



加密貨幣之刑事凍結 與扣押

洪欣昇

臺灣臺南地方
檢察署檢察官

莊明雄

刑事警察局科技
研發科科长

目次

壹、前言

貳、加密貨幣犯罪的偵查流程

參、加密貨幣的凍結

肆、加密貨幣的扣押

伍、對我國加密貨幣凍結及扣押作業之
建議——代結論

壹、前言

隨著2024年初iShares Bitcoin Trust等11支比特幣現貨ETF在美國那斯達克等交易所上市，加密貨幣市場吸引大量資金湧入，強勁的買盤不斷推升加密貨幣價格，2024年3月間市值最大的加密貨幣比特幣突破7萬3千美元創下歷史新高，市值第二大的加密貨幣以太坊（Ethereum）也一度突破4千美元¹，其

他的加密貨幣也獲得投資人青睞，全球加密貨幣市場總市值不斷攀升，迄今已經超過2.63兆美元²。加密貨幣的蓬勃發展不禁讓人聯想到1974年諾貝爾經濟學獎得主海耶克（Friedrich von Hayek）在其著作「貨幣的非國家化」中提議：廢除中央銀行壟斷貨幣發行，允許私人發行貨幣並且自由競爭，在此過程中會出現最好的貨幣。然而這些可能是「最好的貨幣」，卻帶給偵查機關前所未有的挑

戰，原因是加密貨幣交易具有匿名性、去中心化、可跨境交易等特性，與傳統的法定貨幣交易性質頗為不同，偵查機關必須另外建立一套偵查方法來偵辦加密貨幣犯罪。

由於偵辦加密貨幣犯罪，最終希望就是取得犯罪所生或所用的加密貨幣以保全證據並沒收犯罪所得，故本文擬從犯罪偵查實務觀點探討加密貨幣的凍結與扣押程序。在文章架構上，第貳部分先簡要說明加密貨幣犯罪的偵查流程，接序於第參部分說明加密貨幣的凍結程序、第肆部分說明加密貨幣的扣押程序，第伍部分提出對我國加密貨幣凍結及扣押作業之建議，以代結論。有關其他重要的加密貨幣犯罪偵查議題如幣流追蹤、沒收及變價程序等，則待後續研究探討。在文章用語方面，本文所稱加密貨幣，與洗錢防制法所稱之虛擬通貨同義³；加密貨幣犯罪，泛指所有與加密貨幣有關的犯罪行為，根據統計全球常見的加密貨幣犯罪包括但不限於詐欺（scam）、竊盜（stolen funds）、勒索軟體（ransomware）、惡意軟體（malware）、暗網市場（darknet market）等⁴；機關錢包，是指偵查人員於執行扣押時，用以收受加密貨幣使用的檢察機關或司法警察機關所屬錢包；目標錢包，是指偵查人員透過幣流追蹤等偵查方法，鎖定特定地址後，予以凍結、扣押的加密貨幣錢包。

貳、加密貨幣犯罪的偵查流程

一般而言，偵查人員於偵辦加密貨幣犯罪時，從立案之後可能經歷的偵查流程包括：幣種辨別、幣流追蹤、確認目標錢包、凍結、搜索、扣押等階段，以下就幣種辨別、幣流追蹤作簡要說明。

首先，偵查人員一旦發現案件屬於加密貨幣犯罪，應先辨別涉案加密貨幣的幣種。雖然市場上有許多種加密貨幣，但依目前犯罪偵查實務而言，在這個階段只要暫先將加密貨幣分成「穩定幣」與「非穩定幣」兩種即可⁵。穩定幣是一種「中心化的」加密貨幣，由中心化的管理者控制加密貨幣的發行與管理⁶，由於管理者採用的底層技術不同，因此去中心化程度不一⁷。目前市值規模最大的穩定幣是泰達幣（Tether，代號USDT）、第二名是USDC⁸。泰達幣的發行商是泰達公司（Tether Limited），泰達幣的價格穩定維持1美元，由泰達公司提供100%儲備金，每當創造1枚泰達幣時，泰達公司會將1美元作為儲備金；泰達幣換回1美元的時候，泰達公司則會銷毀1枚泰達幣，以此方式支持泰達幣與美元1：1的價格掛勾。USDC的發行商是Circle和Coinbase，價格定錨機制與泰達幣相似。由於穩定幣的發行商對於加密貨幣的發行、移轉及銷毀具有控制權，且部分發行商願意配合偵查機關進行目

標錢包的凍結、扣押、針對異常交易進行回收、以區塊鏈分岔改寫來回收穩定幣，因此偵查機關於偵辦穩定幣犯罪時，可以利用公私部門合作方式達到對抗加密貨幣犯罪的效果⁹。除了泰達幣、USDC……等「中心化」的穩定幣外，其他市場上常見的加密貨幣如比特幣、以太幣、狗狗幣……等都屬於「去中心化」的非穩定幣。由於非穩定幣不具備中心化的發行商，因此不存在一個像泰達公司一樣的管理者可以配合偵查，必須要等非穩定幣進入中心化的加密貨幣交易所（如幣安，Binance）後，偵查機關才有機會開啟公私部門協力偵查模式。

第二階段的幣流追蹤，目的在於確認加密貨幣的來源及去向。由於加密貨幣採用分散式帳本技術（Distributed Ledger Technology, DLT），當加密貨幣被交易後，透過區塊鏈共識協定將分散式帳本的資料庫分布於對等網路的節點上，因此每個節點都複製及儲存於網路加密貨幣交易帳本資訊，也就是說這些加密貨幣金流是公開資訊，偵查人員可以透過帳本查詢網站（例如以太坊 Etherscan、波場鏈 Tronscan 等）或利用幣流軟體（例如 Chainalysis、TRM 等）進行追蹤，涉法找出用來接收、儲存或轉移加密貨幣的不法錢包地址。一旦確認不法錢包地址後，該錢包就成為偵查人員的目標錢包，可能設法凍結錢包的操作，暫時禁止任何形式的轉移，以防止

被告轉移資金。

幣流追蹤紀錄對於後續的凍結、搜索、扣押具有重要意義，因為在現行實務上當偵查機關以某目標錢包涉嫌不法為由，向穩定幣發行商（如泰達公司）或加密貨幣交易所（如幣安）請求凍結目標錢包的時候，偵查機關必須提出幣流追蹤紀錄作為證據，以說明凍結目標錢包的合理性。此外，若偵查機關想要扣押目標錢包內的加密貨幣，而向法院聲請核發搜索票或聲請法院作成非附隨於搜索的扣押裁定時，亦可提出幣流追蹤紀錄，向法官說明辨識目標錢包的過程，說服法官核發搜索票或作成扣押裁定。然而，由於加密貨幣混幣器（Coin Tumbler）或跳鏈（Chain-Hopping）等干擾因素，幣流追蹤紀錄可能有出現非常複雜及不易判定等情形，進而影響該份紀錄的證明力，此部分容後另行撰文說明。

參、加密貨幣的凍結

加密貨幣的凍結，是指暫時限制目標錢包的使用，包括暫時限制目標錢包收受來自其他錢包的加密貨幣，及暫時限制將目標錢包內的加密貨幣移轉至其他錢包。前文已說明市場上常見的加密貨幣多是使用「去中心化」技術的加密貨幣，通常而言並不存在一個中心化的管理者可以控制加密貨幣的移轉，因此

理論上無法進行凍結。然而，例外情形有二，一是當涉案加密貨幣的幣種屬於穩定幣者，二是當涉案加密貨幣已移轉至加密貨幣交易所錢包者，偵查機關可以請求「中心化的」穩定幣發行商（如泰達公司）或加密貨幣交易所（如幣安）協助偵查機關進行凍結，這與傳統的法定貨幣必須由「中心化的」銀行執行凍結的概念相似¹⁰。以下先說明我國加密貨幣凍結的法律依據，再說明操作流程。

在法源依據方面，我國目前關於加密貨幣凍結的主要法源包括洗錢防制法以及依其授權訂定之「洗錢防制法第十五條之二第六項帳戶帳號暫停限制功能或逕予關閉管理辦法」（下稱「帳戶暫停限制關閉辦法」）。首先，2023年6月14日修正公布之洗錢防制法第15條之2第5項規定「違反第一項規定者¹¹（按即俗稱人頭帳戶），金融機構、虛擬通貨平台及交易業務之事業及第三方支付服務業者，得對其已開立之帳戶、帳號，或欲開立之新帳戶、帳號，於一定期間內，暫停或限制該帳戶、帳號之全部或部分功能，或逕予關閉」，明文賦予「虛擬通貨平台及交易業務之事業」¹²凍結人頭帳戶的權限；同條第6項則將上開帳戶、帳號之認定基準，暫停、限制功能或逕予關閉之期間、範圍、程序、方式、作業程序之辦法，授權由法務部會同中央目的事業主管機關定之。其後，法務部會同金融監督管理委員會、數位發展部依

據上開法律授權，於2024年2月間會銜訂定發布帳戶暫停限制關閉辦法，並自2024年3月1日施行。依帳戶暫停限制關閉辦法第7條規定「虛擬通貨平台及交易業務之事業對於行為人之虛擬通貨帳號，應依下列規定辦理：一、拒絕行為人申請開立新帳號。二、行為人原有帳號，應由虛擬通貨平台及交易業務之事業先予暫停該帳號全部交易功能，辦理帳號結清後，逕予關閉」。關於上開規定有幾個問題值得探討，第一個問題是由於洗錢防制法的適用範圍受到洗錢行為的概念限制，本即無法含蓋所有的加密貨幣犯罪類型¹³；再加上洗錢防制法第15條之2及帳戶暫停限制關閉辦法只適用於人頭帳戶，更加限縮加密貨幣帳戶凍結的適用範圍，對於實務運作的影響如何，值得觀察。第二個問題是帳戶暫停限制關閉辦法賦予加密貨幣交易所「結清」及「關閉」帳戶之義務，是否妥適有待商榷。加密貨幣依其市場定價機制，可區分為穩定幣及非穩定幣，穩定幣的價格採取定錨機制，釘住某種基底資產的價格，例如市值規模第一、二名的泰達幣、USDC都是以1比1的方式釘住美元。然而非穩定幣如比特幣、以太坊的價格並無定錨機制，完全由市場供需決定價格漲跌，行情波動相當劇烈，若未經行為人同意，逕將行為人的帳戶內的加密貨幣兌換成新臺幣等法定貨幣予以結清，若將來該加密貨幣的價格大

漲，確認無責任之行為人能否請求價差賠償或請求返還原加密貨幣，不無疑問。因此建議，在確認行為人之責任前，未經行為人同意，不宜逕將加密貨幣帳

戶予以結清。根據筆者實際觀察，境外及境內加密貨幣交易所常見的處理方式仍有分歧之處，整理如下表1。

表1 目前各加密貨幣交易所處置洗錢帳號與虛擬貨幣作法表

境內外	交易所	洗錢帳戶處理	加密貨幣處理
境外	B業者	暫停該帳號全部交易功能	不結清帳號，給予司法機關一定處理期限提出合規司法文書後，將加密貨幣移轉至扣押機關錢包；逾期末處理則開通帳戶。
境外	O業者	暫停該帳號全部交易功能	同上。
境內	M業者	暫停該帳號全部交易功能	辦理帳號結清後，逕予關閉。
境內	B業者	暫停該帳號全部交易功能	辦理帳號結清後，逕予關閉。
境內	A業者	暫停該帳號全部交易功能	辦理帳號結清後，逕予關閉。

(本研究自行製作)

肆、加密貨幣的扣押

加密貨幣的扣押，必須將目標錢包中的加密貨幣移轉至機關錢包內始能完成，本質上是一種對人民財產權的侵害，若未經當事人自願同意，偵查人員必須依法取得法院令狀¹⁴，始得強制為之。在立法例上，有另定加密資產扣押規範而與一般扣押規範作出區別者，例如英國2023年經濟犯罪和企業透明度法案（Economic Crime and Corporate Transparency Act 2023）於Schedule 8「加密資產：沒收令」（Cryptoassets：confiscation orders），特別針對加密資產的搜索及扣押予以明文規定。由於我國並未針對加密貨幣的扣押程序特別立

法，故仍應適用刑事訴訟法有關扣押之規定。

在執行面上，加密貨幣的扣押和一般物品的扣押方式不同，主要差異包括：去中心化的加密貨幣沒有中央管理機構可以協助執行扣押，偵查機關必須自行將加密貨幣從目標錢包移轉至機關錢包；加密貨幣的扣押需要許多的事前準備工作，包括專業人才的訓練、機關錢包及手續費的預備等。此外，加密貨幣的扣押方式也與傳統電磁紀錄不同，傳統電磁紀錄的扣押方式是將電磁紀錄原封不動的複製或移動至偵查機關的儲存裝置內；加密貨幣的扣押方式則必須做成一筆新的交易紀錄，將加密貨幣從目標錢包移轉到機關錢包內¹⁵。再者，偵

查人員在扣押電磁紀錄時，只要將網路阻斷或開啟行動裝置飛航模式，就可以防止他人利用網路遠端登入進行清除或轉移電磁紀錄；但加密貨幣是透過私鑰在網路上區塊鏈中進行轉移，偵查人員即使已經扣押冷錢包或安裝熱錢包的手機、電腦等硬體設備，甚至已經阻斷網路、開啟飛航模式，都無法避免他人利用備用私鑰或助記詞來轉移加密貨幣。惟有在發現不法加密貨幣的第一時間就把它轉移到機關錢包內，才能保全扣押。下文將先說明偵查人員實際執行加密貨幣扣押時可能面臨的不同狀況，再說明扣押作業流程的參考規範及近期國內司法警察機關實務作法。

一、扣押加密貨幣可能面臨的狀況類型：

原則上可依照被告是否同意扣押、幣種是否為穩定幣、目標錢包是否為交易所錢包、是否以搜索方式取得目標錢包私鑰，區分為下列數種狀況類型。

(一)狀況一：被告同意扣押

不論應扣押之加密貨幣是屬於何種幣種、使用何種錢包，亦不論扣押程序是屬於「附隨於搜索的扣押」¹⁶或「非附隨於搜索的扣搜」¹⁷類型，只要錢包持有人自願同意提供錢包地址及私鑰給偵查

機關，偵查機關就可以合法將目標錢包內的加密貨幣移轉至機關錢包內，完成扣押程序。然而，若是錢包持有人不願意提供錢包地址及私鑰時，偵查機關必須改以下列方式進行扣押。

(二)狀況二：扣押之幣種是穩定幣

當扣押的幣種是中心化的穩定幣時，以扣押泰達幣為例，相關扣押流程均可透過執法機關窗口請求泰達公司協助執行，整個幣流過程必須以乾淨的冷熱錢包交易為主，且幣流最終點也應以冷錢包為儲存標的。由於泰達幣是中心化的幣種，只要知道泰達幣錢包地址，就能由泰達公司進行移轉。在程序上，必須由檢察機關或司法警察機關以書面敘明犯罪事實，並提供法院扣押裁定、幣流追蹤紀錄，經泰達公司審查完畢，經過一段時間審議後，才能進入到扣押及返還程序，這樣的時間大約必須花費3個月到6個月不等，整體流程如圖1所示。

(三)狀況三：目標錢包是加密貨幣交易所錢包

所謂加密貨幣交易所錢包，是指境內或境外的虛擬通貨平台及交易業務事業（Virtual Asset Service Providers, VASP）¹⁸提供的託管錢包，開戶時通常要作身分驗證（Know Your Customer，

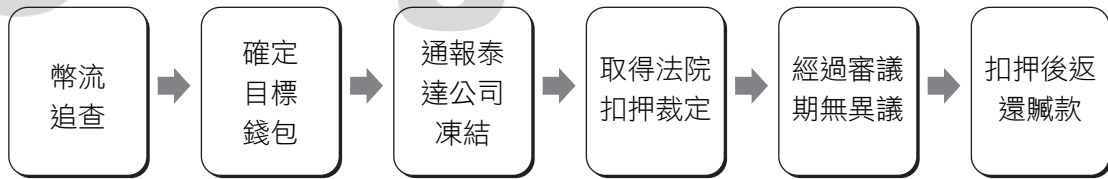


圖1 泰達幣凍結扣押流程圖

KYC)。在偵查實務上，境內加密貨幣交易所如現代財富、幣託、王牌等3大家，都曾配合執行扣押；境外加密貨幣交易所目前透過執法機構主動聯繫之下，能配合我國偵查機關進行扣押的有幣安（Binance）、火幣（HTX）等交易所。基於令狀原則的要求，加密貨幣交易所通常會要求偵查機關提出法院扣押裁定，以避免日後與客戶產生爭議。應注意者，在幣流追蹤紀錄的判讀上，由於大部分交易所會先提供用戶臨時性錢包帳戶作為收款，然後進到主要水庫錢包，其後如果要出金再從另一個加密貨幣錢包帳戶出去，因此一旦加密貨幣進入交易所水庫錢包後就會產生混同效果，後續勾稽追蹤幣流的正確性會大大降低。從而，偵查人員若發現幣流曾經

進入交易所水庫錢包，應避免冒然對經過水庫錢包後的幣流終點錢包進行扣押，以避免錯誤扣押的可能。此外，我國刑事訴訟法第133條之1第1項規定「非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定」，同法第133條之2第1項明定偵查中檢察官得向該管法院聲請扣押裁定、第2項明定司法警察官得報請檢察官許可後，向該管法院聲請核發扣押裁定。據筆者觀察，目前實務上檢察官及司法警察官均曾向法院聲請加密貨幣扣押裁定，於取得法院扣押裁定後，循一定途徑將法院扣押裁定連同幣流追蹤紀錄交給加密貨幣交易所，以完成扣押程序，作業流程如圖2所示。¹⁹



圖2 加密貨幣交易所錢包扣押作業流程圖

(四) 狀況四：以搜索方式取得目標錢包私鑰

當被告不願意提供目標錢包私鑰時，偵查人員可能利用搜索方式尋找私鑰。私鑰通常由一串隨機產生的數字和字母組成，其長度和具體格式取決於使用的加密貨幣和加密演算法。由於要單憑記憶直接記住私鑰相當困難，錢包持有人通常會將私鑰寫在紙張上，或將私鑰拍照或截圖儲存在雲端硬碟、隨身碟、手機、筆電等裝置內。私鑰有時可能是一串助記詞，透過還原的方式可以將原來冷錢包上的權限重新設立在另一個冷錢包上面。應注意者，當偵查人員在搜索現場發現冷錢包或安裝熱錢包的手機、電腦等硬體設備時，單純阻斷網路、開啟飛航模式，都無法防止他人利用備用私鑰或助記詞來轉移目標錢包內的加密貨幣。偵查人員必須進一步設法取得私鑰，儘早將目標錢包內的加密貨幣移轉到機關錢包內，才能避免加密貨幣遭他人從遠端轉移。

二、加密貨幣扣押作業的參考規範及建議作法

目前世界各國執法機關都在努力建立扣押加密貨幣的標準作業流程，筆者參考歐美相關規範，並與國內實務單位的實際操作經驗進行比較，發現我國與其他國家作法並無太大差異。惟我國對

於制定加密貨幣扣押規範仍處於萌芽階段，前述洗錢防制法及相關法規命令、刑事訴訟法之規範密度尚屬不足，須努力催生相關配套規範，才能讓偵查人員於扣押加密貨幣時有所遵循，以達合法保全證據及沒收犯罪所得之效。下文將逐一說明歐美參考規範，並提出建議作法供偵查人員參考。

(一) 歐洲安全與合作組織參考規範

歐洲安全與合作組織（Organization for Security and Cooperation in Europe，OSCE）於2022年7月15日出版「加密貨幣刑事偵查處理手冊」（HANDBOOK FOR DEALING WITH VIRTUAL CURRENCIES IN CRIMINAL PROCEEDINGS）²⁰中，對於中心化及去中心化加密貨幣及虛擬資產參與者（包含交易所、交易者、礦工等）作出定義，並說明加密貨幣在刑事訴訟中的重要性、歐盟北馬其頓加密貨幣立法與斯洛維尼亞共和國處理加密貨幣刑事扣押經驗等資訊。該手冊特別提到引用2001年歐洲等相關國家簽署《布達佩斯公約》，其中規定簽署國之刑事犯罪偵查合作義務，針對非法存取、非法攔截、駭客攻擊等利用電腦網路進行之犯罪行為（例如詐欺、兒童色情製品及智慧財產權犯罪）須予以進行協助調閱及確保數位證據（搜索和扣押、緊急保護等）並透過國與國之間進行合作，這部分也給予跨

國加密貨幣調查法源基礎。此外，該手冊也提到加密貨幣扣押不僅只是將電腦或手機扣走就可以完成，任何擁有私鑰的外部共犯仍然可從遠端將這些虛擬資產轉移走，而且也認為實體或其他電磁紀錄的扣押顯然與加密貨幣型態不同，更應該另外立法規範。以下特別摘錄該手冊中附錄1表格2²¹所提出之加密貨幣扣押具體內容：

1. 檢察官辦公室立案編號 __/__。

2. 針對犯罪嫌疑人__存在合理懷疑犯罪的理由並根據刑法與刑事訴訟法相關規定由檢察官簽發臨時安全措施（臨時扣押物品——加密貨幣）。

3. 來自__的虛擬貨幣錢包（描述它位於哪裡、它是什麼類型的錢包或錢包序號及持有人身分資訊），扣押__（虛擬貨幣的名稱，例如比特幣）在扣押日__月__年大約價值__（如美元）。

4. 加密貨幣的扣押應由__司法警察（警察機關名稱）執行。

5. 扣押加密貨幣__（虛擬貨幣的數量和名稱，如：5枚比特幣），將透過從被扣押者錢包__地址轉帳至__執法機關暫時控管之安全冷錢包並被移交給__（負責保管機構名稱）錢包，並將被暫時保管直至一審法院程序結束。

(二)美國印第安那州警察局參考規範

美國印第安那州警察局於2018年5月15日即已制定「扣押加密貨幣與虛擬

貨幣」(Seizure of Cryptocurrency and Virtual Currencies)作業流程規範²²，明定加密貨幣扣押程序與作法，並針對加密貨幣、冷熱錢包、公私金鑰進行定義，比較特別是印第安納州警察局會特別選任專責扣押加密貨幣執法官員，負責觀察扣押現場的狀況和存放扣押加密貨幣的狀況，這些見證執法官員必須具備足夠的加密貨幣知識與技能，以確保扣押過程無虞。警方在處理扣押加密貨幣前，要先過濾下列幾個問題：

1. 交易所可以協助扣押：當要扣押加密貨幣交易所錢包或熱錢包之贓款，交易所能配合司法機關發出的扣押令辦理，命專人交給交易所執行完成。

2. 交易所無法協助扣押：當要扣押加密貨幣交易所錢包或熱錢包之贓款，交易所不遵守司法機關發出的扣押令且有緊急情況者，或者當加密貨幣處於冷錢包，應採用以下扣押流程：

(1) 扣押人員如果要使用或啟用新冷錢包接收贓款加密貨幣，必須透過專責人員觀察整個過程。

(2) 扣押人員應進行螢幕截圖、拍照或以其他方式記錄將被扣押的加密貨幣數量，並全程由專責人員觀察過程。

(3) 扣押人員須使用能掌控私鑰的錢包進行轉帳，並將加密貨幣發送至該機構控制的錢包，轉移過程都由專人監控。

(4) 扣押人員應進行螢幕截圖、拍照或以其他方式記錄被移轉到機關錢包內

的加密貨幣數量，並全程由專責人員觀察過程。

(5) 扣押人員發現同一個目標錢包內存在多個私鑰時，可以使用同一個機關錢包進行扣押。針對每一個要扣押的目標錢包，都要新增一個機關錢包。

(6) 扣押完成必須透過公開帳本確認已經轉帳成功，並列印或截圖為憑，並提供專責人員全程見證。

(7) 扣押人員將把該機關控制的冷錢包備份儲存至CD或DVD裡面，並提供專責人員全程見證。

(8) 扣押人員製作一份該機關控制的冷錢包的紙本備份（還原助記詞），並提供專責人員全程見證。

(9) 上述包含冷錢包備份的CD或DVD以及紙本，應比照法定貨幣標準作業流程進行包裝及處理。

(10) 扣押人員和見證人員必須依據相關標準作業流程規定，在包含冷錢包備份的CD或DVD以及紙本上簽名、填寫日期、時間及其他相關資訊。

(11) 每個包含冷錢包備份的CD或DVD以及紙本都應比照法定貨幣標準作業流程進行提交儲存。

(12) 現場扣押的電腦設備在事後必須進行複製副本，並提供專責人員全程見證。

3. 被扣押的加密貨幣在被沒收之前，不會轉換為美元，這與其他具有價格波動性的扣押物品（例如貴金屬、房

屋、票據、車輛、藝術品和外幣）的現行政策及作法一致。

(三) 近期國內司法警察機關實務作法

偵查人員於扣押前，必須事先備妥扣押專屬錢包，並備妥足夠的手續費；於扣押中，必須輸入正確錢包地址，且應全程錄影；於扣押後，必須將冷錢包及私鑰入庫，並將加密貨幣從司法警察機關錢包移轉至檢察機關錢包，以下逐一說明。

1. 扣押前：預先備妥扣押專屬錢包，並備妥足夠手續費方便加密貨幣轉移

(1) 扣押專屬錢包選擇

扣押專屬錢包的選擇對於扣押工作來講非常重要，目前加密貨幣錢包種類，依照安全等級先後分為冷錢包、熱錢包、交易所（託管）錢包，主要在於私鑰保存方式來區分，最嚴格仍以冷錢包為主，然後熱錢包，最後才是交易所（託管）錢包，而近期我國臺灣高等檢察署也推動自建虛擬金庫，也就是具備權限控管的錢包，因為兼具冷錢包可離線控管、熱錢包線上容易操作與產生錢包快速等特性，因此有人稱它叫做溫錢包。相關錢包類型如圖3所示，並各別說明如下：

A.冷錢包：安全性高，擁有金鑰且離線網路

冷錢包常被稱為「離線錢包」或「硬體錢包」，通常將私鑰寫入特殊硬體晶片，外型像是一個USB的裝置，而冷錢包之中的私鑰透過良善的加密機制，且只有在交易時才會連接網路，被認為最不容易被駭客入侵竊取，算是安全度較高之儲存方式，但操作麻煩且硬體可能容易毀損。

B.熱錢包：安全性低，私鑰存放於電腦之中，並且連網容易被竊

熱錢包通常為求交易快速，讓使用

者快速檢視持有的加密貨幣。通常會透過電腦、行動載具等能夠連接上網路設備直接運行，例如電腦錢包（如透過Windows程式運作）、手機錢包（錢包運作於手機上，如 Apple 及 Android 的系統）、網頁錢包透過瀏覽器運作，如MetaMask等插件。但因為熱錢包是連接網路的設備生成加密貨幣的私鑰，缺乏安全性，仍具備遭駭客入侵竊私鑰被轉移資產之風險。

C.交易所（託管）錢包：安全性低，私鑰由平台管理

加密貨幣錢包類型

——牽涉私鑰管理是否個人可管理與否

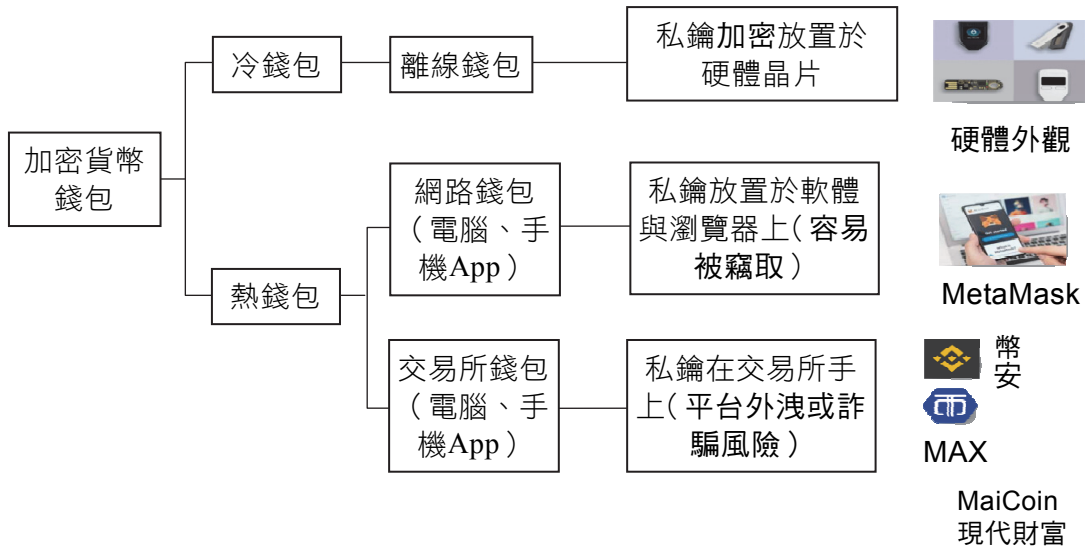


圖3 各種加密貨幣錢包介紹（本研究整理）

加密貨幣交易所託管錢包供應商主要負責向其客戶提供服務以保護私鑰、持有、儲存和移轉虛擬貨幣工作，類似銀行與存戶的關係，但私鑰控制在交易所手上，客戶無法操作真實交易。因此，託管錢包供應商不同於冷、熱錢包，託管錢包供應商的角色反而與金融機構的功能相似。在我國來講，Mycoin的MAX、幣託的BitoEX及王牌ACE等境內交易所錢包即是比較知名之列，而境外則以幣安（Binance）及CoinBase等為大宗。

D. 司法機關自建虛擬金庫（溫錢包）²³

國內越來越多執法單位或司法單位採用「多簽錢包（Multisig Wallet）」，多重簽名允許複數用戶共同執行數位簽章來控管錢包資產。像是把保險箱分為四個人保管鑰匙，要同時開啟才能取得裡面的加密貨幣，但只有其中一把鑰匙時則無法打開，採取類似交易所託管錢包機制，但是私鑰卻不會淪為一人獨掌，而且具備熱錢包特性，操作上介面類似熱錢包，一般執法人員入金只要提供加密貨幣錢包QR Code就可以轉帳，兼具安全與便利特性，但是唯一缺點就是要制定管理規範，來防範內部舞弊問題，另外如果虛擬金庫權限設定不良，也可能會有資安問題。

(2) 交易手續費之處理

任何加密貨幣交易都需要手續費才

能進行轉移，但是並非所有手續費都是透過原生幣種來轉換扣取，舉例來說，比特幣、以太幣或者Omni-USDT、ERC20-USDT等均可從比特幣或以太幣來扣除手續費，但如果是波場區塊鏈的泰達幣TRC20-USDT，則手續費必須另外使用TRX虛擬貨幣來支付。因此，偵查人員在實際執行扣押時，如果目標錢包是冷錢包或非平台熱錢包，則必須另外購買TRX並存入錢包之中來進行轉帳到司法警察機關錢包內；若司法警察機關要再將加密貨幣轉移到檢察機關錢包時，又必須花費另一筆TRX加密貨幣費用。但如果目標錢包是交易所錢包時，因為交易所本身是另外有一個水庫再支付手續費，因此只要當事人同意，其實直接進行轉移即可，手續費也非常便宜，約莫幾十塊新臺幣。此外，扣押所須的手續費，也可以直接由目標錢包支付，因此在扣押現場偵查人員與目標錢包持有人可以溝通討論，合意從目標錢包中扣除手續費。而司法警察機關錢包、檢察機關錢包、法院錢包之間的加密貨幣移轉，亦可透過機關間的溝通討論，合意由何方支付，依筆者實際處理個案的經驗，扣案泰達幣約600萬枚（折合當時價格新臺幣2億多元），該批泰達幣先從目標錢包移轉到司法警察機關錢包、再從司法警察機關錢包移轉至檢察機關錢包，兩次轉帳的手續費約莫新臺幣140餘元，手續費的金額其實並不大，有關加密貨幣手續費的可能支付模式如圖4所示。

2.扣押中：輸入正確錢包地址，且應全程錄影

(1)目標錢包地址應謹慎核對，注意錢包編碼準確度

扣押加密貨幣最大風險在於，一旦輸入錯誤編碼則可能一失足成千古恨，無法返還，而且部分加密貨幣大小寫要一致，否則可能填寫成錯誤錢包地址，通常最方便方式就是直接掃描QR Code來轉移。如同上述，其實對於扣押的過程能夠做成標準化最好，對於不熟稔加密貨幣的執法人員不應該單獨操作扣押動作，且避免爭議，所有轉移過程必須全程錄影。

(2)轉移應先小筆金額再大筆金額

為避免因輸入錯誤而面臨大額加密貨幣損失，應先輸入小額加密貨幣，確認入帳無誤後，再轉移大筆金額，減低轉移錯誤風險。

(3)現場必須取出完整私鑰並進行扣押保存

扣押現場應留意受扣押人有無保存冷錢包或非交易所熱錢包私鑰(助記詞)或備份資訊，連同完整冷錢包商品盒子也要一併扣押，至於交易所錢包的私鑰則非由受扣押人控管。偵查人員應儘量在現場將虛擬資產轉移，避免遭到他人從遠端湮滅證據與藏匿資產。

(4)扣押程序完畢後應重新查證公開帳本，確認加密貨幣是否轉移成功

加密貨幣轉移必須經過既定的區塊鏈並寫入交易才算成功，因此每次扣押工作轉移完畢並非完成，應確認公開帳本已經寫入標註成功才算完成扣押。

3.扣押後：錢包及私鑰之入庫管理

(1)目標錢包及私鑰扣押入庫

目標錢包若是冷錢包，先將目標錢包內的加密貨幣移轉至偵查機關錢包內，然後將該冷錢包及私鑰(助記詞)一併扣押入庫方式，這是最常見的作法。但若沒有先將目標錢包內的加密貨幣移轉至偵查機關錢包內，就直接把冷

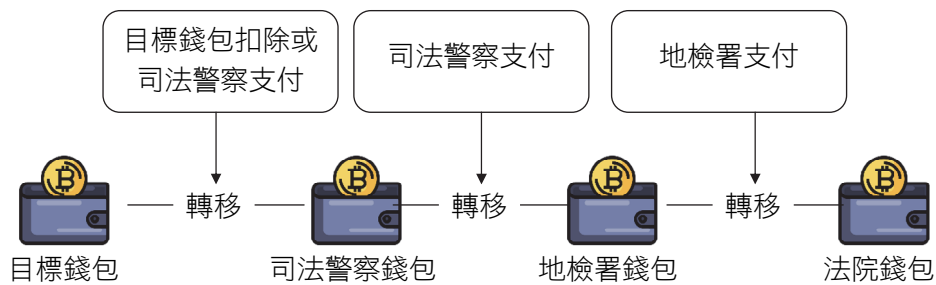


圖4 加密貨幣手續費的可能支付方式

錢包扣押入庫，可能會產生保管風險，大部分偵查機關可能未具備專屬收款加密貨幣設備或系統，且私鑰透過拍照、複寫或抄錄都可能被他人留存或外洩。因此，即使冷錢包離線置於贓物庫內，但是他人仍可能透過私鑰或助記詞來轉移錢包內的加密貨幣，偵查人員可能在下一次打開冷錢包時，發現所有的加密貨幣早已遭他人轉走的窘境。

(2)從司法警察機關錢包移轉到檢察機關錢虛擬金庫或冷錢包

在扣押物保管實務上，司法警察機關和檢察機關各有贓物庫、各自進行保管，當扣押標的是加密貨幣時，亦不例外。為避免發生加密貨幣遺失或遭盜轉的責任歸屬爭議，比較好的方式應該是每次扣押的加密貨幣從司法警察機關入庫至檢察機關時，都要實際進行轉移交易，避免未經移轉交易就直接將司法警察冷錢包送到檢察機關入庫，這個作法雖然花費多次手續費，但是可釐清保管責任。目前實務上司法警察基於便利性考量，多攜帶冷錢包到扣押現場，然後扣押完畢後，直接將冷錢包帶往地檢署進行轉移到指定虛擬金庫或其他錢包，最後確認公開帳本無虞後，完成扣押程序。

伍、對我國加密貨幣凍結及扣押作業之建議 ——代結論

一、應訂定完整扣押程序標準作業流程與法制化辦法

為避免第一線執法人員無所適從或因個人認知或專業知識落差導致偏誤，應儘速比照外國立法例訂定新法或增修既有規範，例如我國刑事警察局所訂定的犯罪偵查手冊應加入加密貨幣凍結及扣押作法、支付手續費之方式等內容，讓執法人員對於偵辦加密貨幣犯罪有所依循，以保障加密貨幣凍結及扣押的合法性。

二、由於加密貨幣扣押與其他動產扣押方式不同，應強化訓練，提升執法者知能

加密貨幣在洗錢防制法上雖被視為某種資產標的，但本質上畢竟與法定貨幣、黃金或其他實體資產有所不同，且與電腦文件、影音檔案、商業機密或電子郵件等電磁紀錄內容亦有差異，執行扣押的執法人員必須具備一定專業知識及技能才能避免錯漏。因此未來教育訓練非常重要，只有擴大提升執法人員對於加密貨幣的知識及技能，才能提升扣押精準度與效能。♣

1. 資料來源：yahoo finance資料庫（最後瀏覽日：2024年3月24日）。
2. 資料來源：CoinGecko，網址：<https://www.coingecko.com/en/global-charts>（最後瀏覽日：2024年3月24日）。
3. 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條第1項第2款：「二、虛擬通貨：指運用密碼學及分散式帳本技術或其他類似技術，表彰得以數位方式儲存、交換或移轉之價值，且用於支付或投資目的者。但不包括數位型式之新臺幣、外國貨幣及大陸地區、香港或澳門發行之貨幣、有價證券及其他依法令發行之金融資產」。從字義上看來，「加密貨幣」一詞強調的是這類貨幣的技術特點，即利用密碼學原理保障交易的安全性和匿名性；而「虛擬通貨」一詞則偏重於表達這類貨幣相對於傳統貨幣（如紙幣和硬幣）的虛擬性質，然而目前在市面上流通、具有經濟價值的「加密貨幣」也都符合「虛擬通貨」的定義，因此二者尚無強作分別的必要。
4. Chainalysis，The 2024 Crypto Crime Report，2024年2月，3頁。
5. 就此容有不同分類標準，例如歐洲理事會網絡犯罪計畫辦公室（Cybercrime Programme Office of the Council of Europe）於2021年發布的加密貨幣扣押指南（GUIDE ON SEIZING CRYPTOCURRENCIES），是將虛擬貨幣區分為四種：可轉換虛擬貨幣（Convertible Virtual Currencies）、不可轉換虛擬貨幣（Non-convertible Virtual Currencies）、中心化虛擬貨幣（Centralized virtual currencies）、去中心化虛擬貨幣（Decentralized virtual currencies），見歐洲理事會網絡犯罪計畫辦公室加密貨幣扣押指南，2021年2月，6頁。
6. 同前註，7頁。
7. 徐珮菱，穩定幣之交易風險與監理，月旦民商法雜誌，82期，2023年12月，72頁。
8. 資料來源：<https://coinmarketcap.com/>。
9. 由歐洲刑警組織（European Union Agency for Law Enforcement Cooperation, Europol）等機構於2023年10月間舉辦的第七屆犯罪金融和加密貨幣全球會議，將「加密貨幣偵查和沒收程序中的公私合作」列為關鍵議題。資料來源：<https://www.europol.europa.eu/media-press/newsroom/news/shaping-international-responses-against-criminal-misuse-of-cryptocurrencies>。
10. 傳統的法定貨幣的凍結程序，必須由銀行配合執行。當偵查機關想要凍結特定銀行帳戶內的資金時，偵查機關必須通知該帳戶所屬銀行，由銀行執行凍結。法源依據為銀行法第45條之2第2項：「銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項。」，同條第3項：「前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶之作業程序及辦法，由主管機關定之。」及金融監督管理委員會依據前開法律授權訂定之「存款帳戶及其疑似不法或顯屬異常交易管理辦法」。
11. 洗錢防制法第15條之2第1項規定：「任何人不得將自己或他人向金融機構申請開立之帳戶、向虛擬通貨平台及交易業務之事業或第三方支付服務業申請之帳號交付、提供予他人使用。但符合一般商業、金融交易習慣，或基於親友間信賴關係或其他正當理由者，不在此限」。
12. 所謂虛擬通貨平台及交易業務事業（Virtual Asset Service Providers, VASP），依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條第1項第1款之定義，係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。

13. 相同見解：羅韋淵，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，2023年5月，39-40頁。
14. 令狀原則之理論，係要求偵查機關在侵犯人民基本權前，必須先由司法機關審核實質理由，以防止無相當理由的強制處分，參照王兆鵬，刑事訴訟講義，元照，2008年，97頁。
15. 參照刑法第359條「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄」之用語，傳統電磁紀錄的扣押較偏向「取得」，而加密貨幣的扣押則較偏向「變更」概念。
16. 最高法院111年度台上字第4767號刑事判決：搜索及所伴隨之扣押處分，因涉及對於人民隱私權、財產權、居住權等基本權的干預，刑事訴訟法第128條乃採取令狀原則，明定搜索須由法官簽發搜索票，作為事前之審查，俾保障人民上開基本權。又未持搜索票所為之搜索，本質上屬無令狀搜索，需受法定程序之限制，如未違背刑事訴訟法第130條附帶搜索、第131條逕行搜索、第131條之1同意搜索等法律規定，自不得執以主張因此所扣押之證據，無證據能力。
17. 最高法院112年度台上字第4818號刑事判決：關於偵查中非附隨於搜索之扣押，參照刑事訴訟法第133條之1、第133條之2等規定，原則上固採法官保留與令狀原則，亦即應經法官裁定始得實施扣押。惟依同法第133條之1第1項規定：「非附隨於搜索之扣押，除以得為證據之物而扣押或經受扣押標的權利人同意者外，應經法官裁定」，顯係以所扣押者為「得為證據之物」或「經受扣押標的權利人同意」之情形，作為令狀原則之例外，亦即扣押物如符合上開情形之一，自得實施非附隨於搜索之無令狀扣押，毋庸經法官裁定，即得予以扣押。
18. 見註12。
19. 近期扣押成功案例：被害人經詐騙集團會冒用Forbes「媒體採訪」的名義社交工程釣魚，並誤入傳送帶有惡意程式的網頁，以填寫資料的名義遭盜取的加密資產，經轉轉進入總部位於塞席爾的境外加密貨幣交易所OKX。我國偵查機關向OKX交易所通報後，凍結14.0789枚以太幣，嗣經取得法院扣押裁定後將該筆加密貨幣返還至我國司法警察機關提供之冷錢包，發還給被害人。網路資料來源：「無被告身分」也能凍結、裁扣、返還境外詐騙資產！XREX交易所與偵查機關共創司法先例，<https://www.blocktempo.com/xrex-plays-key-role-in-taiwans-fraud-combat>（最後瀏覽日：2024年1月13日）。
20. HANDBOOK FOR DEALING WITH VIRTUAL CURRENCIES IN CRIMINAL PROCEEDINGS，OSCE官方網站<https://www.osce.org/mission-to-skopje/522754>（最後瀏覽日：2024年2月24日）。
21. 同註20，82頁。
22. 資料來源：美國印第安納州警局（Indiana State Police），官方網址：<https://www.in.gov/isp/files/Seizure-of-Cryptocurrency.pdf>（最後瀏覽日：2024年3月29日）。
23. 相關新聞：陽光行動／查扣虛擬幣警設多簽錢包防弊，聯合報，<https://udn.com/news/story/12861/7791812>，（最後瀏覽日：2024年3月29日）。

關鍵詞：加密貨幣凍結、加密貨幣扣押、區塊鏈、冷錢包、私鑰

DOI：10.53106/279069732603

（相關文獻☛月旦知識庫 www.lawdata.com.tw；
更多裁判分析☛月旦法律分析庫 lawwise.com.tw）