法院命令強制提出之立法例以資因應[77]。

成功扣押虛擬貨幣之後，接下來的難題便是如何變價。臺灣司法實務目前在此一領域所累積之經驗仍然相當有限，比較為人熟知的案例應為臺灣臺中地方檢察署於民國 107 年 12 月 25 日所進行之比特幣變價拍賣程序，也是臺灣首次進行之虛擬貨幣變價程序。該次拍賣的比特幣為被告等違反銀行法等案件[78]中之犯罪所得，查扣當時在幣託

---

[76] 實際發生之案例如：「被告有將其收取之人民幣及新臺幣款項用以投資虛擬貨幣等情，業經被告自陳屬實，是被告因地下匯兌所得之獲利，應非僅前開犯罪所得，亦包括投資虛擬貨幣之獲利，然因本件因被告始終拒絕提供扣案手機密碼供查證，亦拒絕提供虛擬貨幣相關對帳紀錄，致無法證明被告投資虛擬貨幣之金額及獲利，而無從針對其投資虛擬貨幣之獲利聲請沒收。」臺灣橋頭地方檢察署 109 年度偵字第 2037 號起訴書參照。

[77] 當然，即使引進了這樣的立法例，也無法保證必定能從嫌疑人口中獲取私鑰，因為違反這類提出命令的罰則有限，多半是課以罰鍰或是予以短暫的人身拘束，這對於透過虛擬貨幣犯罪而獲得龐大利益的嫌疑人來說，根本無關痛癢，但無論如何，這樣的規範至少讓司法機關多了一個可資使用的手段以有效扣押虛擬貨幣。除了提出命令之立法例外，亦可考慮比照貪汙治罪條例關於自動繳交犯罪所得可減輕其刑之立法模式，藉以提高被告主動交付私鑰之動機。

[78] 犯罪事實略為：被告等以 IRS 國際儲備體公司（International Reserve System，IRS）為名，架設「儲備系統」網站，並設計內部計價單位 RM（Reserve Money），對外宣稱可推動比特幣匯率之穩定發展，佯以「不論比特幣漲跌都能獲利」、「IRS 推動普及比特幣」、「IRS 目的是儲積大部分的比特幣總量以積極影響比特幣市場」云云招攬投資，在短短的 9 個月吸金達約新臺幣 15 億元、被害人數約 1,000 餘人，被告等人再將所獲得之部分鉅額資金轉購比特幣。嗣於 107

網站（www.bitoex.com）之交易價格為每顆 6,000 至 7,000 美元，經被告同意每顆以最少 5,000 美元為起拍價進行變價，惟因貨幣市場交易價格波動劇烈，拍賣當日每顆均價未達被告同意之起拍價格，致未能成功變價。雖然該次拍賣因故未能變價成功，但其經驗對於將來執行虛擬貨幣之拍賣依然極具參考價值，因為該檢察署為使拍賣程序順利完成，事前已與法務部調查局及虛擬或交易平台業者就帳戶及資金流之實名制進行多次研議，以建立拍賣虛擬貨幣之標準作業流程，其中包含投標人須先簽署承諾書，保證其可供接收比特幣之電子錢包確為其本人所持有，且拍定價金之支付方式限於以拍定人本人、配偶或直系親屬名下之帳戶轉帳，以及不接受現金繳納等作業準則，藉以防制有心人士藉此拍賣程序進行洗錢[79]。未來如有執行虛擬貨幣變價程序之必要，當可借鏡。

誠然，虛擬貨幣的變價難題不只有未達同意起拍價格而已，甚至連是否適宜進行變價，都有爭論，而此一爭論，肇始於虛擬貨幣史上數一數二著名的變價行動——FBI 於西元 2014 年 6 月間起拍賣查扣自 Ross Ulbricht 架設經營「絲路」網站所獲得之犯罪所得，首次進行拍賣之比特幣數量約 3 萬顆，按當時市值計算，價值高達約 1,800 萬美元（折合新臺幣約 54 億元）。數額如此龐大的比特幣拍賣消息甫一公布，市場投資人擔心拍定人可能即刻大量出脫比特幣，致價格

年 6 月間，IRS 網站無預警關閉，導致大量投資人血本無歸。案經承辦檢察官指揮調查局於 107 年 6 月 13 日發動搜索，並依臺灣臺中地方法院裁定而扣押被告等人所有之比特幣共 197 餘顆、乙太幣 8.3 顆。臺灣臺中地方檢察署 107 年度偵字第 17312 號起訴書參照。另拍賣當時，該案雖仍在法院審理中，然該檢察署考量比特幣價格易隨時間經過嚴重貶損，遂於案件確定前先行變價以保存其價值。

[79] 相關新聞可參閱：https://www.tcc.moj.gov.tw/media/167059/81226111028756.pdf?mediaDL=true。（最後瀏覽日期：109 年 10 月 6 日）

跌落，且其他人將難以銷售所持有之貨幣，引發全球恐慌性拋售，比特幣市值隨即應聲下跌約 7%；該次拍賣之比特幣最終由一人全數購得，且和原先所預期的走勢相反，拍定翌日之市值即漲至約 1,900 萬美元，拍定人帳面上現賺 100 萬美元[80]。這樣的變價行為及所引發的市場價格波動令人質疑：國家機關究竟是否適宜進行虛擬貨幣之變價？變價拍賣程序會否經有心人士利用成為操弄市場價格及獲取暴利之手段？質疑歸質疑，現實上有在進行虛擬貨幣變價程序的國家並不只有美國[81]，理由其實也很容易理解——如果不進行變價，這些扣案的虛擬貨幣將來（於追徵犯罪所得後）勢必得發還被告，那麼司法機關當初大費周章地查扣虛擬貨幣，到底是為了什麼？況且發還犯罪所得的本身，也與既有之沒收法制刑事政策明顯相悖。

以本文前開所提到之幣託網站遭駭客盜取幣特幣之案件[82]為例，被告所盜取之比特幣於行為當時（民國 105 年 6 月間）之市值約新臺幣 5,000 萬元，嗣於提起公訴時（民國 106 年 8 月間），市值已漲至約新臺幣 2 億 5,000 萬元，如果司法機關僅僅因為虛擬貨幣之變價程序有其現實上之疑慮與困難而不予變價，則法院該如何為犯罪所得之沒收宣告？又該如何處置所扣案之比特幣？從被告行為時所造成之侵害與犯罪所得來看，法院似乎應該向被告宣告追徵新臺幣 5,000 萬

[80] *See* https://www.wsj.com/articles/fbi-readies-144-341-bitcoins-for-sale-1402606244, https://cointelegraph.com/news/feds-sell-29656-bitcoins-to-single-bidder-in-silk-road-auction, https://www.businessinsider.com/bitcoin-price-government-auction-winners-2017-5 (all last visited Oct. 11, 2020)

[81] https://news.bitcoin.com/global-law-enforcement-has-auctioned-massive-amounts-of-bitcoin/ (last visited Oct. 11, 2020)

[82] 臺灣臺北地方檢察署 106 年度偵字第 17735 號、第 18963 號起訴書參照。現實上，該案仍在審理中，且被告於該案當中所盜取之比特幣共 2292.85 顆並未據檢警機關扣案，然為具體化虛擬貨幣變價與否之現實困境，以下討論係假設本案比特幣於提起公訴時業經查扣在案，並已審理終結。

元，至於扣案之比特幣，由於並非違禁物，至多僅屬犯罪所生之物，依刑法第 38 條第 2 項規定，屬得沒收之物，然而當被告依法院之沒收宣告繳納新臺幣 5,000 萬元之後，理論上被害人之損害已經獲得填補，被告也已就其所造成的侵害付出相應的代價，法院似乎已無理由再就扣案之比特幣予以宣告沒收，則扣案之比特幣似乎也只能發還予被告，假設被告於領回後加以變賣，以本文撰擬完成時之比特幣價格粗估，總市值約為新臺幣 7 億 1,000 萬，被告帳面上依然淨賺新臺幣 6 億 6,000 萬元。由此看來，如果查扣虛擬貨幣之後不進行變價，可能變相容任犯罪行為人自其犯行獲得龐大利益，這顯然與目前之沒收法制規範框架嚴重牴觸，洵非妥適；但換個角度來看，如果司法機關真的成功將扣案之虛擬貨幣變價，且變價所得遠遠超出被害人於案發當時所受損害，這筆鉅額的利益該由誰來享有？當國家機器因為被告之犯罪行為獲有利益，其在處罰被告以及保有利益的面向上，真的還具有正當性嗎？

無論如何，既然虛擬貨幣之變價看來是勢在必行，從速建立全國一致之變價機制即有其必要性，且其準則內容至少應包含：（1）發動變價之時機，例如應該在偵查或審理中的哪個環節發動？在什麼樣的市場價格區間內發動？以什麼樣的標準決定市場價格？應由被告聲請或由司法機關主動為之？司法機關有無義務在最有利被告之價格區間內進行？或者僅需考量何時進行拍賣最易於變價？（2）拍賣數量，例如拍賣應就扣案之虛擬貨幣一次全部為之？或於特定情形下可分批分次進行？是否限制每次拍賣數量或約當市值總額之上下限？（3）應買人之資格限制，例如是否先繳交保證金？如何決定保

證金數額？是否須備有業經驗證之實名制電子錢包、是否允許代理、如何查核應買人之真實身分？(4)交付價金及移轉拍定標的之方式，包含可否允許以現金應買？是否限定由拍定人本人支付價金以使金流單純化等項目。目前我國對於如何進行虛擬貨幣之變價尚無全國通行之作業準則，為了避免在規範真空的情況下，各地方司法機關各行其事導致執行標準不一甚或有所疏漏，主管機關宜儘速制定相關規範，並參考他國之變價作法，以利將來若有進行跨國沒收之司法互助需求時，雙方能有較為一致的執行標準，此舉對於建立雙邊互惠之跨境合作將能有所助益，詳下述。

（四）　強化跨境合作

由於虛擬貨幣犯罪往往具有跨越國界的特性，為能有效進行偵查作為以遏止虛擬貨幣犯罪，國際間的司法合作毫無疑問扮演了至為關鍵的角色。然而不可諱言地來說，各國必然有其內國之利益考量，國與國之間也多有利益衝突甚至敵對的情形存在，期待各國無私合作打擊犯罪，現實上有其困難。基於這樣的考量，各國就與他國間的司法互助多半是在互惠的前提下進行。

1、　美國實務概況

以美國為例，跨國取證的依據來自形形色色的雙邊互惠條約（Mutual Legal Assistance Treaties，MLATs），其中不只規範了美國執法人員在他國政府的請求下於美國境內進行偵查作為，也規範了外國執法人員在美國政府的請求下，於該他國境內為美國進行蒐證

之行為。雖然雙邊互惠條約理論上使美國執法機關的跨境偵查成為可能，但執行上仍有一些挑戰需要克服。

首先，即使是互惠國，美國政府並不必然都會應允外國政府之證據調查請求，反之亦然。可能影響准允與否的因素諸如：證據調查所涉及的關係人是否為內國或外國進行中的訴訟程序當事人、證據調查之請求是否企圖規避既有的證據蒐集限制或政策、證據調查之請求是否過度侵入主權或造成不公平的負擔、所涉訴訟的性質以及彼此互惠的實踐情形等[83]。

其次，除了前述各種可能影響調查請求准否的因素外，針對個別的證據調查請求，依其類型之不同，也有各自需要符合的法律要件[84]。以向虛擬貨幣交換所等網路服務提供者調取足資追查犯罪嫌疑人之資訊為例，能夠向美國政府請求調查的「外國政府」，必須是「具資格的」外國政府（qualifying foreign government），詳言之，必須是：（1）該外國政府與美國政府之間具有已經生效的執行約定；（2）該外國政府提供予網路服務提供者之實體與程序上權益，須與美國政府基於儲存通訊紀錄法所提供之保障相似[85]。此外，不論所調取之資訊是否涉及通訊內容或僅止於內容以外的紀錄，原則上皆在可請求的範圍內[86]，惟該資訊之所有人必須是該外國政府的國民或居民[87]；如果是請求美國政府核發搜索票，美國聯邦法院法官僅有在證據所涉

---

[83] *See e.g.*, United States v. Global Fishing, Inc., 634 F. 3d 563 (9th. Cir. 2011). 該案涉及美國與俄國間關於刑事司法互助之條約，依據條約內容，兩國在互惠的前提彼此基於請求提供廣泛的協助，包含文件、紀錄等物件之提供，且相應之權責單位有權核發傳票、搜索票、法院命令等為旅行請求所必要之權限。*See also* 18 U.S.C. § 2703 (h)(3).

[84] 18 U.S.C. § 2703 and § 3512.

[85] 18 U.S.C. § 2703 (h)(1)(A).

[86] 18 U.S.C. § 3512 (a)(2)(B).

[87] 18 U.S.C. § 2703 (h)(5)(A).

及的行為於美國境內亦構成可罰的犯罪行為且可受一年以上有期徒刑宣告時，始可核發[88]。

除了五花八門的條約與法律規定外，還有一個更根本的問題是：如何區分什麼是境內或境外取證？這個問題在取證行為涉及網路資訊之調取時尤為尖銳，舉例言之，針對坐落美國境外的美國分公司，美國政府可否將之視同美國境內公司，逕依儲存通訊紀錄法向該分公司調取所需資訊？抑或應循雙邊互惠條約向該分公司所在國家請求之？此一爭議在西元 2018 年雲端法案（Clarifying Lawful Overseas Use of Data Act，CLOUD Act）制定前多有爭議，直至雲端法案通過後，才算塵埃落定。與此爭議有關最著名的案例，當屬 *United States v. Microsoft Corp.* 案[89]。

在 *United States v. Microsoft Corp.* 案中，美國執法機關依照儲存通訊紀錄法第 2703 條之規定向法院聲請令狀，命 *Microsoft* 提出其使用者帳戶之通訊資料（包含電子郵件），*Microsoft* 拒絕提出，動議撤銷該令狀，其理由略為「該電子郵件之內容儲存在愛爾蘭都柏林」，經負責核發令狀之法官駁回其動議，案經 *Microsoft* 就法官裁定提起救濟，地方法院予以維持，*Microsoft* 為此再提起救濟，案經美國聯邦第二巡迴上訴法院撤銷原裁定，認定儲存通訊紀錄法並未授權法院得核發令狀命網路服務提供者提出儲存在美國境外伺服器中之資料，即使該網路服務提供者址設美國境內[90]。而在雲端法案通過後，前開爭議大致上獲得了解決。依據該法案之規定，網路服務

[88] 18 U.S.C. § 3512 (e).
[89] United States v. Microsoft Corp., 583 U.S. (2018).
[90] *Id.*

提供者原則上有保存、備份、提出其所持有、監督、控制包含通訊內容及其他相關紀錄在內之通訊資料之義務，不論這些通訊資料儲存在美國境內或境外[91]。此一法案可謂大大地便利了美國執法機關境外取證之便利性。

理論上，網路服務提供者有依據雲端法案向執法機關提出所需資料之義務，但此一義務是否係屬絕對？網路服務提供者得否為反對之表示？為了兼顧內國與他國之利益衡平，當外國之網路服務不願提出其所持有之資訊，雲端法案規定該網路服務提供得提出動議拒卻或修正提出之請求，而法院則於符合以下情形並認為適當時，得予撤銷或修正提出資料之請求[92]：（1）揭露資料之請求將導致外國網路服務提供者違反該國之法律；（2）所調取資料之所有人並非美國公民，亦未居住於美國境內；（3）依據整體情狀（totality of the circumstances）觀之，系爭調取之請求應該被撤銷或修正[93]。

以上這些所謂「顧及內國與他國之利益衡平」所做的規定，終究是從美國本身的國家利益出發，外國政府對於資訊揭露與否勢必會有截然不同甚至敵對的看法[94]，期待每個外國政府與外國網路服務提供者都願意遵守雲端法案的遊戲規則顯然是不切實際的。舉例言之，當美國法院與歐盟委員會（European Commission）針對位在歐洲的網路服務提供者所為之資訊提出與否決定牴觸時，究竟何者的決定勝出？

---

91 18 U.S.C. § 2713.

92 18 U.S.C. § 2703 (h)(2).

93 可能影響法院決定的整體情狀因素諸如：外國政府避免揭露不得揭露之訊息之利益、所請求揭露之資訊對於調查程序進行之重要性、是否可能透過其他可以造成更小損害與負面效應之取證方法而及時、有效地取得證據等。同前註。

94 例如歐盟成員所遵守之一般資料保護規範(the General Data Protection Regulation)對於向第三方國家取證之實體與程序規定，便與雲端法案之規定有所不同。 *See* GDPR Art. 44-50.

對於此一困境，雲端法案並沒有給出任何清楚的答案，事實上，這個問題根本不是雲端法案所能解決的，而是必須仰賴司法案例的累積以及國與國之間的持續雙向溝通、合作、妥協。

2、 臺灣實務概況

為了因應與日俱增的跨境合作需求，我國特別制定《國際刑事司法互助法》以資應對，針對刑事司法互助之原則、主管機關、請求範圍等事項為總則性之規定，其中明白揭櫫刑事司法互助，應在相互尊重與平等之基礎上，本於互惠原則[95]，依條約為之；如無條約或條約未規定者，依本法規定；本法未規定者，適用刑事訴訟法及其他相關法律之規定[96]；至於互助之範圍，則包含取得證據、送達文書、搜索及扣押、沒收或追徵之執行、犯罪所得之返還[97]等，基本上偵辦虛擬貨幣犯罪所可能涉及的各種偵查作為，均已含括在內。至於我國香港及澳門間之司法互助事項，則準用本法之規定[98]。需要留意的是，本法雖為內國法，但在刑事司法互助上仍具有補充法源之地位，於司法互助個案中，縱使與他國之間存有互惠協定或備忘錄，仍須注意請求事項有無違反本法規定之處，例如當他國請求事項對於我國主權、安全、國際聲譽有危害之虞，或者提供協助有使人因種族、國籍、性別、宗教、階級或政治理念而受刑罰或其他不利益處分之虞，我國「應」拒絕提供協助[99]。

[95] 國際刑事司法互助法第 5 條。
[96] 國際刑事司法互助法第 2 條。
[97] 國際刑事司法互助法第 6 條。
[98] 國際刑事司法互助法第 36 條。
[99] 國際刑事司法互助法第 10 條。

雖然《國際刑事司法互助法》明定刑事司法互助應依條約為之，然臺灣由於國際地位特殊，十分不容易透過簽訂國與國雙邊互惠條約的方式建立與他國之間的司法互助法源依據，在跨境合作上所遭遇的挑戰尤為艱難，所幸在政府各部門多年來的努力下，臺灣在打擊跨國犯罪活動上的實力為國際社群有目共睹，各國也逐漸體認到臺灣在跨國犯罪防制網絡中的重要性，陸續透過簽訂備忘錄或互惠協定等方式，建立了司法互助的管道。

目前臺灣與美國間的跨境合作，主要係依據《駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定》，此乃雙方基於相互尊重、互惠與共同利益，藉由刑事事務之司法互助，以增進雙方所屬領土內執法機關有效合作之目的而簽訂。依照協定之內容，雙方將彼此提供有關調查、追訴、犯罪防制及相關刑事司法程序中之相互協助，所稱之「互相協助」，其範圍則包含取得證言或陳述、提供作為證據所用之文件、紀錄及物品、確定關係人之所在或確認其身分、為作證或其他目的而解送受拘禁人、執行搜索及扣押之請求、協助凍結及沒收資產、歸還補償、罰金之執行程序等，以及不違反受請求方所屬領土內法律之任何形式之協助[100]，惟在特定情形下，例如請求之執行將有害於受請求方所屬領土內之安全、公共秩序或類似之重要利益時，受請求方得拒絕提供協助[101]。基此約定，有關打擊虛擬貨幣犯罪所可能涉及到的偵查作為，原則上均在相互協助之範圍內。

[100] 駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定第 2 條。
[101] 駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定第 4 條參照。但仍應注意有無國際刑事司法互助法第 10 條第 1 項所定「應」拒絕提供協助之情形。

詳言之，如果我國偵查機關為確認犯罪嫌疑人之真實身分所需，認有必要請求位在美國境內之虛擬貨幣交換所提供與嫌疑人有關之帳號、交易紀錄與地址等資訊時，即可依前開協定，請求美國政府提供其所持有「得公開之紀錄」，包括任何形式之文件或資料；惟所請求者如屬「不公開之紀錄」，則僅在我方對待美方相同的程度及條件下，請求美方予以提供[102]。如果偵查機關有在美國境內發動搜索虛擬貨幣交換所乃至於扣押虛擬貨幣之必要時，亦可依該協定請求美國政府指定之代表人執行之[103]；除了請求扣押虛擬貨幣以供證據之用外，若我方偵查機關知有虛擬貨幣犯罪所得在美國境內，且美國法律規定亦得予沒收時，得通知美方採取適當行動，包含為沒收、求償、罰金執行等程序之相互協助，以及在此等目的下暫時凍結之虛擬貨幣之行為，以及在適當情形時移轉虛擬貨幣，或變賣虛擬貨幣後之所得予我方[104]。據此，我國偵查機關不只能向美國請求提供偵查所需之資訊，甚至可以請求及時扣押甚至變賣虛擬貨幣，避免犯罪嫌疑人脫產，以利司法程序後階段之沒收與執行程序，如果能善加運用，必能有效打擊虛擬貨幣犯罪。

除了與美國訂有前開司法互助協定外，我國與越南及菲律賓之經濟文化辦事處亦簽有司法互助協定，協定之精神及內容與和美國所簽訂者相當接近，均可援引為請求調取與打擊虛擬貨幣犯罪有關證據之依據。至於未與我國簽訂司法互助協定的國家，如有相互請求調取證據之需求，或許可考慮援引我國調查局與世界各地金融情報中心所簽

[102] 駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定第 10 條參照。
[103] 駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定第 15 條參照。
[104] 駐美國台北經濟文化代表處與美國在台協會間之刑事司法互助協定第 17 條參照。

訂之備忘錄[105]作為請求之基礎，雖然這些備忘錄之簽訂多半是緣於共同打擊洗錢犯罪以及恐怖攻擊之目的，但由於虛擬貨幣犯罪也經常涉及洗錢或洗錢相關之前置犯罪，也因此有了依據洗錢犯罪防制備忘錄向他國請求調取證據之基礎。至於未涉及洗錢及其相關前置犯罪之虛擬貨幣犯罪，在目前臺灣與他國之司法互助架構下，恐形成無法可循之真空狀態[106]，根本解決之道，還是必須持續地與他國建立跨境合作機制。

捌、 心得與建議

從虛擬貨幣問世以來，世人對於虛擬貨幣及其相關之交易與技術應用所投注的熱情不減反增，而且看似沒有盡頭，這也意味著防免虛擬貨幣遭有心人士濫用已成為執法人員無法停歇的任務。洗錢以及與洗錢相關之犯罪固然是最令人擔心的虛擬貨幣犯罪，但以虛擬貨幣為犯罪標的或以虛擬貨幣為名行違法吸金、詐騙之實的犯罪手法，亦屬常見，同為偵查機關需努力打擊防範之對象。

在瞭解到「匿名性」於虛擬貨幣犯罪現場中所扮演的角色後，執法人員應該更善加裝備自己，讓自己對於虛擬貨幣之運作有著充分了

[105] 例如中華民國法務部調查局洗錢防制處與列支敦斯登金融情報中心關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作瞭解備忘錄、中華民國法務部調查局洗錢防制處與教廷金融資訊處關於涉及洗錢、相關前置犯罪及資助恐怖主義金融情資交換合作瞭解備忘錄、中華民國金融情報中心與巴布亞紐幾內亞金融情報中心關於洗錢及資助恐怖分子相關情資交換合作瞭解備忘錄等。

[106] 實務運作上，遇到雙方之間並無互助協定但有向他國跨境蒐證之需求時，還是可以嘗試透過法務部及外交部將請求函轉我國駐外代表處，由駐外代表處與該國外交部及司法機關協調予以提供協助。雖然此種請求並無任何法源上之依據，但仍可能獲得必要之協助，過去亦有成功取得關鍵證據之案例。相對地，若是無互惠雙邊協定之外國向我國請求提供協助時，如果請求事項對於我國主權、安全、國際聲譽並無有危害之虞，或其他國際刑事司法互助法第 10 條所定不得提供協助之情形，建議我國在可能之範圍內，仍予提供協助，以利建立實質上之司法互助。

解，明瞭虛擬貨幣世界中的匿名性並非絕對，並掌握手邊所能運用的各種資源，藉以從匿名的網路世界中找到破口，在現行法制對於個人資訊蒐集的規範框架下，透過向貨幣交換所等網路服務提供者調取和追查犯罪嫌疑人真實身分有關之身分識別資訊，佐以適當之演算分析工具予以分析、比對，以找出藏身幕後的真正犯罪行為人。

除此之外，虛擬貨幣的金流追查，亦是打擊虛擬貨幣犯罪不可或缺的環節，相關資料庫的建置刻不容緩，如何朝向國際資料共享之方向建置，以發揮最大效益，更是無從迴避的挑戰。而這些關於犯罪嫌疑人的身分及其犯罪金流追查所做的全部努力，最終都需仰賴有效地扣押與沒收犯罪所得，才不至於付諸流水，執法人員務須瞭解，成功扣押虛擬貨幣之關鍵在於掌握虛擬貨幣位址及其對應之「私鑰」，於建置專供扣押與執行沒收所用之虛擬貨幣錢包後，根據犯罪嫌疑人所持有之錢包種類之不同，以對應之方式進行扣押。成功扣押虛擬貨幣之後，亦應視偵查、審理之進度以及扣案之虛擬貨幣數量、市場價格等情，在適宜之時機進行虛擬貨幣變價程序，以確保能有效沒收犯罪所得，更重要的是，應從速建立全國一致的虛擬貨幣變價機制，才能確切落實沒收制度之立意，真正遏阻是類犯罪行為。

為了打擊虛擬貨幣犯罪所做的任何努力，都應該盡可能在跨境合作的規模上去規劃，因為這類型的犯罪幾乎無一例外地會有涉外因素，單從內國的角度進行偵查作為，勢必有其侷限。《國際刑事司法互助法》及其他司法互助協定與備忘錄固然已為執法人員提供蒐證、扣押乃至於沒收等許多互助管道，但不可諱言的是，現有的互助管道仍然極為不足，尤其是未涉及洗錢及其相關前置犯罪之虛擬貨幣犯罪，在

既有的司法互助規格下，恐怕大大限制了偵查機關查緝不法的可能性。如何在臺灣國際情勢依然險峻的情況下，開拓更多的跨境合作機會，以讓偵查機關能夠克盡己力，需要仰賴立法、司法與行政部門的專業、相互協力與政治智慧，才能突破目前的困境，讓臺灣能在打擊虛擬貨幣犯罪的國際舞台上扮演好自己的角色。