利用加密虛擬貨幣從事賄選犯罪之防制作為

李秉錡、古慧珍[1]

壹、前言

「錢」是很重要的犯罪動機或犯罪工具，在犯罪調查中，嘗試串起錢的軌跡，有助於勾勒整個犯罪架構或找到藏鏡人。而錢的型態最常見的就是「現金」和「銀行款項」且各有特色，現金難以追查在哪些主體間移動，但量大要移動較為不易；反之，銀行款項好追查，但移動方便。因此，在犯罪的世界中，就有一群人想要找一些「錢」的代替載具，可以兼具追查不易及移動方便的功能，傳聞中國早期的「中華菸」就是很好的例子，這個菸的軟包裝版生產量有限，曾被拿來當作行賄官員的工具，逢年過節就送菸，收到菸的人可以到特定商店以菸包定價約 10 倍出售，形成一個地下市場，有人戲稱「買的人不抽，抽的人不買」，當然如果不懂或找不到地下市場的人，只能把它當成一般的菸看待，無法理解或兌換中華菸應有的不法價值。

在數位時代下，虛擬貨幣（Virtual Currency）[2] 可以和「中華菸」一樣具有在哪些主體間移動追查不易及移動方便的效果，而且虛擬貨幣可以存於無形，交易於無形，連菸包都看不到，用傳統實體追查的方式查緝機會極低，非法利用效果更佳。在虛擬貨幣的發展史中，「促進犯罪」當然也占有一席之地，例如 2011 年在暗網建構的毒品、槍枝等黑市交易平台「絲路」之所以能成功，很重要的關鍵因素之一就是使用匿名性且移轉便利的虛擬貨幣「比特幣」（Bitcoin）作為價值載具。因此，從事犯罪調查工作的人，或許不用每個人都深入了解程式碼如何編寫等技術議題，但必需了解基本的虛擬貨幣概念及應用，不要被根本不懂虛擬貨幣的罪犯，只是粗糙的背誦犯罪集團提供的應付檢警調教戰手冊話術而戲弄，且至少在案件需要時，能作基本查證和分析，甚至和虛擬貨幣技術專家溝通，請求協助查知偵辦所需之事證。

筆者並非虛擬貨幣技術專家，無意也無能力精準詳細介紹所有虛擬貨幣的理論及操作，只是綜合研讀虛擬貨幣不

1. 本文主要由臺灣新北地方檢署檢察官李秉錡撰文；臺灣高等檢察署檢察官古慧珍協助提供 2022 年 4 月 15 日「利用加密虛擬貨幣從事毒品犯罪之防制作為」研商會議後的彙整意見。
2. 虛擬貨幣可不可以稱作「貨幣」有極大爭議，主要是因為貨幣應該要在特定區域內有全面的流通性，而此全面性需要有法規作支持，即為法償性，而虛擬貨幣雖然在特定群體間有流通性，但在沒有法償性前提下，顯然不具備全面的流通性，因此，多數國家官方都保守稱此為虛擬「資產」或「通貨」。惟本文是要從犯罪使用和預防的角度討論此問題，因此仍以通用語虛擬貨幣稱之。

法使用的資料及偵辦過的案件經驗，盡可能以容易理解的文句，概略分享偵辦利用虛擬貨幣犯罪應知悉的基本概念。以下將先鳥瞰虛擬貨幣在犯罪世界應用情況，再針對本文重心「利用加密虛擬貨幣從事賄選犯罪」，利用四個假設情境[3]介紹虛擬貨幣基本概念及可能之因應，另外，本文亦從法制架構及一般性預防角度，提出對虛擬貨幣業的管制建議，最後簡要整理本文結論。

貳、從犯罪角度看加密虛擬貨幣應用

一、虛擬貨幣多元應用的趨勢已形成

加密虛擬貨幣如同其名，並無「實體」的物表彰其價值，它只是一個「虛擬」的數位記錄，而在開發原始碼的時代，要創造各式各樣的數位記錄（即虛擬貨幣），在技術上都不是難事。目前市面上已經有超過16,000種虛擬貨幣，但數位記錄本身原則上是沒有價值的（某些NFT[4]除外，文後介紹），所以創造虛擬貨幣後，必需要賦予它價值，在市場上吸引人來買這個數位記錄，這才是難事。而吸引人的手法，不外乎就是講故事，講一個讓人相信這個虛擬貨幣可以保值、增值，或者如何在真實世界換取商品或服務等等的故事，而要讓這個故事看起來可信，可以設計公平合理的程式邏輯運作確保它的價值，也可以用真實世界的法定貨幣或其他資產作擔保，也可以找有名望的人來見證或承諾，甚至可以實際舉辦活動讓虛擬貨幣真實兌換成商品或服務，手法相當多元。當人們相信虛擬貨幣有價值，就會願意用真實世界有價值的東西去交換這個虛擬貨幣（例如用現金去買虛擬貨幣，或接受虛擬貨幣購買商品），當越多人相信虛擬貨幣有價值，虛擬貨幣交易市場就會形成，就具備流通性了，又因為虛擬貨幣本質上是數位記錄，而數位世界沒有國界，所以虛擬貨幣的市場流通是全球性的，相較於傳統法定貨幣有國內流通使用的限制，虛擬貨幣作為表彰價值的新興工具，在價值移動的市場上有極大的優勢。

二、虛擬貨幣的不法利用的模型

虛擬貨幣是中性的，對社會影響是好或壞，取決於使用人如何使用，以及政府如何監理管制，而本文是從犯罪防制角度撰文，因此重心會放在虛擬貨幣的非法使用面討論，其中又以「匿名性」最為關鍵。虛擬貨幣擁有者的身分具有高度隱匿性，尤其是以同樣具有匿名性的真實世界價值表彰工具「現金」購買虛擬貨幣，再讓虛擬貨幣在不同錢包地址移動，最後再以現金形式回到真實世界，將會使價值移動軌跡的透明度降到非常低，若有犯罪集團想要避免犯罪偵查單位透過價值移動軌跡查知犯罪或洗錢行為人，虛擬貨幣就會是很好的工具。

再者，因為我國並未全面禁止虛擬貨幣交易，而虛擬貨幣的價值取決於故事取信於大眾的強度及廣度，這些故事五花八門且推陳出新速度非常快，市場上很多投資者並沒有清楚了解故事的真實性，在沒有監管機關作基礎把關，投資者盲目跟風投資，有些故事根本上就是虛構的詐欺腳本，利用虛擬貨幣詐欺顯然成為犯罪集團一門好的生意，且嗣後東窗事發，因為虛擬貨幣的匿名性，就算知道詐欺所使用的虛擬貨幣移動軌跡，也很難查知背後操控錢包地址之人身分，這些詐欺詐團只需要再發行一種新的虛擬貨幣，講一個新的故事，就可以重操舊業了[5]。

此外，多數的虛擬貨幣是小眾市場，亦即只有少部分相信的人認可它的價值並願意投資交易，而這個價值高低取決於參與者的「主觀」想法，很難有

3. 這四個例子都是筆者自行發想，非真實或改編自真實案例，筆者是為了帶出虛擬貨幣的概念而刻意設例，讀者無需深究案件發生的可能性。
4. NFT（Non-Fungible Token, 簡稱NFT）異質化代幣，詳後述。

客觀標準，因此就存在了「以投資交易之名，行流通黑錢之實」的空間。深言之，只要有一群人相信市場上會有人以適當的價格收取特定虛擬貨幣，這群人不管此幣的來源為何，認幣不認人，此幣就可以當成乘載犯罪所得的價值載具，在這一群人中任意變現，如果犯罪偵查單位查扣到某人有這個虛擬貨幣，該人只是主觀上相信這個貨幣的價值，且該貨幣確實存在小眾市場，很難僅憑此認定該人有何違法，縱使查扣該貨幣實益也不大，因為除了這一群人之外，找不到適當市場變現，很可能淪為一堆沒有意義的電子紀錄。

參、加密虛擬貨幣運用在賄選犯罪之可能及因應

隨著虛擬貨幣技術的成熟與普及，個人使用虛擬貨幣門檻逐漸降低，虛擬貨幣極有可能被用來當成選舉犯罪工具，對2022年底地方公職人員選舉產生衝擊之風險性，也大幅提高。而什麼是「賄選犯罪」？賄選，就是利用金錢或其他不正利益影響選舉投票公正性的不法行為。不正利益，則是指足以供人需要或滿足人慾望的一切有形或無形利益，且不以經濟上之利益為限，例如：提供或介紹工作機會或職位，也算是不正利益。又依照公職人員選舉罷免法、刑法規定，依行使賄選的對象區分，可分成三大類：（一）對候選人的行賄。（二）對有投票權人的行賄。（三）假借捐助名義對團體、機構的行賄[6]。若依據賄選提供或交付利益的態樣區分，常見的態樣有：現金買票、禮品賄選、餐會賄選、旅遊賄選等類型。由於虛擬貨幣去中心化、匿名性，以虛擬貨幣作為期約、交付賄賂之工具，不易被查覺且難以追查，可能成為年底九合一選舉各候選人進行賄選之新興手法。以下嘗試列舉利用虛擬貨幣從事賄選犯罪的幾種可能情境：

一、以直接轉發虛擬貨幣方式行賄

1、設例

候選人小李的團隊想要以各100萬元鞏固選區的5位樁腳，請樁腳協助拉票，先找幣商用現金面交方式以500萬元買等值17.86萬顆USDT（1:28計算），並準備五個硬體錢包，直接要求幣商將USDT分成五等份，各3.572萬顆存在硬體錢包中，將硬體錢包交付給5位樁腳，並請盡量在選後再找幣商兌換成現金。

（小李及其樁腳向有投票權人行求、期約或交付賄賂或不正利益時，可能涉犯公職人員選舉罷免法第99條罪嫌。）

2、技術基本觀念

(1)虛擬貨幣

虛擬貨幣的近代簡史可以從2008年說起，當時全球正處於金融海嘯的苦悶中，而美國政府強力介入，推出量化寬鬆制度，在市場上大量投入美金，試圖振興經濟，但這個舉動使美金貶值，引

5. 相關案例有興趣可以參考近日有人公布黃立成利用虛擬貨幣不法獲利的「麻吉大哥的故事：22,000 ETH 被挪用、超過 10 個項目失敗」調查內容，https://www.blocktempo.com/22000eth-embezzled-10-projects-failed-machi-big-brother-story/。

6.（一）依照公職人員選舉罷免法規定，對候選人（或具有候選人資格的人）以金錢或其他不正利益，要求候選人（或具有候選人資格的人）『放棄競選或為一定之競選活動』，處最輕本刑3年以上有期徒刑；若候選人（或具有候選人資格的人），同意『放棄競選或為一定之競選活動』，亦有相同的罪責。（二）依照公職人員選舉罷免法及刑法的規定，對有投票權人以金錢或其他不正利益，要求有投票權人『不行使投票權或為一定之行使（如：投票給某特定候選人）』，處最輕本刑3年以上有期徒刑；而有投票權人同意『不行使投票權或為一定之行使（如：投票給某特定候選人）』，則依刑法規定處以3年以下有期徒刑。（三）依照公職人員選舉罷免法規定，對於選舉區內的團體或機構，假借捐助名義，以金錢或其他不正利益，使其團體或機構的成員『不行使投票權或為一定之行使（如：投票給某特定候選人）』，處最輕本刑1年以上有期徒刑；而團體或機構的成員有受賄的行為，則回歸刑法的規定處罰之。

來不少批評，甚至有些自由派人士在思考每個國家的法定貨幣都很容易受到政府操控，且法定貨幣在銀行體系流通，也很容易被政府監控，如果市場上的貨幣可以擺脫政府的手，達到去中心化，獲得完全的自由該有多好，而中本聰[7]在此之際推出的比特幣白皮書正好趕上時代，成為虛擬貨幣爆發的引線。

比特幣有二大重點，一是「去中心化」，二是「區塊鏈」（blockchain）。去中心化強調透過公鑰加密電子郵件並搭配私鑰的制度完成帳戶位址對帳戶位址的點對點交易，不需透過權威中心認證也無從干預；區塊鏈強調不可竄改性，願意參與這個制度的人都可以把自己的電腦當成節點，無數多台節點中都有一套所有比特幣的交易記錄總帳，透過這種分散式記帳方式，避免有心人士竄改紀錄，而此記帳方式是讓節點將數個有效的點對點交易打包成區塊，並透過加密及獎勵最快解密者（俗稱挖礦）的機制，將含有交易的區塊加到總帳戶中，形成區塊相連的區塊鏈。

比特幣於2022年5月間，市值超過5,600億美元，若把它當成一個國家的法定貨幣，可排在全球前20名。由此可知，比特幣的運作方式成功獲得市場的高度認可，尤其是它的區塊鏈概念成為後來所有虛擬貨幣的基石，但比特幣系統的設計只限於記錄比特幣的點對點移轉，功能相當陽春。而野心更大的以太坊（Ethereum）系統趁勢而起，這個系統有二套區塊鏈：一個區塊鏈是記錄以太幣及利用以太坊系統所發行的虛擬貨幣移轉，類似比特幣移轉的區塊鏈；，另一個比較特殊的是「智能合約（Smart Contract）」區塊鏈，這個區塊鏈又開啓後來虛擬貨幣百花齊放的時代。

(2)穩定幣

穩定幣強調其幣值恆定特定法定貨幣，最有名的穩定幣是2014年由泰達公司（Tether Limited）發行的USDT（泰達幣）。泰達公司透過持有發行量等值的美金或相關資產作擔保，讓USDT價值恆定美金，當USDT價值跌破1美元，玩家可將手上的USDT以1美元賣回給泰達公司，只要市場信心及流通性足夠，就可避免USDT價值低於1美元；反之，如果USDT市場價格過高，泰達公司就會在市場上放出更多USDT，讓USDT價格回到1美元。此外，USDT的交易方式，也是透過區塊鏈方式記帳，不過值得注意的是，泰達公司有在不同系統的區塊鏈上發行USDT，目前發行最多的是在以太坊系統及波場（TRON）系統上的區塊鏈上，而不同區塊鏈上所使用的帳戶地址（又稱電子錢包）並不相容。

USDT在2022年5月間，其市值超過700億美元，僅次於比特幣和以太幣，但其單日交易量超過500億美元，交易量是所有虛擬貨幣之冠。而其交易量如此之大，最大的原因就是它的穩定性，虛擬貨幣的玩家想要透過不同的虛擬貨幣漲跌賺價差，但如果每次買賣都要用法定貨幣相當不方便，所以玩家多會先用法定貨幣買入USDT，在特定虛擬貨幣低點時用USDT買入，高點時賣出換回USDT，將價值停泊在較穩定的USDT，等待下次好的機會再入場低買高賣，不斷累積USDT，直到想退出這個市場或特殊需求才換回法定貨幣。

(3)冷錢包

虛擬貨幣錢包（Cryptocurrency wallet）是用來記錄持有多少虛擬貨幣，本質就是一個帳戶地址。虛擬貨幣移轉，是利用密碼學搭配區塊鏈的記帳技術，在某個系統的區塊鏈上記錄某個虛擬貨幣從A帳戶地址移轉到B帳戶地址，所以，要在區塊鏈上記錄持有虛擬貨幣的前提，是要先有一個帳戶地址，這個帳戶地址內有多少虛擬貨幣是公開資訊，任何人都可以在區塊鏈上輕易查知。另

7. 此人真實身分不詳，是公認比特幣的發行者，其身分介紹可參https://zh.wikipedia.org/zh-tw/%E4%B8%AD%E6%9C%AC%E8%81%AA。

外，玩家取得帳戶地址同時，會取得一組對應該地址的公鑰（Public Key）和私鑰（Private key），私鑰表彰了帳戶地址的所有權，當玩家想要移轉虛擬貨幣給別人時，需要用私鑰簽名授權，私鑰極其重要，帳戶地址內的虛擬貨幣移轉認私鑰不認人，而私鑰是一長串超過50個數字及英文字母組合起來的亂碼[8]，人腦難以熟背，所以如何保存私鑰是玩家最重視的議題之一。

虛擬貨幣錢包的分類，可用有無自己記錄、保存私鑰分成「託管錢包（custodial wallet）」和「非託管錢包（Non- custodial wallet）」。所謂，「託管錢包（custodial wallet）」是指，有些玩家不想費心保存記錄私鑰，就會把虛擬貨幣錢包託管給託管平台，可能是交易所或保管商，玩家如果有需要，還是可以有一個錢包地址讓其他人把虛擬貨幣轉入或轉出給其他人[9]，這時不需要使用私鑰，而是改用託管平台的驗證身分機制確認身分，託管最主要的好處就是方便交易，壞處就是託管商存有倒閉的信用風險。反之，由自己記錄、保存私鑰的電子錢包就是「非託管錢包」。「非託管錢包」又可再以玩家保存記錄私鑰的方式有無連網，區分成熱錢包（Hot Wallet）和冷錢包（Cold Wallet）：前者，玩家可以利用瀏覽器或電子錢包APP儲存私鑰，只要連網，使用熱錢包平台的密碼就可以呼叫出私鑰來移轉虛擬貨幣，這種熱錢包最主要的好處是方便存取，壞處就是連網有被駭客盜取的風險；反之，不透過網路保存私鑰的錢包就是冷錢包，常見的就是類似USB裝置的硬體錢包（Hardware wallet），用這個儲存私鑰，只要將硬體錢包插入在電腦，輸入PIN碼就可叫出私鑰，從電腦拔除，儲存私鑰的裝置就與網路斷開，不用擔心駭客盜取。另外，最陽春的冷錢包就是不借助任何平台或裝置，自己把私鑰列印在紙上保存的紙錢包。

3、技術偵查難點

(1)「非託管錢包」控制權人身分查緝困難

犯罪集團主要是想利用虛擬貨幣當作承載犯罪所得的載具，並非想透過虛擬貨幣賺價差，所以，流通性最高的穩定幣USDT是實務上最常見到的犯罪或洗錢載具。又託管錢包平台，目前多會執行確認客戶身分（Know your customer；KYC）等洗錢防制程序，犯罪集團為避免身分曝光，自然會優先考慮使用「非託管錢包」。以設例來說，如果有幸找到椿腳的硬體錢包並查知地址，就可輕易的在區塊鏈上查到公開透明的交易紀錄，溯源查知上手的錢包地址；但只要該地址是「非託管錢包」，要查知該錢包地址的控制權人身分就相當困難，即很難從椿腳的錢包地址回溯確認幣商的身分，進而再向上查到候選人小李的團隊。

(2)幣商以現金交易虛擬貨幣查緝困難

買賣虛擬貨幣的管道，主要是到交易所買賣或找個人幣商買賣，而因為交易所一樣多會履行洗錢防制程序，所以不問身分，不問資金來源的個人幣商，就會是犯罪集團的首選。幣商的工作是媒合買賣雙方交易虛擬貨幣，利基在於能找到出高價的買家及出低價的賣家，

8. 例如密碼為「5f2f318d1dc28ff71a72218c8705893960be5540b2217e1328d5e260d36323bd」。

9. 交易所會有自己的大錢包地址，存放交易所自己的虛擬貨幣，如果玩家只是單純的向交易所買或賣虛擬貨幣，試圖賺取中間價差，沒有要向交易所以外的人移轉或接受虛擬貨幣，這時有些交易所可能只會在自己的系統紀錄該玩家有多少數量的虛擬貨幣，但不會幫玩家創造一個錢包地址，並將虛擬貨幣從自己的大錢包轉到該地址，因為將移轉虛擬貨幣的記錄上到區塊鏈需要費用，若玩家只是單純的和交易所交易，對交易所而言，只需要紀錄在自己的系統，不需要支出費用上到區塊鏈上，所以有些交易所就不會提供這種玩家錢包地址。

從中賺取利差及手續費，所以幣商多不會讓買賣雙方直接聯繫，否則之後的交易就很可能直接跳過幣商，不讓幣商賺一手。幣商找買家或賣家的管道，常見是在Telegram（俗稱紙飛機）等通訊軟體內的群組找人，幣商與這些人多數都是陌生人，沒有信賴關係，交易金額只要大一點，多會約面交，避免他方不轉幣或付錢。以設例來說，如果透過交易紀錄溯源找到幣商，並有幸查知幣商身分，就可以詢問幣商是誰付錢給幣商，讓幣商轉幣給椿腳的？但很多幣商根本就不知道買、賣家是誰，甚至避免知道客戶身分，很可能無法確認付款的買家身分，或充其量只知道是某個軟體暱稱者，真實身分不明，一樣很難查到候選人小李的團隊。

4、偵查突破思考

(1)即時查詢虛擬貨幣的移轉軌跡

虛擬貨幣不論使用什麼錢包，所有交易紀錄都要上傳區塊鏈，因此如果在偵查個案中發現電子錢包地址，可以自行上網使用免費資源查知該錢包地址是否確實存在，以及該錢包地址現存的虛擬貨幣數量及過往移轉紀錄。具體上要查詢時，首先要知道該電子錢包地址及虛擬貨幣移轉是透過哪個系統下的區塊鏈，搞錯區塊鏈會查不到錢包地址的資訊，例如：USDT支援在數個區塊鏈上保存及移轉[10]，但多數都集中在「以太坊」和「波場」二大區塊鏈，而判斷USDT在哪個區塊鏈上交易最簡易的方式是看電子錢包的開頭，如果是「0x」[11]就是以太坊；如果是「T」[12]就是波場。確認後就可以到相關查詢網站查該錢包及交易，例如：在以太坊移轉的USDT，可以透過「Etherscan」網站[13]，將要查的錢包地址完整打在該網站內的搜索欄位中查詢，甚至可以將該錢包的歷史移轉紀錄下載成excel檔分析，如果在波場移轉，則可以透過「TRONSCAN」網站[14]查詢。此外，「OKlink」網站[15]還有提供特定期間內錢包地址的溯源視覺化交易查詢分析，可清楚知道幣從哪裡來，跑去哪裡，有無在相關地址內循環移轉，找到關聯錢包。

(2)搜索要注意電子錢包的線索

虛擬貨幣本質上是電子紀錄，所以如果有搜索，一定要注意電腦、手機、平版或其他載具，查看有無上虛擬貨幣交易所的網站紀錄或使用行動載具的交易所APP的情況。如果有，該人很可能有在使用託管錢包，最好能直接向該人詢問平台會員帳號密碼，再登入查知錢包地址及交易明細，如果該人不願意提供，可以嘗試查看網站、APP有無記憶登錄的帳號或代號，或以該人的個人資料向該平台查詢。此外，也可以查看照片、記事本或其他檔案中有無一長穿數字和字碼的亂碼，或者翻拍的QR Code，這些都有可能是錢包地址。

又如果是熱錢包，一樣可以注意電腦的上網歷程、桌機下載的桌面錢包，或手機、平版等行動載具下載的行動錢包APP[16]，如果是硬體錢包，則要注意有無類似USB、汽車搖控器、簡報筆等樣式的不明載具，這些都有可能是硬體錢包[17]。而使用這些非託管錢包，玩家要自己保管私鑰，私鑰原型是一長串亂碼，但私鑰很難記，多數熱錢包平台會讓玩家以自設密碼加密私鑰，只要打入自設密碼就可以叫出私鑰要操作錢包內的虛

10. 泰達公司官網公告支援Bitcoin (Omni & Liquid protocol), Ethereum, TRON, EOS, Algorand, Solana, OMG Network, and Bitcoin Cash (SLP). 等區塊鏈系統。
11. 例如「0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8」。
12. 例如「TY39KopmB4q3y4WcYmPbLeDXojPcPdnqfz」。
13. 可GOOGLE查詢網站，或直接輸入網址https://etherscan.io/。
14. 可GOOGLE查詢網站，或直接輸入網址https://tronscan.org/#/。
15. 可GOOGLE查詢網站，或直接輸入網址https://www.oklink.com/en。這個網站相當好用，筆者在許多個案中都有使用並找到重要線索，非常值得推薦。

擬貨幣，但平台怕玩家忘記自設密碼，多會再使用「助記詞」讓玩家有第二個選擇控制錢包，擁有助記詞就和擁有私鑰一樣可以移轉錢包內的虛擬貨幣，而助記詞是由12、15、18、21個固定順序英文單字組成[18]，最後一個選擇就是讓玩家可以以原始亂碼或QR Code匯出私鑰，並印下來保存。所以在搜索時，如果發現電腦文件、照片、筆記本等中有一長串亂碼、QR Code或標記順序的無關聯單字都要連想到有可能是私鑰。

(3)訊問交易虛擬貨幣者專業交易細節問題

投資虛擬貨幣獲利是近年火紅的議題，但與此同時，犯罪者也看上虛擬貨幣的匿名性來操作犯罪或洗錢，如果他們被發現有在碰觸虛擬貨幣，一定也會想辦法佯裝自己和其他人一樣是在投資虛擬貨幣獲利，企圖以他人的合法交易掩飾自己的非法交易。而這些人有的根本都不太了解投資虛擬貨幣如何獲利。因此，在發現案件中有牽涉到虛擬貨幣，最好提前查知錢包地址的移轉紀錄，第一次詢問時，如果錢包持有人表現出不甚了解的態樣，就要展現對虛擬貨幣的專業了解，並拿出準備好的交易紀錄等實證給持有人解釋，讓持有人供出虛擬貨幣在犯罪過程中扮演的角色。以設例觀之，如果執行對象是椿腳，並扣到硬體錢包，可以問他們為什麼要花錢買硬體錢包？用熱錢包不是很方便嗎？為何要挑這個牌子的硬體錢包？裡面有多少個錢包地址？如何操作？哪裡買的？虛擬貨幣具體交易的時間、地點、對象？交易上鏈等了多久時間？如果有椿腳不太懂，就可以質問該椿腳是何人指示或教導他使用或持有虛擬貨幣？試圖找到關鍵證人加以突破。

(4)傳統偵查手法同步進行

虛擬貨幣在任何犯罪中充其量也只是扮演承載犯罪所得的載具，但犯罪的全貌絕對不只有犯罪所得，還有涉案人的動機、共犯的連結關係、涉案人移動軌跡等多樣線索。所以在偵查犯罪時，千萬不要陷入看到虛擬貨幣就覺得很難偵辦而消極搜證，這世上沒有完美的犯罪，不要放棄任何線索，一定可以找到突破點，所以在查虛擬貨幣的同時，傳統偵查手法也要同步進行。以設例觀之，五位椿腳平常的移動軌跡、通聯紀錄、銀行帳戶、刷卡紀錄等事證，都有可能串起與候選人小李團隊的關連性，或者監聽到五位椿腳有向小李團隊成員回報拉票進度等，都有助於本案偵辦。而建立對虛擬貨幣的了解，只是更有助於案件的釐清或找到突破點的機會罷了。

二、以智能合約方式行賄

1、設例

候選人小王的團隊設計一個「Wang Win」智能合約，合約內容是玩家支付0.1個USDT(大約3元)，且特定條件成就後第60天，自動從合約附加的錢包地址向玩家移轉100個USDT(大約3000元，移轉到乙方支付0.1個USDT的錢包地址)，而特定條件就是「小王當選」，並透過預言機獲知此條件是否成就，另合約創造人需先向合約附加之錢包地址移轉20萬個USDT，合約才開始執行，且最大容許玩家數為2000人，將此合約部署在以太坊。候選人小王的團隊隨即移轉20萬個USDT啟動此合約，並委由社群媒體分析公司，針對小王選區內的無政黨傾向選民小規模投放精準廣告，以近乎無償的方式誘使此類選民參與合約，而參與的選民為取得合約的100個USDT，會提高投票給小王之動機。

16. 目前實務上常見的有imToken、MetaMask等行動錢包APP，建議可以下載APP實際操作，會更清楚錢包地址的概念。
17. 建議可以GOOGLE了解硬體錢包的樣式，就可以更清楚了解。
18. 例 如「1.erase 2.edit 3.chest 4.close 5.disease 6.unhappy 7.ten 8.museum 9.novel 10.faculty 11.upper 12.february」。

（小王及其團隊對有投票權人投放廣告時，已可能涉犯公職人員選舉罷免法第99條罪嫌；有投票權之選民於參與合約時，知悉小王當選後即可取得100個USDT，即可能涉犯刑法第143條罪嫌。）

2、技術基本觀念

(1)以太坊與以太幣

比特幣所屬的系統是一個獨立的區塊鏈系統，在這個鏈上功能比較陽春，只有帳戶地址，記錄虛擬貨幣的移轉。以太坊系統又是另一個獨立的區塊鏈，功能更強大，它有二種地址，一種是外部地址，主要是記錄虛擬貨幣的移轉，和比特幣所屬系統的帳戶地址功能雷同，操控這個地址的虛擬貨幣需要用私鑰來啟動。另一種是合約地址，玩家可以在區塊鏈上部署智能合約，部署完成就會產生合約地址，這個地址上的合約完全由合約的程式邏輯執行，沒有私鑰，沒人可以操控，而部署合約及未來合約的執行都需要用以太坊的原生幣「以太幣」來支付燃料費，呼叫合約運作。

(2)智能合約

智能合約可以把它想成是一個遊戲或制度的「運作規則」，發行人設計好這個規則後，會上傳在公開的區塊鏈上，讓專業玩家檢視這個遊戲或制度是否公平。一般玩家可以直接玩看看是否吸引人，而這種遊戲或制度的應用層面非常廣，包括發行自己專屬的代幣、開發一套線上遊戲等都可以是智能合約，凡是可以把遊戲或制度編寫成「若…則…」（if…then…）的條件程式碼，都可以編寫成智能合約，編寫完成就可部署在區塊鏈（目前多數都是在以太坊）上，部署後縱使是編寫人都無法再更改合約[19]，這個運作規則已經無法再調整了，只要合約接收到條件成就的訊息，就會自動執行。這種智能合約的好處在於，凡是能條件化的事情，都可以編寫成程式，而且無數個條件綑綁包裝成多複雜都沒關係，演算法都能執行，甚至將應用程式（APP，傳統上是利用一個中央伺服器在運作，有人為操作的機會）上鏈成為去中心化應用程式（DAPP）都可以，而且這些合約上鏈後公開透明，任何人都能檢視合約內容是否合理公平，再決定是否要參與這個合約（例如有些手遊APP和玩家說抽中寶物的機率是1%，但不公開的系統設定機率卻是0.1%，DAPP可避免這個問題）。最重要的是合約上連後，就不再允許任何人為介入，凡是按合約規則走，演算法自動執行，不用擔心條件成就後有不履行的情況發生。

(3)預言機

智能合約的條件可以是真實世界的一個事實發生，例如「小王當選」，但

19. 這裡講的無法再更改合約是指不能改已上區塊鏈的這個合約，但如果智能合約中計設符合一定條件，則變更合約中設定的某個機制，那就可以改變智能合約原本設定的機制，但這個機制改變不是嗣後去改一開始上區塊鏈的合約程式碼，而是因為符合合約明定的條件所以改變。現在有些去中心化自治組織（Decentralized Autonomous Organization；DAO）會設計二個智能合約，一個是治理代幣（Governance Token）合約，一個是某種制度運作的合約，前者設計成擁有治理代幣的人可以有投票權，符合特定投票權比例就可以決定後者合約條件是否更改或是否成就，舉例來說，設計一個治理代幣「Singer Token」合約，再設計一個票選「年度最佳歌手」的合約，任何人都可以向合約支付10個USDT而將歌手列在參選名單，而擁有治理代幣「Singer Token」的玩家可以參與投票，以曆制年為單位，最高票者可以獲得當年度最後一天後者合約內所有USDT的70%充當獎金，且擁有「Singer Token」的玩家，都可以在後者合約提出增加參選歌手之某些資格限制或調整獲獎歌手獎金比例的權利，提出後如果一個月內有「Singer Token」發行量過半數投票同意，則可變更之。目前治理代幣圈最有名的是從事去中間化金融（Decentralized Finance；DEFI）業務的「maker DAO」發行的「MKR」治理代幣，「maker DAO」一開始的主要業務是利用智能合約發行去中間化的穩定幣「DAI」，擁用「MKR」代幣的人就像是經營這個DEFI業務的股東，可以投票決定穩定幣「DAI」業務的相關協議，目前「maker DAO」的運作已經進化且相當複雜，有興趣可自行上網用關鍵字「DAO maker」搜尋相關資料閱讀。

合約要在沒有人為介入的情況下正確獲得小王當選與否的訊息，避免有心人士讓合約獲取錯誤的資訊而導致錯誤的結果，如果只是直接去中選會的網站自動搜尋當選資料，有心人士可以在特定時間癱瘓或竄改該網站，讓錯誤的資訊上鏈，這時合約獲得不正確的條件，當然就會執行出錯誤的結果，且上鏈後的不可竄改性，將使這個錯誤無法弭補，因此如何在把外部數據正確導入區塊鏈，將會是智能合約能否大放異彩的關鍵。目前多數智能合約要接收外部數據，多會利用預言機（oracle）[20]，這是一種資訊提供商，確保提供正確的外部數據輸入智能合約的區塊鏈以驅動合約正確執行。

3、技術偵查難點

(1)智能合約創造者的身分難以確認

在以太坊上鏈的智能合約一樣是公開透明，可以在「Etherscan」網站首頁的搜尋欄位輸入合約地址查知合約。在合約地址頁面可以看到「Transactions」的項目，這個意思是智能合約雖然是由合約的程序邏輯執行，但還是要有人支付燃料費呼叫合約執行。「Transactions」就是記錄誰在呼叫合約，這紀錄的欄位「From」就是呼叫合約並支付燃料費的外部地址，而第一筆紀錄必然是有人支付燃料費而創造合約，「Transactions」是以時間近到遠排列，所以要拉到最後一筆才會看到是哪個外部地址為了「Contract Creation」而支付燃料費，該人就是創造者，但這個外部地址就是前面講的電子錢包，具有匿名性，且許多合約創造人會有使用專屬外外部地址創造合約，之後就不再使用該地址，因此很難從合約或嗣後的呼叫執行等資訊查知該人真實身分。

(2)從智能合約其他資訊亦難查知創造人的身分

在「Etherscan」網站中的合約地址頁面，除了看到「Transactions」的項目外，還可以看到「Internal Txns」項目，這是記錄因合約執行而移轉以太幣到哪些外部地址；「Erc20 Token Txns」項目，這是記錄因合約執行而移轉Erc20協議代幣到哪些外部地址；「Contract」項目，這是記錄合約內容；「Events」項目，這是記錄外部地址呼叫合約執行什麼指令；「Analytics」項目，這是網站提供的額外分析，可以從時間軸瀏覽呼叫合約的情況、合約價值餘額等資訊；「Comments」項目，這是讓玩家來留言評論。這些資訊看起來相當豐富，但要深入分析並不容易，且這些資訊大多是合約創造後的參與執行資訊，縱使合約創造人亦有參與其中的過程，但只要他想要隱藏真實身分，使用多個一次性外部地址，亦難查知。

4、偵查突破思考

(1)找專家協助分析合約相關資訊

如果這個合約是熱門合約，有許多玩家在玩，區塊鏈上的公開資訊其實已經相當豐富，只是我們閱讀程式碼的能力有限，且逐一查詢相關外部地址相當費時，所以需要專業人士協助我們分析。以設例觀之，案件偵查的起點，很可能是參與的玩家講出這個合約，這時可以先向玩家索取其參與的外部地址及該合約地址，再自行上網確認玩家所講的地址是否真實存在，初步判斷確實存在，且有多位玩家參與合約，就可以找專家分析合約。「Wang Win」合約需要先由創造者投入20萬個USDT，所以可以從順著投入20萬個USDT的外部地址查虛

20.2020年夏天，去中心化金融DEFI快速發展，而預言機技術市場領先者「Chainlink」所發行的「LINK」代幣當時也水漲船高，DEFI業務和預言機技術相生相息，因為去中心化金融業務許多還是要連結實體商品價格、指數、股價等實體金融業務的資訊，為了正確將實體資訊上鏈，預言機成為當時非常重要的存在。

擬貨幣的來源找合約創造者的線索，雖然不容易，但值得一試，另外，也可以從參與合約的玩家外部地址試著找出更多的玩家。

(2)從選民玩家切入找線索

以設例觀之，智能合約只是工具，目的是要用USDT利益換取選民投票，所以候選人小王團隊會盡可能讓參與的玩家是選區選民，或可影響投票意願之人。因此可從玩家切入，詢問玩家為何會知道「Wang Win」智能合約？能否幫忙查找有無其他親友鄰居也參與此合約？如果能找到更多的玩家，就可以分析這些玩家的共通點，例如是否都是小王選區的選民？是否都是看到同一個廣告而參與等線索？如果知道這些廣告是在某幾個社群媒體平台推播，則可進一步向平台查詢是何人投放廣告，且投放廣告的群眾對象如何設定，再循投放廣告者的身分向上追查。

(3)傳統偵查手法同步進行

以設例觀之，發現有人部署「Wang Win」智能合約，讓玩家在小王當選後獲取報酬，必然會聯想到小王團隊有牽涉其中，所以傳統監控小王的手法一樣可以使用，包括：打聽小王團隊中有無對虛擬貨幣較熟悉的成員、查找小王或其家屬或其核心團隊成員有無大額提款金額合計達600萬元(約20萬個USDT)等。如果有搜索時，一樣要注意與外部地址、合約地址，或者其他相關虛擬貨幣的事證，所有的電子設備載具都要查扣並盡速分析，另外，在執行前要讓參與之執法人員都對本案的虛擬貨幣運用有基本概念，避免重要證據在眼前，卻發生「心中無概念，證據看不見」的憾事。

三、以發行專屬代幣方式行賄

1、設例

候選人小明的團隊利用ERC20協議架構發行100萬顆日月幣，並以「虛擬貨幣推廣基金會」名義，在選前3個月左右，在選區內舉辦多場「認識虛擬貨幣」活動，吸引有興趣的人報名參加(非選區選民亦可參加，參加者請自備支援以太坊的虛擬貨幣錢包)，並在活動當場以有獎徵答方式，從報名名單中大量找選區有投票權的選民贈送1個日月幣，且聲稱日月幣只是活動教學用並無價值。後來在選前1個月左右，透過境外消息管道放出消息「如果小明當選，將建立日月幣的商品生態區，可使用日月幣作網路交易，且於小明就職後一年內，日月幣會在虛擬貨幣交易平台上架，交易價值取決上架當時市場的認同，很可能落在50到100元美金，聽說已經有人在用1000元新臺幣收日月幣」，已獲贈日月幣之選民，為使日月幣順利上架交易而獲利，提高投票給小明之動機。

(小明於選前1月放出消息影響選民投票意願，而此迂迴方式對有投票權人行求賄賂而約其為一定投票權之行使，可能涉犯公職人員選舉罷免法第99條罪嫌。)

2、技術基本觀念

(1)ERC20協議

以太坊為了讓部署在區塊鏈上的合約有一套基本規則，因此針對常用的功能合約發佈協議(Ethereum Request for Comment；ERC)，這些協議提供了常見的智能合約所需的功能程式碼，讓創造者可以方便套用，且按照協議編寫出來的不同合約，還可以相互串連。目前最常使用的是ERC20同質化代幣(Fungible Token)協議，這個協議中包括了部署同質化代幣合約所需要的所有基本功能程式碼，只要援引ERC20協議，就可以輕易的在以太坊部署專屬代幣合約來發行代幣，前面有介紹泰達公司發行的USDT有支援以太坊的交易，泰達公司就是遵循ERC20協議來發行[21]，但發行代幣不限於大公司，任何人都可以發行，甚至網路上有許多教學影片，幾分鐘內就可以帶玩家利用模版部署好專屬代幣[22]，因此，全球現在有上萬種代幣也就不足為奇了。附帶一提，要

發行代幣不一定要在以太坊的區塊鏈，也可以使用其他的區塊鏈，例如在波場的區塊鏈發行，而波場同樣也有類似ERC20的TRC20，玩家也可以遵循TRC20協議輕易的在波場部署專屬代幣，泰達公司也有在波場的區塊鏈遵循TRC20協議發行USDT。

(2)ICO及STO概念

創造者在區塊鏈上部署好專屬代幣合約，發行出自定數量的專屬代幣，接下來的問題就是要如何賦予這個專屬代幣「價值」，吸引玩家願意參與合約，持有或購買這個專屬代幣，創造者想好一套價值故事後，可以選擇私下找朋友，用口耳相傳的方式找玩家，也可以搞大一點，找一個虛擬貨幣交易所，規畫將此代幣上架到該交易所，讓想要購買這個代幣的玩家，知道有一個公開市場可以出售這個代幣，同時公開一份載明專屬代幣價值故事的「白皮書」，招募玩家向交易所購買代幣，甚至有些還會搭配廣告，再免費空投少量代幣到特定外部地址，引起市場上的注意，加大招募購買的力道，這樣的運作就是「首次代幣發行」（Initial Coin Offering；ICO），這概念很像公司在證券市場募資的「首次公開發行」（Initial public Offering；IPO），所以金管會也有採納這種新的募資模式，讓非上市櫃公司在證券商經營的交易平台發行具證券性質之虛擬通貨（Security Token Offering；STO），且指定此類代幣是證券交易法之有價證券[23]並制定辦法納管，不過這只是多提供一個募資管道的選擇[24]，並不表示沒有遵守STO辦法的發行代幣募資就一定違法。發行代幣的技術本身沒有必要規範，要規範的重點還是要看發行人怎麼講「故事」並讓人相信故事是真的，也就要看是否符合「具證券性質之虛擬通貨」的定義[25]，例如發行人ICO時，沒有說他有出資，代幣當然也不是表彰他的出資，他沒有運用任何資產擔保他的代幣，而是發行限量的代幣，以市場供需決定代幣價值[26]，這樣就不是金管會要納管的範圍，可以自由ICO。簡言之，金管會在發行代幣募資技術中，畫出了一個小範圍納管，但不是全部都管。

3、技術偵查難點

(1)發行代幣者之身分難以確認

發行代幣本質上也是寫一個智能合約，不管將智能合約部署在哪個區塊鏈系統上，一樣很難從部署的合約中查知發行者的身分，一般在網路線上活動最常鎖定該人身分的線索就是IP位址，但在區塊鏈上部署合約的過程中，完全不會留下IP位址，當然無從循此線索查知發行人身分。

(2)發行代幣和故事賦值切割而難以認定對價關係

發行代幣是技術問題，故事賦值是市場問題，前者容易，後者困難，多數情況是以故事賦值為主，發行代幣為輔，這二部分由同一群人緊密合作執行。但如果有人想要從事違法行為，就會考慮將二者切割，就算找到發行代幣者，他們也會辯稱不知道故事賦值者後來如何運用代幣，或者不是以發行代幣者預期計畫運用代幣，簡言之，他們會說自己也是被利用的。以設例觀之，當發行代幣和故事賦值切割，並拉長二者的時間間隔，選民在選前3個月左右，透過有獎徵答拿到「日月幣」的當下，「日月幣」毫無市場價值，這個時間點當然沒有足以影響選民投票給小明的對價關係，但選前1個月左右，故事賦值者開始讓「日月幣」有「預期價值」，就算可以認定這個預期價值足以影響選民投票意向而認定有對價關係，但仍舊無法

21. 泰達公司在以太坊之智能合約地址為「0xdac17f958d2ee523a2206206994597c13d831ec7」。
22. 有興趣可以在YouTube網站上以關鍵字「ERC20教學」搜尋影片，並依照教學嘗試自創代幣，將更有助於了解ERC20協議的強大之處。

直接認定發行人即「虛擬貨幣推廣基金會」是違法行為人，他們很可能會說自己也是被利用的。

4、偵查突破思考

(1)從整體活動中找出相關線索

以設例觀之，「日月幣」是ERC20協議代幣智能合約，可以在「Etherscan」網站找到合約地址，並找到收受日月幣的電子錢包。因為收受日月幣的人沒有意識到要作違法行為，所以可能不會排斥使用託管錢包，因此只要找到有使用託管錢包收受「日月幣」的玩家，可以嘗試向託管平台詢問該玩家的真實身分，如果託管平台在台灣有公司或辦公室，例如：幣託(BitoPro)、MAX等，可以電聯討論如何在平台政策下索取資料，如果沒有或找不到連絡方式，可以在平台網站找尋有無提交執法協助的頁面，例如幣安(Binance)網站首頁就有「執行申請」的選項[27]供執行單位申請查錢包地址之身分。再者，雖然不能從「虛擬貨幣推廣基金會」發行並贈送「日月幣」之活動，就認定此基金會涉有違法，但可以多利用前揭方式找尋取得「日月幣」者之身分，或以到場車牌或其他方式找到參與活動者身分，若有找到這些參與者，就可詢問活動如何宣傳(是否針對選民)？是否知悉更多參與者身分(是否多數是選民)？受贈「日月幣」者有哪些人(是否多數是選民)？進而推論基金會主要是針對選區選民舉辦活動和贈送代幣。

(2)傳統偵查手法同步進行

以設例觀之，整體犯罪計畫軸心還是要提供對價，促使選民票投小明，「虛擬貨幣推廣基金會」非常有可能就是小明團隊在操控，所以要想辦法用傳統偵查手法查出其間的關係，包括人流、金流或地域重疊性等。另外，也可以想辦法找出透過口耳相傳或網路傳播放消息說「日月幣」有預期價值的人是何人？消息來源為何？此外，如果在基金會辦活動前就有收到這種活動情資，一定要有違法風險的敏感度，盡可能安排對虛擬貨幣有概念的人到場搜證，以利後續偵辦。

四、以發行NFT方式行賄

1、設例

候選人江哥的團隊用電腦亂數著色出10,000個同款不同花色的帽子電子圖檔，並在上面編有1-10,000號，且都打上「支持江哥」四個字，再以此發行10,000個NFT鐵粉帽，並在選前100天推出「江哥鐵粉站出來」線上活動，並在活動官網讓選區選民上網登記註冊成為鐵粉，每天從鐵粉中抽出50位贈送NFT鐵粉帽，另外5,000個NFT給椿腳自由發送，並和椿腳說若有選民需要打點，可以給該選民NFT，並回報該選民的NFT編號，請該選民至特定平台上架該NFT，並以新臺幣2,500元折算上架時以太幣顆數掛出售價，團隊人員會在

23. 中華民國108年7月3日金管證發字第1080321164號。

24. STO制度推行至今無人申請，因此金管會於2022年著手放寬相關規範，詳情請參金管會發佈之「金管會進一步放寬證券型虛擬通貨發行(Security Token Offering, STO)相關規範」新聞稿，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202201200002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News。

25. 函令定義「具證券性質之虛擬通貨」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，且具流通性及下列投資性質者：(一)出資人出資。(二)出資於一共同事業或計畫。(三)出資人有獲取利潤之期待。(四)利潤主要取決於發行人或第三人之努力。」

26. 例如比特幣就不符合STO的定義，因為比特幣的白皮書告知比特幣沒有任何資產擔保它的價值。比特幣的發行量限制為2100萬顆，定量後由市場供需決定它的價值，物以稀為貴，當擁有者惜售，市場價格就漲，反之就跌。

3天內購買，以此方式向數百位選民支付2,500元。

（江哥及其椿腳對有投票權人發送NFT時，已可能涉犯公職人員選舉罷免法第99條罪嫌；有投票權之選民於收受該NFT且知悉未來可上架售出時，即可能涉犯刑法第143條罪嫌。）

2、技術基本觀念

(1)NFT異質化代幣基本概念

一般講的代幣是同質化代幣，以前揭「日月幣」為例，甲的1個「日月幣」和乙的1個「日月幣」都表徵同樣的價值，沒有差異性。但有一種代幣強調每1個代幣都是獨一無二的，它不強調流通性，反而強調專屬性，這種代幣叫異質化代幣（Non-fungible token；NFT）。代幣本質上是電子紀錄，只要是電子紀錄都可以轉化並發行代幣，所以在數位時代，任何歌曲、影片、圖畫、文件等數位檔案都可以發行代幣，並且強調檔案代幣化後的獨一無二性，例如在實體唱片式微的年代，歌手製作唱片銷售很多都滯銷而虧損，所以已經很少歌手出唱片，大多是在影音平台上傳新曲MV，所有人都可以免費觀看甚至下載，當然這些人都無法宣稱「擁有」這個MV，而這種模式顯然對很多歌手而言，失去了獲利的機會，相對的，有些歌手的死忠鐵粉以前可以買唱片，透過「擁有」唱片來表示自己是支持歌手的鐵粉，但現在沒有唱片可以買，苦於沒有機會支持歌手，這時NFT就一個新的機會，例如A歌手在平台上傳新單曲MV，同時發行並販售1000個此MV的NFT，這些NFT都是獨一無二的，鐵粉沒機會「擁有」唱片，沒辦法「擁有」影音平台上的MV，但總算可以「擁有」限量MV的NFT了。當然發行人對特定電子紀錄要發行1個或數個NFT都可以，主要是看市場的接受度和發行人的目的，例如世界知名畫家針對某一幅畫，數位化後只發行1個NFT，價值很可能是天文數字，再例如奇摩和家扶基金會有推出小小藝術家[28]，把基金會兒童的畫作拿來發行NFT，每幅畫作發行近百個NFT，定價1000元讓善心人士購買。

NFT的主要功能就是要突顯擁有者的獨特性，發行人發行NFT讓玩家「擁有」，除了彰顯對發行人與眾不同的支持功能外，也可能是讓玩家可以向發行人主張某些權利的特殊地位（或稱賦權），例如新開業的年輕A律師可以發行100個VIP證NFT，並以6,666元販售，「擁用」這個NFT的玩家，從發行日起十年內，每年可以有6小時的法律諮詢權利，如果覺得A律師夠專業，且未來收費可能會大漲的客戶，就有動力買這個NFT，如果客戶沒用到，還可以在A律師有名氣後出售給別人，有可能還會有小眾市場形成，但這種NFT賦權的功能是否可兌現，取決於發行人的信用，如果發行人不能或不願兌現，很可能就會產生糾爭[29]。

NFT除了透過虛擬貨幣串連真實世界，具有支持、賦權的功能外，還有一個非常重要的功能就是虛擬世界中數位資產獨一無二的「數位所有權表彰」，建構元宇宙虛擬世界有一個關鍵因素是如何特定某個數位資產的所有權，讓它能清楚歸屬於特定玩家。未來元宇宙世界中，精品業者推出的全球限量數位虛擬包，可能才是貴婦們爭搶的商品，才是品味及身分的展現，而不是真的背在身上的包包[30]。

27.https://www.binance.com/zh-TW/support/law-enforcement。筆者曾以此方式向幣安請求協助查詢錢包地址申請人身分，並獲得幣安回覆資料，在請求協助時，建議在去個資化的前提下，簡要告知為何懷疑被查詢錢包涉及不法，此外，幣安為了確認申請人的官方身分，除了要用官方email信箱作為聯絡信箱外，建議製作正式函查公文，連同自己的工作證掃描上，以筆者的經驗，幣安回應速度很快，提供的資料也相當豐富，包括KYC資料、身分證翻拍、交易紀錄、登入IP位址、使用手機門號等等，非常有幫助。

綜上，NFT這種代幣之所以叫做代幣，最主要是因為把電磁紀錄代幣化、單元化，但千萬不要從「幣」字就把它理解成具有同質性和高度流通性，反而應該要清楚理解NFT的功能，是要利用區塊鏈技術的不可竄改性，彰顯並確認擁用者的特殊身分、地位或權利，它本質上是一種數位認證。

(2)NFT發行及交易模式

要發行NFT非常簡單，這種代幣一樣要運用區塊鏈技術，本質上也是一種智能合約。目前發行者最常將NFT部署在以太坊區塊鏈，以太坊最有名的協議除了前揭ERC20同質化代幣協議外，就是ERC721、ERC1155的NFT協議[31]，玩家可以輕易套用協議的指令部署NFT在以太坊，甚至很多NFT交易平台網站都有提供部署NFT的模組，以最大的NFT交易平台網站OpenSea[32]為例，玩家只要先準備電子錢包及上鏈所需的以太幣，再到網站首頁點「Create」的選項，綁定準備好的電子錢包，再上傳圖畫、歌曲等電磁紀錄，就可以將自製NFT上鏈而完成部署，之後可以決定要不要支付些許服務費，在交易平台上架販售自製的NFT。不過，要部署NFT不一定要在以太坊，也可以選擇在波場的區塊鏈[33]，或幣安智能鏈（Binance Smart Chain；BSC）[34]部署。另外，想要出售NFT也不一定要在常見的交易平台上架，出售者在自建的網站上架，或私下找買家也都可以。

3、技術偵查難點

(1)NFT擁有者的真實身分難以確認

NFT利用區塊鏈技術，當然也就可以在所屬區塊鏈上找到交易紀錄。假設某個NFT智能合約部署在以太坊，一樣可以在「Etherscan」網站首頁的搜尋欄打上NFT的合約地址，找到這個NFT過去的交易紀錄和目前在哪個電子錢包內，但和一般同質化代幣同樣的問題，從這些區塊鏈公開資訊找不到真實玩家身分。再者，NFT和同質化代幣使用的交易平台不同，同質化代幣流通性很強，有些玩家會在幣安、FTX、火幣、MAX等交易所頻繁交易，並使用交易所的託管錢包，這時有機會透過交易所查知使用託管錢包者留存的實名認證資料，但NFT發行者或擁有者會把NFT當成藝術作品放到OpenSea、Oursong、Nifty Gateway等平台讓想買的玩家慢慢挑選，但這類NFT交易平台通常都不是納管的交易平台，無需依法要求玩家履行實名認證，雖然有些平台要求玩家用email註冊會員，還是可以嘗試連絡平台查詢涉案玩家註冊資料，不過玩家可以輕易使用境外免費email信箱規避查緝。以設例觀之，不論是在「Etherscan」網站或上架NFT的交易平台，都很難查到需打點的選民或買回NFT者的真實身分。

(2)NFT的價值沒有客觀標準而難以認定對價關係

藝術品的真跡是獨一無二，許多富人爭相高價收購，至於該藝術品的價值多少，非常取決於主觀判斷，很難有客觀標準去認定價格是否合理，因此藝

28. https://tw.yahoo.com/nft/collection/ccflittleartist?utm_source=desktop&utm_medium=homepage&utm_campaign=nb&ncid=desktop_homepage_nb。
29. 近日網紅「勾惡」在媒體上指控連千毅發行NFT詐欺玩家就是一個可參考的實例，有興趣可自行以「連千毅＆勾惡&NFT」為關鍵字搜尋相關報導參考。
30. 參報導「4大精品搶攻NFT誰最狂？Dolce & Gabbana賣破3千萬元　虛擬比能穿的還貴」，https://fashion.ettoday.net/news/2190687。
31. ERC721協議和ERC1155協議最大的差別就是單一圖畫、歌曲等數位電磁紀錄要製造出1個或數個（1個以上）NFT，以前面所舉知名畫家針對某一幅畫，數位化後只發行1個NFT為例，這個就是走ERC721協議，但如果是把基金會兒童的畫作拿來發行數個限量NFT，就是走ERC1155協議。
32. https://opensea.io/。

術品有很大的操作空間，使用藝術品交付或過水不法所得的案件時有所聞，藝廊甚至常與洗錢牽涉上關係。而NFT也是另一種強調認證獨一無二的數位藝術品，所有操作藝術品洗錢的功能都可以複製在NFT上。以設例觀之，就算查到出售鐵粉帽的賣家和買家的真實身分，但買家和賣家是在交易平台上交易，相互不認識，買家如果說他是江哥的支持者，也特別喜歡這個鐵粉帽的顏色，他覺得2,500元很值得，這時要推翻2,500元和鐵粉帽間的對價關係，進而積極建立2,500元和選民投票意願的對價關係，並不容易。

4、偵查突破思考

(1)先找活動主辦人了解NFT在本案的功能

以設例觀之，候選人用一個複雜的公開活動掩飾行賄不法行為，大多會自信公開活動沒有太大的破綻，所以可以先直接向活動主辦方初步了解活動方式，例如詢問主辦人NFT是團隊自行發行還是委包廠商？發行多少NFT？如何發送？發送對向是隨機抽籤決定還是有人為指定？有無註冊鐵粉及中獎者名單可以提供？等問題，目的是要先釐清活動架構，找出行賄的可能手法，同時搜集參與者資料，再循線找參與者詢問主辦方所述是否實在？有無聽過非抽籤管道取得NFT？有無聽過主辦法回購NFT或其他出售獲利的方式？等問題，這些初步詢問或許很難直接找到關鍵的線索，但可以找到可疑之點，例如為何發送NFT要有人為指定對象的配額？決定發送對象的人是誰？進而試著找出決定發送的人，以及從這種管道取得NFT的玩家，抽絲剝繭追查取得及拍賣過程可疑之點。

(2)傳統偵查手法同步進行

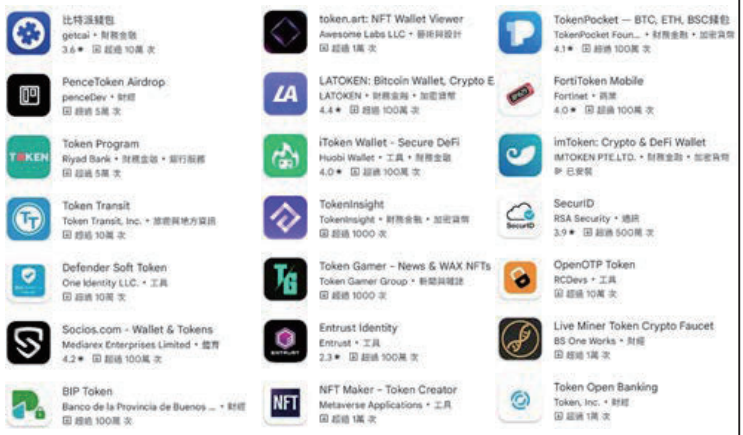
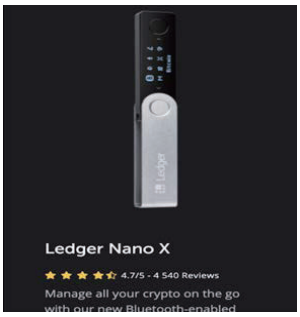
以設例觀之，了解NFT的概念，並從這個「工具」角度切入找出合法掩飾非法的可能性，固然是一種偵查思考脈絡，但一樣不應放棄傳統偵查手法，既然已經大膽假設江哥利用NFT行賄，一樣要從江哥及其團隊核心成員這個「嫌疑人」角度切入找證據，例如江哥或核心成員是否有留下指示椿腳、玩家或在拍賣平台買回者操作NFT的對話紀錄，這些嫌疑人的金流紀錄、網站瀏覽或APP下載使用紀錄、移動軌跡紀錄等等，尤其現階段還是很多人都不太了解虛擬貨幣的概念，尤其是長者，如果初步詢問嫌疑人發現他不是很懂，就要懷疑背後有人幫忙嫌疑人操作或教導，這個藏鏡人的角色就會很關鍵。

肆、虛擬貨幣管制之未來展望—代結語

鑒於虛擬貨幣金流追查對於查緝新型態犯罪模式之重要性，警、調機關已陸續引進加密貨幣金流分析工具，臺高檢署亦已於2021年底購置「Chainalysis Reactor」加密貨幣金流分析工具，藉以協助檢察官追查加密貨幣金流並特定加密貨幣金流受益人的身分。然而，利用虛擬貨幣從事犯罪之查緝仍有以下困境：1. 現行虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法未規範管制個人幣商，存有監理空窗；2. 不法利用非託管錢包尚未有適當因應措施；3. 多數境外交易所之資料調取困難；4. 比特幣自動櫃員機（BTM）管制力道不足。面對虛擬貨幣不法利用之因應，期盼能建立虛擬貨幣業全面層級化納管之法制體系，及可疑非託管錢包資料庫，並教育強化個人幣商之守法觀念，更透過公私部門資訊共享方式有效防制虛擬貨幣遭不法利用[35]。

33. 波場有發佈類似ERC20協議的TRC721協議。
34. 幣安有發佈類似ERC20協議的BEP721協議。
35. 本文礙於篇幅，僅能簡要點出問題，並粗略提出因應方向。

附件：查虛擬貨幣流檢核重點[註]

檢核重點	釋例	檢核
檢查有無使用虛擬貨幣APP(APP非常多，無法全數列舉，只要有可疑就點進去查看看)		
檢查有無錢包私鑰之記錄或照片	如「5f2f318d1dc28ff71a72218c8705893960be5540b2217e1328d5e260d36323bd」	
檢查有無助詞紀錄或翻拍畫面		
搜索時注意有無硬體錢包	 	
檢查有無電子錢包之記錄或照片	「0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8」 「TY39KopmB4q3y4WcYmPbLeDXojPcPdnqfz」	
檢查簡訊有無虛擬貨幣平台認證碼	XX平台認證碼034572	

註：此檢核表由新北地檢署洪三峯主任檢察官於111年10月提供。

檢核重點	釋例	檢核
查有錢包地址後，確認錢包真實性及交易內容	0x 開頭者（0xEA674fdDe714fd979de3EdF0F56AA9716B898ec8），至 etherscan T 開頭者（TY39KopmB4q3y4WcYmPbLeDXojPcPdnqfz），至 tronscan 並將虛擬貨幣交易紀錄下載成 excel 檔分析交易紀綠	
查錢包內尚有虛擬貨幣時，盡可能移轉至檢警調可保管之錢包	移轉虛擬貨幣需要錢包地址對應的私鑰，盡可能請當事人配合	
查有可疑錢包有利用虛擬資產業者為可疑交易，立即聯絡業者禁止該錢包使用	不論有無在台灣落地成立公司，均可嘗試，目前有在金管會聲明作洗錢法遵的有現代（MaiCoin）、王牌（Ace）、跨鏈（CHAINSS）三家公司，但就算不是這三張公司，如果能找到聯絡方式，還是可以請業者配合，目前幣安、幣托等較大家的業者應該都會自願性配合執法	
查有相關虛擬貨幣交易紀錄，可以調閱相關時間錢包所有人之銀行交易紀錄	要查虛擬貨幣交易者身分，可嘗試查錢包所有人所有開戶紀錄，再向銀行調閱相關期間之交易紀錄，再比對時間和金額，從銀行交易紀錄處找虛擬貨幣交易者之身分	
查有相關虛擬貨幣交易紀錄，可以與其共犯或本案相關人所查得電子錢包序號，互相比對有無往來	可將查得疑似同一集團之共犯或案件相關人之電子錢包序號或與以往保存於資料庫之電子錢包序號加以比對，確認彼此間有無交易往來，進而擴大偵辦。	