新興金融科技遭濫用於犯罪之研究

成果報告書

履約單位：恆業法律事務所

研究主持人：律師林繼恆博士

協同主持人：楊岳平博士

專案經理：李鎧如顧問

研究期程：中華民國 110 年 1 月至 110 年 12 月

研究經費：新臺幣 68 萬 4 千 700 元

研究計畫編號（GRB）：110-A-001

中華民國 110 年 11 月

目 錄

圖目錄

新興金融科技遭濫用於犯罪之研究

摘要

一、新興金融科技加速支付服務之發展，更促使人類的消費或投資進而利用電子支付工具進行連線或離線的資金移轉。此外虛擬通貨更因有區塊鏈或加密技術的加持，使人類可有價值儲存及交換的新選項，促使許多國家貨幣監理或發行機構，非但對於虛擬通貨進行監理，進而本身也規畫中央銀行數位貨幣（Central Bank Digital Currency, “CBDC”），可知新興科技對於現代化支付面的影響既深又廣且快。(詳如第一章)

二、電子支付工具——包括電子支付與第三方支付——作為一新型態的支付工具，存在五大特性（匿名、快速、追蹤困難、非面對面、跨境）使其易於成為犯罪者使用的犯罪工具。國內亦已屢見電子支付工具用於犯罪的案例發生，本研究團隊透過類型化分析，發現電子支付工具經常涉及的案件類型包括詐欺、賭博、竊取被害人之資訊綁定支付帳號供自己消費、盜用被害人資訊設立帳戶等案件，整體而言電子支付工具已逐漸成為犯罪常用的工具。(詳如第二章)

三、虛擬通貨本身的價格波動大，投資風險較高，再加上近年來有些以區塊鏈、虛擬資產為名目的吸金詐騙案件屢見不鮮。現行法令除了「具證券性質的虛擬通貨」為有價證券而受證券交易法及洗錢防制法規範外，對於虛擬通貨產業治理、經營管理、消費者保護等事項之主管機關為何尚有疑義，以致主管機關金融監督管理委員會（下稱「金管會」）只能以新聞稿方式提醒投資大眾風險因素。在法院實務具體個案中，本研究團隊分析出六大犯罪類型，並發現因為現行有關虛擬通貨監管法令不足，導致有關虛擬通貨之刑事偵查犯罪資料相對不足，法務部調查局辦理之洗錢防制申報資料甫上路，尚難形成有意義之統計數

據，上述問題都有待司法與執法部門能夠對虛擬通貨有更全面性的認識，方能適用有限的法條規範於多樣化的新興交易。(詳如第三章)

四、本研究觀察到現行我國就虛擬通貨之監理態度偏向保守，首先針對應用型代幣我國尚無特定之監理規範；支付型代幣（虛擬通貨）之監理則付之闕如；證券型代幣上，金管會已訂定規範納管，然而因虛擬通貨之應用及發展歷程不夠久遠，現行法下何種虛擬通貨之功能及態樣可能構成我國法下之證券型虛擬通貨，則容有疑義，令行為人無法合理預期該虛擬通貨發行是否受刑法或相關證券法令之規範，同時也提高執法機構執法、查緝的難度。(詳如第四章)

五、本研究進行比較法分析，就美國、英國、新加坡及歐盟等國家或地區之新興金融科技遭濫用於犯罪之現狀與法規，觀察到比較法分析結果之四大面向趨勢：(一)金融機構及金融科技業者協助執法之重要性；(二)跨越國境統一執法標準之重要性；(三)應提升執法機關職權或組織編整；(四)應有效健全犯罪相關之查緝制度。此外，於完成日本、美國、英國、新加坡及瑞士等國之自律組織比較法研究，結果發現已出現由金融科技業者之自律組織協力進行法令遵循、風險控管等國際趨勢。(詳如第四章)

六、本研究經分析外國統計資料以及我國司法判決實證研究，發現犯罪人例如詐騙集團多以人頭或盜用他人身分創建支付帳戶的方式遂行犯罪或洗錢，進而造成相關金流追查之不易。此外，不論國際間或國內有關虛擬通貨濫用於犯罪等案例仍層出不窮，且因為相關經濟活動逐步成長，虛擬通貨遭濫用於犯罪也有逐年嚴峻之情。若各國政府及主要電子支付業者、第三方支付業者及虛擬通貨業者能夠確實落實洗錢與資恐防制等措施，或可

減少犯罪偵查面臨的挑戰，或於犯罪發生後將影響範圍降至最低。(詳如第五章)

七、近期相關法令之修正，已確認第三方支付業者與虛擬通貨業者的洗錢防制義務，但相關主管機關欲監督業者確實落實其義務，仍有一定挑戰。本研究建議犯罪偵查機關與主管機關建立聯繫，將偵查時發現的洗錢防制義務落實不力的業者通報主管機關，作為主管機關加強檢查與執法的優先對象，以落實風險基礎方法之監理；此外我國犯罪偵查機關可進一步建立金融科技犯罪資料庫，彙整相關偵查資料並針對金融科技用於犯罪的情形進行分析，透過科技方法協助自身在有限的監理資源下，盡可能全面且即時地對龐大的複雜系統施以監管，並鎖定應重點加強執法的金融科技業者。最後，為期得降低利用金融科技工具犯罪之可能，本研究建議新增偽造變造數位支付工具之刑法規定以補足新興金融科技工具因欠缺實體而不適用刑法第 201 條之 1 偽造變造卡式支付工具而遺留的立法不足，以強化數位支付工具的真實性。(詳如第五章)

關鍵詞：電子支付、第三方支付、虛擬通貨、虛擬資產、洗錢防制、金融科技、法令遵循、刑事偵查

Executive Summary

FinTech (Financial Technology) has speeded up the development of payment servicesand promoted the consumption and investment using electronic payment instruments to transfer funds online/offline. In addition, backed by the blockchain and cyptography technologies, cryptocurrency provides the public a new option to store and exchange value, prompting many countries' government to rethink not only their currency policies and supervision but also the plan to issue digital currency (Central Bank Digital Currency, "CBDC") instead. These developments have deeply impact modern ways of payment, and the impact is wider and faster. (See chapter 1)

Electronic payment instruments, including electronic payments and third-party payments, have five general characteristics, namely, anonymity, speed, difficult tracking, non-face-to-face, and cross-border, which provide a new criminal instrument for crimes. Many criminal cases in Taiwan have employed electronic payment instruments. Through a comprehensive empirical analysis and typology, we found that criminals often use electronic payment instruments to commit fraud, gambling, theft of electronic payment account for consumption, theft of personal information to create fraudulent payment account, and others. The case number and monetary amount of the above criminal cases are also considerable, showing that the current electronic payment instrument businesses contain a considerable degree of loopholes in terms of regulations and anti-money laundering supervision. As a result, electronic payment instruments have gradually become an instrument for crimes. (See chapter 2)

Cryptocurrency itself with high price fluctuates, and investment risk is relatively high. In addition, in recent years, it is common for some cases of fraud collect public money under the name of blockchain and/or cryptocurrency. Except for Security Token as a security regulated by Securities and Exchange Act, and Money Laundering Control Act the

current laws and regulations do not directly regulate cryptocurrency; as a result, Financial Supervision Commission release a press release to remind the public of risk factors of cryptocurrency investment. In the specific cases of court practice, we analyzed all the relative court judgement and classify six major types of crimes related to cryptocurrency. We found that due to the lack of cryptocurrency supervision and regulations, and also lack of criminal investigation information or data related to cryptocurrency crime, which cause difficulty to police, enforcement agencies to investigate into specific crime. The above-mentioned problems require the judicial and law enforcement agencies to have a more comprehensive understanding of cryptocurrencies before promoting amendment bill and regulations to diversified emerging transactions. (See chapter 3)

The study observes that our current supervisory policy towards virtual currencies tends to be conservative. First of all, except AML/CFT （Anti-Money laundering/countering the financing of terrorism）field and security token, there is no specific competent authority for Cryptocurrencies. However, since the application and development of Cryptocurrencies are not long enough, it is doubtful that under the current laws, whether may violate Securities and Exchange Act or not. and it also increases the difficulty for criminal investigations and enforcement.(See Chapter 4)

This study conducts comparative method observing different countries'/ regions' regulations including United States, United Kingdom, Singapore, and the European Union where emerging four major characteristic and trend: (1) The importance of private agencies assisting in law enforcement; (2) The importance of uniform law enforcement standards; (3) Promote authority or organize reorganization; (4)

Improve the criminal investigation system. In addition, It turns out that self-regulatory organizations are working together with governments with legal compliance and risk control.(See chapter 4)

After analyzing the global statistical data and Taiwan's court judgments, we found that criminals often use the inadequate know-your-customer procedure of electronic payment instruments to create payment accounts under the name of aiders or theft accounts so as to commit crimes or money laundering, which causes challenges to the investigation of the money-flow. Besides, there are endless cases of abuse of cryptocurrency in crime both internationally and domestically. Moreover because of the gradual growth of related cryptocurrency activities, the abuse of cryptocurrency in crime are still growing year by year. Only if the electronic payment businesses, third-party payment businesses and cryptocurrency buisnesses implement the measures of money laundering could the the government reduce the challenges to criminal investigation and prevent crime or minimize the impact of crime. (See chapter 5.)

Recent regulatory amendments have affirmed the AML obligations of third-party payment business and cryptocurrency businesses. That said, related competent authorities remain facing the challenges when supervising the businesses to implement their said obligations. Finally, to reduce the crimes using FinTech as a criminal instrument, this research proposes to introduce a provision under the Criminal Law penalizing the counterfeits of digital payment instruments to fill the loophole under the current Article 201-1 of the Criminal Law that applies only to card payment instruments. In this way, the authenticity and trustworthiness of digital payment instruments may be enhanced. (See chapter 5.)

Keywords:Electronic Payment, Third-party Payment, Cryptocurrency, Virtual Asset, Money Laundering, Fintech, Legal Compliance, Criminal Investigation

第一章　緒論及背景

第一節　研究背景及主旨

新興金融科技加速支付服務之發展，更促使人類的消費或投資進而利用電子支付工具進行連線或離線的資金移轉。此外虛擬通貨更因有區塊鏈或加密技術的加持，使人類可有價值儲存及交換的新選項，促使許多國家貨幣監理或發行機構，非但對於虛擬通貨進行監理，進而本身也規畫中央銀行數位貨幣（Central Bank Digital Currency, “CBDC”），可知新興科技對於現代化支付面的影響既深又廣且快。但另一方面，此類新興金融科技衍生的支付工具，亦逐漸成為犯罪者使用的犯罪工具或洗錢工具，而對犯罪偵查產生不小的挑戰。

本研究之主旨即在整理新興金融科技於我國遭濫用於犯罪之類型與實務——包括電子支付工具與虛擬通貨，進而提議可行的政策因應方向。本研究第二章主要針對電子支付工具涉及的新興犯罪背景成因及類型進行分析，電子支付工具——包括電子支付與第三方支付——作為一新型態的支付工具，存在五大特性——包括匿名、快速、追蹤困難、非面對面、跨境，使其易於成為犯罪者使用的犯罪工具。國內亦已屢見電子支付工具用於犯罪的案例發生。本研究團隊透過類型化分析，發現電子支付工具經常涉及的案件類型包括詐欺、賭博、竊取被害人之資訊綁定支付帳號供自己消費、盜用被害人資訊設立帳戶等案件，整體而言電子支付工具已逐漸成為犯罪常用的工具。

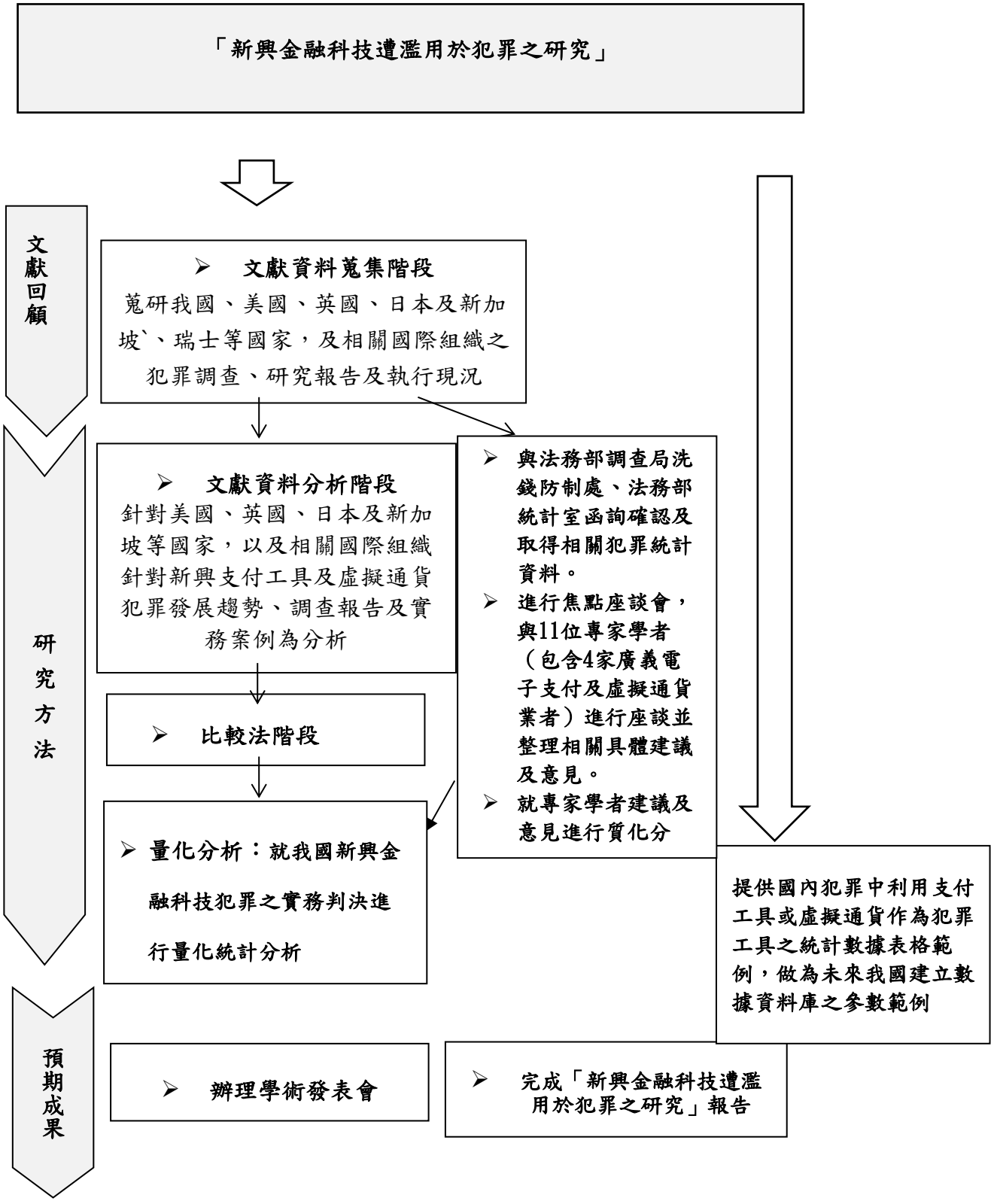
本研究第三章則係針對虛擬通貨涉及的新興犯罪背景成因及類型進行分析，首先評估虛擬通貨經濟活動之重要性和市場發展趨勢是確定虛擬通貨濫用於犯罪趨勢之重要前提，故本研究總結現行虛擬通貨之主要四大經濟活動現況（發行虛擬通貨、涉及虛擬通貨商業之業務、挖礦、去中心化金融服務），以及研析近年國際統計數據及綜合案例，將虛擬通貨犯罪分為四大類型，包括詐欺行為、網路駭客竊取行為、網路勒索以及以虛擬通貨作為犯罪交易對價；本章第四節則就我國虛擬通貨之法律定性、監管法制及虛擬通貨濫用於

犯罪之實務判決進行盤點及研析。

本研究第四章進一步探討電子支付工具及虛擬通貨相關犯罪之偵查及私部門協力議題。首先第一節研究我國網路犯罪偵查之現行法及法律解釋問題，尤其是電磁紀錄與整體搜索、扣押制度之問題。接著研究實務上偵查電子支付工具及虛擬通貨犯罪面臨之困境，例如主管機關監理態度不明確、金融科技犯罪匿名性、快速性等形成之偵查困境。第二節探討美國、英國、新加坡、歐盟等比較法，研究各國家或地區之金融監理制度、犯罪執法機關、金融科技犯罪調查工具及方法、私部門協力程度及方式、未來犯罪立法與執法方向等不同面向。第三節研究新興金融科技犯罪相關之自律組織協力之國際發展，並以日本、美國、英國、新加坡及瑞士作為比較制度整理。

本研究第五章為研究結論及政策建議。近期相關法令之修正，已確認第三方支付業者與虛擬通貨業者的洗錢防制義務，但相關主管機關欲監督業者確實落實其義務，仍有一定挑戰。故本研究結論部分建議犯罪偵查機關與主管機關建立聯繫，將偵查時發現的洗錢防制義務落實不力的業者通報主管機關，作為主管機關加強檢查與執法的優先對象，以落實風險基礎方法之監理；此外建議我國犯罪偵查機關可進一步建立金融科技犯罪資料庫，彙整相關偵查資料並針對金融科技用於犯罪的情形進行分析，透過科技方法協助自身在有限的監理資源下，盡可能全面且即時地對龐大的複雜系統施以監管，並鎖定應重點加強執法的金融科技業者。政策建議部分，為期降低利用金融科技工具犯罪之可能，本研究建議新增偽造變造數位支付工具之刑法規定，以補足新興金融科技工具因欠缺實體而不適用刑法第201條之1偽造變造卡式支付工具而遺留的立法不足，強化數位支付工具的真實性，並開放金融監理沙盒實驗洗錢防制的監理科技。

第二節　研究架構


「新興金融科技遭濫用於犯罪之研究」
文獻回顧
➢ 文獻資料蒐集階段
蒐研我國、美國、英國、日本及新加坡`、瑞士等國家，及相關國際組織之犯罪調查、研究報告及執行現況
研究方法
➢ 文獻資料分析階段
針對美國、英國、日本及新加坡等國家，以及相關國際組織針對新興支付工具及虛擬通貨犯罪發展趨勢、調查報告及實務案例為分析
➢ 比較法階段
➢ 量化分析：就我國新興金融科技犯罪之實務判決進行量化統計分析
➢ 與法務部調查局洗錢防制處、法務部統計室函詢確認及取得相關犯罪統計資料。
➢ 進行焦點座談會，與11位專家學者（包含4家廣義電子支付及虛擬通貨業者）進行座談並整理相關具體建議及意見。
➢ 就專家學者建議及意見進行質化分
提供國內犯罪中利用支付工具或虛擬通貨作為犯罪工具之統計數據表格範例，做為未來我國建立數據資料庫之參數範例
預期成果
➢ 辦理學術發表會
➢ 完成「新興金融科技遭濫用於犯罪之研究」報告

第三節　研究方法

本研究首先採取「文獻回顧研究法」進行研究資料蒐集，文獻回顧範圍將包括初級資料（如與新興金融科技有關之國際規範或官方文件）與次級資料（如書籍與期刊論文），並將文獻資料進行分析歸納；其次採取「判決實證研究法」，針對我國刑事判決中涉及新興金融科技使用於犯罪之案例，進行回顧、彙整與統計，以分析新興金融科技於我國目前使用於犯罪之犯罪種類、規模、手法、特性等資訊；最後採取「比較法研究法」，將相關國際規範、外國法制規範與我國現行法制為落差分析與參採性分析。

而因本研究之研究目的係為提出具體新興金融科技遭濫用於犯罪之類型，並研擬可行之監理方式，故須利用質性研究法中之「深度訪談法」，故本研究亦與國內之行政機關、相關專家學者進行做座談及/或深度訪談，並蒐集國內外具代表性之新興支付暨虛擬通貨業者，進行訪談，以實際瞭解新興科技濫用於犯罪之現況。

第一項 文獻回顧研究法

一、文獻資料蒐集

(一)國際金融組織（如 FATF 防制洗錢金融行動工作組織）網站資料蒐集。

(二)美國、英國、新加坡官方金融科技及犯罪偵查官方網站蒐集。

(三)法規資料庫實例蒐集：例如 Lexis、Westlaw 等。

資料庫名稱	簡介	圖示
Lexis	可蒐集英美法相關法規。	LexisNexis™
Westlaw	可蒐集英美法相關法規。	Westlaw

(四)英文期刊文獻或民間企業(如 J.P. Morgan, PwC)之研究報告。

(五)英文媒體報導或文章。

二、文獻資料分析

(一) 以時間區段歸納新興金融科技之犯罪類型及發展規模趨勢。

(二) 美國、英國、新加坡法規範之背景與犯罪偵查實務。

(三) 我國新興金融科技犯罪之犯罪成因、類型、發展規模趨勢，並

綜合我國金融科技犯罪之偵查實務。

第二項 判決實證研究法

一、利用我國刑事判決資料庫，搜尋涉及電子支付工具與虛擬通貨的刑事判決。

二、分析刑事判決搜尋結果，針對不同犯罪類型進行分類，並且歸納相關犯罪手法。

三、統計不同犯罪類型的相關資訊，包括案件數、犯罪金額規模、犯罪特性等，以歸納新興金融科技犯罪於我國的趨勢。

第三項 比較法研究法

一、針對美國、英國、新加坡之新興金融科技犯罪發展趨勢、法制現況及犯罪偵查組織架構及運作實務為分析。

二、將外國法制及實務現況與我國現行法制及實務現況為落差分析。

三、將外國法制規範及實務作法納入我國之可行性分析（包含政策、立法、機構權責不同、經濟層面、國情不同等）。

第四項 專家/業者焦點座談會(含學術倫理審查)

一、焦點座談會－邀集相關領域專家及業者

本研究團隊與本計畫相關之國內偵查機構、專家學者及加密貨幣業者於2021年3月31日進行焦點座談，透過犯罪偵查機關實務之分享，對於現行實務案件以及案件監管及執法方式有更深入之理解，並且透過學者分享其分析研究結果，理解實務和法制面臨的問題，最後本研究團隊統整本次焦點座談會之專家學者針對電子支付工具犯罪及虛擬通貨遭濫用於犯罪之座談重點，進進行質化分析，並藉由新興金融科技業者分享新興犯罪型態，以及犯罪實務上所發生的問題及現象。

本研究團隊已邀請相關政府機關代表及學者專家 6 名參與學術發表會。政府機關代表包含法務部調查局、法務部司法官學院，學者專家則包含金融科技、刑事犯罪學、區塊鏈及虛擬通貨法規領域專家，並邀請新興金融科技之 5 間業者，包含第三方支付業者及虛擬通貨交易所等產業界代表，出席之學者專家及產業代表名單如下：

(一)　法務部司法官學院：鄭元皓助理研究員

(二) 恆業法律事務所：計畫主持人律師林繼恆博士、專案經理李鎧如律師、研究員林紘宇律師

(三) 國立台灣大學法學院：楊岳平協同主持人、蘇凱平教授

(四) 法務部調查局臺北市調查處：蘇文杰調查官

(五) 東吳大學法學院：林育廷教授、蕭宏宜教授、李相臣教授

(六) 街口電子支付股份有限公司：林芝羽法務經理

(七) 現代財富科技有限公司：陳明惠營運長

(八) 幣託科技有限公司：鄭學豐法務暨法遵經理

(九) 博歐科技有限公司：范紀鍠執行長

(十) 艾米佳科技有限公司：林淦鈞執行長

透過前述學術發表會，讓不同意見之各方代表於會上形成意見交流模式，進而達成意見溝通之效果，俾利後續監理政策研擬。

二、發函詢問法務部目前相關執法模式

金融科技相關監理議題之推動是重要實務議題，故須瞭解目前我國之監理模式為何，並且了解有無相關法制逐步配合制定，為了解我國犯罪偵查及監理實務之最新進展，本研究團隊已以發函的方式，諮詢我國執法機關法務部，函詢之表格可參見本研究報告附錄三。

本研究計畫函詢/詢問單位			
名稱	**函請法務部提供電信詐欺及網路犯罪數據及資料**	**函請法務部調查局洗錢防制處提供可疑交易申報資料**	**詢問法務部調查局臺北市調查處/各大金融科技業者**

具體成果	■ 經法務部 2021 年 7 月 19 日回函表示現行防治電信詐欺與網路犯罪統計資料中，並無相關數據。 ■ 經研究團隊多次電詢法務部其他有關部門亦無偵查階段相關統計資料。 ■ 本研究團隊製作國內犯罪利用支付工具或虛擬通或作為犯罪工具之統計數據表格範例（如附錄三）。	■ 經法務部調查局臺北市調查處協助，函請法務部調查局洗錢防制處提供可疑交易申報資料。 ■ 經本研究團隊爭取及說明，法務部調查局洗錢防制處內部協調及研析後例外協助提供行動支付暨虛擬通貨之可疑交易申報資料(去識別化資料，如附錄四)。	■ 經法務部調查局臺北市調查處協助，函請法務部調查局洗錢防制處提供可疑交易申報資料。 ■ 取得業界內最新金融科技監理工具之資訊及簡介。

三、學術倫理審查

本計畫依照我國人體研究法第 5 條規定，經國立臺灣大學行為與社會科學研究倫理委員院會於 2020 年 12 月 29 日審查核可，同意免予審查。

第四節　文獻探討與比較

第一項 電子支付工具犯罪

一、國內文獻回顧

(一)國內電子支付工具的概念討論與發展因素

新興支付工具的定義與分類，沈中華教授等人[1]指出現行的官方統計與分類過於混亂，政府機關因為各自權責不同而各自對我國行動支付市場有相異的統計，再加上電子化支付的概念混亂，導致無法對我國行動支付的現況作全盤的檢視。其因此建議所謂行動支付

[1] 沈中華、王儷容、蘇哲緯(2020)，〈臺灣行動支付發展與歸類檢討〉，《存款保險資訊季刊》，第 33 卷第 1 期，頁 60 以下。

3+3的分類方式，將新興支付工具區分為電子支付、電子票證、第三方支付，以及電子錢包、裝置載體支付、紅利點數貨幣數位化，並以之分別依其交易總額除以民間消費支出後計算其各自於我國之滲透率。

針對行動支付的未來發展，財金公司的翁世吉組長與田育任工程師[2]認為包括其交易安全與服務的分工模式，均為行動支付是否得以穩定蓬勃發展的關鍵，此外其亦指出有鑑於客戶群體的異質性與客戶需求的複雜，金融機構持續提供多樣、高效、安全的支付服務選擇是必然且必須的，故於發展行動支付服務的同時，宜以與傳統的卡片支付工具共存、互補為原則。

(二)電子支付工具的監管

針對我國目前電子支付工具監管區分第三方支付與電子支付差別監管，朱瑞翔研究生[3]指出我國以日經手10億元新台幣為標準，區別第三方支付業者與電子支付業者，該10億元標準可能過於寬鬆，導致大量電子商務平台保管金額雖然相當可觀、卻因日經手金額未超過該門檻而無須受監理，因此可能引發資金規模以及市場影響力過大之風險，故其比較美國法（UMSA 與各州訂定之資金傳遞法）與歐盟法（PSD2）後，建議參考歐盟法監理模式，使僅代表一方之代收代付業者可不受監理，且設定門檻應評估金融市場承受風險之能力再設定適當之數額。

蔣念祖博士與戴凡芹研究生[4]則回顧近期電支條例的修正，指出其雖嘗試以支付機構之資本額作為差額化管理及業務開放項目之規範，但對於何謂小額匯兌及金額大小分別管理仍缺乏明確定義與規範，因此存在法規不明確地帶，例如小額度的犯罪仍可能累計而成總數甚鉅的鉅額案件，因此應審慎考慮倘若使非金融機構得辦理匯兌業務，是否應以相同甚至高於銀行監理的角度視之，同時考量業

[2] 翁世吉、田育任(2014)，〈「行動商務」支付應用發展趨勢〉，《財金資訊季刊》，第78期，頁19以下。

[3] 朱瑞翔(2019)，〈由系統性風險控管論電子支付業之定義－以代收代付業為中心〉，《中華國際法與超國界法評論》，第15卷，頁217以下。

[4] 蔣念祖、戴凡芹(2019)，電子支付管理條例修正草案評析，萬國法律，第228期，頁83以下。

者的監理遵循成本。

謝孟珊博士[5]則認為現行法僅設定日平均額新台幣10億元以下的網路代理收付實質交易款項為監管的例外，尚有不足。其參照英美法制後，建議應將一、純粹的技術服務提供者，而未涉及資金之經手亦未曾持有移轉之資金；二、基於慈善或公益目的之款項移轉服務、以及；三、已受特別法規範的證券、期貨等交割系統，納入電子支付機構的例外。其並建議金管會應保持彈性，多以函釋對新型支付方式是否屬於電支條例規範範疇進行解釋。

(三)電子支付工具與洗錢防制

謝孟珊博士二度為文[67]指出，第三方支付具有大量吸收資金之特性及資金結算之功能，基於消費者保護與洗錢防制之考量，應予納管。但如參照 FATF 及美國的銀行保密法(Bank Secrecy Act, BSA)，將相關業者一律定義為洗錢防制之主體並課與大額及可疑交易申報義務，恐有過苛，故建議應區分系爭資金移轉與商品或服務交易是否可分，倘係一不可分之實質交易、並且得以有效追查收受款人，規範密度上即可低於不具實質交易基礎的匯兌業務。具體落實上，其建議可將第三方支付納入我國洗錢犯罪防制網中，除參考現有銀行之 KYC 機制要求客戶以真實身分註冊外，尚應課予第三方支付業者留存交易紀錄之義務。

此外，對於電子支付機構辦理身分驗證一事，官瑀婕研究員[8]指出國內電子支付機構多已自發性採取雙重或多重驗證機制，相關規範重點應包含持續性身分驗證流程、雙重多重驗證方式交互運用、必要時視情形提高使用者身分認證強度（如異常大量交易時）、驗證手段應合理有效且符合比例原則、技術中立原則等，此外平台業者因身分驗證所得到之個人資料應受到個人資料保護法之保障。

---

[5] 謝孟珊(2017)，〈電子支付業務管制範疇之比較法研究〉，《月旦法學雜誌》，第 263 期，頁 153 以下。

[6] 謝孟珊(2016)，〈網路代理收付服務於 FATF 及美國之洗錢防制監管規範分析〉，《科技法律透析》，第 28 卷第 2 期，頁 28 以下。

[7] 謝孟珊(2013)，〈第三方支付法制問題研析〉，《科技法律透析》，第 25 卷第 2 期，頁 14 以下。

[8] 官禹婕(2014)，〈網路使用者身份驗證機制研析──以電子支付機構國際立法及推動經驗為中心〉，《科技法律透析》，第 26 卷 11 期，頁 12-18。

(四)電子支付工具的犯罪防制

詹德恩教授[9]分析傳統金融犯罪的特性後，認為傳統金融犯罪特徵有缺乏犯罪現場且蒐證困難、被害人不明顯但損害性高、被告社經地位高且屬於共犯結構、犯罪手法具高技術性且複雜、被告容易串供並湮滅證據、容易影響資本市場造成投資人權益受損、產生鉅額犯罪所得進行洗錢被告有潛逃國外之虞。傳統金融犯罪偵查的難題，則包括偵審時間長、行政司法未能互相協力、洗錢防制申報有疏漏等。

針對金融科技的犯罪防制，陳俊成研究生[10]建議應先以「資訊安全防禦技術」著手，再以「三級預防理論階層」研擬防制預防犯罪對策後，進一步探究犯罪偵查機關與金融主管機關之組織架構與防制作為。

二、國外文獻回顧

外國文獻對於新興支付工具犯罪的研究有相當數量聚焦於洗錢防制議題，例如 Angel L. Rodriguez Santiago[11]即指出新興科技將影響傳統洗錢的手段與管道，例如近期逐漸嚴重的網路洗錢(cyber laundering)，其並分析網路時代下新型態支付工具用於洗錢犯罪時之特性，並針對美國的網路洗錢法制探討其實效性、缺點以及可能的替代管制手段。

EverComplaint 的白皮書則[12]觀察到，近期因新興支付工具的興起，以之作為洗錢工具的比例正在逐年攀升；Tookitaki 的研究報告亦[13]觀察到高比例之毒品、賭博與成人內容相關之犯罪，已開始利用新興支付工具洗錢。

---

[9] 詹德恩(2013)，〈我國金融犯罪特性與抗制難題〉，《中正財經法學》，第七期，頁 159 以下。

[10] 陳俊成(2018)，〈金融科技犯罪與防制-結合資訊安全觀點〉，《南臺財經法學》，第 4 期，頁 161 以下。

[11] *See generally* Angel L. Rodriguez Santiago, *New Payment Methods and Insufficiencies in Their Regulatory Scheme*, 7 J. L. & CYBER WARFARE 101 (2019).

[12] EverComplaint, *White Paper: How to Prevent Transaction Laundering*, EverComplant (Oct., 2018), https://f.hubspotusercontent30.net/hubfs/20130485/Everc_June_2021/PDF/ECWhitepaper_HowtoPreventTransactionLaundering_20182.pdf.

[13] Tookitaki, https://www.tookitaki.ai/compliance_hub/what-is-credit-card-money-laundering-and-its-schemes/ (last visited June 15, 2021).

對於新興支付工具的洗錢防制策略，FATF 於其報告[14]中指出重點應該擺在成本效益分析，換言之，縱然新興支付工具帶來許多洗錢防制上的問題與漏洞，然而監管機關仍須考量例如 AML/CTF 的措施所帶來的效益是否足以正當化其所造成的額外花費？系爭政策措施是否會為現有的使用者帶來不利，例如犧牲便利性或提高使用服務之成本等)？該不利是否會造成現有服務使用者轉而使用其他未受監管之服務？

Association For Financial Professionals[15]則針對支付詐欺進行研究。其統計 548 家不同大小、分屬不同產業之國際公司受到支付詐欺之情形，作成相關統計數據。調查發現電子商務郵件詐騙 (BEC) 為詐欺既遂與詐欺未遂之主要來源，且超過八成以上受調查之公司曾經受到支付詐欺攻擊。該調查亦統計被用以詐騙之支付工具比例，其中約有超過三成以上之企業藉由新興支付工具支付被詐騙之價款。另外 2015 年至 2019 年曾經受到 BEC 詐騙攻擊之機構比例，自 2016 年至 2019 年受支付成長約 20%。

第二項 虛擬通貨之法律定性

中本聰於 2008 年發表《比特幣：一種對等式的電子電金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）一文宣示區塊鏈革命，區塊鏈技術利用分散式帳本技術以及密碼學技術創造出之「虛擬通貨」，對於金融市場造成之震撼持續至今，截至 2021 年初統計全球共有 8800 種虛擬通貨，總市值有 1.6 兆美元，其中比特幣佔約六成居首[16]。但是欲定性虛擬貨幣有其困難性，鑑於虛擬通貨種類繁多且性質各殊，瑞士金融監理局（Swiss Financial Market Supervisory Authority，簡稱 FINMA）認為應將虛擬通貨分為三類：一，支付型代幣：僅單純做為支付用，而並未有進一步功能或連接到其他開發

[14] FATF- GAFI, *Money Laundering Using New Payment Methods*, FATF (Oct.,2010), https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf .

[15] Association For Financial Professionals , *2020 AFP Payments Fraud and Control Survey Report: Key Highlights*, AFP (Apr., 2020), https://lead.bank/docs/default-source/default-document-library/2020paymentsfraudandcontrolreport-highlights-final.pdf?Status=Temp&sfvrsn=4f145bfd_2.

[16] 中央銀行(2021)，〈虛擬通貨近期發展及國際監管概況〉，頁 72。

項目；二，效用型代幣：提供應用或服務之數位近用權之代幣；三，資產型代幣：用以表彰對於實體標的、公司之盈餘或股利之代幣，性質和股票、債券及衍生性金融商品類似[17]。鄭婷嫻認為此種分類方式揭示了虛擬通貨性質變異快速而有定性不易的問題，造成主管機關權責難以事先劃定的問題[18]。

有關貨幣之定義，學界普遍認為貨幣應具有三種性質：價值儲存、交易媒介、記帳單位[19]。若貨幣可以在各手之間不必經由背書便可以流通，該貨幣便是通貨（circulating medium）[20]。我國中央銀行認為，人們以貨幣交易意味著貨幣使用者對於商品內含價值以及貨幣發行者之信賴，故貨幣背後有重要的「信任機制」為底，而法定貨幣（legal tender，亦有稱法償貨幣）則是透過嚴密之法規與監管機制賦予貨幣支付能力[21]。至於虛擬通貨是否為貨幣，我國金融監督管理委員會認為，虛擬通貨儘管可作為交易媒介，但是市場流通性小；又因為比特幣等虛擬通貨價格波動幅度過大，不適合作為記帳單位，也不具價值儲存功能，故綜合評量之下並非貨幣[22]。我國中央銀行並認為，虛擬通貨除了不符合上述貨幣功能外，又因為虛擬通貨供給量無法調整，且有易遭不法使用、耗能等問題，故無法取代現有貨幣體系[23]。

雖我國金融主管機關對於虛擬通貨之貨幣定性持否定看法，惟文獻上仍有在分類上將虛擬貨幣視為電子貨幣的一種。電子貨幣係將相對於鑄幣、紙幣等實體貨幣，以電子方式存在和交易使用。楊岳平教授將電子貨幣再以是否以法償方式計價，分為「虛擬通貨」

---

[17] *See* FINMA, *FINMA publishes ICO guidelines*, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/ (last visited June 15, 2021).

[18] 鄭婷嫻(2021)，〈論證券型虛擬通貨引進後證券法規應用與監理機制調適〉，《臺灣財經法學論叢》第 3 卷 第 1 期，頁 154。

[19] *See* Ali, Robleh, Barrdear, John, Clews, Roger and Southgate, James, *The economics of digital currencies* ,Bank of England Quarterly Bulletin, 54, issue 3 (2014), at 276-286.

[20] 參閱韋柏字典條目，https://www.merriam-webster.com/dictionary/circulating%20medium （最後瀏覽日：2021 年 6 月 20 日）

[21] 中央銀行(2018)，〈數位金流與虛擬通貨－－央行在數位時代的角色〉，《存款保險資訊季刊》，第 31 卷第 4 期，頁 34-35。

[22] 金管會，虛擬通貨（或稱虛擬資產），https://moneywise.fsc.gov.tw/tabf/FW/FW14_index.html （最後瀏覽日：2021 年 6 月 20 日）

[23] 中央銀行，同註 16，頁 40。

及「非虛擬通貨」，而非以法償計價之虛擬通貨可再以否涉及密碼學，再分為「密碼貨幣」或「非密碼貨幣」[24]，並認為若非以維持金融穩定之目的出發，並不排除將特定虛擬通貨解釋為貨幣[25]。林盟翔教授則根據國際貨幣基金與歐洲中央銀行對於虛擬通貨之定義，認為虛擬通貨之定義應觀察其與真實金錢和真實經濟之互動，而虛擬通貨係多為私人發行、以數位形式存在並非以法償計價之數位通貨[26]。陳榮傳教授認為，虛擬通貨可能得表彰一種或數種貨幣功能，但不具法償效力，虛擬通貨之流通能力非來自任何管轄區域之發行或擔保，而係以虛擬供通貨使用者之合意為依據[27]。

貨幣在法律上之定性為何，因虛擬通貨可表彰財產上利益，故其是否為民法上之物權、債權，抑或無體財產權，學說上有不同見解。以比特幣為例，陳榮傳教授認為因比特幣僅係網路上之紀錄區塊，依據物權法定原則（民法第 757 條），不宜將比特幣視為物權法上之「物」，也不一類推適用物權法相關規定，惟比特幣之經濟價值與交易功能在現實上已無疑義，故應將比特幣視為無體財產[28]。有相反見解肯定比特幣為民法上之「物」，並認為民法上物的概念應至少可包含可支配之自然力，又電磁紀錄僅係電力之變形，將比特幣是為物較符合現實交易型態，而因為比特幣並無所謂發行商，且可經由挖礦原始取得，故不具備「持有人得向特定人主張為一定行為之權利」之債權特性，又因比特幣可以跨越國境且無主張權利時效之問題，故比特幣並非債權或智慧財產權[29]。

楊岳平教授認為，定性虛擬通貨時應係細究所定性者為何種虛擬通貨，蓋不同種類虛擬通貨本就表彰不同權利，不可一概而論，且定性虛擬通貨時宜避免跨法律體系，蓋主管機關定性時有其主管

[24] 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〉，《臺大法論叢》，第 48 卷特刊，頁 1290-91。

[25] 楊岳平(2020)，〈論虛擬通貨之法律定性——以民事法與金融法為中心〉，《月旦法學雜誌》，第 301 期，頁 56-58。

[26] 林盟祥(2017)，〈數位通貨與普惠金融之監理變革──兼論洗錢防制之因應策略〉，《月旦法學雜誌第 267 期》，頁 33-34。

[27] 陳榮傳(2019)，〈論比特幣與比特幣之債〉，《軍法專刊》，第 65 卷第 6 期，頁 14。

[28] 同前註，頁 16。

[29] 沈易(2019)，〈淺論比特幣在民事法律上之定性〉，《司法新聲》，第 129 期，頁 22-25。

法規之法律體系和不同目的解釋考量[30]。楊岳平教授認為在民事法上，虛擬通貨本身應係無體財產權，惟可暫將其定性為物以避免法律空窗期；至於虛擬通貨表彰之權利定性須依個案探討而定，若係功能型虛擬通貨，其係表彰持有人對於發行人之債權，若係資產型虛擬通貨，則須個案探討所表彰資產之權利定性，若係支付型虛擬通貨，其係表彰持有人就虛擬通貨網路所形成之合同行為關係，基本上屬於對於該網路關係人之債權[31]。

最後，我國金管會參考美國 Howey Test，核定具證券性質之虛擬通貨，為證券交易法第六條之有價證券。所稱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[32]。可知個案認定下虛擬通貨可能被定性為有價證券。

第三項 虛擬通貨之外國監管情形

對於虛擬通貨之監管上，勢必因為主管機關所持不同主管法規，且各有不同監理目的，故對於虛擬通貨會有不同之定性及監理態度。

首先在虛擬通貨交易之監管方面，宋皇志教授與吳婕華律師整理認為，國際上可分為三種監管模式：（一）註冊許可型：承認虛擬通貨作為支付工具合法流通，惟負責進行交易之虛擬通貨交易所須經註冊方可進行虛擬通貨和法幣之交易，如日本模式。（二）發布風險警示：未明文得合法流通亦為未明無禁止者，例如我國以及新加坡。（三）明令禁止：明文禁止虛擬通貨之流通以及虛擬通貨與法幣之間的兌換[33]。

楊岳平教授以國際證券管理機構組織（International Organization of Securities Commissions, 簡稱 IOSCO）針對各國虛擬通貨交易平台

[30] 楊岳平，同前註 25，頁 47-48。
[31] 楊岳平，同上註，頁 50-56。
[32] 金管會 108 年 7 月 3 日 1080321164 號函。
[33] 宋皇志、吳婕華(2021)，〈虛擬貨幣之法律性質與監理規範〉，《臺北大學法學論叢》，第 117 期，2021.03，165-68。

之監理模式分類，以之作為基礎，將各國模式分為（一）無為而治模式：以該國既有之金融監理法規監理之，我國、英國及加拿大為此種模式。（二）以支付監管為基礎之特別許可模式：1，美國紐約州：美國 SEC 採無為而治模式，不另為交易平台設立規定，回歸證券交易所管理。但州層次的監管有不同模式，以紐約為例，紐約州於 2015 年制定虛擬通貨規則 Bit License 規則，對於交易平台之財務及內控、消費者保護、交易平台使用者資產保護等要較高之要求。2，日本：日本 2017 年頒布支付服務法，對於平台使用者資產保護作出較嚴格規範。（三）以證券監管為基礎之特別許可模式：此係旨在既有之證券監管法制中，將虛擬通貨交易平台納入，若個案中虛擬通貨非有價證券，仍會受到特殊之規定監管，泰國、馬來西亞為此模式[34]。

首次代幣發行之比較法監管上，鄭婷嫻教授整理美國數起 ICO 實例，美國證管會皆以案例發行之虛擬通貨符合 Howey Test 認定具有證券性質。後美國頒布群眾募資法放寬小型企業對公眾募資之限制，2019 年 7 月 11 日出現第一家 SEC 批准合法 STO 募資之企業 Blockstack，具有未來可能讓其他企業仿效的指標意義[35]。宋皇志教授與吳婕華律師整理認為比較法上就 ICO 監理模式可分為（一）全面事前核准制：無論是否為證券類型，所有 ICO 均須事前核准使得發行，如泰國、日本。日本方面，日本金融服務局於 2019 年 11 月宣布，日本虛擬貨幣兌換協會為日本之支付服務法下的自律組織，與金融服務局進行 ICO 監管。（二）以是否具有證券性質區別化事前核准制：有證券性質之 ICO 須事前核准始能發行，例如美國、瑞士、新加坡、香港。（三）為禁止但發布警示風險：此係未禁止 ICO 發行亦未有實質監管，但是有發佈風險警示，例如英國、德國。（四）全面禁止 ICO 發行：例如中國、韓國[36]。

蔡英欣教授研究日本法規認為，日本法從功能層面定義虛擬通

[34] 楊岳平，同前註 24，頁 1354-73。
[35] 鄭婷嫻，同前註 18，頁 178-84。
[36] 宋皇志、吳婕華，同前註 33，頁 174-87。

貨，有利於主管機關監管，且從功能性出發之立法對於業者較易理解且較為公平，同時可避免監理套利。另外日本法低密度監理又重視業者自律下，此較容易鼓勵金融創新業者投入市場[37]。

第四項 金管會最新證券型虛擬通貨監管方案

虛擬通貨所採用之區塊鏈技術具有去中心化、可跨國傳輸之特性，有助於簡化金融交易[38]，因而透過發行虛擬通貨代幣（Initial Coin Offering，ICO）向大眾募集資金成為近年一種新的募資管道。

我國金管會於 2017 年針對坊間招攬投資虛擬貨幣之活動，包括 ICO 募資行為表明立場，強調虛擬貨幣或 ICO 發行方如有以虛偽不實之技術，或以不合理之高報酬，吸引投資人參與，則可能構成詐欺或違法吸金等刑事案件，而 ICO 行為如有涉及有價證券之募集與發行，應依證券交易法相關規定辦理。至於 ICO 代幣是否屬證券交易法規範之有價證券，應視個案情況認定[39]

我國金管會於 2019，發布新聞稿將具有證券性質之虛擬通貨核定為有價證券[40]，並就證券型代幣發行（Security Token Offering，STO）採分級管理，募資金額新臺幣(下同)3,000 萬元(含)以下豁免其應依證券交易法第 22 條第 1 項之申報義務，募資金額 3,000 萬元以上應依「金融科技發展與創新實驗條例」申請沙盒實驗，實驗成功後依證券交易法規定辦理。嗣財團法人中華民國證券櫃檯買賣中心（下稱「櫃買中心」）依金管會授權於 2020 年發布多個虛擬通貨業務管理辦法，包括 STO 之公開說明書應行記載事項準則、證券商經營 STO 之業務管理辦法及 STO 之會計議題、審計議題指引等，供

---

[37] 蔡英欣(2018)，〈試論虛擬貨幣之監理與法律地位——以日本法為中心〉，《管理評論》，第 36 卷第 4 期，頁 58, 64。

[38] 李宜雯，黃曉盈，周玉娟(2019)，〈我國對證券型代幣發行、交易及平台監理之規劃方向〉，《證券暨期貨月刊》，第 37 卷第 11 期，頁 6。

[39] 金管會再次提醒社會大眾投資比特幣等虛擬商品的風險，2017-12-19，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712190002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News，最後瀏覽日：2021 年 6 月 16 日。

[40] 金管會對「證券型代幣發行(Security Token Offering, STO) 相關規範」之說明，2019-06-27，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News，最後瀏覽日：2021 年 6 月 16 日。

STO之發行人及經營交易平台業務之業者遵循。

而分級管制之方式，有認為金管會立意雖是先以小額募資測試市場對 STO 的接受度及反應[41]，但亦有批評指出此辦法規範過嚴，且無視國內證券發行管道選擇較少、流程複雜且成本高昂之特性，卻設法限制發行市場讓原本開放的美意淪為象徵意義，不但有違區塊鏈去中心化與跨國界之特性，同時也扼殺外國資本挹注的可能性，並有立法委員據此而於 108 年聯署提案，針對虛擬通貨特別增訂「證券型虛擬通貨交易法」[42]。

所謂具有證券性質之虛擬通貨，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，且具流通性及下列投資性質者：

1. 出資人出資；
2. 出資於同一共同事業或計畫；
3. 出資人有獲取利潤之期待；
4. 利潤主要取決於發行人或第三人之努力」[43]

上述標準金管會乃參考美國聯邦最高法院針對「投資契約」所操作之標準「Howey Test」，就此，楊岳平教授指出[44]，目前我國就證券型虛擬通貨之監管方式存在以下問題：第一，依據金管會前述對證券型虛擬通貨之定義，有部分類型之虛擬通貨無法受上述定義所涵蓋，如不具分潤機制的功能型虛擬通貨在交易即無法受證券交易法所監管；第二，有價證券與投資契約本質上仍有別，使用「Howey Test」來建立是否屬於有價證券之定義標準亦有疑義；第三，非以密碼學及分散式帳本或其他類似技術所發行之投資契約，縱符合上述「Howey Test」之標準，目前並不構成有價證券，而無庸受證交法所納管，此會造成對待虛擬通貨與其他金融商品之差別待遇。此外，鄭婷嫻教授亦建議，應將具有投資契約性質者納入證

[41] 李宜雯，黃曉盈，同前註 38，頁 10。
[42] 立法院第 9 屆第 8 會期第 13 次會議議案關係文書，提案字號：院總第 707 號委員提案第 23812 號。
[43] 金管證發字第 1080321164 號 令「有關核定具證券性質之虛擬通貨為證券交易法所稱之有價證券之令」。
[44] 楊岳平，前註 24。

交法第 6 條第 1 項規定之有價證券定義中，並明確化引進「Howey Test」四要件於我國法上之檢視標準。

金管會於 2021 年 4 月 20 日再次發布新聞稿[45]，重申除符合上述定義之「具證券性質之虛擬通貨」，其他像比特幣或類似性質的虛擬資產，均非金管會核准發行的金融商品，亦非屬貨幣，但此類「虛擬商品」，但考量其洗錢風險，我國洗錢防制法(以下簡稱洗防法)已將「虛擬通貨平台及交易業務事業」納入洗錢防制範疇。

第五項 虛擬通貨相關犯罪理論

所謂虛擬通貨，依我國法下之定義，係指「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。」[46]。目前國際上之多數先進國家尚未將單純使用虛擬通貨視作犯罪行為，然而虛擬通貨由於其表彰價值及於數位環境下使用之特性，因具有表彰一定資產價值之功能，於作為投資工具或支付手段使用時已衍生國內外投資詐騙[47]、涉犯洗錢防制[48]、違反證券交易法[49]或非法吸金[50]等經濟犯罪之案件。

依林東茂教授之整理[51]，所謂經濟犯罪[52]是指攻擊總體經濟及其

---

[45] 金管會提醒社會大眾有關虛擬資產的相關風險，2021-04-20，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202104200003&dtable=News，最後瀏覽日：2021 年 6 月 16 日。

[46] 行政院院臺法字第 1100167722 號令：「（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。」

[47] 剛買瑪莎拉蒂就被捕，桃園警方破獲「比特幣詐騙集團」犯罪所得近千萬，2020-06-19，動區動趨，https://www.blocktempo.com/another-crypto-fraud-being-caught/，最後瀏覽日：2021 年 6 月 16 日。

[48] 鑫棧虛擬貨幣工作室盜領泰達幣 8 年級首腦涉洗錢遭訴，聯合報，2021-05-26，https://udn.com/news/story/7321/5486640，最後瀏覽日：2021 年 6 月 16 日。

[49] 是證券不是幣？美國 SEC 大陣仗起訴瑞波幣母公司！，2020/12/23，TNL Media，https://www.inside.com.tw/article/23783-akamai-gaming-2021，最後瀏覽日：2021 年 6 月 16 日。

[50] Q 點虛擬貨幣吸金 2.5 億 9 人起訴，2021/04/24，中國時報，https://www.chinatimes.com/newspapers/20210424000443-260106?chdtv，最後瀏覽日：2021 年 6 月 16 日。

[51] 林東茂(1999)，〈經濟犯罪的幾個現象面思考〉，《刑事政策與犯罪研究論文集》，第 2 期，頁 61-77 頁。

[52] 我國司法偵查實務上就經濟犯罪之認定標準定有「法務部調查局重大經濟犯罪案件認定要點」。

重要分支部門之犯罪行為，而行為人的終極目的是獲得財產利益[53]。而經濟犯罪之發生將受到具體經濟條件影響，包含：(1)景氣上的原因；(2)國家干涉經濟活動；（3）國家管制與營業上管制的疲弱；（4）經濟活動的匿名性；（5）經濟活動的複雜性與經濟犯罪的發生具有關聯性；（6）公司型態；（7）企業的資本結構脆弱；（8）經濟犯罪的仿效傳染；（9）經濟制度等[54]。

自上述學者整理之經濟犯罪影響條件影響以觀，對照虛擬通貨近年之發展，全球於 2020 年起因受新冠肺炎疫情影響，各國為提振經濟紛紛下修利率[55]，可能導致市場上熱錢湧向新的投資標的，虛擬通貨交易市場並因此而活絡，故衍生相關之多起詐騙投資，且虛擬通貨乃基於密碼學之基礎，具有去中心化、可匿名之特性，且必須於網路環境上交易，取得和流通操作相對於法定貨幣而言較為複雜困難，符合上述經濟活動的匿名性和複雜性之特色，可能為繼而易引發犯罪發生之原因。

此外虛擬通貨以數位方式於網路環境上儲存及交易，亦衍生駭客竊盜虛擬貨幣[56]、勒索軟體要求以虛擬通貨支付贖金[57]等網路犯罪之可能風險。

關於網路犯罪之定義，依陳靜慧檢察官之整理[58]，網路犯罪之定義學說上多有分岐，有認為屬於電腦犯罪中具有網際網絡特性者，為電腦犯罪之延伸，惟在性質上較偏重於網際網路之應用；另有論

[53] 林東茂，同前註 51，頁 63-65

[54] 林東茂，同前註 51，頁 70-71；Franzheim, Krimimologene Faktoren der Wirtschaftskriminalitat, Kriminalistik,1980,S. 278 ff..

[55] BBC 中文，肺炎疫情：美聯儲緊急降息至零利率 「一次性打完所有彈藥」，2020 年 3 月 16 日，https://www.bbc.com/zhongwen/trad/business-51906250 ，最後瀏覽日：2021 年 6 月 16 日。；駐英國台北代表處經濟組，駐英經（109）經字第 102/P200 號（商情文號:第 102 號）：英國央行緊急調降利率以抑制新冠病毒帶來的經濟衝擊 ，2020-03-12，https://www.trade.gov.tw/Pages/Detail.aspx?nodeid=45&pid=690749 ，最後瀏覽日：2021 年 6 月 16 日；鉅亨網，2020/09/03，日本央行審議委員：須調降利率減輕企業家計利息負擔 抑制通縮壓力，https://news.cnyes.com/news/id/4520576 ，最後瀏覽日：2021 年 6 月 16 日。

[56] 日本加密貨幣交易所遭駭 35 億日圓一夕消失無蹤，2019-07-12，中央廣播電臺，https://www.rti.org.tw/news/view/id/2027140 ，最後瀏覽日：2021 年 6 月 16 日。

[57] 勒索軟體頻攻擊科技廠 立委籲政府協力防護 ，2021/4/21，中央社，https://www.cna.com.tw/news/aipl/202104210115.aspx ，最後瀏覽日：2021 年 6 月 16 日。

[58] 陳靜慧(2015)，〈網路犯罪之新趨勢與規範狀態之初探～從物聯網之發展談起〉，《臺灣嘉義地方法院檢察署 104 年度自行研究報告》，頁 4

者認為，所謂網路犯罪係指利用網際網路之特性，包括：大量傳播、即時性、匿名性等特性，以之為犯罪手段或犯罪工具，性質上為網路濫用行為。

而就網路犯罪之相關成因，林宜隆教授及黃讚松研究生指出[59]，造成網路犯罪發生之主要因素包括(1)網路本身特性；(2)網路偵查的技術限制；及(3)對網路犯罪之法律規範機制尚未完備等。

網際網路本身具有之跨國性、分散性、開放性、互通性，使犯罪並無法由單一司法管轄區能全面掌控，各司法管轄區亦無一共通之網路法律標準[60]，此外，由於網路具有匿名特性且資料以電磁方式存在，導致確認網路使用者於真實社會之身分及證據保存等構成司法偵查之困難[61]，且網路犯罪有朝向科技化及專業化發展之趨勢，使犯罪手法不斷更新，更讓執法機關疲於應付。

[59] 林宜隆，黃讚松(2002)，〈網路使用問題分析與犯罪預防之探討〉，《資訊科技與社會學報》，第 3 期，頁 95-114。
[60] 同前註，頁 103-104。
[61] 林宜隆，黃讚松，同前註 59，頁 104。

第二章　電子支付工具新興犯罪背景成因及類型分析

第一節　犯罪背景

第一項 我國電子支付工具概述

一、電子支付工具之定義

根據金管會「行動支付與電子化支付普及之關鍵」一文，新興支付工具包括行動支付與電子化支付[62]。所謂行動支付，係指應用新興技術，將實體支付工具如信用卡、電子票證等下載至行動裝置(包括手機或手環、指環等穿戴式裝置)，讓行動裝置變錢包，消費者經過申請及身分驗證等程序後，即可持行動裝置進行消費交易的支付方式，可分為行動信用卡、行動金融卡、行動電子票證、電子支付機構實體通路支付服務（行動電子支付）及行動收單五種類型[63]。至於所謂電子化支付，則泛指非現金之支付工具，包含信用卡、電子票證（如悠遊卡等）、電子支付或第三方支付、轉帳等進行支付[64]。

本研究受委託的研究對象為電子支付工具。參酌現行電子支付機構管理條例之規定，包括代理收付實質交易款項、收受儲值款項、辦理國內外小額匯兌、以及辦理與以上業務有關之買賣外國貨幣及大陸地區、香港或澳門發行之貨幣業務，故本研究所稱的電子支付工具，係指自上述業務衍生的支付工具，包含取得金管會許可而綜合經營上述業務的電子支付，以及僅經營小規模代理收付實質交易款項而毋需取得金管會許可的第三方支付。為避免與現行其他相類似概念造成混淆，以下將以「電子支付工具」一詞統稱前開「電子支付」與「第三方支付」，如有必要專指綜合經營上述業務的電子支付，則另以「狹義電子支付」指稱之，合先敘明。

二、電子支付工具的發展現況

電子支付工具於我國起步較晚，惟近年使用電子支付工具進行交易之人數與金額均持續成長。以狹義電子支付為例，截至 2021 年 6 月底止，國內計有 5 家專營電子支付機構及 23 家兼營電子支付機

[62] 金管會（2018），〈行動支付與電子化支付普及之關鍵〉，《臺灣經濟論衡》，第 16 卷第二期，頁 29-30。
[63] 金管會，同前註，頁 30、37。
[64] 金管會，同前註，頁 29。

構（含銀行、中華郵政股份有限公司及電子票證發行機構），總使用者人數約 1,389 萬人，單月代理收付實質交易款項金額約 70.8 億元；單月電子支付帳戶間款項移轉金額約 51.9 億元；單月收受儲值款項金額約 128.9 億元；支付款項餘額約 56.7 億元[65]。

以下圖三為自 2018 年 4 月起每月的狹義電子支付業務數據彙總。整體而言，專屬電子支付機構的收受儲值業務與電子支付帳戶間移轉款項業務均有大幅的業務規模提升，可見電子支付市場正在顯著成長中。

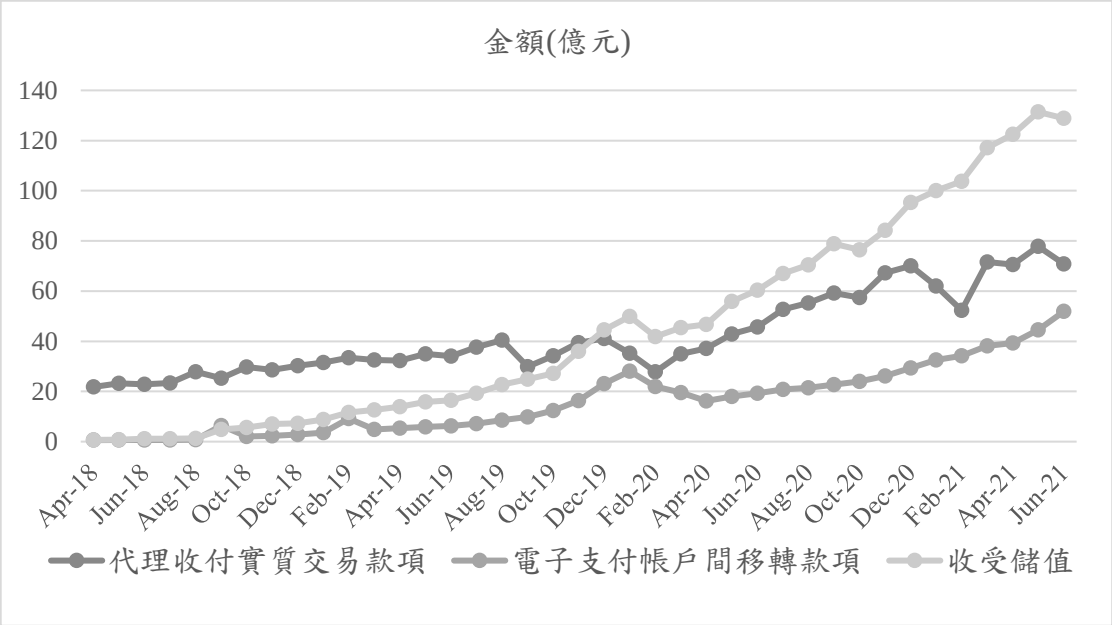


圖 1 2018~2021 年狹義電子支付業務之當月交易金額統計

資料來源：金管會銀行局歷年新聞稿[66]

除狹義電子支付外，第三方支付於我國市場亦有顯著的成長。依行政院近期之定義與金管會過往之說明，第三方支付係指僅提供

[65] 金管會新聞稿（2021/8/12），110 年 6 月份信用卡、現金卡、電子票證及電子支付機構業務資訊，https://www.banking.gov.tw/ch/home.jsp?id=540&parentpath=0,524,539&mcustomize=news_view.jsp&dataserno=202106100005&dtable=News（最後瀏覽日期：2021/06/14）。

[66] 金管會銀行局新聞稿，https://www.banking.gov.tw/ch/home.jsp?id=540&parentpath=0,524,539&mcustomize=（最後瀏覽日期：2021/08/16）。

代理收付網路實質交易款項服務而非屬電子支付機構管理條例所稱電子支付機構者，亦即僅經營代理收付實質交易款項之業務且日平均餘額未超過新台幣二十億元者[67]。其於我國現行法下不受金融監管，僅登記於經濟部商業司「第三方支付服務業」中，由經濟部商業司對第三方支付服務業者進行一般商業管理。

截至 2021 年 08 月 01 日為止，我國共有 13,113 家已核准登記或核准設立之第三方支付服務業者（已扣除已解散、廢止、撤回認許之公司）[68]。較為知名者例如：Line Pay、綠界科技(ECPAY)、藍新科技、PChomePay 支付連、奇摩輕鬆付、HyPocket（全球聯網）、Swipy（紅陽科技）、SmilePay（訊航科技）等。

第二項 電子支付工具的分類

本研究以下透過對不同電子支付工具進行分類，以進一步具體說明本研究的研究對象。

一、狹義電子支付

依 2021 年 7 月 1 日施行之《電子支付機構管理條例》第 3 條第 1 款、第 4 條第 1 項及第 2 項之定義，電子支付機構係指辦理代理收付實質交易款項、收受儲值款項、國內外小額匯兌、以及與上述三款業務有關之買賣外國貨幣及大陸地區、香港或澳門發行之貨幣業務之機構[69]。凡辦理上述業務者，原則上須申請取得電子支付機構許可方可經營之[70]。目前國內計有 5 家專營電子支付機構（包括街口支付、橘子支付、歐付寶、智付寶、簡單付(ezPay)）、4 家舊法下的電

[67] 行政院 110 年 8 月 18 日院臺法字第 1100181600 號函；金管會（2015/07/02），〈電子支付機構及第三方支付服務業之異同〉，https://fscmail.fsc.gov.tw/POP30/（最後瀏覽日：2021 年 6 月 14 日）；經濟部 107 年 1 月 22 日經商字第 10600106330 號函；電子支付機構管理條例第五條第二項授權規定事項辦法第 3 條。

[68] 經濟部商業司，公司登記（依營業項目別）--第三方支付服務業，https://data.gov.tw/dataset/22184（最後瀏覽日期：2021/08/03）。

[69] 此外電子支付機構亦辦理提供特約機構收付訊息整合傳遞、提供特約機構端末設備共用、提供使用者間及使用者與特約機構間訊息傳遞、提供電子發票系統及相關加值服務、提供商品（服務）禮券或票券價金保管及協助發行、販售、核銷相關服務、提供紅利積點整合及折抵代理收付實質交易款項服務、提供儲值卡儲存區塊或應用程式供他人運用、提供電子支付業務有關之資訊系統及設備之規劃、建置、維運或顧問服務，以及其他經主管機關許可之業務。

[70] 電子支付機構管理條例第 5 條第 1 項。

子票證機構（包括悠遊卡、一卡通、愛金卡、遠鑫）及 23 家兼營電子支付機構。

另依照《與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法》，經核准之電子支付機構、非兼營電子支付機構業務之銀行或金融資訊服務事業及資料處理服務業者，可與境外機構合作在我國境內辦理電子支付相關業務。典型案例包括 PayPal 與玉山銀行合作使我國用戶可透過玉山銀行帳戶提領 PayPal 帳戶款項、Alipay 與玉山銀行合作提供我國用戶使用支付寶等。例如於我國常見的支付寶，其法律實質關係實為玉山銀行提供的電子支付服務。

二、第三方支付

第三方支付之起源係為了保障交易之安全性，而由買方及賣方以外之中介機構協助進行代收及代付。如上述，根據行政院與金管會的定義，第三方支付係指僅經營代理收付實質交易款項業務且所保管代理收付款項之一年日平均餘額未逾新臺幣 20 億元者[71]。第三方支付非屬須受金融監管的業務，我國目前對第三方支付之規範，主要為經濟部所頒布之《第三方支付服務定型化契約應記載及不得記載事項》。

三、電子支付工具與其他行動支付的區辨

本研究所稱的電子支付工具，並不包含以下常見的其他行動支付工具：

1. 行動信用卡：行動信用卡係指信用卡發卡機構與代碼化服務業者合作，運用代碼化技術，使得持卡人經過申請及身分驗證等程序後，即可將實體信用卡卡號轉換成代碼載入手機等行動裝置，進而可持該行動裝置進行消費交易[72]。常見如：

[71] 行政院 110 年 8 月 18 日院臺法字第 1100181600 號函；金管會（2015/07/02），〈電子支付機構及第三方支付服務業之異同〉，https://fscmail.fsc.gov.tw/POP30/（最後瀏覽日：2021 年 6 月 14 日）；經濟部 107 年 1 月 22 日經商字第 10600106330 號函；電子支付機構管理條例第五條第二項授權規定事項辦法第 3 條。

[72] 金管會，前揭註 62，頁 29-30。

Apple Pay、Google Pay 以及 Samsung Pay。

2. 行動金融卡：係指透過空中傳輸下載個人化資料至行動裝置，發行具行動交易功能之金融卡[73]。常見如：台灣 Pay「金融卡雲支付」。

3. 行動收單（mPOS）：又稱行動刷卡機，係指將行動電話或平板電腦搭配 APP 配件變成收單裝置，再經由刷卡或晶片插卡方式，讓商店端可以隨時接受信用卡付款[74]。

第三項 電子支付工具與犯罪

電子支付工具作為一新型態的支付工具，存在一定特性使其易於成為犯罪者使用的犯罪工具。以下謹根據國際組織與學理上的觀察，說明電子支付工具之特性與潛在的犯罪風險。

一、FATF 之觀察

防制洗錢金融行動工作組織（The Financial Action Task Force, FATF）於其 2013 年發布之「預付卡、行動支付與網路付款服務風險基礎方法指引（Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services）」指出，全球的「新型態支付產品與服務」（new payment products and services, NPPS）的快速發展、功能增加以及使用率提高，對各國與私部門在確認該等產品與服務是否遭洗錢（money laundering）與資助恐怖分子（terrorist financing）目的濫用方面帶來挑戰，其所討論的 NPPS 即包含電子支付工具[75]。

依照 FATF 所提出之支付工具風險因子（payment methods risk factors）[76]，NPPS 主要具有下列幾種有別於傳統現金交易之特性：

(一)匿名性：

---

[73] 金融機構辦理行動金融卡安全控管作業規範第 2 條第 1 款

[74] 金管會網站，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201411250002&toolsflag=Y&dtable=News (最後瀏覽日：2021/06/15)

[75] FATF-GAFI, *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, at 4 (June. 2013), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.

[76] *Id.* at 19.

NPPS 係透過網路或通訊技術之運用以完成交易，不須提供交易人之姓名及身分識別資訊，具有一定程度之匿名性，有利於犯罪行為人隱匿席真實身分。此一特性可以藉由法規強制要求實名制而緩解，惟犯罪行為人仍有可能以盜用他人身分或創建虛假身分等方式進行註冊，而達到匿名之效果。

(二)無法審查資金來源、金流追查不易：

NPPS 的資金來源多元，可能係以簽帳金融卡直接扣款、以現金儲值方式扣款、綁定信用卡，亦或是電子支付工具，而配合前述提及之匿名性，資金透過在帳戶及帳戶間以多層架構之方式，或透過空殼公司進行轉移，均造成偵查機關追查資金來源之困難。

(三)跨境移轉資金：

NPPS 使用者通常得以透過全球支付網路於國內及國外進行交易，對於透過NPPS遂行之犯罪行為難以有效執法，且各管轄地對於洗錢防制及反資恐的規範程度不同，犯罪行為人會傾向選擇規範相對鬆散的地區進行犯罪活動。然而，因我國非國際刑警組織(The International Criminal Police Organization, INTERPOL)之成員國，因此執法機關的困境之一乃在難以取得偵查此種犯罪上所必需之資訊。

二、學理觀察

除 FATF 外，國際學者有由網路洗錢的角度出發，分析網路時代下新型態支付工具例如電子支付工具用於洗錢犯罪時之犯罪特性如下[77]。

(一)匿名性

政府如欲採取偵查行動以調查犯罪，往往需掌握犯罪背後交易金流的流向。但新型態支付工具因為係利用網路技術，因此具備網路世界常見的匿名性，從而增加犯罪偵查的困難。

(二)快速性

新型態支付工具因為使用電腦設備與網路技術處理資料，因此

[77] *See generally* Angel L. Rodriguez Santiago, *New Payment Methods and Insufficiencies in Their Regulatory Scheme*, 7 J. L. & CYBER WARFARE 101 (2019).

資料處理速度較傳統支付工具更快，進而使交易速度乃至洗錢的速度均可加快。犯罪行為人因此可利用新型態支付工具在境內甚至境外快速且大量地進行交易，進而快速達到其洗錢目的，並且使洗錢過程的成本更為低廉。

(三)追蹤困難性

許多利用新型態支付工具的洗錢活動，可以利用網路技術進行藏匿交易軌跡的處理，進而增加追蹤金流的困難度而更有助洗錢犯罪。例如 IPv4 的結構，即允許用戶在數據包中創建錯誤的返回地址，從而使某些通訊或交易幾乎無法被追蹤。

(四)非面對面接觸

網路金融服務是利用電腦軟體與銀行或金融機構的伺服器連結，連結過程經常是自動進行、而欠缺人為參與。金融機構伺服器在客戶登入時，主要亦係以帳號與密碼進行認證，只要帳號與密碼正確，金融機構伺服器就會給予登入者訪問的權限，而不會亦難以確實檢查登入者的真實身分，因此冒用身分的情形即可能發生。

(五)跨境性

電子支付工具服務提供商的地址通常與其伺服器的實際位置、管理伺服器的位置、或是客戶登入的地點不完全相同，以達到跨境支付的便利性。但此新興支付技術亦使犯罪行為可能橫跨多個法律體系，進而牽涉多個司法管轄區而面臨跨境執法的挑戰。儘管許多國際條約或公約試圖克服或緩解跨境執法的困難，但其具體實施成效仍是巨大的挑戰。

第四項 常見使用電子支付工具之犯罪類型及案例

基於以上特性與犯罪風險，犯罪行為人開始利用電子支付工具發展新的犯罪手法，包括誤導民眾連結至詐騙網站、偽造或竄改 QR Code 等。以實務上最常見的犯罪態樣之一即詐騙為例[78]，近年的詐騙態樣也開始利用電子支付工具的特性而更加多樣化，並且伴隨洗

[78] Karsten Witke, *The Seven Types of E-commerce Fraud Explained*, Information Age (Nov. 25, 2019), https://www.information-age.com/seven-types-e-commerce-fraud-explained-123461276.

錢活動的發生。以下舉例說明之。

一、盜用型詐騙

盜用型詐騙具體而言包含身分竊盜（identity theft）與帳戶竊盜（account theft）。傳統的盜用型詐騙案例多係透過創建身分之方式，進而盜用被害人身分進行犯罪，但在電子支付工具普及後，由於現代人的生活大量依賴行動裝置─例如使用手機付款、購物網站及社群網路等，導致大量的資訊集中在個人的行動裝置上─例如手機綁定的信用卡或金融卡資訊。犯罪行為人如利用行動裝置的資訊安全漏洞，例如透過釣魚（phishing）、網址嫁接（pharming）或中間人攻擊（Man-in-the-middle attack）等方式騙取或盜用信用卡帳號密碼，即可以更低廉的成本更方便地竊取他人的個人資料與身分，進而增加盜用型詐騙的機率。

以近期新聞報導已提及的實務案例為例，就已包含以下種類：

(一)配合政府口罩購買政策進行釣魚以盜用帳戶

犯罪行為人以政府名義發送有關口罩購買或催繳健保費之資訊[79]，或假扮集運公司寄宿包裹派發簡訊[80]，引誘民眾點選連結，進而竊取帳號密碼並開通手機小額付款。

(二)以惡意程式創建虛假帳號詐騙全聯 PX Pay 會員點數

例如全聯 PX Pay 為進行會員促銷，對於首次開通及推薦他人加入會員之均贈與會員點數。犯罪行為人即以電腦惡意程式產生之姓名、電話、出生年月日等個人資料創立為數眾多的假會員帳號，並在獲得點數後轉入自己名下[81]。

(三)竄改、偽造或覆蓋 QRcode

目前多數電子支付均支援手機掃碼 QRcode 來進行支付。金管會為此曾於 2019 年底時提醒民眾，國外以竄改、偽造或覆蓋 QRcode 連結至詐騙帳戶或惡意網站之案例頻傳[82]。

---

[79] 中央健康保險署新聞稿（2020/05/06），〈不會有連結！口罩進化，小心詐騙也進化〉，https://www.mohw.gov.tw/cp-16-53090-1.html（最後瀏覽日：2021/03/21）。

[80] 自由時報（2020/03/28），〈網購包裹到家了？恐損失近萬元、「簡訊連結」千萬別點！〉。

[81] 自由時報（2020/10/15），〈「全聯」APP 會員贈點活動遭惡意程式詐騙 盜取 1500 萬點數〉。

[82] 蘋果日報（2019/11/03），〈防手機掃碼支付成詐騙漏洞　金管會設 3 大控管機制〉。

此外於國內新冠疫情期間，政府為因應疫情推出「1922 簡訊實聯制」，使民眾出入公共場合登記更方便，減少操作時間。然而即傳出有不肖人士偷偷調換置於店家門口的 QR Code，導致民眾掃描該偽造連結後被引導至詐騙頁面、或被引導傳訊至高額付費號碼，因此被詐取錢財[83]。

二、其他詐騙態樣

以第三方支付為例，第三方支付原係為了在買賣雙方間發揮其監管及保障作用，由買家將款項轉入第三方支付平台所與金融業者合作提供之虛擬帳戶，在買家確認收受貨品後，再由平台將款項支付予賣方。惟由於此類虛擬帳戶容易以假個資申請或竊取他人個資申請等方式取得、且不易追查帳戶持有人的真實身分，帳戶所在位置亦可能因為在國外而導致執法困難，因此虛擬帳戶及第三方交易流程也淪為實務上常見之詐騙犯罪工具[84]。

常見之手法包含謊稱網路購物錯誤設定為分期付款，要求被害人配合將款項轉入「虛擬帳戶」協助解除分期；利用第三方支付虛擬帳戶詐騙[85]，以便宜的價格促銷商品，在買家支付款項後，以推託等方式延遲或拒絕給付商品；或利用第三方支付公司進行三方詐騙，向賣家買入遊戲點數，再假裝轉賣予第三方，請第三方匯款至賣家的虛擬帳戶[86]等。

第五項 小結

綜上，電子支付工具近年於我國已有長足的發展，規模亦逐漸擴大中。但電子支付工具的諸多特性，使得其具有成為犯罪工具的潛力，國內亦已屢見電子支付工具用於犯罪的案例發生。為此有必要系統性地研究電子支付工具被使用於犯罪的情形，以確實掌握電

[83] 科技新報（2021/08/06），〈發送實聯制前先注意，詐騙集團偷換 QR Code 讓民眾傳到高額付費電話〉。

[84] 自由時報（2020/02/26），〈虛擬帳戶成詐騙工具 警：個資外流小心成幫助犯〉。

[85] 數位時代（2016/12/09），〈別以為透過第三方支付購物就保險，刑事局偵九隊宣佈偵破新型態第三方支付詐欺集團，〉https://www.bnext.com.tw/article/42275/new-third-party-payment-fraud-group（最後瀏覽日：2020/10/22）。

[86] 聯合報（2020/05/11），〈第三方支付管理鬆成詐騙洗錢管道〉。

子支付工具的犯罪風險具體樣貌，進而可對症下藥研擬因應之道。

第二節　電子支付工具犯罪之類型化分析

本部分彙整公開資料顯示的電子支付工具被使用於犯罪的國際案例與發展情形。有鑑於一般支付工具涉及的犯罪類型主要為詐騙與洗錢[87]，以下將以電子支付工具用於詐騙與洗錢的國際犯罪發展情形為主要分析對象。

第一項 詐騙類型

一、國際發展趨勢分析

詐騙活動向來是國際商務活動中面臨的主要犯罪類型之一。根據 Association for Financial Professionals（AFP）於 2020 年的研究顯示，B2B 交易活動中的詐騙數量在過去五年有明顯的增長，如以下圖 4 所示，至 2018 與 2019 年，已有超過 80%的受調查機構表示其曾遭遇詐騙。

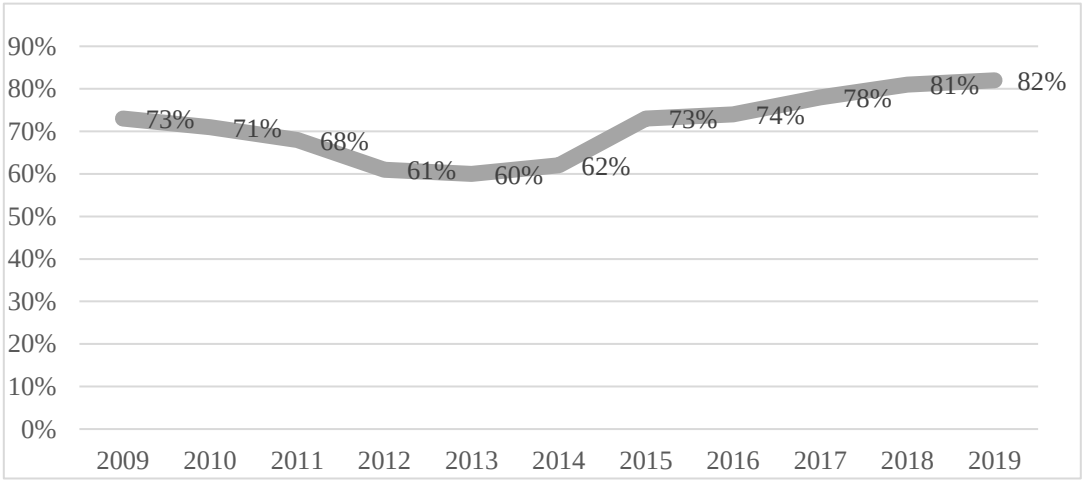


圖 2 國際商務機構受詐騙的比率（2009~2019）

資料來源: 2020 AFP Payments Fraud and Control Survey Report: Key Highlights[88]

[87] Emerging Payments Association, *Facing Up to Financial Crime: Analysis of Payments-Related Financial Crime and How to Minimise Its Impact on the UK,* https://midasalliance.org/wp-content/uploads/2019/02/EPA-Facing-Up-to-Financial-Crime-Whitepaper-Full-Version-v2.0-1.pdf (last visited: June 20, 2021).

[88] *Supra* note 15, at 7.

而隨著支付方式近年的轉變，詐騙活動應用的支付方式也有一定程度的變化。如以下圖 5 所示，詐騙活動所使用的支付方法最大宗仍為支票與電匯，其次則為信用卡、金融卡、公司商業卡等媒體交換自動轉帳服務（Automated Clearing House, “ACH”）。但新興的支付方式例如快速支付系統乃至電子錢包，也已逐漸成為詐騙活動會使用的支付方式。

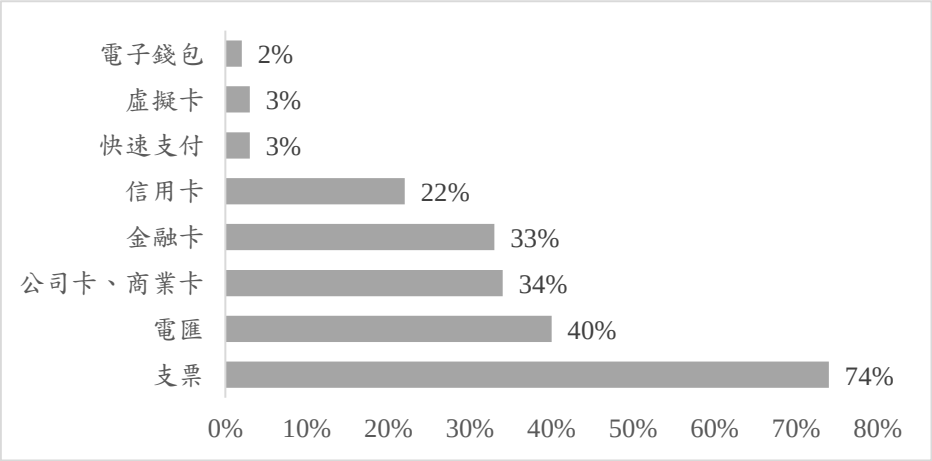


圖 3 國際商務機構受詐騙的支付形式（2019）

資料來源: 2020 AFP Payments Fraud and Control Survey Report: Key Highlights[89]

而隨著國際商務活動中電子商務的發展，衍生的線上支付詐騙也受到相當的關注。根據 Ingenico Payment Services 的統計資料，如以大型公司受交易詐騙的價值佔其總體交易價值之比率計算線上支付詐騙率，全球線上支付詐騙率約為 0.47%，以單一國家而言，如以下圖 6 所示，最高者前三名依序為墨西哥（1.31%）、荷蘭（0.80%）及法國（0.74%）。

[89] *Supra* note 15, at 8.

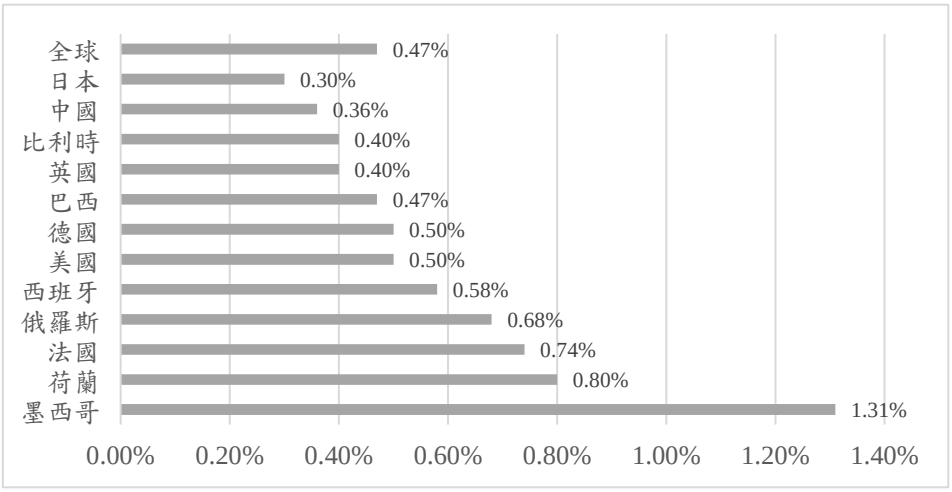


圖 4　主要國家線上支付詐騙率

資料來源: Online Payment Fraud Whitepaper 2016-2020[90]

如以產業而言，線上支付詐騙相對集中於若干特定產業。以詐騙交易數量佔總體交易數量為基礎，如以下圖 7 所示，航空業（46%）、匯兌業（16%）以及電腦電子業（13%）相對存在明顯較高比例的詐騙交易情形。

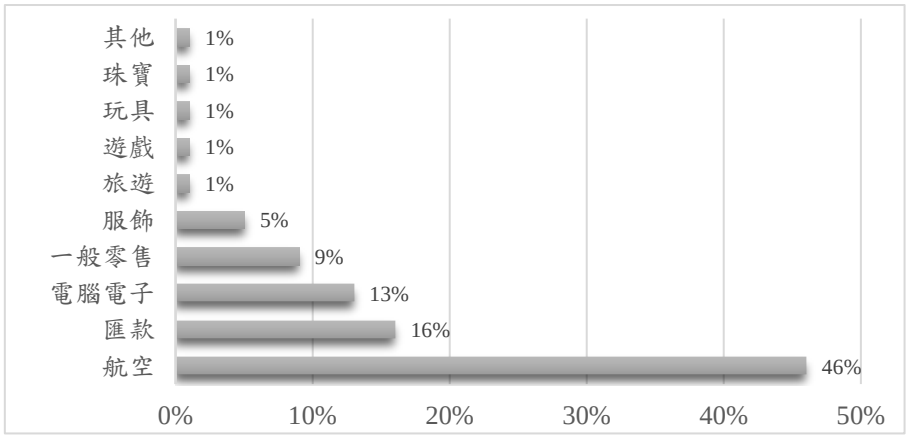


圖 5 主要產業線上支付詐騙交易比例

資料來源: Online Payment Fraud Whitepaper 2016-2020[91]

[90] Juniper Research, *Online Payment Fraud Whitepaper 2016-2020* 11, (2021) (unpublished working paper).
[91] *Id.* at 10.

如繼續觀察主要產業遭遇線上支付詐騙交易的額度，部分產業中的平均詐騙交易價值甚至較平均合法交易價值高出許多，如以下圖 8 所示，航空業的平均交易價值約為美元 600 元，但線上詐騙的平均交易價值竟可達到 1,900 美元，顯示線上詐騙交易的情形不僅嚴重，犯罪所得亦相當可觀。

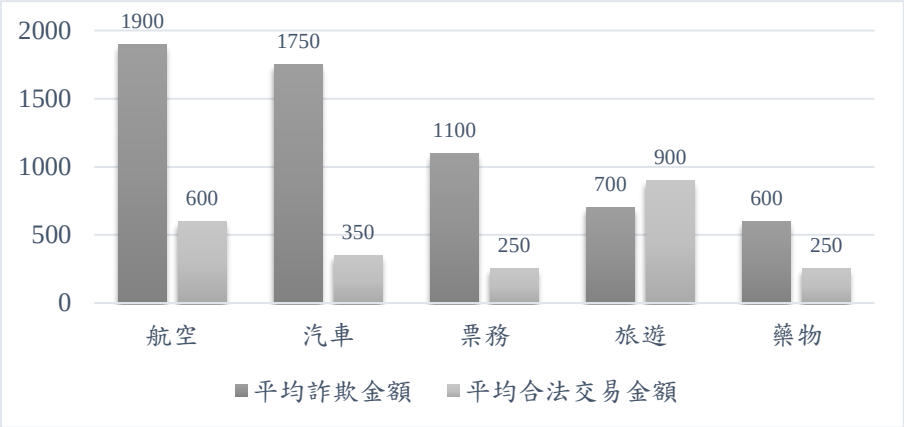


圖 6 主要產業的線上詐騙平均金額與合法交易平均金額

資料來源: Online Payment Fraud Whitepaper 2016-2020[92]

二、電子支付工具詐騙案件的代表案例

國際上電子支付工具詐騙案件主要係以盜用型詐騙為主。所謂盜用型詐騙，係指犯罪行為人透過網路釣魚攻擊，或冒充受信任之身分，取得他人的個人、財務、帳戶資料或付款訊息後，基於此盜用的訊息進行交易。依據 Javelin Strategy & Research 之統計，2020 年度身份詐欺使美國人總共損失了約 560 億美元，約有 4,900 萬消費者成為受害者。其中 130 億美元的損失來自所謂「傳統身份詐騙」，即犯罪者利用網路竊取個人身份資料後將其用於自己的收益。但更大宗達 430 億美元的損失，係由「身份盜用詐騙」所產生，亦即犯罪者利用網絡釣魚電子郵件等方法與消費者直接進行互動後，再進而竊取訊息[93]。

[92] *Id.*

[93] Elisabeth Hershman, *Total Identity Fraud Losses Soar to $56 Billion in 2020*, Berkshire Wire (Mar. 23, 2021), https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-

電子支付工具詐騙所涉及的支付工具，包括傳統的卡式信用卡與匯款機構，以及新型態的電子支付帳戶與QR碼等。以下擷取若干案例作為參考。

(一)盜用信用卡資訊詐騙

2020 年 1 月，一個香港經營的跨國信用卡詐騙集團竊取了至少 21 位新加坡人的信用卡訊息，該集團將竊取到的訊息用於線上購買電子產品。具體犯罪手法如下：詐騙集團首先佯裝成科技媒體服務提供商，寄發電子郵件予被害人，提示被害人更新他們的付款詳細資料，被害人點入後隨即被導入詐騙集團偽裝成服務提供商的網站，進而陷於錯誤而輸入信用卡與一次性密碼等訊息，詐騙集團從而取得被害人的信用卡資訊，並憑藉此於網路上購買電子產品。大多數被害人直至發現信用卡對帳單上有未經授權的交易時，始發現受騙[94]。

(二)西聯匯款或速匯金詐騙

犯罪行為人自合法的寵物主人處或合法寵物運輸網站竊取寵物的照片或影像後，將之發送給潛在的購買者，或製造假廣告放到相關社群媒體平台甚至盜用寵物運輸公司網站，進而利用極低價格將實際上不存在的寵物出售予被害人，接著犯罪行為人要求買家透過西聯匯款（Western Union）或速匯金（MoneyGram）匯款，並且陸續收取文件費用、運輸費用等其他假費用，甚至虛構運輸過程飛機失事造成鉅額法律費用等要求被害人支付[95]。

一般認為犯罪行為人之所以通常選擇使用西聯匯款或速匯金等匯兌管道，是因為相較於其他經許可的信用卡商家系統或電子支付機構而言，通過西聯匯款或速匯金支付的金流通常較難以追查和取回[96]。

(三)QR 碼詐騙

Losses-Soar-to-56-Billion-in-2020.

[94] Dominic Low, *At Least 21 People in Singapore Fall Prey to Transnational Online Credit Card Fraud Syndicate*, The Straits Times (July 28, 2020), https://www.straitstimes.com/singapore/courts-crime/at-least-21-people-in-singapore-fall-prey-to-transnational-online-credit-card.

[95] International Pet and Animal Transportation Association, *Beware: Holiday Pet Scams*, IPATA (Nov. 9, 2018), https://www.ipata.org/beware-holiday-pet-scams ; Jetpets, https://www.jetpets.com.au/pet-scams/ (last visited Mar. 21, 2021).

[96] *See* Jetpets, https://www.jetpets.com.au/pet-scams/ (last visited Mar. 21, 2021).

QR 碼詐騙可能透過劫持使用 QR 碼（所謂「QRL Jacking」）的方式為之。具體而言，當有人使用QR碼作為一次性密碼、並將其顯示在螢幕時，犯罪者將QR碼從合法網站複製到釣魚網站，然後再將其精心製作的帶有有效更新的QR碼的網絡釣魚頁面發送給受害者。受害者使用特定設備掃描QR碼後，攻擊者即取得了受害者帳戶的控制權[97]。

QR碼詐騙亦可能係以假URL取代或覆蓋QR碼的方式遂行。由於QR碼難以自肉眼識別真假，一些犯罪行為人將自己的QR碼覆貼在原始QR碼上，以非法詐騙金錢[98]。典型案例如2017年3月中國廣東省廣州發生有9,000萬元人民幣透過QR碼詐騙被盜取，行為人即是透過自己的虛假付款網址替換付款的 QR 碼，進而達成詐騙目的[99]。

(四)電子支付帳戶駭客

日本郵政銀行於2020年9月16日表示，2020年共有109起利用相關電子支付系統服務的安全漏洞盜竊客戶帳戶資金之案件，盜竊金額已累計達1,811萬日元，涉及的電子支付服務系統共有七個，包括 Docomo、Merpay 以及 Line Pay 等知名電子支付，其中以Docomo電子支付帳戶為最大宗，佔總損失高達60%。日本郵政銀行和 Docomo 之所以遭受上述巨大損失，主要是因為其電子支付系統缺乏充足的資訊安全支持，因此特別容易受到攻擊。例如 Docomo的電子支付服務帳戶並未採用兩階段驗證系統，而當 Docomo 電子支付帳戶連結至日本郵政銀行後，日本郵政銀行也未採用兩階段驗證系統，因此衍生上述問題[100]。

第二項 洗錢與資恐

一、國際發展趨勢分析

[97] Security Boulevard, *QRL Jacking*, https://securityboulevard.com/2018/07/qrl-jacking/ (last visited Aprl. 14, 2021).

[98] Vincent Fong, *With Mobile Payments on the Rise, Creator of QR Codes Thinks It Needs a Security Revamp*, FinTech Singapore (Sept. 12, 2019), https://fintechnews.sg/33563/security/qr-payment-security-inventor-masahiro-hara/.

[99] *QR Codes Too Easily Misused by Criminals*, China Daily (March 2, 2017), http://www.chinadaily.com.cn/opinion/2017-03/02/content_28400890.htm.

[100] Fumiko Kuribayashi, *18.11 Million Yen Stolen from Japan Post Bank in E-pay Scam*, The Asahi Shimbun (Sept. 17, 2020), http://www.asahi.com/ajw/articles/13736152.

根據 EverCompliant 於 2018 年的研究報告顯示，2018 年全球約有 38.1%的洗錢行為會透過商業交易系統完成，涉案金額超過 2,000 億美金，且預計將以每年 8.4%的增幅繼續增加[101]，其中電子支付工具提供者亦為上述商業交易系統之一[102]。該報告亦指出當今科技與電子商務的蓬勃發展，將導致信用卡、電子錢包等電子支付工具大量被使用在洗錢活動[103]。

調查另顯示，大約 50%至 70%的線上非法交易（例如毒品、成人內容等）會利用商業交易系統與支付工具進行洗錢，以將金流匯至合法支付體系，此外就線上賭博案件而言，甚至有超過 90%的案件會運用前開管道以遂行其洗錢行為[104]。

二、電子支付工具洗錢案件的案例

FATF 指出，新型態支付工具涉及的洗錢或資恐犯罪案件，主要為以下三項洗錢類型：第三方資金、濫用非面對面交易特性、以及支付業者或其員工間的共謀[105]。

(一)第三方資金

若干新型態支付工具可以進行點對點（peer-to-peer）的支付，因此在同謀的犯罪行為人之間、或是被害人與犯罪行為人之間，可以透過該點對點支付的功能以移轉資金。對此 FATF 具體指出以下涉及電子支付工具的案例，其犯罪事實均涉及第三方因詐騙而移轉金錢[106]。

1. 某犯罪行為人首先竊盜他人之物或收受竊盜之贓物，再於轉賣時透過線上付款系統辦理其與贓物買受人間之金流移轉。
2. 某法國人提供自身的線上支付系統帳戶與銀行帳戶予一犯罪公司作為人頭帳戶，之後該犯罪公司即以該帳戶作為收

[101] *Supra* note 12.
[102] *Id.* at 1.
[103] *Id.* at 6.
[104] Tookitaki, https://www.tookitaki.ai/compliance_hub/what-is-credit-card-money-laundering-and-its-schemes/ (last visited Mar. 14, 2021).
[105] *Supra* note 14.
[106] *Id.* at 40.

受犯罪金流之節點，再以該帳戶將犯罪金額匯至該公司位於法國之帳戶。

3. 某犯罪行為人先透過木馬程式與網路釣魚取得被害人的銀行帳戶，並將該帳戶轉交予代理人(financial agent)。代理人自該銀行帳戶取出現金後，利用取出之現金，以該現金於不同之地購入數張線上支付系統之現金券，再將現金券之 pin 碼等資訊透過電子郵件傳送給上述犯罪行為人，完成資金之移轉。
4. 某犯罪行為人為販售違禁品例如毒品等，首先運用假名至郵政系統寄件，再藉由線上付款系統收款，並利用網路聊天室至論壇確認訂單。該犯罪行為人之收付款甚至會透過朋友與其伴侶之帳戶為之，以混淆視聽。
5. 某犯罪行為人對被害人施以詐術，使被害人誤以為他的伴侶出車禍需要支付醫藥費，進而誘使被害人運用電子支付工具付款與移轉金流。
6. 某犯罪行為人利用簡訊對被害人施以詐術，使被害人誤以為其中獎而需繳納稅金，進而運用電子支付工具支付被害款項。
7. 某犯罪行為人竊得第三人的信用卡資料，以此購入電話預付卡，隨後再將該預付卡出賣予他人，並藉由點對點的支付服務取得交易價款。

(二)濫用非面對面交易特性

由於新型態支付工具往往無須透過面對面交易即可完成支付，因此也衍生了許多利用身分竊盜、駭客或釣魚等犯罪手法遂行的財產犯罪，犯罪集團亦會利用他人帳戶或假帳戶做為犯罪的金流節點，當現金匯至前開帳戶時，犯罪集團隨即將現金提領而出或是以之購入貨品，進而不利犯罪偵查金流。FATF 就此指出以下具體案例[107]。

1. 某犯罪行為人偽造了 384 個位於外國的銀行帳戶，並以此等帳戶申請設立 568 個線上拍賣網站的帳戶進行洗錢，該網站係使用線上點對點的支付系統。犯罪行為人基此帳戶對外謊

[107] *Id.* at 43.

稱出售大學專用教課書，總共獲益美金 530 萬元，進而將該帳戶內的獲利現金轉至數個位於新加坡的銀行帳戶。

2. 某犯罪行為人盜走他人之銀行及身分資訊後，以之申請線上支付服務帳號，先將被害人帳戶中之款項移轉至其申設的上開線上支付帳戶，旋即又將款項利用線上支付系統轉出。其為躲避偵查機關的追查，甚至於兩個月內將轉出的線上支付帳戶所連結的銀行帳戶更換有四次之多。

(三)支付業者或其員工間的共謀

此種洗錢架構下的主體，牽涉支付服務提供者或其員工，其多半被犯罪集團所掌控，並且基於故意或過失對犯罪集團的洗錢或資恐行為提供幫助[108]。

1. 犯罪行為人即透過經營一未經許可的匯兌機構，以幫助違法線上賭博公司辦理金錢流動。
2. 某美國電子支付工具(digital currency)業者未對客戶進行任何身分驗證，即使明知客戶為犯罪機構亦然。該業者甚至指派沒有任何經驗的員工負責設計與管理整個系統。

第三項 小結

上述彙整顯示，國際上較常見的電子支付工具相關犯罪主要為「詐騙」與「洗錢及資恐」，此主要係因電子支付工具具有「匿名性」與「跨境移轉資金」之兩大特性，一方面使犯罪行為人得以更便利地擴大其犯罪對象的範圍，且因無需面對面交易進而提升犯罪成功率；另方面也提升金流移轉的效率，使犯罪流程更加順暢與迅速。

[108] *Id.* at 45.

第三節　我國電子支付工具濫用於犯罪之分析

第一項 我國法院實務之主要電子支付工具犯罪類型

相較國際上偶有的電子支付工具所涉犯罪分析報告，我國就此面向的相關數據相對缺乏。為分析電子支付工具於我國使用於刑事犯罪的具體情形，本研究規劃透過蒐集與彙整涉及電子支付工具的刑事判決作為實證資料，用以具體分析電子支付工具於我國使用於刑事犯罪的具體態樣與密集程度。

具體而言，本研究以司法院之裁判書查詢系統為基礎，使用電子支付工具與主要電子支付業者等關鍵字，包括:「電子支付」、「第三方支付」、「行動收單」、「mPOS」、「行動電子票證」、「行動信用卡」、「行動金融卡」、「橘子支付」、「國際連」、「智付寶」、「ezpay」、「街口支付」、「歐付寶」、「紅陽」、「綠界」、「藍新」、「支付寶」、「悠遊付」、「Gash」、「台灣 pay」、「Linepay」、「androidpay」、「samsungpay」、「applepay」以及「pay」，蒐集民國 103 年至 110 年 07 月 29 日間之地方法院刑事判決，初步共蒐得 2,070 筆結果。

以此初步搜尋結果為基礎，本研究進一步進行二階段之人工篩選，首先判斷系爭案件與前開關鍵字之關聯，並汰除顯無相關者，例如部分案件中出現被告將自有之社交帳戶名稱取為支付寶、部分判決法院引用電子支付機構管理條例惟個案中並未出現使用電子支付工具的情形等。第二階段本研究再進一步深入閱讀判決中所載之犯罪事實，對照判決中所附之各項供述證據及非供述證據，判斷電子支付工具於該犯罪中所扮演之角色，並汰除不符合本研究之條件者，例如部分案件僅被告於警詢或訊問筆錄中提及相關電子支付工具名稱，惟實際上於該案件中電子支付工具並未被實際使用，或者無法確定相關金流是否通過電子支付工具。經此二階段之篩選，最終獲得與電子支付工具相關的判決共 1,078 則。

經本研究進一步整理與分類後，初步觀察得出電子支付工具於我國主要使用於以下五種犯罪類型，分別為：

1. 利用電子支付工具遂行詐騙；
2. 網路賭博儲值；

3. 竊用他人信用卡或電子支付帳戶資訊消費；

4. 盜用他人資訊設定電子支付帳戶；

5. 其他。

本研究以下將根據前開分類，分別類型化個案的犯罪手法與電子支付工具的使用情形，並且挑選各類型犯罪中的指標性案件進行介紹，以具體化電子支付工具於各犯罪類型中所扮演之主要角色。本研究亦將陳報各類案件件數與特點的統計結果以供參考。

一、利用電子支付工具遂行詐騙

本種犯罪之手法多係犯罪集團利用人頭自願提供之資訊向電子支付工具業者申請設立帳戶，或犯罪行為人使用自有之帳戶，再對被害人施以詐術，使被害人透過電子支付工具交付款項，達到詐騙之目的。

以下圖 7 顯示此類犯罪的犯罪行為時點趨勢，其行為數至 2018 年為止均呈現逐年成長之態勢。補充者為，為如實反映時間及行為趨勢，本研究所採取的行為認定基礎會以自然意義下之一行為作為劃分，故可能因單一案件中有複數行為而存在複數時點，導致總行為數與總案件數有所出入之現象。

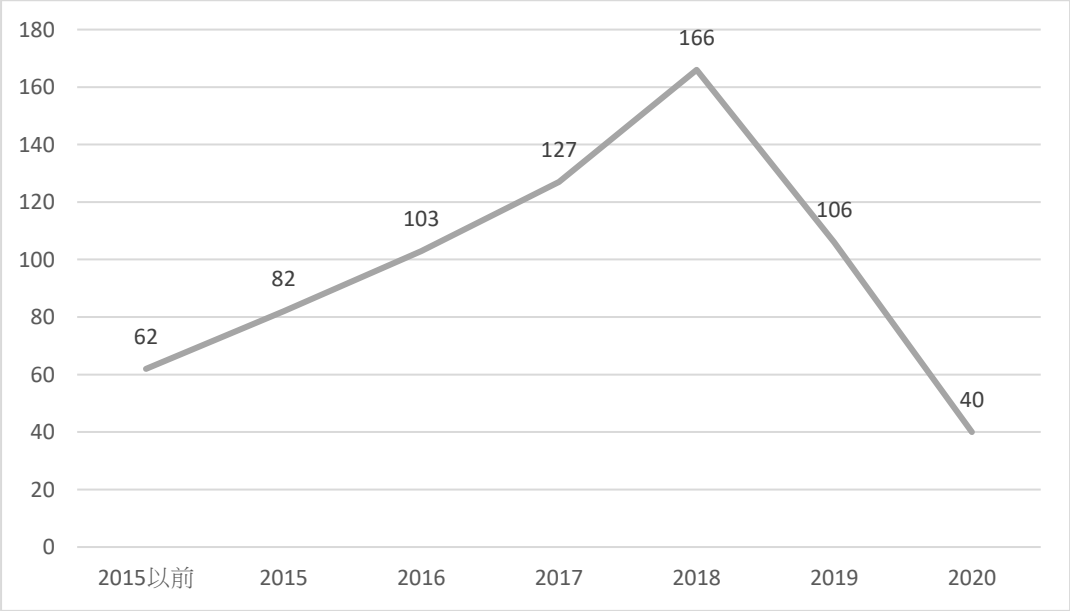


圖 7 利用電子支付工具遂行詐騙案件之犯罪行為時點分布

資料來源:研究團隊自製

自金流過程而言，此類犯罪之金流通常係經由銀行至電子支付業者，或者係由被害人流至超商經電子支付業者再到犯罪行為人指定之銀行帳戶，牽涉之主體包含被害人、銀行或超商、以及電子支付業者，電子支付工具於此類犯罪中主要係扮演犯罪工具之角色。

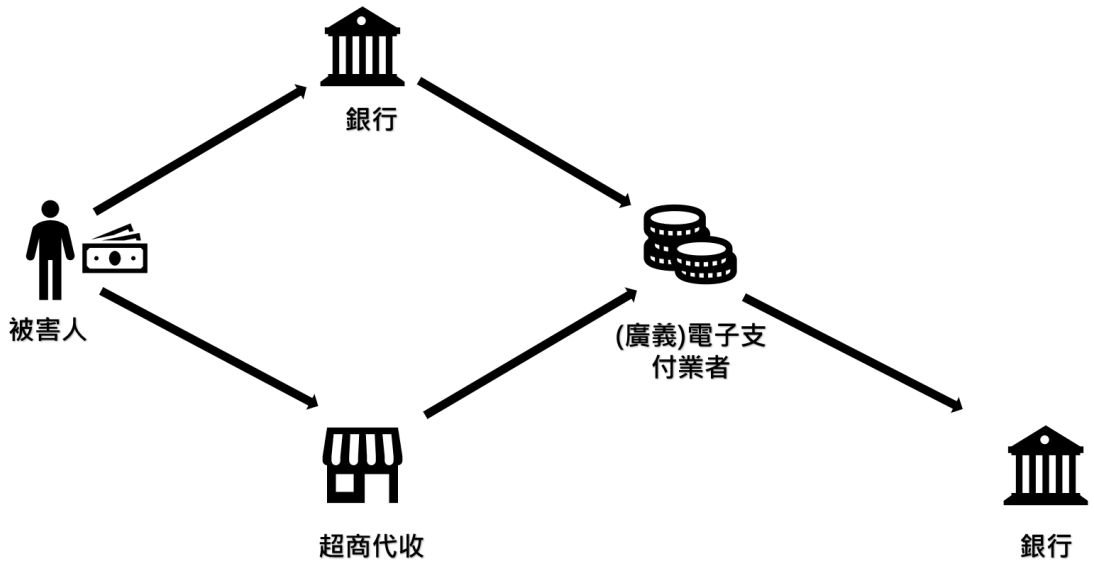


圖 8 利用電子支付工具遂行詐騙金流圖

資料來源:研究團隊自製

值得注意者為，於此類案件中，屬因出借帳戶或個人資訊予他人做為人頭帳戶而遭認定為幫助犯者總數為 311 件，佔此類案件總數約 48.5%，比例甚高。由此可知，此類案件在偵查實務上並不容易追溯至最終之正犯，導致經常僅得以幫助犯之方式起訴與定罪提供人頭帳戶之人。此種人頭帳戶常係由被告以有償或無償之方式提供自身持有之金融機構帳戶、電信門號或身分資訊予犯罪行為人，犯罪行為人再以前開資訊向電子支付業者申請設立人頭帳戶，並以該帳戶遂行後續詐騙款項之收款行為。

另外補充者為，本研究於判決中亦觀察到相當比例之遊戲點數詐騙之案件，犯罪手法大致有二：

(一)犯罪行為人於寶物交易網上向不知情之遊戲點數賣家表示欲承購遊戲點數，賣家因此提供其電子支付帳戶之繳款資訊。隨後犯罪行為人對被害人施以詐術，使被害人陷於錯誤繳款至前開賣家提供的電子支付帳戶。遊戲點數賣家收款後，誤以為繳款者為行為人，故轉讓其遊戲點數予犯罪行為人，犯罪行為人最終得以免費取得遊戲點數。圖示如下：

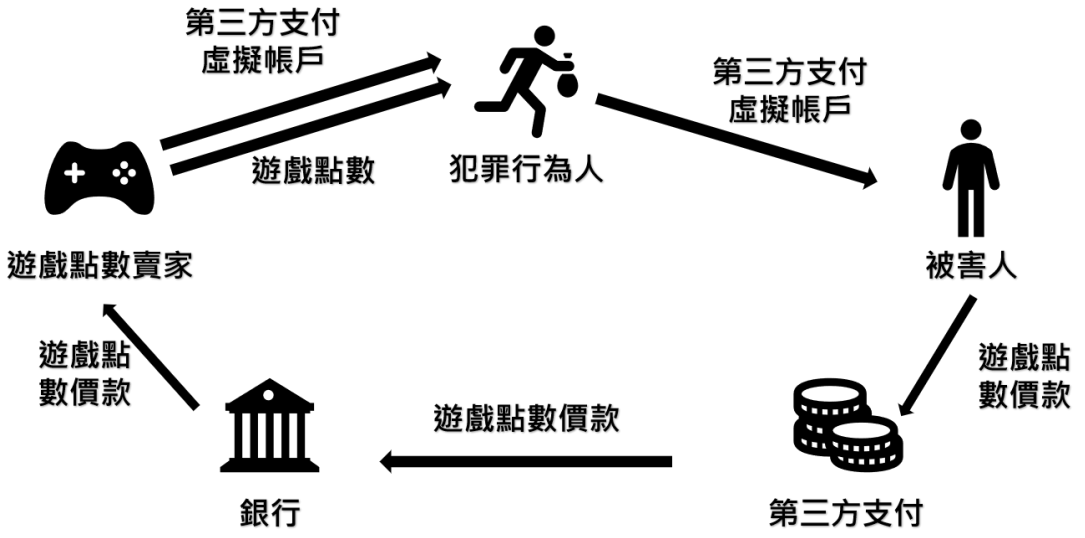


圖 9 遊戲點數三角詐欺示意圖

資料來源:研究團隊自製

(二)犯罪行為人對被害人施以詐術，使被害人購入遊戲點數並交付予犯罪行為人，其中被害人購入遊戲點數係使用電子支付工具做為其付款工具。

需特別說明者為，因遊戲點數本身並非本研究定義下之電子支付業者，故本研究於判決實證中僅統計遊戲點數詐騙中涉及電子支付工具之案件。而根據偵查機關內部統計之不起訴處分數據，與遊戲點數相關之詐騙案件不起訴處分占總詐欺案件不起訴處分之之比

例，由民國 108 年之 0.97%上升至 109 年之 7.69%，110 年 8 月以前則已達到 13.95%，節節攀升，反映遊戲點數詐騙之嚴重性逐年上升，惟因遊戲點數詐騙不在本研究之研究範圍內，僅能留待後續進一步研究。

以下謹以五則具體刑事判決所涉之犯罪事實說明此類犯罪的具體案件情形以及電子支付工具於此類犯罪中扮演的角色。

(一)台中地方法院 107 年度訴字第 821 號刑事判決

詐欺機房集團及外務車手集團成員，意圖為自己不法之所有，基於三人以上詐欺取財之犯意聯絡，由其成員向俗稱「車商」之人頭帳戶收購集團成員，購買大陸地區人頭帳戶資料、U 盾、銀行卡等物，並撥打電話向大陸地區之被害人行騙，使被害人受騙後，將人民幣款項匯入其成員提供之大陸地區人頭帳戶內，再以網路轉匯方式，將所掌控之大陸地區人頭帳戶內之人民幣贓款轉匯至大陸地區之電子支付平台，例如支付寶或其他博奕平臺。上開大陸地區電子支付平台之業者扣除所抽取之手續費後，再以不詳方式將其餘人民幣贓款匯兌為新臺幣，由外務車手集團成員予以提領現金後，轉交給第三人。本件犯罪金額總計 201,946 元。

(二)台北地方法院 107 年審簡字第 643 刑事判決

被告將其彰化銀行存摺、提款卡、密碼以及身分證交付不知名之詐騙集團人士，詐騙集團取得前開資料後，即向歐付寶電子支付股份有限公司申請設立一虛擬帳戶，再以電話佯稱為超商主管，對超商店員謊稱客人使用網路訂購商品時輸入資料錯誤，要求店員協助辦理取消訂購並依指示操作 ATM，致使店員陷於錯誤，於超商內以 ATM 方式將 2 萬元匯入前開歐付寶公司之虛擬帳戶內，詐騙集團最後將該虛擬帳戶內之款項提領一空。本件犯罪金額總計 59,985 元。

(三)桃園地方法院 105 年度簡字第 316 號刑事判決

被告於網路上對被害人佯稱自己為女性，並陸續以生活上需要花費、積欠他人債務、住院急診費用、遭人搶劫經濟拮据、遭檢警逮捕需要保釋金、需要繳納刑事罰金、需要前往與被害人會面之交通費用、友人出事急需借款、遭他人挾持需要贖款、規劃財務需要、

辦電話門號換現金等理由，使被害人至便利商店透過歐付寶超商代收服務購買網路遊戲點數交予被告，使其得以該遊戲分數、點數向網路遊戲幣商兌換現金花用。本件犯罪金額總計 47,625 元。

(四)新北地方法院 108 年金訴字第 39 號刑事判決

被告意圖為自己不法之所有，基於網際網路對公眾詐欺取財之故意，利用臉書對公眾刊登、或藉由私訊回覆之方式，表示其有意販售遊戲點數或演唱會門票，被害人因此陷於錯誤而向被告承購遊戲點數或演唱會門票；被告並以人頭作為驗證會員向橘子支付申請會員帳號並指示被害人將購入款項匯至對應其橘子支付會員帳號之銀行虛擬帳號內，或持超商繳費代碼至超商繳費後轉存入被告之銀行虛擬帳號內。本件犯罪金額總計 26,400 元。

本件後經檢察官上訴至高等法院，並作成臺灣高等法院 108 年上訴字第 4078 號刑事判決。臺灣高等法院維持原審之認事用法，認為被告同一詐財行為係犯刑法第 339 條之 4 第 1 項第 3 款之以網際網路對公眾散布而犯詐欺取財罪以及洗錢防制法第 14 條第 1 項之一般洗錢罪，故從一重以網際網路對公眾散布而犯詐欺取財罪處斷。

(五)屏東地方法院 109 年度訴字第 701 號刑事判決

被告於經由通訊軟體臉書私訊被害人，佯稱其有販賣線上遊戲天堂 M 之序云云，被告因而陷於錯誤，依其指示使用行動電話以網路轉帳方式，匯款至由第三方支付平台隨機產生之虛擬帳號，以支付被告向第三人購買 GASH 遊戲點數 1,680 點之價金，第三人因而誤認被告已支付遊戲點數價金，遂給付 GASH 遊戲點數 1,680 點予被告。被告於被害人匯款後，隨即封鎖被害人。

二、網路賭博儲值

本種犯罪類型大致上係由犯罪人經營線上簽賭平台，並利用電子支付或第三方支付業者連接指定之銀行帳戶，使賭客利用超商列印代碼繳款或匯款等方式支付款項予被告。以下圖 10 顯示此類犯罪的犯罪行為時點趨勢，目前初步觀察大體上集中於 2016 年。

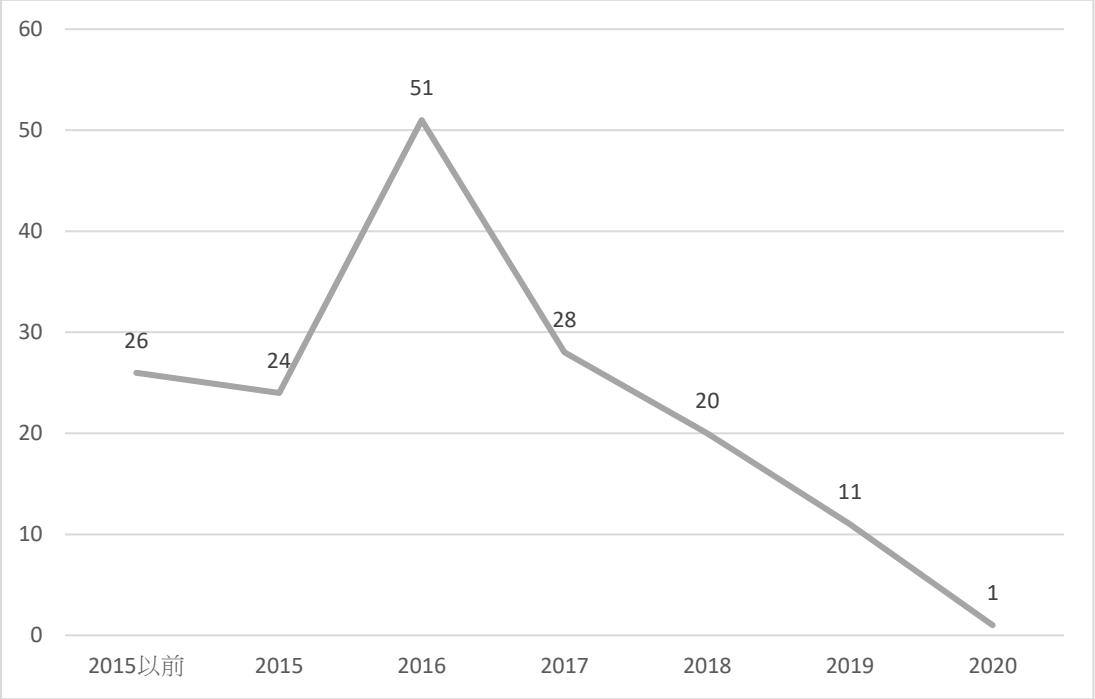


圖 10 網路賭博儲值案件之犯罪行為時點分布

資料來源:研究團隊自製

以金流而言，此類案件之金流大體上係由賭客流至超商、再經電子支付業者匯至被告指定之銀行帳戶。故本種犯罪所涉之主體包含賭客、被告、銀行、超商及電子支付業者，而電子支付工具於此種案件中同樣係扮演犯罪工具之角色。

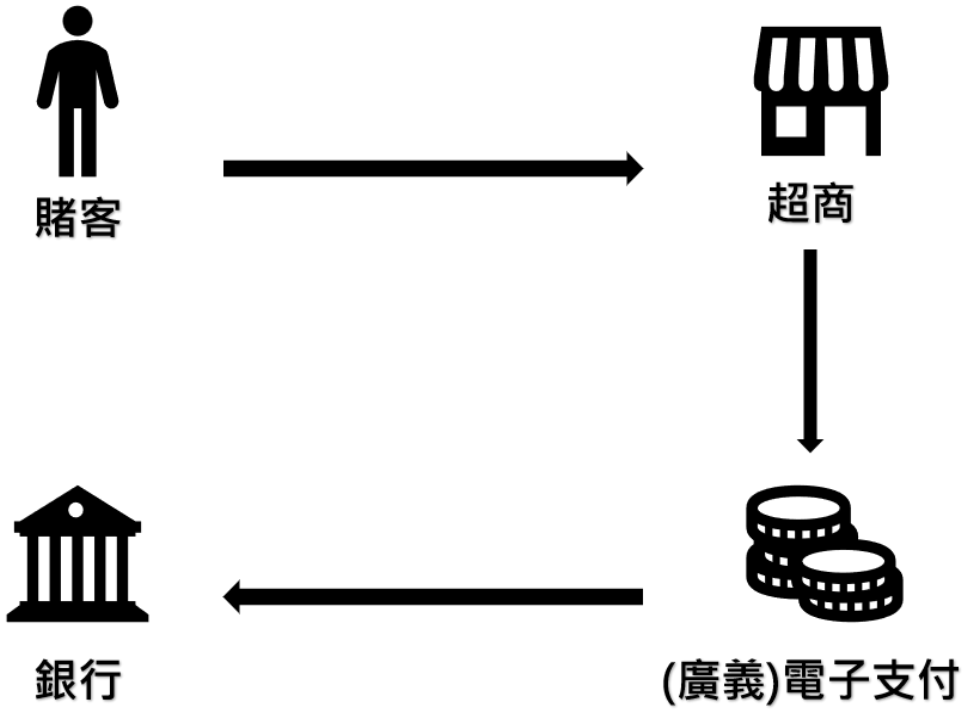


圖 11 賭博案件金流圖

資料來源:研究團隊自製

以下以三則具體刑事判決所涉之犯罪事實說明此類犯罪的具體案件情形以及電子支付工具於此類犯罪中扮演的角色。

(一)台北地方法院 106 年簡字第 982 刑事判決

被告基於賭博、意圖營利供給賭博場所及意圖營利聚眾賭博之犯意，以電腦設備登入網際網路，經營可供不特定人線上賭博之網站，並向歐付寶電子支付股份有限公司申請設立「小胖商城」會員資格，委託歐付寶公司透過全家便利商店及統一便利超商之各地分店付款系統，收取各地賭客購買歐付寶公司點數儲值所繳納之賭資，最終均轉往被告設於中信商銀的帳戶。本件犯罪金額總計 145,943 元。

(二)新北地方法院 108 年簡字第 3455 號刑事判決

被告意圖營利，基於供給賭博場所及聚眾賭博之犯意，向歐付寶電子支付股份有限公司申請會員作為收款之帳戶以經營賭博遊戲。賭客直接向被告或透過下線代理商購買進入遊戲的房卡，房卡費用

與賭資均透過歐付寶支付，被告則透過歐付寶帳號收受之。本件犯罪金額總計 100,000 元。

(三)臺中地方法院 106 年易字第 3102 號刑事判決

被告基於幫助賭博的不確定故意，將其國泰世華銀行帳戶（本案帳戶）之存摺、金融卡及國民身分證影本等資料，交付予真實姓名年籍不詳之成年男子使用並收取報酬。經營賭博網站之犯罪集團成員於取得本案帳戶資料及國民身分證影本後，以被告之名義，與不知情之藍新公司負責人簽訂「非信用卡收付款機制服務租用合約書」。本案賭客再以儲值方式係於便利商店儲值賭金，該儲值金額先匯入臺灣支付公司向第一商業銀行申設之帳戶後，再由臺灣支付公司將款項匯入本案帳戶。本件判決並未詳細記載犯罪金額，推估至少有 293,000 元。

三、竊用他人資訊消費

此種犯罪主要以信用卡或電子支付工具作為犯罪客體或工具。犯罪事實多係被告竊走被害人之信用卡、金融卡或電子支付帳戶之資訊後，持之於線上透過線上商家提供的電子支付工具金流服務進行消費。故此種犯罪下，電子支付工具主要係扮演犯罪之金流中介者，而所涉及之主體包含發卡銀行、電子支付服務提供者、消費商家、犯罪行為人及被害人。

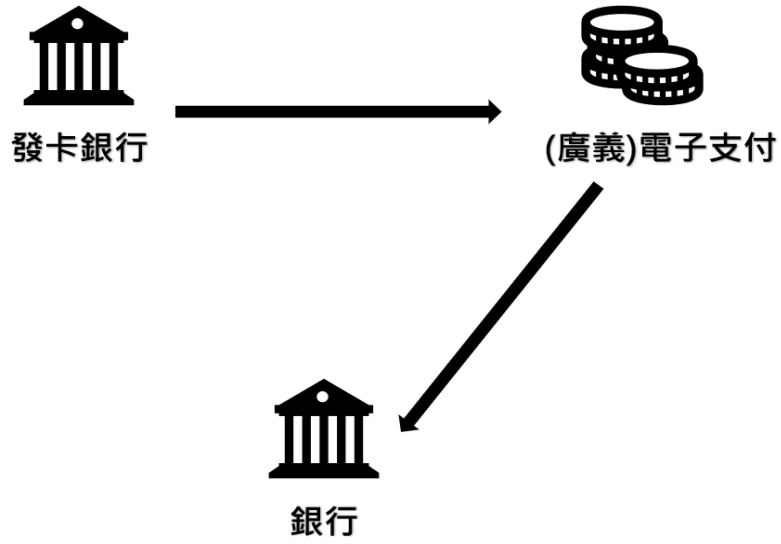


圖 12 竊用他人資訊消費案件金流圖

資料來源:研究團隊自製

於此種案件類型中，本研究團隊亦觀察到相當比例之遊戲點數犯罪。於此種案件中，多係犯罪行為人盜刷他人之卡式工具用以購入遊戲點數，並且遊戲點數之出賣人多係使用第三方支付做為收款工具。

以下圖 13 顯示此類犯罪的犯罪行為時點趨勢，目前初步觀察大體上集中於 2016 年。

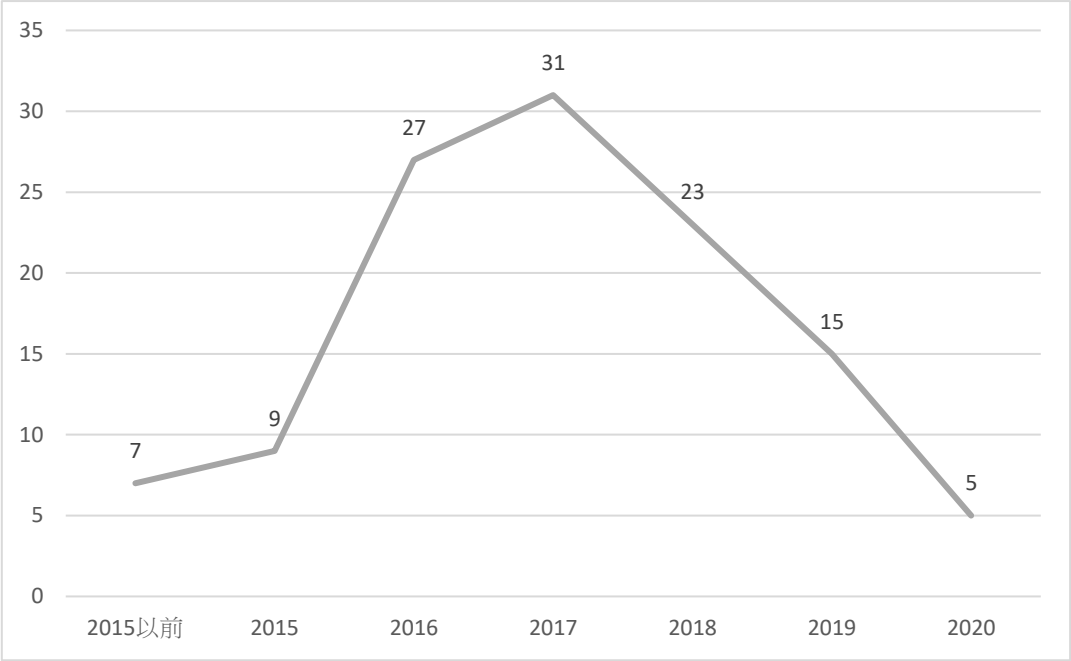


圖 13　竊用他人資訊消費之犯罪行為時間點分布

資料來源:研究團隊自製

以下以三則具體刑事判決所涉之犯罪事實說明此類犯罪的具體案件情形以及電子支付工具於此類犯罪中扮演的角色。

(一)桃園地方法院 107 年桃簡字 883 號刑事判決

被告拾獲其胞弟所持用之彰化商業銀行股份有限公司信用卡 1 張（下稱上開信用卡）登入網銀國際股份有限公司（下稱網銀公司）後，點選購買價值新臺幣（下同）1,000 元之遊 e 卡虛擬點數，並於消費資訊欄位上填載上開信用卡資訊而予以盜刷，使網銀公司及歐付寶第三方支付股份有限公司（下稱歐付寶公司）均陷於錯誤，誤認為係被害人本人持卡消費，網銀公司遂提供上開遊 e 卡虛擬點數予洪國恩，歐付寶公司則亦同意先行撥款予網銀公司。本件犯罪金額總計 1,000 元。

(二)基隆地方法院 108 年度基簡字第 1474 號

被告在其叔叔住處房間打掃時，發現地上有其叔叔所申辦彰化商業銀行之信用卡，先抄寫該卡正面卡號及背面授權碼，再伺機將該卡放回包包內。嗣被告在其姪子之房間內，以其姪子所有之電腦

上網連結使用歐付寶第三方支付服務之商家進行消費。本件犯罪金額總計 3,500 元。

(三)新北地方法院 109 年審易字第 2115 號判決

被告先前竊走被害人之信用卡資訊，嗣後並輸入被害人上開信用卡之持卡人姓名、卡號、有效年月、授權碼等資料，而進行線上交易。致商家及發卡銀行陷於錯誤，以為係被害人使用上開信用卡消費，陳奕家因此詐得遊戲點數價款之財產上利益。其中，該商家所使用之金流即歐付寶之第三方服務。本件犯罪金額總計 900 元。

四、盜用他人資訊設定電子支付帳戶

此種犯罪中，犯罪行為人首先取得被害人之個人資訊，包括身分資訊、銀行帳戶資訊、信用卡或電信門號等，嗣後以該資訊綁定特定電子支付帳戶，並據以進行消費或詐欺等行為。以下圖 14 顯示此類犯罪的犯罪行為時點趨勢，目前初步觀察大體上集中於 2016 至 2018 年。

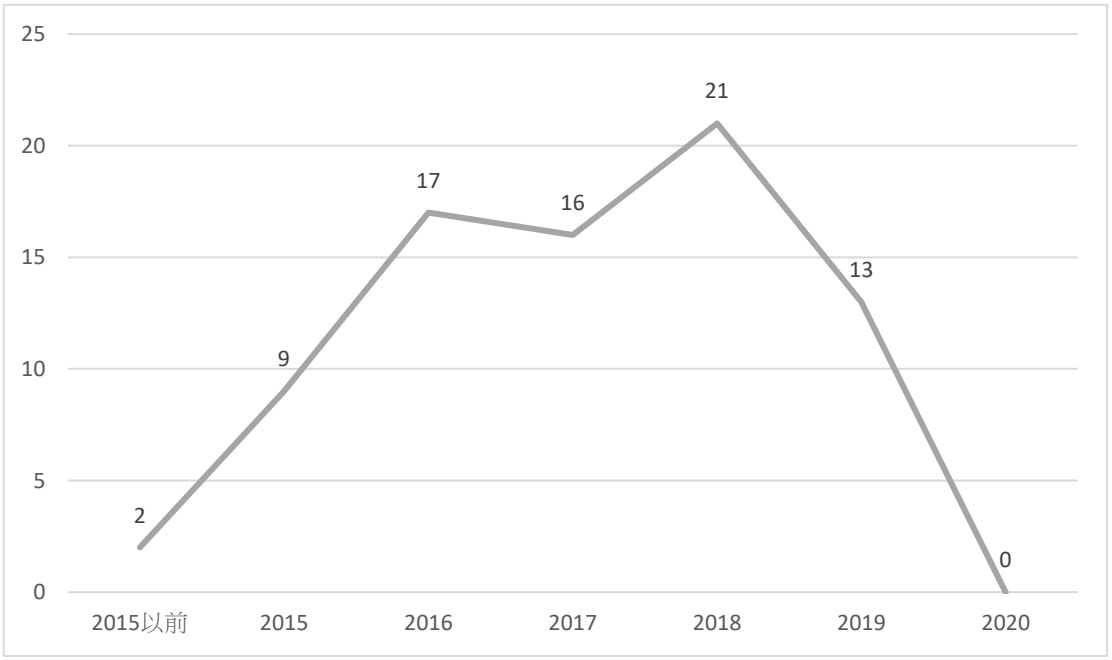


圖 14 盜用他人資訊設定電子支付帳戶之犯罪行為時間點分布

資料來源:研究團隊自製

此種犯罪之金流係由被害人之銀行帳戶流至電子支付機構，最終流至相關商家以滿足行為人之消費需求或流至詐欺行為人之帳戶以供提領。涉及之主體包含銀行、電子支付業者與商家，電子支付工具於此種案件中係用作犯罪工具。圖示如下：

圖 15 盜用他人資訊設定電子支付帳戶案件金流圖

圖片來源:研究團隊自製

以下以三則具體刑事判決所涉之犯罪事實說明此類犯罪的具體案件情形以及電子支付工具於此類犯罪中扮演的角色。

(一)台北地方法院 109 年審簡字第 642 號刑事判決

本件被告取得不知情之被害人之國民身分證資料及台新銀行之信用卡資料（包含信用卡卡號、有效期限等資料）後，未經被害人之同意即將該信用卡綁定「街口支付」應用程式並創設被告之街口支付帳戶，進而連續在台灣大車隊與三創之得宜科技數位股份有限公司所設之 APPLE 專櫃消費使用「街口支付」進行付款，款項來源即為被害人之信用卡。本件犯罪金額總計 64,960 元。

(二)臺中地方法院 106 年訴字第 2311 號刑事判決

被告以協助辦理貸款為幌子向另案被害人甲詐得姓名、身分證字號、出生年月日年等戶籍資料，進而以之向經營電子支付功能之歐付寶電子支付股份有限公司申請虛擬帳戶；並以向他案被害人乙騙取之門號為認證工具，成功註冊歐付寶公司會員帳號。

嗣後，被告在臉書社團佯稱出售二手智慧型手機，並以上開行動電話門號為連絡門號，適有本案被害人丙上網瀏覽訊息，乃陷於錯誤，依指示於統一超商，以歐付寶代碼繳費至歐付寶會員帳號。

本件犯罪金額總計 4,500 元。

(三)新北地方法院 107 年審訴字第 767 號刑事判決

本件被告基於職務之便取得三被害人之信用卡資訊，並以每個 2,500 元之代價購買兩門號。被告旋以前開門號向遠傳電信申請 FriDay 錢包之服務，並綁定所取得之被害人信用卡資訊進行消費。本件犯罪金額總計 69,722 元。

五、其他犯罪

除上述四種常見的犯罪類型外，本研究亦摘錄部份數量較少但具有一定代表性之犯罪類型供參考。此類犯罪事實多涉及大量的被害人與大量款項交付活動，具有遠距離款項支付之需求，而電子支付工具的特性或有助此類犯罪的規模擴大與成本降低。本研究摘要其具體類型如下。

第一種為違反銀行法第 125 條第一項之違法辦理國內外匯兌。於此種案例，行為人招攬有匯兌需求之相對人，透過指定日期方式決定匯率與所需匯入之新台幣金額。於相對人匯入指定之新台幣金額與手續費後，行為人再於指定地點將指定金額之人民幣匯入相對人指定之帳戶。此類犯罪多數會透過支付寶之服務遂行大陸地區之款項收付，金流具體而言分為台灣地區與境外地區，台灣地區部分主要係由相對人之匯款銀行流至犯罪行為人之收款銀行，至於境外地區部分則係由支付業者內部或當地匯款銀行及收款銀行辦理清算。故此種犯罪涉及之主體包含國內的匯款銀行與收款銀行、國外的電子支付業者、匯款銀行、收款銀行以及犯罪行為人。在此種犯罪結構下，電子支付工具主要係用作犯罪之工具。

第二種為洗錢罪。此類犯罪多會連結到詐欺犯罪中之人頭帳戶或資訊之提供者。具體而言，此種犯罪多係由犯罪行為人提供自身之銀行帳戶、電信門號或身分資料等訊息供犯罪行為人綁定電子支付工具，嗣後以該電子支付工具遂行其犯罪中之收款行為。至於具體之金流及涉案主體，於我國多與詐欺或賭博共同出現。在此種犯罪結構下，電子支付工具主要係被用作遂行犯罪之工具，但關於提

供人頭帳戶或相關個人資訊給他人遂行詐欺行為是否另構成洗錢罪（或幫助洗錢罪），或僅構成幫助詐欺，目前法院見解仍有歧異。

第三種為未經許可經營期貨顧問業。此類犯罪之行為人係向不特定多數人提供股市或期貨市場預測，並吸收其成為會員，會員則透過電子支付工具給付會費予行為人。其金流主要係由會員藉由線上刷卡、超商代碼、超商條碼、ATM 虛擬代碼、網路 ATM 等方式，將款項支付予電子支付業者，再由電子支付業者扣除一定比例之費用後將款項後匯至行為人指定之銀行帳戶。故本類犯罪涉及之主體包含會員、犯罪行為人、付款之超商或銀行、電子支付業者、收款之銀行，在此種犯罪結構下，電子支付工具主要係被用作犯罪之工具。

第四種為違法經營多層次傳銷。此類犯罪之犯罪手法主要係由行為人經營一家以拉下線為主之多層次傳銷公司，並透過匯款、信用卡或電子支付業者的收款服務等收取會員費。具體而言，欲加入會員之人通常持現金前往超商，透過電子支付業者與超商合作之支付服務，將金錢匯至行為人指定之銀行帳戶，金流係由欲加入會員之人流向超商，再由超商支付予電子支付業者，最後由電子支付業者扣除一定比例之費用後流至犯罪行為人指定之銀行帳戶。故此種犯罪所涉及之主體包含欲加入會員之人、超商、電子支付業者、銀行及犯罪行為人，電子支付工具主要係用作犯罪之工具。

以下分別以具體刑事判決所涉之犯罪事實，說明各類犯罪的具體案件情形以及電子支付工具於此類犯罪中扮演的角色。

(一)違反銀行法第 125 條第一項之辦理國內外匯兌：

1. 台北地方法院 108 年金訴字第 48 號判決

櫻桃公司之營運方式為先向藍新科技股份有限公司經營之藍新金流平台申請網路金流收款服務，再以該平台生成之虛擬帳戶連結前揭櫻桃公司帳戶或其他自然人提供之金融帳戶，從而對外辦理收付款。當任一會員有跨境匯兌需求時，得以會員身分向櫻桃公司提出訂單，於訂單中指定資金匯入國別、幣別、金額及收款之金融帳戶或電子支付工具帳戶等，並將等值之本國貨幣匯入

櫻桃公司指定之前揭金融帳戶。櫻桃公司於取得訂單資訊後，即將該訂單資訊公告給匯入國之會員觀覽，匯入國之會員全體任一人均得接受訂單而成為服務會員，並依訂單之指示金額，將資金以匯入國貨幣匯入訂單所指定之金融或收款機構。服務會員完成匯款後，櫻桃公司再將等值之匯出國貨幣，匯入服務會員於匯出國所指定之金融帳戶，櫻桃公司則收取1～2%不等之服務費，而以此方式完成需求會員及服務會員之匯兌要求，進而在我國經營與中國大陸、泰國及韓國間之匯兌業務。於105年10月1日起至107年8月6日止之期間內，櫻桃支付即以此方法非法辦理國內外匯兌業務，交易金額總計11億1,933萬7,928元。

2. 嘉義地方法院110年度金訴字第84號刑事判決

被告之友人將其等所欲匯往大陸地區金融帳戶人民幣換算為等額新臺幣後，匯款至被告所申辦之銀行帳戶或以交付現金方式予被告，被告再操作支付寶轉存特定金額之人民幣至指定之支付寶帳戶，或委託其在大陸地區之親友將特定金額之人民幣匯至指定之大陸地區金融帳戶。被告於上開期間違法辦理匯兌業務經手之金額合計達新臺幣（下同）4,656,390元

(二)洗錢罪

1. 士林地方法院110年度金簡字第11號刑事判決

被告明知任意提供金融帳戶供人使用，可能幫助他人遂行詐欺取財犯行及隱匿不法所得，竟仍基於幫助洗錢及幫助詐欺之不確定故意，將其申設之中國信託、合作金庫帳戶提供予某年籍不詳之人使用；取得該等帳戶資料之詐騙集團所屬成員，嗣後即利用上開帳戶進行金融驗證，而於向一卡通票證股份有限公司申請取得電子支付帳戶。而該詐騙集團某成員，遂撥打電話向被害人佯稱其先前在福澳背包客棧之訂單誤設定為12筆，需依銀行行員指示操作，始可解除扣款設定，致使被害人因而陷於錯誤，於同日依假冒星展銀行行員之人指示操作ATM自動櫃員機轉帳新臺幣4萬9,988元至上開虛擬帳戶，詐騙集團所屬

成員隨即於同日轉出他人帳戶完成犯罪。

2. 臺中地方法院 108 年度金訴字第 106 號刑事判決

「Google Maps」及被告以不正方法取得他人向金融機構申請開立之帳戶使用，經不詳之人透過金恆通公司、易沛公司等第三方支付匯入合計 2998 萬 8590 元。本案法院認定被告與「Google Maps」以不正方法取得他人向金融機構申請開立之帳戶而為收受、持有之財物，且無合理來源且與收入顯不相當之情形，係犯洗錢防制法第 15 條第 1 項第 2 款之特殊洗錢罪。

(三)未經許可私自經營期貨顧問事業：台中地方法院 108 年金訴字第 121 號刑事判決

本件被告未經主管機關許可，私自利用通訊軟體成立付費群組，此外並於臉書上成立社團，用以對其會員提供個別股票或期貨未來趨勢之預測服務，或不定期舉辦座談會以招攬會員。其會費每季約 30,000 至 39,990，會員係透過歐付寶、綠界科技及智付通等支付服務，定期交付會費予被告。本件犯罪金額總計 14,607,160 元。

本件後經提起非常上訴後，作成最高法院 110 台非字第 63 號判決。最高法院大致維持原審之判決，僅就罰金易服勞役部分進行糾正。

(四)違反多層次傳銷管理辦法：臺中地方法院 108 年度金訴字第 7 號刑事判決

被告基於非法多層次傳銷之犯意，向綠界科技股份有限公司申請入會後，自民國 107 年 1 月間某日起，在網路上成立「GWD 黃金世界交易平臺」，透過社群網站或通訊軟體公開招攬不特定民眾投資金塊，且現有會員可藉由招攬新進會員、發展下線賺取推薦獎金。被害人先申辦帳號成為正式會員後，再為購買金塊而轉帳或匯款至被告於綠界公司開設之虛擬帳戶，綠界公司扣除手續費後，撥入游翔皓於綠界公司之會員帳戶合計金額新臺幣 29,193,810 元。

第二項 國內電子支付工具涉及犯罪之統計結果

於本研究所蒐得之地方法院刑事判決中，各類型犯罪的數量分布如以下圖 16 所示。補充說明者為，部分案件中涉及複數案件類型，

故此處所得之數據總和高於本研究蒐集之案件數，合先敘明。

相關犯罪類型中，利用電子支付工具遂行詐騙的案件所占比例最高，於本研究蒐集之判決中所記載所佔 640 件，約 53.9%。其餘犯罪的數量分布依序為：網路賭博儲值案件共 112 件（約 9.4%）、竊取他人信用卡或電子支付帳戶資訊消費共 114 件（約 9.5%）、盜用他人資訊設定電子支付帳戶共 72 件（約 6%）、其他共 250 件（約 21.2%）。

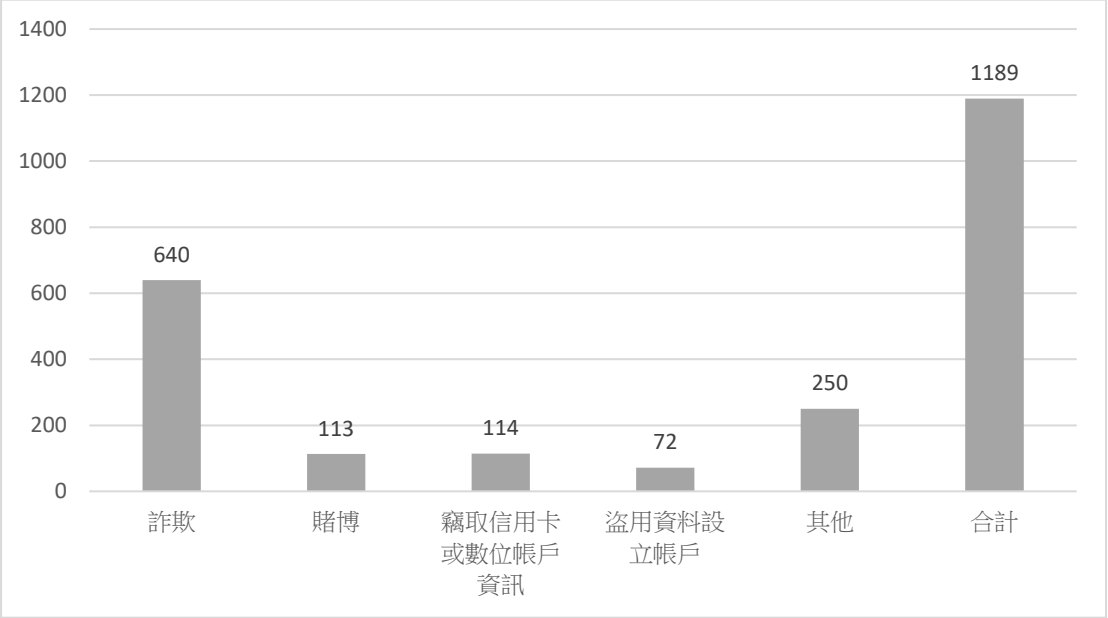


圖 16 電子支付工具涉及犯罪案件類型分布

資料來源:研究團隊自製

此外，主要電子支付工具被使用於犯罪的次數如以下圖 17 顯示，補充說明者為，由於單一案件可能涉及數種電子支付工具，故此處所得之數據總和高於本研究蒐集之案件數。由此圖可知，主要電子支付工具當中，較常被使用於犯罪之電子支付業者分別為綠界科技 235 件，歐付寶 214 件，藍新科技 172 件，支付寶 158 件與紅陽 54 件。此類業者中，綠界、紅陽、藍新屬於第三方支付，歐付寶與支付寶則屬於狹義之電子支付機構。

此外支付寶涉及的犯罪又可區分為兩種型態。一種為在我國境內使用的支付寶，其實質上係玉山銀行依照「與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法」第 4

條第 1 項第 1 款規定，經金管會核准與支付寶進行合作，協助提供客戶就跨境網路實質交易價金匯入或匯出之代理收付款項服務（即「兩岸支付通」產品），此本質上屬於狹義之電子支付；另一種則為於中國使用之支付寶，此相對並非我國管轄的電子支付工具。

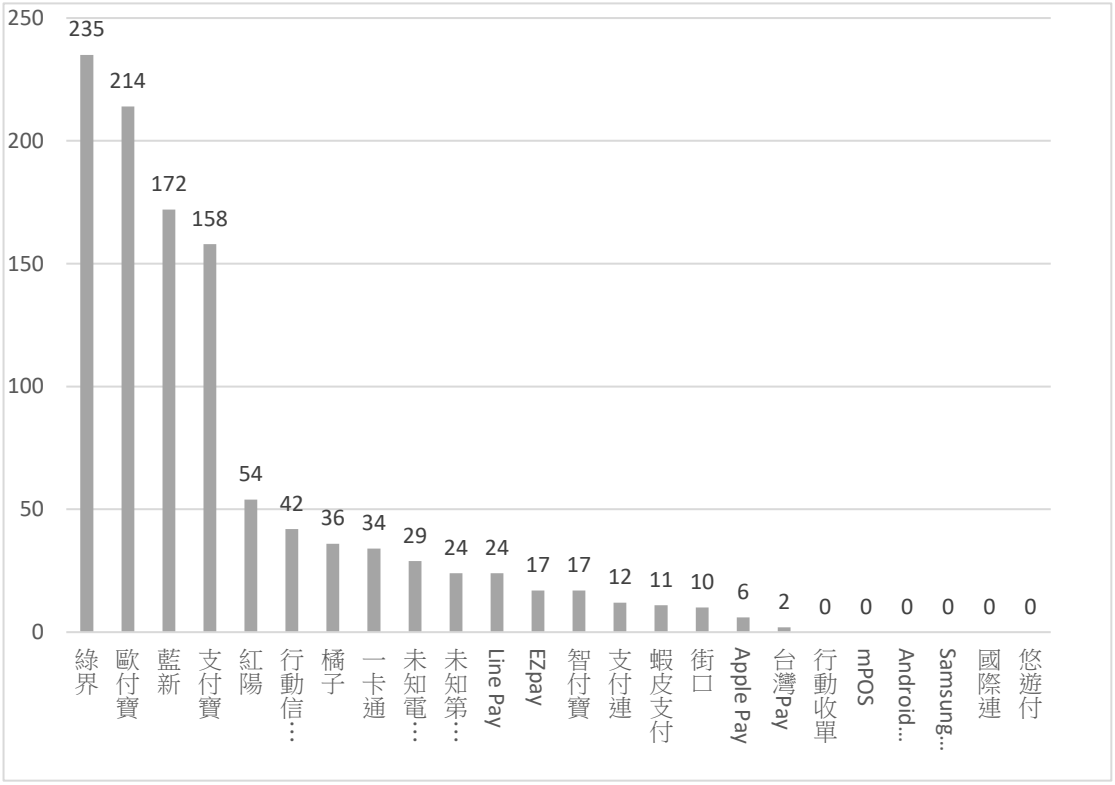


圖 17 主要電子支付工具涉及犯罪案件數分布

資料來源:研究團隊自製

另外，下圖 18 為本次研究所蒐集而得之判決中是否涉及跨境犯罪[109]之統計。所蒐得之案件中，共有 947 件屬於本土為主之案件，約佔判決總數之 87.8%，涉外案件比例則約為 12.2%。而於涉及跨境犯罪的案件中，涉及中國大陸之案件數量最多，共 124 件，其中多為詐騙集團與違法經營國內外匯兌之案件為主，而所使用之支付工具則多為支付寶，相關案例可參考前述之台中地方法院 107 年度訴字第 821 號刑事判決以及台北地方法院 108 年金訴字第 48 號判決。

[109] 本研究所稱之跨境犯罪，係觀察個案中「犯罪人所在地」、「被害人所在地」以及「其他關連地」中任何一者是否存在境外因素。

其餘涉外案件則為菲律賓四件，泰國、馬來西亞各兩件以及越南一件。

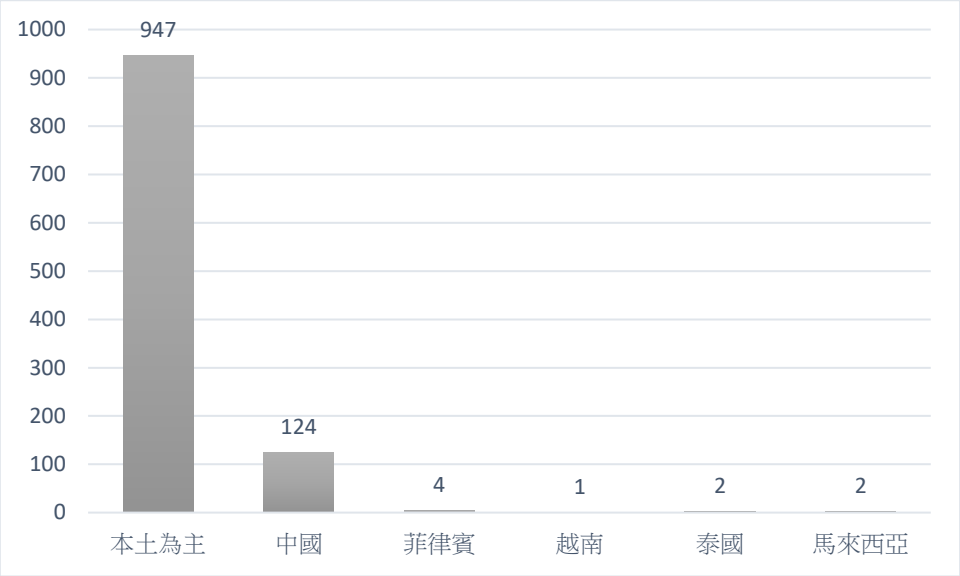


圖 18 案件所涉國家統計

資料來源:研究團隊自製

最後就犯罪金額而言[110]，圖 19 顯示各類電子支付工具涉及犯罪的犯罪金額統計。由此圖可知，不涉及洗錢的其他類型案件雖然數量較少，但涉案金額相當可觀，涉及超過 88 億元之犯罪金額；相對而言，案件數占比達 53.9%的利用電子支付工具遂行詐騙案件，犯罪總金額卻僅有約 5 億 3000 萬元，顯見詐騙案件平均每件之犯罪金額相對偏低。其餘依序則為賭博約 2 億 8000 萬元，洗錢相關案件約 7700 萬，盜用資訊設立帳戶約 800 萬與竊取信用卡或帳戶資訊消費約 300 萬。

[110] 本部分的統計將排除若干未記載或記載不明犯罪金額的判決。

圖 19 電子支付工具涉及犯罪的犯罪金額分布

資料來源:研究團隊自製

第三項 小結

透過上述司法判決實證研究，本研究發現，詐騙案件中之詐騙集團多以人頭申請行動支付帳戶，除詐騙類型中所列之 311 件詐欺幫助犯案件外，尚包含部分被認定為洗錢罪之案件[111]。此外考量犯罪行為人盜用他人身分或其他資訊創建電子支付帳戶的案件占比亦相當可觀，足見當前電子支付帳戶的設立有虛偽資訊充斥之風險，且似有過度浮濫之傾向。前開結果將導致追查相關財產犯罪之金流相對困難，並且因為電子支付帳戶之申設成本較低，亦可能使電子支付工具對犯罪產生相當程度之吸引力。

此外，本研究亦觀察到大量的第三方支付服務被運用於犯罪。搭配前開人頭帳戶的大量創建，此將導致相關金流追查上出現許多真空地帶。如上述，我國目前共有 13,113 家第三方支付業者登記在案，但此前第三方支付業者的洗錢防制監管相對較為混亂，因此對於交易雙方之身分資訊查核與留存均有不足，金流追查容易出現斷點，使得第三方支付吸引相關犯罪的大量使用。

[111] 此種提供帳戶資料供他人犯罪之案件究應論以洗錢罪或詐欺幫助犯，我國司法見解目前尚不統一，導致部分案件最終係以洗錢定罪。

除詐騙案件外，本研究亦發現，電子支付工具運用於其他犯罪例如非法匯兌、非法經營期貨顧問事業、非法多層次傳銷以及線上賭博等犯罪之犯罪金額，相較於其他犯罪為高，反映電子支付工具之「快速性」與「跨境性」特性，此類特性有助犯罪行為人快速且跨境地收取款項，進而有助犯罪行為人擴大其違法業務之範圍至不限於特定地區之人民參與。

補充者為，本研究亦認知到電子支付工具相關的犯罪手法日新月異，而判決作成時點與犯罪時點往往存在時間差，因此單憑司法判決實證研究所歸納之犯罪趨勢，未必能充分反映現行犯罪與偵辦現況，此為本研究方法不可避免的研究限制。

第三章　虛擬通貨新興犯罪背景成因及類型分析

第一節　犯罪背景

第一項 我國虛擬通貨市場概況

根據FATF指引之定義，虛擬通貨交易平台係指從事虛擬通貨與實體貨幣、其他虛擬通貨或貴金屬間之集中搓合交易為業，並賺取費用(手續費)之業者[112]。FATF 指引此處就虛擬通貨之用語為「虛擬資產」，惟意義與我國現行法規中所稱之虛擬通貨相同，均為應用密碼學及分散式帳本技術之物，以下行文仍以虛擬通貨稱之。

根據我國中央銀行所描述的虛擬通貨市場，目前市場規模相對傳統金融市場仍小，在市場深度不足且無適當的主管機關或價格管理機制(例如漲跌幅限制、熔斷機制等)的情況下，價格更易受大戶影響。近期國際間開始有機構法人投入比特幣市場，若其於短時間內大量進出市場，便可能左右價格走勢[113]。由於新冠肺炎疫情衝擊全球經濟，主要國家央行實施量化寬鬆政策，在各國資金寬鬆、低利率的大環境下，投資人可能將資金投入高風險資產，以求獲取較高報酬，另由於近期美元持續貶值，故以美元計價之比特幣更水漲船高[114]。

根據全球最大民間虛擬通貨交易資料庫 CoinGecko，每日 24 小時即時統計各國虛擬通貨交易平台之交易量，統計顯示我國虛擬通貨交易所之交易金額約占全體虛擬通貨交易所之 0.02%，市場規模尚小，目前對我國支付系統、金融穩定及中央銀行貨幣政策之執行，尚無明顯影響[115]；惟中央銀行仍舊表示將持續關注虛擬通貨之發展。

---

[112] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 109 (June. 2019), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

[113] 根據富達投資集團(Fidelity Investments)在對歐美 774 家機構投資者的調查中發現，截至 2020 年第 2 季，有 36%的機構投資者持有虛擬通貨。另根據美國銀行(Bank of America Merrill Lynch)於 2020 年 12 月進行之調查，在 217 個受訪的基金經理人中，有 15%表示其持有比特幣之多頭部位(long positions)。

[114] 中央銀行，〈比特幣價格大幅波動之說明〉，https://www.cbc.gov.tw/tw/cp-1170-128220-09e31-1.html?fbclid=IwAR1Qgs4Vwo1ud_8RZ355t7xnmo6fMiMlhbQ1ynLhnbv5jGuFl-YbcUUL0iw ，最後瀏覽日:2021 年 2 月 26 日。

[115] 中央銀行，〈比特幣價格大幅波動之說明〉，https://www.cbc.gov.tw/tw/cp-1170-128220-09e31-1.html?fbclid=IwAR1Qgs4Vwo1ud_8RZ355t7xnmo6fMiMlhbQ1ynLhnbv5jGuFl-YbcUUL0iw ，最後瀏覽日:2021 年 2 月 26 日。

我國現行較知名之虛擬通貨交易平台約有 6 間，交易標的包含多樣虛擬通貨間之交易、法幣與虛擬通貨間之交易及場外交易等，部分業者更進一步與金融業者合作，進行法幣帳戶信託託管。我國代表之虛擬通貨交易平台如：幣託(BitoPro)以及魚幣金科(Max)交易平台，我國虛擬通貨交易平台之整理比較如下圖 16[116]：

台灣主要虛擬通貨交易所整理						
名稱	BitoPro	MAX	ACE	BITGIN	BitAsset	BINANCE
成立時間	2017.12	2018.03	2018.11	2020.09	2017.12	2017.07
台幣出入金	有	有	有	有	有	無
法幣銀行信託	遠東銀行	遠東銀行	凱基銀行	有	無	無
業務類型	幣幣交易、法幣	幣幣交易、法幣	幣幣交易、法幣	幣幣交易、OTC	幣幣交易、法幣	幣幣交易、OTC
發行平台幣	BITO	MAX	ACEX	無	無	BNB
24小時交易量 (2021.03.09)	4.7億元	5.6億元	4,900萬元	–	620億元（全球）	7200億元（全球）

圖 20 台灣主要虛擬通貨交易平台整理表

第二項 虛擬通貨之經濟活動

評估虛擬通貨活動的重要性和趨勢是確定行為性質及適法性的重要前提，以下根據歐洲財務報導諮詢小組於 2020 年發布之「*Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective*」報告，總結現行虛擬通貨之主要經濟活動現況，以及虛擬通貨之經濟活動涉及不法之概況整理。

一、發行虛擬通貨（ICO 或其他初始代幣發行）

ICO 是指企業透過發行「以區塊鏈技術為基礎」之專屬虛擬代幣（Token），來向特定或不特定的公眾募集法定貨幣或是虛擬貨幣之募資行為，概念上類似於證券市場的首次公開發行股票(Initial Public Offerings，IPO)，只是發行標的由股票等有價證券轉換為代幣，而投資人取得的是使用權而非股權[117]。其他類型的初始發行例如證

[116] 研究團隊自製圖表。

[117] 鍾欣宜(2019)，〈首次代幣發行(ICO)監理趨勢初探〉，《國家發展研究院經濟研究》，第 19 期，頁 19。

券型代幣（STO，Security Token Offering，即「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，且具流通性及投資性質者[118]。相關虛擬通貨發行等經濟行為整理如下：

(一)首次ICO發行的項目發生於2013年，名稱為Mastercoin，此後，ICO 市場經歷了快速增長，至西元 2019 年第一季度末，總計募集約 247 億美元，完成了 5,000 多個 ICO 項目，發生於 50 多個國家或地區[119]。

(二)隨著區塊鏈初創公司的出現，ICO 作為某些業務部門的資金來源的重要性越來越明顯，ICO 超過了風險投資（VC）的融資。自 2017 年 1 月至 2018 年 2 月的 14 個月中，區塊鏈初創企業籌集了全球傳統風險投資近 13 億美元；相比之下，ICO 項目籌集了 45 億美元[120]。

(三)ICO 在 2018 年第三季達到最高峰，短短不到三個月，到第四季 ICO 的募資金額已從高峰滑落，持續下探。根據 2020 年 1 月報告顯示[121]，相對於 2017 年和 2018 年，2019 年通過 ICO 發行代幣的項目數量和募資額均顯著下降。

---

[118] 金融監督管理委員會於 2019 年 6 月 27 日發布新聞稿，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News，最後瀏覽日:2021 年 2 月 26 日。

[119] *Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective*, 2020 July, European Financial Reporting Advisory Group, p.35.

[120] *Id*.

[121] PwC, *6th Edition ICO/STO report- A Strategic Perspective.* PWC (Jan. 28, 2020), https://www.pwc.ch/en/publications/2020/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf.

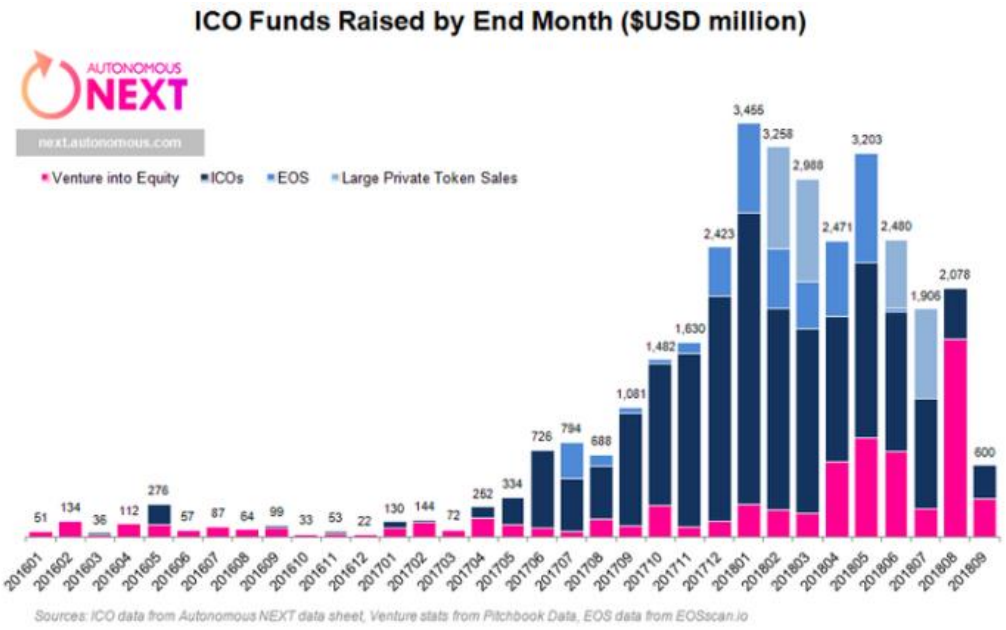


圖 21 2016 至 2018 ICO 募資金額

資料來源: The Ultimate List of ICO Pools in the Bear Market—Q4 2018[122]。

相較於 ICO 的規模急遽萎縮，STO 發行量於 2018 年及 2019 年有所增加，惟增加的趨勢並不穩定。STO 發行之標的包括發行代幣化之公司債券和部分金融機構和集團之會員點數計畫及相關系統，發行機構包含：奧地利政府（14 億美元）、中國銀行（28 億美元）、桑坦德銀行（2000 萬歐元），西班牙對外銀行（1.5 億歐元）、戴姆勒（1 億歐元）、法國興業銀行（1 億歐元）等[123]。

二、涉及虛擬通貨商業之業務

國際貨幣基金組織 2019 年 12 月特別指出，現行涉及虛擬通貨商業之業務主體為金融科技新創企業，也包含主要金融機構，例如富達投資均在積極開發虛擬通貨等虛擬資產之解決方案[124]。而虛擬通貨商業之業務，根據歐洲財務報導諮詢小組定義，包括下列業務[125]：

[122] *The Ultimate List of ICO Pools in the Bear Market—Q4 2018*, https://hackernoon.com/the-ultimate-list-of-ico-pools-in-the-bear-market-q4-2018-81ffc4df5a9b (last visited: Feb. 26, 2021).
[123] *Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective*, 2020 July, European Financial Reporting Advisory Group, p.35.
[124] Cristina Cuervo, Anastasiia Morozova, Nobuyasu Sugimoto, *Regulation of Crypto Assets*, IMF (Dec. 2019) https://www.imf.org/~/media/Files/Publications/FTN063/2019/English/FTNEA2019003.ashx.
[125] Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective, 2020 July, European

(一)持有虛擬通貨資產；

(二)接受虛擬通貨抵押品之貸款業務；

(三)使用虛擬通貨衍生性金融商品之交易、結算或清算業務；

(四)投資其他虛擬通貨，依照 2019 年 3 月美國律師協會報告指出，專注於虛擬通貨對沖基金和風險基金之規模迅速增長，截至 2018 年 12 月，共計有超過 780 個虛擬通貨基金管理超過價值 150 億美元的資產[126]；

(五)向虛擬通貨商業業者提供貸款；

(六)提供法定資產兌換為虛擬通貨的服務，或為虛擬通貨兌換為其他虛擬通貨之服務。ESMA Advice 於 2019 年 1 月統計，全球有超過 200 個大型虛擬通貨交易平台在歐盟以外的地區，包括在美國及亞洲。

由上可知，虛擬通貨業務包含之金融業務範圍甚廣，該業務類別對於金融市場之影響不言而喻。又「防制洗錢金融行動工作組織」（Financial Action Task Force, FATF）於西元（下同）2019 年修正發布建議（The FATF Recommendations，下稱 FATF 建議），FATF 建議第 15 項將虛擬資產服務業者（virtual assets service provider）列入應受洗錢防制與打擊資助恐怖主義（AML/ CFT）監管之範疇，並進一步提出虛擬資產服務業之範圍。

為因應國際趨勢，配合 FATF 建議及「亞太防制洗錢組織」（Asia/Pacific Group on Money Laundering, APG）評鑑，我國「洗錢防制法」已於 2018 年 11 月修法，於第 5 條將「虛擬通貨平台及交易業務之事業」納入管制，適用關於金融機構之規定，包含建立洗錢防制內部控制與稽核制度、進行確認客戶身分程序及資料保存、交易紀錄留存、達一定金額以上或疑似洗錢申報義務等。

一、挖礦（Mining Activities）

挖礦是獲取比特幣或其他虛擬通貨勘探方式的暱稱，比特幣礦工透過解決具有一定工作量的證明機制問題，來管理比特幣網路，

Financial Reporting Advisory Group, p.36.

[126] Autonomous, https://www.autonomous.com/ (last visited: Feb. 26, 2021).

確認交易並且防止雙重支付[127]。

挖礦早期主要由個人進行，但是目前多有以企業參與挖礦（例如，Antpool、Bitfury、Bitmain、Nicehash 等專職挖礦之大型企業）[128]，並衍生出礦池、礦機、礦機操作系統、雲端算力等挖礦產業鏈，如下圖 17[129]所示：

圖 22 區塊鏈礦業生態

資料來源: 2020 上半年區塊鏈挖礦產業研究報告：TokenInsight。

於 2017 年後，網絡犯罪的重心由勒索軟件攻擊，轉向所謂的

[127] 挖礦(數位貨幣)，維基百科，https://zh.wikipedia.org/wiki/%E6%8C%96%E7%A4%A6_(%E6%95%B8%E4%BD%8D%E8%B2%A8%E5%B9%A3)，最後瀏覽日:2021 年 2 月 26 日。

[128] Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective, 2020 July, European Financial Reporting Advisory Group, p.36

[129] https://www.blocktempo.com/tokeninsight-mining-report2020/ ，最後瀏覽日:2021 年 2 月 26 日。

「挖礦綁架」(Cryptojacking)。自 IBM 發布的網絡安全威脅報告指出，勒索軟體攻擊模式的事件數量，在 2018 年降低了 45%，而挖礦綁架在同一區間則大幅成長了 450%。「挖礦綁架」是指透過惡意程式控制受害者的電腦用以「挖礦」，或者說啟動某些程式以產生加密貨幣（虛擬通貨），這些竊取他人電腦算力進行挖礦惡意程式出現在各式各樣的地方，包括美國法院的網絡系統、Google Chrome 的擴充功能，以及電動車製造商特斯拉（Tesla）的雲端系統等等[130]。

二、去中心化金融服務

去中心化金融（Decentralized Finance ，下稱「Defi」）與區塊鏈技術及虛擬通貨之演進，密不可分。區塊鏈發展之去中心化借貸交易模式多元，2019 年 DeFi 用戶數量增加 30 倍，在以太坊進行「去中心化借貸」(Decentralized Lending and Borrowing）交易量占總體約 80%，廣受歡迎[131]。去中心化金融之運行，於以太坊加入智慧合約之程式碼後，發展起與區塊鏈 1.0 不同且可提供群眾互聯網募資、借貸、物聯網交易、賭博、保險、拍賣等多樣化之交易模式[132]。

Defi 目前發展成以太坊之核心驅動力功能，DeFi 係以提供一全新、未經許可之金融服務生態系統為核心，無須中央政府授權，世界上任何身分者皆可自由參與使用，並保管自己的私鑰。在去中心化生態系統中，用戶充當自己資產之保管者，在鏈上透過持有私鑰保有對資產之完全控制權，此生態鼓勵完全的所有權和對所有相互分離的市場和平台的訪問權。 Defi Lending（去中心化借貸）係一自主之生態圈，以去中心化網絡為運作基礎，由非許可制區塊鏈及 P2P 點對點協議建構之應用程式組成，促進借貸或與其他金融工具進行交易。Defi 生態系統之分類如下圖 23[133]所示：

---

[130] 網絡犯罪再進化：勒索軟件被「挖礦綁架」取代，https://www.thenewslens.com/article/115359 ，最後瀏覽日:2021 年 3 月 19 日。

[131] 徐珮菱、高培勛(2020)，〈中心化金融之法律規範研究─以 Defi 借貸為核心〉，《高大法學論叢》，第 16 卷第 1 期，頁 185-186。

[132] 田篭照博著，朱浚賢譯（2018），《區塊鏈智慧合約開發與安全防護實作》，台北旗標出版社，頁 9。

[133] DeFi 生态系统：核心基础设施, https://www.keyeinfo.com/depth/depth-hot/45248.html ，最後瀏覽日: Feb. 26, 2021。

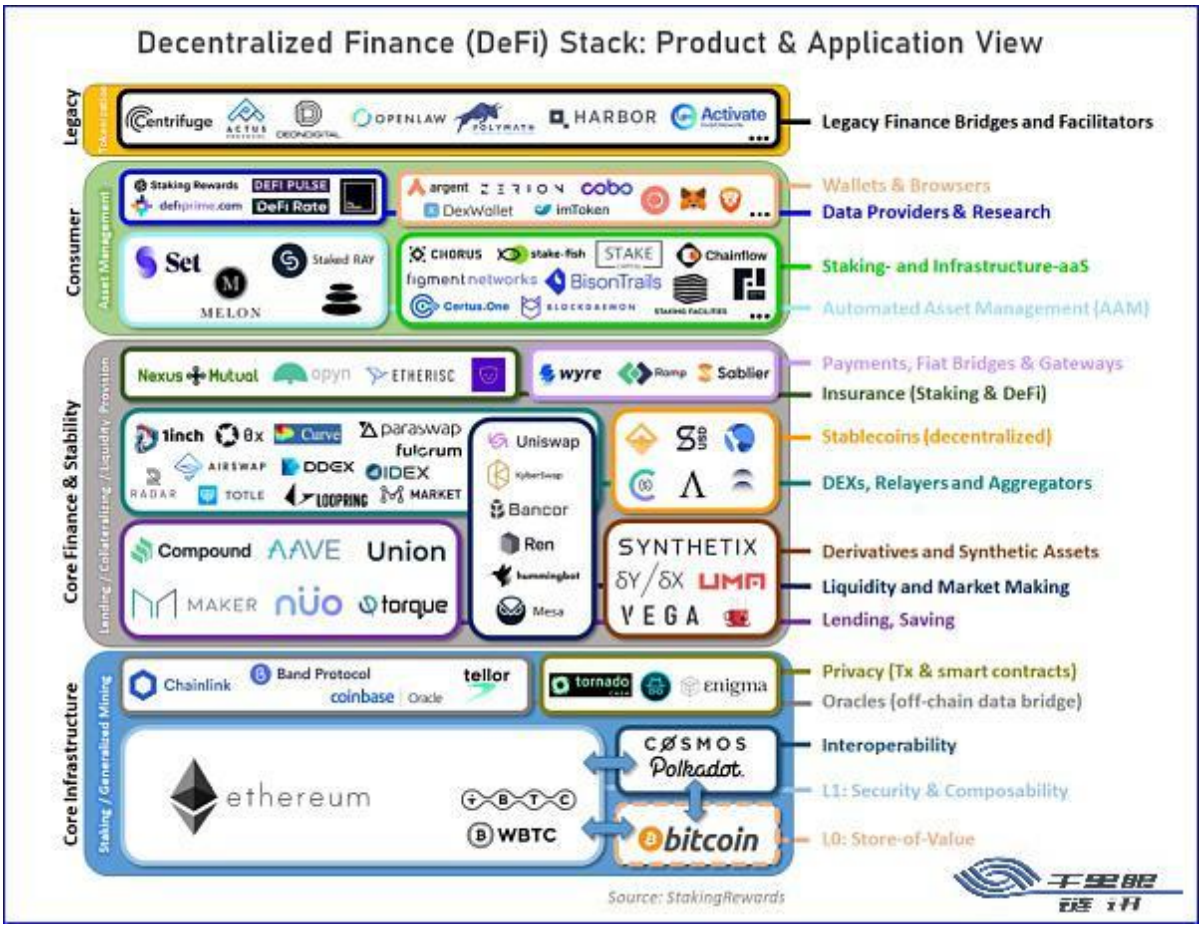


圖 23　DeFi 生態系統

資料來源: DeFi 生態系統：核心基礎設施。

也因為 Defi 於 2018 年始逐步開展，於 2019 年持續成長，並於 2020 年呈現爆發性成長，目前 Defi 產業生態圈已正式成形，且有關 Defi 之虛擬通貨經濟活動亦蓬勃出現，相應地由 Defi 應用而衍生之虛擬通貨濫用於犯罪之行為，也於 2019 年開始成為新興犯罪型態之一，相關 Defi 犯罪之統計數據如下分析。

第三項 涉及虛擬通貨犯罪之成因及統計數據分析

一、犯罪成因

(一)匿名性

比特幣是近幾年所發展出來的一種新興虛擬貨幣基於去中心化網絡的虛擬通貨，允許用戶進行點對點交易，避免傳統的中心實體

管理資金交換。比特幣經濟使用整個P2P網絡中眾多節點構成的分布式數據庫來確認並記錄所有的交易行為，並使用密碼學的設計來確保貨幣流通各個環節安全性。交易由網絡本身記錄和驗證，所有參與交易者組成分布式數據庫，所有交易的歷史都儲存在「區塊鏈」中。比特幣可以和其他貨幣一樣使用，用於支付商品或服務。比特幣的設計優勢之一是匿名性。儘管每個交易都在區塊鏈中以唯一標識符記錄和發佈，但交易者的名稱從未公開，使得即使系統不是完全匿名，卻很難追溯買賣雙方的真實身份[134]。由於比特幣的發行及交易與任何中央實體無關，例如銀行、政府，因此在過去無任何洗錢防制措施的要求下，使用比特幣網路的使用者可以某程度以匿名（非實名制Anonymity）方式使用、交易比特幣。

使用者基於各種不同理由使用比特幣。Yelowitz 及 Wilson[135]分析四種比特幣使用者類型及理由：（1）對電腦程式人員而言，著重在比特幣挖礦與獎勵回饋；（2）對投資客而言，可由比特幣市價節節高昇獲取利益；（3）對自由主義者而言，比特幣可某程度擺脫中央政府機構之監管，達成自由經濟之理想；（4）對犯罪者而言，則可利用其匿名性=從事犯罪或洗錢等非法行為[136]。

(二)成為經濟價值載體

此外，由於虛擬通貨擁有去中心化驗證、難以竄改等技術特徵，已逐漸證明了能將之作為一種經濟價值載體的價值。雖然加密貨幣應賦予如何的法律定性、如何監管，國際間目前尚有多種不同的嘗試與取徑，由於虛擬通貨已被廣泛地接受其具備經濟價值，從而至少具備金融工具(financial instruments)之特性，但也因此如同絕大多數金融工具一般，同時存在著成為犯罪行為之工具，或成為犯罪行

[134] CYBAVO:什麼是比特幣？，https://www.cybavo.com/zh-tw/knowledge-center/what-is-bitcoin/ (最後瀏覽日：2021 年 11 月 14 日)

[135] Yelowitz, A., & Wilson, M. (2015), Characteristics of Bitcoin users: an analysis of Google search data. Applied Economics Letters, 22(13), 1030-1036.

[136] 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》，第 18 期，頁 65。

為之標的的問題[137]。

(三)各國針對虛擬通貨監管法令不健全

虛擬通貨作為犯罪工具使用，乃是虛擬通貨最早開始受到關注與探討的法律議題之一。由於虛擬通貨在絕大多數國家非屬法定貨幣，僅透過網絡傳輸與認證，且其去中心化之特性使之監管更加困難，在當前尚無完整對應之監管機制下，輔以其已被承認之經濟價值，使虛擬通貨具備將犯罪所得移轉，進一步達到規避監管之可能性[138]。

二、虛擬通貨犯罪成因相關統計數據

近年來像比特幣這樣的加密貨幣價值的驚人增長吸引了投資者、投機者和小偷。僅在過去 2017、2018 兩年中，少數犯罪分子就從虛擬通貨交易平台中盜取 12.1 億美元等值之虛擬通貨。光 2018 年上半年遭盜取走的虛擬通貨(價值)就是 2017 年全年的三倍。

[137] 范建得、劉嘉彥，檢視加密貨幣（Cryptocurrency）可能涉及之犯罪問題及其規範，https://blpc.site.nthu.edu.tw/p/406-1390-152227,r7141.php?Lang=zh-tw，最後瀏覽:2021 年 6 月 20 日。

[138] 同前註。

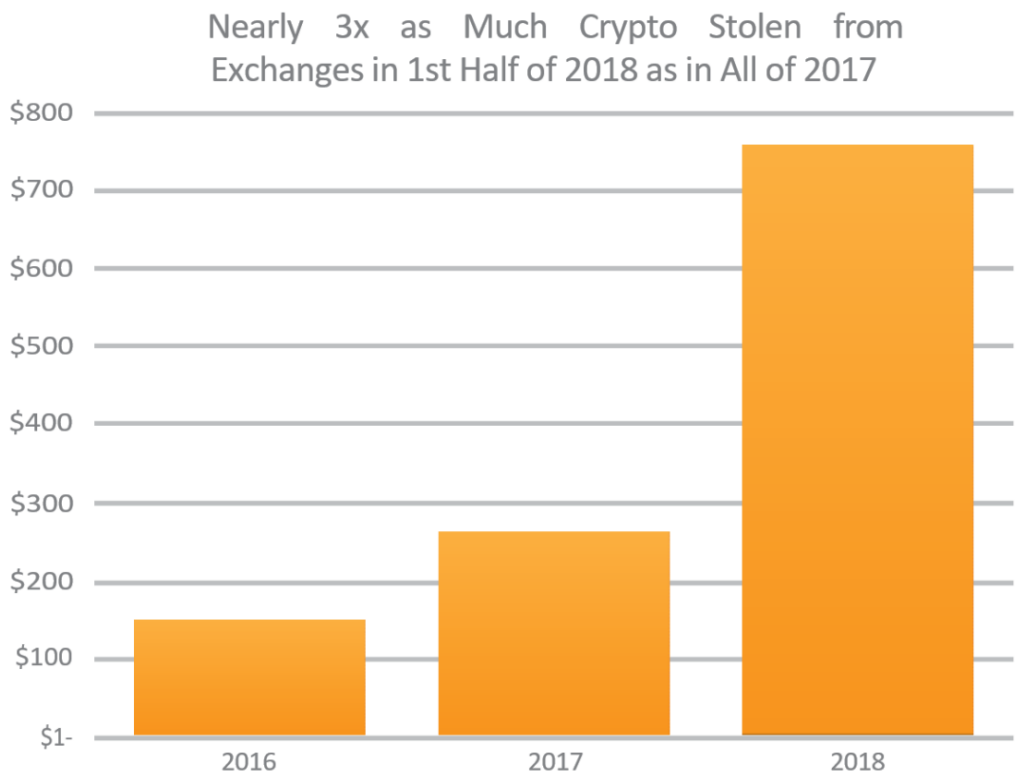


圖 24　2016 至 2018 交易平台遭盜取之虛擬通貨價值

資料來源: Q2 2018 Cryptocurrency Anti-Money Laundering Report[139]。

[139] Q2 2018 Cryptocurrency Anti-Money Laundering Report, https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/ (last visited Oct. 13, 2021).

根據 CipherTrace 於 2020 年發布之虛擬通貨犯罪及反洗錢報告，2020 年涉及虛擬通貨、駭客攻擊和詐欺之總金額達到 19 億美元，為年度史上第二高[140]，相比 2019 年的 45 億美元卻有顯著的下降。

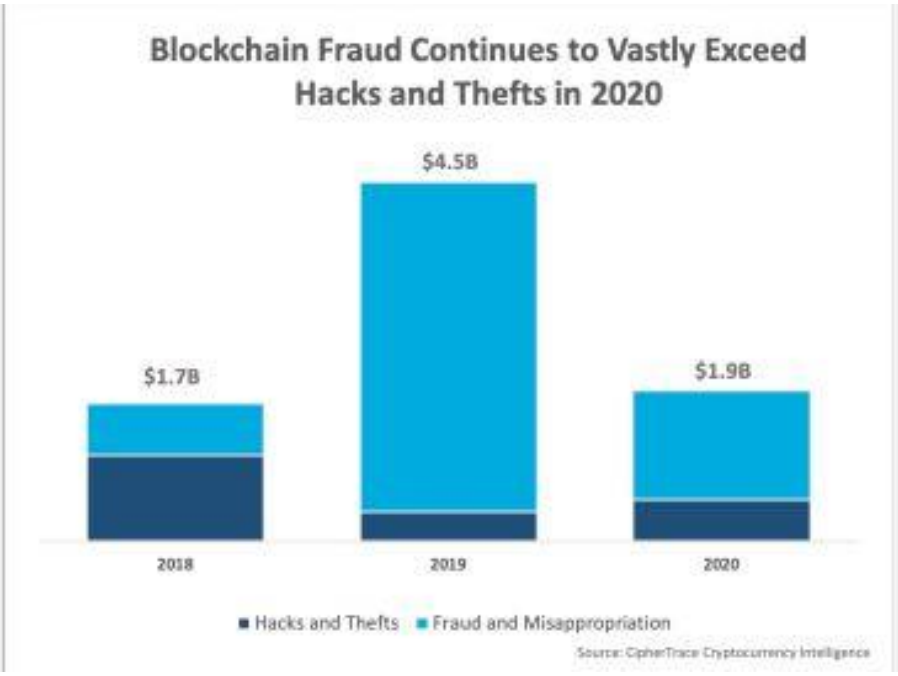


圖 25　2018 至 2020 虛擬通貨詐欺與駭客攻擊趨勢

資料來源: Cryptocurrency Crime and Anti-Money Laundering Report, February 2021[141]。

在過去的兩年中，大規模的跨境網路騙局已成為虛擬通貨犯罪的主要來源之一，在 2019 年爆發之 PlusToken 龐氏騙局產生了高達 29 億美元的不法所得，占當年 64%主要虛擬通貨涉及犯罪之金額。2020 年出現了 WoToken，這是由傳銷架構人為運營傳銷計劃，類似於 PlusToken，在傳銷騙局解體後，共計騙取投資人超過 11 億美元，占 2020 年因詐騙所損失金額總額的 58%。儘管 2020 年涉及虛擬通貨重大詐欺行為的犯罪數量相較過去有顯著減少，但仍然占 2020 年當年度犯罪總數的 73%。

[140] CIPHERTRACE, *Cryptocurrency Crime and Anti-Money Laundering Report*, Feb. 2021, CipherTrace, https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/ (last visited: Mar. 05, 2021) .
[141] *Id*. at 7.

數據顯示，2020 年所發生的網路駭客攻擊(含竊取)和詐欺事件數量相較 2019 年持平(已停止成長)外，2020 年犯罪所涉及之不法獲利相比 2019 年則有顯著地下降，2019 年平均每件犯罪不法獲利比 2020 年高出 160%，表示強化資安系統並採取防範措施能夠有效因應來自內部及外部的威脅。2020 年發生 KuCoin 虛擬通貨交易所遭駭客入侵事件，且損失高達 2.81 億美元，但 KuCoin 交易所表示已經追回了 84%的遭盜取的資金，這在過去幾年幾乎是前所未聞的情形[142]。

2020 年發生之駭客盜取虛擬通貨之事件中，有一半以上是採用 DeFi 協議（此種模式在過去非常稀少，幾乎可以忽略不計），而光是 2020 年下半年，有將近 99%的主要詐欺行為係源自於 DeFi 協議[143]，此新興的犯罪行為態樣也顯示出 Defi 之虛擬通貨經濟活動之蓬勃發展，連帶讓犯罪行為猖獗，類似於 2017 年的 ICO 狂熱。

綜上所述，虛擬通貨已成為洗錢的溫床，以及部分不法分子手中利用之工具[144]，同時虛擬通貨的出現也持續對傳統金融監管產生挑戰，例如利用 ICO（Initial Coin Offering）及 Defi 協議進行全球同步募集(或吸收)虛擬通貨之行為，因為其跨域特性，導致現行證券法令無從管理各種不斷發生的全球募集資金（虛擬通貨）行為。

[142] *Id*, at 7.
[143] *Id*, at 8.
[144] 同前註**錯誤! 尚未定義書籤。**

第二節　虛擬通貨犯罪之類型化分析

經本研究團隊研析近年國際統計數據及綜合案例，將虛擬通貨犯罪分為二大類型，包括詐欺行為及網路駭客竊取行為。此外，本研究團隊觀察到近期網路犯罪之勒索病毒中，越發常見將虛擬通貨作為交付贖金等支付工具，以及將虛擬通貨作為犯罪交易對價等，以下分別就二大犯罪類型、交付贖金工具以及犯罪交易對價等情形進行分析：

第一項 詐欺行為

詐欺行為係透過對受害人的故意施以詐術，利用虛擬通貨之不同經濟活動類型遂行詐騙，以從受害者手中獲得特定虛擬通貨。較常見的詐欺行為類型有:初始代幣發行騙局(Initial Coin Offering, ICO)、拉高出貨(Pump and Dump Schemes)、不當的市場操縱、龐氏騙局、經紀/經銷商詐欺、無良推銷(unscrupulous promoters)[145]及透過 Defi 協議遂行詐欺等。

一、犯罪原因

以太幣長期以來被認為是詐欺犯罪的首選加密貨幣，主要原因為從 2017 年 ICO 熱潮，以及近期 Defi 協議均係利用以太坊智能合約所致。根據美國波士頓大學研究報告指出，2018 年 5 月前完成的 2,390 件 ICO 專案，從代幣公開發行到交易所上架進行交易，所得平均報酬率高達 179%[146]。

犯罪者利用這種新的熱潮，以及人們害怕沒有跟上熱潮的 FOMO(Fear of Missing Out)心理，透過創建涉及假投資頁面等網絡釣魚騙局，使人們在其假網頁中輸入詳細個人信息，包含將個人所有之加密貨幣自主移轉予犯罪集團。ICO 顧問公司 Satis Group 報告也指出，2017 年的 ICO 活動超過 8 成都是詐欺[147]。

---

[145] Cryptocurrency Fraud, CONSTANTINE CANNON , https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/ (last visited Mar. 05, 2021).

[146] Hugo Benedetti, Leonard Kostovetsky, *Digital Tulips? Returns to Investors in Initial Coin Offerings*, 66 J. Corp. Finance No. 101786, 3 (2021).

[147] 張庭妤，識破 ICO 騙局，「拒當韭菜」教戰守則，https://www.bnext.com.tw/article/50799/how-

此類型騙局並非以太坊智能合約功能所獨有，但是由於有 82%的 ICO 建立在以太坊區塊鏈上，因此很快成為犯罪者的首選。除了假投資頁面等網路詐騙外，其他常見的詐騙類型還包括龐氏騙局等[148]。

經本研究團隊分析，虛擬通貨交易若未透過虛擬通貨交易商，在無進行相關洗錢防制措施（AML）下，不需要犯罪分子使用其真實姓名、銀行帳號等，使犯罪分子得以逃避執法人員和其他調查人員的監視，且虛擬通貨的轉移不需要經由其他金融中介機構（例如 PayPal），故犯罪者難以被執法機構逮捕到案，因此得更加肆無忌憚進行網路詐欺詐取受害者資產（虛擬通貨），並透過其他虛擬通貨交易所遂行洗錢。

二、犯罪規模及趨勢分析

(一)2017-2018 年間

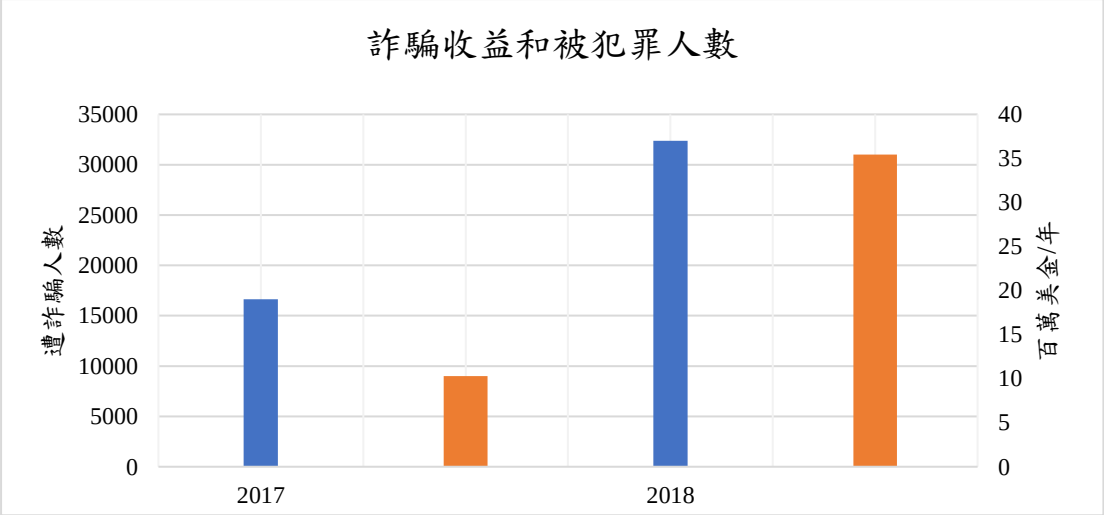


圖 26　2017 至 2018 詐騙收益和被犯罪人數

資料來源: Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams[149]。

to-avoid-ico-scam（最後瀏覽日：2021 年 03 月 05 日）。

[148] *Supra* note 140, at 16.

[149] Chainalysis, Crypto Crime Report Decoding increasingly sophisticated hacks,darknet markets, and scams, Chainalysis (Jan. 2019),https://uploads-ssl.webflow.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda_Chainalysis%20January%

從2016年末到2018年底根據以太坊上之公開錢包位址進行分析後，發現有2,000多個詐騙地址，這些地址已收到來自近40,000個個別用戶的資金，此40,000多名用戶中有近75%在2018年間遭到詐騙，可顯示於2018年之虛擬通貨詐騙活動急劇增加，從2017年到2018年間遭詐騙的人數增加了四倍，其中2018年第一季詐騙活動大幅增加，主要原因與2017年末ICO市場炒作熱潮有關，數據顯示，所有詐騙收益中有近45%發生在2018年第一季[150]。

本研究團隊發現，2017年ICO詐騙的成功導致其他犯罪者加入此類犯罪型態，但使用者也以得到教訓，變得更不容易上當，使得ICO網絡釣魚詐騙的效率遠不如過去，根據數據統計，2018年遭詐取金額的中位數約為94美元，遠低於2017年的144美元。此外，犯罪者的平均總收入在2017年超過6,500美元，而2018年為2,440美元。2017年，只有49名詐騙犯罪者的收入低於100美元，而在2018年，這一數字提升至181名，其中65名的收益低於10美元。在2018下半年，一些創新的犯罪者執行了更複雜的龐氏騙局和ICO exit詐騙，帶來了數百萬收益，此為下半年主要的詐騙收益來源[151]。

總體而言，2018年，交易所和基礎設施(infrastructure)遭竊取之加密貨幣價值9.5億美元。在整個2018年，韓國和日本是大多數竊盜案的發生地，占了58%。在前三季，來自駭客的竊盜在加密貨幣犯罪為大宗，而第四季則主要是內部團隊監守自盜(inside jobs)或詐欺[152]。

(二)2019-2020年間

Chainalysis針對以太坊的犯罪進行了分析，並於2019年1月的報告中指出，在2018年，只有0.01%的以太幣(價值3600萬美元)被詐取(scam)，是2017年的1700萬美元的兩倍。此數據也顯示在以太

202019%20Crypto%20Crime%20Report.pdf, at 18.
[150] *Id.,* at 18.
[151] *Supra* note 140, at 21. (last visited: Mar. 05, 2021).
[152] Cryptocurrency Anti-Money Laundering Report – Q4 2018, https://ciphertrace.com/cryptocurrency-anti-money-laundering-report-q4-2018/ (last visited Mar. 05, 2021).

坊區塊鏈上的詐騙是 2018 年加密貨幣犯罪中收入最低的犯罪之一。此外，2018 年詐騙的數量有所下降，而規模更大、更複雜、而且利潤更大[153]。

2020 年與 2019 年相比，詐欺和盜用為 2020 年加密貨幣犯罪之大宗 (相較於駭客與竊盜)，此趨勢是從 2019 年延續到 2020。在被盜的 13.6 億美元中，詐欺和盜用占總價值的 98%，接近 13 億美元。同時也因為疫情的擴散，與 Covid-19 有關的釣魚網站也變得更多[154]。詐欺為主要虛擬通貨犯罪，再來是偷竊及勒索。儘管重大詐欺案件數量大幅下降，但詐欺類型仍占 2020 年犯罪總數的 73%。

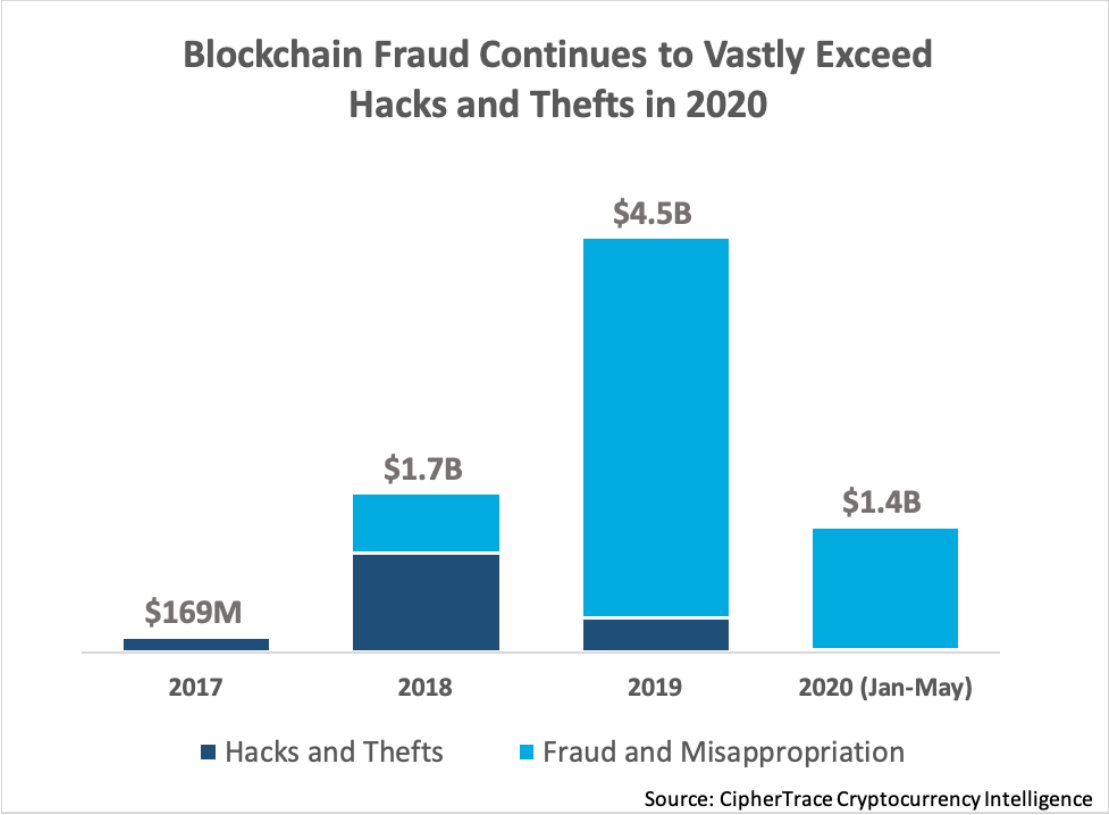


圖 27　2017 至 2020 虛擬通貨詐欺與駭客攻擊趨勢

資料來源: Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report[155]。

[153] *Supra* note 149.
[154] Spring 2020 Cryptocurrency Crime and Anti-Money Laundering Report, https://ciphertrace.com/spring-2020-cryptocurrency-anti-money-laundering-report/ (last visited Mar. 05, 2021).
[155] *Id.*

三、指標案件

(一)龐氏騙局-Pincoin

越南加密貨幣公司 Modern Tech 為其 Pincoin 代幣啟動了首次代幣發行(ICO)，從大約 32,000 人籌集了 6.6 億美元。 該公司首先運行 Pincoin ICO，承諾為投資者帶來持續性的回報，即每月 48%的固定回報，投資者也可以因引入新投資者而獲得 8%的佣金。該公司接著又推出了另一個基於以太坊的代幣 iFan。Picoin 投資者首先從其投資中獲得現金，然後團隊開始以 iFan 代幣支付給 Pincoin 投資者，接著團隊便消失了，由七名越南國民組成的團隊似乎已離開該國。這種所謂的龐氏騙局(Exit scam)可能是近期(2018 年 4 月)發生最大規模的騙局，也預示著 ICO 領域可能會發生的犯罪行為[156]。

(二)龐氏騙局-Plus Token

1. 犯罪手法

Plus Token 發生於 2019 年，是一個偽裝成高收益投資程序的加密貨幣龐氏騙局。該案主要投資者在中國和南韓，提供每月 9%至 18%的投資回報率，較大的投資可獲得更多回報。Plus Token 假裝資金用於開發與加密貨幣相關的產品（例如 Plus Token Wallet 和 Exchange），從而保持了可持續業務的錯覺。同時，Plus Token 還具有很強的傳播性，它向將該計劃推薦給朋友和家人的任何會員提供豐厚的獎勵。根據投資者的投資額和推薦次數，將投資者分為 4 個“層次”，成員推薦的次數越多，回報率就倍數增加，致使成員開始推薦他們的朋友和家人去投資大量的加密貨幣。

2. 受害人數及金額

這場騙局讓數百萬不知情的加密貨幣投資者損失了高達29億美元的資金，占整年的犯罪金額的 64%。這場騙局也導致比特

[156] John Biggs, *Exit scammers run off with $660 million in ICO earnings*, Techcrunch (Aprl. 13, 2018), https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/

幣價格在 2019 年下跌。中國新聞媒體 CLS 於 2020 年 7 月 30 日的報導稱，有 109 人因 PlusToken 計劃而被捕。 其中包括 27 名被認為是該騙局的主要嫌疑犯，以及另外 82 名核心成員[157]。

第二項 網路駭客竊取行為

網路駭客(不限於個人或團體)係指惡意取得他人電腦系統之權限，或是發送釣魚電子郵件來竊取資金。

一、犯罪原因

較大宗的駭客攻擊或偷竊主要針對交易所，通常會從交易所直接竊取到幾千萬甚至幾億美元之加密貨幣。而比特幣是點對點的電子現金系統，是抗審查的替代貨幣系統，再加上比特幣並非由中心化機構控制，又是市值最大的加密貨幣，自然地就成為駭客眼中的「帶洗錢屬性」的貨幣。除了非中心化所以政府無法控制外，駭客選上比特幣尚有下述三大理由：交易不可逆、半匿名、以及流動性高[158]。

[157] Michael, *Plus Token (PLUS) Scam – Anatomy of a Ponzi*, Boxmining (Nov. 27, 2020), https://boxmining.com/plus-token-ponzi/.

[158] Inside，推特駭客為什麼要選比特幣？駭客有辦法逃過執法機構的追蹤嗎？，Inside（2020 年 07 月 22 日）https://www.inside.com.tw/article/20437-what-would-twitter-hackers-choose-bitcoin-is-there-a-way-for-hackers-to-escape-the-tracking-of-law-enforcement-agencies，（最後瀏覽日:2021 年 11 月 13 日）

二、犯罪規模及趨勢分析

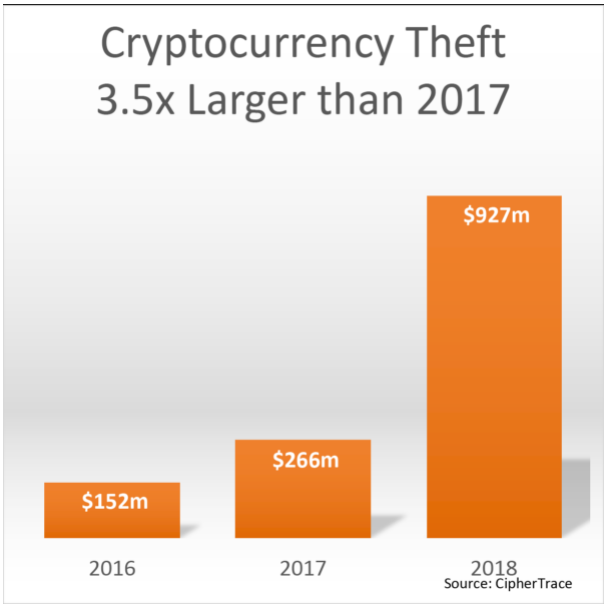


圖 28　2016 至 2018 虛擬貨幣遭竊取金額

資料來源: Q3 2018 Cryptocurrency Anti-Money Laundering Report[159]。

(一)2016-2018 年間

1. 在 2018 年前三季，駭客竊取了 9.27 億美元的加密貨幣，是 2017 年全年的 3.5 倍;自第二季以來，CipherTrace 又新增了 1.66 億美元的記錄[160]。而在交易所和平台層(platform layers)的加密貨幣竊盜仍是 2018 年第三季的主要問題。在 CipherTrace《2018 年第二季度加密貨幣反洗錢報告》中提到，與 2017 年全年相比，2018 年上半年加密貨幣竊盜案增加了三倍。最值得注意的是日本 Coincheck 價值 5.3 億美元的竊盜案和 BitGrail 價值 1.95 億美元的虛擬貨幣竊盜案。

[159] Chainalysis, Q3 2018 Cryptocurrency Anti-Money Laundering Report, https://ciphertrace.com/q3-2018-cryptocurrency-anti-money-laundering-report/ **(last visited:** Mar. 05, 2021).
[160] *Id.*at 4. (last visited Mar. 05, 2021).

2. 2018 年第四季竊盜的總價值低於第三季的數字，部分原因是加密貨幣的價格下跌[161]。而 2018 年第四季的竊盜數量顯著降低，主要是由於缺乏像 2018 年前期在義大利、日本和韓國發生的大規模竊盜案(heists)。下半年所有加密貨幣的價格大幅下跌也導致被盜貨幣的總價值下降。即便如此，2018 年的失竊總量仍是 2017 年的 3.6 倍、2016 年的 7 倍以上。

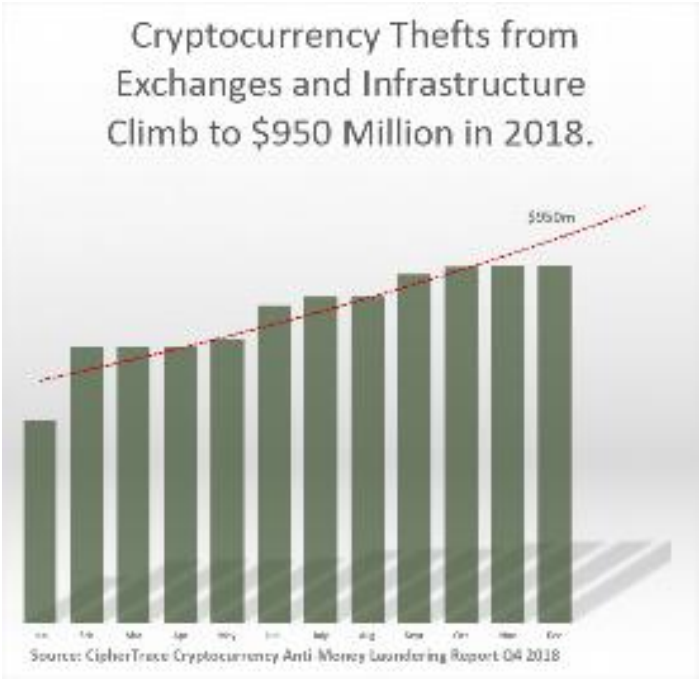


圖 29 虛擬貨幣被盜趨勢

資料來源: Q3 2018 Cryptocurrency Anti-Money Laundering Report[162]。

(二)2019-2020 年間

1. 根據數據統計報告，虛擬貨幣的犯罪是很多元且快速變化的，截至 2019 年 1 月，針對交易所的駭客行為是最大宗的加密貨幣犯罪類型，僅在 2018 年就產生了約 10 億美元的收益。這些收益主要來自兩大犯罪集團，金額在有通報的駭客案件中占了至少 60%。在所有的虛擬貨幣犯罪中，駭客

[161] *Supra* note 152, at 3, (last visited: Mar. 05, 2021).
[162] *Supra* note 159.

跟偷竊是最有利可圖的[163]。

2. 根據聯合國安理會於 2019 年 3 月 6 日出具之報告，北韓政府支持的駭客在 2017 年 1 月至 2018 年 9 月期間成功突破了亞洲至少五家加密貨幣交易所，造成 5.71 億美元的損失。
3. CipherTrace 2019 年第一季度的報告中提及，偷竊和詐騙犯罪者(Thieves and scammers)在這個季度中從交易所和個別用戶竊取了超過 3.56 億美元。
4. 根據數據統計截至 2020 年 10 月底，因偷竊和駭客行為造成的損失增至 4.68 億美元，相較於 2019 全年的 3.61 億美元增長 30%。其中約 20%(約 9800 萬美元)的駭客犯罪行為係來自“Decentralized finance(去中心化金融)”生態系中發生。

(三)涉及 Defi 協議之犯罪數據

1. 在 2020 年所有竊盜案中，有超過 50%是 DeFi hacks，約相當於 1.29 億美元，占全年被盜數量的 25%以上，而在 2019 年 DeFi hacks 數量幾乎可以忽略不計。
2. DeFi 竊盜案的金額範圍可以涵括從幾十萬到數千萬美元的加密貨幣。據 CipherTrace 估計，2020 年平均 DeFi 駭客攻擊價值約為 600 萬美元164。知名的駭客案件 KuCoin(下有詳細案件內容)也有包含 Defi 的利用，犯罪者試圖透過世界上最大的去中心化交易所之一 Uniswap 來進行被盜資金的洗錢。犯罪者選擇使用去中心化犯罪的原因是去中心化交易平台通常不會蒐集有關其用戶的 KYC 訊息，也無法像集中式交易平台一樣凍結資金。

三、指標案件: Kucoin

總部位於新加坡的數位資產交易所 KuCoin 在 2020 年 9 月份遭到駭客攻擊，涉案金額達 2.81 億美元，北韓的駭客團隊 Lazarus Group 被指控為這起 2020 年最大加密貨幣竊盜案的實施者。根據

[163] The 2021 Crypto Crime Report, Chainanalysis (Feb. 16, 2021) at 6, https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.
[164] *Supra* note 140 (last visited Mar. 09, 2021).

Chainalysis 的數據，該金額代表了 2020 年所有被盜加密貨幣的一半[165]。

KuCoin 執行長兼創始人 Johnny Lyu 聲稱，截至 2020 年 10 月 3 日，已經追回了 2.01 億美元的加密貨幣，並稱肇事者已被抓獲。Lyu 接著在 2021 年 2 月的部落格文章中表示已與交易所和項目合作夥伴合作，追回了 2.22 億美元（占 78%），並與執法機構合作追回 1,745 萬美元（占 6%）。同時，KuCoin 和保險基金支付了剩餘部分，約 4,455 萬美元（占 16%）。最後，KuCoin 確保沒有用戶在此事件中蒙受任何損失。

第三項 勒索病毒將虛擬通貨作為交付贖金等支付工具

勒索病毒（Ransomware）又被稱為「勒索軟體」，是一種惡意程式，旨在加密設備上的檔案。使任何依賴其運行之檔案和系統無法使用[166]當勒索病毒進入電腦，會挾持電腦系統，對檔案加密。受害者不僅無法進入系統、存取檔案，還會跳出「支付贖金」的訊息，唯有支付贖金（大多要求難以追蹤的比特幣作為贖金），才能得到解碼程式，將檔案復原、重新拿回電腦的使用權。由於勒索病毒變異迅速，加害者可以直接索取錢財，因此勒索病毒成為散播最快速的電腦病毒之一，不僅對一般電腦使用者造成負面影響，更成為政府機關、大小企業資訊安全的重大威脅。

一、犯罪原因

勒索行為的犯罪者更偏好比特幣，FBI 指出，網路犯罪中心 2017 年報告中包含的虛擬貨幣價值為 5830 萬美元，理由是當犯罪者要求支付贖金時，通常要求以比特幣等虛擬貨幣支付。 他們還指出：“通常要求使用虛擬貨幣作為支付機制，因為在實施這些計劃時，虛

[165] North Korean Hackers Accused Of ‘Biggest Cryptocurrency Theft Of 2020’—Their Heists Are Now Worth $1.75 Billion”, https://www.forbes.com/sites/thomasbrewster/2021/02/09/north-korean-hackers-accused-of-biggest-cryptocurrency-theft-of-2020-their-heists-are-now-worth-175-billion/?sh=65bb54035b0b (last visited: Mar. 05, 2021).

[166] Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. MS-ISAC, RANSOMWARE GUIDE, CISA (Sept. 2020) at.2, https://www.cisa.gov/sites/default/files/publications/CISA_MSSAC_Ransomware%20Guide_S508C.pdf.

擬貨幣為犯罪分子提供了額外的匿名性[167]。”

根據比特幣行業從業人員解釋，選擇比特幣當贖款的原因大致為: 匿名性、去中心化、交易無法被凍結、在不同國家間便捷流通等等[168]。

二、犯罪規模及趨勢分析

美國司法單位於 2016 年開始示警勒索軟體之數量有上升趨勢[169]，2017 年著名的勒索程式“Wannacry 攻擊了數千台電腦系統並要求受害者向駭客支付比特幣贖金，受害者包括醫院、銀行與企業，這些攻擊估計已造成了 80 億美元的損失[170]。區塊鏈分析公司 Chainalysis 的一份新報告顯示，2020 年虛擬貨幣詐欺(第一類別)及犯罪金額大幅下降。然而，勒索攻擊在 2020 年卻是最嚴重的一年，增長了三倍(311%)，原因是疫情導致在家工作模式更為普遍，而網路罪犯利用了此一趨勢。數據顯示，2019 年支付給勒索攻擊的總額略高於 660 萬美元，10 月份為高峰，而 2020 年的金額高達 3.5 億美元。然而需要注意的是，如果受害者沒有提出遭受勒索攻擊，也很難完全量化勒索攻擊的案件數及金額，因此這些數據極可能被低估。

---

[167] *Supra* note 139.

[168] 36 氪，3 分鐘看懂為什麼 WannaCry 勒索病毒，要選擇比特幣作為支付方式？，科技橘報（2017 年 05 月 16 日），https://buzzorange.com/techorange/2017/05/16/wanna-cry-why-bitcoin/（最後瀏覽日：2021 年 03 月 05 日）。

[169] FEDERAL BUREAU OF INVESTIGATION, Incidents of Ransomware on the Rise, FBI (Aprl. 29, 2016), https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.

[170] Risha Pragg-Jaggernauth, *AML CFT 101 How can Virtual Assets be used for the commission of Financial Crime*, CAFT (Mar. 24, 2021) 8, https://www.cfatf-gafic.org/documents/research-corner/15221-aml-cft-101-how-can-virtual-assets-be-used-for-the-commission-of-financial-crime?format=html (last visited Jun. 17, 2021).

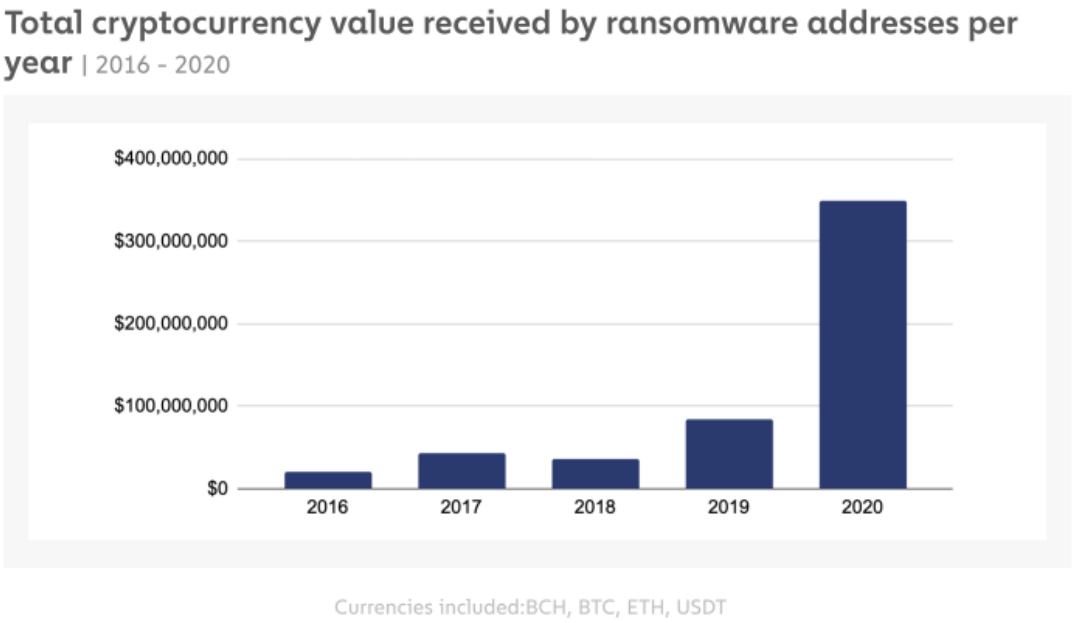


圖 30 2016 至 2020 虛擬貨幣遭勒索金額

資料來源: The 2021 Crypto Crime Report[171]。

根據美國國土安全部發布的數據[172]，自 2016 年以來，每天發生的勒索攻擊超過 4000 起，比 2015 年的每天約 1000 起增加了 300%。McAfee Labs 8 月份的一份報告稱，勒索攻擊每年約增加一倍。這些數據可能低估了真實的數字，因為許多企業只是選擇支付贖金，而沒有向相關單位反映遭受攻擊，原因是一些公司擔心，承認遭到勒索攻擊可能會使它們的股價下跌。

三、指標案件

(一)阿根廷政府遭網路勒索病毒攻擊導致癱瘓

阿根廷政府於 2020 年 8 月 27 日遭受到了 Netwalker 勒索病毒的攻擊，一群駭客入侵了國家移民機構的資料庫並加密檔案，要求 200 萬美元的贖金，以換取解密私鑰。該攻擊暫時使阿根廷邊境入境和

[171] *Supra* note 163.
[172] How to Protect Your Networks from Ransomware, https://www.justice.gov/criminal-ccips/file/872771/download (last visited: Mar. 05, 2021).

出境全面停止，全國各地的移民局和管制站不得不被迫下線近四個小時。

儘管針對城市和地方機構的勒索攻擊已變得較為常見，但這可能是首次使某國針對聯邦機構的攻擊導致中斷營運。經過 7 天，阿根廷政府當局決定拒絕支付贖金，勒索集團決定提高贖金到 355 個比特幣（約為 400 萬美元），然而阿根廷政府宣稱將不會與勒索集團談判，也不會支付贖金。

(二)Netwalker 病毒攻擊加州大學

2020 年 6 月 1 日，Netwalker 病毒攻擊了加州大學舊金山分校，並加密了與重要學術研究有關的數據。加州大學舊金山分校最終支付了大約 114 萬美元的贖金。根據英國廣播公司（BBC）的報告，這個 NetWalker 勒索軟體家族最近轉變為勒索軟體及服務（ransomware-as-a-service, RaaS）模式，營運此軟體的人將重點放在瞄準和吸引技術先進的受害者上。醫療保健行業一直是勒索軟體集團的主要目標，尤其是在疫情持續擴大流行的期間。在對加州大學舊金山分校的網路攻擊中，攻擊者向該大學發出了 300 萬美元的初始贖金要求。經過反覆的談判，勒索軟體營運商最終報價為 1.14 美元。加州大學舊金山分校已將 116.4 比特幣轉移至攻擊者的電子錢包中，並收到解密軟體[173]。

(三)鴻海遭網路病毒勒索

根據 2020 年 12 月的新聞報導，鴻海北美廠區遭受勒索軟體攻擊，除墨西哥廠驚傳遭到勒索病毒「DoppelPaymer」侵入，威州廠區也被侵入。

對此鴻海官方發佈聲明，公司沒有支付一毛錢，但證實中毒，對此北美廠已提高防護層級，受影響廠區網路逐漸恢復正常，對營運影響不大。根據外媒報導，勒索信要求鴻海集團支付 1804.0955 枚

[173] Lindsey O'Donnell, *UCSF Pays $1.14M After NetWalker Ransomware Attack*, threatpost (Jun. 30, 2020), https://threatpost.com/ucsf-pays-1-14m-after-netwalker-ransomware-attack/157015/ (last visited Oct. 13, 2021).

比特幣，相當於 3468.6 萬美元（約台幣 10 億元），鴻海發出聲明，證實遭受網路勒索病毒攻擊，已經完成應變。

鴻海科技集團聲明中證實[174]，「美洲廠區近日遭受網路勒索病毒攻擊，目前內部資安團隊已完成軟體以及作業系統安全性更新，同時提高資安防護層級。本次攻擊，受影響廠區網路逐漸恢復正常中，對集團整體營運影響不大，相關資訊也已與客戶、供應鏈夥伴同步。」

(四)美國燃油管線業者 Colonial Pipeline 遭勒索攻擊

美國燃油管線營運業者 Colonial Pipeline 為美國最大之精煉油管道系統，於 2021 年 5 月 7 日因遭到駭客勒索軟體 DarkSide 攻擊導致管道系統關閉，引起美國東南部燃料供應中斷及美國運輸部發布緊急聲明，為恢復營運，Colonial Pipeline 依據勒索信件的要求向 DarkSide 支付相當於 440 萬美元的比特幣作為贖金。此後美國司法部透過追蹤錢包地址於 2021 年 6 月 8 日扣押追回相當於 230 萬美元的比特幣[175]。

第四項 其他以虛擬通貨作為犯罪交易對價

依國際清算銀行(Bank for International)之研究報告，2019 年所有加密貨幣交易中約有 1.1%（價值約 110 億美元）為與非法活動有關之交易，而 2019 年因虛擬通貨犯罪所導致之損失約 45 億 2000 萬美金，與 2018 年相較成長了 2.6 倍[176]。此類非法交易例如毒品、軍火、人口販運、賭博，結合匿名通訊軟體、匿名覆蓋網路與匿名虛擬通

[174] Lawrence Abrams, *Foxconn electronics giant hit by ransomware, $34 million ransom*, BLEEPING COMPUTER (Dec. 07, 2020), https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/ (last visited: Mar. 05, 2021).

[175] *See* Department of Justice, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside*, THE UNITED STATES DEPARTMENT of JUSTICE (Jun. 7, 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside (last visited: Jun. 18, 2021).; Evan Perez, Zachary Cohen & Alex Marquardt, Jun. 8, 2021, First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers, https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html (last visited: Jun. 18, 2021).

[176] Rodrigo Coelho, Jonathan Fishman and Denise Garcia Ocampo, Supervising cryptoassets for anti-money laundering, BIS (Aprl. 07, 2021), https://www.bis.org/fsi/publ/insights31.htm (last visited: Jun. 18, 2021).

貨進行。

一、犯罪原因

美國財政部的金融犯罪執法網絡 FinCEN 指出，虛擬貨幣（Convertible Virtual Currencies (CVCs)）作為支付方式，有時甚至是唯一的支付方式，結合了匿名覆蓋網路之暗網市場，提供非法商品和服務的交易機會，包含毒品銷售、兒童剝削或是人口販運、網絡犯罪、洗錢、恐怖主義融資、和規避制裁等[177]。

二、犯罪規模及趨勢分析

以人口販運為例，所謂人口販運，係指透過使用武力、詐欺、脅迫、濫用權力或地位不對等，為強迫勞動、性剝削、使人為奴隸、摘取器官而招募、窩藏、運輸、提供或接收人員之行為[178]。根據國際勞工組織的數據[179]，人口販運是一個龐大的全球性犯罪產業，每年產生的收入超過 1500 億美元。FATF 並於 2018 年發布報告[180]，指出人口販運是一種日益增多的國際犯罪形式，衝突戰爭或脆弱地區增加了人口販運的情況。此外，經濟發達的國家中，販運人口仍是主要人口販運之流入目的地，而受害者則往往來自經濟欠發達的國家[181]，FATF 建議各國金融機構及主管機關應透過資金流動情況確認、調查和起訴人口販運中的洗錢活動。依據該報告，虛擬通貨參與於

---

[177] FinCEN, Advisory on Illicit Activity Involving Convertible Virtual Currency, FinCEN (May 9 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf (last visited: Jun. 17, 2021).

[178] *See* generally 18 U.S.C. §§ 1581, 1584, 1589, 1590, 1591, 2421, 2422, 2423, and 2425; 22 U.S.C. §§ 7102(4) and (11); The Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. No. 106-386); applicable state laws; and U.S. Department of State, "Report on U.S. Government Efforts to Combat Trafficking in Persons," (December 1, 2017); *See also* the Palermo Protocol defines human trafficking as:" the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs".

[179] International Labour Organization (ILO) ,ILO says forced labour generates annual profits of US$ 150 billion, ILO (May 20 2014), https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_243201/lang--en/index.htm (last visited: Jun. 17, 2021).

[180] FATF-APG, *Financial Flows from Human Trafficking*, FATF (Jul. 2018),https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.

[181] *Id*., at 11.

人口販運之方式包含以比特幣來支付刊登性交易廣告之費用，或是將人口販運所得之不法資金以虛擬通貨進行洗錢。

此外，區塊鏈分析工具服務商於 Chainalysis 分析了可能與兒童性剝削有關之比特幣和以太坊交易，因加密貨幣採用率的增加此類犯罪相關交易 2017 年、2018 年有大量增長[182]。此外，Chainalysis 也觀察到個人向兒童性剝削相關網站所為之支付，其所支付之加密貨幣價值大致介於 10 到 50 美元之間，若進一步分析這些交易模式，Chainalysis 發現可能代表這些個人都訂閱了相同的網站，大量不同使用者對於同一地址之小額頻繁交易或特定時間（例如夜間 11 點至凌晨 5 點）之頻繁交易，可能是評估風險的切入點[183]。

三、指標案件

(一)性交易廣告網站 Backpage.com

Backpage.com 為刊登性交易廣告之最大論壇，自 2015 年起主要信用卡公司停止持卡人於 Backpage 網站上付款後，該網站轉向以虛擬通貨收取對價，透過以虛擬通貨收取網站上刊登兒童及成人性交易廣告之費用外，促進了相關的兒童和成人的性剝削和人口販運。2018 年美國司法部及美國國稅局刑事調查處（Internal Revenue Service Criminal Investigation, IRS-CI）查緝並關閉該網站，營運者被控洗錢、媒介性交易等多項罪名[184]。

(二)兒童色情網站 Welcome to Video

2019 年美國司法部宣布185破獲全球最大的兒童色情網站 Welcome to Video (WTV)，Welcome to Video (WTV) 是一個在韓國營運的兒童色情網站，註冊該網站後，用戶會收到專屬的比特幣地址，

---

[182] Chainalysis Team, *Making Cryptocurrency Part of the Solution to Human Trafficking*, Insights (Aprl. 21, 2020), https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020 (last visited: Jun. 17, 2021).

[183] *Id.*

[184] US Department of Justice, *Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment*, THE UNITED STATES of JUSTICE (Aprl. 09, 2018) https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads (last visited: Jun. 17, 2021).

[185] US Department of Justice, *South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin*, THE UNITED STATES of JUSTICE (Oct. 16, 2019), https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child (last visited: Jun. 17, 2021).

並可使用比特幣來購買或上傳自己的內容。2018 年，美國國稅局刑事調查處（Internal Revenue Service Criminal Investigation, IRS-CI）、國土安全部與英國、韓國之警調機構合作查緝 WTV 並查獲了大約 8 TB 的兒童性剝削影片，為此類犯罪查獲量史上最大的一次。警調機構透過區塊鏈分析工具分析網站上之比特幣地址及其交易活動，追蹤區塊鏈上之進出 WTV 地址的資金流向及交易所資訊，並再透過交易所提供之資訊，於 38 個國家共逮捕了 337 名犯罪嫌疑人。

(三)現行洗錢防制架構下產生之穩定幣可疑交易問題

1. 案例背景

Bitfinex 是一國際虛擬通貨交易平台，由境外公司 iFinex Inc 擁有及營運，其總部設於香港，而 iFinex Inc 的關係企業 Tether 發行虛擬美元—泰達幣（Tether Coin）[186]，也是現行流通及交易量最大的穩定幣（虛擬通貨）被稱為「虛擬通貨界的央行」。

據報導，iFinex過去曾把其公司資金金庫設在台灣，又因自身涉及數起洗錢和金融違規案件，遭德意志銀行調查 iFinex Inc 有關的帳號，寫成一份可疑交易調查報告，並於 2016 年 11 月 28 日遞交給美國財政部金融犯罪執法局。

[186] 維基百科，Bitfinex，https://zh.wikipedia.org/wiki/Bitfinex（最後瀏覽日：2020 年 10 月 21 日）。

該可疑交易調查報告指出，iFinex 的三個德銀帳戶在 2015 年 11 月至隔年 10 月，短短一年間，就觸動了 5 次德銀可疑交易警報，交易金額達 1377 萬美元（約 4.1 億台幣）。包括 144 筆交易中，竟發現台灣共有 7 家銀行涉入其中。

2. 虛擬通貨挑戰洗錢防制體系

從 Bitfinex 交易所/iFinex 案例可知，虛擬通貨同時具有價值儲存以及全球流通的特性，故特定主流虛擬通貨時常成為特定事業或不法業者的洗錢標的之一，未來將持續挑戰我國金融體系及洗錢防制體系的穩定。

目前我國金管會、法務部及相關自律組織亦展開研訂一連串之法規命令及自律規範，以完備我國洗錢防制及資安防制之法律體系[187]，相關虛擬通貨洗錢之犯罪手段，在追求洗錢防制法制完備之趨勢下，容有進一步研析之必要。

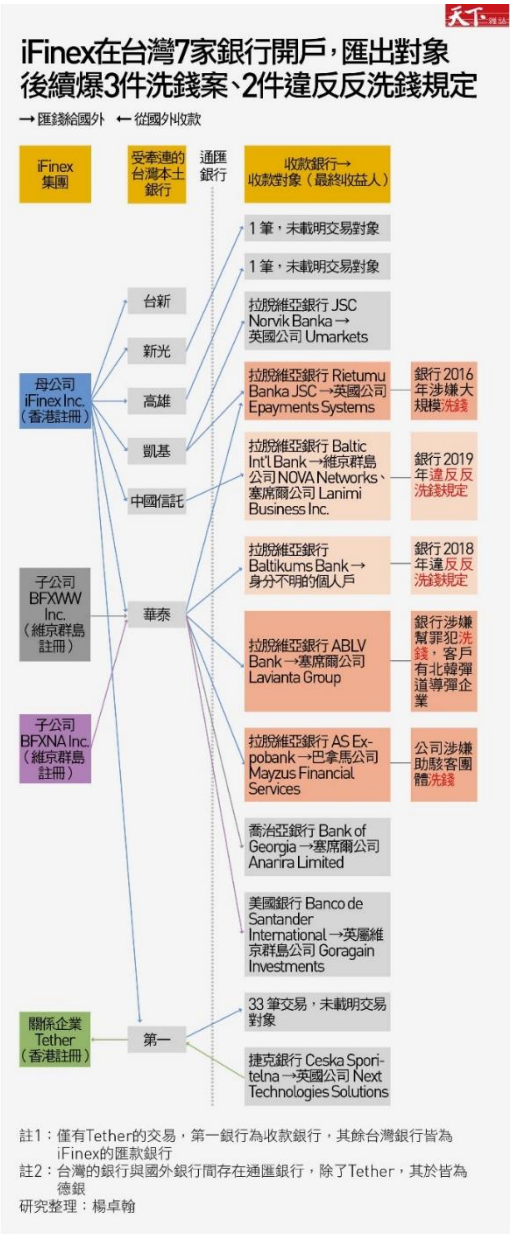


圖 31 iFinex 在台灣 7 家銀行開戶，

匯出對象後續爆 3 件洗錢案、2 件違反反洗錢規定

資料來源: 台灣被捲入洗錢風險？金融犯罪嫌疑者 iFinex，曾是 7 家本土銀行客戶[188]。

第五項 小結

[187] 王志誠，洗錢防制法之發展趨勢-金融機構執行洗錢防制之實務問題，月旦法學雜誌第 267 期，2017 年 8 月，頁 1。

[188] 台灣被捲入洗錢風險？金融犯罪嫌疑者 iFinex，曾是 7 家本土銀行客戶，https://www.cw.com.tw/article/5101992，最後瀏覽日:2020 年 10 月 21 日。

經本研究團隊持續追蹤，DeFi 協議 Poly Network 於 2021 年 8 月 10 日發生史上最大的 DeFi 駭客攻擊事件，失竊資產總價值約 6.11 億美元，根據慢霧安全團隊稱「結合資金流向及多項指紋資訊可以發現，這很可能是一次規劃已久的、有組織有準備的攻擊行為。」本案如同先前本研究團隊研究之 Kucoin 交易所案例如出一轍，事發後 Poly Network 的交易池(O3 Swap)暫停功能，官方並聯絡各大區塊鏈之礦工協助，包括各大虛擬通貨交易所 OKEx、幣安與穩定幣 USDT 發行商 Tether 均提供支援。在各方協助圍堵下，成功避免本案被盜取的虛擬通貨遭快速轉移、洗錢。

最終本案竟然出現轉折，先是駭客願意歸還資產，現在 Poly Network 除願提供 50 萬美元揭露漏洞獎金，並邀請駭客但任公司「首席安全顧問」。上述事件即可知，本研究案所研析之虛擬通貨濫用於犯罪仍層出不窮，惟若各國政府及主要虛擬通貨業者，能夠落實洗錢防制及防資恐等措施，確實能夠有效預防犯罪，或是於犯罪發生後將影響範圍降至最低。

惟同一時間，在各國建構虛擬通貨之洗錢防制制度之同時，一種被稱為區塊鏈數位帳本上的數據單位，每個代幣可以代表一個獨特的數碼資料-非同質化代幣（Non Fungible Token, NFT）橫空出世，由於非同質化代幣不能互換，且可證明為唯一，固非同質化代幣可以代表特定數位文件，如畫作、聲音、影片、遊戲中的項目或其他數位形式的創意作品，並且快速發展。

NFT 很可能且已經被不法人士用於以類似實體藝術品的方式遂行洗錢，NFT 轉移贓款的方式可能比起虛擬通貨更加容易，因為目前國際防制洗錢金融行動組織(FATF)指出，高價藝術品、文物、奢侈品極易被利用於洗錢或資助恐怖活動，但是否納入洗錢防制規範，交由各國依本國風險評估決定。而 NFT 發行及交易平台是否正式納入洗錢防制制度之範疇之一，仍在討論中，導致高市場價值之 NFT 標的容有淪為新興洗錢工具之一，此點未來有必要修正虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法，擴大適用洗錢防制範圍及於 NFT 發行及交易平台。

第三節　我國虛擬通貨濫用於犯罪之分析

第一項 我國對於虛擬通貨之法律定性

我國民法採取權利主體、權利客體二元論，「動產」、「不動產」均屬「物」，為權利客體。法律行為之客體在科技發展及交易之多元化，法律行為客體已包含權利或無體物[189]。再參照我國刑法第 10 條第 6 項，稱電磁紀錄者，謂以電子、磁性、光學或其他相類方式所製成，而供電腦處理之紀錄。不論虛擬通貨是區塊鏈系統創建或是由特定發行人發行的，均屬之，故虛擬通貨本身係我國刑法下電磁紀錄之一種，而我國司法實務亦認為電磁紀錄為無體物[190]，故虛擬通或本身為無體物，應無疑義。

有疑義者係，虛擬通貨並非嚴格意義之貨幣，在我國不具有法定清償效力，對於虛擬通貨之法律上定性說明，難免為價值預判的結果，且應就虛擬通貨之分類與用途進行價值判斷[191]，目前分類尚可概略分為：原生幣（例如比特幣）嚴格來說比特幣並無所謂「發行人」，而係 2008 年中本聰白皮書發布後，依據比特幣網路匿名礦工挖礦產出的；應用幣（Token），例如前述提及之穩定幣、證券型代幣或其他特殊工具而非證券之代幣，各國監管單位並根據不同虛擬通貨之分類及用途，而有不同之法律定性之判斷。

然而，我國政府機關目前並未針對虛擬通貨之分類與用途進行不同價值判斷，一律將比特幣及其他不同類型之虛擬通貨定性為非貨幣、屬於數位「虛擬商品」；至於是否屬於證券交易法規範之有價證券，須視個案情況認定，故有論者謂探究比特幣在我國法律的性質，確定其非屬貨幣、電子錢、數位貨幣，而屬於無體財產及洗錢防制法規定的虛擬通貨[192]。以下整理我國不同主管機關對於虛擬通貨之法律定性：

一、中央銀行

[189] 最高法院 93 台上字第 4180 號刑事判決參照。
[190] 最高法院 93 年台非字第 184 號刑事判決參照。
[191] 陳丁章、范建得、黎昱萱(2021)，自比特幣技術的特徵論虛擬貨幣的法律特性及其相關議題-虛擬貨幣的法律屬性，元華：台北，頁 48。
[192] 陳榮傳，同前註 27，頁 41。

(一)我國中央銀行（下稱「央行」）於 2013 年 12 月 30 日新聞稿公開表示：「比特幣不是貨幣...（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，央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。」

(二)央行並於 2019 年 2 月 1 日公開央行內部虛擬通貨研究報告，報告指出：「（四）結語...**虛擬通貨不是貨幣，係屬高度投機之加密資產或商品**，鑒於其不具備貨幣之主要特性...避免虛擬通貨被誤導為貨幣。」

(三)由上可知，**央行認為比特幣或由其他機構或單位發行之虛擬通貨，並非由央行發行，更不具備中央銀行法第 13 條第 2 項之法定清償效力，故非我國之法定貨幣**。

二、金融監督管理委員會

(一)央行與我國金融監督管理委員會（下稱「金管會」）於 102 年 12 月 30 日聯合發布新聞稿，認為比特幣並非貨幣而係屬高度投機之虛擬商品。

(二)金管會並於 103 年 1 月 6 日發布新聞稿，要求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。金融機構應配合落實辦理。

(三)金管會於 106 年 12 月 19 日發布新聞稿再次提醒社會大眾投資虛擬商品的風險，表示：「金管會...將比特幣定位為具有高度投機性的數位『虛擬商品』，並提醒社會大眾務必要審慎評估投資風險...**三、首次代幣發行(ICO)行為是否屬證券交易法規範之有價證券，視個案情況認定**」。

由上可知，金管會與央行均認為比特幣等虛擬通貨並非貨幣，且禁止我國金融機構收受、兌換比特幣等虛擬通貨，認為**該等業務並非金融機構得受理之業務範圍**；此外，金管會認為**發行之虛擬通貨是否屬證券交易法規範之有價證券，須個案認定**，非得一概而論。

第二項 我國主管機關對於虛擬通貨之監理模式

本研究團隊就現行根據區塊鏈技術（或稱為「分散式帳本技術，Distributed ledger Technology, DLT」）發展而生之虛擬通貨應用層面，綜合整理於我國監理模式，並從發行監理、交易（行為）監理二方面進行研析，冀望未來能夠進一步強化我國對於虛擬通貨之監管，以減少虛擬通貨之犯罪以及對被害人之危害：

一、虛擬通貨在台發行之監理

(一)發行之法律上定義

我國現行法規提及發行者，包括證券交易法及著作權法，其中我國證券交易法第 8 條之規定，證券交易法所稱之「發行」，係指發行人於募集後製作並交付，或以帳簿劃撥方式交付有價證券之行為；同法第 5 條則就發行人定義：「募集或發行有價證券之公司，或募集有價證券之發起人」；參照著作權法第 4 條規定所謂發行，係指權利人散布能滿足公眾合理需要之重製物而言。

根據法規範之立法目的不同，證券交易法所指之發行係指與資金募集及交付有價證券有關者，此與虛擬通貨中之證券型代幣有關；著作權法所指之發行，則係以使用（消費）為目之行為[193]，此與應用型代幣有關，例如支付型代幣、非同質化代幣（Non Fungible Token, NFT[194]）等。

(二)證券型代幣（STO）之發行及交易限制

針對 STO 兼具虛擬代幣及證券性質的資本市場交易，美國證券交易委員會(SEC)、防制洗錢金融行動工作組織(Financial Action Task Force, FATF)相繼表態數位資產應受相關的監管要求。SEC 提出「數位資產證券發行與交易聲明」，強調STO發行與交易都必須符合相關

[193] 陳丁章、范建得、黎昱萱，同前註 191，頁 72。

[194] 非同質化代幣是一種被稱為區塊鏈數位帳本上的數據單位，每個代幣可以代表一個獨特的數碼資料。由於其不能互換，非同質化代幣可以代表數位文件，如畫作、聲音、影片、遊戲中的項目或其他形式的創意作品。雖然文件（作品）本身是可以無限複製的，但代表它們的代幣在其底層區塊鏈上被追蹤，並為買家提供所有權證明。(維基百科: https://zh.wikipedia.org/wiki/%E9%9D%9E%E5%90%8C%E8%B3%AA%E5%8C%96%E4%BB%A3%E5%B9%A3 ，最後瀏覽日:2021 年 11 月 14 日)

現行證券法規規範，例如需符合 Regulation D 中私募人數上限、合格投資人與合格機構投資人、發行方式以及資訊揭露等監管要求[195]。

此外 FATF 指出恐怖組織濫用虛擬資產是非常嚴重且急迫性的議題，針對反洗錢和打擊恐怖主義融資，FATF 發布「虛擬資產監管方針」要求國家主管機關需要監督、監管虛擬資產行業，並對於監管環境進行風險評估及制定相關監管政策，全面性的實施反洗錢措施、預防資助恐怖主義的措施，包括：客戶盡責調查、保存完整之交易紀錄、通報潛在可疑交易[196]。

虛擬通貨逐步發展成為資本市場籌資工具之際，觸及為數可觀的證券法制。我國金管會於 2019 年 7 月核定 STO 為有價證券[197]，開啟對 STO 證券監管，並採取「分級管理，小額豁免」的基本方針，以募資金額是否達 3000 萬元區分大額與小額 STO 案，大額案件鼓勵業者依金融科技發展與創新實驗條例申請金融監理沙盒實驗，小額案件則可以豁免適用證券交易法第 22 條之申報要求，但必須符合下述發行管制[198]：

1. 資格條件：依我國公司法組織，且非屬上市、上櫃及興櫃之股份有限公司得發行 STO。
2. 認購上，僅限專業投資人得參與認購，但每一 STO 案之專業自然人投資人之認購額不得逾新台幣 30 萬元。
3. 發行流程：發行流程：發行人限透過同一平台募資，平台業者應確認發行人符合相關應備條件及編製公開說明書。如係平台業者自行發行 STO，應由財團法人中華民國證券櫃檯買賣中心複核後始得辦理。故發行人僅限透過同一平台募資，平台業者應確認發行人符合相關應備條件及編制

[195] U.S. Securities And Exchange Commission, *Statement on Digital Asset Securities Issuance and Trading*, Nov. 16, 2018, https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading (last visited: Jun. 17, 2021).。

[196] *Supra* note **錯誤! 尚未定義書籤。**。

[197] 金管會對「證券型代幣發行(Security Token Offering, STO) 相關規範」之說明，中華民國 108 年 7 月 3 日金管證發字第 1080321164 號，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News，最後瀏覽日：2021 年 6 月 16 日。

[198] 同前註 24，頁 1326。

公開說明書，並制定「證券商經營自行買賣具證券性質之虛擬通貨業務管理辦法」及「申請發行具證券性質之虛擬通貨於證券商營業處所買賣之公開說明書應行記載事項準則」。

(三)STO 監理制度評析

金管會豁免小額 STO 案件適用法遵成本較高的現行證券發行規範，而責成櫃買中心與平台業者制定相關規則把關。但金管會將小額發行門檻訂為新台幣 3000 萬元，並限制小額 STO 案之認購者須為專業投資人，專業自然人尚有投資限額，亦引發開放有限之批評[199]。有論者認為目前台灣 STO 法令限制過多，包括：一、合規成本跟募資金額不成比例：STO 發行及交易平台一年法遵成本至少新台幣 500 萬，惟法令限制一年只能發行一檔 STO 小額募資（3000 萬元），難以負擔發行成本；二、投資人限制過多，STO 只限專業投資人投資，但金額過低，且專業投資自然人認購限額 30 萬元無從說服任何「理性」投資人投資；三、STO 政策前景不明，目前有意願投入經營 STO 發行及交易平台商係預想未來台灣能成為國際區域型 STO 的初級（發行）市場，惟金管會並未開放大額（新台幣 3000 萬元以上）的 STO，致並未有業者正式申請發行 STO[200]。

金管會自 2018 年開始推動 STO 法制，到 2020 年 1 月相關配套法案完備，依照金管會於 2019 年 6 月 27 日發布之「對證券型代幣發行相關規範之說明」新聞稿 STO 募資金額 3000 萬元以上者，應依「金融科技發展與創新實驗條例」申請沙盒實驗，實驗成功後依證券交易法規定辦理，目前已有業者向金管會洽詢辦理 3000 萬元以上 STO。。

二、虛擬通貨交易之監理

[199] 同前註 24，頁 1327。

[200] 設新創板，請踏著 STO 棺材板前進，數位時代，https://www.bnext.com.tw/article/58696/sto-taiwan，最後瀏覽日：2021 年 6 月 16 日。

(一)洗錢防制及打擊資恐

我國洗錢防制法之虛擬通貨商業的適用範圍於計畫執行期間有最新發展，行政院已於 2021 年 4 月 12 日正式發布行政院令，依「洗錢防制法」第 5 條第 4 項指定同條第 2 項所稱虛擬通貨平台及交易業務事業之範圍，且將自 2021 年 7 月 1 日生效[201]。

依最新行政命令，被劃定為虛擬通貨平台及交易事業之業者，應依洗錢防制法第 5 條以下規定，落實 KYC（認識客戶）以及洗錢防制（包括實地查核、交易監控、通報）等義務。經本所金融科技研究團隊研析，對照 2019 年 6 月 FATF 發布之 VASP 指引，針對 VASP 的分類與適用範圍，與本次行政院發布之範圍有高度類似，故 FATF 之指引內容，應為未來我國法令解釋上之重要參照。

為因應行政院指定金管會為虛擬通貨平台及交易業務事業之洗錢防制主管機關，並指定本事業之範圍，金管會已於 2021 年 5 月 25 日正式預告「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」(下稱「本辦法」)，本辦法已於 2021 年 7 月 1 日公告生效，依洗錢防制法第 5 條第 2 項規定，虛擬通貨平台及交易業務事業（下稱「本事業」）適用該法關於金融機構之規定，包含應建立洗錢防制內部控制與稽核制度、進行確認客戶身分、紀錄保存、一定金額以上通貨交易申報及疑似洗錢或資恐交易申報等事項，條文重點如下[202]：

1. 本事業之範圍(指在國內設立登記者)及用詞定義(本辦法第 2 條)。
2. 本事業進行確認客戶身分、強化確認客戶身分、客戶身分持續審查等規定(本辦法第 3 條至第 6 條、第 8 條至第 9 條)。
3. 本事業進行虛擬通貨之移轉時應遵循之規定(本辦法第 7 條)。
4. 本事業紀錄保存之規定(本辦法第 10 條)。
5. 本事業對達一定金額以上通貨交易申報之規定(本辦法第 11

[201] 行政院臺法字第 1100167722 號函令。

[202] 金管會發布「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」，中華民國 110 年 6 月 30 日金管銀法字第 11002720402 號，https://www.fsc.gov.tw/ch/home.jsp?id=128&parentpath=0,3&mcustomize=lawnew_view.jsp&dataserno=202106300005&dtable=NewsLaw，最後瀏覽日：2021 年 6 月 16 日。

條)。

6. 本事業對客戶交易持續監控，及對疑似洗錢或資恐交易申報之規定(本辦法第 12 條)。
7. 本事業對資恐防制法第 7 條第 3 項之通報方式及程序(本辦法第 13 條)。
8. 本事業防制洗錢及打擊資恐內部控制與稽核制度之實施內容(本辦法第 14 條至第 16 條)。

(二)多層次傳銷事業監管

依市場現況，不少虛擬通貨的發行銷售都是透過多層次傳銷的方式為之。也就是我國多層次傳銷管理法第 3 條所稱「透過傳銷商介紹他人參加，建立多層級組織以推廣、銷售商品或服務之行銷方式」。依照多層次傳銷管理法等規定，若虛擬通貨之銷售模式合於多層次傳銷管理法之定義，應依法進行報備，多層次傳銷行為之實施，應受多層次傳銷管理法第三章之監理，特別是傳銷商之收入不得以介紹他人參加為主要收入來源[203]。

參照多層次傳銷管理法第 4 條可知，所謂多層次傳銷事業者，乃包括統籌規畫或實施第 3 條傳銷行為之「團體」與「個人」，也就是不以公司、工商行號為限；再按多層次傳銷管理法第 5 條可知，所謂傳銷商就是參加多層次傳銷事業之人，也就是俗稱之「參加人」，參加人因為推廣或銷售商品、服務或介紹他人加入等作為，而對多層次傳銷事業享有給付佣金、獎金或其他經濟利益的請求權。

現行有不少虛擬通貨之銷售、推廣乃是由部分人士或組織（不限於公司或商號）將已發行之虛擬通貨以多層次傳銷方式為之，依法應依多層次傳銷管理法之報備監理模式進行，尤其應使其傳銷商之收入來源以合理市價推廣、銷售商品為主，不得以介紹他人參加為主要收入來源，否則將涉及刑事、行政罰鍰等責任。

三、穩定幣之法令監管現況

[203] 陳丁章、范建得、黎昱萱，同前註 191，頁 88。

(一)現行虛擬通貨市場發行之穩定幣有三種：

1. 法定資產抵押型穩定幣：包括法定貨幣及實質資產（例如不動產、股票等），法定資產抵押型係指以法定資產擔保經發行之穩定幣具備一定價值。發行方需具有一定數量之法定貨幣或實質資產，並按比例發行虛擬通貨。法定資產抵押型是目前國際主要穩定幣採行之模式，並為經美國紐約州金融服務廳 NYDFS (下稱「**DFS**」)核准之擔保模式。目前已獲 DFS 核准並核發牌照之法定資產抵押型穩定幣共計超過 30 種幣種[204]；
2. 虛擬通貨資產抵押型穩定幣：與法定資產抵押型主要區別在於係以「虛擬通貨」作為抵押擔保物，其貨幣政策多由社群投票決定，而非由發行機構單方決定。虛擬通貨資產抵押型穩定幣是目前去中心化金融應用（Decentralized finance, Defi）主要採行之擔保模式，此模式目前未受各國政府之監管。。
3. 演算法穩定幣：係透過演算法和智慧合約來管理發行之虛擬通貨，其貨幣政策類似於中央銀行之貨幣控管，以控制市場上虛擬通貨之發行量確保市場價格之穩定。演算法穩定幣並沒有法定資產或其他虛擬通貨做為擔保，此模式目前亦未受各國政府之監管。

(二)現行法尚無針對穩定幣等相關業務訂定有監管法令

1. 經本所研究團隊研析，目前國際上有外國主管機關將穩定幣納入其金融支付監管框架下，例如新加坡於 2019 年修正通過之支付服務法（Payment Services Bill），該法案規範之「E-money」包含以任何數位方式儲存貨幣價值[205]；瑞士 FINMA 於 2019 年發布之 Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin

[204] https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/approved_entities_number (last visited: Mar. 05, 2021).

[205] NEW YORK STATE, Virtual Currencies Number of Entities Approved to Use Coin, https://www.mas.gov.sg/news/speeches/2021/payment-services-amendment-bill (last visited: Mar. 05, 2021).

offerings 法案，亦明確將穩定幣納入其監管範圍。

2. 我國於 2020 年 10 月 25 日立法院三讀通過修正電子支付機構管理條例（下稱「管理條例」），將電子支付、電子票證整合管理，未來不同電支平台，也能相互轉帳，並可進行外幣買賣、紅利整合折抵等多項新業務，以打造完整支付生態圈，惟查穩定幣等業務並未納入於我國電子支付機構管理條例之範疇，故我國**除洗錢防制法外，現行法尚無針對穩定幣等相關業務訂定有監管法令。**

3. 管理條例第 3 條規定：「本條例所稱電子支付機構，指經主管機關許可，以網路或電子支付平台為中介，接受使用者註冊及開立紀錄資金移轉與儲值情形之帳戶...。」，依照本條規定，電子支付機構為金融特許行業之一。

4. 另依電子支付機構管理條例修正草案總說明，金管會表示[206]：「電子支付機構業務項目，包含以實質交易為基礎之『代理收付實質交易款項』、吸收社會大眾資金之『收受儲值款項』及非以實質交易為基礎資金移轉之『電子支付帳戶間款項移轉』等，涉及金融特許範疇，業務型態介於銀行等收受存款機構與電子票證發行機構之間」，因此電子支付機構亦涉及金融特許範疇，業務形態介於銀行等收受存款機構與電子票證發行機構之間，故依照現行法解釋，虛擬通貨服務似並非電子支付機構業務項目。

[206] https://lci.ly.gov.tw/LyLCEW/agenda1/02/pdf/08/06/02/LCEWA01_080602_00109.pdf，最後瀏覽日: 2021 年 4 月 15 日。

第四節　我國法院實務之主要虛擬通貨犯罪類型

第一項 我國虛擬通貨涉及犯罪類型及統計

經本研究團隊於司法院法學資料庫上之判決檢索結果，自 2016 年起至 2021 年 9 月 27 日止以虛擬通貨、虛擬貨幣、加密貨幣為關鍵詞所搜索之法院刑事裁判共計 919 筆，扣除雖提及上述關鍵字但與案情無實質關聯之判決，實際分析共計 819 筆。於此 819 筆法院判決中，依據被告應用虛擬貨幣於犯罪中之方式，本研究團隊認為依據犯罪罪名及虛擬貨幣遭應用之方式，可初步歸納以下為六大犯罪類型：

一、交易標的型

本類型案件於 2018 年開始迅速增加，並於 2020 年達到高峰，經檢視，迅速增加之案件來源主要與近年虛擬通貨虛偽買賣、侵占、投資糾紛有關。此類案件為目前數量最多之案件類型，總計 432 件，占所有案件總數之 53%。

圖12

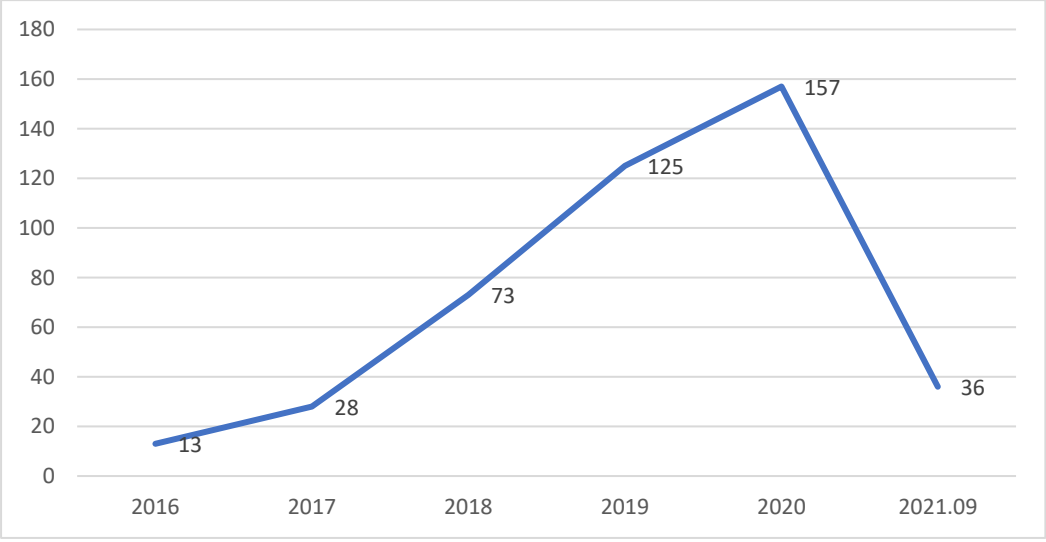


圖 32 歷年交易標的型案件數量趨勢圖

資料來源：本研究團隊自製。

(一)犯罪流程

被告以虛擬貨幣作為投資或買賣標的。基本手法為詐騙集團訛

稱可販售虛擬貨幣，或辦理虛擬貨幣說明會進行詐騙、吸金致使告訴人受騙上當而匯入款項。

(二)臺灣高等法院 107 年度金上訴字第 83 號判決

被告等人，透過網際網路對公眾散布以類似「老鼠會」的方式，招攬民眾將比特幣投入被告向幣託公司申請使用之幣託帳戶後，再依照投資者投入比特幣之順序，後一輪次投資者投入每滿 3 枚以上之比特幣，前一輪次投資者即可依所投入之 1 枚比特幣，獲得 2.5 倍的比特幣（即 150%之獲利），被告再從中抽得比特幣為佣金。

本案法院認為被告等構成三人以上共同以網際網路對公眾散布而犯加重詐欺得利罪。

本案特色有二，第一，雖以被告等人所為乃典型老鼠會之犯罪手法，惟判決認定被告等人不成立銀行法之違法經營收受存款業務罪，理由在於，銀行法第 125 條第 1 項之違法經營收受存款業務罪所謂「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)；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。而銀行得吸收之「資金」，雖非以通行貨幣為限，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。我國發行貨幣之主管機關即中央銀行、銀行法主管機關即金管會，目前仍否定比特幣具有貨幣性質(銀行等金融機構不得收受、兌換比特幣)，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，故被告等人不成立銀行法第 125 條第 1 項前段之違法經營收受存款業務罪。

第二，本案虛擬通貨價額之換算，經法院認定本案應沒收之犯罪所得係 1,158.715 枚比特幣，然被告已將詐得之比特幣轉賣或轉出一空，爰以犯罪行為時點及 105 年 3 月 6 日至 16 日間比特幣買賣新臺 28 幣平均均價 13,463 元加以估算，1,158.715 枚比特幣換算為 29 現金，總計為 15,599,780 元，扣除前述被害人已實際受償之 366,300 元，為 15,233,480 元，此即為被告等人將詐得比特幣變得現金後所應沒收之數額。

(三)臺灣高等法院台中分院 106 年度上訴字第 1014 號判決

被告為「數位比特股份有限公司」（下稱數位比特公司）之負責人。數位比特公司經營網路虛擬貨幣「比特幣（Bitcoin）」之交易平臺（下稱本案操作平臺），交易方式為加入前開網站之會員，得上網登錄欲買入或賣出之比特幣數量與單價，待該交易平臺撮合後完成交易，數位比特公司則針對前開交易收取手續費以牟利。另依數位比特公司之規定，買方欲購買比特幣時，需先將購買之現金匯入數位比特公司開設在下稱遠東商銀之帳戶，經數位比特公司員工確認匯入金額無誤後，再通知本案交易平臺核可，此後會員方得將賣方所欲出售之比特幣，以變更電磁紀錄方式，移轉至買方之電子錢包；反之，賣方欲出售比特幣時，則需先支付比特幣至數位比特公司，買方則循前開購買比特幣之方式，以確保本案交易平臺撮合之交易，買賣雙方均得拿到現金或比特幣。詎料，被告在本案網際網路交易平臺上，虛偽刊登欲以高於市場行情之價格購入比特幣之訊息，致使賣家誤認為有人願以高於市值之價格購買比特幣，又在數位比特公司網路上刊登延後支付賣家款項之公告，以拖延賣家發現遭詐騙之時間，續刊登將調漲賣幣手續費之公告，促使賣家儘速將比特幣轉至本案交易平臺出售。被告以此方式騙取被害人所出售之比特幣，被告並將前開詐騙取得之比特幣輾轉移至電子錢包藏匿、變賣。

本案被告遭判網際網路對公眾散布而詐欺得利罪，本案判決特色有二，其一在於法院認為數位比特公司會員與遠東銀行間乃消費寄託關係，消費寄託即應適用民法關於消費借貸之規定，其金錢之所有權即已移轉於受寄人，故受寄人嗣後提領該帳戶內款項供己支用，係屬處分自己財產之合法行為，縱然因此而未能返還相同數額之金錢予寄託人，亦屬民事債務不履行問題，與侵占刑責要屬無涉。故數位比特公司會員為購買比特幣而匯入遠東商銀帳戶內之款項，於匯入後即歸遠東商銀所有，數位比特公司則對遠東商銀取得相同數額金錢之返還請求權，而各該會員對數位比特公司依彼此其間之約定，僅取得於比特幣交易平台撮合交易成功後之支付比特幣請求權，或未撮合交易時之價金返還請求權。故被告以數位比特公司負

責人身分實際上並未持有各該會員所寄託之款項，縱其因其他原因逕將數位比特公司在遠東商銀帳戶內之款項提領或轉匯他用，致無法返還相同數額款項予各會員，揆之前揭說明，自不能構成侵占罪。

第二，本案法院認為於宣告沒收時，被告所詐取者既為比特幣，其犯罪所得即該比特幣，原判決卻逕將各該被害人出售比特幣時價當成沒收標的，於法未洽；仍應先宣告沒收比特幣，並於全部或一部不能沒收或不宜執行沒收時，始追徵其價額。

二、交付個人資料型

被告涉及提供金融帳戶、手機門號等個人資料，或擔任詐騙集團車手，而遭訴以幫助詐欺或洗錢罪之案件。此類犯罪手法並非新穎，然而與虛擬通貨為名目者於 2018 年開始逐年增長，並在 2021 年突然大幅增加。此類案件為目前數量第二多之案件類型，總計 222 件，占所有案件總數之 27%。

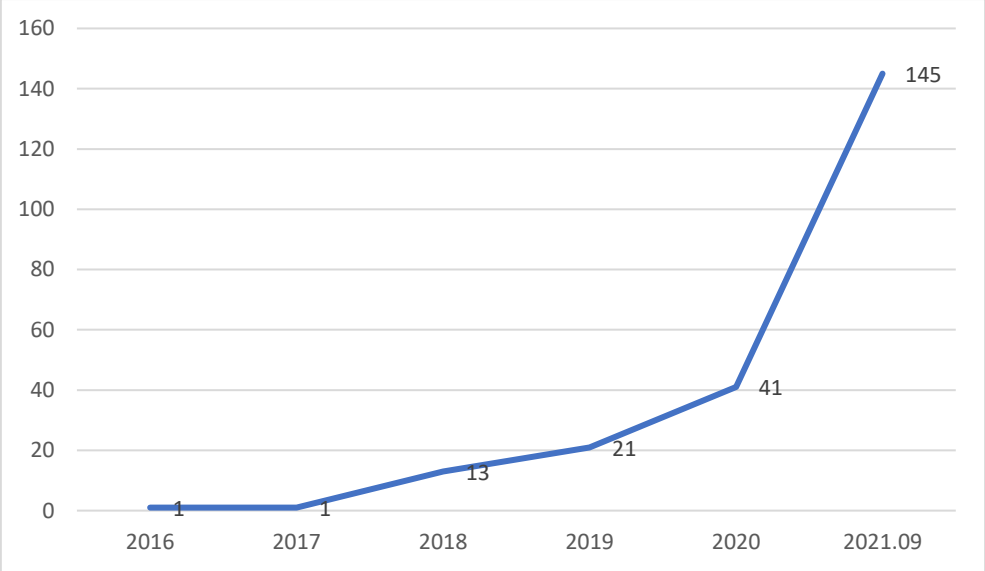


圖 33 歷年交付個人資料型案件數量趨勢圖

資料來源：本研究團隊自製。

本類型案件於 2021 年開始增加之原因可能為虛擬通貨市場交易活絡，因而導致詐騙集團改以虛擬通貨之投資、買賣為名目來吸收個人金融帳戶資料及車手。

(一)犯罪流程

此類案件之典型犯罪流程，依據案件與虛擬貨幣有關之原因可再分為兩種。一種為被害人係因誤信詐騙集團偽稱之販賣、投資虛擬貨幣等訊息因而匯款至被告之金融機構帳戶，嗣被害人發覺遭詐騙後告訴犯罪，例如：臺灣新竹地方法院110年度金簡上字第8號刑事判決、臺灣臺北地方法院刑事判決110年度易字第123號。

另一種為詐騙集團以教導虛擬貨幣投資、代操虛擬貨幣帳戶或提供虛擬貨幣工作機會為餌，吸收被告等提供包括金融帳戶、手機門號等個人資料或擔任車手，例如：臺灣高等法院臺南分院 110 年度金上訴字第360號刑事判決、臺灣臺中地方法院110年度金訴字第184號刑事判決，惟部分被告辯稱乃係因對虛擬通貨之交易模式不熟悉，始誤信虛擬通貨交易有必要提供個人金融帳戶帳號密碼。上述兩種類型之被告均係因交付個人資料或擔任車手而成立犯罪，但依據虛擬貨幣用作與被害人間之交易名目還是與被告交易之名目有所不同。

又，被告交付之資料除金融機構帳戶外，因應我國主要虛擬通貨交易所之用戶，均應於註冊時提供行動電話門號以供驗證，故本類型判決中近年開始出現與虛擬通貨有關之人頭門號案件，即被告將其使用行動電話門號及電子郵件信箱提供予詐欺集團成員供其向虛擬通貨交易所申辦數位貨幣帳戶使用因而成立幫助詐欺案件，例如：臺灣彰化地方法院 108 年度金訴字第86號刑事判決、臺灣臺北地方法院109年度審簡字第318號刑事簡易判決。

(二)嘉義地院110年金訴字第133號刑事判決

被告於民國109年10月26日向現代財富科技有限公司申請MAX虛擬貨幣儲值帳戶（下稱「虛擬帳戶」），並綁定其向京城商業銀行申設帳戶（下稱「京城銀行帳戶」），復於109年10月29日至京城商業銀行辦理該京城銀行帳戶之網路銀行約定帳戶為虛擬帳戶，再於109年11月2日在不詳地點，將上開京城銀行帳戶之存摺、提款卡(含密碼)、網路銀行代號(含密碼)、上開虛擬帳戶代號(含密碼)及其國民身分證統一編號等資料，以不詳之方式交予真實姓名不詳之詐

欺成員(無證據證明為三人以上)，供該詐欺成員使用。進而以此方式幫助詐欺集團成員詐欺取財與洗錢，使被害人陷於錯誤，匯款如本判決附表所示之金額至上開京城銀行帳戶內，隨即遭詐欺成員以智慧型手機連結網路，再以被告提供之網路銀行代號等資料，以被告身分登入京城商業銀行 APP 之方式，自上開京城銀行帳戶，將款項先後匯出至虛擬帳戶內而提領一空，並為詐騙款項去向之隱匿。嗣被害人發覺遭騙，乃報警循線查悉上情。

本案法院認以，金融機構之存摺、提款卡(含密碼)、網路銀行帳號及密碼及國民身分證等資料，事關存戶個人財產權益之保障，一般人均妥善、親自保管。若遺失者發現帳戶資料不見，必會立即掛失、變更密碼並報案；再者，金融機構開設帳戶，請領存摺及提款卡，係針對個人身分之社會信用而予以資金流通，具有強烈之屬人性格，且均係與個人隱私有密切關係之重要物件，一般人若非基於特殊目的或情誼，斷無任意交由他人保管或使用之理。被告對將己有且具有個人專屬性之物品交付他人，極可能遭行騙者用作詐取財物之工具，衡情應有所預見，竟猶將之交付他人使用，顯有容任犯罪事實發生之本意，亦堪認定。是被告主觀上有幫助詐欺取財及洗錢之不確定故意甚明。

本案判決特色在於法院認定被告為智識能力正常之人，其交付京城銀行帳戶與不詳之人，主觀上當有認識他人取得人頭帳戶之目的係為不法用途，金流經由人頭帳戶被提領後將產生追溯困難之情，是以被告仍提供帳戶資料以利洗錢實行，同時另成立幫助洗錢之行為。

三、交付虛擬通貨帳戶型

目前我國主要幾大虛擬通貨交易所於申辦帳戶時均應踐行使用者實名制認證程序，使用者應提供個人姓名、手機帳號、郵件信箱等資訊並驗證後始得開始進行交易。本類交付虛擬通貨帳戶型基本手法為被告將自己於虛擬通貨交易註冊之帳戶，出租或出賣予詐騙集團成員使用，因而成立幫助詐欺或洗錢罪。

此類案件於 2018 年前未曾出現，乃 2018 年開始之新興犯罪類型，近年數量並快速成長。此類總計案件數量 63 件，占所有案件數量之 8%。

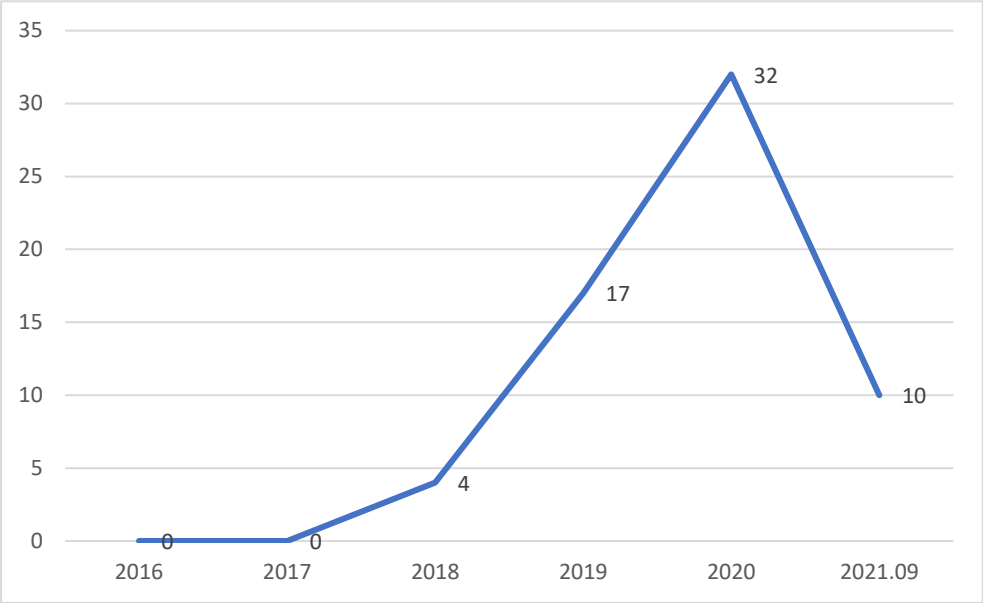


圖 34 歷年交付虛擬通貨帳戶型案件數量趨勢圖

資料來源：本研究團隊自製。

(一)犯罪流程

典型之犯罪流程為被告先向虛擬通貨交易所申辦虛擬通貨交易帳戶後，復將虛擬通貨帳戶出租或是出賣予詐騙集團成員使用，嗣詐騙集團成員再向被害人訛稱交易，並要求被害人以虛擬通貨來支付交易價金，使被害人至超商列印繳款帳單，而以新台幣繳費後使指定數量之虛擬通貨匯入被告所申設之虛擬通貨帳戶，例如：臺灣桃園地方法院 109 年度壢簡字第 1151 號刑事判決、臺灣高雄地方法院 109 年度簡字第 3481 號刑事判決均屬之。

(二)臺灣高等法院 109 年上訴字第 4067 號刑事判決

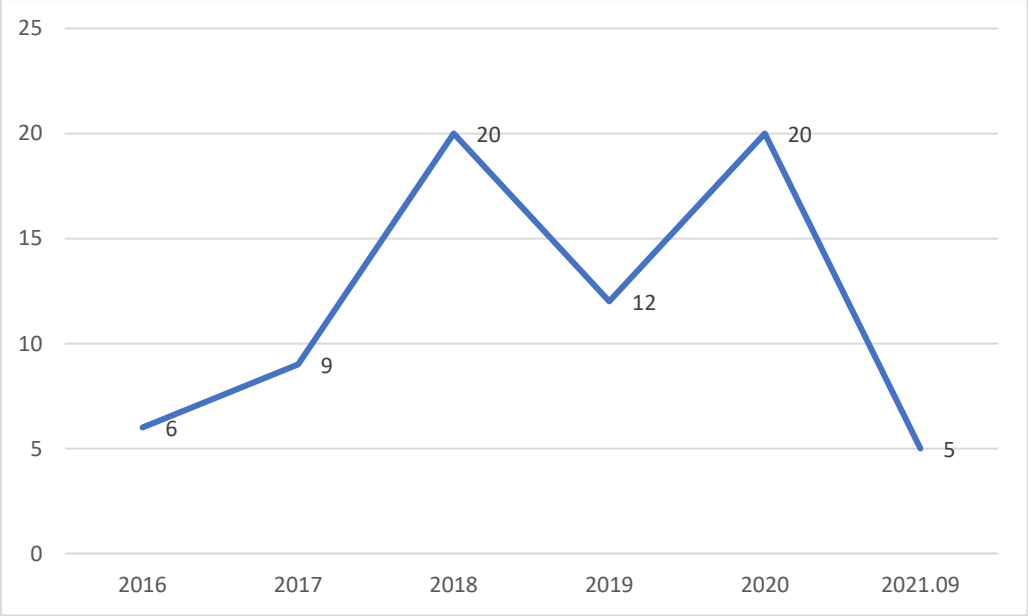
被告於民國 108 年 7 月 7 日將其透過在泓科科技有限公司（下稱泓科公司）所架設之 BitoEX 平臺，經泓科公司驗證、以電子郵件信箱申辦之兩個比特幣虛擬貨幣帳戶交付予真實姓名不詳、LINE 暱稱「林彥宏」之成年人及其所屬之詐欺集團成年成員使用。嗣詐騙集

團成員向被害人佯稱欲進行全套按摩服務，須購買 eGASH 點數及第三方支付繳費方式購買虛擬貨幣比特幣云云，致李○諠陷於錯誤，至萊爾富北縣平安店購買 1 千元 eGASH 點數，並至全家便利商店中和景平店內操作「Fami Port」機臺，列印代碼繳費序號繳款憑證，支付兩筆 2 萬元（合計 4 萬元）購買比特幣至上訴人所申設之上開兩個比特幣虛擬貨幣帳戶內。法院認以被告就上開事實，係犯刑法第 30 條第 1 項前段、第 339 條第 1 項之幫助詐欺取財罪。

本案特色在於被害人為未成年人，故判決理由中就是否應適用兒童及少年福利與權益保障法第 112 條第 1 項規定：「成年人教唆、幫助或利用兒童及少年犯罪或與之共同實施犯罪或故意對其犯罪者，加重其刑至二分之一。但各該罪就被害人係兒童及少年已定有特別處罰規定者，從其規定」有所討論，惟法院認為被告雖對詐欺集團成員之詐騙行為提供助力，惟並非直接對被害人行騙之人，自難逕認被告業已知悉或可得而知其等之詐騙對象有仍屬少年之情。是以，此部分尚毋庸改以幫助成年人故意對少年犯詐欺取財罪論處。

四、支付對價型

本類型案件為被告利用虛擬通貨之隱密、便利性，將虛擬貨幣作為交易對價用作買入、販出違禁物品之價金或，因而成立違反毒品防制條例或是懲治走私條例等罪名。此類總計數量 72 件，占所有



案件數量之 9%。

圖 35 歷年支付對價型案件數量趨勢圖

資料來源：本研究團隊自製。

(一)犯罪流程

典型之犯罪流程為被告透過通訊軟體或是遊戲對話紀錄達成購買毒品之合意，再以具有經濟價值之遊戲幣或虛擬通貨作來支付買受毒品之價金，例如臺灣彰化地方法院刑事判決 110 年度訴字第 140 號、臺灣高等法院 109 年度上更一字第 206 號刑事判決均屬之。

我國法院判決最早於 2017 年開始出現以比特幣支付毒品價金之案件，但在此之前，亦有使用遊戲幣來購買毒品之案例。此外，被告支付虛擬貨幣之方式包含透過匿名暗網、非中心化交易所之錢包或超商之繳費機台等。

(二)案例分析

被告於持其所有 SAMSUNG 廠牌行動電話 2 具連接網際網路，並以暱稱「黃小洋」登入網路「星城 Online」遊戲，以網路「星城 Online」之訊息為聯絡工具，與網路「星城 Online」遊戲上與甲 OO，雙方約定以新臺幣（下同）1,500 元之價格，由被告販賣甲基安非他命 1 公克及愷他命煙 1 支予甲 OO；本件毒品交易對價為 1,500 元，證人被告販售甲基安非他命後，係向證人收受星城遊戲幣。被告係犯毒品危害防制條例第 4 條第 2 項、第 3 項之販賣第二級毒品罪、販賣第三級毒品罪。

五、不法所得洗錢型

本類型犯罪為將虛擬貨幣用作不法所得之洗錢，被告先實施詐騙、竊盜等前置犯罪後，再將詐騙、竊盜等不法所得透過兌換為虛擬貨幣、或是轉入非實名制之虛擬通貨錢包來形成金流斷點，因而成立洗錢罪名。此類型為於 2018 年方開始出現之新興犯罪案件，總計案件數量 15 件，占所有案件數量之 2%。

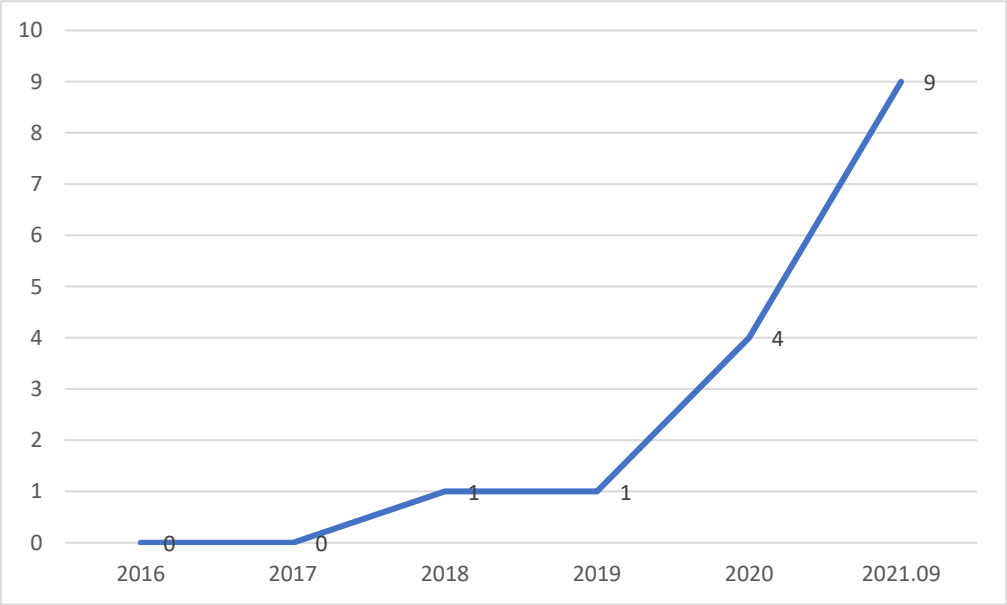


圖 36 歷年不法所得洗錢型案件數量趨勢圖

資料來源：本研究團隊自製。

(二)犯罪流程

典型之犯罪流程為被告向告訴人詐得新台幣或虛擬通貨後，再將虛擬通貨轉入非實名制之虛擬通貨錢包，致偵察機關難以追蹤犯罪流向，例如：臺灣臺北地方法院 109 年度訴字第 940 號刑事判決。另有涉及跨境洗錢犯罪者，例如臺灣臺中地方法院 110 年訴緝字第 45 號刑事判決、臺灣高等法院臺中分院 109 年度金上訴字第 1503 號刑事判決，為被告等先將詐欺所得之人民幣贓款轉匯至人頭帳戶後，將人頭帳戶款項兌換為虛擬通貨，再將虛擬通貨轉回新台幣轉匯或現金提領回台。

(二)臺灣臺中地方法院 110 年訴緝字第 45 號刑事判決

被告犯罪事實分為「轉帳洗錢水房」與「電信機房詐欺」兩部

分，而其中與虛擬通貨洗錢有關聯為前者，以下僅析論「轉帳洗錢水房」之部分，合先敘明。

轉帳洗錢水房之犯罪手法，及洗錢流程分述如下：

1. 首先，通訊軟體 SKYPE 暱稱「變形金剛」、「五路財神世界盃介紹」等詐欺機房以不詳方式，向大陸地區人民施用詐術，致大陸地區人民陷於錯誤，依指示將受騙款項匯進「變形金剛」、「五路財神世界盃介紹」等詐欺機房提供之大陸地區人頭金融帳戶（俗稱大車）

2. 許文濱等人會於入帳前5分鐘進行「洗車」（即透過小額捐款至中國社會福利基金會等帳戶以測試「水舞鑽」水房向車商取得之人頭金融帳戶未遭凍結）

3. 確認人頭帳戶可用後，通知客戶（即變形金剛等詐騙集團）可將詐騙所得款項（俗稱「草」，即大陸人民幣）匯入人頭帳戶

4.隨即透過U盾操作先將「變形金鋼」、「五路財神世界盃介紹」等詐欺機房詐騙所得之人民幣款項陸續轉入「水舞鑽」水房自行使用之大陸地區人頭金融帳戶。

5. 接著，透過「支付寶」將該人民幣款項轉入幣商「四方金梨子」指定之大陸地區人頭金融帳戶，同時由「四方金梨子」依草/比特幣匯率、比特幣/USDT（泰達幣）匯率換算後，直接將虛擬貨幣 USDT 轉至水舞鑽水房指定之梁瑞麟（即被告）及劉承訓以實名認證申請註冊之幣安平台 USDT 電子錢包充值地址（即將人民幣轉換成 USDT 幣之流程）。

6. 再來，水舞鑽水房再將 USDT 轉至幣商「王陽明」等指定之 USDT 電子錢包充值地址，水舞鑽水房老闆劉附易再指派集團成員外務黃洺智及許文濱拍攝其等身上之新臺幣鈔票號碼，張貼至通訊軟體 TELEGRAM「水舞鑽」群組，再由劉附易將前揭鈔票照片轉貼至通訊軟體 TELEGRAM「馬雲專屬群」群組予幣商「王陽明」作為標記，並由水舞鑽水房外務黃洺智與許文濱復依劉附易指示至指定地點，出示身上之鈔票（鈔票號碼須與通訊軟體 TELEGRAM「水舞鑽」群組上之鈔票號碼相同）予幣商「王陽明」確認，向「王陽明」

收取新臺幣現金（即將 USDT 幣轉換為新台幣現金之流程）。

7. 最後，外務黃洺智及許文濱前往約定地點將收取之新台幣現金轉交予「變形金剛」、「五路財神世界盃介紹」等詐欺集團指定之水房外務或機房外務。

其中，水舞鑽水房會依「水舞鑽遊戲規則」向客戶收取平台水服務費，依客戶係轉一層帳戶後再匯款至「水舞鑽」水房所提供之金融帳戶，或客戶係轉二層帳戶後再匯款至水舞鑽所提供之金融帳戶，分別向客戶收取 3.5%或 3%服務費，並以通訊軟體 TELEGRAM 或 SKYPE 對帳後製作業績表。

就本判決定罪之重要證據，詳參下表：

證據編號	扣押物編號	定罪證據	詳細內容
2	5-2	林偉翔座位電腦 1 台	列印資料
10	5-10	IPHONE 廠牌手機 1 支	(1)簡訊內容
			(2)六六大順與變形金剛 6.5%收 2.51 之 SKYPE 對話紀錄
23	6-3	遭拔除之硬碟(一)	列印資料
24	6-4	遭拔除之硬碟(二)	擷取列印之「089547.xlsx」檔案資料
42	7-18	ASUS 筆電 1 台（硬碟丟棄至屋外）	(1)水舞鑽與變形金剛 SKYPE 對話紀錄截圖
			(2)TELEGRAM 聯絡人截圖及 SKYPE 聯絡人截圖
			(3)水舞鑽水房業績統計表（即附表一）
			(4)中國農業銀行之交易明

			細
			(5)Chat Message 之對話紀錄
			(6)洪金寶與水舞之 message 對話紀錄
			(7)時捷與水舞之 message 對話紀錄
			(8)888 群組之 message 對話紀錄
			(9)STD 報價群組之 message 對話紀錄
			(10)王浩然 wsa0000000 雲端資料/彼特幣/車單檔案資料、王浩然 wsa0000000 雲端資料/彼特幣/彼特幣帳戶檔案資料、王浩然 wsa0000000 雲端資料/彼特幣/LB 客戶/客戶名稱檔案資料、王浩然 wsa0000000 雲端資料/支付保流程/支付保帳號檔案資料、桌面/新文字文件檔案資料及六六出貨資料及桌面/新增資料夾/帳之檔案資料
			(11)水舞鑽與【客】鵬程車業、【客】五路財神世界盃介紹及【客】變型金鋼之 SKYPE（Chat Message）對話紀錄
43	7-19	ASUS 廠牌筆電資料光碟	(1)水舞鑽遊戲規則
			(2)水舞鑽群組之對話紀錄

		片 1 片	(3)馬雲專屬群群組之對話紀錄
			(4)馬雲與水舞之對話紀錄
			(5)煙捲與水舞之對話紀錄
			(6)107 年 8 月 18 日起至第 107 年 8 月 31 日之水舞鑽水房業績表
44	8-1	銀聯卡及相關資料 1 袋	資料與照片

依據上表所列之證據，本判決認定水舞鑽水房之洗錢流程，以及被告確實有提供其自拍照、身分證正反面等資料，供水舞鑽成員申請幣安平台之 USTD 帳戶等事實。

被告可預見提供其與劉承訓之自拍照、身分證正反面影本，供許文濱等人申請幣安帳戶，可能淪為許文濱等人所屬「水舞鑽」水房洗錢之工具，並因此遮斷金流而掩飾或隱匿特定犯罪贓款之去向、所在，竟仍以縱係如此亦不違背其本意而為之，主觀上係基於幫助犯一般洗錢罪之不確定故意，且所為係屬一般洗錢罪構成要件以外之行為。

是被告就轉帳洗錢水房之犯罪事實部分所為，係犯係犯刑法第 30 條第 1 項前段、洗錢防制法第 14 條第 1 項之幫助一般洗錢罪。另外，被告以一提供其與劉承訓之自拍照、身分證正反面影本，供許文濱等人申請幣安帳戶之行為，幫助許文濱等人所屬水舞鑽水房，犯本案一般洗錢罪 17 罪，為一行為觸犯數罪名之幫助想像競合犯，應從重論以幫助一般洗錢罪 1 罪。又被告係基於幫助之犯意，幫助「水舞鑽」水房成員實行一般洗錢罪，並未實際參與洗錢之犯行，所犯情節較正犯輕微，就被告所涉幫助一般洗錢罪部分，爰依刑法第 30 條第 2 項規定，按正犯之刑減輕之。

六、挖礦竊電型

本類型犯罪為被告等設置機房及設備以進行虛擬通貨挖礦，為供挖礦所需電力，以私接導線等手法竊取電能而成立竊盜罪。

本類型犯罪為 2019 年開始出現之新興犯罪類型，總計案件數量 12 件，占所有案件數量之 1%。

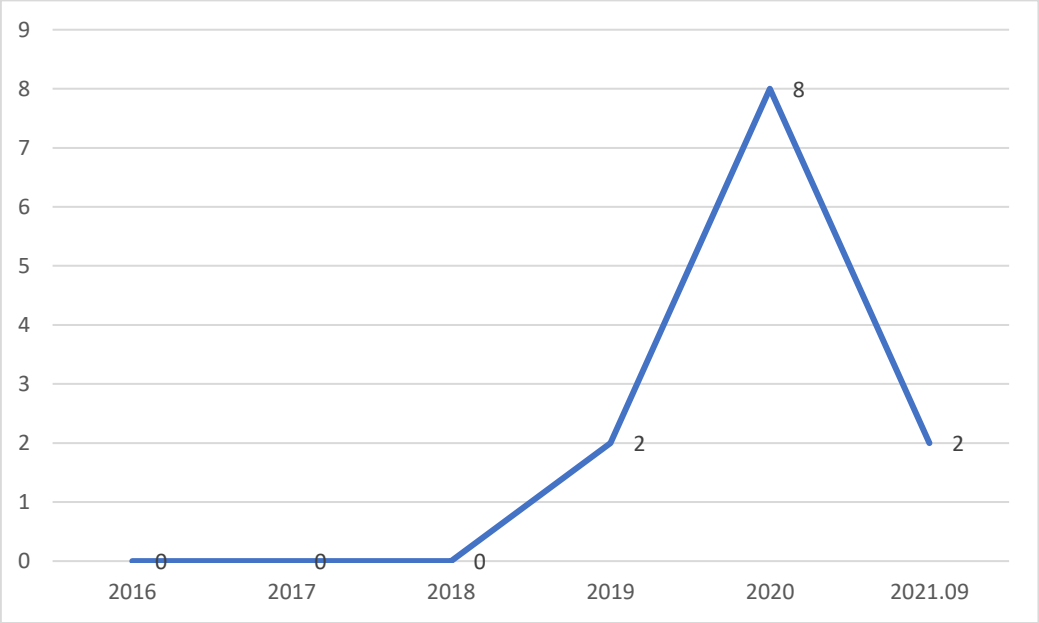


圖 37 歷年挖礦竊電型案件數量趨勢圖

資料來源：本研究團隊自製。

(一)犯罪流程

虛擬通貨之挖礦原理為利用電腦運算力進行密碼學之運算解碼以獲取虛擬通貨，因而易造成大量耗電。本類型案件之典型流程為被告等設置挖礦機房，並使用剝皮刀、壓著鉗、螺絲起子及虎頭鉗等工具，私自以 PVC 電纜線連接分流繞越電表或與其它店號電錶組合，繞越電錶計費，以供特定挖礦設備使用，自台灣電力股份有限公司竊取電能使用，例如臺灣嘉義地方法院 109 年易字第 82 號刑事判決。

(二)臺灣嘉義地方法院 109 年易字第 82 號刑事判決

被告知悉以電腦相關設備從事虛擬貨幣「萊特幣」之探採（即俗稱的「採礦挖幣」，下將該行為稱採礦挖幣），於民國（下同）107 年 8 月 13 日至 108 年 9 月 2 日，在嘉義縣竹崎鄉灣橋村、民雄鄉文

隆村、中埔鄉安家厝段等地點 ，使用剝皮刀、壓著鉗、螺絲起子及虎頭鉗等工具（下稱「竊盜工具」），私自於接戶點後，以 PVC 電纜線連接分流繞越電表於被告之特定設備使用，而未經電表計費，或於本電表之負載側 C 相與電號:00-0000-00 之電表 N 相跨接組合使用，未經電表計量繞越電表等方式，從台灣電力股份有限公司（下稱「台電公司」）接續竊取電能使用，共計 821,804 度電力，直至台電公司嘉義區營運稽查人員發現上情，於 108 年 8 月 3 日偕同警方至上述處所進行搜索扣押為止。經法院認定被告係犯刑法第 323 條、第 321 條第 1 項第 3 款之攜帶兇器竊取電能罪。

本案判決特色有二，一為被告雖因挖礦取幣進而竊電之行為將構成刑法第 323 條竊取電能罪，惟因使用之工具被認定具有兇器性質，而依刑法第 321 條第 1 項第 3 款：「攜兇器而犯之」加重條款，構成加重竊取電能罪。

第二，判決中提及挖礦機之運作原理，依據證人證言指出，依據查緝經驗，挖礦機通常都是 24 小時運作，因為是利用機器作解碼動作才能挖礦。並且，本判決函詢內政部警政署刑事警察局、法務部調查局關於虛擬貨幣挖礦機運作之時間等問題，前者回覆稱「因虛擬貨幣挖礦之主要目的為獲取虛擬貨幣，故通常會利用相關設備 24 小時不間斷進行挖礦，以提高獲取虛擬貨幣之機會或數量；惟行為人亦可依自身條件或其他考量，逕行設定挖礦之行為，故若行為人每日均固定設定一段期間中斷不進行挖礦之情境，難謂是否符合理性」，後者回覆稱：「謂『挖礦』，係提供電腦等設備之運算資源，用以維護虛擬貨幣公開帳本並獲取獎勵之機制，投入越多運算資源，可取得獎勵之機會越高，故『24 小時不間斷進行挖礦』屬常見行為，惟挖礦易造成大量耗電、設備過熱等問題，因此不排除礦工設定部分時間暫停挖礦之可能性」。本判決認為，24 小時不停挖礦取幣，利用機器解碼挖礦，係一般情形，但並非絕對，無法排除行為人每日均固定設定一段期間中斷不進行挖礦之可能性。故基於相關事證，以及罪證有疑利於被告法則，仍認定被告之竊電行為係每日僅運轉早上 7 時至晚上 10 共 15 小時。

另外，除上述本判決揭示之重點外， 1.將竊取之電能供挖礦設備運作使用，而用於挖礦取幣，所獲得之虛擬貨幣，該等虛擬貨幣是否能應認作係犯罪所得？若應認作為犯罪所得，則如何計算其價額？2.台電公司及其員工是如何發現被告有大量用電之情形，進而發現被告係在竊取電能，並用於挖礦取幣？本研究團隊認為，上述兩點亦值得深入探究，以做為未來犯罪查緝之重點。

第二項 小結

以虛擬貨幣通貨作為投資或買賣標的、提供金融帳戶／手機門號等個人資料，或擔任詐騙集團車手，而遭訴以幫助詐欺或洗錢罪、將自己於虛擬通貨交易所註冊之帳戶，出租或出賣予詐騙集團成員使用，成為我國涉及虛擬通貨幣犯罪之前三大犯罪類型。

此外，因區塊鏈技術之特質易遭洗錢犯罪者所利用 ，而成為犯罪之洗錢工具，洗錢問題是虛擬通貨無法迴避的問題之一 。，惟我國實務判決有一特殊現象：近三年出現大量被告提供個人資料以供詐欺集團進行虛擬通貨幣詐欺洗錢罪之「幫助犯」判決。

觀察我國法院有關洗錢防制法之適用，已逐漸呈現一穩定見解 ，即認為行為人為提供個人比特幣錢包帳戶位址，或其他類型虛擬通貨之帳戶位址予詐騙集團，而該錢包位址有不法所得存入者，則原錢包帳戶位址之使用人，亦將構成洗錢防制法之洗錢罪行為主體幫助犯。亦即將虛擬通貨之錢包帳戶位址，定位為類似等同於網路詐騙案中車手所提供之銀行帳戶，然查虛擬通貨之錢包帳戶位址，為去中心化治理結構下之產物，與單一金融機構提供之銀行帳戶，性質上容有差異，未來是否有罪刑法定原則或過度擴張刑罰權之質疑，有待後續觀察。

第四章　電子支付及虛擬通貨相關犯罪之偵查及私部門協力

第一節　電子支付及虛擬通貨與犯罪相關之特性

電子支付工具在理論上存在若干利於用作犯罪工具的特性，可能構成犯罪偵查之障礙或挑戰，已受到包括 FATF 與國際學術研究文獻的重視。本研究第二章以我國司法判決實證資料為基礎，歸納得出電子支付工具於我國用於犯罪的情形，進而發現電子支付工具對我國犯罪偵查帶來的挑戰主要與以下特性——包括匿名性、多層化特性、快速性、非面對面接觸以及跨境性——有關。以下分述之。

一、匿名性

電子支付工具利用網路技術的結果，具有網路世界常見的匿名性，進而增加犯罪偵查上的困難。需強調者為，此處所指之匿名性不限於完全未使用真名的絕對匿名情形，也包括身分較容易隱藏、在追溯真實身分時需要經過較複雜程序的相對匿名情形。

具體而言，本研究第二章的研究結果顯示，許多涉及電子支付工具的犯罪有利用所謂「虛擬帳號」（或稱「虛擬帳戶」）[207]，例如台北地方法院 109 年易字第 783 號刑事判決、台北地方法院 107 年審簡字第 643 號刑事判決、台中地方法院 106 年訴字第 2311 號刑事判決等均屬之。此類犯罪係利用電子支付或第三方支付進行交易，此類支付業者於交易發生時會產生一組對應的虛擬帳號以供受款之用，犯罪人於取得該虛擬帳號後，再將該虛擬帳號告知被害人以供被害人匯入金錢，因此產生財產損害。

實務上，電子支付業者或第三方支付業者提供給網路交易買家予以匯款給賣家之虛擬帳號，係業者與銀行簽約申設之帳號。虛擬帳號原本的作用是為了保護消費者，希望作為買賣雙方交易金流的暫時中繼點，於確認賣方出貨且買方取得貨物之後，買方匯入虛擬

[207]所謂的虛擬帳號，乃相對於傳統的銀行實體帳戶而言。傳統的銀行實體帳戶為 10 至 12 碼，而虛擬帳號則比實體帳戶多了 2 至 3 碼，達到 14 至 16 碼（前幾碼多為商家自訂、金額、身分證或電話的混合編碼）。內政部警政署刑事警察局，常見詐騙案例犯罪手法及預防方式一覽表 103 年 12 月，https://ws.moe.edu.tw/Download.ashx?u=C099358C81D4876C3B9F4DB251A3E128B6568CE24EAB6398606E5A06CB34EB3F8FB4BA3CB16A8AE25A9294879A9651B34BA2391548479E7962A393612749197401FB3F6CB488F130&n=3DA6E342909BCD886AB46890B00A3E90E336EE74C02B93E20227F4D3D8E32FEA&icon=..pdf（最後瀏覽日：2021/08/13）。

帳戶的金額才會轉入賣方的實體帳戶[208]。然而由於電子支付業者對客戶審查存在缺失，常見犯罪行為人盜用他人個資創建虛擬帳號，或是幫助犯主動提供個資作為人頭供正犯創建虛擬帳號的行為。而相對於銀行實體帳戶，虛擬帳號由於創建條件較為寬鬆，與其背後真實身分的連結較不緊密，具有一定程度的相對匿名性，檢調機關雖然並非完全無法追溯虛擬帳號創建者的真實身分，但仍需要一定的資料調閱時間，因而增加犯罪偵查的困難度。

另外，實務上虛擬帳號多僅供單次使用，亦即通常於當次線上交易結束後即失效[209]，也增加了電子支付工具的相對匿名性與犯罪偵查的困難度。申言之，檢調機關固然在理論上最終可以辨識虛擬帳戶所連結的銀行實體帳戶，進而由該帳戶所屬銀行處調取資料知悉虛擬帳號連結的實體帳戶所有人身分[210]，但虛擬帳號與銀行實體帳戶不同之處在於，於犯罪人使用銀行實體帳戶時，檢調機關得於得知犯罪案件時快速凍結該實體帳戶，並且鎖定特定帳戶之持有人；反觀虛擬帳號因為僅具有與實體帳戶持有人間「間接」的連結，具有相對匿名性，付款方於受害報案時，由於僅知悉虛擬帳號數字而不知受款方身分，導致偵查單位無法直接鎖定犯罪人，而必須透過向銀行與電子支付業者調閱資料方可鎖定犯罪人，因此增加犯罪偵查的時間與成本，進而使犯罪人在此時間差內仍可重複利用虛擬帳號的手法犯案。

此外，根據偵查機關所提供之內部統計資料，亦可觀察出虛擬帳戶對於偵查上造成的負擔與困難。自 108 年及 109 年之數據以觀，有關虛擬帳戶被利用於犯罪之情形於 108 年合計 721 件，其中 593 件為不起訴；109 年合計 1,644 件，其中 1,441 件為不起訴，可知利用虛擬帳號遂行犯罪之數量正在增加，且本研究合理推論，多數案件

[208] 同前註 84。

[209] 內政部警政署刑事警察局，常見詐騙案例犯罪手法及預防方式一覽表 103 年 12 月，https://ws.moe.edu.tw/Download.ashx?u=C099358C81D4876C3B9F4DB251A3E128B6568CE24EAB6398606E5A06CB34EB3F8FB4BA3CB16A8AE25A9294879A9651B34BA2391548479E7962A393612749197401FB3F6CB488F130&n=3DA6E342909BCD886AB46890B00A3E90E336EE74C02B93E20227F4D3D8E32FEA&icon=..pdf（最後瀏覽日：2021/08/13）。。

[210] 同前註 84。

甚至可能係犯罪行為人盜用他人之資料或者以不知情之人頭創建，真正之犯人因虛擬帳號之匿名性而得以藏身於幕後。

本研究亦發現，許多利用電子支付工具進行犯罪（特別是詐騙）的案件通常係發生於網路平台的購物交易。於此種交易中，買家通常並不知悉賣家的真實身分，僅知悉應付款的繳款帳號或虛擬帳號；實務上買家甚至常至便利商店利用超商代碼繳費的方式，以現金支付至該虛擬帳號，因此除了賣家利用虛擬帳號存在相對匿名性外，即使是被害人即買家端亦存在匿名性。於犯罪人與被害人均具有某程度匿名性的情形下，無論在案件通報、調查、蒐證，甚至是相牽連案件的偵查與審理的資源利用，均可能造成一定程度的偵查負擔。

二、多層化特性

電子支付工具的另一特色，在於其增加了資金流向當中的中介業者，進而增加金流的層次與複雜性。具體而言，用戶申請創建其電子支付帳戶時，通常會綁定其既有的銀行實體帳戶，而該電子支付業者本身於銀行亦需設立專戶，因此形成「付款人銀行→電子支付業者→受款人銀行」的多層次支付體系，例如新竹地方法院 106 年易字第 1114 號刑事判決、桃園地方法院 106 年審易字第 2293 號刑事判決均屬適例。

電子支付業者中介金流的直接效果，是使得付款人的銀行與受款人的銀行均僅與電子支付業者辦理金流，故付款人銀行無法掌握受款人資訊、受款人銀行也無法掌握付款人資訊。當檢調機關進行偵查時，即不易直接從銀行端的記錄勾勒出金流全貌，而必須仰賴扮演中介功能的電子支付業者方能掌握完整的金流相關資訊。

更複雜者為，實務上亦有第三方支付業者與狹義的電子支付業者合作，因此形成更複雜的支付關係。例如狹義的電子支付業者歐付寶由於須遵守實名制等洗錢防制規範，因此要求買賣雙方均為其會員才可以歐付寶進行收付款交易，但為擴展業務，其於 2016 年 9 月起與旗下之第三方支付公司綠界科技之間達成技術合作，使來自

非歐付寶會員之金流收款由綠界科技辦理[211]。於此種情形，狹義的電子支付業者可能並未直接與付款人或受款人往來，因此並無付款人或受款人的相關資料，而第三方支付業者固然直接與付款人或受款人往來，但因其受到的洗錢防制要求較為混亂（詳下述），故可能並未充分落實相關洗錢防制程序。在此種第三方支付業者與狹義電子支付業者同時參與其中的情形，金流實際上更為複雜，檢調機關於偵查犯罪時，認定資金流向即可能面臨更大的挑戰。

三、快速性

電子支付工具具備帳戶創建的便利性，且其資金移轉過程相較於傳統金融機構例如銀行而言更為方便快速，所需的驗證程序亦較為簡便。特別是搭配行動裝置的結果，付款與收款程序可以迅速完成，此亦為電子支付工具相較於傳統支付的優勢。然而在加快交易速度的同時，電子支付工具亦因此更容易被用作犯罪工具。

例如上述以電子支付工具創設虛擬帳號的情形，由於虛擬帳號具有創建方便的特性，且如上述常僅用作單次交易，故犯罪人得以於短時間內大量創設多個虛擬帳號以供收款之用。當檢調機關接獲報案而向電子支付業者或連結銀行調取實體帳戶資料的公文往來期間，犯罪人即可以大量的虛擬帳戶遂行更多犯罪[212]。因此即使檢調機關最終得以追查至犯罪人使用的人頭幫助犯或甚至犯罪人本人，但由於電子支付工具的快速性，受害人數與規模可能在偵查過程中不斷擴大。

事實上，如本研究的司法判決實證研究顯示，電子支付工具大量被用於小額詐欺案件。然而許多小額詐欺案件的受害人數不少，犯罪期間亦可橫跨多年，例如台東地方法院 108 年原金訴字第 47 號刑事判決的案件即橫跨 2018 年至 2019 年、台中地方法院 108 年簡上

[211] 參考綠界科技 ECPay 整合金流服務平台於 2016 年 9 月 9 日之官網公告，https://www.ecpay.com.tw/Content/EDM/20160905/edm.html（最後瀏覽日：2021/8/18）；歐付寶官方網站討論版官方管理員發表，https://forum.opay.tw/forum.php?mod=viewthread&tid=429（最後瀏覽日：2021/08/18）。

[212] 同前註 84 。

字第 445 號刑事判決的案件則橫跨 2015 年至 2016 年。由此類案件的受害人數與時間分佈可知，電子支付工具的快速性可能加劇相關犯罪案件之整體受害程度，並增加檢調機關偵查的時間壓力。

四、非面對面接觸特性

電子支付服務係仰賴網路系統提供支付服務，故電子支付業者並未直接與支付服務使用者面對面接觸，而是於伺服器端透過辨識認定帳號密碼的正確性，以決定是否授予訪問或使用特定帳號之人使用權限。於此背景下，不僅電子支付工具的使用者例如交易相對人彼此間無法知悉對方的真實身分，電子支付機構本身於使用者申請設立帳戶或申請啟動特定交易時，亦面臨使用者身分辨識的挑戰，犯罪人可能冒用支付帳號持有人的身分進行交易，進而造成帳號持有人的損害。

例如於第二章所述竊用他人身分資訊並利用電子支付工具消費的情形，犯罪人可能竊取被害人的信用卡資訊進入被害人的電子支付帳戶進行線上消費付款，造成被害人的財產損失。此際電子支付業者係在辦理信用卡交易款項的代收代付服務與金流結算，於此過程中，電子支付業者係連線至刷卡認證中心自銀行取得認證，因此只要卡號與授權碼填寫正確，即會撥付款項[213]，從而不易辨識消費者實際上並非信用卡持卡人或電子支付帳戶持有人，進而不易於第一時間阻止盜用事件發生。誠然，上述盜用手法亦可能發生於實體信用卡時，例如盜用盜刷信用卡，然而電子支付工具的非面對面接觸特性，使犯罪人無須盜竊或偽造實體卡片，即可透過帳號與授權碼等方式進行認證程序，從而大幅降低盜用盜刷信用卡的成本，而可以更快速的方式遂行犯罪。

另一種常見的犯罪手法，係犯罪人一方面以賣家的身分利用社群網站張貼特定的拍賣資訊引誘被害人下單，一方面再以買家的身分向不相關的賣家購買等值商品，進而取得來自賣家的一組虛擬帳

[213] 例如紅陽科技，參見紅陽科技金流服務_信用卡─常見問題─紅陽科技全方位金流服務，http://www.msts.21tw.net/sub_7.html（最後瀏覽日：2021/08/13）。

號，犯罪人再將此賣家提供的虛擬帳號傳給被害人，指示被害人付款至該虛擬帳號，但犯罪人於取得自己購入的商品後並未出貨給被害人，造成實質上係由被害人代犯罪人向賣家付款、但被害人卻未取得其自犯罪人處購入的商品，最終等於由犯罪人取得免付費的商品，例如新北地方法院107年度簡字第103號刑事判決與新北地方法院109年審訴字第2352號刑事判決等均屬此例。此種犯罪手法之所以得以成立，亦係利用電子支付工具非面對面接觸的特性，使犯罪人得以輕易將他人的虛擬帳號挪為己用並藏身於網路之後[214]。

除上述盜用他人電子支付帳戶外，非面對面接觸的特性亦造成我國實務上常見的「盜用他人資訊設定電子支付帳戶」案例。蓋在非面對面接觸下，犯罪人只要取得他人的個人基本資料，即可經由設定一連串的帳號密碼資訊創設一個表面上屬於他人名下的電子支付帳戶，之後即可透過犯罪人設定的帳號與密碼通過認證完成所有交易，犯罪人因此可利用此不知情之他人的電子支付帳戶掩護其犯罪。於此種犯罪手法下，檢調機關在偵查時可能僅偵查到個資被盜用供申設帳戶的他人，但如無證據顯示此人有幫助犯之故意，檢調機關僅能為不起訴處分，因此增加檢調機關犯罪偵查的困難。

五、跨境性

電子支付工具係利用網路提供支付服務。由於網路無遠弗屆的特性，電子支付業者支援的支付服務可涵蓋我國境外的使用者，且可遍佈各國，因此具有一定的跨境性，可能被用作跨境犯罪的用途，進而使檢調機關面臨跨境偵查的挑戰。

本研究第二章的司法判決實證研究顯示，電子支付工具於我國用於跨境犯罪的比例雖非極高，但仍然值得關注。於本研究蒐集的案件中，涉及跨境犯罪的案件包含違法經營線上賭博平台、違法經營匯兌業務、違反多層次傳銷管理辦法等規模較大的犯罪類型。由

[214] 此類詐騙案型實務上多見，警方已列為提醒民眾之內容，詳見內政部刑事警察局、海山分局發布（2015/05/06），〈遊戲點數詐騙〉，https://www.zhonghe.police.ntpc.gov.tw/cp-2450-11749-13.html。

此可知，電子支付工具於我國用於跨境犯罪的案件數量雖然不多，但金額相對龐大，且多為持續一段期間的長期犯罪，故犯罪行為人亦相當程度地利用電子支付工具的跨境性於我國遂行犯罪。

六、執法機構查緝虛擬通貨相關犯罪之困難

虛擬通貨為廣義定義下之電子支付工具之一，同樣得利用區塊鏈網路提供同等支付服務，故虛擬通貨相關犯罪在理論上存在電子支付工具之前述五大利於用作犯罪工具的特性。除此之外，虛擬通貨尚有其他構成犯罪偵查之障礙或挑戰，以下分述之。

(一)暗網之非法活動

查緝虛擬通貨之一大挑戰為暗網的非法活動。暗網的非法活動與虛擬通貨有著密切關係，虛擬通貨使犯罪者能夠從事一些地下非法行動（例如買賣毒品）並逃避洗錢查緝，不法份子為了避免在支付虛擬通貨或資料傳輸的過程中，遭他人竊取或竊聽，許多類似洋蔥瀏覽器(Tor)[215]等匿名網路，逐漸受到重視。許多非法網站亦開始蓬勃發展。而暗網交易盛行以虛擬通貨作為支付媒介，其中以比特幣(Bitcoin)為最大宗，由於加密貨幣可隱藏用戶真實身分，又可規避政府和銀行監管，以確保交易安全及保密。根據區塊鏈分析組織 Chainalysis 研究顯示，2018 年暗網市場之比特幣交易量平均每天高達 200 萬美元[216]。如前述「絲綢之路」洗錢案，該網站在毒品買賣以外，也提供了殺手買兇及人口販運等犯罪[217]。

利用比特幣進行第三方支付是近年逐漸被世人廣為重視的一種線上支付方式。此即結合虛擬通貨（比特幣）與既有線上支付技術，透過 CNC 伺服器（Command & Control Server）[218]與網路殭屍病毒，

---

[215] 洋蔥瀏覽器(Tor Browser Bundle，官方網站 https://www.torproject.org/index.html.en)之核心技術源自於美國海軍研究 實驗室主導，與數學家、電腦科學家共同研發之秘密通訊工具，最初為軍用程式，後交由民間單位持續開發而發展為 今日所見之洋蔥瀏覽器(Tor)，由於連結該伺服器網站須穿過層層加密之節點及網路，故以洋蔥瀏覽器命名。

[216] 科技新報「2018 暗網比特幣交易量翻倍，平均每天 200 萬美元」黃彥鈞，2019 年 1 月 22 日，網址 http://technews.tw/2019/01/22/bitcoin-transactions-on-darknet-markets-double-in-2018/ （最後瀏覽日：:2021 年 6 月 5 日）。

[217] 同前註 261。

[218] https://www.itread01.com/content/1545928942.html，最後瀏覽日：:2021 年 6 月 7 日。

組合成了一種新興「複合式的犯罪態樣」及「隱匿犯罪金流」之方法。惟當犯罪行為人快速頻繁的使用比特幣進行洗錢時，同時也可能是罪犯的「致命弱點」。因為加密貨幣交易雖然隱密，但其所使用之區塊鏈使得執法機構得以依據其數據追蹤犯罪活動，實際上為執法機關提供了能夠識別「使用者」的工具；意即，執法機關多半都希望這些犯罪者繼續使用加密貨幣作為資助非法活動，因為如此查緝日漸容易。區塊鏈上的全球帳本（Global Ledger）也提供良好的線索，在無需傳喚銀行前提下，政府部門等就能檢視這些資料[219]。

防制洗錢金融行業工作組織（Financial Action Task Force on Money Laundering，FATF）監管方針建議各國應該確保虛擬資產服務商（VASPs）在移轉資金時必須保留發送方以及受款方必要且精準的用戶訊息，並將這些訊息提交給受款方的機構，而隱私幣的主要特色與這些監管方針似乎有所衝突，多數隱私幣都強調「完全匿名且不可追蹤」，這樣也讓隱私幣幾乎無法達成 FATF 對虛擬資產服務上保留用戶資訊的要求[220]。然而，根據美國緝毒署（DEA）資料顯示，雖然比特幣以外之隱私幣為更具有吸引力的替代品[221]，但它們目前規模太小，且現行世界主要虛擬通貨交易所均下架隱私幣導致其市場流動性不足，無法在比特幣以外成為罪犯可行的支付工具。

我國數件涉及比特幣相關犯罪案件，例如以比特幣進行詐欺行刑事犯罪為例，不法分子以比特幣作為詐欺騙取財物之標的，而非以法幣作為不法吸金之標的，遂行詐欺得利罪，迥異於傳統吸金手法(臺灣高等法院刑事 107 年度金上訴字第 83 號判決)；臺北地方法院亦曾於 2013 年判決一例關於涉嫌人利用網路下載匿名上網瀏覽器套件軟體 Tor 後，再登入 Mt.Gox 比特幣交易網站開立帳戶，匯入相當數額之美金後，再登入「絲綢之路」網站以比特幣付款予墨西哥、義大利籍賣家購買二級毒品大麻並運送至國內指定地點，因而違反

[219] 蘇文杰、李穎、葉永全(2018)，毒品交易虛擬金流偵查新模式－以本局與荷蘭警方合作偵查個案為例，107 年毒品犯罪防制工作年報，頁 95。

[220] 比特幣以外之 Monero 門羅幣和 Zcash 等較具隱私性之虛擬通貨，https://www.blocktempo.com/okex-korea-fatf-delisting-5-privacy-coins/ ，最後瀏覽日：:2021 年 6 月 7 日。

[221] 蘇文杰，同前註 219，頁 95。

毒品危害防制條例（臺北地方法院102年訴字第222號、第644號判決）。除了人頭帳戶問題外，販毒者為了避免在支付加密貨幣或資料傳輸的過程中，遭他人竊取或竊聽，許多類似Tor網路的匿名網路，逐漸受到重視。許多非法網站亦開始蓬勃發展，如前述「絲綢之路」洗錢案，該網站在毒品買賣以外，也提供了殺手買兇及人口販運等犯罪。

以下對於暗網交易，及基於暗網交易所衍生的芬太尼（Fentanyl）事件，再進一步探討及分析：

1. 暗網交易

黑暗網站（Darknet; Dark Web），簡稱為暗網，為沒有經過一般搜尋引擎索引，並且使用特殊通訊協定及加密機制來達到匿名與隱私目的之電腦網路及電腦網路上網站。相對於能經由一般大眾所常使用的搜尋引擎存取的明網網路（Surface Web/Clearnet），深網則是沒有或無法經由此類搜尋引擎索引（例如電子郵件服務、網路銀行、線上資料庫等）。而暗網則為深網中一小部分，須特殊設定及專屬的瀏覽器才能瀏覽該暗網網站。

暗網最原始的來源為美國海運研究實驗室，基於確保政府的網路通訊隱密性所開發，於 2006 年登記為非營利組織，取名為洋蔥路由計畫（Tor Project），自此，一般大眾便能使用洋蔥路由計畫瀏覽器來成為 Tor 網路使用者。由於其具匿名之效果，使有心人士可利用該隱密性，逃避政府監督，進行違法交易。

根據英國樸茨茅斯大學（University of Portsmouth）學者 Owen 及 Savage 在 2015 年 9 月所公布的暗網調查報告[222]，在暗網上網站內容類型分類中，以毒品相關內容之網站最多，其次則是黑市以及詐欺相關，本文整理如下：

類別	毒品	黑市	詐欺	比特幣	電子郵件	維基	吹哨人	假鈔
比重%	15.4	9	9	6.2	5.7	5.2	5.2	5.2
類別	論壇	匿名	搜尋	駭客	網頁寄存	色情	部落格	索引目錄
比重%	4.75	4.5	4.25	4.25	3.5	2.75	2.75	2.5

[222] Owen, G., & Savage, N.(2015). The Tor Dark Net. Centre for International Governance Innovation.

類別	電子書	虐待	新聞	聊天	槍械	賭博
比重%	2.5	2.2	2.2	2.2	1.4	0.4

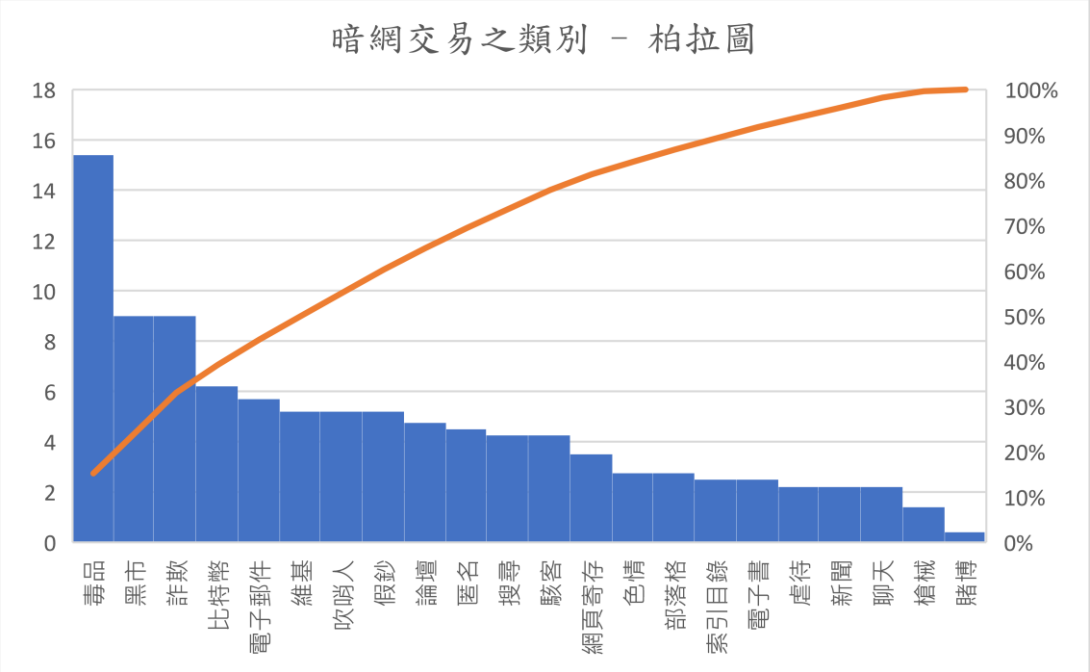


圖 38 暗網交易之類別 – 柏拉圖

資料來源：本研究團隊自製

由上述分類可知，諸多的暗網交易均夾雜著違法犯罪，這也使得各國政府開始加深其介入程度，以防止暗網成為犯罪的溫床，並杜絕國家機密資料的外洩。

日前，美國司法部與歐洲刑警組織抓到一件史上規模最大的網路販毒案，逮捕 150 人，截獲美金 3100 萬以及槍枝跟毒品。此起案件即是源自於暗網市集中所破獲的重大犯罪，不僅犯罪的軌跡出現在澳洲、保加利亞、法國、德國、義大利、荷蘭、瑞士、英國及美國等地，所破獲的犯罪物品更包含有 45 把槍、一些比特幣及 234 公斤毒品。美國緝毒局長米爾格拉姆指出，「這些藥其中有些含有芬太尼（Fentanyl），有些含有冰毒，我們現在看到這些假藥，在國內每個州都有在賣，我們已經查獲超過 1150 萬顆，是 2019 年的 4 倍。」[223]

223 公視新聞網，「跨國警破獲史上最大暗網交易 逮捕 150 人、截獲美金 3100 萬」，

由此可知，暗網所造成的犯罪問題，已有日漸擴大之勢，必須嚴肅以對。

2. 芬太尼（Fentanyl）事件

(1) 芬太尼實為人工合成之鴉片類止痛劑，然有上癮之虞：芬太尼並非新產品，作為一種人工合成的鴉片劑，其實在醫學上已沿用多年，作為藥物的止痛效果強大，比嗎啡強 50 至 100 倍。很少份量已可以鎮痛，副作用卻又比嗎啡來得少。具治療吸毒病人經驗的多倫多家庭醫生陳敬熙稱：「嗎啡本身有很多副作用，例如嘔吐、身體痕癢，不宜用量過多；但芬太尼用很少份量，已有很好的效果，可以說是一種非常理想的止痛藥。」然而，因為芬太尼屬於鴉片類藥物（Opioid），因此就有上癮的機會。「有痛需要醫治是對的，但長期服用就會出現後遺症，如果不經醫生指引或監管，很容易出現上癮或過量服用的危險。」芬太尼在止痛之餘，也會同時帶給服用者一種很滿足，很鎮定、很鬆弛的感覺，這就是令人著迷上癮之處，長期在心理或生理上倚賴藥物，便形成吸毒的癮癖。

(2) 芬太尼利潤太驚人：

前加合拿大衛生部副醫療官 Hakique Virani 醫生，在加拿大成癮醫學會中指出，向國外郵購非法芬太尼藥粉一公斤，加上製藥丸的機器，本錢不過 10 萬元，但可出產藥丸 100 萬粒，以每粒 20 元的卡加里市價，毒犯收入高達 2,000 萬。「只需要很少的芬太尼藥粉便可製成毒品，本小利大，利潤遠超海洛英，是毒販的理想藥物。」陳醫生稱，這些非法芬太尼不受監管，非常危險，藥的份量多少無從知曉，有時更會混進其他如可卡因等毒品內，

https://news.pts.org.tw/article/551193，最後瀏覽日：2021/11/1。

近年多宗芬太尼致死的個案，都和這些非法藥物有關。[224]

(3) 透過虛擬貨幣於暗網中交易芬太尼造成之危害：

近年來造成美中關係緊張的芬太尼事件，即為中國的芬太尼販售者，大量運用虛擬貨幣透過暗網進行全球性買賣，造成美國國內的威脅。美國緝毒局（DEA）指出，即使僅攝入低至 0.25 毫克的劑量，芬太尼亦足以致命。因此，美國僅容許處方芬太尼作止痛藥，用於治療癌症等重症引起的嚴重疼痛。然而走私商會將芬太尼與海洛英等藥物混合製成毒品，以增強其效果。根據美國疾病控制和預防中心（CDC）的數據，芬太尼每年導致超過 1.8 萬名美國人死亡，成為美國濫用藥物案中致命率最高的藥物。美國執法部門更於 2018 年 5 月，於內布拉斯加州檢獲 54 公斤的芬太尼，數量足以毒死 2,600 萬人。

美國聯邦調查局（FBI）曾表示，流至美國的芬太尼等藥物當中，高達 95%出自中國。美國國家貿易委員會主任納瓦羅（Peter Navarro）更表示，不論中美兩國簽署甚麼貿易協議，芬太尼走私仍是中國必須解決的「七大罪」（seven deadly sins）之一。美國因應芬太尼危機，持續向中國政府施壓，要求其加強管制芬太尼走私情況[225]。

根據《HealthDay》報導，美國德克薩斯大學的一項研究顯示，暗網上非法銷售藥物的情況非常普遍，不僅難以發現，且加劇了美國鴉片類藥物氾濫。且暗網上有許多使用加密貨幣的芬太尼經銷商，比如 Nightmare Market 和

---

224 號角月報-加拿大版，勁毒狠毒芬太尼，
https://www.heraldmonthly.ca/newspaper/web/articleView.php?date=201705&id=5235，最後瀏覽日：2021/11/2。

225 香港經濟日報，【中美貿易戰懶人包】，芬太尼是什麼，為何使中美關係緊張，
https://inews.hket.com/article/2491803/%E3%80%90%E4%B8%AD%E7%BE%8E%E8%B2%BF%E6%98%93%E6%88%B0%E6%87%B6%E4%BA%BA%E5%8C%85%E3%80%91%E8%8A%AC%E5%A4%AA%E5%B0%BC%E6%98%AF%E7%94%9A%E9%BA%BC%20%E7%82%BA%E4%BD%95%E4%BD%BF%E4%B8%AD%E7%BE%8E%E9%97%9C%E4%BF%82%E7%B7%8A%E5%BC%B5，最後瀏覽日：2021 年 10 月 29 日。

Empire Market，雖然有些交易平台考慮到芬太尼極度危險的藥性而選擇了禁止交易，但不少賣家依然會使用一些化名來稱呼芬太尼，還有些人會把芬太尼添加到各種不同的假冒藥品之中繼續交易，這些行為更加劇了終端用戶出現用藥過量的風險226。

(二)虛擬通貨之流向難以掌握

洗錢防制法於 107 年 11 月 7 日修正公布，依同法第五條第二項規定，虛擬通貨平台及交易業務事業（以下稱本事業） 適用該法關於金融機構之規定，包含應建立洗錢防制內部控制與稽核制度、進行確認客戶身分、紀錄保存、一定金額以上通貨交易申報及疑似洗錢或資恐交易申報等事項。另防制洗錢金融行動工作組織（Financial Action Task Force, 以下稱 FATF）已要求虛擬資產（即虛擬通貨）服務提供者應遵循 FATF 第十五項建議等防制洗錢規範。

行政院於民國 107 年 11 月 7 日指定金融監督管理委員會為本事業之洗錢防制主管機關，並於一百十年四月七日指定本事業之範圍，爰參酌 FATF 發布之建議，訂定「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」（以下稱本辦法），本辦法第二條所規定之虛擬通貨平台及交易業務事業指下述:

1. 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。
2. 虛擬通貨間之交換。
3. 進行虛擬通貨之移轉。
4. 保管、管理虛擬通貨或提供相關管理工具。
5. 參與及提供虛擬通貨發行或銷售之相關金融服務。

換言之，非本事業範圍之虛擬通貨業者（典型如「未提供保管私鑰」之錢包軟體業者），即非我國洗錢防制法體系下應進行確認客戶身分、紀錄保存、一定金額以上通貨交易申報及疑似洗錢或資恐交易申報等事項之業者。但經本研究團隊處理相關虛擬通貨偵查實

226 聯合新聞網，美暗網非法交易 助長鴉片類藥物濫用，
https://udn.com/news/story/6813/5366613，最後瀏覽日：2021 年 10 月 29 日。

務可知，相關金融科技犯罪之不法所得，容有透過非洗錢防制法下之虛擬通貨業者進行洗錢或移出至人頭帳戶，完成不法所得之藏匿，相關虛擬通貨之流向難以被偵查機構所掌握。

此外，本辦法第七條規定（即「Travel Rule（旅行規則）」），「本事業如擔任虛擬通貨移轉之轉出方，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資訊，且應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...；本事業如擔任虛擬通貨移轉之接收方，應採取適當措施，以辨識是否缺少必要資訊之虛擬通貨移轉，及適當之後續追蹤行動，並應保存所取得之轉出人及接收人資訊。」，故若落實旅行規則之法定義務，虛擬通貨之轉出方及接收方等實名制及虛擬通貨金流資訊，可以由司法偵查機構所掌握。

FATF 於西元 2018 年 10 月修正通過第 15 條建議中，提及各國應確保虛擬通貨服務提供者（VASP）受到防制洗錢與防資恐之監管，2019 年 6 月，FATF 就第 15 條建議發布監理虛擬通貨服務提供者之具體指引。嗣 FATF 於 2020 年 6 月發布之審查報告，承諾將進一步修訂指引並評估修訂第 15 條建議[227]；FATF 並於 2021 年 3 月發布虛擬通貨業者洗錢防制指引草案[228]（下稱「FATF 指引草案」），並甫於同年 4 月結束公眾評論程序。FATF 預計將於 2021 年 10 月討論並公告指引草案最終版本，包含重新修訂之虛擬通貨之定義、適用業者範圍、防制洗錢之具體建議作為及是否訂定「Travel Rule（旅行規則）」等[229]。FATF 發布上述 FATF 指

[227] FATF, *12-month Review Virtual Assets and VASPs*, FATF (Jun. 2020), www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html ,paragraph 70-72, pp.19-20. ([**The FATF should consider future amendments to the revised Standards if this work identifies issues which updated Guidance cannot resolve.** The FATF must also closely monitor the risks posed by so-called stablecoins, anonymous peer-to-peer transactions via unhosted wallets and the broader virtual asset market. If there does appear to be a significant change to the market structure or ML/TF risk profile, **the FATF should consider whether amendments to the revised Standards are warranted**.])

[228] FATF, *Draft updated Guidance for a risk-based approach to virtual assets and VASPs*, FATF (Mar. 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf.

[229] *Id.*

引草案後（包括 Travel Rule），由於對現有洗錢防制標準措施之修正幅度頗鉅，並大幅增加虛擬通貨業者之相關義務，各國之行業公會及學術機構均已就 FATF 指引草案表示諸多公開意見[230]，FATF 指引草案訂定之標準是否為未來正式公布之標準，尚無定論，故現行各國政府多尚未依照 FATF 指引草案啟動正式修法程序[231]，包括我國本辦法第 18 條規定：「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。」，因此現行法下，若虛擬通貨之金流涉及到不同虛擬通貨平台間之轉移，尤其是涉及到外國虛擬通貨平台之業者（並未在台灣設立分公司或子公司），相關虛擬通貨之流向亦難以被偵查機構所掌握，增加偵查及扣留不法所得之難度。

[230] 例如日本虛擬通貨商業協會於 2021 年 4 月 20 日就 FATF 之指引草案提出了 30 項修正意見，參見 Japan Cryptoasset Business Association, *Comments of Japan Cryptoasset Business Association on the draft revised VASP Guidance*, Japan Crytoasset Business (Aprl. 20, 2021), https://cryptocurrency-association.org/cms2017/wp-content/uploads/2021/04/Comments-of-Japan-Cryptoasset-Business-Association-on-the-draft-revised-VASP-Guidance.pdf

[231] 英國財政部於 FATF 第 15 條建議公布後推遲了將虛擬通貨業者納入監理之時程，以便讓業者能有時間開發解決方案，其並提及於**有國際公認之標準後**，政府始會修正其洗錢防制相關規則，參見 HM Treasury, *Transposition of the Fifth Money Laundering Directive: response to the consultation*, at 10, GOV.UK (Jan. 2020), https://www.blockchainwg.eu/wp-content/uploads/2020/03/5MLD_Consultation_Response-2.pdf, (［The government notes the concern surrounding the time needed to comply with these requirements and **will not be legislating for this obligation to form part of the UK's AML/CTF cryptoasset regulatory regime at this time.** This delay is intended **to provide time for firms to develop compliance solutions** ahead of the introduction of the new obligations. Firms should consider solutions as soon as possible and should refer to section IV of FATF's June 2019 guidance on Virtual Assets and Virtual Asset Service Providers, which proposes several potential technologies to facilitate compliance. **It is the government's intention to amend the MLRs to include this requirement as soon as it is clear there are globally recognised ways to comply.**］)；此外，日本金融廳於 2021 年 3 月 31 日亦公布將予業者 1 年時間（自 2021 年 3 月 31 日至 2022 年 4 月）研議是否依據 FATF 草案修正相關規範，包括引進 Travel Rule，可參見日本金融廳網站，暗号資産の移転に際しての移転元・移転先情報の通知等（トラベルルール）について，https://www.fsa.go.jp/news/r2/sonota/20210331.html ，最後瀏覽日：:2021 年 6 月 7 日。

第二節　我國執法機構之現況與困境

於今日數位資訊社會，對抗網路犯罪成為刑法與相關刑事訴訟法的重大議題，當新興金融科技成為犯罪工具之一，則有必要進一步盤點有無可得相對應之網路犯罪偵查手段，以及有無適當基本權干預之授權條款以利執法機構合法進行犯罪偵查，成為金融科技犯罪網路追訴的首要課題，而本節將盤點我國偵查網路犯罪之方式，數位證據及線上取證等現行法適用疑義，並進一步研析我國執法機構於濫用新興金融科技犯罪之困境。

第一項 我國偵查網路犯罪之刑事追訴

一、網路犯罪偵查之相關法令及手段

單就一國刑事法領域而言，從實體法的網路犯罪認定、網路釣魚、妨害網路通訊隱私等，至刑事訴訟線上偵查之合法性，都是伴隨網路而生的議題。我國實定法方面，中國民國刑法在十多年前已注意電腦網路犯罪，並於西元2003年增訂刑法第36章「妨害電腦使用罪」，新增第358條至第363條，立法理由提及「保護電腦系統之安全性」（刑法第358條）、「電腦已成今日日常生活之重要工具，民眾對電腦之依賴性與日俱增，若電腦中之重要資訊遭到取得、刪除或變更，將導致電腦使用人之重大損害」（刑法第359條）、「鑒於電腦及網路已成為人類生活之重要工具，....有必要以刑法保護電腦及網路設備之正常運作」（刑法第360條），近年更於西元2014年增訂「以電信、網路對公眾加重詐欺罪」（刑法第339條之4第1項第3款），立法理由提及「詐欺案件...結合網路、電信、通訊科技，每每造成廣大民眾受騙，此與傳統犯罪型態有別」。

而於刑事追訴之程序法上，立法者則似無相應的網路追訴配套，唯一相關修正是西元2001年在刑事訴訟法第122條將「電磁紀錄」增列為搜索客體（並搭配修改第128條第2項搜索票記載事項），但搜索電磁紀錄之意義為何，立法理由諱莫如深。值得注意且具備實務重要性者，係西元1999年制訂的「通訊保障及監察法」（下稱「通保法」），網路追訴一旦干預人民的秘密通訊自由，就應該且只

能依通保法為之。然而通保法的法律干預授權可涵蓋所有網路偵查的取證行為嗎?[232]答案為否定的[233]，以下說明之。

(一)現行法下關於電磁紀錄及通訊監察之規範

我國現行法下對於電磁紀錄及通訊監察之規範，主要見於刑法、刑事訴訟法及通保法。

1. **刑法規定：**

刑法第 10 條第 6 項規定，電磁紀錄的定義是指「以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。」

刑法第 339 條之 3 之規定：「意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人之財產者，處七年以下有期徒刑，得併科七十萬元以下罰金。」此項係規範了以不正方法刪除、更改相關電磁紀錄而獲取他人利益者，構成電腦詐欺罪。

刑法第 36 章則規範關於妨害電腦使用罪責，主要見於刑法第 359 條規定，無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，及第 360 條無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，均違反本章之保護電磁紀錄之法益。

2. **刑事訴訟法規定：**

依刑事訴訟法第 122 條明文規定，在有相當理由時，得搜索特定人的身體、物件、「電磁紀錄」及住宅或其他處所。另依同法第 129 條第 2 項第 3 款規定，若欲搜索關於電磁紀錄時，應記載於搜索票之中。

(二)電磁紀錄之搜索與扣押

舉凡不涉及秘密通訊過程之電子郵件、電子文件、交易帳本記錄、通訊軟體對話紀錄、虛擬通貨交易之錢包位址、保存及存取虛擬通貨之私鑰等，一般來說會儲存在電腦硬碟、行動裝置，或網路

[232] 王士帆，網路之刑事追訴—科技與法律的較勁，政大法學評論，第 145 期，法源資訊重新校編，頁 3-4。

[233] 立法理由如下：一、本條隊搜索之對象增列「犯罪嫌疑人」及「電磁紀錄」。二、重新界定「被告」之概念，將偵查中之「被告」證明為「犯罪嫌疑人」，與經檢察官偵查終結予以追訴之審判中之「被告」資以區別。

伺服器上，性質上均為一種電磁紀錄，從物理性質言，上述標的均非實體物，不能成為扣押之「物」，但由於存在於實體物件上，國家機關欲取得實體物件的占有支配，應循一般搜索、扣押規定，扣押上述標的所在的儲存載體，例如直接扣押個人電腦硬碟或電子郵件伺服器[234]。

電磁紀錄已於今日刑事程序中扮演極為令人矚目的角色，在許多的個案中，其皆成為偵查機關用以證明犯罪事實的重要證據。然而，由於電磁紀錄不若有體物，係無體的資訊，無法直接由人的感官得知其內容，必須附著於載體之上，為要搜尋載體內有無所需的資訊，偵查機關多必須要長時間扣押載體，甚至是電腦相關設備。無疑地，其勢必會對相對人財產權益造成不小的衝擊。

此外，電磁紀錄載體中，多存放有與本案無關之個人私秘資訊，而在透過電腦鑑識技術對載體中的資料進行調查時，該等私秘資訊勢必會曝露於偵查人員之中，此將造成對人民隱私權的侵害。故從隱私權等憲法基本權來看，電腦鑑識實屬於實質意義的搜索。無論偵查機關所提出的名義為何，其之鑑識流程，應與傳統之搜索，受相同程度的限制，方能有效保障人民之基本權。

1. **與傳統搜索扣押之比較：**

相較於傳統搜索扣押的一階段搜索模式，即偵查官會在現場同時完成搜索及扣押兩動作，電磁紀錄的執行方式，則是採取二階段搜索模式。在二階段模式中，第一階段將類似於傳統之搜索扣押，當扣押得電磁紀錄之載體後，再藉由電腦鑑識之程序，搜尋載體內是否有所需之電磁資訊。且基於技術上因素、有效執法及保障民眾之權利而言，通常第二階段會於其他地點進行鑑識[235]。但也無疑的，在二階段的搜索扣押模式下，將會對被搜索扣押之人的權利造成侵害，除了上述的財產權直接侵害外，更會造成個人隱私權的危害。

[234] 王士帆，同前註 232，頁 10。

[235] 因為搜索人員多半不具科技背景，且現場立即進行鑑識，多半頗為耗時，造成執法上之無效率及延長侵害民眾權益之時間。

2. **電磁紀錄之搜索應屬實質意義之搜索：**

為進行電腦鑑識，偵查機關多須扣押於搜索現場所發現之電腦設備及載體，而此一扣押短則數周，長則數月，這樣的作法已對受搜索人構成財產上之侵害。其次，在所扣押之電磁紀錄中，亦多含有大量與本案無關之個人資訊，而在鑑識過程中為鑑識人員所接觸，亦無可避免的侵害被搜索人之隱私權。

因此，從搜索、扣押到電腦鑑識的整個程序，將侵害被搜索人之財產權及隱私權。有鑑於過去傳統對於搜索的定義過於狹隘，無法有效保護人民權益，現今在界定搜索意涵時，已不再侷限於以物理性空間或是財產權的觀念來理解，而是改採偵查機關的行為，是否已經侵害相對人對於其所有之物品、空間或資訊，具有「隱私合理期待」作為判斷其是否屬於搜索[236]。

故在刑事程序上，電磁紀錄之搜索屬實質意義之搜索，應與傳統搜索受有相同程度的規範，方得兼顧保障人民之基本權。

3. **電磁紀錄搜索扣押之問題：**

當扣押物為有體物時，依傳統流程為偵查官必須事先向法院聲請搜索票，並至特定之處所搜索，於搜得扣押物後予以扣押。而於待扣押物為電磁紀錄載體時，可能的爭議包含下述：

（1） 對於電磁紀錄載體及相關電腦設備的扣押

依刑事訴訟法第 133 條第 1 項的規定，於搜索時執行機關得扣押可為證據或得沒收之物，故若為實體之物為扣押無現行法適用疑義；若欲扣押之物為載體內的資訊且欲作為證據之用，則較有爭議。

純從法條文義上來說，現行刑事訴訟法第 133 條第 1 項僅規定「物」，然載體本身並不是可為證據之物，而係其內所儲存之電磁紀錄才是，故本條之法條文字上似有進一步酌修及釋明之必要[237]。

---

[236] 李榮耕(2009)，〈個人資料外洩及個資外洩通知條款的立法芻議〉，《東吳法律學報》，20 卷 4 期，頁 254-258 頁。

[237] 李榮耕(2012)，〈電磁紀錄的搜索及扣押〉，《國立臺灣大學法學論叢》，第 41 卷 3 期，頁 1072。

（2） 取得載體內資訊的問題

若經扣押之載體是屬於得沒收之物，依刑事訴訟法第 133 條第 1 項及刑法第 38 條第 1 項第 2 款、第 3 款規定，在有相當理由足認電磁紀錄載體為「供犯罪所用或犯罪預備」或「因犯罪所或所得」之物，均得以扣押[238]。

若載體僅為得為證據之物，則對人民的基本權侵害較大。基於電腦鑑識需要及現實技術上的考量，執法官員多是先扣押載體，再於偵查機關內進行鑑識。除極少數情形外，該載體之資訊內容，大都包含大量與本案無關的個人私秘資訊，卻可能逐一的暴露於偵查權限之下。如此大範圍的強制處分，有論者謂確有過度侵害人民權益的疑慮，似違反刑事訴訟法第 133 條第 1 項對於相當理由及特定明確原則的要求[239]。

（3） 製作扣押物清單

刑事訴訟法第 139 條第一項規定：「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。」然而，在肯認電腦鑑識屬於實質意義的搜索情況下，是否需要對載體內的檔案，制作詳細的細目交予被扣押人呢？依學者李榮耕的看法，以採否定說為宜[240]，主要原因為保護被扣押者之隱私，試想若是程序上要求電腦鑑識人員必須制作檔案細目，勢必要詳盡地檢視載體中的各項資訊，如此反而使得受扣押人之隱私完全暴露於偵查權力之下，似有違反比例原則等疑義，極為不當。

（4） 小結

基於實務上對於犯罪偵查的需要，確保追訴犯罪的重要利益，應容許執法官員扣押於搜索現場所發現的載體，惟如何同時確保人民的財產權及隱私權，程序上的重點應在於有客觀公正的法院於事前的監督制衡。例如搜索扣押前，偵查機關應基於令狀原則，取得法院開立的搜索票，且必須於需要扣押電磁

[238] 王兆鵬，刑事訴訟法講義，4 版，頁 86。
[239] 王兆鵬，同上註，頁 138。
[240] 李榮耕，同前註 237，頁 1084。

紀錄時特別釋明之，法院同意後方可搜索扣押，如此方能取得兩者間之平衡。

在電磁紀錄載體中，尤其是現代科技的進步，其可儲存的資訊量，已遠多於傳統紙本文件式的資料，在這些龐大的資料中，多存放有與本案無關的私密資訊，而在電腦鑑識的過程中曝露於偵查權限之下，造成對於人民隱私的侵害。因此，取證手段，便應該因應「資訊量」的不同，給予標的不同的取證方式[241]。

有論者謂，從隱私等憲法權利侵害的角度來說，電腦鑑識屬於實質意義的搜索。無論偵查機關實施的名義為何，其皆應與傳統搜索受有相同程度的規制，方得有效保障人民的權利[242]。而最高法院近年來之判決，業已突破財產、有體物或物理空間的窠臼，改以合理隱私期待的觀念來判斷偵查機關的行為是否屬於搜索，以保障人民之權益[243]。

(三)網路搜索脈絡下的網路偵查

網路搜索主要可分成「雲端搜索」及「秘密線上搜索」,「雲端搜索」以及「線上搜索」最大的區別在於，前者係介接載體延伸的取證，亦即，該數位證據並非存放於特定可得扣押之載體標的內，而係存放在延伸但空間分離之載體標的（如雲端空間）；後者則屬於不以介接載體為必要之遠端取證，通常係藉由木馬等遠端鑑識軟體，經過現場或遠端植入後，便能取得管理者權限，進而掃描和移轉資料。

---

[241] 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〉，《月旦裁判時報》，頁 58。

[242] 李榮耕，同前註 237，頁 1055。

[243] 參最高法院 99 年度台上字第 4117 號判決：「…本件係警察接獲匿名檢舉有人在該網咖販毒，遂以臨檢名義進入該網咖，對被檢舉遊戲桌之上訴人進行臨檢，未持有任何搜索票，即要求上訴人打開包包，進而查獲包包內之上述物品。而警察人員以臨檢名義進入該網咖時，上訴人坐在電腦桌前打電動，似不符合前述警察職權行使法第七條第一項第四款所定『有明顯事實認其有攜帶足以自殺、自傷或傷害他人生命或身體之物』之情況，警察應僅能查核上訴人之身分，警員吳瑞麟卻要求上訴人打開包包供其檢查，在上訴人對其所攜帶之包包有合理隱私期待之情況下，警員吳瑞麟所為是否已該當於刑事訴訟法所定『搜索』之行為，除非符合前開搜索發動之要件，否則不能任意為之。」

1. **雲端搜尋**

與刑事訴訟偵查措施較有密切關聯性的是雲端儲存，雲端儲存這種電腦服務將可為證據的檔案散存在分散系統，當搜索被告電腦或手機等資訊設備時，發現應扣押之物存放在網路連結的雲端硬碟時，可否依搜索扣押規定加以保全？依我國刑事訴訟法第 128 條第 2 項第 3 款之規定，即將電磁此一特性之證據資料，列為搜索之標的中。有學者認，若搜索令狀自始便明示其範圍涵蓋延伸之載體與相關資訊標的，即以刑事訴訟法第 128 條第 2 項之「應加搜索之.....電磁紀錄」為基礎，進而避免過分模糊而產生空白搜索票或取證範圍之疑慮，同時亦未涉及干擾或破壞雲端業者系統的正常運作，則此等取證手段，仍為現行法所相容[244]。

然而，此等介接載體而延伸之取證手法，相較於針對載體本身內的數位證據之取證，其問題在於，可能會使搜索扣押的內容無限延伸，甚至可能有進一步干預延伸載體所有人以及對第三人搜索、扣押的疑慮[245]。

2. **秘密線上搜索**

秘密線上搜索是指偵查機關成為國家級駭客，透國傳輸、安裝木馬程式或後門程式至被告的個人資訊系統，並藉此獲取相關證據之方法。

秘密線上搜索問題則在於，其將對人民基本權造成更嚴重的干預。線上搜索乃藉由遠端之掌控，而未必需要藉由干預載體標的之手法，便能夠全面性地針對資訊標的進行取證，是以，載體標的之物理性質不一定會因線上搜索而遭到破壞或限制，致對人民基本權之干預可能發生於無形，甚至產生更嚴重、廣泛的干預效果[246]。

由於該刑事偵查手段嚴重侵害人民基本權，且不符合通訊監

[244] 施育傑，同前註 241，頁 69。
[245] 施育傑，同前註 241，頁 62。
[246] 施育傑，同前註 241，頁 64-65。

察之範圍，因為此時並非監察被告與他人之間的通訊，而是在通訊之前，即啟動所儲存的電腦資料至偵查單位，故無法符合現行刑事訴訟法要求搜索之執行程序應符合公開性原則，即執行人員須向在場人提示搜索票（刑事訴訟法第 144 條）、命令或通知特定人在場（刑事訴訟法第 148 至 150 條），從而秘密線上搜索此一新型態的偵查措施，在解釋上便無從被涵蓋在現行法的搜索概念下，有待另外進行立法規範[247]。惟有學者提出，在未來立法上似可以考量在重罪及犯罪可能性極高的情形下，例外許可秘密線上搜索取證[248]。

3. 小結

科技犯罪越趨常態，實務上可能作為「科技偵查」的手段也漸趨多元。但對照我國目前法制，關於偵查程式的干預處分，大致上僅有刑事訴訟法明文增修「電磁紀錄」作為搜索客體，以及通訊保障及監察法授權通訊監察、調取通訊紀錄的條款，如何兼顧科技時代下偵查效率與權利保障的衡平，遂成重要問題[249]。

因此，基於現今科技日新月異，偵查機關大量運用科技設備或技術，進行必要之科技偵查行為，為規範偵查機關實施此類調查之合法性，切實保障人民基本權，並避免犯罪調查之手段落後於科技發展之腳步，影響國家安全及社會秩序[250]，因此，法務部已於民國 109 年 9 月 8 日公告「預告制定科技偵查法草案」[251]。對此，因為其中部分內容侵入人民私生活領域有過深入的疑慮，而遭到部分外界非議[252]，於各界檢討聲浪後科技偵查法也撤案，立法院也要求相關部門進一步研析及檢討後再行

[247] 施育傑，同前註 241，頁 64-69。

[248] 同前註 232，頁 339-390。

[249] 施育傑(2020)，〈科技時代的偵查干預處分–兼論我國法方向〉，《月旦法學雜誌》，第 306 期，頁 154。

[250] 參考科技偵查法草案第一條之立法理由。

[251] 法務部於 2003 年即完成「臥底偵查法草案」，惟迄今尚未施行，https://www.moj.gov.tw/2204/2795/2796/53975/，最後瀏覽日：2021 年 8 月 14 日。

[252] 法務部網站，https://www.moj.gov.tw/Public/Files/202009/70320090817536d83f.pdf，最後瀏覽日：2021 年 8 月 14 日。

送案[253]。

民間司改會董事長林永頌則指出，《科技偵查法》草案中明定，檢察官若認為有必要，可透過定位系統及設備調查，他質疑何謂「有必要」？且草案中是否必要單由檢察官決定，2個月內不需經法官同意，將影響人民的行動自由及集會結社自由。另草案允許在非隱私空間進行錄音、錄影等行為，在隱私空間經法院許可也可從外部進行監看、錄音、錄影，同樣影響言論自由與居住自由。

台灣人權促進會則指出，本次最大的爭議是合法化入侵個人裝置的「設備端通訊監察」。草案使用《通訊保障及監察法》對監聽的案類限制及保護措施，問題是入侵個人裝置的隱私侵害遠比傳統監聽嚴重。光是使用通訊軟體傳輸的資料，就涵蓋影片、相片、語音、文字，更別說手機內的其他個資[254]。

本研究團隊認為，科技偵查法草案或許有侵犯人民隱私等基本權疑慮，然不可否認的，現行的法律對於日新月異的犯罪手法，確已有不足之處，偵查機關若侷限於目前法律窠臼，可能將因無適當基本權干預之授權條款以利執法機構合法進行犯罪偵查，造成台灣成為金融科技犯罪的溫床[255]。

二、數位證據之載體—雲端與線上取證之分析

隨著科技的發展，傳統刑事取證方法，就常會遇到解釋上的困難，例如電磁紀錄與整體搜索、扣押制度的問題，乃至於行動電話內資訊的附帶扣押、網際網路的線上搜索、雲端資料的保全等，都存在著如何與現行法配合使用的問題。

數位資訊原則上以 1 與 0 的二進位方式儲存，再透過解碼的方

[253] 林誠澤，法律白話文運動，沒上太空就進場維修的科技偵查法？https://plainlaw.me/2020/11/25/%E6%B2%92%E4%B8%8A%E5%A4%AA%E7%A9%BA%E5%B0%B1%E9%80%B2%E5%A0%B4%E7%B6%AD%E4%BF%AE%E7%9A%84%E7%A7%91%E6%8A%80%E5%81%B5%E6%9F%A5%E6%B3%95%EF%BC%9F%EF%BD%9C%E6%9E%97%E8%AA%A0%E6%BE%A4/，最後瀏覽日：2021 年 8 月 14 日。

[254]參見 The News Lens 關鍵評論，https://www.thenewslens.com/article/140643，最後瀏覽日：2021 年 8 月 13 日。

[255] 同前註。

式，轉換成人類所能理解的文字、號碼或符號等。而數位資訊之儲存，以現今之技術而言，主要的載體有光碟片、隨身碟及硬碟等。而在資訊的傳輸方式上，主要是透過所謂的封包（package）傳送，例如在 A 電腦下指令，指示將某資料傳到 B 電腦，此時 A 電腦便會透過封包送傳資料到 B 電腦，再 B 電腦接收、處理及儲存該資料。

基於上述對於數位資訊的理解，主要的意義在於，面對不同的取證標的與方式時，「干預權利領域」的有無及其程度，亦即現今的程序規範，是否足以套用於對數位資訊的取證。

以資訊量的多度而言，數位資訊所能承載的資訊量，遠大於傳統的紙張文件，而在現今的雲端時代，更是讓數位資訊之儲存及傳輸，有更不同於以往革命性的進步。而此一發展，即使得傳統的取證手段，是否足以相容於數位科技時代的取證，就有許多探討的空間。例如在可接近性上，以往一定要有空間上及物理上的接觸，方有辦法對可為證據之物做搜索及扣押，而在數位時代，除了物理性地取得數位資訊之「載體」外，更能透過網路，直接的從雲端上，跨越空間的侷限，直接取得證據。因此，取證手段的方法及實際規範於現行法律的應用，在現今的社會，就顯得非常的重要，以下分論之。

(一)資訊與載體

在數位資訊的取證上，很重要的一個區分點，即在於資訊與載體的關係，若欲扣押之資訊實際均存在於載體之中，與非存在於載體之中，就會產生不同之法律關係，分別探討如下：

1. **資訊與載體同一**

資訊與載體同一的情況，是目前最廣泛應用及理解的面向，即是以載體本身作為搜索及扣押的標的，雖然最終的目的仍為獲取載體內的數位證據，而非載體。但因為數位證據的特性，一般的傳統的實體物搜索及扣押流程，將有若干變化。真正的證據不是載體，而是載體內的檔案，故在檢視載體內的資料時，將構成實質的搜索。而此搜索，就引申出是否夾雜著附帶搜索之問題，例如警方於附帶搜

索時，發現嫌犯之手機一台，警方能否直接檢視嫌犯手機內容，以獲取其是否有其他的犯罪證據。鑑於手機內的資料可能存有大量個人的隱私資料，若要檢視內部資訊，另行取得搜索令狀似為妥當之方式。

而由於資訊與載體同一，當物理性地扣押住載體後，載體內的資料是否就都可以探查及保全內部的全部資料，於我國法下應採否定說，蓋載體內的資訊量是相當龐大的，並不因載體與資料的緊密結合，而概括的認為只要合法的扣押住載體後，便同理的推論一切的檢視載體內內容的行為亦為合法，否則將大開搜索之門，並直接的侵害憲法上更重要的個人基本權利。

2. **資訊與載體不同一**

一般針對載體的搜索、扣押，主要是為了獲取載體內之數位證據，但如果數位證據並不是存放於特定可得扣押的載體標的內，而是存放於不同空間的載體標的時，我國因刑事訴訟法第 122 條已將電磁紀錄作為搜索的客體，故於現行法規範上是具備合法依據。惟原本的載體內容限制，將有無限延伸之可能，例如存放於雲端的資料，當對雲端的資料作搜索時，可能會有干預雲業者權利及產生對第三人搜索及扣押的疑慮。因此，在我國法律的規範下，仍必須取得搜索令狀及可得特定之搜索範圍。

3. **遠端取證（不以載體為媒介）**

這一類取證行為，一般最常用的方法是線上搜索，而最常使用的工具則是遠端鑑識軟體，亦是一般俗稱的後門程式或是木馬，亦即在欲取得資訊資料的目標上，植入預先寫好的程式，藉此取得權限並移轉資料。

不透過載體而直接由遠端取得證據，此手段反而未必會干預載體標的，也不介入第三人的領域，然這種手法，是否為最小干預手段而符合比例原則之要求？雖然在物理性質上，此手法並不會直接的破壞或限制個人的持有，但

是載體標的內的系統已經受到取證的干擾。另外，用戶端能做的事情，遠端的控制者亦能完全做到。換言之，用戶端的一舉一動，完全被隱藏在遠端的某人或機構觀察著[256]，由此可知，此種技術，將會造成更嚴重及更廣泛的基本權干預。

(二)現行法適用問題

面對刑事追訴的數位證據取證新技術，規範面上應如何理解及審查，應回歸權利的保護範圍審查，以決定新型偵查手段的容許性。電磁紀錄的干預處分，不應僅僅是著眼於發動時，在審查時，亦必須考量過程中的適用問題。在對於載體的搜索扣押，於載體標的無誤下，避免空日搜索票及兼顧個案比例原則。而在刑事訴訟法第130條的附帶扣押規定下，若附帶扣押之物例如手機，因不會對執法者產生立即之危險，亦無滅失之風險，不得逕行開啟手機檢視內部資料，應要另取得令狀方得對手機內容搜索檢視。

在介接載體延伸之取證，若已有相關令狀，依刑事訴訟法第128條第 2 項之規定，得以適用目前相關搜索扣押規定，而不以介接載體為必要的遠端取證，並不在目前現行法規範的範圍內，故不能合法的使用。

三、小結

數位證據之載體、雲端與線上取證，如同前述所討論，區分載體標的與資訊標的是否一致而有相異之法律適用結論。數位證據仍有適用於現行搜索扣押規範，即必須有令狀的搜索扣押。惟在遠端操控程式的線上搜索，在我國現行法上並不容許。在科技一日千里的現代，偵查手段可能趕不及犯罪的手法，而造成法律制裁功能的喪失，因此要如何在這個數位時代下，同時保障人權及嚇阻犯法，將是未來法律人的挑戰及使命[257]。本研究團隊建議除了刑事偵查部

[256] 施育傑，同前註 241，頁 64-69。
[257] 施育傑，同前註 241，頁 55-70。

門應持續引進先進科技偵查手段外，亦應推動修法或制定科技偵查新法，確保刑事偵查機構有事當基本權干預之授權條款，同時要落實事前的公平法院審查原則，及事後的司法救濟，如此方能兼顧社會法益及人民基本權。

第二項 查緝利用金融科技遂行網路犯罪之障礙及挑戰

一、國家現行監理政策不明確

根據本研究第三章第四節第二項有關虛擬通貨監理模式之研析可知，我國針對虛擬通貨之監理態度偏向保守，首先針對應用型代幣我國尚無特定之監理規範[258]；支付型代幣（虛擬通貨）之監理，則以其是否涉及金錢儲值來觀察，一旦涉及儲值，可能有電子支付機構管理條例適用與否之問題，然而參照管理條例修正草案總說明可知[259]，金管會表示電子支付機構亦涉及金融特許範疇，業務形態介於銀行等收受存款機構與電子票證發行機構之間，故虛擬通貨服務並非電子支付機構之業務項目，故發行支付型代幣之業者似無從適用我國支付監管體系。此外，如果虛擬通貨被認為是資金或款項，而得做為匯兌業務之客體，則應適用銀行法之監管。

證券型代幣上，金管會已訂定規範納管，依據證券交易法第 6 條第 1 項規定，核定具證券性質之虛擬通貨為證券交易法所稱之有價證券，並有限度豁免證券交易法第 22 條第 1 項之申報規定等。然而因虛擬通貨之應用及發展歷程不夠久遠，現行法下何種虛擬通貨之功能及態樣可能構成我國法下之證券型虛擬通貨，則容有疑義[260]，常令行為人無法合理預期該虛擬通貨發行是否受刑法或相關證券法令之規範，同時也提高執法機構執法、查緝的難度。

二、執法機構向私部門調取可疑社群軟體帳戶不易

經本研究團隊研析，目前電子支付工具在我國已成為常態，並

[258] 陳丁章、范建得、黎昱萱，同前註 191，頁 96。
[259] 電子支付機構管理條例草案總說明，立法院第 8 屆第 6 會期地 2 次會議關係文書，院總字 1777 號。
[260] 陳丁章、范建得、黎昱萱，同前註 191，頁 98-99。

進一步結合社群軟體（例如 LINE）以及虛擬通貨交易所 APP，資訊流、金流及幣流(虛擬通貨)之產生極為迅速，例如犯罪者常以社群軟體設立私密群組、設定權限進行不法交易等資訊交換，而若欲進行交易時，犯罪者在手機上登入虛擬通貨交易所，將交易金額以「打幣」方式傳送至犯罪者之虛擬通貨錢包帳戶，犯罪者再將虛擬通貨「入金」至虛擬通貨交易所，轉換為法幣，再「出金」至一般銀行帳號，如此模式相當便捷迅速，可能轉眼 30 分鐘內即入帳完畢，若無完善配套及事後偵查手段介入，實為防不勝防。然而，在相關洗錢防制配套措施尚未落地以前，執法機構在查緝虛擬通貨尚容有許多障礙，其一即為向私部門調取可疑社群軟體帳戶不易，增加查緝困難度[261]。

為保障個人生活私密領域免於他人侵擾及個人資料之自主控制，我國憲法第 12 條明確規範「人民有秘密通訊之自由」。具體上保障人民的秘密通訊自由，則是由通訊保障及監察法（下簡稱「通保法」）規範之。通保法保障之通訊內容為「現時或未來發生」的通訊，為保障人民的隱私，若偵察機關在偵查的過程中，需要「通訊資料」或是監聽「通訊內容」則需依通保法規定聲請法院核發「調取票」與「通訊監察書」[262]。

而針對「過去已結束」的通訊內容，最高法院 106 年台非字第 259 號刑事判決認為「人民對於過去已結束之通訊內容，既享有一般隱私權，且通訊內容往往含有與本案無關之大量個人私密資訊，比其他身體、物件、處所、交通工具等之搜索，其隱私權之保障尤甚，應有法官保留原則之適用」，因此偵查機關原則上應向法院聲請核發搜索票，始得搜索、扣押，也導致偵查機關若需該犯罪嫌疑人之過去通訊資料或調取私部門(例如 Line)之使用者通訊內容，實務上並不容易。

更有甚者，由於 LINE 為境外日本公司主體，因此台灣偵查機構

[261] 蘇文杰、李穎、葉永全，毒品交易虛擬金流偵查新模式－以本局與荷蘭警方合作偵查個案為例，107 年毒品犯罪防制工作年報，頁 95。

[262] 通保法：Line 資料是警察想調就可以調嗎？，法操，自由評論網，https://talk.ltn.com.tw/article/breakingnews/2907573，最後瀏覽日：:2021 年 6 月 5 日。

若想要調取他國用戶資料，仍須適用與日本相同的處理原則，包括須取得搜索票及須經隱私權保護機構的驗證等[263]。LINE 最新發布之 LINE Transparency Report（透明度報告）中詳細分析計載「執法機關之用戶資訊調閱及內容刪除要求」。根據 LINE 公司統計，在 2020 年下半，台灣有 346 個調閱請求，實際處理比重不到 50%，共計有 197 件搜索票的聲請，影響台灣用戶總數為 327 人[264]。

[263] 同前揭註。

[264] https://linecorp.com/zh-hant/security/transparency/2020h2 ，最後瀏覽日：:2021 年 6 月 5 日。

第三節　金融科技犯罪其他國家主管機關及偵查制度比較分析

為深入瞭解其他國家執法機關於查緝電子支付工具及虛擬通貨相關犯罪所採行之調查工具、程序及方法，私部門協力方式及程度，作為我國之參考，確有必要進行比較法之研究與分析，本研究團隊以美國、英國、新加坡以及歐盟作為研究比較之對象。以下就各國金融科技犯罪偵查制度探討分析：

第一項 美國

一、美國金融監理制度概述

美國金融監理制度採多元監理體系，其聯邦監理機構包含財政部貨幣監理署（Office of the Comptroller of the Currency, OCC）、美國聯邦準備理事會（Board of Governors of the Federal Reserve System, Fed）、美國聯邦存款保險公司（Federal Deposit Insurance Corporation, FDIC）、證券交易委員會（The Securities and Exchange Commission, SEC）、商品期貨交易委員會（The Commodity Futures Trading Commission, FTC）等，而各州依照組織架構之不同，亦有其各自之銀行、證券、保險等監理機關，或其他金融監理機關例如紐約州金融服務廳（New York State Department of Financial Service）。

二、金融科技犯罪執法機關

美國並無單一金融科技犯罪之執法單位，由於金融科技犯罪涉及的犯罪型態非常多樣，例如虛擬通貨可能涉及的犯罪活動即包含各式聯邦詐欺相關罪名，例如電匯詐欺（wire fraud）、郵件詐欺（mail fraud）、證券詐欺（securities fraud）、存取詐欺（access device fraud）、身分竊盜及詐欺（identity theft and fraud）等；或是洗錢相關罪名，例如洗錢（money laundering）、涉及非法活動收益的交易（transactions involving proceeds of illegal activity）、非法經營貨幣傳輸業務（operation of an unlicensed money transmitting business）、違反銀行秘密法（failure to comply with Bank Secrecy Act requirements）、刑事沒收（criminal forfeiture）及民事沒收（civil forfeiture）等[265]。

[265] U.S. Department of Justice, *Report of the Attorney General's Cyber Digital Task Force:*

美國司法部（Department of Justice, DOJ）於 2018 年時成立網路數位專案組（Cyber-Digital Task Force）以對於新型態的科技發展強化其執法能力，根據網路數位專案組在 2020 年 10 月提出的虛擬通貨執法報告（Cryptocurrency Enforcement Framework）係將不當使用虛擬通貨的犯罪歸納為下列三種：(1)與交易相關的金融犯罪、(2)洗錢及避稅、(3)直接與虛擬通貨市場相關的犯罪，例如竊盜。[266]也因為犯罪的型態多樣，因此執法時，需由有權監理機關與執法機關密切合作，DOJ 作為負責調查及起訴犯罪的機構，即與各個監理機關及執法機關間建立強大的合作關係，包含與 SEC, FTC 及美國財政部(US department of the Treasury)旗下包含金融犯罪防制局（Financial Crimes Enforcement Network, FinCEN）、外國資產管制處（Office of Foreign Assets Control, OFAC）及及稅務局（Internal Revenue Service）。

茲以虛擬通貨最常見的幾種犯罪態樣，說明其監理機關與執法機構合作之模式：

1. **SEC 與美國司法部：**在違反美國證券交易法初次代幣發行（ICOs）案件中，由 SEC 與司法部密切合作。2018 年 1 月 25 日，SEC 在德州聯邦法院提起民事訴訟，試圖停止 AriseBank 涉嫌詐欺的 ICO， SEC 與 FBI 協調在 ICO 發行人臨時住所的搜索時間並執行民事訴訟中的凍結命令，使受害的投資人得以受償。其後，在 DOJ 的相關刑事案件中，達拉斯的聯邦大陪審團於 2018 年 11 月 20 日起訴 AriseBank 首席執行官 Jared Rice 詐欺投資者價值 400 萬美元的虛擬通貨資產，DOJ 的調查顯示 Jared Rice 有關 ICO 的聲明為不實陳述。最終，Jared Rice 在刑事案件中對於證券詐欺的指控認罪，在 SEC 的民事案件中同意賠償將近 270 萬美元的賠償金[267]。

Cryptocurrency Enforcement Framework, THE UNITED STATES DEPARTMENT JUSTICE (Oct. 2020), https://www.crowdfundinsider.com/wp-content/uploads/2020/10/DOJ-cryptocurrency_white_paper-10.8.20.pdf, at 29 (last visited Mar. 05, 2021).

[266] *Id*.

[267] *See* U.S. SEC, Executives Settle ICO Scam Charges, https://www.sec.gov/news/press-release/2018-280 (last visited: Oct. 22, 2020)

2. **美國財政部與美國司法部：**在洗錢防制及打擊恐怖主義方面，美國聯邦監理機構主要有外國資產管制處 OFAC、防制洗錢金融行動小組 FATF 及金融犯罪防制局 FinCEN，主要適用法規為銀行秘密法（Bank Secrecy Act, BSA）。在美國愛國者法案（USA Patriot Act）[268]的授權下，FinCEN 根據 BSA 透過接收和維護金融交易數據來執行其任務，分析、分享及協調各個金融機關以達成執法目的，以保護金融體系免於遭到非法使用，打擊洗錢活動以維護國家安全，而 FinCEN 作為美國的中央金融情報機構，同時也與其他國家的金融機關和國際機構建立全球合作[269]。
3. **FinCEN 與 DOJ 的合作通常在於兩大部分：**透過合規要求來防止洗錢及恐怖主義活動，及透過可疑活動的監管報告來協助調查。舉例來說，FinCEN 與美國聯邦檢察官加州北區辦公室（United States Attorney's Office **for** the Northern District of California）合作，處以 Ripple Labs Inc.及其子公司美金 700,000 的民事懲罰金。Ripple 是一家提供虛擬資產交易的公司，FinCEN 與 DOJ 各自的調查中都發現 Ripple 違反了幾項 BSA 的要求，沒有向 FinCEN 進行註冊並踐行 AML 的程序。最終 Ripple 與 DOJ 達成和解協議，沒收其美金 450,000 作為民事賠償的一部分，並免除刑事指控。

三、金融科技犯罪調查工具及方法

1. **BSA 數據追蹤**：2020 年時美國移民及海關執法局、美國郵政調查局及美國特勤局共同藉由 BSA 數據來辨識潛在的參與毒品銷售的暗網交易商[270]， 提供了一個路徑追蹤非法的數位貨幣，以確認這些暗網的毒品交易者，使執法機關成

[268] USA Patriots Act, https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act (last visited Oct. 22, 2020).
[269] FinCEN, What We Do, https://www.fincen.gov/what-we-do (last visited Oct. 22, 2020).
[270] FinCEN, Recognizes Law Enforcement Cases Significantly Impacted by Bank Secrecy Act Filings , https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act (last visited Oct. 22, 2020).

功取得搜查令並進行逮捕。這起行動共逮捕了 42 人，扣押價值共2200萬美元之多種數位貨幣、350萬美元之現金、藥物製造機器及各種管制藥物，並由德克薩斯州北區美國檢察官辦公室提起訴訟。

2. **執法人員發出傳票搜索**：2019 年美國紐約南區聯邦檢察官偵獲一起線上比特幣交易[271]，並成功起訴 7 人非法經營貨幣傳輸、詐欺、共同及賄賂。大多的交易都是為了促進非法活動，像是勒索軟體計劃或在暗網進行非法購買。大量的財務數據有助於確認交易平台使用的付款處理帳戶，以及與帳戶創建和營運相關者，使調查人員可以發出傳票，以獲得交易所營業賬戶和交易的完整帳目，調查人員也從中得知該交易平台其中一個所有人，同時經營一家大型國際犯罪企業，該企業從美國金融機構竊取超過 1 億人的個人數據，而該交易所則是被用來協助這家企業對其不法所得進行洗錢。

3. **透過新興科技進行調查**：目前美國參議院（United States Senate）審查中之推動創新協助執法法草案(H.R.2613 - **Advancing** Innovation to Assist Law **Enforcement** Act)[272]，要求 FinCEN 應對於 AI、數位身分技術、區塊鏈等新興技術領域之應用進行研究，並研究是否能夠利用這些技術來提升 FinCEN 的數據分析工作，以便更有效率地提供並協助聯邦、州或其他執法機構進行調查。

四、私部門協力程度與方式

根據 FATF 所發佈之私部門資訊共享指引（Private Sector Information Sharing）[273]，洗錢、資助恐怖主義及其他金融犯罪，因為其跨地域的特性，公部門及私部門間的資訊分享極為重要，尤其

[271] *Id.*

[272] H.R.2613 - Advancing Innovation to Assist Law Enforcement Act, https://www.congress.gov/bill/116th-congress/house-bill/2613/text?r=6&s=1, (last visited Oct. 22, 2020).

[273] FATF Guidance-Private Sector Information Sharing, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/guidance-information-sharing.html?hf=10&b=0&s=desc(fatf_releasedate), (last visited Oct. 25, 2020).

是金融機構之間，及金融機構與監理、執法機關之間。前述提及，金融犯罪防治局(FinCEN)作為美國的中央金融情報機構，在洗錢防制及打擊恐怖主義方面與其他國家的金融機關和國際機構建立全球合作[274]。FinCEN 會向私部門之金融機構蒐集金融數據，在洗錢、資助恐怖主義、或其他金融犯罪等案件執法具有重要價值。FinCEN 甚至每年頒獎予成功起訴的案例，一方面是表揚成功起訴的執法機構，另一方面也做為對金融機構提供有資訊價值之鼓勵。

依據美國特勤處調查辦公室發布之預訂工作報告[275]，財產扣押或犯罪沒收是打擊犯罪活動的重要執法工具，然而扣押虛擬通貨所面臨之執法上的困難，首先涉及與交易平台之合作及資訊交換，包括是否有權限命平台應交出用戶私鑰或是使其提供被移轉錢包之第三人之資訊。此外，此類資產如何再迅速返回或是兌換成法定貨幣給受害者，仍需要建構相對應的法制及監理機構與私部門的持續公開對話。

五、未來犯罪立法及執法方向

1. **金融科技保護法：**為了集中打擊金融科技犯罪，2019 年 1 月 28 日美國眾議院（United States House of Representatives）通過金融科技保護法（H.R.56 - Financial Technology Protection Act）[276]，目前正由參議院之銀行、住房和城市事務委員會（Committee on Banking, Housing, and Urban Affairs）審查該法案旨在提供對於新金融科技(例如數位貨幣)及其應用於恐怖主義及其他非法融資活動之調查，內容包含：
2. 設立一個打擊恐怖主義及非法融資之金融科技專案組（Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing）：

(1) 該專案組將由財政部長領導，與司法部長、國家情報局

[274] *Supra note* 269。

[275] U.S.Secret Service Office Of Investigations, Office Of Investigations Strategy Fy2021–2027, https://www.secretservice.gov/sites/default/files/reports/2021-01/inv-strategy-fy21-27.pdf (last visited Jun 18, 2021).

[276] H.R.56 - Financial Technology Protection Act, https://www.congress.gov/bill/116th-congress/house-bill/56/text?r=4&s=1, (last visited Oct. 22, 2020).

局長、FinCEN 局長，特勤局局長、聯邦調查局局長，及六名經財政部長徵詢其他成員候選任之私部門代表(包含銀行代表、非營利組織及金融科技專家顧問)組成；

(2) 專案組應對恐怖主義及非法使用新金融科技(包含虛擬通貨)進行獨立調查；

(3) 專案組應提出立法和監管建議，以改善反恐和反非法融資工作；每年應向國會提交年度報告。

3. 鼓勵民眾提供足以將涉及使用數位貨幣進行恐怖主義者定罪之資訊，提供資訊之人得享有不超過美金 450,000 元之獎金。

4. **美國特勤局網路詐欺專案組**[277]：為因應新型的金融科技犯罪，美國特勤局在 2020 年 7 月時宣布將下轄的電子犯罪專案組（Electronic Crimes Task Forces, ECTFs）及金融犯罪專案組（Financial Crimes Task Forces, FCTFs）整合，成立了網路詐欺專案組（Cyber Fraud Task Force, CFTF），期望透過整合可以讓傳統的電子犯罪及金融犯罪領域的專業知識及資源共享，以有效解決線上支付、跨境銀行業務及虛擬通貨之問題。

第二項 英國

一、英國金融監理制度概述

英國現行金融監理制度之機構，包含英格蘭銀行底下成立之金融政策委員會(Financial Policy Committee, FPC)，FPC 負責整體審慎監管(macro-prudential regulation)任務，維護英國全國金融系統之安全及穩定性[278]。另外成立金融行為監理總署(Financial Conduct Authority, FCA)，FCA 係獨立運作之政府機構，運作資金來源均來自於其管轄

[277] United States Secret Service, Field Offices, https://www.secretservice.gov/investigation/cftf/ , (last visited Oct. 22, 2020).

[278] *See* HM Treasury, *A new approach to financial regulation: building a stronger system*, 4-5, HM Treasury (Feb. 2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/81411/consult_newfinancial_regulation170211.pdf.

之金融機構繳交之規費，其主要建立健全之規則與機制，以保護消費者和金融市場[279]。另外審慎管理局(Prudential Regulation Authority, PRA)為英格蘭銀行轄下組織，成立主要係因全球金融海嘯暴露出金融機構系統性風險問題，其負責訂立規範及監理金融服務及產品之安全性，PRA 日常監理工作主要交由其成立之審慎監理委員會(Prudential Regulation Committee)負責[280]。FCA 和 PRA 兩者為緊密合作之不同組織，前者負責維護金融機構與消費者之間的健全關係，後者則是訂定審慎監理政策以控制風險。

二、金融科技犯罪執法機關

(一)執法機關

英國內政部(Home Office)管轄之英國國家打擊犯罪調查局(National Crime Agency, NCA)係就組織犯罪、人口或違禁品販運、網路犯罪、經濟犯罪等重大刑案之全國性執法單位[281]。關於網路犯罪，近年焦點多勒索軟體(ransomware)犯罪上，尤其是 2017 年 5 月起影響全球的「WannaCry」攻擊事件，英國之國民健保署受到該軟體攻擊。又 WannaCry 之勒索係要求以比特幣為解密文件之贖款，該次犯罪事件之跨國性與技術新穎性凸顯出執法機關專業之重要，NCA 表示，網路犯罪相較於全部犯罪事件之占比高達 47.5%，但是民眾實際遇到網路犯罪多未向執法機關通報，未來網路犯罪更加需要民眾及企業之資訊通報[282]。

NCA 於 2018 年成立國家經濟犯罪調查中心（National Economic Crime Centre, NECC），中心成員包含各個相關機關之代表，包含內政部、皇家檢控署(Crown Prosecution Service, CPS)倫敦市警察(City of London Police)、重大犯罪詐欺偵查署(Serious Fraud Office, SFO)、

[279] *See* FCA, About the FCA, https://www.fca.org.uk/about/the-fca (last visited Aug. 24, 2021).
[280] See Bank of England, What is the Prudential Regulation Authority (PRA)?, https://www.bankofengland.co.uk/knowledgebank/what-is-the-prudential-regulation-authority-pra (last visited Aug. 24, 2021)
[281] *See* NCA, What we do, https://www.nationalcrimeagency.gov.uk/what-we-do (last visited Aug. 24, 2021)
[282] *See* Warwick Ashford, *WannaCry a signal moment, says NCA*, ComputerWeekly.com (Jul. 04, 2017), https://www.computerweekly.com/news/450421936/WannaCry-a-signal-moment-says-NCA.

稅務海關總署 (HM Revenue and Customs)、金融行為監理總署 FCA、NCA，負責結合公部門及民間協力蒐集經濟犯罪情報並負責追訴[283]。另外 NECC 裡面包含防制洗錢之執法機關聯合洗錢情報工作組(Joint Money Laundering Intelligence Taskforce, JMLIT)，工作組包含超過 40 個金融機構、FCA、反詐欺民間組織(Cifas)以及其他執法單位，負責整合情報、調查並追訴洗錢犯罪[284]。以上部門合作組成之組織，標誌著打擊新興金融型態犯罪公部門合作及資訊交換之重要性。

(二)英國金融犯罪執法行動

1. NCA 對於虛擬通貨之態度

NCA 之網絡犯罪組主管曾接受採訪表示，任何鉅額虛擬通貨之交易都會被認為可能有犯罪疑慮，蓋一交易為何需要匿名、為何需要加密技術方能作成交易，不免有瓜田李下之嫌，不過其後 NCA 主管補充道，虛擬通貨交易本身並不可疑，但是因為現行金融法規對於虛擬通貨交易之監管未盡完善，故執法部門仍然傾向會對於各種類似交易作檢查[285]。另外執法單位也對於虛擬通貨用作洗錢或者犯罪標的表達疑慮，例如組織犯罪得以更隱密的方式從事不法交易，或者以虛擬通貨進行勒索以躲避追查。2018 年 5 月間，英國連鎖超市 Tesco 發現店內販售嬰兒食用奶粉遭到放置金屬碎片，並收到勒索信要求給付比特幣，其後警方經歷兩年調查，終於逮捕名叫 Nigel Wright 的農民，並向 Wright 追回犯罪調查期間臥底警察向其匯送超過 13 萬美金的比特幣[286]。

---

[283] *See* NCA, National Economic Crime Centre, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre (last visited: Aug 24, 2021)

[284] *See Id.*

[285] AMLi Correspondents, *INSIGHT: Top Cyber police chief warns about risks of exploitation by crime gangs when allowing bitcoin to purchase luxury property and private jets* (Jun. 12, 2021), https://www.amlintelligence.com/2021/06/insight-top-cyber-police-chief-warns-about-risks-of-exploitation-by-crime-gangs-when-allowing-bitcoin-to-purchase-luxury-property-and-private-jets/

[286] Scott Chipolina, *Farmer demanded £1.4 million of Bitcoin in Tesco blackmail plot* (Aug. 21, 2020), https://decrypt.co/39359/farmer-demanded-1-4-million-of-bitcoin-in-tesco-blackmail-plot

2. 跨國洗錢集團之逮捕行動

NCA 於 2019 年參與針對國際洗錢集團 QQAAZZ 的跨國調查行動，逮捕一共六名成員。QQAAZZ 嚴格來說並非網路犯罪集團本身，而其係為許多網路犯罪集團提供洗錢服務，例如為勒索軟體犯罪洗錢。此類行動標誌著新興金融犯罪往往具有跨越國界的性質，有賴跨國執法單位之合作，該次行動中除了 NCA 於英國的行動，另有洗錢集團成員於美國、澳洲等地落網[287]。2020 年 10 月，美國及葡萄牙主導包含英國等一共 16 個國家啟動「Operation 2BaGoldMule」計畫，展開空前大規模的跨國行動，搜索約 40 間民宅並且逮捕 20 名 QQAAZZ 洗錢集團之嫌疑人，美國、葡萄牙、西班牙及英國同步起訴該集團成員[288]。

三、金融科技犯罪調查工具及方法

(一)執法層面之工具

演算法及數據分析是執法層面首要工具之一，蓋資料分析可以及時辨別出哪些行為可能為異常行為，或者預測犯罪行為何時、何地出現，例如先進之資料分析可以預測罪犯之再犯機率有多高。同時人工智慧也可以應用於治安預防，例如透過閉路監視畫畫面分析人臉辨別身分[289]。在金融科技犯罪之執法方面，AI 和大數據分析亦有運用於偵測不法金融活動之潛力。

(二)英國監管科技之創新

英國於 2015 年率先提出監管科技(Regulation Technology, RegTech)之概念，以利用新科技監管市面上提供金融服務是否符合法規[290]。金融行為監理總署(FCA)近年持續投入於監管科技之創新與

[287] *See* Alex Scroxton, *Arrests and indictments made in cyber money laundering ring*, ComputerWeekly.com (Oct. 15, 2020), https://www.computerweekly.com/news/252490604/Arrests-and-indictments-made-in-cyber-money-laundering-ring.

[288] *See* Europol, 20 ARRESTS IN QQAAZZ MULTI-MILLION MONEY LAUNDERING CASE, Europol (Oct. 15, 2020), https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case.

[289] See UK Parliament, AI in policing and security, https://post.parliament.uk/ai-in-policing-and-security/ (last visited Aug. 24, 2021)

[290] 參硬塞科技字典，什麼是監管科技，https://www.inside.com.tw/article/7029-what-is-regtech (最

試驗，起初係為了解決以既有之方式偵測可疑金融交易之不足，然因為金融機構對於偵測犯罪亦有高度興趣，故 FCA 近年有相當多相關作為，例如舉辦 TechSprint 金融科技暨反洗錢論壇，供金融業界人士以及執法單位討論最新金融科技問題之活動。或者研發數位監管申報系統（Digital Regulatory Reporting, DRR）技術，降低金融業者回復監理機關報告之成本降低並提高資料之準確性。另外還有讓讓機器學習辨識客戶之數位身分，如此便不必由銀行行員臨櫃以人工方式核對客戶身分並輔以隱私強化技術(privacy enhancing technologies', PETs)，可以在不破壞資前提下，讓金融機構、監管機關以及國際執法單位分享情報，另外 PETs 亦可用於建立「黃金池」，避免公司內部資訊和主管機關資料有落差，以有效辨別實質受益人[291]。

(三)可疑交易報告

可疑交易報告(Suspicious Activity Reports, SAR)制度主要依據英國 2002 年犯罪得利法(POCA)以及 2000 年恐怖主義法案(TACT)，並輔以其他反洗錢法規所組成。根據犯罪得利法，若為受規定之特定行業人員，例如銀行業、會計業、不動產業等，若於業務過程中知悉或懷疑有企圖洗錢或資恐者，必須予以通報；另外根據恐怖主義法案，任何人若知悉或懷疑有洗錢活動或者應犯罪財產，便有通報可疑交易之義務，違反通報義務有刑事責任。SAR 由英國金融情報部門(UKFIU)接收，並可分享予需要之機構，例如給予稅務機關令其知悉是否有應課徵稅捐、令執法單位知悉是否有不法活動，或者令金融監理機關知悉可疑交易是否來自於監管不足或者金融服務或產品有缺陷[292]。

四、私部門協力程度與方式

金融機構或民間企業主動通報疑似犯罪情事或者事前預防偵測，

後瀏覽日：2021 年 8 月 24 日)

[291] *See* FCA, Turning technology against financial crime, Turning technology against financial crime (last visited Aug. 24, 2021)

[292] Suspicious Activity Reports, https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports (last visited:

可避免犯罪發生後造成之損害及成本，對於金融市場之誠信與穩定有其裨益。有鑒於 2020 年新冠肺炎疫情，全球人民生活型態巨變，避免人與人實體接觸的非現金支付及交易更顯常態，相應的詐騙手法也日益猖獗。金融機構透過參與英國財政大臣及財政部主持之經濟犯罪策略會議（Economic Crime Strategic Board），與執法單位合作，強化其與公部門之合作與資訊共享[293]。

金融行為監理總署(FCA)於 2018 年 6 月發表一封給國內金融機關執行長有關虛擬資產與金融犯罪之公開信，其說明儘管虛擬資產通常是被作非犯罪用途，如高風險投資或者企業募資，但是銀行應避免被當成幫助虛擬資產金融犯罪之幫兇，倘若發現客戶有頻繁從事虛擬資產交易或者以虛擬資產獲利龐大，比方銀行為客戶從事虛擬資產與法幣之匯兌服務，或者參與 ICO 時，金融機構應採取適當之安全措施，包含：

1. 教育訓練員工，幫助其偵測有金融犯罪高度風險的客戶活動；
2. 確保銀行從事之虛擬資產交易有既存法規可依循，且確保法規對於該種金融交易之未來發展亦可加以規範；
3. 和客戶溝通並了解其商業活動本質及其風險；
4. 對於客戶商業活動中的重要人物進行實地查核，並注意是否有負面情報；
5. 客戶要求為虛擬資產匯兌時，注意客戶自我查核是否有不足；
6. 若為ICO時，注意該投資大眾之組成、企業發起人為何、該虛擬資產之用途為何，以及該虛擬資產之流通範圍[294]。

除了政策教導呼籲之外，FCA 亦有立法要求金融機構在特情形下應通報情報。根據歐盟相關法規，其國內之洗錢與資金移轉法規定，受 FCA 監管之支付服務業者(payment service providers, PSPs)，

[293] UK Finance, FRAUD - THE FACTS 2021, 13 https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf (last visited: Aug 24, 2021)

[294] *See* FCA, *Dear CEO CRYPTOASSETS AND FINANCIAL CRIME*, 1-2, FCA (Jun. 11, 2018), https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-cryptoassets-financial-crime.pdf.

包含中間支付服務業者(intermediary payment service providers, IPSPs)，若發現有其他 PSP 頻繁地遺漏法律規定應提供之交易資訊(例如支付方之姓名、帳號、身分證明文件、地址等)，PSP 應通報 FCA 相關情事。通報事項應包含：

1. 遺漏應提供資訊之 PSP 或 IPSP；
2. 該 PSP 或 IPSP 之管轄國家；
3. 違反法規之具體細節，例如：(1)遺漏資訊之頻率；(2)發現遺漏資訊之期間；(3)PSP 或 IPSP 頻繁遺漏資訊是否有正當理由；
4. 詳細通報步驟。以上遺漏資訊之通報，應於發現有頻繁遺漏情事後三個月內為之[295]。

五、未來犯罪立法及執法方向

(一)虛擬資產與反洗錢法規註冊

自 2020 年 1 月 10 日起，事業主體之業務有涉及虛擬資產者皆須符合英國之「洗錢防制與打擊資助恐怖主義」(Anti-Money laundering/countering the financing of terrorism, AML/CFT)法規。符合此主體者包含提供虛擬資產匯兌者、提供虛擬資產 P2P 交易者、協助 ICO 者，以及虛擬資產託管錢包業者[296]。基於 AML/CFT 目的，金融行為監理總署(FCA)頒布虛擬資產業者之註冊措施，唯有通過 FCA 反洗錢審核者方能經營虛擬資產業務，惟多數申請註冊之業者多不符 FCA 規定，FCA 遂於 2020 年 12 月 16 日頒布暫時註冊規則(Temporary Registration Regime , TRR)，讓一些仍在受審核的業者可以繼續從事交易，目前 TRR 計畫之實施期間至 2022 年 3 月 31 日止[297]。須注意者，本註冊規定主要係考量業主有無遵守 AML/CFT 法規，消費者和以上業者從事交易時未必會較有保障，例如向金融消費評

[295] *See* FCA, Payment Service Providers that repeatedly fail to provide information, https://www.fca.org.uk/firms/financial-crime/payment-service-providers-repeatedly-fail-provide-information (last visited Aug. 24, 2021)
[296] *See* FCA, Cryptoassets: AML / CTF regime, https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime (last visited Aug. 24, 2021)
[297] *See Id*.

議中心申訴，或者可以從金融消費補償計畫（FSCS）得到補償金，業者應主動告知消費者其之間做成的交易有無相關金融消費者保護制度之適用[298]。

(二)數位執法之願景

英國警察局長理事會（The National Police Chiefs Council , NPCC)和警察及犯罪協會（The Association of Police and Crime Commissioners, APCC）共同發布了一份名為「全國警察數位政策」之報告，該報告強調數位執法之重要性，，並提到先進數位技術例如大數據、人工智慧對於執法有所幫助，例如在犯罪之前加以識別，但是有幾項主要挑戰須予以克服：

1. 第一是技術普及問題，若警方有能力分析資訊，意味著犯罪者可能也有相同能力，基於隱私及公眾安全考量，保管數據和建立起一個專屬於公部門、國家級的資訊中心便相當重要。
2. 第二是遺留技術（legacy technology）問題，舊有的技術缺乏可擴充性以及資訊可移植性，此會造成推動數位進程不可免的技術障礙[299]。該報告提出了未來十年希望達成的五項目標：
   (1) 無縫公民體驗：民眾得有更多多元管道可以和執法單位互動，同時要注意溝通時要注意安全隱私性；
   (2) 處理傷害：利用數據分析威脅、傷害及風險，以保護實體和網路世界之弱勢群體；
   (3) 提供執法單位提算所需的數位技術；
   (4) 和公共系統結合：和其他公部門合作，並確保資訊之在不同單位之間皆有可視讀性；
   (5) 賦權予私部門：制定明確規範讓私部門必要時可和警察合作交流資訊[300]。

---

[298] *See Id.*

[299] *See* Insight, How the UK Can Deliver its Digital Policing Vision, https://www.uk.insight.com/en-gb/content-and-resources/2020/articles/how-the-uk-can-deliver-its-digital-policing-vision (last visited Aug. 24, 2021)

[300] *See* NPCC, APCC, *NATIONAL POLICING DIGITAL STRATEGY: DIGITAL, DATA AND*

第三項 新加坡

一、新加坡金融監理制度概述

新加坡金融管理局(Monetary Authority of Singapore, MAS)為新加坡之中央銀行，兼具監管金融機構之職權，為世界上少數具有整合性監理功能之金融監理單位。新加坡金融管理有其特色，其對於金融檢查之比重較低，MAS 更重視金融集團整體審慎控管，如此一來可以降低金融監理機關為財務檢查的高額成本。又因為 MAS 金融檢查的重心較小，其更重視金融機構本身的自律，此作法同時也可以刺激優良金融業者有更多的創新空間，較不會被法規所侷限[301]。因新加坡本身有成為全球金融中心的野心與實力，MAS 對於金融科技與創新採取十分積極的態度。正在進行金融科技計畫舉例有：

(一)「金融部門技術與創新計劃」(Financial Sector Technology and Innovation Scheme, FSTI)，鼓勵金融機構成立創新中心，研發出解決問題的跨領域技術運用。

(二)電子支付領域：成立電子支付理事會，其由銀行、支付業者、一般企業及商會代表組成，負責推廣支付技術[302]。另外新加坡 2019 年通過的支付服務法(Payment Services Act , PSA)，要求支付業者必須申請執照納入監管。值得注意的是，PSA 監管範圍除了傳統的支付，也含括了虛擬貨幣的支付及對數位資產的監管，管理局已經從 2020 年開始用此法對未經許可的加密貨幣交易採取行動[303]。2021 年新加坡國會又通過支付服務法修正案，以擴大 MAS 監管範圍(例如將虛擬資產業者之範圍擴大為代幣轉讓、代幣保管及代幣匯兌)，以降低洗錢資恐等金融風險[304]。

TECHNOLOGY STRATEGY 2020–2030, 7-8, https://www.apccs.police.uk/media/4886/national-policing-digital-strategy-2020-2030.pdf (last visited Aug. 24, 2021)

[301] 參賴威仁，整合性金融監理的新思維，頁 1-2，http://www.tabf.org.tw/BECommon/Doc/FormEdit/1147.pdf (最後瀏覽日：2021 年 8 月 24 日)

[302] *See* MAS, MAS Establishes Payments Council, https://www.mas.gov.sg/news/media-releases/2017/mas-establishes-payments-council (last visited Aug. 24, 2021)

[303] 參區塊客，《支付服務法》正式上路 新加坡金管局：將促進支付領域的成長和創新，並減輕風險，https://blockcast.it/2020/01/30/sg-payment-service-act-come-into-effect/ （最後瀏覽日：2021 年 10 月 13 日）。

[304] 參科技法律研究所，新加坡國會通過支付服務法修正案，以降低洗錢及犯罪風險，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8622 （最後瀏覽日：2021 年 10 月 13 日）。

(三)建立智慧監管通報系統：其目的類似前述英國之 DRR 技術，係為了降低金融監管通報成本，並將通報資料標準化、自動化，且為了能將金融機構提供之資料用作學術研究，同時能將資料作去識別化[305]。

二、金融科技犯罪執法機關

針對商務事件或者白領犯罪，新加坡主要執法機關為新加坡警察局(Singapore Police Force)之商業事務局(Commercial Affairs Department, CAD)，另外新加坡檢察總署(Attorney-General's Chambers, AGC)同樣為具有執法權之檢察機關，當中的經濟犯罪與治理部(Economic Crimes and Governance Division)負責處理金融犯罪及貪腐案件。2015 年 3 月起，新加坡金融管理局(MAS)和 CAD 就金融犯罪案件採取合作辦案模式，結合監理以及執法兩個職權以增進偵辦案件效率[306]。涉及新興金融科技犯罪之執法實績例如：

(一)未經申請辦理支付服務犯罪案件。

一名 21 歲男子經網路應徵廣告要求，提供其帳戶給廣告主收受支付服務交易的款項。因該男子行為該當提供支付服務，其未經申請註冊且並非支付服務法規定除外不必註冊之人，該違法行為可處三年以下有期徒刑或處 125,000 新加坡元以下罰金[307]。男子未經註冊從事支付業務行為，因警方接獲超過 40 起網路消費詐欺之通報而調查發現之，CAD 最後將其逮捕。

(二)維卡幣詐騙案件

維卡幣（OneCoin）係一多層次傳銷型騙局，係由一保加利亞人 Ruja Ignatova 創立，其聲稱具有區塊鏈加密貨幣之特性，主打超越

---

[305] 參中央銀行業務局，〈金融科技破壞式創新：重塑金融與監管〉，頁 32，file:///C:/Users/CYL/Downloads/C10602508.pdf (最後瀏覽日：2021 年 8 月 24 日)

[306] *See* Financier Worldwide Magazine, Financial crimes in Singapore – an overview, https://www.financierworldwide.com/financial-crimes-in-singapore-an-overview#.YQ0Z5tQzY2w (last visited Aug. 24, 2021).

[307] *See* Singapore Police Force, MAN TO BE CHARGED FOR PROVIDING PAYMENT SERVICES WITHOUT LICENCE UNDER THE PAYMENT SERVICES ACT 2019, https://www.police.gov.sg/Media-Room/News/20201105_man_charged_for_providing_payment_servc_wo_licence_under_payment_servc_act_2019 (last visited Aug. 24, 2021).

比特幣之名號，後來被揭露其利用龐氏騙局手法吸金之詐騙，全球不法吸金所得將盡 50 億美元[308]。2019 年 4 月 10 日，兩名男子因為推銷維卡幣遭到起訴，本案 CAD 調查得發現民眾可以透過購買線上教育課程獲得代幣，該代幣可被用於維卡幣之挖礦，後來其中一名嫌疑人被以創立公司從事多層次傳銷違反相關管制法規起訴。MAS 已將 OneCoin 列入投資人警示清單（Investor Alert List），該清單中列舉了看似有合法經營外觀但實際上並未經過 MAS 核准之金融服務業者名單[309]。新加坡現今對於虛擬資產交易業者採取擴大監管之態度，業者必須先經過註冊方能合法執業，不過本件特別之處在於其實質上並未涉及虛擬資產業務，而係以虛擬資產名義違法吸引。MAS 也警示道，有業者宣稱新加坡未來會將發行虛擬貨幣作為法幣，而該業者為獨家銷售廠商，引誘投資人洩漏身份及金融資料[310]。

(三)網路詐騙偵查

2021 年 1 月間 CAD 和地區警方合作於全國進行為期二週的大規模執法，調查 251 名涉及網路詐欺之嫌疑人，嫌疑人年齡 15 歲到 74 歲不等，涉及案件包含網路愛情詐欺、網路購物詐欺、網路身份冒用、偽網路賭博平台及借貸詐欺，整體涉案金額高達 350 萬元新加坡幣。嫌疑人可能會被以詐欺罪以及洗錢罪起訴[311]。

三、金融科技犯罪調查工具及方法

(一)引進數據分析人才協助偵查金融犯罪

新加坡金融監理機關、執法單位以及民間金融機構組成之反洗

---

[308] 參動區，最大龐氏騙局｜150 億詐騙「OneCoin」主謀的弟弟與投資人和解，逃過 90 年監禁，https://www.blocktempo.com/onecoin-cofounder-agreed-on-a-settlement/（最後瀏覽日：2021 年 8 月 24 日）

[309] *See* Singapore Police Force, TWO MEN CHARGED FOR PROMOTING A MULTI-LEVEL MARKETING SCHEME INVOLVING CRYPTOCURRENCY (ONECOIN), https://www.police.gov.sg/media-room/news/20190410_arrest_two_men_charged_for_promoting_a_mlm_cad (last visited Oct. 13, 2021).

[310] *See* MAS, Warning on Fraudulent Websites Soliciting "Cryptocurrency" Investments,. https://www.mas.gov.sg/news/media-releases/2019/warning-on-fraudulent-websites-soliciting-cryptocurrency-investments (last visited Aug. 24, 2021).

[311] *See* CNA, 51 people under investigation for suspected involvement in scams, including 74-year-old: SPF, https://www.channelnewsasia.com/singapore/scams-spf-251-people-under-investigation-money-mules-412266 (last visited Aug. 24, 2021).

錢及反資恐合作計畫（Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership, ACIP）於 2018 年 11 月 29 日發表報告指出，利用大數據分析技術可預防洗錢以及資恐，以解決人工方式監管錯誤率過高、解讀法規錯誤等問題[312]。惟新加坡銀行業面臨數據人才不足之問題，因此報告建議銀行應與新加坡銀行與金融學院（The Institute of Banking & Finance, IBF）合作，積極培育數據人才，同時引進國外人才[313]。

(二)可疑交易報告處（Suspicious Transaction Reporting Office, STRO）

STRO 為新加坡警察底下之單位，負責接受可疑交易申報並且協助將資訊傳遞給金融監管單位和其他執法機關。可疑交易例如 1. 貴重金屬寶石業者、典當業者若為貴重金屬寶石之交易，若發現交易金額逾越兩萬新加坡幣、或者同一客人於單日從事兩件以上貴重金屬寶石交易等，此便可能係可疑交易。2. 賭場若發現賭客從事超過一萬元新加坡幣之現金兌換，若單日內累積交易超過一萬元，亦為需要申報之可疑交易[314]。

(三)監理科技 SupTech 之運用

前述提到的 Regtech，係用以偵測新興金融科技是否符合法規，故金融機構本身可運用 RegTech 檢視自身產品或服務是否符合監管法規。而 SupTech 特指監理機關一方所運用之科技手段，例如搜集所有金融機構之數據並分析，或者即時進入金融機構資料庫監看之技術，故亦有文獻稱 SupTech 為「RegTech for supervisor」[315]。根據

---

[312] *See* ACIP, *Industry Perspectives – Adopting Data Analytics Methods for AML/CFT*, 3, https://abs.org.sg/docs/library/acip-working-group-paper---data-analytics-for-aml.pdf (last visited Aug 24, 2021).

[313] 參台灣經貿網，新加坡銀行業將增加數據分析人才以更準確偵查金融犯罪案件，https://info.taiwantrade.com/biznews/%E6%96%B0%E5%8A%A0%E5%9D%A1%E9%8A%80%E8%A1%8C%E6%A5%AD%E5%B0%87%E5%A2%9E%E5%8A%A0%E6%95%B8%E6%93%9A%E5%88%86%E6%9E%90%E4%BA%BA%E6%89%8D%E4%BB%A5%E6%9B%B4%E6%BA%96%E7%A2%BA%E5%81%B5%E6%9F%A5%E9%87%91%E8%9E%8D%E7%8A%AF%E7%BD%AA%E6%A1%88%E4%BB%B6-1672046.html（最後瀏覽日：2021 年 8 月 24 日）

[314] *See* Singapore Police Force, SUSPICIOUS TRANSACTION REPORTING OFFICE (STRO), https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office (last visited Aug. 24, 2021)

[315] *See* Toronto Centre, FinTech, RegTech and SupTech: What They Mean for Financial Supervision, 10-11, https://res.torontocentre.org/guidedocs/FinTech%20RegTech%20and%20SupTech%20-%20What%20They%20Mean%20for%20Financial%20Supervision%20FINAL.pdf (last visited Oct.

國際結算銀行 2018 年 7 月發佈關於 SupTech 之報告，新加坡金融管理局(MAS)已經有下列 SupTech 技術運作實施中[316]： 1. 機器可讀取規定（Machine-readable regulation）及自然語言處理（Natural Language Processing, NLP）：NLP 簡言之係讓電腦理解人了語言之技術，而利用自然語言技術可將法規範文字轉換成機器可讀取之格式，以降低立法目的與解釋適用後之落差； 2. 大數據及人工智慧：3. 機器學習。

四、私部門協力程度與方式

2017 年 4 月，新加坡金融管理局(MAS)以及新加坡警察局之商業事務部(CAD)宣布結合監管機關、民間企業、執法單位及公部門組成「洗錢防制及打擊資助恐怖主義產業合作」(Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership, ACIP)。ACIP 由 MAS 及 CAD 主持、並和八家銀行及組織組成指導小組，由其決定何種洗錢防制與打擊資助恐怖主義(AML/CFT)風險須優先研究，並交由底下之工作小組研究，而工作小組交由指導小組成員之一以及金融機構或其他相關產業成員組成，以加強 AML/CFT 業務交流之制度化[317]。

因金融機構每日經手大筆交易資訊，且具有資歷建立先端科技整理分析資訊，公部門及金融機構合作監管及搜查犯罪可以大幅降執法成本。CAD 便和華僑銀行合作「Project POET (Production Orders: Electronic Transmission)」計畫，利用華僑銀行自動處理和傳遞資訊之技術將交易訊息傳給執法機關，此流程以往需要以人工方式並花十天至三個月，華僑銀行只須一至二個工作天便可以完成。此外「Project POET」還可以人工智慧和數據分析監看金融交易是否有實

13, 2021).

[316] *See* Bank for International Settlements, *FSI Insights on policy implementation No 9: Innovative technology in financial supervision (suptech) – the experience of early users*, 5, https://www.bis.org/fsi/publ/insights9.pdf (last visited Aug. 24, 2021).

[317] *See* MAS, *CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes*, https://www.mas.gov.sg/news/media-releases/2017/cad-and-mas-partner-industry-stakeholders-to-fight-financial-crimes (last visited Aug. 24, 2021).

質受益人或者可疑交易人或團體，有助於 AML/CFT 制度之落實[318]。

除了科技方法以外，最傳統的民眾通報亦為不可或缺的力量。CAD 於 2021 年 6 月便表揚 114 位民眾及 17 個組織（包含企業、銀行或民間協會），其在 2020 年間一共偵測或阻止了 83 件詐騙案件，大多數案件為網路愛情詐欺，阻止了約 320 萬新加坡幣的損失[319]。

五、未來犯罪立法及執法方向

(一)執法機關動向

近年新加坡詐欺問題日漸嚴重，2019 年期間詐欺案件量比去年上升了 54%，佔整體犯罪量 27%。新加坡於 2020 年成立跨部會委員會專門解決詐騙問題（Inter Ministry Committee on Scams），部會包含內政部、通訊資訊部、貿易產業部，手段包含辨識潛在的詐騙份子並且禁止其行為、協助減輕受害損失以及教育大眾。另外打擊詐欺犯罪同時有賴支付業主與銀行業之合作，以及提升民眾防詐意識[320]。其他相關作為還有組成前線計劃（Project FRONTIER），結合警察、金融機構以及通訊業者及時攔截詐騙份子之不法收益並迅速回復受騙損害，該計劃於 2020 年成功收回 570 萬新加坡元之損害[321]。

新加坡在亞太地區的執法角色也日漸重要。2021 年 5 月國際刑警組織發動「Operation Haechi-I」行動，於亞太地區攔截了 830 萬美金的詐騙不法獲益，並逮捕 585 位嫌疑人。當中有受害人收到宣稱為「新加坡高等法院」來電，並指示其將金融資料提供給一個假的新加坡警方網站。新加坡警方後來調查發現該假網站伺服器係在韓

---

[318] *See* Finextra, *Singapore police force taps OCBC transaction data to fight financial crime*, https://www.finextra.com/pressarticle/79162/singapore-police-force-taps-ocbc-transaction-data-to-fight-financial-crime (last visited Aug. 24, 2021).

[319] *See* The Strait Times, *17 organisations, 114 people get awards from Commercial Affairs Department for thwarting scams*, https://www.straitstimes.com/singapore/courts-crime/17-organisations-114-people-get-awards-from-commercial-affairs-department-for (last visited Aug. 24, 2021).

[320] *See* CNA, *New Inter-Ministry Committee to be set up to combat scams*, https://www.channelnewsasia.com/singapore/new-inter-ministry-committee-be-set-combat-scams-768621 (last visited Aug. 24, 2021).

[321] *See* Ministry of Home Affairs, *Association of Banks in Singapore Financial Crime Seminar 2021, "Deepening Partnerships to Combat Financial Crime" – Keynote Address by Mr Desmond Tan, Minister of State, Ministry of Home Affairs and Ministry of Sustainability and the Environment*, https://www.mha.gov.sg/mediaroom/speeches/association-of-banks-in-singapore-financial-crime-seminar-2021-deepening-partnerships-to-combat-financial-crime/ (last visited Aug. 24, 2021).

國架設，故警方向通知韓國下架該網站，並在進一步偵查後，後續便與國際刑警組織開啟大規模跨國執法[322]。

(二)洗錢防制規定動向

根據新加坡洗錢防制一般規定「貪腐、販毒及其他嚴重犯罪(利益沒收)法」規定，任何人知道有可疑交易時，負有向新加坡警察局商業事務部通報之義務，未通報者可能負有刑事責任，此規定適用於所有財產交易，故虛擬通貨交易若有可疑交易疑慮，亦為須通報案件；另外根據「恐怖份子(融資抑制)法」，任何人若有恐怖份子或恐怖份子組織就任何財產為占有、保管或控制之資訊，均負有揭露義務，故恐怖份子持有虛擬通貨同樣會被認定為應通報事件[323]。以上對於反洗錢規定現已擴及將虛擬通貨交易列為執法對象，同時配合新加坡 2019 年支付服務法將虛擬通貨業者納入監管，以上措施對於虛擬通貨金融有更加嚴格的監控管理。

另外，新加坡金融管理局(MAS)於 2021 年 10 月發布新聞稿表示，將和六家商業銀行合作建立一個名為「COSMIC」數位平台，讓金融機構可以交換客戶交易資訊以洗錢防制、打擊資恐及防制資助武器擴散(proliferation financing)，COSMIC 平台企圖打造世界第一個具有標準化中心的平台以提升資訊匯入及分析，平台目前預計於 2023 年上半年上線[324]。

第四項 歐盟

一、歐盟金融監理制度概述

歐盟於 2008 年全球金融海嘯後，訂立歐洲金融監管體系(European System of Financial Supervision, ESFS)，ESFS 分為兩大架構，其一為整體審慎監理之歐盟系統風險委員會（European System

[322] *See* The Strait Times, S'pore police played 'critical role' in Interpol's online financial crime probe; $110m intercepted, https://www.straitstimes.com/singapore/spore-police-played-critical-role-in-interpol-probe-into-online-financial-crimes-us83m (last visited Aug. 24, 2021).
[323] Kenneth Pereire, Lin YingXin, *Blockchain & Cryptocurrency Laws and Regulations | Singapore*, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/singapore
[324] MAS, *MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering* (Oct. 1, 2021), https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering

Risk Board, ESRB），其二為金融個體層面之監理系統，共有三個歐盟監理機關（European Supervision Authorities, ESAs）：1. 歐洲銀行管理局（European Banking Authority, EBA），歐洲保險和職業養老金管理局（EIOPA）和歐洲證券及市場管理局（ESMA）。監理機關當中之歐洲銀行管理局(EBA)以及歐洲中央銀行（European Central Bank, ECB）為共同管理歐元區金融機構之組織，並對於

會員國之內國法及金融政策有一定程度之強制力，例如其可以訂立統一規定要求各會員國落實、若有損害金融市場事件時得要求會員國主管機關調查、要求會員國主管機關分享資訊等，由上可知歐盟對於內國法之形成以及金融監理具有實質影響力[325]。

二、金融科技犯罪執法機關

(一)歐洲刑警組織

歐盟就經濟、商業、外交上緊密不分，警政及司法合作亦為重要之一環。面對現代犯罪型態日漸組織化、跨國化，以國家為單位之執法模式會面臨執法各種執法上的困境，例如罪犯潛逃出境難以跨境逮捕、刑事程序裁定效力不及於國外、一國檢警單位搜查到之證據可能不被他國司法機關承認種種問題，近年恐怖活動及洗錢問題尤其受到重視，故歐盟就重大犯罪，尤其是就金融犯罪之國際合作近年改革頻頻。

歐洲刑警組織(Europol)於 1997 年 1 月開始運作，根據 1995 年 7 月簽訂之歐洲刑警組織協定第三條規定，Europol 之主要職責為：1. 促進會員國間之資訊交換；2. 蒐集、核對並分析資訊及情報；3. 有犯罪情形時通報會員國主管機關；4. 促進會員國就轉發之資料予以調查；5. 建立電子化資料庫保存資料[326]。可見 Europol 主要職權為情報交換及整理，不過其並無法源依據可以主動展開調查行動，亦無對於會員國境內展開逮捕拘提之權限。2009 年 4 月歐盟修改 Europol 憲章，賦予 Europol 所有調查跨國犯罪之權限，不再僅限於觀察及資

[325] 參李貴英、聶家音，歐洲聯盟經濟治理與金融監理架構之改革，月旦法學雜誌 232 期，頁 90-91，2014 年 9 月。

[326] *See* Europol l Convention, Article 3.

料情報分析[327]。Europol 底下另成立歐洲金融經濟犯罪中心(European Financial and Economic Crime Centre)專門調查洗錢、詐騙集貪汙等犯罪，其主要職責為就上述經濟金融犯罪之情報中心、協助調查及情報分析、提供培訓、促進金融經濟犯罪執法，不過同樣並無主動為刑事拘捕等強制處分之權限[328]。

金融犯罪以及網路犯罪同樣在 Europol 的打擊範圍。就支付工具犯罪的部分，Europol 將支付卡詐欺分為有卡詐欺(信用卡、簽帳卡)，主要發生 ATM 或者零售店；以及無卡詐欺，通常發生在網路上。據統計，2013 年間無卡詐欺犯罪金額為 14.4 億歐元，在單一歐元支付區(SEPA)之支付卡詐欺中占 66%，Europol 參與之無卡詐欺案件，客戶之金融資料通常係在私部門中被內部人或者惡意軟體盜用[329]。至於虛擬資產方面，Europol 曾於一個歷經 6 年的「Operation Warenagent」行動，協助破獲一件網路詐欺兼洗錢犯罪。該案中犯罪集團盜用他人資料並購買高價值商品，並招募人員先在德國簽收包裹後再轉寄給東歐地區由犯罪者收取贓物，而犯罪集團透過加密技術及虛擬資產來協調行動、隱匿足跡並洗錢，Europol 協助分析資訊最後定位犯罪集團之關鍵巢穴位於賽普勒斯，最後成功在 9 個國家逮捕 15 名嫌疑人[330]。

(二)歐洲司法合作機關

如前所述，歐洲刑警組織為收集並分析資料之機關，並不具有偵查逮捕權限。歐盟真正具有調查權限之機關為歐洲司法合作機關(Eurojust)。其設立於 2002 年，其具有法人格，機關所在地為荷蘭海牙，組成員為會員國各派遣一名之法官或檢察官，負責協調會員國或者第三國的檢察機關對於跨國犯罪偵查或起訴[331]。Eurojust 另可要

[327] 參鄭文中，淺論歐盟刑事司法合作之歷史發展，台灣國際研究季刊，14 卷 3 期，頁 27-30，2018 年 9 月。

[328] *See* Europol, European Financial and Economic Crime Centre, https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc (last visited Aug. 24, 2021).

[329] *See* Europol, Payment Fraud, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud (last visited Oct. 13, 2021).

[330] *See* Europol, ONLINE SCAMMERS CAPTURED AFTER CAUSING EUR 18 MILLION OF DAMAGE IN MORE THAN 35 000 CASES, https://www.europol.europa.eu/newsroom/news/online-scammers-captured-after-causing-eur-18-million-of-damage-in-more-35-000-cases (last visited Aug. 24, 2021).

[331] *See* Eurojust, Who we are, https://www.eurojust.europa.eu/about-us/who-we-are (last visited Aug. 24,

求會員國成立聯合調查小組(Joint investigation teams)以調查跨國刑事犯罪，小組由會員國之執法及司法機關組成(包含法官)，由 Eurojust 提供小組營運、法律及財務之支持[332]。Eurojust 必要時，亦有權向會員國調閱資料，自己接手啟動犯罪偵查及追訴，若會員國拒絕提供協助時，需說明其拒絕之理由為何[333]

新興金融科技犯罪時常與網路犯罪、洗錢犯罪結合，而使用惡意軟體、網路釣魚、利用虛擬資產洗錢等網路犯罪為 Eurojust 重點負責案件之一。執法實績方面，Eurojust 在前述之「Operation Warenagent」行動以組成聯合調查小組之身分參與調查與執法。另外 Eurojust 曾與歐洲刑警組織、英國籍荷蘭當局破獲一起價值 2400 萬英鎊之竊盜案件，該竊案嫌疑人架設仿冒之虛擬資產網站，受害人進入網站後嫌疑人便有機可乘得進入受害人之比特幣錢包竊取資訊及資產。英國警方調查後發現本案嫌疑人疑似在荷蘭，便將資訊交由歐洲刑警組織(Europol)彙整分析，並由 Eurojust 展開協調會議擬定作戰計畫，最後與荷蘭及英國兩地逮捕 6 名嫌疑人[334]。2020 年 7 月，Eurojust 協助相關當局與義大利及羅馬尼亞破獲一個涉及大額金融詐欺、網路犯罪及洗錢之犯罪網路，該網路與義大利部下人頭帳戶，透過各種詐騙手法(例如出售不存在之貨品、出租不存在之房屋)與全歐洲至少有 2000 萬元之不法獲利。Eurojust 協助義大利及羅馬尼亞執法機關進行即時的訊息交換，以及協調兩者之執法行動[335]。

三、金融科技犯罪調查工具及方法

(一)跨境之刑事偵查手段

2021).

[332] *See* Eurojust, Joint investigation teams, https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams (last visited Aug. 24, 2021).

[333] 鄭文中，同前註 327，頁 31。

[334] *See* Eurojust, €24 million cryptocurrency theft unraveled with Eurojust's support, €24 million cryptocurrency theft unraveled with Eurojust's support | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu) (last visited Aug. 24, 2021).

[335] *See* Eurojust, Italian and Romanian judicial authorities; with Eurojust's support; dismantle major criminal network in financial fraud; cybercrime and money laundering, https://www.eurojust.europa.eu/italian-and-romanian-judicial-authorities-eurojusts-support-dismantle-major-criminal-network (last visited Aug. 24, 2021).

刑事偵查及之強制處分為國家主權之展現，且部分刑事手段象徵背後之政治或人權問題(例如相同罪名在一國中最高可判處死刑但是在另一國已經廢除死刑，另一國可能不願意引渡罪犯至可能判處死刑之國家；或者部分罪犯可能被認定為政治犯便有引渡爭議)，故跨國執法為國家敏感事務；相對地恐怖主義、組織犯罪以及洗錢犯罪往往為各國共同打擊目標，此時又有執法合作之需要。歐盟為了解決跨境執法之爭議，有下列手段予以解決執法困境[336]：

1. 歐盟逮捕令(European Arrest Warrant)：由特定會員國簽發，要求另一國對於特定人完成逮捕並且移交至簽發國。
2. 歐盟證據令(European Evidence Warrant)：由特定會員國司法機關裁定，要求取得對另一國境內之物品、文件或資料。此係為各國之間調查證據可以互相承認並執行。
3. 歐盟偵查令(European Investigation Order)：因會員國之間可能互相不承認他國之取證，從而影響歐盟證據令之效益，故歐盟針對各過互相承認證據之效力規定出一套框架，規定取得證據之方法、取證之限制以及拒絕其他會員國請求取證之理由。

歐盟在努力消弭跨國執法之障礙上已經有諸多努力，根據歐洲司法合作機關(Eurojust)於 2020 年發布之成果報告，其自從 2011 年成立協調中心協助各會員國就執法行動及訊息交換，已經有 1722 起和各國當地執法機關合作之逮捕行動、3355 起搜索行動、查獲 2 億 1 千萬歐元不法獲利，案件類型包括走私、網路犯罪、恐怖主義、性剝削、金融詐騙以及洗錢[337]。

(二)數位執法之引進(Digital Criminal Justice)

歐洲司法合作機關(Eurojust)在 2018 年提出了數位執法之願景，以期能夠更快地交換刑事案件之證據及資訊，其並在 2020 年 7 月提出報告。報告指出，有鑒於好幾個刑事或執法機關已建立起

[336] 鄭文中，同前註 327，頁 33-36。

[337] *See* Eurojust, Eurojust action days: Financial impact of EUR 2 billion and more than 1 700 arrests, https://www.eurojust.europa.eu/eurojust-action-days-financial-impact-eur-2-billion-and-more-1-700-arrests (lats visited Aug. 24, 2021).

先進之數位系統可進行資訊之收集、分享及分享，例如歐洲刑警組織(Europol)、歐洲大型 IT 系統維護機構（European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, eu-LISA）以及邊境管理局（Frontex），但是 Eurojust 的跨國執法協調機制卻十分落後，Eurojust 應該建立起一個可讓司法人員快速且容易進入取得資訊的系統，並且重新設計案件管理系統和案件交差比對系統，另外也必須讓系統足以應付巨量資訊傳送以及儲存[338]。

四、私部門協力程度與方式

歐洲刑警組織(Europol)於 2010 年以四年為週期之執法計畫「EMPACT」，其目的為更有效地打擊跨國及組織犯罪，希望結合歐盟、其他歐盟機關、會員國、會員國以外第三國、國際組織與其他私部門能夠以具有方法論一致地之手段合作打擊嚴重犯罪。歐盟理事會於 2017 年 5 月 18 日啟動了 2018 年到 2021 年的計畫，專注打擊包含網路犯罪、金融洗錢犯罪等[339]。因 Europol 主要職責為訊息收集與分析，故私部門協力主動分享資訊十分重要。

EMPACT 計畫之合作實績，例如 2019 年時 Europol 啟動「2019 e-Commerce Action」行動，該行動係 EMPACT 計畫底下之延續，結合銀行、零售業者以及物流業者共同打擊電子商務詐欺(此指利用網路平台或者應用程式竊取他人信用卡資訊購買商品或服務之犯罪)，並有全球 535 家網路業者組成之商品風險委員會最為重要參與者之一。不過因，為電子商務詐欺近年來到盜買服務而非盜買實體商品的案件越來越多，例如行為人盜買火車票再轉賣給第三人，或者盜買現金券之後行為人再去銀行贖回現金，此現象增加查緝難度，因此該行動也倡議應乾提升防詐意識，並且加強事前預防之機制，例如強化身分驗證機制(Strong Customer Authentication, SCA)[340]。

---

[338] *See* Eurojust, Digital Criminal Justice, https://www.eurojust.europa.eu/judicial-cooperation/judicial-cooperation-instruments/digital-criminal-justice (last visited Aug. 24, 2021)

[339] *See* Europol, EU POLICY CYCLE – EMPACT, https://www.europol.europa.eu/empact (last visited Aug. 24, 2021).

[340] *See* Europol, 60 E-COMMERCE FRAUDSTERS BUSTED DURING INTERNATIONAL

五、未來犯罪立法及執法方向

(一)虛擬通貨最新監管架構

歐洲證券及市場管理局(ESMA)於 2019 年 1 月作出一份針對 ICO 以及虛擬資產法律地位之完整報告[341]。該報告就較側重於初級市場層面，其強調虛擬資產首先應經過個別之測試檢視其是否為金融工具。若答案為肯定，其才會有落入金融監管法規範疇內之問題，過有鑑於虛擬資產之特殊性，現有法規可能還有尚未解決之漏洞和問題；若答案為否定，該虛擬資產便不受監管，消費者便需要注意為相關交易時的風險，ESMA 支持英對所有虛擬資產有關的交易都列入反洗錢反資孔之範圍內[342]。歐洲銀行管理局(EBA)提出另一份報告，認為目前市面上的虛擬資產不受到金融法規監管，須注意可能引發的消費者保護、營運彈性以及市場健全性之問題，EBA 另外同樣肯定將虛擬資產之交易活動納入反洗錢反資孔之範圍內[343]。近期歐盟監理機關(ESAs)於 2021 年 3 月再度表態，對於加密資產發出警示，表示因歐盟地區大部分之加密資產大多未經過核准，投資人購買或持有虛擬資產不會受到現有法規之保障，可能承受高額金錢之損失[344]。

(二)歐洲檢察署之成立

歐盟的執法機關層面，儘管歐洲司法合作機關(Eurojust)似乎已經具有主動就跨國犯罪追訴之權限，惟 Eurojust 有人手不足問題，且因聯合偵查欠缺具體規範架構，多係以個案方式進行，此會花費過多時間在前置協調及磋商程序上[345]。2021 年 6 月 1 日歐盟正式開始

OPERATION, https://www.europol.europa.eu/newsroom/news/60-e-commerce-fraudsters-busted-during-international-operation (last visited Aug. 24, 2021).

[341] *See* ESMA, *Advice: Initial Coin Offerings and Crypto-Assets*, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (last visited Oct. 13, 2021).

[342] *See* Simmons & Simmons LLP, https://www.simmons-simmons.com/en/publications/ck0bbibrqepe40b59a0g15p8n/100118-esma-and-eba-publications-on-crypto-assets (last visited Aug. 24, 2021).

[343] *See Id*.

[344] *See* EBA, Crypto-assets: ESAs remind consumers about risks, https://www.eba.europa.eu/financial-innovation-and-fintech/publications-on-financial-innovation/crypto-assets-esas-remind-consumers-about-risks (last visited Oct. 13, 2021).

[345] 鄭文中，同前註 327，頁 32, 40。

營運新的跨國執法組織：歐洲檢察署(European Public Prosecutor's Office, EPPO)。歐洲檢察署具有獨立的調查權及起訴權限，主要針對侵害歐盟經利益（指根據歐盟預算或條約設立之組織、團體、機構等所衍生之各式收支財務事務）的大型金融犯罪為執法案件，例如金額超過一千萬歐元之跨境增值稅詐欺（VAT fraud）、侵害歐盟利益之詐欺或者貪污案、洗錢及組織犯罪等[346]。EPPO 和 Eurojust 為平行平等機構，兩機構於 2021 年 2 月簽署工作安排計畫，兩者與歐洲刑警組織(Europol)可以互相合作[347]。

(三)歐盟洗錢規定新進展

2021 年 7 月 20 日，歐盟發佈新聞稿表示要全面翻新歐盟地區的反洗錢法規。該項極具野心的計畫包含要新設一個專門負責洗錢防制與打擊資助恐怖主義(AML/CFT)的歐盟機關 AMLA（EU-level Anti-Money Laundering Authority），該機關將和金融情報機關（Financial Intelligence Units, FIU）合作並負責協調各會員國的中央機關，確保全歐盟各國有一致性地法規可落實，並且可以對於高風險的金融機構直接監管[348]。另外歐盟也要頒布一個新的 AML/CFT 第六號指令已取代舊有規定，該指令會直接轉變為內國法，作為金融機構及金融情報機構之遵循依據，另外各會員國的國家銀行帳戶系統將被連結起來，執法機關被賦予權限進入該連結系統以便能更快速地調查洗錢活動[349]。值得注意的是，新的 AML/CFT 規定要求將所有虛擬資產產業全部納入監管，除須對客戶盡職調查，所有虛擬資產交易必須有可追溯性，並且禁止匿名錢包存在[350]。同時，因為現金交易無法偵測是否有洗錢情事，歐盟統一對於各國設下 10.000 歐元之現金交易限制。另外歐盟也將參考 FATF 名單對於國際上其他國

[346] *See* EPPO, Mission and tasks. https://www.eppo.europa.eu/en/mission-and-tasks (last visited Oct. 13, 2021).
[347] *See* Eurojust, Eurojust and EPPO sign Working Arrangement to facilitate cooperation, https://www.eurojust.europa.eu/eurojust-and-eppo-sign-working-arrangement-facilitate-cooperation (last visited Oct. 13, 2021).
[348] *See* European Commission, Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690 (last visited Oct. 13, 2021).
[349] *See Id.*
[350] *See Id.*

家以黑名單或灰名單分類，以確保與各國金融交易之風險[351]。

第五項 小結

虛擬通貨交易由於匿名性、缺乏中央化的實體、跨國移轉迅速等特性增加了政府機關監管相關犯罪的困難度，而相關之偵查手法亦無法向大眾公開[352]。目前各國對於虛擬通貨之監管亦均尚在起步階段，監理的實際狀況仍在不斷變化。而電子支付工具同樣因為交易速度快、可能利用人頭帳戶，導致查緝衍生之詐騙、洗錢犯罪亦有賴監管機關及執法機關更加專業、資訊交流並整合式地作犯罪預防及犯罪偵查。

本文根據以上美國、英國、新加坡及歐盟等地區新興金融科技遭濫用於犯罪之現狀與法規，觀察到以下的方向：

一、金融機構及金融科技業者協助執法之角色日漸重要

執法機關與民間合作最重要者為資訊共享，例如英國的金融機構參閱由財政部舉辦之經濟犯罪策略會議，強化資訊共享。或者更加制度化之選項，例如新加坡的洗錢防制及打擊資助恐怖主義產業合作，係由執法機關和金融監理機關共同主持，與民間一同研究犯罪風險議題並交流資訊。

民間合作的力量同樣用於更具體的犯罪執法層面。例如虛擬通貨業者在協助識別不法資金來源可如同金融機關，扮演著關鍵作用，除了向執法機關申報可疑交易外，暫停可疑帳戶交易、資產扣押及證據之保存均需相關業者之協力。例如全球四大虛擬通貨交易所 Coinbase、Paxful、Gemini 和 BitFinex 於 2020 年宣布他們將加入反人口販賣加密貨幣聯盟（ATCC）[353]，透過虛擬通貨服務提供商、商

---

[351] *See Id.*

[352] 例如美國司法部雖然於 2021 年協助 Colonial Pipeline 追回了 230 萬美元比特幣贖金，然而如何追蹤到錢包地址之偵查細節被拒絕透漏，參見 Amanda Macias, Christina Wilkie, U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom, CNBC, […The FBI declined to say precisely how it accessed the bitcoin wallet, citing the need to protect tradecraft.], https://www.cnbc.com/2021/06/07/us-recovers-some-of-the-money-paid-in-the-colonial-pipeline-ransom-officials-say.html (last visited Jun. 18, 2021).

[353] Rachel Wolfson, Coinbase, Gemini and others join forces to combat human trafficking, Nov. 03, 2020, https://cointelegraph.com/news/coinbase-gemini-and-others-join-forces-to-combat-human-trafficking (last visited Jun. 18, 2021).

業情報公司和執法機構藉由共同參與非營利組織，分享監控交易及潛在的可疑活動模式，執法機關與私部門共同協作並分享資訊。加強跨國合作：包括確認何司法管轄區具有犯罪之管轄權、各國虛擬通貨犯罪之跨國資訊交換管道。

最後，金融機構與金融科技業者提供給監理機關或執法機關資訊時，在人工智慧和大數據分析之範疇下，最重要者為提供管道制度化及資訊之標準化，無論是英國之數位監管申報系統，或者新加坡的智慧監管申報系統，在監管層面上可以節省收送資料雙方之人力成本成本，且經過標準化及去識別化之資訊，可以使得資訊容易儲存及分析，便可以運用在學術研究、犯罪預防及犯罪偵查上。

二、跨越國境統一執法標準之重要性

本文所討論之金融科技犯罪，往往具有跨越國境、金錢流動快速、匿名性等問題，各國法規範標準不一致便會產生各種執法問題，例如犯罪構成要件不一致、取證方式及限制不一致、跨國執法機關合作等障礙，甚至也會有類似「監管套利」的問題產生，亦即犯罪者會從規範嚴格的國家或地區移動至法規範密度低的地區犯罪。為降低以上問題，在虛擬通貨方面，因虛擬通貨之匿名性有巨大犯罪風險，FATF 正統一各國之執法標準，並透過創建實名制、「旅行規則」等相關規定，確保虛擬通貨使用者之網路身分能與真實世界身分一致，降低相關金流及資訊流之追索困難。

另外統一執法標準的範例可參考歐盟法規。歐盟法現今在刑事訴訟程序、洗錢防制及打擊資助恐怖主義(AML/CFT)法規、虛擬通貨在 AML/CFT 目的下納管之規定，均逐漸成形當中。此跨越國境統一法規範標準之雄心，未來是否有植髮成功範例或者適用上遭遇之障礙，值得吾人關注。

三、提升執法機關職權或組織編整

如美國特勤局在 2020 年 7 月時宣布將下轄之電子犯罪專案組（ECTFs）及金融犯罪專案組（FCTFs）整合成立了網路詐欺專案組（CFTF）。另外美國於 2018 年將國土安全部下之網路安全基礎設施署（Cybersecurity & Infrastructure Security Agency, CISA）升級為聯邦

政府單位，使其獲得更多預算與職權協助聯邦及各州政府間之資安計畫，此部門針對駭客攻擊會發布相關的勒索細節及指南，並與犯罪偵查機關FBI互相合作。其餘如英國之國家打擊犯罪調查局(NCA)成立國家經濟犯罪調查中心(NECC)，或者歐盟的歐爭檢察署(EPPO)之成立，均係因為新興金融犯罪所涉及者具有跨職權、跨專業領域之性質，已非傳統執法模式可以應付之案件類型，有賴公部門更具彈性的與時俱進方能打擊犯罪。

四、健全犯罪相關查緝制度

科技執法雖有節省人力、更加迅速或者能預防犯罪的優點，不過執法方式亦須有明確清楚立法，且應注意是否有侵犯人民權利疑慮。例如即時搜索、或是修改通訊監察保障法或與業者合作監控回報，在隱私以及犯罪查緝間如何取得平衡為問題，應透過立法方式獲得正當性之授權。美國FinCEN亦在進行如何向虛擬通貨服務供應商取得用戶私鑰資訊之立法公聽程序[354]。另外許多先進技術如人工智慧及大數據分析，其究竟應如何制度化供執法機關及監管機關得以低成本方式應用於執法實務上，以及如何確保資訊安全，以免執法過程違反刑事程序或資料外洩於不法分子利用，以上問題均有賴各國繼續嘗試、除錯，已建立起更明確的科技執法流程。

[354] Fin CEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions，https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering (last visited Jun. 18, 2021).

第四節　虛擬通貨及相關行業自律組織協力之國際趨勢

根據 FATF 所發佈之私部門資訊共享指引（Private Sector Information Sharing）[355]，洗錢、資助恐怖主義及其他金融犯罪，因為其跨地域的特性，公部門及私部門間的資訊分享極為重要，尤其是金融機構之間，及金融機構與監理、執法機關之間。前述提及，FinCEN 作為美國的中央金融情報機構，在洗錢防制及打擊恐怖主義方面與其他國家的金融機關和國際機構建立全球合作[356]。FinCEN 向私部門之金融機構蒐集金融數據，在洗錢、資助恐怖主義、或其他金融犯罪等案件執法具有重要價值。FinCEN 甚至每年頒獎予成功起訴的案例，一方面是表揚成功起訴的執法機構，另一方面也做為對金融機構提供有資訊價值之鼓勵。

依據美國特勤處調查辦公室發布之預訂工作報告[357]，財產扣押或犯罪沒收是打擊犯罪活動的重要執法工具，然而扣押虛擬通貨所面臨之執法上的困難，首先涉及與交易平台之合作及資訊交換，包括是否有權限命平台應交出用戶私鑰或是使其提供被移轉錢包之第三人之資訊。此外，此類資產如何再迅速返回或是兌換成法定貨幣給受害者，仍需要建構相對應的法制及監理機構與私部門的持續公開對話。

就此，本研究團隊觀察國際實務趨勢上，為落實洗錢防制、法令遵循、風險控管及投資人保護等重要目標部分國家透過形成虛擬通貨行業公會及/或自律組織（Self -Regulatory Organization，SRO），制定行業公會/自律組織之章程內部規範，以加強虛擬通貨之業者自律，同時以行業公會/自律組織之名義，統合產業中不同業者之意見，並加強與目的事業主管機關間之溝通及訊息交換，透過上述措施以達成私部門協力，並有效達成洗錢防制、法令遵循、風險控管及投資人保護等目標。

---

[355] FATF, FATF Guidance-Private Sector Information Sharing, FATF (2017), https://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-information-sharing.html.

[356] *Supra* note 269 (last visited Oct. 25, 2020.).

[357] U.S.Secret Service Office Of Investigations, Office Of Investigations Strategy Fy2021–2027, https://www.secretservice.gov/sites/default/files/reports/2021-01/inv-strategy-fy21-27.pdf (last visited Jun. 18, 2021).

國際證券委員會組織（International Organization of Securities Commissions, IOSCO）亦認為自律組織為協助監理機關之重要監理方法，例如自律組織得透過制定自律規則鼓勵行業落實「最佳實踐標準」（Standards of Best Practice）。特別是自律組織因為組成份子為產業同行，將擁有對於該特定產業之專門知識，能快速修正自律組織規則以回應靈活多變的市場變化[358]。隨著金融市場複雜性提高，自律組織能提供業界知識和制度背景，並作為監管機關與市場之間的溝通橋樑，能比政府更快、更靈活地對市場做出反應，提高監管效率，節省監理成本。

此外，自律組織與產業合作所發展之行業行為準則（Code of Conduct），可補充及執行既有規範之不足。由於監理機關之權責可能因其國界或政府部門之分工限制，無法完全涵蓋產業需求，自律組織能提供更好的靈活性。以下本研究團隊盤點性行現行各國(包括日本、美國、英國、新加坡及瑞士等)上落實虛擬通貨業自律組織之立法例，瞭解相關各國如何聚集新興金融科技產業之不同利益方，並使監理資源得以聚焦，達成更有效率之合作及資訊共享。

第一項 日本

一、虛擬通貨法制

日本為最早將建立虛擬通貨業法制之國家之一，日本於西元（下同）2016 年 5 月修正支付服務法，要求虛擬通貨交易業者應向政府進行登錄，並於同年修正犯罪收益移轉防止法將虛擬通貨交換業者納入適用主體，使虛擬通貨業者應遵守洗錢防制之相關規範。

統計至 2018 年中，日本國內發生之虛擬通貨相關犯罪共計 169 件，犯罪被害金額達 677 億日圓以上，然而與此同時，虛擬通貨交易業者之事業規模亦正在急速成長[359]，2018 年 1 月，日本最大的加密貨幣交易所 Coincheck, Inc.宣布因遭到駭客攻擊損失約等值於 5.3

[358] IOSCO, Model for Effective Regulation, May 2000, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD110.pdf (last visited: Aug. 17, 2021).

[359] 日本国家公安委員会，犯罪収益移転危険度調査書，令和元年 12 月 https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk011219.pdf (最後瀏覽日：2021 年 8 月 15 日)。

億美元的加密貨幣，這起事件導致日本金融廳對於虛擬通貨交易所採取更嚴格的監管措施，除催生了日本金融應於同年 3 月成立了虛擬貨幣交易所研究小組外，上述事件也加速了交易所行業的整合。日本虛擬貨幣交易所協會於 2018 年 3 月 29 日成立，該協會並被金融廳指定為支付服務項下的自律組織。

2019 年，日本修正了包含支付服務法、金融商品交易法[360]及犯罪收益移轉防制法等規定，不僅將虛擬通貨之用語改為密碼資產（暗号資産，以下稱密碼資產）[361]，並擴大了適用之業者範圍[362]。

所謂密碼資產交換業者，依據支付服務法第 2 條第 1 項第 7 款之定義，指以下列行為為業者：

(一)進行密碼資產之買賣或密碼資產間之交換。

(二)為前款行為之媒介、代辦或是代理。

(三)與前兩款行為有關所進行之使用者金錢之管理。

(四)為他人進行密碼資產之管理（除其他法律對於以該管理為業者有特別規定者外）。

二、密碼資產交換業之自律組織協力情形

依支付服務法第 2 條第 8 項之規定，符合上開定義之密碼資產交換業者，應向政府申請登錄。於業者申請登錄之審查項目包含業者是否已確實建立包含建立洗錢防制在內之適當體制？業者是否已加入政府認可之自律組織？若業者未進行登錄，仍得進行上開業務，但可能會受到較高密度之監理，例如發生消費者糾紛時可能會受到金融廳之警告，或是直接要求其停止業務及進行登錄等。透過登錄之審查，實際上已對業者達成行政指導之目的[363]。

---

[360] 日本近年對密碼資產之監理措施，可參考蔡英欣（2018），試論虛擬貨幣之監理與法律定位—以日本法為中心，管理評論 第 36 卷 第 4 期，頁 53-67。

[361] 日本於 2019 年修正支付服務法將虛擬通貨（仮想通貨）之用語改稱為密碼資產（暗号資産）以配合國際潮流，並避免因原有通貨之用語產生誤認為法定貨幣之可能性，參考劉蕙綺，淺談日本針對加密資產/虛擬通貨相關法規之修訂，金融聯合徵信 第 36 期，2020 年 6 月，頁 104-108。

[362] 日本国家公安委員会，同前註 359 。

[363] 日本金融庁，マネー・ローンダリング及びテロ資金供与対策の現状と課題，https://www.fsa.go.jp/news/r1/20191021amlcft/20191021amlcft-1.pdf，頁 26（最後瀏覽日：2021

日本對於密碼資產業者之金融監督有部份透過自律組織來分擔，倘業者未加入政府認可之支付服務業者協會之自律組織，且未將自律組織所訂之自律規則納入公司內部規則者，依支付服務法第 63 條之五第 6 項規定政府可拒絕其登錄。

政府認可之支付服務業者協會，為依據支付服務法第 87 條規定，由密碼資產交換業者所設立之一般社團法人，須建立自律規則並經過審查後始得向政府申請認定為支付服務法上之支付服務業者協會，協會除有對會員為監督、資訊提供、行業指導、處理消費者爭議等義務外，依支付服務法第 97 條規定，得由業者協會代表從業者與政府間進行資訊交換。

日本目前有兩個自律組織受到政府承認得協助金融廳進行行業監督：一般社團法人日本密碼資產交易業者協會（一般社団法人日本暗号資産取引業協会 JVCEA - Japan Virtual and Crypto assets Exchange Association）以及一般社團法人日本 STO 協會（一般社団法人日本 STO 協会 JSTOA-Japan Security Token Offering Association），上述二自律組織雖均與密碼資產交易有關，但前者為依據支付服務法第 87 條取得自律組織資格，成員主要為密碼資產之交易所；後者為依據金融商品交易法第 78 條第 1 項取得自律組織資格，成員主要為證券機構，特別著重與代幣發行及眾籌有關之項目。

(一)一般社團法人日本密碼資產交易業者協會（一般社団法人日本暗号資産取引業協会 JVCEA - Japan Virtual and Crypto assets Exchange Association）

本協會於 2019 年 3 月成立，並於同年 10 月取得金融廳之認定為支付服務法第 87 條之自律組織，為日本密碼資產交換業及密碼資產關聯衍生商品交易業之重要自律組織，協會成員目前計有 38 名[364]，協會組成主要為密碼資產之交易所及錢包管理業者，協會理事除由加密貨幣業者組成外，另包含大學教授、資安業者、消費者保護協

年 8 月 15 日）。

[364] JVCEA，一般社団法人日本暗号資産取引業協会（JVCEA）会員一覧，更新日：2021 年 8 月 10 日，https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/jvcea-member.pdf （最後瀏覽日：2021 年 8 月 15 日）。

會代表及律師等[365]。協會宗旨為確保協會會員之業務能圓滑且確實實施及健全，並未利用者和投資人保護為目的[366]。

(二)一般社團法人日本 STO 協會（一般社団法人日本 STO 協会 JSTOA-Japan Security Token Offering Association）

本協會於 2019 年 10 月成立，於 2020 年 4 月依據金融商品交易法第 78 第 1 項經金融廳認定為金融商品交易業協會之自律組織，目前會員數 62 名，會員主要以證券公司等金融商品仲介業者為主。

依據金融廳發布之指引[367]，上述自律組織之職責包含：

1. 制定自律規則：

自律組織之規則應依金融廳之指引訂定，其變更及運用狀況，將由金融廳與協會進行密切合作[368]。會員並應依據組織之自律規則修訂其公司之內部規章，並向公司人員公告[369]、依據自律規則計算每日密碼資產之基準價格、外匯風險比率[370]、制定使用者財產管理之有關規則[371]、制定販賣新型密碼資產之有關規則

2. 監督會員及提供資訊：

會員應向自律組織提出申報書及報告書。協會並得於必要時，依據法令或協會規章要求會員就其業務及財產提出說明及資料，並就會員對法令之遵循狀況、業務及財產之狀況、帳簿等進行監察。

3. 對會員為行業指導、勸告：

確保會員遵循包含支付服務法及金融商品交易法等相關法規及組織之自律規則，例如指導會員修正使用者條款。

4. 受理密碼資產交換業相關之消費者客訴及糾紛解決：

例如向律師公會所營運之紛爭解決機關委託紛爭解決，或是委

---

[365] JVCEA，一般社団法人日本暗号資産取引業協会（JVCEA）役員一覧 2021 年 6 月 25 日更新 https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/jvcea-yakuin.pdf （最後瀏覽日：2021 年 8 月 15 日）。

[366] JVCEA，協会概要，https://jvcea.or.jp/about/ （最後瀏覽日：2021 年 8 月 15 日）。

[367] 日本金融庁，事務ガイドライン第三分冊：金融会社関係 16・仮想通貨交換業者関係 https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf （最後瀏覽日：2021 年 8 月 15 日）。

[368] 同前註，頁 84-85。

[369] 同前註，頁 35。

[370] 同前註，頁 38。

[371] 同前註，頁 40。

託金融訴訟外紛爭解決機構等。金融廳並會就使用者紛爭解決之動向定期與協會進行意見交換[372]。

5. 向使用者提供資訊：公告密碼資產相關犯罪或不當交易之案例。
6. 對業者之業務及財務狀況進行統計調查
7. 對會員進行教育宣導，辦理會員法遵講座等
8. 進行強制處分：

如會員違反上述章程規定者，得對會員處以譴責、罰金、停止會員權利或除名等處分。就會員違反法令但事態輕微之情形，金融廳授權協會得行使改善指導及調查之權[373]。

縱使業者未加入自律組織，然而其公司體制包含章程和內部規則之制定仍應參照並以自律組織之所定之規則準，當自律組織規則有所更改時，並應依照協會規則之變更修正其公司內規。且如前所述，對於未加入自律組織之業者，金融廳將提升監理密度，倘此類業者未及時依據自律組織規則修該公司內規時，金融廳甚至得停止其業務[374]。

第二項 美國

一、虛擬通貨法制

美國並未針對虛擬通貨業者訂立獨立之業法，而是在維持法制框架下，針對不同商業模式之虛擬通貨活動，依據其活動類型適用於既有之金融法規。例如當虛擬通貨構成可兌換之虛擬通貨（Convertible Virtual Currencies, CVC）時，接受和傳輸可兌換之虛擬通貨者應向 FinCEN 註冊為貨幣服務業（Money Services Businesses, MSB），例如從事涉及證券、商品或期貨合約和法定貨幣、可兌換之虛擬通貨或其他替代貨幣的價值的交易所。貨幣服務業者應並遵循銀行保密法（Bank Secrecy Act）下之洗錢防制義務規範，建立洗錢防制之內部控制，遵守記錄保存、監控和向 FinCEN 申報可疑交易紀

[372] 同前註，頁 84-85。
[373] 同前註。
[374] 同前註，頁 71。

錄活動等。

二、自律組織協力

目前美國尚未建立虛擬通貨業者自律組織之相關法制，關於自律組織仍在進行中或正在討論中。2018 年 8 月，四家美國加密貨幣交易所——Bitstamp、bitFlyer、Bittrex 和 Gemini——自發性地建立了虛擬商品協會（Virtual Commodity Association，VCA），旨在建立一個由行業發起的自律組織來監督虛擬商品市場，但目前似尚未建立具體的規範和影響。，10 家機構交易公司創建了數位資產市場協會（Association for Digital Asset Markets ADAM），協會會員應遵守協會之行為準則，未遵守行為準則之會員，協會得予以除名。

第三項 英國

一、虛擬通貨法制

英國自 2020 年 1 月 10 日起，於英國進行密碼資產活動之現存企業及新進者應遵循洗錢防制法規之規定（Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, MLRs），包含應向英國之金融監理主管機關即金融行為監理署（Financial Conduct Authority，FCA）註冊，應註冊而未註冊者，於 2021 年 1 月 10 起不得進行任何密碼資產活動，否則將可能構成刑事犯罪。

所謂進行密碼資產活動，包含提供密碼資產與法幣間之交換、密碼資產間之交換、代表客戶持有、儲存和轉移密碼資產之業者或個人[375]。

英國目前對密碼資產業者採臨時註冊制度，進行密碼資產活動之業者依據 MLRs 第 8 條應向 FCA 提出註冊申請，而尚未通過註冊審核者仍得暫時營業，然而由於有大量企業無法符合 MLRs 所定之標準，有大量公司於事後撤回註冊申請，為此，英國將臨時註冊制度自 2021 年 7 月 9 日進一步延長至 2022 年 3 月 31 日，於 2020 年 12

[375] FCA, Cryptoassets: AML / CTF regime, Last updated: 03/06/2021, https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime (last visited Aug. 14, 2021).

月 16 日前申請註冊之密碼資產公司仍得繼續交易[376]。

二、自律組織協力

2018 年由密碼資產之業者共同組成 CryptoUK[377]，是英國代表密碼資產行業的自律貿易協會，現有約 50 位協會成員，包含密碼資產交易所、交易經紀人、數據比較網站、第三方交易服務商及資產管理者等。協會職責包含制定行為準則、與代表業者與其他金融體系和之利益相關者合作，協助密碼資產業者融入其他金融服務業。該協會並規劃了三個主要工作領域[378]，包含：

(一)尋求與政策制定者合作，為金融行為監理署監管的金融機構建立公平、透明和一致的方法，評估密碼資產相關業務在與開設銀行帳戶之風險。

(二)尋求定期與英國財政部合作，以支持密碼資產之創新及商業模式。

(三)就零售客戶銷售密碼資產的投資產品，建立與其他投資商品包含期貨、ETF 等之平衡、公平和一致的方法。

該協會所制定之會員行為準則包含幾大面向[379]：

1. 強化合作：會員和監管及法律部門的監管和合作
2. 消費者信任：會員承諾將對消費者主動接漏有關定價、槓桿成對和費用及相關風險的明確資訊
3. 透明度：與客戶和潛在客戶的溝通應公平、清晰而無誤導性
4. 資訊安全：會員承諾會依據資料保護規定，確保對於 IT 基礎設施的管理，防止個人資料之洩漏、遺失及損壞
5. 資產隔離：會員承諾將客戶及公司自有資金之資產隔離，並確保公司發生破產事件時仍能支付客戶之投資。
6. 降低風險：對於流動性低、不用於交易或轉移目的之客戶

[376] *Id.*
[377] CryptoUK, https://cryptouk.io/ (last visited Aug. 14, 2021).
[378] CryptoUK, https://cryptouk.io/about/ (last visited Aug. 14, 2021).
[379] CryptoUK, https://cryptouk.io/codeofconduct/ (last visited Aug. 14, 2021).

資金，應有 90%以上之私鑰均應保存於冷錢包中。

7. 盡職調查：會員承諾會對平台用戶進行盡職調查，以防止非法活動，包含反洗錢及反資恐活動。

第四項 新加坡

一、虛擬通貨法制

新加坡於 2019 年通過支付服務法（Payment Services Act of 2019, PSA），自 2020 年 1 月開始，為電子支付代幣服務提供商，且於新加坡設有辦公室或是公司董事位於新加坡者，應遵循支付服務法之相關規定，除應向新加坡金融管理局（Monetary Authority of Singapore，MAS）註冊外，並取得 MAS 營運牌照，遵守洗錢防制法之相關要求。所謂電子支付代幣服務提供商包含：1. 建立或營運電子支付代幣交易所 2. 參與或提供與發性或出售電子支付代幣相關之金融服務 3.協助移轉電子支付代幣、勸誘他人購買或出售電子支付代幣者。而未遵循洗錢防制要求者，MAS 將拒絕發給牌照。

二、自律組織協力

新加坡加密貨幣企業和初創企業協會 (ACCESS，Association of Crypto Currency Enterprises and Start-ups Singapore) 於 2014 年 5 月 30 日成立。ACCESS 與新加坡銀行協會共同發布了一份草案，旨在通過提出一套標準化的最佳實踐方法[380]，來補充新加坡的支付服務法，然而目前此套行為準則僅對會員公開。

第五項 瑞士

一、虛擬通貨法制

瑞士並未針對虛擬通貨及制定特定的行業業法，而是將虛擬通貨納入原有的法律框架中列管，包含將證券法令、洗錢防制、金融

[380] ACCESS Singapore, *ACCESS rolls out Code of Practice to facilitate application of payment service provider licence under Singapore's Payment Services Act*, ACCESS (Aug. 13, 20200, https://www.access.org.sg/blogs/press-release/access-rolls-out-code-of-practice-to-facilitate-application-of-payment-service-provider-licence-under-singapore-s-payment-services-act.

市場基礎設施監理等適用於虛擬通貨業者。瑞士於 2019 年 11 月 27 日提出 DLT 法案[381]，將採用分散式帳簿技術之虛擬通貨業者納入現有法制中，依據瑞士之反洗錢法（The Anti-Money Laundering Act），在瑞士設有註冊辦事處或分支機構之金融中介機構，應隸屬於指定之自律組織，或獲得瑞士聯邦金融市場監理局 (Swiss Financial Market Supervisory Authority，FINMA) 的授權[382]。

所謂金融中介機構，依據瑞士反洗錢法第 2 條之定義，包含受到特別法定監理之金融中介機構例如：銀行、投資基金、資產管理公司、保險公司及證券經紀人等，以及具有準銀行地位之其他金融中介機構，包含以專業身分接受、持有、協助投資或是移轉屬於第三人之資產者，例如：

(一)經營信貸業務（從事消費或抵押放貸、融資性租賃）。

(二)提供第三方支付工具（包含信用卡或是電子轉帳）。

(三)協助進行通貨、貴金屬、證券及其衍生品之交易等。

如個人或機構從事上述金融中介活動，則其應加入自律組織，或是於開始從事上述營業後兩個月內向 FINMA 提交營業許可，否則不得與任何客戶建立任何上述活動之業務關係[383]。

根據上述定義，提供包含支付型代幣等虛擬通貨者將構成金融中介機構，符合金融中介定義的自然人或法人均須獲得 FINMA 之許可始能開始營業，許可可以兩種方式獲得，一為接受 FINMA 之直接監管，或是透過參與 SRO 獲得 FINMA 之間接監管。

二、自律組織協力

依據瑞士打擊洗錢及反資恐跨部門協調小組（Interdepartmental coordinating group on combating money laundering and the financing of terrorism, CGMF）於 2018 年發布之犯罪風險評估報告，隨著金融主管機關對於從事加密貨幣交易之金融中介者提供更明確的定義，而

[381] Financial Technology Law Review Third Edition, https://www.nkf.ch/app/uploads/2020/06/chapter-23-switzerland-may-2020.pdf (last visited Aug. 14, 2021).
[382] VQF, Duty of Subordination, https://www.vqf.ch/en/sro/duty-of-subordination (last visited Aug. 14, 2021).
[383] *Id.*

密碼資產的金融中介者更加完善其對客戶進行盡職調查之義務，洗錢辦公室因此而收到了更多洗錢的可疑活動報告[384]。

自律組織應獲得 FINMA 之認可，其自律規則應依反洗錢法制定，其修訂亦必須通過 FINMA 之審核，並由 FINMA 負責監管和監督。取得認可之自律組織應滿足下列要件[385]：

(一)依據反洗錢法制定會員規章。

(二)監督會員規章之遵循狀況。

(三)制定監督會員之辦法及程序，包含稽核程序及訂立會員違規之罰則。

(四)設立自律組織之稽核部門，稽核部門並應維持獨立性並滿足專業資格要求。

(五)確保組織之稽核滿足反洗錢法之要求。

目前獲得FINMA承認之自律組織共有11間[386]，以瑞士最大的金融自律組織即金融服務標準協會（The Financial Services Standards Association ，VQF）為例，該協會於1998年成立，定期對會員進行稽核、舉辦有關反洗錢法之培訓，對會員行使法律規定之監督職能，發布行為準則、對個別會員提供專屬之法律遵循建議、舉辦反洗錢法領域之培訓及研討會、代表行業業者利益參與相關立法程序和政府協商[387][388]。

第六項 小結

自上述比較法之模式可知，目前虛擬通貨業者，由各國金融主管機關先依據業法（例如日本、新加坡之支付服務法及美國之貨幣

[384] CGMF, National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, https://www.sif.admin.ch/dam/sif/en/dokumente/Integrit%C3%A4t%20des%20Finanzplatzes/nra-bericht-krypto-assets-und-crowdfunding.pdf.download.pdf/BC-BEKGGT-d.pdf (last visited Aug. 18, 2021).

[385] FINMA, Self-regulatory organisations (SROs), https://www.finma.ch/en/authorisation/self-regulatory-organisations-sros/ (last visited Aug. 14, 2021).

[386] FINMA, List of self-regulatory organisations (SROs) recognised by FINMA, https://www.finma.ch/en/~/media/finma/dokumente/bewilligungstraeger/pdf/sro.pdf?la=en (last visited Aug. 14, 2021).

[387] Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF) , https://www.vqf.ch/en/vqf/services (last visited Aug. 14, 2021).

[388] Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF) , https://www.vqf.ch/en/vqf (last visited Aug. 14, 2021).

服務法）或是透過洗錢防制法之修訂，納入洗錢防制法之義務主體（例如英國、瑞士及我國），要求其進行洗錢防制法上之客戶盡職調查、可疑交易活動申報等，再由業者透過上述法律之遵循，向犯罪偵查機關提供可疑之犯罪資料，形成金融主管機關、業者及犯罪偵查機關之三方關係。

此外，目前上述比較法國家，多數已要求提供虛擬通貨交換服務之業者應進行登錄或是註冊[389]。其中，日本及瑞士，除採取註冊制外，另並要求業者應加入自律組織，或是將業者應將自律規則納入公司體制作為合法營業之前提，因此此二國家之自律組織相較其他國家而言，對於承擔監理職責及與政府間互相協力，有較明確之規範及發揮空間。

依據 IOSCO 之報告[390]，自律組織之監理協力可能包含：1.透過調查和紀律處分來執行規章制度；2.　實地檢查財務和營運狀況；3.進行市場及行業調查；4.處理客戶投訴；5.制定違規行為之監理計畫；6.與其他自律組織共享資訊及合作 7.提供爭端解決平台等。日本針對虛擬通貨業者之營業活動，透過修正支付服務法及金融商品交易法，並指定之自律組織協助監理，建立了良好的法制，而目前日本指定之兩個自律組織具有上述 IOSCO 設定之自律組織之監理功能，對此，日本之金融主管機關金融廳亦指出，政府與自律組織及行業團體間之官民協力，能夠協助主管機關辨識及評估風險，透過可疑交易態樣之申報及統計，使主管機關能確實掌握行業業務之具體風險所在[391]。

我國目前尚未以法制要求虛擬通貨業者應經註冊或取得特別營業許可，亦並未針對虛擬通貨訂立專門業法管制，而是透過行政命令指定為洗錢防制法之義務主體，並由金管會制定虛擬通貨平台及交易業務事業防制洗錢及打及資恐辦法，本辦法已於 2021 年 7 月 1

[389] FATF 發布之建議第 15 條亦建議各國應對虛擬資產服務提供者進行審核或要求其登記註冊，*See*: FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF (2012-2021), www.fatf-gafi.org/recommendations.html (last visited: Aug. 14, 2021).

[390] *Supra* note 358.

[391] 日本金融庁，同前註 363（最後瀏覽日：2021 年 8 月 15 日）。

日正式施行（詳情可參見本報告第三章第四節第二項我國主管機關對虛擬通貨之監理模式）。然而，洗錢防制法以明文規定有大量細部事項應徵詢公會之意見，包含：同法第 6 條有關建立洗錢防制內部控制與稽核制度規定：「制度之實施內容、作業程序、執行措施...於訂定前應徵詢相關公會之意見。」、第 7 條有關客戶盡職調查（CDD）程序規定：「確認客戶身分範圍、留存確認資料之範圍...於訂定前應徵詢相關公會之意見。」、第 8 條有關交易紀錄之留存規定：「辦理國內外交易...留存交易紀錄之適用交易範圍、程序、方式之辦法...於訂定前應徵詢相關公會之意見。」、第 9 條達一定金額以上之通貨交易申報義務規定：「金額、通貨交易之範圍、種類、申報之範圍、方式、程序...於訂定前應徵詢相關公會之意見。」此外，本辦法第 14 條規定：「（業者）每兩年應製作風險評估報告」，因主管機關未限定風險評估之方式及格式，預計未來也是應由公會匯集業者，共同討論合適的風險評估報告製作格式及發布方式。

參照台灣銀行業、證券及期貨業等金融機構等金融實務，通常會由其所屬同業公會訂定防制洗錢及打擊資恐注意事項範本、指引及實務參考做法，以促請同業執行洗錢防制等合規要求，例如「中華民國銀行商業同業公會全國聯合會」、「中華民國證券商業同業公會」，指導同業業者落實法令遵循。若能由「虛擬通貨商業同業公會」帶領整體產業之洗錢防制義務主體，建立業者得以共同遵循之洗錢防制流程及作業標準範本，預計可降低金管會或相關單位的執法成本及管理難度，並提升台灣洗錢防制工作的落實程度。

我國之洗錢防制法令既已正式於虛擬通貨業中落實，本研究團隊建議，除可參考 FATF 之建議 15 對於虛擬通貨業者採取一定之審核制度外，相關配套措施包括我國是否應盡速對虛擬通貨業者設置「虛擬通貨商業同業公會」，結合產業公會推動虛擬通貨之產業自律、法規調適及落實洗錢防制措施等，日本對密碼資產業者之管制模式及自律組織之經驗應可提供我國良好之參考，考量到現行我國法對於購買虛擬通貨之投資人或消費者榮有法律保障不足等問題，亦欠缺訴訟外紛爭解決機制，故透過自律組織等私部門協力，應為目前

新興金融科技產業迫切需要落實保障消費者及打擊犯罪的必要措施。

第五章　研究結論及政策建議

第一節　電子支付工具及虛擬通貨犯罪之研究結論

第一項 電子支付工具犯罪研究結論

本研究團隊參酌前開司法判決實證統計結果與相關國內外文獻後，分別針對近期、中期及長期的法制發展提出具體建議如下：

一、近期建議——確認執法重點

本研究透過盤點我國司法判決實證研究，發現利用電子支付工具遂行詐欺案件中之詐騙集團，多以人頭申請行動支付帳戶。此外犯罪行為人盜用他人身分或其他資訊創建電子支付帳戶的案件占比亦相當可觀，足見當前電子支付帳戶的設立存在虛偽資訊充斥之風險；此外因為電子支付帳戶之申設成本相對不高，對犯罪行為人有一定程度之吸引力，故電子支付帳戶似乎漸有被濫用為犯罪工具之傾向。此均將導致偵查機關較難追查相關財產犯罪之金流。

此外，本研究亦觀察到上述案件中有一定比例之案件涉及第三方支付服務提供者。此或與此前第三方支付業者的洗錢防制監管相對較為混亂有關，故第三方支付業者對於交易雙方之身分資訊調查與留存現實上存有不足，導致追查金流時容易出現斷點，進而對犯罪行為人產生一定程度之吸引力。考量到我國目前共有 13,113 家第三方支付業者登記在案，第三方支付業者形成的追查金流斷點，必須慎重因應並加強未來執法。

本研究以我國司法判決實證研究的內容為基礎，分析主要電子支付業者涉案的情形，並具體歸納得出較常涉及犯罪的特定電子支付業者，此研究結果可作為相關主管機關未來執法上加強關注的重點。

二、中期建議——盡速通過第三方支付業者的洗錢防制措施

本研究團隊建議盡快通過相關法規落實第三方支付業者的洗錢防制措施，以降低犯罪人利用第三方支付匿名性遂行犯罪的空間。電子支付工具的若干特性例如匿名性、多層化特性、快速性、非面對面接觸特性等，如上述有利犯罪人遂行犯罪。欲緩和上述挑戰，主要須仰賴電子支付業者確實踐行若干洗錢防制義務，例如認識客

戶、客戶盡職調查、留存交易相關紀錄以及可疑交易通報等，方可相對緩和電子支付工具的上述特性，減少檢調機關偵查涉及電子支付工具犯罪時面臨的挑戰。

我國法下的電子支付業者包括狹義的電子支付機構與第三方支付業者。此二業者本質上均提供 FATF 四十項建議中定義的金錢或價值移轉服務（money or value transfer service, MVTS）[392]，而依 FATF 四十項建議之定義，MVTS 提供者亦屬金融機構[393]，應適用 FATF 關於金融機構洗錢防制的相關建議[394]，故狹義的電子支付機構與第三方支付業者理應比照金融機構洗錢防制的規定，例如適用我國的金融機構防制洗錢辦法。

依我國現行金融機構防制洗錢辦法規定，狹義的電子支付機構屬應適用相關洗錢防制規定之金融機構，較無疑義[395]。較有疑問者為第三方支付業者。現行金融機構防制洗錢辦法第 2 條第 1 款定義之金融機構僅包含電子支付機構，並未包含第三方支付業者，故第三方支付業者似不適用金融機構防制洗錢辦法；但法務部與經濟部於 2014 年曾共同頒布行政函釋「指定第三方支付服務業自即日起適用洗錢防制法有關金融機構之規定」[396]，似已指定第三方支付業者應適用金融機構的洗錢防制義務，故第三方支付業者看似又應適用金融機構防制洗錢辦法。

就第三方支付業者的洗錢防制義務，行政院於 2021 年 8 月 18 日發布院臺法字第 1100181600 號函，依洗錢防制法第 5 條第 4 項規定之授權指定第三方支付服務業為該法第 5 條第 3 項第 5 款之非金融事業或人員，並指定第三方支付服務業不適用洗錢防制法第 9 條第 1 項

[392] 依 FATF 的定義，所謂 MVTS，係指涉及收受現金、支票、其他貨幣工具或其他儲值工具，再經由通訊、訊息、轉帳等方法，或透過該 MVTS 提供者所屬清算網路，以現金或其他形式對受益人支付相對金額的金融服務。FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS 125 (Jun. 2021).

[393] *Id.* at 122-23.

[394] FATF, GUIDANCE FOR A RISK-BASED APPROACH: MONEY OR VALUE TRANSFER SERVICES 12 (Feb. 2016).

[395] 金融機構防制洗錢辦法第 2 條第 1 款第 4 目。

[396] 法務部 103 年 2 月 19 日法令字第 10204554850 號函釋；經濟部 103 年 2 月 19 日經商字第 10202146100 號函釋。

之一定金額以上通貨交易的申報規定，且上述指定自函釋發布日起即日生效。故於2021年8月18日以後，應認第三方支付業者屬我國洗錢防制法下所稱之「指定之非金融事業或人員」而非金融機構，但仍應負相當之洗錢防制義務。經濟部並已於110年9月27日公告「第三方支付服務業防制洗錢及打擊資恐辦法」草案，明確第三方支付業者的洗錢防制義務具體內容。

行政院上開函釋明確肯認第三方支付業者的洗錢防制義務，並將第三方支付定位為非金融機構，釐清了過往我國關於第三方支付洗錢防制法制的不明之處，值得肯定。只是參照FATF四十項建議，第三方支付似屬FATF所稱之MVTS，故依FATF之建議似應負金融機構之洗錢防制義務，行政院將第三方支付業者定位為非金融機構是否符合FATF之建議，或有商榷之空間。

惟無論如何，行政院上開函釋至少已確認第三方支付業者負有一定的洗錢防制義務，且經濟部上開草案至少已對第三方支付業者的洗錢防制義務具體內容提供了更明確的基本規定，故中期而言，本研究建議應盡速使經濟部上開草案生效施行，使第三方支付的洗錢防制法規盡速上路，以在法源上提供相關主管機關執行第三方支付業者洗錢防制義務的基礎，進而降低犯罪人利用第三方支付遂行犯罪的空間。

三、長期建議——落實電子支付業者的洗錢防制義務

於法制上明確電子支付業者（包括電子支付機構與第三方支付業者）應負洗錢防制義務後，下一步之重點即在落實電子支付業者的上開洗錢防制義務，包括客戶之身分確認與持續審查、交易資料保存與可疑交易申報等。此除有賴電子支付業者建置內部法令遵循程序外，亦須仰賴主管機關實施外部監督，以督促業者落實洗錢防制相關措施，故主管機關對電子支付業者理應定期[397]與不定期[398]查

[397] 洗錢防制法第6條第2項。

[398] 銀行業及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法第10條。

核其洗錢防制措施落實情形。

我國專營電子支付機構目前僅有 5 家專營業者，加上舊法下的 4 家電子票證發行機構後為 9 家，故金融主管機關承擔的監理壓力應尚屬可控；較有疑義者為第三方支付業者，其目前登記在案者即有 13,113 家，主管機關經濟部顯然難以對所有業者實施高強度的監理，故勢必須依洗錢風險及業務規模採取風險基礎方法的監理，針對有較高風險的業者優先採取重點式監理，方可在有限的監理資源下維持一定的監理品質。

長期而言，如欲落實電子支付業者的洗錢防制義務，除須仰賴相關主管機關的外部監理外，於主管機關監理電子支付業者的權責已如上述獲法制上釐清後，本研究建議檢調機關於偵查犯罪而須向特定電子支付業者調取相關資料時，如有發現特定電子支付業者未確實落實其洗錢防制義務者，應主動通報主管機關查核與裁罰，以發揮行政部會間的橫向整合，適度緩解主管機關的外部監理壓力。透過檢調機關與相關主管機關（例如金管會或經濟部）間建立的此種資訊傳遞管道，相關主管機關較能鎖定涉案比例較高、洗錢防制又不確實的電子支付業者加強檢查與監理，從而真正意義的實現風險基礎方法的監理。

第二項 虛擬通貨濫用於犯罪研究結論

經本研究團隊研析，國際間虛擬通貨濫用於犯罪等案例仍層出不窮，惟若各國政府及主要虛擬通貨業者，能夠落實洗錢防制及防資恐等措施，確實能夠有效預防犯罪，或是於犯罪發生後將影響範圍降至最低。

虛擬通貨交易由於匿名性、缺乏中央化的實體、跨國移轉迅速等特性增加了政府機關監管相關犯罪的困難度，而相關之偵查手法亦無法向大眾公開。目前各國對於虛擬通貨之監管亦均尚在起步階段，監理的實際狀況仍在不斷變化。查緝衍生之詐騙、洗錢犯罪因此有賴監管機關及執法機關更加專業、資訊交流並整合式地作犯罪預防及犯罪偵查。自各國比較法之模式可知，目前虛擬通貨業者，

由各國金融主管機關先依據業法（例如日本、新加坡之支付服務法及美國之貨幣服務法）或是透過洗錢防制法之修訂，納入洗錢防制法之義務主體（例如英國、瑞士及我國），要求其進行洗錢防制法上之客戶盡職調查、可疑交易活動申報等，再由業者透過上述法律之遵循，向犯罪偵查機關提供可疑之犯罪資料，形成金融主管機關、業者及犯罪偵查機關之三方關係。

此外，目前根據國際上相關國家實踐情形，多數政府已要求提供虛擬通貨交換服務之業者應進行登錄或是註冊，其中日本及瑞士，除採取註冊制外，另並要求業者應加入自律組織，或是將業者應將自律規則納入公司體制作為合法營業之前提，因此此二國家之自律組織相較其他國家而言，對於承擔監理職責及與政府間互相協力，有較明確之規範及發揮空間。

惟同一時間，在各國建構虛擬通貨之洗錢防制制度之同時，NFT 的快速發展，很可能且已經被不法人士用於以類似實體藝術品的方式遂行洗錢。NFT 轉移贓款的方式可能比起虛擬通貨更加容易，因為目前國際防制洗錢金融行動組織(FATF)指出，高價藝術品、文物、奢侈品極易被利用於洗錢或資助恐怖活動，但是否納入洗錢防制規範，交由各國依本國風險評估決定。而 NFT 發行及交易平台是否正式納入洗錢防制制度之範疇之一，仍在討論中，導致高市場價值之 NFT 標的容有淪為新興洗錢工具之一，未來似有必要盤點並追蹤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適用範圍，並評估是否有擴大適用洗錢防制範圍及於 NFT 發行及交易平台之必要性。

本研究團隊謹提出具體研究建議如下，以期得降低虛擬通貨相關犯罪之發生可能：

一、建議應成立「虛擬通貨商業同業公會」等公會組織，以落實虛擬通貨洗錢防制、法令遵循、風險控管及投資人保護等目標

本研究團隊觀察國際實務趨勢上，為落實洗錢防制、法令遵循、風險控管及投資人保護等重要目標部分國家透過形成虛擬通貨行業公會及/或自律組織（Self -Regulatory Organization，SRO），制定行

業公會/自律組織之章程內部規範，以加強虛擬通貨之業者自律，同時以行業公會/自律組織之名義，統合產業中不同業者之意見，並加強與目的事業主管機關間之溝通及訊息交換，透過上述措施以達成私部門協力，並有效達成洗錢防制、法令遵循、風險控管及投資人保護等目標。

此外，我國洗錢防制法第 5 條已將虛擬通貨商業業者納入成為義務主體，同法第 6 條至第 9 條明文金融監督管理委員會(下稱「金管會」)有關相關辦法之訂定應徵詢公會意見，故為蒐集同業意見，落實法令要求，故應有設立「虛擬通貨商業同業公會」之必要。

虛擬通貨依其商業模式可能涉及虛擬通貨與虛擬通貨間之交易（Crypto to Crypto），或法定貨幣與虛擬通貨間之交易（Fiat to Crypto），交易架構及洗錢防制作業程序均與傳統金融機構有間，所提供之服務及客戶之交易風險亦有別，現行虛擬通貨平台及交易業務事業除面臨洗錢防制法等合規要求外，並無專業經營限制、非特許業務，且目的事業主管機關掌管事項限於防制洗錢及打擊資恐，為有效蒐集同業意見、遵循洗錢防制法令及根據不同業務特性制定洗錢防制配套措施，並落實產業自治、經營管理自律，以及消費者保護等事項，應有成立「虛擬通貨平台及交易業務商業同業公會」之必要，以協助金管會訂定與虛擬通貨相關之洗錢防制配套措施。

未來虛擬通貨商業同業公會可具有協調業者符合法令規範之功能，亦可扮演業者與主管機關溝通之橋樑，同時也可協助制定與虛擬通貨有關之消費者保護機制，以謀求整體產業之良性發展。觀察現行「中華民國銀行商業同業公會全國聯合會（下稱銀行同業公會）」、「中華民國證券商業同業公會」及「中華民國期貨業商業同業公會」均有類似消費者權益保障之功能。例如：過去銀行同業公會曾成立「金融消費爭議案件評議委員會」，協助處理金融消費者申訴之案件，以達保護金融消費者權益之目的。

經本研究團隊分析，近年台灣以區塊鏈、虛擬資產為名，暗地為洗錢、吸金、詐騙等案例屢見不鮮，金管會亦於近期發布第三次虛擬資產風險警示：「虛擬資產價格波動大，投資風險高，社會大眾

從事相關交易前，應充分瞭解其運作模式，務必審慎評估可能產生的風險。」故虛擬通貨之消費者、投資人保障機制實有建立必要，然而我國現行消費者保護機制，並不適用於虛擬通貨商業及相關糾紛，故未來得透過自律組織或相關同業公會建立有效的消費者保護機制，以維消費者權益，解決現行虛擬通貨投資人保護之問題。

二、訂定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七條（旅行規則）之施行日

經本研究團隊研析虛擬通貨犯罪之偵查實務，可知涉及虛擬通貨犯罪之不法所得時常透過虛擬通貨業者進行洗錢，或利用人頭帳戶移出不法所得，完成不法所得之藏匿，且相關虛擬通貨之流向難以被偵查機構所掌握。

FATF 於西元 2018 年 10 月修正通過第 15 條建議中，提及各國應確保虛擬通貨服務提供者（VASP）受到防制洗錢與防資恐之監管，2019 年 6 月，FATF 就第 15 條建議發布監理虛擬通貨服務提供者之具體指引。嗣 FATF 於 2020 年 6 月發布之審查報告，承諾將進一步修訂指引並評估修訂第 15 條建議；FATF 並於 2021 年 3 月發布虛擬通貨業者洗錢防制指引草案（下稱「**FATF 指引草案**」），包含重新修訂之虛擬通貨之定義、適用業者範圍、防制洗錢之具體建議作為及是否訂定「Travel Rule（旅行規則）」等，由於對現有洗錢防制標準措施之修正幅度頗鉅，並大幅增加虛擬通貨業者之相關義務，各國之行業公會及學術機構均已就 FATF 指引草案表示諸多公開意見，FATF 指引草案訂定之標準是否為未來正式公布之標準，尚無定論，故現行各國政府多尚未依照 FATF 指引草案啟動正式修法程序。

經查，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（下稱「本辦法」）第七條雖訂定有「Travel Rule（旅行規則）」），即要求虛擬通貨之轉出方及接收方應落實實名制及虛擬通貨金流資訊保存，應可有效解決虛擬通貨之流向難以被偵查機構所掌握之問題。

惟依本辦法第 18 條規定：「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。」，因此現行法下，若虛擬通貨之金流涉及到不同虛擬通貨平台間之轉移，尤其是涉及到外國虛擬通貨平台之業者，相關虛擬通貨之流向亦難以被偵查機構所掌握，增加偵查及扣留不法所得之難度，故建議得於適當時機下擇期另訂本辦法第七條之施行日期。

第二節　政策建議

第一項 建議新增偽造變造數位支付工具之刑法規定

新興金融科技工具由於多係利用網路進行交易，具有匿名與非面對面接觸的特性，因此可能發生盜用身分資料創設帳戶的犯罪事件，犯罪人甚至可能以盜設的帳戶作為犯罪工具進行其他犯罪，例如本研究第二章的司法判決實證研究即顯示我國已有相當數量的盜用他人資訊設定電子支付帳戶的案例；此外，國內亦已有若干QR碼詐騙、電子支付帳戶駭客、虛擬通貨交易平台駭客等案例，涉及偽造QR碼或變造他人帳戶紀錄的犯罪態樣。

上述犯罪行為在我國現行刑法下面臨的刑事責任，就立法論而言似有商榷空間。上述犯罪行為通常係成立刑法第 210 條之偽造變造私文書罪以及第216條與第220條之行使偽造準私文書罪，以及刑法第358條無故入侵他人電腦設備罪與第359條無故變更他人電磁紀錄罪；如有涉及詐騙行為，另可能成立刑法第 339 條之詐欺罪、刑法第339條之3之以電腦相關設備製作不實財產權得喪紀錄得利罪或刑法第339條之4之以網際網路對公眾散布而犯詐欺取財罪。但進一步分析之，刑法第 339 條、第 339 條之 3、第 339 條之 4、第 358 條以及第 359 條之犯罪均屬財產犯罪，其保護法益僅為個人法益，並未考量上述犯罪行為對整體支付系統秩序之影響；至於刑法第 210 條、第216條及第220條犯罪之保護法益雖為社會法益，惟其僅係保護一般文書真實性此一社會法益，並未特別考量支付系統秩序的特殊性。故整體而言，現行刑法規定似尚未充分保護新興支付工具形成的支付系統秩序此一新興社會法益。

現行刑法規定的不足，對照刑法第201條之1之偽造變造支付工具罪的規定，尤其明顯。刑法第 201 條之 1 之規定係於 2001 年增訂，當時金融卡與信用卡等卡式支付工具屬於該時代的新興支付工具，但偽造、變造金融卡、信用卡之犯罪行為層出不窮，產生之犯罪案件多為企業化、多角化及跨國性集團之犯罪，已嚴重危害該支付系統之健全，進而危害整體社會經濟秩序，故立法者以高於詐欺罪之法定刑處罰偽造變造卡式支付工具的行為，制訂一年以上七年以下

之有期徒刑[399]。惟因當時的時空背景係以卡式支付工具為主，故該罪之犯罪客體係定為「信用卡、金融卡、儲值卡或其他相類作為簽帳、提款、轉帳或支付工具之電磁紀錄『物』」，換言之僅限於具有實體的支付工具。

該條制訂至今已二十年，新興支付工具種類更加多元，包含電子支付、第三方支付、虛擬通貨等數位支付工具陸續出現。但此類新興支付工具並無實體，故偽造變造此類新興支付工具帳戶紀錄之行為，基於罪刑法定主義尚無從適用刑法第 201 條之 1 之規定，導致現行刑法僅保護卡式支付工具的真實性、但卻未保護數位支付工具的真實性。

新興的數位支付工具需取得公眾的信任，方可維持基本的交易流通性，進而支應大眾支付需求；偽造變造新興支付工具的帳戶紀錄行為可能影響公眾對新興支付工具的信任，進而不利我國發展新興支付工具。故本研究建議比照刑法第 201 條之 1 針對卡式支付工具的規定，新增刑法第 201 條之 2 之偽造變造數位支付工具罪，並置於偽造有價證券罪章下，以完整本罪章保護之法益，此外亦建議修正現行刑法第 205 條規定之文字作為配套。

本研究團隊之具體修法建議如以下修正對照表內容：

修正條文	現行條文	說明
第二百零一條之二 意圖供行使之用，而偽造、變造電子支付帳戶紀錄、第三方支付帳戶紀錄、虛擬通貨或其他相類作為支付工具之電磁紀錄者，處一年以上七年以下有期徒刑，得併科九萬元以下罰金。	(本條新增)	一、考量近年新興數位支付工具例如電子支付、第三方支付、虛擬通貨等之興起，而現行刑法第二百零一條之一第一項規定僅適用於偽造變造信用卡、金融卡、儲值卡等具有實體物的卡式支付工具，故有必要增訂關於偽造變造無實體的數位支付工具的規範，以保護數位支付系統的健全。爰參照

[399] 2001 年 6 月刑法第 201 條之 1 立法理由說明二。

行使前項偽造、變造之電子支付帳戶紀錄、第三方支付帳戶紀錄、虛擬通貨或其他相類作為支付工具之電磁紀錄，或意圖供行使之用，而受讓或轉讓於他人者，處五年以下有期徒刑，得併科九萬元以下罰金。		刑法第二百零一條之一第一項規定，增訂本條第一項規定，以規範偽造變造數位支付電磁紀錄之犯罪行為。 二、爰參照刑法第二百零一條之一第二項規定，增訂本條第二項規定規範行使、受讓或轉讓偽造變造數位支付電磁紀錄之行為。
第二百零五條 偽造、變造之有價證券、郵票、印花稅票、信用卡、金融卡、儲值卡或其他相類作為提款、簽帳、轉帳或支付工具之電磁紀錄物、電子支付帳戶紀錄、第三方支付帳戶紀錄、虛擬通貨或其他相類作為支付工具之電磁紀錄及前條之器械原料及電磁紀錄，不問屬於犯人與否，沒收之。	第二百零五條 偽造、變造之有價證券、郵票、印花稅票、信用卡、金融卡、儲值卡或其他相類作為提款、簽帳、轉帳或支付工具之電磁紀錄物及前條之器械原料及電磁紀錄，不問屬於犯人與否，沒收之。	配合第二百零一條之二之文字修正。

第二項 建議應建立金融科技犯罪相關之追蹤工具及資料庫

電子支付工具與虛擬通貨等金融科技工具運用科技技術改變支付方式，體現金融科技帶來的便利性與新穎性，但同時也增加犯罪偵查的挑戰，因此須受一定程度的監理例如洗錢防制。但對所有金融科技工具一律施以高強度的監理，可能增加此類新興金融科技的法律遵循成本而不利創新，進而引發普惠金融問題。為平衡監理目的與普惠金融，FATF 明白指出關鍵在於主管機關應採取風險基礎方

法（risk-based approach）的監理手段，不宜未經適當的風險評估與風險減輕措施即一概終止或限制金融科技業者的業務，否則反而會使客戶轉移至更高犯罪風險的服務或管道[400]。

欲採取風險基礎方法的監理，相關主管機關自須對金融科技工具在我國的犯罪風險進行評估，此有賴對金融科技工具過往涉及的犯罪進行實證調查。但如學者所觀察，金融科技對主管機關帶來的監理難題除監理資源匱乏與監理協作困難外，尚有監理實證不足的問題[401]。本研究雖試圖透過既有司法判決資料庫建立金融科技工具的犯罪實證資料，以協助評估金融科技工具涉及的具體犯罪風險，並已提出實證研究發現於第二章與第三章，但因司法判決資料庫僅涵蓋經起訴的案件，而未涵蓋所有發生的犯罪事件，故仍有其侷限。此外據本研究團隊之了解，目前政府部門相關資料庫並無特別針對電子支付工具或虛擬通貨等金融科技工具調查統計其涉及犯罪的情形，故我國針對金融科技工具的犯罪風險評估確實面臨監理實證不足的挑戰。

在監理人力與資源有限的條件下，監管科技（supervisory technology, SupTech）的概念近年逐漸受到重視，亦即監理機關運用科技有效落實其監理職責，透過科技方法協助自身在有限的監理資源下，盡可能全面且即時地對龐大的複雜系統施以監管[402]。欲落實監理科技，使相關科技方法例如大數據分析或人工智慧等技術發揮作用，監理相關資料的數位化為核心前提，如此方可建立數位資料庫供相關數據分析技術進行分析，從而確實掌握金融科技工具在我國的具體犯罪風險樣貌。本研究第四章即說明英國數位監管申報系統(Digital Regulatory Reporting)和新加坡智慧監管通報系統，即為建置金融監理資料庫不可或缺的利器之一，其除具有降低人力通報成本之優點，數位申報及通報可將資料標準化和去識別化，金融資料

[400] FATF, *supra* note 394, at 17-18.

[401] 臧正運(2020)，〈論金融科技發展的監理難題與法制策略——以我國的規範與實踐為核心〉，《政大法學評論》，第 163 期，頁 139-218。

[402] 臧正運（2021），〈金融科技法制與監理變革的形塑力量與關鍵趨勢〉，《萬國法律》，第 236 期，頁 2-10。

便可以大數據或人工智慧技術整理分析，用作犯罪預防、犯罪偵查及學術研究等用途。

此外，針對虛擬通貨，目前業者亦有開發相關虛擬通貨追蹤工具--Chainalysis[403]，此為美國聯邦調查局所採用的地址追蹤及分析虛擬通貨錢包地址的服務商，以其不斷完善的地址資料庫及地址標記功能受到國際間司法單位的採用。我國目前亦有虛擬通貨交易所業者引進使用，其主要功能包括：

1. 地址資料庫：整合全世界各國司法單位之定罪地址及自建可疑資料地址庫，標記地址超過百萬筆，類別包含暗網、毒品、色情、博弈等。
2. 地址追蹤：地址過往交易紀錄及關聯錢包圖像化，方便追蹤可疑或遺失資產。
3. KYT 交易掃描：利用 API 串接，可檢測交易所或錢包用戶之交易，如有可疑地址轉入，會提醒服務提供商有可疑虛擬通貨轉入；若是要轉出至可疑地址，該系統可禁止用戶轉出至可疑地址，如交易所間皆使用同一套系統並分享可疑地址資訊，結合各國司法單位及 Chainalysis 資料庫，可降低交易所用戶誤轉虛擬通貨至可疑地址，往後甚至可以為每一個錢包的風險等級進行評比。

虛擬通貨為全球交易市場，故需要建立全球性的地址資料庫及不斷更新地址標記才能完善整個金流紀錄，而類似於 Chainalysis 等在虛擬通貨地址的搜集的服務提供商，屬於監管科技之重要一環，故各國司法單位皆有導入相關監管科技做為其調查工具，本研究建議我國相關執法機構亦應考慮是否有相對應之監管科技可進行犯罪偵防。

此外，本研究建議相關主管機關可著手建立金融科技相關犯罪的資料庫，以俾長遠評估金融科技工具涉及的犯罪樣貌。具體而言，目前檢調機關的犯罪偵查資料可能並未全面數位化，即使有數位化者亦可能係以較不方便檢索的文件格式儲存，導致現有資料庫未能

[403] Chainalysis, https://www.chainalysis.com/, (last visited Aug. 30, 2021).

由既有犯罪偵查資料中辨識個別案件是否涉及金融科技工具，進而不易提煉出有助益的犯罪風險評估資訊，也不易分析資料中不同的信號與監理意涵。故建置相關資料庫首先須將犯罪偵查資料數位化與標準化，建立統一的檔案與資料輸入格式或進行資料編碼等；其次，於相關資料數位化與標準化後，可進一步利用相關數據分析技術爬取犯罪偵查資料中涉及利用金融科技工具犯罪者，進而分析相關犯罪類型、涉及犯罪金額與案件數、涉及的具體金融科技工具、偵查與破案情形、被害人背景、犯罪嫌疑人背景、是否涉及跨境等面向（本研究團隊研擬之金融科技犯罪相關之資料參數範例如附錄三）。

金融科技犯罪的數位資料庫除有助辨識金融科技工具的犯罪風險具體樣貌外，亦有助提升政府機關間的監理協力與監理品質。如上述，金融科技業者特別是第三方支付業者數量龐大，主管機關難以定期施以高強度的監理查核，但透過上述數位資料庫的資料累積，可進一步分析較常涉及犯罪事件的金融科技業者，進而可協助主管機關聚焦其查核的主要對象，將監理重點置於較高犯罪風險的金融科技業者，進而協助更有效率地落實對金融科技業者的洗錢防制監理，此亦符合以風險基礎方法實施監理的精神[404]。

第三項 建議落實洗錢防制之分級管理措施以促進普惠金融

聯合國普惠金融倡議（UN Secretary-General's Special Advocate for Inclusive Finance for Development, UNSGSA）於 2013 年 9 月出版之年度報告（Annual Report）中指出：「普惠金融為穩定且繁榮的金融體系及社會經濟發展之關鍵因素」[405]。金管會亦將普惠金融列為其政策之一，鼓勵金融業者推出符合社會各界或不同族群需要及量身訂做之多元金融商品及服務，並強化國人金融素養及善用金融服務[406]。

針對金融科技服務如何在犯罪防制與普惠金融間達成平衡，如

[404] FATF, *supra* note 394, at 16.

[405] UNSGSA, UNSGSA Annual Report to The Secretary-General, UNSGSA (Sept. 2013), https://www.unsgsa.org/publications/unsgsa-2021-annual-report-secretary-general.

[406] 金管會網站，https://www.fsc.gov.tw/ch/home.jsp?id=642&parentpath=0,7（最後瀏覽日：2021 年 08 月 13 日）。

上述 FATF 已指出關鍵在於確實落實風險基礎方法的監理手段。本研究認為，不論電子支付工具或虛擬通貨，於我國均有為數可觀的非金融機構（例如第三方支付業者與虛擬通貨業者）提供相關服務，法制上我國固然可將其納管並要求其負洗錢防制義務，但在相關主管機關具體執行監理措施時勢必有其極限，因此更需踐行風險基礎方法的監理手段，著重針對高犯罪風險的業者實施監理措施（例如重點查核或加強查核頻率）。

經比特幣及虛擬通貨發展協會[407]研究指出，現行《虛擬通貨平台及交易業務防制洗錢及打擊資恐辦法》（下稱「本辦法」）並未依據虛擬通貨業者之營業種類、營業規模、交易量分別適用相關洗錢防制措施，但目前世界主要國家就虛擬通貨業者如何遵守防制洗錢及資恐之現行規範，多係依據業者之規模、營業種類或交易額度分級管理，並調整不同的適用反洗錢措施之密度，此分級管理機制亦與 FATF 於 2021 年 3 月發布虛擬通貨業者洗錢防制指引草案[408]（下稱「FATF 指引草案」）所揭示針對不同之虛擬通貨業者規模、營業種類訂立風險係數，給予部分遵循之簡化措施[409]相符。

相較而言，本辦法第二條第一項第一款各目所訂之各類事業，其營業種類、規模、交易量均有不同，而本辦法未根據適用主體之不同而調整相應反洗錢措施之密度。實則，我國除少部分支持法幣入金之虛擬通貨交易所外，我國其餘虛擬通貨業者多數為具備未來發展潛力但員工團隊成員數量少於三十人之新創公司，一律適用相同強度之監理可能與 FATF 指引及國際洗錢防制實踐揭示之「分級管

[407] 比特幣及虛擬通貨發展協會為依內政部以 1100011800 號函核准籌備成立之非營利社團法人，團體會員主要為我國主要虛擬通貨交易平台、託管、錢包及其他虛擬通貨商業等業者，個人會員主要由學者或具法律及會計背景等專業人員組成，並以推動虛擬通貨有關之法規調適、虛擬通貨之應用及發展為宗旨，協助建立我國良好健全之虛擬通貨業環境，促進我國之相關產業及整體經濟向上發展，https://reurl.cc/xG5qrz（最後瀏覽日：2021/08/13）。

[408] *Supra* note **錯誤! 尚未定義書籤。**.

[409] 例如其草案第 135 段指出未進行 CDD 而建立臨時性交易的可能性，參見前註**錯誤! 尚未定義書籤。**，頁 46，paragragh 132: [In practice, VASPs typically open and maintain accounts (i.e., establish a customer relationship) and collect the relevant CDD information when they provide services to or engage in covered VA activities on behalf of their customers. **In cases where a VASP carries out an occasional transaction, however, the designated threshold above which VASPs are required to conduct CDD is USD/EUR 1000**, in accordance with INR. 15, paragraph 7(a). **The FATF agreed to lower the threshold amount for VA-related transactions to USD/EUR 1 000, given the ML/TF risks associated with and cross-border nature of VA activities**.].

理」方向不符。進一步言之，未採取分級管制而採用一體適用之結果，可能造成我國虛擬通貨業者之洗錢防制遵循成本遠較其他虛擬通貨業者高，對於我國虛擬通貨產業發展產生先天不利影響，除不利於普惠金融外，並可能導致我國軟體及高科技人才和產業外流之虞。

檢調機關作為第一線犯罪偵查的機關，基於犯罪偵查的需要，有相當機會與新興金融科技業者接觸，例如其可能為釐清金流軌跡，而請求金融科技業者提供其依洗錢防制規範應留存之客戶身分與交易紀錄等資料，從而有機會觀察涉案金融科技業者的洗錢防制措施實施情形。檢調機關如能將其第一線偵查時的觀察結果有效傳遞至主管機關—特別是通報洗錢防制措施實施不力的金融科技業者，主管機關即可以較低的成本取得高品質的監理實證資料，進而決定其重點監理對象。換言之，跨政府機關的監理協力，有助落實風險基礎方法的監理手段。

除透過檢調機關於偵查時的觀察外，本研究建議設置的金融科技犯罪數據資料庫，如上述亦有助落實風險基礎方法的監理手段。透過此資料庫的建置，相關主管機關得以統合各檢調機關的偵查資料，以此為基礎分析較常涉及犯罪的金融科技業者，進而對此類犯罪風險較高的金融科技業者實施較高強度的監理；相對而言，犯罪風險較低的金融科技業者即可面臨較低密度的監理，從而實質上承擔較低的法令遵循成本。最終犯罪風險較低的金融科技業者得以更有效率地提供金融服務，此亦符合普惠金融的目標。

第四項 重新檢視我國監理沙盒制度與洗錢防制之扞格

科技犯罪越趨常態，實務上可能作為「科技偵查」的手段也漸趨多元。但對照我國目前法制，關於偵查程式的干預處分，大致上僅有刑事訴訟法明文增修「電磁紀錄」作為搜索客體，以及通訊保障及監察法授權通訊監察、調取通訊紀錄的條款，如何兼顧科技時代下偵查效率與權利保障的衡平，遂成重要問題。

近年除金融科技（FinTech）與上述的監管科技（SupTech）興

起外，金融機構亦嘗試導入新興科技，以降低其遵循相關法令的成本或提升其遵循相關法令的能力，此又稱為法遵科技（regulatory technology, RegTech）。為使金融科技業者得以更有效率地配合檢調機關犯罪偵查之需要，本研究建議法制上應在犯罪風險可控的前提下，給予金融科技業者一定的實驗空間嘗試引入新興科技或其他創新業務模式，以提升其法令遵循的效率。

我國現行法制下給予金融科技業者實驗空間的相關法規，主要為金融科技發展與創新實驗條例引入的所謂監理沙盒制度。但依該條例第 25 條第 1 項規定：「創新實驗範圍涉及主管機關或其他機關（構）訂定之法規命令或行政規則者，主管機關基於創新實驗進行之必要，得於會商其他機關（構）同意後，核准創新實驗於實驗期間排除該等法規命令或行政規則全部或一部之適用，並免除申請人相關行政責任。但洗錢防制法、資恐防制法及相關法規命令或行政規則不得排除。」故依現行規定，金融科技業者如欲應用新興的法遵科技或創新模式取代目前法定的洗錢防制或資恐防制措施，僅能循修法途徑，尚不得利用監理沙盒實驗其創新的洗錢防制或資恐防制措施。

針對現行監理沙盒制度如此絕對嚴守洗防資恐規定，部分新創業者[410]曾表示如此將墊高其實驗成本，進而產生不利創新之效果。事實上，國外研究亦有指出，2017 年全球多達 48%的金融科技業者認為反洗錢與反資恐措施是行業成長的阻礙[411]，該研究亦指出當前金融科技新創業者多係從事小額交易，故其客戶與本身規模亦相對較小，加諸繁重的洗錢防制義務不僅可能不利此類業者的發展，對於洗錢防制之具體效果亦有待商榷[412]。

本研究認為，我國現行監理沙盒制度既已設有交易規模之限制，應足以控管沙盒實驗過程中的洗錢資恐等犯罪風險，故似可放寬現行監理沙盒規定，以給予申請業者實驗不同洗防資恐措施的空間。

---

[410] 工商時報(2019/05/10)，〈金管會：進沙盒有碰錢 就要防洗錢〉。

[411] Laurence Ingle, *Why Build a Sandbox on a Beach? An Analysis of Fintech Regulation in New Zealand*, SSRN (Aprl.12 4, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3156088.

[412] *Id.*

雖有論者認為，金管會已訂定「金融科技創新實驗防制洗錢及打擊資恐辦法」，故業已考量創新實驗的特性於符合洗錢防制法及資恐防制法下訂定差異化規範；然本研究團隊認為，依現行金融科技創新實驗管理辦法第 5 條之規定，實驗者與參與者簽訂契約之資金、交易或暴險金額最多不得逾新台幣 2 億元或等值外幣[413]，此外對非專業機構的參與者亦設有資金、交易或暴險金額的上限[414]，故實驗過程中的金融業務規模實際上甚小，洗錢犯罪風險因此亦較可控。基於風險基礎方法的監理原則，本研究認為至少立法上可考慮不排除申請者得利用監理沙盒機制實驗創新的洗防資恐措施，如此主管機關亦可於實驗進行中觀察申請者實驗的情形，一方面控管犯罪風險，一方面亦可藉由實驗測試較適合新興金融科技的洗防資恐等犯罪防制措施。

[413] 金融科技創新實驗管理辦法第 5 條第 2 項第 1 款、第 5 項但書。
[414] 金融科技創新實驗管理辦法第 5 條第 2 項第 2 款。

附錄一 專家座談會會議記錄

第一節 期中座談會議記錄

一、 **時間**：2021 年 3 月 31 日（星期三）9 時 00 分

二、 **地點**：恆業法律事務所 會議室

三、 **主席**：林繼恆專案主持人

四、 **記錄**：孔祥翎、洪振騰（楊岳平教授研究助理）

五、 **出（列）席人員**：

(一)法務部司法官學院：鄭元皓助理研究員

(二) 恆業法律事務所：計畫主持人律師林繼恆博士、專案經理李鎧如律師、研究員林紘宇律師

(三) 國立台灣大學法學院：楊岳平協同主持人、蘇凱平教授

(四) 法務部調查局臺北市調查處：蘇文杰調查官

(五) 東吳大學法學院：林育廷教授、蕭宏宜教授、李相臣教授

(六) 街口電子支付股份有限公司：林芝羽法務經理

(七) 現代財富科技有限公司：陳明惠營運長

(八) 幣託科技有限公司：鄭學豐法務暨法遵經理

(九) 博歐科技有限公司：范紀鍠執行長

(十) 艾米佳科技有限公司：林淦鈞執行長

六、 **討論事項**

(一) 主席致詞(略)：

(二) 法務部司法官學院致詞(略)：

(三) 楊岳平協同主持人、林紘宇研究員(略)：研究團隊報告

(四) 學者專家討論：

1. 東吳蕭宏宜教授發言:

(1) 剛好今天新聞說：使用虛擬貨幣可能會成為犯罪天堂、洗錢等等，此問題就現在台灣不是刑事實體法的問題，而是偵查手段與技巧怎麼樣精進的技術面操作問題，還有心態。

(2) 執法單位希望透過既有法律規範達到犯罪溯源的目的，既然（區塊鏈）每一個交易的過程都是透明的，我們可能沒有辦法去查到當時是誰去開虛擬貨幣的帳戶，有可能是人頭，且如果這個帳戶又開在境外，應如何處理這個行為？

(3) 就行動支付與虛擬貨幣可以從兩個層面觀之，行動支付會涉及較新的個資法問題（個資法四十一條與四十二條有附屬刑罰之規定），行動支付在過程中可能會掌握到每個消費者的消費習慣、地點等等，實務見解一般認為是可以受（個資法）保護的資訊，但卻很少人願意站出來去研究電子支付或行動支付、第三方支付等業者對於個資的取得及其將來之使用所造成潛在的風險的規範，反而都是將重心放在如何進一步針對交易過程去保護（比較多是藉由AES[415]+NDS[416]討論）。

(4) 當我們意識到虛擬通貨構成犯罪標的或作為進一步掩飾隱匿或持有犯罪所得的手段或方法時，我們如何確知行為人其實擁有虛擬貨幣？不論是行政調查或犯罪偵查都會面臨到這個技術瓶頸。又假設有證據可以證明確實擁有虛擬貨幣，下一個問題是，就比特幣來說，要怎麼命他交付私鑰？刑事訴訟法上的搜索扣押似乎不夠用，私鑰不見得有實體載體，如何進一步命其交付或取得，這邊會產生侷限性。

(5) 另外就是說，因為比特幣不是貨幣，當我們用來作為交易媒介時，

[415] Advanced Encryption Standard

[416] Neural Data Server

團隊可能漏掉一個在台灣也是犯罪的租稅問題，不管是租稅詐欺或稅捐的規定，這也可能是一個在研究虛擬貨幣遭到濫用於犯罪時可能會出現的點。

(6) 最後一個問題，我們在 2002 年曾經思考過要竊盜罪在刑法第 323 條納入電磁紀錄，但發現電磁紀錄並不適合符合傳統之「竊取」概念，對象也不是物，最後的解決方法是把它放到刑法第 359 條，但刑法第 359 條的變更刪除或取得，刑責只有五年以下，洗錢防制法則是七年以下。對刑法來說真正的意義應為，如同洗錢防制法第 15 條（關於特殊洗錢）還有第 18 條第 2 項（擴大利得沒收規定是對抗組織犯罪的重要利器，沒收第三人的財產不以有罪的確定判決為前提或必要）。

林繼恆計畫主持人回應：

謝謝蕭宏宜教授，我覺得剛才一個很重要的問題，的確我們都看到車手面，無法看到犯罪的全局。我特別介紹李相臣李教授，我們一起過去在 2001 年到 2011 年，因為信用卡犯罪極為猖獗的時候，當時銀行公會、中央金融研訓院以及法官學院（當時司法官訓練所）定期每年與法官、檢察官進行研訓與對話，讓司法界了解信用卡、金融卡犯罪的嚴重性。後來在信用卡犯罪經過立法後（增加支付工具罪）確實達到很好的嚇阻犯罪效果，今天第一階段請李教授分享他的觀察。

2. 東吳大學 李相臣教授發言：

(1) 當時之所以把竊盜電磁紀錄刪掉，是因為執法之實務上最主要的案型是寶物（虛擬寶物被盜取），當時並沒有修正刑法，故使用的是竊盜罪，竊盜是公訴罪，因此導致執法機關產生大量的案件，而且問題是涉案人都是年輕人，為了避免年輕人動輒涉及公訴罪，

這樣的執法及法規適用容有重新檢討的必要，我們也轉達與法務部相關的情形。

(2) 本計畫研究團隊簡報內容令我非常印象深刻，非常好的內容。現在我建議，在偵查面與法律面個人的想法補充，報告中分析了很多行動支付與虛擬貨幣的司法判決等資料，但我覺得資料不夠多，因為涉及到偵查面的資料，可能是占了十分之九（多數沒有進入到司法判例中，或是尚未破案），沒有破案的部分，警察機關跟調查機關都會與法務部防治電信詐欺與網路犯罪工作小組說明原因，因此建議，可以透過法務部司法官學院（委託單位）與法務部防治電信詐欺與網路犯罪工作小組函詢調取相關資料，到底我國執法部門針對虛擬貨幣、行動支付、網路電信等等，執法面上為何破不了案，偵查時碰到的困境是什麼，有無推動科技偵查法之必要等等。執法部門(調查局、刑事局)都會把所有科技犯罪資料(行動支付或虛擬貨幣)記載起來。

(3) 行動支付上面，我們先講信用卡，各位可能不知道，全世界台灣是第一個信用卡全部使用晶片的，因為台灣那時候是全世界信用卡犯罪最嚴重的，所以 VISA、Master Card 下重本（信用卡晶片成本高昂）。回到底層來說，建議研究團隊報告中可能要針對行動支付犯罪的發生原因予以補充：

A. 資安的問題：手機就有資安、訊息轟炸的問題

B. APP 功能：丹麥獨立記者曾經發現手機中如果超過十個 APP，有四個是會拿走使用者的資訊，有三個會存取你在手機的影片，有兩個會開啟你的麥克風跟攝影機，有一個會拿你現在打電話跟傳的 mail，這些全部都是經過使用者同意的（在下載 APP 時按確定），你等於把信用卡金融卡都放在手機裡面。

C. 沒辦法分辨訊息真假

(4) 對於行動支付遭濫用於犯罪之原因在於，我們只是把資料這些虛

擬化，但放在手機裡面，本身就會有這些問題，我們要怎麼樣回應這些問題，我會建議可能把區塊鏈、行動支付、手機本身的缺陷點出來，而資安是一個大問題。

(5) 比特幣就是網路的特性、虛擬通貨特性（可能就是匿名化、去中心化），所以實名制、多中心化可能是潛在解決方法，但現在很麻煩的是台灣中央銀行一直不認為比特幣是貨幣，所以我們的法令及執法上仍然有缺失。賴英照前大法官公開說：駭客入侵取得公司內部資料是否構成內線交易？參照歐盟法規該當、美國法則是看是否為利用電腦的漏洞（不構成）或偽冒他人的身分（構成），而參照台灣法令，則通通不構成（因為駭客並非公司之內部人或關係人）。不管是行動支付或虛擬通貨最大的問題是：我們執法機構沒有辦法自商業巨頭(資訊平台方)取得資料。

林繼恆博士補充：

從以前信用卡到現在，我們看到都是車手的活動都是年輕人，您過去的經驗觀察到更上層（首腦）如何利用車手、犯罪最原始的做法為何？

國際信用卡犯罪是國際分工，製造偽卡都是在境外，當時台灣因為法律特別低，後來我們的作法是以鄰為壑，把我們的堤防架高，不讓它們進來。我不曉得現在電子支付或虛擬貨幣上層的國際犯罪分工均在境外？

李相臣教授補充：

一般詐騙集團現在都是專業分工，建平台的人、打電話的人、領錢的人。例如過去承辦案件的經驗，寫木馬程式的集團、跟佈置木馬程式的集團（植入木馬的集團）跟領錢的集團是三個不同的黑幫組織，我寫完木馬告訴你這個木馬對某個系統可以運作，將這個木馬賣給植入的人，而犯罪風險最高的是車手，植入的人再把植入好的犯罪品賣給車手，最後可能被抓的是車手。

電話詐騙也是，建平台的人、打電話的人跟領錢的人，現在都只抓得到打電話的人或車手，幕後的人只有一個 IP 位址或虛擬電話。

電子支付也有可能是台灣人到境外去做，因為境外犯罪管轄權不到，我們不是國際刑警組織的會員國之一，這也是台灣的執法困境之一。

林紘宇計畫研究員回應：

感謝兩位教授，我簡單回應兩位教授。針對蕭教授所提出的問題，的確在偵查上面面臨最大的困難就是如何確定錢包位址是誰持有，這也就是 FATF 持續在強調的，要建立一個完整的洗錢防制 AML 防護網，是要把所有的虛擬通貨商都成為一個斷點，然後串接起來。因為一般的比特幣、以太幣錢包是匿名的，可是如果你要在虛擬通貨商進行註冊，並落實虛擬通貨業者把實名制（跟自然人綁定和法人實質受益人追蹤），誰持有這件事情是可以解決，各國在這塊上落實的進度也算是蠻超前的。

執法上面，等一下我們可以請蘇調查官分享一下目前我國實務進行的狀況，目前執法上的確會有一些扣押跟強制執行的案例，但大部分案例執法上的確是有一些限制的。另外蕭教授提醒的刑法電磁紀錄規範及規避租稅這部分我們之後也會進一步補充。

楊岳平協同主持人回應：

行動支付這邊面臨的困境也請各位回應或建議，像現在虛擬通貨業者是朝著建立完整的洗錢防制網去解決問題，但我們觀察到行動支付這邊面臨到的問題是，讓行動支付業者（例如超商代收代付業者）也應該建置類似的洗錢防制似乎並不現實。很難想像去超商繳代收代付款時，還要經實名制查證，影印身分證留存等等。但現實上代收代付業者確實經手大量的金流，類似的狀況也會發現在各種行動支付業者。電子支付業者已經被納入洗錢防制網當中，但全台灣還有大概九千多家第三方支付業者其實並沒有做類似的事情。實名制

是一個好的努力方向，也許套用到虛擬通貨業者目前可行，但若要繼續進一步延伸擴大（例如第三方支付業者）可能會面臨到一些阻力，這待會也希望聆聽大家的建議。

剛才李教授也提到超脫實名制以外其他可能的解決方案，包括從資安的角度或手機犯罪的角度思考，說不定與電信公司有著密切關係，這可能也是另外一個思考用來補足實名制實際實行上的困難與執行手段。

3. 陳明惠營運長：

其實台灣虛擬貨幣交易所於 2018 年 8 月時，銀行局跟銀行同業公會有發函給銀行說，如果未來虛擬貨幣業者要進行法幣交易，必須完成實名制，而虛擬通貨商業業者之後也確實依據公會的要求，並聘請外部機構進行查核，落實相對應的內稽內控。我們也會分享虛擬通貨交易所在現行實務上，是如何與我國刑事局、調查局協作對接，如何針對刑事詐騙、進行洗錢防制。

4. 林淦鈞執行長：

(1) 其實國際現在針對 Travel rule 已經有一套國際標準正在制定中，但現在處於是草案，草案內容可能還會再做修正，我是參與草案擬定人員之一，草案內容已經涉及到個資法的問題，也就是你今天的錢包位址，包含護照資料全部都在交換資料之內容裡面。

(2) 雖然此部分業者可能透過技術的方法做匿名性的規劃，但因為還要考慮各國之間個資法規的問題，變成說我們在制定這個 Travel rule 時我們有一定的局限性。

(3) 在國與國司法互助上，台灣是一個很特殊的案例，我們怎麼去跟別人做資訊交換，會變成一個窒礙難行之處，變成說到時候有很多國內外的交易所必須要跟台灣的業者進行交換。

(4) 就租稅的部分，其實 OECD 已經在此部分有所著墨，預計在今年會發布一虛擬通貨的租稅規範之補充文件。

【下半場】

5. **艾米佳科技有限公司 林淦鈞執行長發言：**新型態虛擬資產犯罪說明

(1) 今天我分享新型態的虛擬資產犯罪，我舉兩個例子跟各位說明。第一個例子【假的 USDT】；另外一個案例就是【假鈔混合真 USDT】

(2) 現在民間已經有假的 USDT 在流竄，可能衍伸兩個層面：詐欺與地下匯兌自己的準備金。在錢包地址我們發現，真的 USDT 有專屬的錢包地址合約，有多少錢、數量多少、錢包合約地址、發行商在哪裡，至於假的 USDT 錢包位址都沒有（但會有發行量、智能合約地址，也會有現在持有人的狀況）

(3) 我們發現到有現行四個假的 USDT 地址裡面，會收取到很多的假的 USDT（類似地下匯兌承兌商），代表有人拿現金或其他資產跟他做交換，他拿到假的 USDT，因為種種原因(例如覺得受騙)，再把這些假的 USDT 轉給其他下手。假的 USDT 智能合約現象於 2019 年就產生了。重點是：所謂假的 USDT 交易承兌商是用假的 USDT 當作準備金（就是銀行系統準備金的概念，用假的 USDT 代表未來我就是有這麼多的 USDT 存在），然後由主要的承兌商將假的 USDT 分散到它的其他下線的子承兌商。

(4) 第二個類型，有一則新聞是刑事局在偵查假仿真台幣，用一比十方式用真台幣換成假台幣，有一堆人去購買，一般流通的地方像是檳榔攤、雜貨店。這部分的案子在 USDT 也已經存在的，可能是未來我們必須要做關切的整個虛擬貨幣跟實體上金融上面所衍生的問題。

范紀鍠執行長補充：這種所謂 USDT 通常是屬於 ERC20，就是說在

乙太坊的網路上發行代幣，發代幣的 symbol（符號）是可以隨便取得，這也是為什麼我們可以用 ERC20 的代幣去發行 USDT，因為 USDT 本身也有 ERC20 的版本。根據我們系統的調查，已太坊上面其實有假的 ERC20 的 USDT 合約高達數十個以上，所以他是可以交易的，幣也是這樣轉來轉去，只是那個幣最終拿給 USDT 發行方，對方是不會承認的，拿到其他交易所也不會認。

6. 蘇文杰調查官發言：

(1) 目前執法機關第一線查獲虛擬貨幣相關的犯罪，第一個誰持有這個虛擬貨幣，第二個是我們怎麼樣使他交付虛擬貨幣。這兩個的確是目前實務上遭遇很大的瓶頸。

(2) 誰會持有這個虛擬貨幣，我們案件偵辦的流程，會有一些檢舉人提供的資料，比較不會發生到現場不知道要找誰持有幣的問題，因為我們都會有一個搜索扣押的標的。比較常見的問題是，我們怎麼知道他有多少種虛擬貨幣？當然目前有研發相關的軟體，到電腦裡面跑一跑，比較困難是說我們怎麼在窮盡一切偵查手段下，要求遭搜索人交付虛擬貨幣，如何請被告或犯罪嫌疑人交付相不法所得，是目前司法機關遭受到的問題。

(3) 我認為可透過法務部司法官學院這邊發文向內政部警政署刑事警察局資訊室成立的電腦犯罪偵查小組，要求提供相關資料。

(4) 第三，剛才計畫團隊林紘宇律師提到的虛擬貨幣部分進行回應，我自己偵辦（包含學術研究與案例偵辦），包含詐欺、包含駭客入侵竊取虛擬貨幣、包含電腦犯罪的勒索，這三類型的犯罪我都有參與過，我再補充一種類型，就是毒品案件，很多此類型犯罪都是用 line 這些通訊設備，我們發現很多人在暗網裡面用加密貨幣去買毒品，例如毒梟在加拿大，暗網中支付加密貨幣後請他從加拿大直接寄來，我覺得這也是屬於加密貨幣有關的犯罪類型。

(5) 金融犯罪的部分，我歸結目前涉及虛擬通獲犯罪特性五大特點：速度更快、手法更雜、受害者更多、金額更高、追查困難。

(6) 速度更快？因為加密貨幣屬於只要 button 按下去，很多犯罪不法移轉速度是彈指之間。

(7) 手法更雜，我觀察傾向於複合型犯罪（綜合電腦犯罪以及金錢犯罪），勒索手法搭配金錢犯罪，以及可能是內線交易、駭客入侵。

(8) 因為屬於群組散播，透過 line 或 Wechat 口耳相傳，群組都上千人以上，受害者更多金額也更高。

(9) 追查更難，追查手段需涉及科技偵查部分，目前的追查手段不足，也的確對我國執法機關追查面遇到不少挫折。

(10) 我很欣賞計畫團隊報告後面有講到國際合作的部分，透過國際的合作去追查虛擬金流，以及司法互助，對查緝的效能是會提升的。針對國際金融監理的部分，兩年 FATF 中連續發佈的兩則虛擬通貨監管指引，特別是去年九月，對整個 VASP 業者來講是一個非常大的提醒或幫助。

(11) 我國虛擬通貨監理的部分，我覺得需要我國法律面上更多的關注，因為洗錢防制法第 5 條已經把所有的幣納入犯罪，但相關的子法還沒有訂出來，這會影響預防犯罪，就洗錢防制來看，對後端執法會造成很大的困難，包括調查局、警方都會出現刑案中涉及的疑似不法金流，很快就轉到境外。以目前我國洗錢防制來說，銀行跟證券交易所都按照規定（洗錢防制法第 9、10 條）要申報，但虛擬通貨交易所這裡沒有相應的洗錢防制子法。

(12) 我覺得傳統金融與新興金融之間有一個溝通上鴻溝，那時我在立法院上我有提出跟委員報告說：這五十三項防制洗錢交易表徵不能全部移植到 VASP 業者，或者應該進行什麼樣的調整？

(13) 這需要熟悉兩塊的專家/學者，協助如何把洗錢交易表徵套用到 VASP 業者上面，以現在來說調查局（FIU）目前沒有收到任何有

關 VASP 業者所申報的資料，因為業者怎麼申報的格式內容都還沒訂出來，所以其實就算業者申報的話，調查局也會覺得這個沒辦法處理。我現在只希望金融監理單位或相關部門，或是能夠盡快把洗錢防制子法訂出來，這樣會大大影響及改善到後面預防犯罪的部分。其

(14) 跟國外例如美國的調查局(FIU)性質不同，我們調查局的性質偏向司法型的，FIU 每個國家都不一樣，有行政型、混合型、司法型，台灣是屬於司法型，台灣如要受理金融單位所申報這些資料是有一定的格式，我覺得研究報告中可以納入，對於 VASP 業者怎麼樣提出可疑交易申報的項目或規則之類。

7. 東吳大學 林育廷教授發言：

我個人希望從金融法制跟監理提供一些過去的經驗以供參考，主要在行動支付部分。

(1) 執行單位這個研究報告我個人非常印象深刻，資料量非常豐富，整個邏輯都非常好。我想說一件事情是說，包括楊老師剛才提到目前行動支付犯罪涉及到第三方支付或超商，我覺得這個地方可能要先去定調一下，我們現在不會再講代理收付，即使現在在名詞定義上還是會算入電子支付這個類型，其實超商與第三方支付是不太一樣的。超商在做的只有代收而沒有代付。為什麼可以拿中華電信帳單去超商付錢，是因爲超商是中華電信的代理人，超商不是代理收付的概念底下，是因為超商與本人之間有委任契約、代理契約，從這個部分去做收款方的一個監控可能是比較容易的作法。

(2) 另外談到第三方支付部分，我個人長期研究下來覺得第三方支付是國內行動支付上一個蠻大的問題。回到當年 2006 年我們國內斷掉線上第三方證券支付，開始十年立法爭論的過程。現行分成電

子支付與第三方支付，這樣的過程形成一個現況上很大的問題，我回應計畫主持人與李教授提到當時信用卡犯罪的立法背景，我們當時信用卡犯罪數量不是第一就是第二。其實是一個法規面下的磁吸效力，因為當時只有偽造私文書，刑度很低（六個月以下，甚至可緩刑），犯罪成本非常低，就造成很大的磁吸效應，當時一把刑度拉高就產生嚇阻效果。

(3) 2021 年 2 月時國內大概有九千多家第三方支付業者，2020 年 12 月時有破萬家。相較於在座的街口支付他們所受到的高度監管，相較於電子支付業者主管機關是金管會，有很高的資安要求、資本要求，第三方支付是幾乎完全無監管的；當年申請第一家第三方支付的業者叫寬庭，寬庭是在賣床單的。相信目前以統計數據來看，國內站在收款方、付款方之間做代理收付市占率不是第一也是第二的就是 Line pay，它是第三方支付。

(4) 假設我們今天在講犯罪偵防、資安管理、實名認證等要求時，現階段從金管會下去的只有涉及到電子支付，第三方支付就是形成三不管地帶，這裡面有一些完全沒在做代收付，但也有一些整個交易量已經衝高的第三方支付。磁吸效應就是一個犯罪行為人會看犯罪成本，透過第三方支付就是典型一個非常容易誘使犯罪人去使用的工具之一。我知道這涉及到金融監理的議題，但法務部或司法官學院這部分其實可以去提出一個建議，即使我們 2020 年 12 月底剛完成電支機構法的修法，仍然沒有正視這個問題。Line pay 現在國內可以轉帳，是因為後面有一卡通，但基本上呼應李教授提到的，執法機構在跟 Line Pay 等第三方支付機構要資料時碰到很多困難。

(5) 第三方支付背後那九千多家業者，包括摩斯、星巴克、麥當勞，他們目的其實不是要去做第三方的代理收付，比較不容易成為行動支付詐騙的工具，若將他們跟 Linepay 放在一起一樣的管理，我認為是有問題做法，如何抽離開來分別進行監管，我覺得是值得再被討論。

(6) 各位如果申請信用卡，拿到信用卡一定要先開卡之後才能刷。開卡這件事情是地方法院判決、法官所促成的。國內當時常見的信用卡詐騙常見的手法是，拿到資料後打進發卡銀行改掉信用卡地址，然後掛失，新卡就會寄到假的地址，所以不用太高深的技術，只要買到個資就可以拿到新的卡片。當時有非常多這樣的詐騙。印象很深的是那時候法院實務形成一個共識：這類開卡型詐欺案件原則上都判信用卡公司敗訴。這件事情也促成金融監理主管機關或銀行公會形成相關風險管控的措施，所以後來才多了信用卡開卡這件事情。

(7) 行動支付詐騙裡面有一些案件，持卡人拿到電信個資就去變更手機號碼，重新提出綁定，也出現類似的詐騙手法，詐騙金額累積起來很可觀。這件事情不需要太複雜的修法，透過業者形成一定的風險管控機制，給主管機關、同業公會壓力即可達成。如果當初改資料時，業者可以在後面加上管控措施，即可有效降低行動支付被濫用於犯罪工具的情形。

(8) 我們目前國內的信用卡還是失卡零風險，但如果在美國待過就知道，在美國持有 visa、master 就是完全持卡零風險，掉了就去掛失，掛失之後就能夠失卡零風險，這是 2000 年所提出的。過去幾年採用智慧偵測，使其能夠對危險交易、高風險交易、可疑交易能夠做非常好的切斷、阻斷，也加強了即時授權，信用卡業者在科技這部分進步之後，透過技術反而可以去解決這些問題。

(9) 技術進步是一回事，它可以改變交易、改變風險，但我覺得法官再教育也是必要性的。消費者教育也很重要，一個手機上綁那麼多東西的時候，你要有安全意識。信用卡現在為什麼還是有自付額三千元，這其實就是風險管理下的結果，信用卡在你手上，應該要有善良管理人的注意義務。行動支付這些科技，所謂的消費者教育能不能做到是一件事，但是一個可努力的：行動支付的詐騙、行動支付作為犯罪的工具，不管是哪一個類型，都是能夠透過讓消費者知道手上的媒介，可能成為犯罪的工具，進而落實犯

罪的預防。

楊岳平教授補充：

就超商部分補充，超商背後當然是有一個委託機構，我目前看到國際上洗錢防制要求，如果超商背後的委託機構有洗錢防制義務，就會要求超商（等於手足延伸）也會去要求超商去做類似的事情。很多第三方支付業者搭配超商的合作，因此衍伸很多金流活動，追根究底回到第三方支付沒有洗錢防制義務，透過超商的情形下當然也沒有。這部分當然是法制跟現實上的落差。

8. 台灣大學 蘇凱平教授發言：

首先是肯定研究團隊在做這個計畫非常用心，以一個一年的計畫做成這樣個人很佩服。

(1) 我的領域是刑事法相關的，特別是用到數位證據、區塊鏈、支付工具對犯罪、銀行法、洗錢防制法這部分，我建議在這個報告中或許可以嘗試從偵查到審判整個關於金融支付工具相關以及犯罪的流程去描繪出來，並將相對應的實務問題或其他補充資料予以補充。因為今天來的很多學者專家，大家工作以及專業的關係，往往都會集中在某一個階段，很多時候金流串不起來、資訊流串不起來、偵查手段上的完整描述也都做不起來。像上次在洗錢防制的討論、區塊鏈的討論或者是虛擬貨幣的追索過程討論裡面，很多時候我想偵查機關可能（調查局、檢警這邊）比較清楚，但到檢察官可能就不太清楚整個偵查手段在哪裡遇到障礙，到法官就更不清楚了。

(2) 行動支付方面在超商這一塊，我能夠理解超商是金流看得到的出入口，我只是建議)：在政策上還有在以法院判決為主的情況下，超商是一個政策機關或法院很喜歡拿來要求負責的對象，因為相對於金流跟資訊流，超商是實體的存在，看起來比較好

掌控。但超商有沒有這個能力去掌控，我個人是保持懷疑的態度，當然還要進一步的研究。

(3) 就虛擬貨幣的部分，報告中提到一個台灣高等法院 107 年金上字 83 號判決，我提醒在幣圈或新創圈的老闆（執行長、營運長）需要意識到這件事的潛在刑事責任風險。按銀行法第 125 條規定刑責至少要三年，所得超過一億（不考慮成本）至少判七年，法人犯罪將處罰公司負責人。

(4) 107 年金上字 83 號可能不會是指標性判決，到目前為止沒有任何其他地方法院判決引用，比較大的原因是因為判決做成後九天（109.4.18）銀行法第 125 條有進行修正。立法理由提到違法吸金案例層出不窮，犯罪手法有透過虛擬貨幣吸金。

(5) 現在台北地院、新北地院都有新創圈、幣圈因為發行虛擬貨幣的案子在偵查中，去年就有發生台北地檢署以違反銀行法為由起訴，我呼籲到在銀行法部分、洗錢防制法上我國需要有完整規劃，此點也應該在報告中呈現出來。

9. 街口支付 林芝羽法務經理發言：

各位先進好。針對剛才講到新興的金融工具，我們電子支付是比較受到高度監管的行業。

(1) 先回應幾位教授提到的問題，針對我們在偵查流程中遇到的問題，像盜用的話可能就是相關的身分登入帳號，被其他人用新的技術方式取得。這部分如果請被害人去警局報案，警方適用妨害電腦使用罪去偵辦，因為是告訴乃論，有些消費者在面對這樣金錢損害可能還會有消費者保護，現在電支的法規就是說應該是電支機構要去負相關的舉證責任，不然相關的損害是電支機構要負擔。用戶端在面對這樣盜用的情形可能會覺得在這樣立法例下會受到全額的求償，自己本身就沒有意願進行完後面的告訴流程。以盜用來說是告訴乃論的話，在電支機構或相

關平台想要去瞭解後面的犯罪的手法或者相關新興的犯罪技術在執行面上就會遇到一些困難。我們自己在去年八月遇到有八筆盜用案件，相關金額就大概一百萬。這部分其實以現在的法令，我們也有銀行公會內部也有針對，因為電支條例也有修法，其也有針對相關盜用的規則或者是定型化契約，是否要課予消費者更多的注意義務其實我們在銀行公會上面也有提出討論，銀行公會也有說在行政院消保會那邊永遠都過不了，因為台灣非常保護金融消費者。公會那邊討論是說不然就告到法院去，看法院怎麼判，因為現在沒有電子支付機構告過這樣的案件，銀行來說幾乎是每告必敗。以我們自己去看相關的犯罪手法，我們會去質疑說如果這個東西不去改，會不會犯罪集團只要A用戶去登入，B拿A的身分資料去登入但可是說不是我登入的，相關的金額變成電支機構要全額吸收，可能會有磁吸效用。因為手法簡單、容易否認、相關後續法院也不是這麼了解，所有的風險就會到平台跟機構業者身上，這部分也是可以一併在偵查跟司法歸責判斷上稍加著墨。

(2) 那針對消費者保護跟驗證的部分，用戶知不知道是哪些資料？因為像我們之前在一些案件偵辦上，警官有時也不知道需要哪些資料，我們資料對外提供也是受到許多法規的限制，必須要司法機關特定哪些資料我們才能提供。

(3) 之前遇到的盜用案件，像是電支機構在身分驗證這端其實比較嚴格，不像信用卡一樣很容易掛失或更改地址，我們的登入機制跟身分驗證機制都有比較高的要求。像我們去年八月遇到的盜用案件是用戶被強行從另外一個裝置登入，我們在驗證他是換裝置登入時就會重新執行一次身分驗證的流程，但是當用戶他的很機密的資料像是身分證字號（因為我們主要是驗身分證字號）還有我們驗證裝置的 OTP，但是現在有很多新的技術可以透過木馬的方式去複製或得到你曾經收到的 OTP 驗證碼。在這樣的情況下，用戶就從另外一個裝置去登入了，我們後續去

報案，警方要我們提供的資料像是 IP 或其他更細節登入的東西，在立法例上其實沒有要求電支機構要記載，或者我們之後希望在犯罪偵查手法上可以有更多的資料，像剛剛李教授有提到木馬或其他的方式，這部分如果明定在一些立法例裡面說如果你使用時我可能會取得這些資料，可能對於個資保護用戶是否願意提供這麼多的資料在一間機構裡面，及針對這個機構後續資安的管理是一個蠻複雜的問題。平台端也會希望通過用戶自己的教育，你的工具可能會受到盜用可能有什麼資訊在裡面，教育提高也應該相對負擔多一點點責任。

(4) 但這可能在台灣金融環境大概是很難達到的，這也是後續在業者跟消費者爭訟時法院判決，對相關的犯罪預防，甚至是助長可能都會有很大的關係。可能可以讓相關的調查局、法官更了解這些機構或金流運作的方式。

(5) 剛有蠻大一部分提到超商，那針對超商的代收可能也可以從法制上面增加一些限制，現在電支機構針對代收其實也有直接的法規去規範只有哪些風險低的項目可以透過其他人代收。相關的代收目前是兩萬塊的限制，第三方支付業者如果也沒有相關的反例去約束只有哪些東西能透過現金的方式去其他地方代收，否則只能透過 ATM 轉帳或是連結銀行帳戶的方式，或許可以降低超商端相關的犯罪行為。可能針對業者跟各位教授有提到的部分就我自己碰到的狀況提供一些分享。

10. 現代財富科技有限公司 陳明惠營運長發言：

(1) 其實我們虛擬通貨交易平台，目前有許多難處，第一我們完全沒有主管機關，不管央行、經濟部、內政部、金管會、調查局、法務部都回覆說不歸我管，數位科技部先前討論時，似乎已得到相同的答案。

(2) 目前台灣最熟悉虛擬貨幣犯罪大概是刑事局的「打擊詐欺犯罪

中心」，很多案例中通過以虛擬通貨投資的名義去詐騙，這些詐騙相關的案件處理其實都回到打詐中心。

(3) 詐騙方面我們觀察到，其實最常見的是投資詐騙跟愛情詐騙。投資詐騙又分兩種，一種是我幫你投資比特幣，另外一種是直接詐騙新台幣，例如在集團犯罪型的案例中，常常是犯罪集團告訴被害人說，把錢給我，我幫你做任何投資，等於是要被害人交出所有個資，包含雙證件跟銀行帳號，甚至要求被害人直接去電信公司開一個新的電信帳戶，等於辦一個手機號碼。因此呼應林教授提到的，是要教育使用者。這是最典型的投資詐騙。

(4) 另外是朋友之間的詐騙，朋友告訴他說我投資了比特幣超好賺，朋友之間把錢集資去投資，但朋友拿了錢就跑掉，或沒辦法如約定返還投資獲利，而涉及到民刑事糾紛。

(5) 愛情詐騙，其實不只有比特幣，其他各個行業都會看到的愛情詐騙的模式，我們交易所持續在進行交易監控，該樣態通常是法幣入金虛擬通貨出金，我們有內部虛幣地址的黑名單（哪些虛幣地址是可疑的，還有虛幣流向過於複雜或都流向某個特殊地址時），並於必要時暫停該地址之交易，避免類似詐騙案件既遂。國內三大有法幣入金的虛擬通貨交易所都有跟刑事局合作，我們會把可疑地址透過刑事局交換的方式通報給刑事局，刑事局有一內部平台去搜集這些可疑的錢包地址。

(6) 洗錢手法我們看到的通常是虛幣換法幣，通常會需要把拿到的虛擬貨幣在交易平台出去，就交易平台自立自強的方法就是防止這些人把他的虛幣換成法幣，就回頭做好實名制。實名制目前我們的作法通常就是除了雙證件以外，還要手持證件自拍（因為這樣才能確認他真的是本人去做這個交易），我們自己會把客戶填進來的資料做風險分析（我們內部有風險分數），當風險分數高的時候我們其實是要電話報回的，或者必要時我們會

要求更多的財力證明資料，證明是本人來做，且你確實知道你在做虛擬貨幣投資。這是我們在做詐騙跟洗錢的防範。

(7) 洗錢的樣態通常是虛擬貨幣入金，法幣出金，在洗錢方面分成幾個階段，尤其是在暗網。暗網裡頭的人都知道其實很難利用虛擬貨幣洗錢，因為他騙到的虛擬貨幣最後要從虛擬貨幣交易所出金，但交易所通常都是實名制，所以這個目標難以達到。因此犯罪集團的分工之一專門找交易所的漏洞，找到漏洞之後就會在暗網上公開販售交易所的漏洞，就會有另一批人專門在買虛擬貨幣交易所的人頭帳號。人頭帳號現在的行情以台灣交易所為例，一個平均都超過新台幣五萬塊；之後會有另外一批人，把人頭帳戶跟收到的虛擬貨幣交易所漏洞，整合後再賣出，然後由另一批人專門做駭客攻擊，得手的幣再拿到另外一個交易所。通常會在假日結束之後，交易所因為必須跟銀行進行法幣信託之交易，(尤其是廉價結束後)非假日天會有大量的法幣交易量，也會是駭客攻擊比較常發生的時間點。

(8) 回到我們實際上的方向，是我們自己本身看到的問題（我們三不管），我們虛擬通貨交易所在落實的洗錢防制措施各有不同，包含實名制這塊，實名制的強弱是一個標準，再來是內部反洗錢的制度怎麼做，如何進行洗錢的監控。其實我認為檯面上這三家法幣交易所應該都做得不錯，但我們在跟相關部門溝通過程中非常辛苦，因為目前台灣欠缺一個可疑交易地址的資訊平台，我們交易所之間不會互相分享彼此的錢包地址，我們只會通報給刑事局。刑事局拿到這些虛幣地址或錢包地址時，他也不能分享給其他交易所，就會變成是我們覺得有問題的地址，我們去問，刑事局可以告訴我們好像有問題，但我要不要封鎖這個客戶？目前我們交易所是只要有問題就通通封鎖掉，可是這種做法就會衍生不斷的客訴，還有額外的消費糾紛。

(9) 如果用戶把幣打到可疑地址，我們會凍結用戶的資產，禁止將幣打出。除非他提出證明說資金來源是正常的，如果資金來源

是法幣，我們會把法幣還回去給他，如果資金來源是虛擬通貨，虛擬通貨來源是可以查得到購買地，假設是其他交易所，用戶就必須證明帳號是他個人的，我們就會把幣還給他，然後再把帳戶關掉。但可疑地址是所有人都不能打入錢。

(10) 我們目前每一家業者實名制強度都不一樣，我們一直從去年開始就一直在跟相關主管機關溝通，並說明**我們需要有虛擬通貨商業同業公會、自律規範**。再來就是，洗錢防制上我們業者到底要怎麼執行，涉及法幣的這段我們都可以參考銀行相關作業規定，但虛擬通貨的洗錢防制要怎麼做，還有業者跟主管機關要怎麼通報，卻無所知悉，因為雖然法律規定，金融機構及指定之非金融事業或人員對於達一定金額以上之通貨交易應向法務部調查局申報，但其實實務上會通報的機關，並進行打擊犯罪的是刑事局，這兩個機構的資料如何共享，這也是一個問題。

(11) 我們通報調查局後，根據經驗似乎調查局較少處理後續的洗錢調查，也無法獲知該案件是否真的是涉及到洗錢。我們告訴刑事局時，刑事局就會去搜查前面是不是有涉及詐騙，但其實詐騙與洗錢是不一樣的，如果刑事局查並非涉及詐騙，就也不會進一步調查，但調查局這邊的相關洗錢搜查似乎較為欠缺，我覺得這是在整個虛擬通貨涉及犯罪的通報體制上可以再調整的。

11. 幣託科技有限公司 鄭學豐法務暨法遵經理發言：

(1) 有關面對這些不管是詐欺或是洗錢，我們自己會分成兩種，一種是【可追蹤的案件】，有直接受害者（不管是詐騙或龐氏騙局投資詐騙），這些受害者會跑到警局或跑到 165 報案，資料已經有一直接受害者蒐集完畢，我們交易所也比較容易透過相關資料數據，協助調查統計受害人跟犯罪金額。

(2) 另外一種相對困難是【無法追蹤的案件】，現在兩邊（跟現代財富）人頭帳戶的行情是差不多價格，因為我們現在實名制做的

越來越用力，所以人頭帳號越來越值錢。我們幣託設立一個帳號可能要費時五到七天以上。

(3) 實名制之外，外面買人頭帳號的情況是，連銀行帳號、手機帳號，甚至把手機都一併買下來，因為裝置就不會變，每次送出去的交易驗證都不會有任何問題，一包五、六萬元新台幣很常見。且他們犯罪集團會是在實際地面推廣，根本不牽涉到網路，因此它不會是一個直接受害者帳戶，它會是一個衍生帳戶，一個人頭帳戶可能一到兩天大概就失效，種種原因導致我們難以追蹤調查。不管是直接帳戶或人頭帳戶，這些金流我們在遇到的時候，通常就來不及阻止，金流就流掉了。

(4) 我們在做 KYC 的時候，我們會偵測可疑帳戶及可疑交易，不管是身分或交易的資訊，我們認為是可疑的時候，就直接把它封鎖了。還有另外一種不可追蹤的案型，我們叫做地下幣商，這種業者在我們交易所這邊開的是正常帳戶，前面跟想要交易的人收台幣，由地下幣商幫你把所有虛擬貨幣打到你指定帳戶。這樣的幣商某程度可以提供相關交易資訊，也是正常營用的公司或個人，這樣的狀況其實防不勝防。當我們發現可疑的時，我們會想盡辦法將這些帳戶的交易金額上限降低，甚至直接關掉，可是還是有蠻多我們沒有辦法辨識出來他們的行為到底是什麼，在有眾多這幾種無法追蹤的案型，我們很難去把它進一步統計及量化。

(5) 接下來我們想要回幾位教授剛才提到的，我們交易所在做 KYC 時其實會遇到的是強度問題。我自己是金融業出身，金融業在交易對象跟交易限度的時候，我們甚至會要求他提出這筆錢、虛幣要拿出國外時，可不可以提供我相對應的交易證明。這在虛擬貨幣也不是做不到，這就是 KYC 裡面更深入的 CDD、EDD 盡職調查的程度，可是目前虛擬貨幣業可能還做不到這件事。若有一包錢打到國外的某個地址（國外一個大交易所的地址），可是我們也沒辦法跟對方交易所交換資訊，這都是目前我們可

能會遇到的資訊交換上的困境。

(6) 以上其實也希望能夠在報告上呈現，因為我們交易所畢竟只是整個犯罪鏈中某個犯罪工具的問題，把這些問題整合起來，整個犯罪全貌會更為清晰，進而提出其他預防措施。

12. 博歐科技有限公司 范紀鍠執行長發言:

(1) 我們是資安技術解決方案的提供商，主要的解決方案是在做私鑰管理，台灣幾個大型虛擬通貨交易所都是我們服務的對象，我們在幫他們解決最底層交易的私鑰保管的工作。因為做個事情，我們會涉及到相關虛擬通貨交易。

(2) 過去我們自己也在做資安的業務，像是網路釣魚、反詐欺，所以我們在交易上面我們也就做 AML 技術解決方案。我們現在累積大概五十多萬筆名單的地址，也就是被我們貼上標籤的地址，這些標籤中其實有有三萬多筆是列為黑名單，其中有 34.89%是詐欺位址，這部分呼應研究團隊林紘宇律師調查報告的結果，大部分涉及犯罪的案型還是以詐欺為主；另外 39%是來自暗網的地址（曾經在暗網，或接觸過的地址），因為暗網中涉及的交易很複雜，我們可能沒辦法細分裡面的類型，比如說是跟毒品交易、槍枝交易有關，但只要來自暗網，我們百分之百列為高風險地址；另外還有比較大的比例是網路釣魚，去欺騙用戶，不管是交易所或暗網上的地址，我們都會鎖定追蹤。

(3) 我們在提供這些地址，除了服務給我們客戶端，目前也提供這種 AML 解決方案給來自全球的虛擬通貨商業業者，一般 AML 技術解決服務提供商的服務費用很高，一個錢包地址大概是 0.5 到 1 塊美金，這其實對交易所來講是一個非常大的成本負擔。所以我們希望把這樣的服務門檻降低，希望更多的業者能有這樣的能力去辨識交易對象的地址的風險係數，進而落實洗錢防制

的措施，有效降低洗錢風險。

(4) 所以台灣現在有一個問題是，我們希主管機關這邊能進一步確定，然後虛擬通貨相關的適法性確定。從技術面來看，區塊鏈這個技術，或新型態的支付技術會被用在不法犯罪，是不可避免的。我們的態度是，要先去了解它，經由最本質的基礎架構中去嘗試，並思考裡面如何做好防範。

(5) 或許比較激進的建議是，以區塊鏈網路來看，規範的是 VASP 跟交易所，從我了解整個區塊鏈的技術架構來看，節點是一個最根本的基礎，我建議應該把最基礎的礦工（節點）也列為實名制的規範。因為所有的交易都是經過這些節點廣播出去的，那這些節點的 IP 在哪裡，它收了第一份廣播的交易從哪邊來，其實有了 IP 這個匿名就不是問題，就是匿名性可以解決的。同時礦工落實實名制，對於稅收也是有幫助。從我了解整個區塊鏈的技術架構來看，節點是一個最根本的。

(6) 其他補充，我覺得在研究團隊報告中當講的滿好的，包含新型態犯罪類型，像是 Defi，Defi 除了在 cyber attack 上面偷取 Defi 上的資產外，現在還有透過 Defi 來遂行洗錢的動作。在幣圈鏈裡面也有混幣聚合器（混幣服務），在美國已經有相關執法經驗及判例，處理相關問題，這些在台灣好像還沒看到。

13. 法務部司法官學院 鄭元皓助理研究員發言：

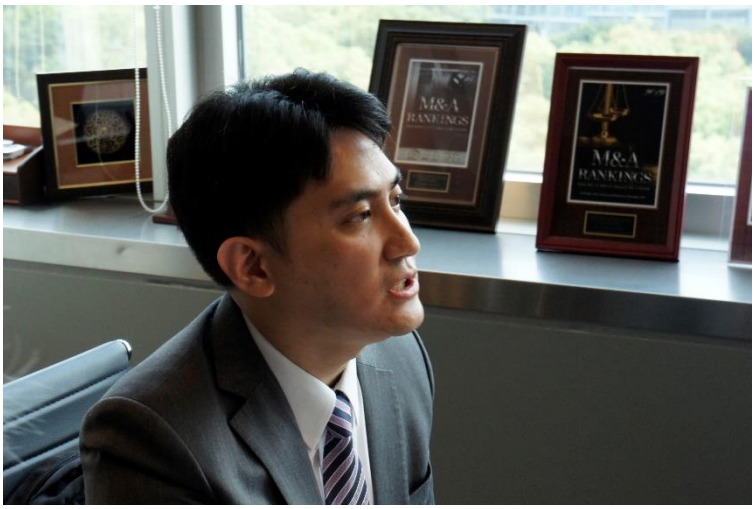
謝謝各位先進指教。法務部這邊大概有兩個可以協助的地方，第一個就是透過計畫報告呈現一些重要結論，進而提供給其他相應機關長官們瞭解，相關的法令的修正在立法院預期仍會遇到很多阻礙，包括之前科技偵查法草案。

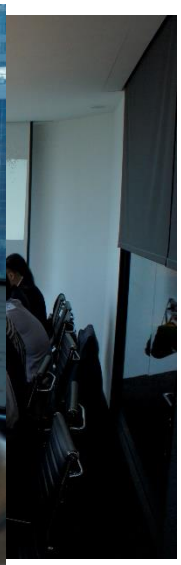
另外金融犯罪部分，我們在假訊息假帳號的部分，我們有跟刑事局、調查局做業務研析，因此本次討論有提到法務部司法官學院這邊發

文，向法務部防治電信詐欺與網路犯罪工作小組、電腦犯罪偵查小組要求提供相關資料，本院將可協助進行此部分工作，請本計畫研究團隊先行撰擬所需之資料類別，以利本院後續進行資料調取的工作。

（五）散會：12 時 40 分

第二節 期中座談會議照片






新興金融科技遭濫用於犯罪之研究
- 期中座談會 -
恆業法律事務所-大會議室
台北市松山區敦化南路一段2號11樓
2021 / 03 / 31 (三) AM 9:00 - PM 12:00
LIN & PARTNERS
恆業法律事務所

附錄二 研究倫理審查證明

國立臺灣大學
行為與社會科學研究倫理委員會

Research Ethics Committee
National Taiwan University
No. 1, Sec. 4, Roosevelt Rd., Taipei, Taiwan 10617, R.O.C
Phone: 3366-9956 Fax: 2362-9082

審查核可證明

核可日期：2020 年 12 月 29 日

倫委會案號：202012ES043
核可證明之有效期限：2021 年 1 月 1 日至 2021 年 12 月 25 日
計畫名稱： 新興科技遭濫用於犯罪之研究
校/院/系/計畫主持人： 恆業法律事務所/林繼恆律師
計畫文件版本日期：【研究計畫書，2020 年 12 月 21 日】、【知情同意書，2020 年 12 月 21 日】

上述計畫業於 2020 年 12 月 29 日經國立臺灣大學行為與社會科學研究倫理委員會同意，符合研究倫理規範並免除審查。本委員會的運作符合國立臺灣大學行為與社會科學研究倫理準則與規範及政府相關法律規章。

本案需經研究經費補助單位核准同意後，該計畫始得執行。

計畫主持人須依國內及國立臺灣大學相關法令規定通報計畫變更與嚴重不良反應事件。

行為與社會科學研究倫理委員會主任委員 蔡博文 蔡博文

Ethical Review Approval
National Taiwan University

Date of approval：December 29, 2020

NTU-REC No.：202012ES043
Validity of this approval: from January 1, 2021 to December 25, 2021
Title of protocol：Research on the Criminality of Fintech Abuse
University/College/Department/Principal Investigator：Lin & Partners attorneys-at-law/Managing Partner JI-HENG LIN
Version date of documents：【Research Protocol, December 21, 2020】,【Informed Consent Form, December 21, 2020】

The protocol has been approved by Research Ethics Committee of National Taiwan University and has been classified as exempt on December 29, 2020. The committee is organized under, and operates in accordance with, Social and Behavioral Research Ethical Principles and Regulations of National Taiwan University and governmental laws and regulations.

Approval by funding agency is mandatory before project implementation.

The investigator is required to report protocol amendment and Serious Adverse Events in accordance with the National Taiwan University and governmental laws and regulations.

Chairperson Bor-Wen Tsai
Research Ethics Committee Bor-Wen Tsai

2015 年 5 月 7 日國立臺灣大學研究倫理中心修正通過

國立臺灣大學行為與社會科學研究倫理委員會
新案審查送件核對單

（本清單請置於首頁） 2020 12ES043

計畫名稱：新興金融科技遭濫用於犯罪之研究

計畫主持人服務單位/姓名：恆業法律事務所/林繼恆

請勾選您已檢附之表單，並依下列順序置放：

項次	表單	備齊(V)	備註	REC 確認欄(V)
1	新案審查申請書（請以中文書寫）	V	必備，計畫主持人與單位主管需簽章	V
2	研究計畫書(含中英文摘要並加註版本)	V	必備，計畫主持人需於首頁簽章	V
3	研究參與者知情同意書(文件須加註版本) ■使用本中心格式之知情同意書 □使用自行設計之知情同意書 （請檢附「知情同意要素檢核表」） □不適用或申請免除研究參與者知情同意書 （請檢附「免除知情同意書或修正知情同意內容申請書」）	V	必備，計畫主持人需於首頁簽章	V
4	問卷(若屬訪談類計畫請附訪談大綱) (文件須加註版本) 資料蒐集表(Data Collection Sheet) (文件須加註版本)		若有(計畫主持人需於首頁簽章)	
5	招募研究參與者廣告文宣品(文件須加註版本)		若有(計畫主持人需於首頁簽章)	
6	本人類似或相關研究參考文獻		若有(請附近五年內參考文獻兩篇)	
7	主持人及協同研究人員之學經歷、著作及所受倫理相關課程訓練之背景資料	V	必備，計畫主持人需於首頁簽章	V
8	其他補充檔案或相關證明	V	*研究若使用次級資料，請附上說明原始資料正當性之補充文件，如：通過其他IRB/REC 審查之核可證明	V 合約書
9	碩士或博士論文大綱1份（論文目錄頁）		若協同主持人為研究生	na
10	上述申請文件請備妥紙本文件乙份	V	必備，雙面列印即可	V
11	上述申請文件請備妥電子檔案乙份（電子檔案無需簽章）	V	必備，請合併為一整份（Word 或 PDF 檔）並上傳至本中心之電子檔上傳系統	V
12	研究倫理審查費繳款資料表（無須電子檔，僅需紙本乙份）	V	必備，計畫主持人需簽章	V

若有需要，請依所屬學校或機構之規定將申請書及相關文件副知研發主管相關單位，以利計畫管控

上述申請文件之紙本請以長尾夾裝訂並依序置放表單、加註標示，掛號寄至國立臺灣大學研究發展處研究倫理中心：臺北市中正區思源街18號水源校區思源樓2樓2-5室。

送件人簽章/日期： 林繼恆 2020.12.23

研究倫理中心收件人簽章/日期： 行為與社會科學研究倫理委員會執行秘書 朱宗慧 收件受理

□ 文件不足，請補件予本案承辦人員（若需寄送紙本請註明「補件」）

☑ 確認送件資料與上述勾選項目一致 本案申請免審

國立臺灣大學 行為與社會科學研究倫理中心 109.12.25 送審證明章

REC-O-01

附錄三 國內犯罪中利用支付工具或虛擬通貨作為犯罪工具之統計數據表格範例

本研究團隊擬定國內犯罪中利用支付工具或虛擬通貨作為犯罪工具的統計數據表格範例供未來相關單位參考，並說明函詢表格內容如下：

一、 表格於每一年度中均含以下五個表格：全般刑案統計指標、案件偵結後處分與科刑、被害人背景調查、犯罪嫌疑人背景調查、本國案件與涉外案件：

(一)「全般刑案統計指標」表格中，所謂破獲總金額，乃指偵察機關破獲之案件中所涉之金額合計之數額而言；所謂沒收犯罪所得，則係指相關案件經法院裁判為應沒收並實際執行沒收後所得之金額。

(二)所謂涉外案件者，係指刑事案件中，有被告或被害人非我國籍人士，或行為（預備、實施或結果）之任一部分非在我國境內者而言。同理，所謂本國案件，乃指不具前開特性之案件。

(三)「本國案件與涉外案件」表格中列有數先前案例研究中發現支付工具犯罪較為熱門之地區或國家。然若 貴機關發現有其他熱門國家或地區，，還請 貴機關協助指明並提供相關數據。

二、 本研究計劃所稱的「支付工具」，可區分為電子支付、第三方支付、以及行動支付等三大類別，以下分別為其定義及所屬業者：

(一)電子支付：電子支付機構係指辦理代理收付實質交易款項、收受儲值款項、國內外小額匯兌、以及與上述三款業務有關之買賣外國貨幣及大陸地區、香港或澳門發行之貨幣業務之機構。目前國內計有 5 家專營電子支付機構及 23 家兼營電子支付機構，常見如：街口支付(街口)、橘子

支付、歐付寶、智付寶、簡單付(ezPay)等。

(二)第三方支付：係指僅經營代理收付實質交易款項業務且所保管代理收付款項之一年日平均餘額未逾新臺幣 10 億元。常見如：LINE Pay、綠界科技(ECPAY)、藍星科技、PChomePay 支付連、奇摩輕鬆付、HyPocket（全球聯網）、Swipy（紅陽科技）、SmilePay（訊航科技）等。

(三)其他行動支付：包含行動信用卡、行動金融卡、行動收單（mPOS）、行動電子票證等四項，分述如下：

4. 行動信用卡：係指信用卡發卡機構與代碼化服務業者合作，運用代碼化技術，使得持卡人經過申請及身分驗證等程序後，即可將實體信用卡卡號轉換成代碼載入手機等行動裝置，進而可持該行動裝置進行消費交易。常見如：Google Pay、Apple Pay、Samsung Pay 以及台灣 Pay。

5. 行動金融卡：係指透過空中傳輸下載個人化資料至行動裝置，發行具行動交易功能之金融卡。常見如：台灣 Pay「金融卡雲支付」。

6. 行動收單（mPOS）：又稱行動刷卡機，係指將行動電話或平板電腦搭配 APP 配件變成收單裝置，再經由刷卡或晶片插卡方式，讓商店端可以隨時接受信用卡付款。

7. 行動電子票證：係將電子票證載入手機 APP 等行動裝置，使用戶可透過 NFC 功能或掃描 QRcode 等方式進行消費交易的支付工具。常見如：悠遊付、NFC 手機一卡通、NFC 手機 icash2.0（聯名卡）等。

(四)本研究計劃所稱的「虛擬通貨」，包括：一、支付型代幣：僅單純做為支付用，而並未有進一步功能或連接到其他開發項目；二，效用型代幣：提供應用或服務之數位近用權之代幣；三，資產型代幣：用以表彰對於實體標的、公司之盈餘或股利之代幣，性質和股票、債券及衍生性金融商品，包括但不限於比特幣（Bitcoin）、以太幣

（Ethereum）、泰達幣（USDT）或其他作為犯罪客體或犯罪工具之虛擬通貨。

一、全般刑案統計指標

(一)犯罪類型(普通刑法)

全般刑案統計指標	發生數(件)	破獲數(件)	嫌疑人(人)	被害總金額(萬元)	破獲總金額(萬元)	沒收犯罪所得(萬元)	犯罪時鐘(分鐘)
犯罪類型（普通刑法）							
一般傷害							
妨害自由							
妨害名譽							
侵占							
賭博							
重利							
詐欺							
性交猥褻							
妨害秘密							
妨害家庭及婚							
誣告							
遺棄							
重傷害							
強盜							
對幼性交							
妨害秩序							
故意殺人							
強制性交							
毀棄損壞							
竊佔							
妨害公務							
搶奪							
贓物							
妨害電腦使用							
恐嚇							
背信							
偽造文書印文							
妨害風化							
公共危險							
竊盜							
其他							

一、全般刑案統計指標

(二)犯罪類型(特別刑法)

全般刑案統計指標	發生數(件)	破獲數(件)	嫌疑人(人)	被害總金額(萬元)	破獲總金額(萬元)	沒收犯罪所得(萬元)	犯罪時鐘(分鐘)
犯罪類型（特別刑法）							
毒品危害防制							
家庭暴力防治							
著作權法							
槍砲彈藥刀械							
商標法							
妨害兵役治罪							
洗錢防制法							
藥事法							
廢棄物清理法							
兒童及少年性							
公職人員選舉							
銀行法							
個人資料保護							
稅捐稽徵法							
組織犯罪防制							
貪污治罪條例							
就業服務法							
公司法							
森林法							
政府採購法							
臺灣地區與大							
其 他							

二、案件偵結後處分及科刑

(一)犯罪類型(普通刑法)

案件偵結後處分與科刑	不起訴處分		緩起訴處分		定罪人口率	科刑				
	(%)	件數	(%)	件數	(人/十萬人)	死刑(件)	無期徒刑(件)	有期徒刑(件)	拘役(件)	罰金(件)
犯罪類型(普通刑法)										
一般傷害										
妨害自由										
妨害名譽										
侵占										
賭博										
重利										
詐欺										
性交猥褻										
妨害秘密										
妨害家庭及婚										
誣告										
遺棄										
重傷害										
強盜										
對幼性交										
妨害秩序										
故意殺人										
強制性交										
毀棄損壞										
竊佔										
妨害公務										
搶奪										
贓物										
妨害電腦使用										
恐嚇										
背信										
偽造文書印文										
妨害風化										
公共危險										
竊盜										
其他										

二、案件偵結後處分及科刑

(二)犯罪類型(特別刑法)

案件偵結後處分與科刑	不起訴處分		緩起訴處分		定罪人口率	科刑				
	(％)	件數	(%)	件數	(人/十萬人)	死刑(件)	無期徒刑(件)	有期徒刑(件)	拘役(件)	罰金(件)
犯罪類型（特別刑法）										
毒品危害防制										
家庭暴力防治										
著作權法										
槍砲彈藥刀械										
商標法										
妨害兵役治罪										
洗錢防制法										
藥事法										
廢棄物清理法										
兒童及少年性										
公職人員選舉										
銀行法										
個人資料保護										
稅捐稽徵法										
組織犯罪防制										
貪污治罪條例										
就業服務法										
公司法										
森林法										
政府採購法										
臺灣地區與大										
其 他										

三、被害人背景調查

(一)犯罪類型(普通刑法)

被害人背景調查	年齡(%)							性別(%)		教育程度(%)					經濟狀況(%)		
	0-10歲	11-20歲	21-30歲	31-40歲	41-50歲	51-60歲	61歲以上	男性	女性	國小(含自修)	國中	高中(職)	專科以上	不詳	貧困	普通	富裕
犯罪類型（普通刑法）																	
妨害自由																	
妨害名譽																	
侵占																	
賭博																	
重利																	
詐欺																	
性交猥褻																	
妨害秘密																	
妨害家庭及婚																	
誣告																	
遺棄																	
重傷害																	
強盜																	
對幼性交																	
妨害秩序																	
故意殺人																	
強制性交																	
毀棄損壞																	
竊佔																	
妨害公務																	
搶奪																	
贓物																	
妨害電腦使用																	
恐嚇																	
背信																	
偽造文書印文																	
妨害風化																	
公共危險																	
竊盜																	
其他																	

三、被害人背景調查

(二)犯罪類型(特別刑法)

被害人背景調查	年齡(%)							性別(%)		教育程度(%)					經濟狀況(%)		
	0-10歲	11-20歲	21-30歲	31-40歲	41-50歲	51-60歲	61歲以上	男性	女性	國小(含自修)	國中	高中(職)	專科以上	不詳	貧困	普通	富裕
犯罪類型（特別刑法）																	
毒品危害防制																	
家庭暴力防治																	
著作權法																	
槍砲彈藥刀械																	
商標法																	
妨害兵役治罪																	
洗錢防制法																	
藥事法																	
廢棄物清理法																	
兒童及少年性																	
公職人員選舉																	
銀行法																	
個人資料保護																	
稅捐稽徵法																	
組織犯罪防制																	
貪污治罪條例																	
就業服務法																	
公司法																	
森林法																	
政府採購法																	
臺灣地區與大																	
其 他																	

四、犯罪嫌疑人背景調查

(一)犯罪類型(普通刑法)

犯罪嫌疑人背	年齡(%)							性別(%)		教育程度(%)					經濟狀況(%)		
景調查	0-10歲	11-20歲	21-30歲	31-40歲	41-50歲	51-60歲	60歲以上	男性	女性	國小(含自修)	國中	高中(職)	專科以上	不詳	貧困	普通	富裕
犯罪類型（普通刑法）																	
妨害自由																	
妨害名譽																	
侵占																	
賭博																	
重利																	
詐欺																	
性交猥褻																	
妨害秘密																	
妨害家庭及婚																	
誣告																	
遺棄																	
重傷害																	
強盜																	
對幼性交																	
妨害秩序																	
故意殺人																	
強制性交																	
毀棄損壞																	
竊佔																	
妨害公務																	
搶奪																	
贓物																	
妨害電腦使用																	
恐嚇																	
背信																	
偽造文書印文																	
妨害風化																	
公共危險																	
竊盜																	
其他																	

四、犯罪嫌疑人背景調查

(二)犯罪類型(特別刑法)

犯罪嫌疑人背景調查	年齡(%)							性別(%)		教育程度(%)					經濟狀況(%)		
	0-10歲	11-20歲	21-30歲	31-40歲	41-50歲	51-60歲	60歲以上	男性	女性	國小(含自修)	國中	高中(職)	專科以上	不詳	貧困	普通	富裕
犯罪類型（特別刑法）																	
毒品危害防制																	
家庭暴力防治																	
著作權法																	
槍砲彈藥刀械																	
商標法																	
妨害兵役治罪																	
洗錢防制法																	
藥事法																	
廢棄物清理法																	
兒童及少年性																	
公職人員選舉																	
銀行法																	
個人資料保護																	
稅捐稽徵法																	
組織犯罪防制																	
貪污治罪條例																	
就業服務法																	
公司法																	
森林法																	
政府採購法																	
臺灣地區與大																	
其 他																	

五、本國案件與涉外案件

(一)犯罪類型(普通刑法)

本國案件與涉外案件	本國案件		涉外案件		涉外案件中之熱門地區					
	件數	(%)	件數	(%)	中國(件數)	泰國(件數)	印尼(件數)	越南(件數)	菲律賓(件數)	其他熱門地區
犯罪類型（普通刑法）										
一般傷害										
妨害自由										
妨害名譽										
侵占										
賭博										
重利										
詐欺										
性交猥褻										
妨害秘密										
妨害家庭及婚										
誣告										
遺棄										
重傷害										
強盜										
對幼性交										
妨害秩序										
故意殺人										
強制性交										
毀棄損壞										
竊佔										
妨害公務										
搶奪										
贓物										
妨害電腦使用										
恐嚇										
背信										
偽造文書印文										
妨害風化										
公共危險										
竊盜										
其他										

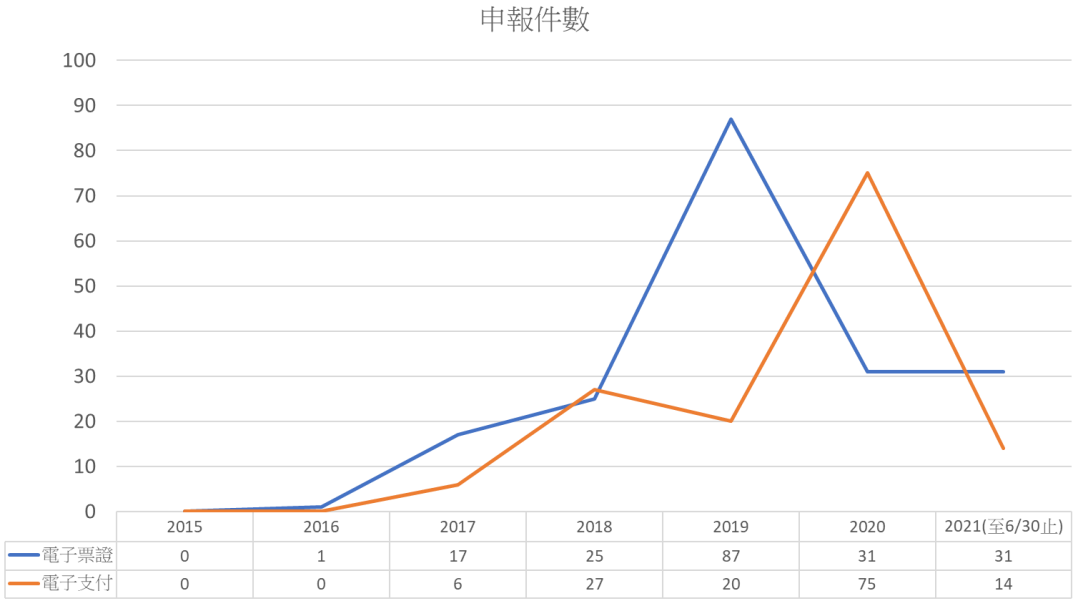
五、本國案件與涉外案件

(二)犯罪類型(特別刑法)

本國案件與涉外案件	本國案件		涉外案件		涉外案件中之熱門地區					
	件數	(%)	件數	(%)	中國(件數)	泰國(件數)	印尼(件數)	越南(件數)	菲律賓(件數)	其他熱門地區
犯罪類型(特別刑法)										
毒品危害防制										
家庭暴力防治										
著作權法										
槍砲彈藥刀械										
商標法										
妨害兵役治罪										
洗錢防制法										
藥事法										
廢棄物清理法										
兒童及少年性										
公職人員選舉										
銀行法										
個人資料保護										
稅捐稽徵法										
組織犯罪防制										
貪污治罪條例										
就業服務法										
公司法										
森林法										
政府採購法										
臺灣地區與大										
其 他										

附錄四 國內電子支付、虛擬通貨等業可疑交易申報情形統計資料

1.調查局洗錢防制處受理電子支付電子票證業可疑交易報告申報情形：



2.調查局洗錢防制處受理電子支付電子票證可疑交易態樣：

排名	疑似洗錢交易態樣	件數
1	使用者開立電子帳戶後立即有達特定金額以上款項存入，且又迅速移轉者	99
2	其他有疑似洗錢交易情形者	54
3	電子支付帳戶突有不尋常之大額款項存入、移轉或提領，且該電子支付帳戶並未有實質交易行為，或者實質交易行為與存入金額顯不相當，或與過往交易紀錄相較異常者	43
4	電子支付帳戶密集存入多筆款項達特定金額以上或筆數達一定數量以上，且又迅速移轉者	43
5	同一電子支付帳戶在一定期間內之現金存入交易，分別累計達特定金額以上者	37
6	電子支付機構發現使用者具「電子支付機構防制洗錢及打擊資恐注意事項範本」之應申報情形致無法完成確認身分相關規定程序者	31

7	不活躍電子支付帳戶突有達特定金額以上資金出入、且又迅速移轉者	28
8	使用者每筆存、提金額相當且相距時間不久，且累計達特定金額以上者	20
9	同一人之記名電子票證無正當理由，突然同一營業日累計交易新台幣五十萬元以上之金額	10

3. 我國虛擬通貨遭濫用於犯罪之量化分析與相關防制洗錢規範：

申報時間起迄	2021 年 7 月 1 日起至 2021 年 8 月 31 日止
件數	14 件
涉及虛擬通貨種類/數量(合計)	1. 泰達幣(USDT):4,318,665.966 顆(折合新台幣約 **1 億 1970 萬 6358 元**) 2. 比特幣(BTC):2.2927238 顆(折合新台幣約 **266 萬 1549 元**)

虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法

總說明

洗錢防制法於一百零七年十一月七日修正公布，依同法第五條第二項規定，虛擬通貨平台及交易業務事業（以下稱本事業）適用該法關於金融機構之規定，包含應建立洗錢防制內部控制與稽核制度、進行確認客戶身分、紀錄保存、一定金額以上通貨交易申報及疑似洗錢或資恐交易申報等事項。另防制洗錢金融行動工作組織（Financial Action Task Force，以下稱 FATF）已要求虛擬資產（即虛擬通貨）服務提供者應遵循 FATF 第十五項建議等防制洗錢規範。

4.調查局洗錢防制處受理虛擬通貨平台交易業務士業可疑交易報告申報情形：

編號	虛擬通貨平台及交易業務事業可疑交易態樣	有無申報案件
1	**客戶疑似使用匿名、假名、人頭、虛設行號或虛設法人、團體，或持用偽、變造身分證明文件及資料建立業務關 係**	有
2	客戶建立業務關係之網路位置(如 IP 位址等)與客戶國籍、註冊所在國家或地區不同，且無合理原因者	尚無

3	無合理原因開立多個公司或團體之交易帳號，且實質受益人為同一人	尚無
4	數個不同客戶之交易帳號留存相同地址、電話或電子郵件等資料，但依據個別留存資料(如姓名、年齡、居住地點及電話等)，各客戶間並無明顯關係	尚無
5	客戶無合理原因頻繁變更客戶資料，或拒絕配合提供確認客戶身分措施相關文件	尚無
6	知悉客戶已被其他虛擬通貨平台及交易業務事業(以下稱 VASP)拒絕建立業務關係或交易，或其客戶身分已被終止	尚無
7	**客戶大量或短期密集買賣及交換虛擬通貨，且與其身分顯不相當或無合理原因者**	有
8	**新註冊或一定期間無交易之帳號突然有大量交易，且與其身分顯不相當或無合理原因者**	有
9	同一 IP 位址使用數個無關連之交易帳號進行交易，而無合理原因者	尚無
10	客戶無合理原因將交易分拆為小額交易，以規避臨時性交易確認客戶身分之門檻者	尚無
11	**客戶買入或接收虛擬通貨後，迅速轉出或交換成其他虛擬通貨，一定期間內合計達特定筆數或金額，且交易內容與客戶身分顯不相當或無合理原因者**	有
12	客戶小額接收多種或多筆虛擬通貨後，將虛擬通貨整筆轉出或賣出取得法定貨幣款項，且無合理原因者	尚無
13	客戶涉及電視、報章雜誌或網際網路等媒體即時報導之特殊重大案件，且交易顯屬異常者	尚無

14	知悉客戶交易之 IP 位址、法定貨幣資金、虛擬通貨來源位址或交易位址與暗網、使用混和服務、虛擬通貨混幣器、 國際防制洗錢組織公告之洗錢或資恐高風險國家或地區或不法活動相關	尚無
15	客戶來自或客戶交易 IP 位址屬於國際防制洗錢組織公告之洗錢或資恐高風險國家或地區、高避稅風險之國家或地區 ，而進行頻繁大量交易者	尚無
16	**無論交易金額多寡或交易是否完成，發現其他明顯異常情形或交易，經本事業內部程序認定屬疑似洗錢或資恐交 易者**	有
17	**客戶與多家未受洗錢防制規範之 VASP 或多個疑似非本人持有之私有錢包頻繁進行虛擬通貨移轉，交易內容與客戶 身分顯不相當或無合理原因者**	有
18	客戶本人或其實質受益人為外國政府或國際組織認定或追查之恐怖活動或資恐相關個人、法人或團體，或有合理 理由懷疑其與恐怖活動、恐怖組織或資恐有關聯者	尚無
19	客戶本人或其實質受益人為外國政府或國際組織認定或追查之資助武擴目標性金融制裁之個人、法人或團體，或 有合理理由懷疑其與資助武擴有關聯者	尚無

附錄五 相關參考資料

一、 中文參考文獻

1. 中央銀行(2017)，臺灣電子支付之發展，立法院第 9 屆第 3 會期財政委員會第 15 次全體委員會議。
2. 中央銀行(2018)，數位金流與虛擬通貨－－央行在數位時代的角色，存款保險資訊季刊第 31 卷第 4 期。
3. 中央銀行(2021)，虛擬通貨近期發展及國際監管概況。
4. 王士帆(2016)，〈網路之刑事追訴—科技與法律的較勁〉，《政大法學評論》，第 145 期。
5. 王士帆(2016)，網路之刑事追訴—科技與法律的較勁，政大法學評論，第 145 期。
6. 王兆鵬(2010)，《刑事訴訟法講義》，4 版。
7. 王志誠(2017)，〈洗錢防制法之發展趨勢-金融機構執行洗錢防制之實務問題〉，《月旦法學雜誌》，第 267 期。
8. 立法院，

   https://lci.ly.gov.tw/LyLCEW/agenda1/02/pdf/08/06/02/LCEWA01_080602_00109.pdf。
9. 田篭照博著，朱浚賢譯（2018），《區塊鏈智慧合約開發與安全防護實作》，台北旗標出版社。
10. 朱瑞翔(2019)，〈由系統性風險控管論電子支付業之定義－以代收代付業為中心〉，《中華國際法與超國界法評論》，第 15 卷。
11. 宋皇志、吳婕華(2021)，〈虛擬貨幣之法律性質與監理規範〉，《臺北大學法學論叢》，第 117 期。
12. 李宜雯，黃曉盈，周玉娟(2019)，〈我國對證券型代幣發行、交易及平台監理之規劃方向〉，《證券暨期貨月刊》，第 37 卷第 11 期。
13. 李貴英、聶家音(2014)，〈歐洲聯盟經濟治理與金融監理架構

之改革〉,《月旦法學雜誌》,232 期。
14. 李榮耕(2009),〈個人資料外洩及個資外洩通知條款的立法芻議〉,《東吳法律學報》,20 卷 4 期。
15. 李榮耕(2012),〈電磁紀錄的搜索及扣押〉,《國立臺灣大學法學論叢》,第 41 卷 3 期。
16. 沈中華等(2020),〈臺灣行動支付發展與歸類檢討〉,《存款保險資訊季刊》,第 33 卷第 1 期。
17. 沈易(2019),〈淺論比特幣在民事法律上之定性〉,《司法新聲》,第 129 期。
18. 官禹婕(2014),〈網路使用者身份驗證機制研析——以電子支付機構國際立法及推動經驗為中心〉,《科技法律透析》,第 26 卷 11 期。
19. 林宜隆,黃讚松(2002),〈網路使用問題分析與犯罪預防之探討〉,《資訊科技與社會學報》,第 3 期。
20. 林東茂(1999),〈經濟犯罪的幾個現象面思考〉,《刑事政策與犯罪研究論文集》,第 2 期。
21. 林盟祥(2017),〈數位通貨與普惠金融之監理變革——兼論洗錢防制之因應策略〉,《月旦法學雜誌》,第 267 期。
22. 金管會(2018),行動支付與電子化支付普及之關鍵,臺灣經濟論叢,第 16 卷第 2 期。
23. 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》,第 18 期。
24. 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〉,《月旦裁判時報》,第 64 期。
25. 施育傑(2020),〈科技時代的偵查干預處分–兼論我國法方向〉,《月旦法學雜誌》,第 306 期。
26. 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》,第 288 期。
27. 徐珮菱、高培勛(2020),〈中心化金融之法律規範研究—以 Defi 借貸為核心〉,《高大法學論叢》,第 16 卷第 1 期。

28. 翁世吉、田育任(2014)，〈「行動商務」支付應用發展趨勢〉，《財金資訊季刊》，第 78 期。
29. 陳丁章、范建得、黎昱萱(2021)，《自比特幣技術的特徵論虛擬貨幣的法律特性及其相關問題-虛擬貨幣(通貨)的法律監理》，元華：台北。
30. 陳俊成(2018)，〈金融科技犯罪與防制-結合資訊安全觀點〉，《南臺財經法學》，第 4 期。
31. 陳榮傳(2019)，〈論比特幣與比特幣之債〉，《軍法專刊》，第 65 卷第 6 期。
32. 陳靜慧(2015)，〈網路犯罪之新趨勢與規範狀態之初探～從物聯網之發展談起〉，《臺灣嘉義地方法院檢察署 104 年度自行研究報告》。
33. 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〉，《臺大法論叢》，第 48 卷特刊。
34. 楊岳平(2020)，〈論虛擬通貨之法律定性——以民事法與金融法為中心〉，《月旦法學雜誌》，第 301 期。
35. 經濟部中小企業處(2018)，〈普及智慧支付 開創數位經濟〉，《臺灣經濟論衡》，第 16 卷第二期。
36. 詹德恩(2013)，〈我國金融犯罪特性與抗制難題〉，《中正財經法學》，第七期。
37. 臧正運(2020)，〈論金融科技發展的監理難題與法制策略——以我國的規範與實踐為核心〉，《政大法學評論》，第 163 期。
38. 臧正運(2021)，〈金融科技法制與監理變革的形塑力量與關鍵趨勢〉，《萬國法律》，第 236 期。
39. 臺灣證券交易所(2015)，英國證券市場相關制度。
40. 劉蕙綺(2020)，〈淺談日本針對加密資產/虛擬通貨相關法規之修訂〉，《金融聯合徵信》，第 36 期。
41. 蔡英欣(2018)，〈試論虛擬貨幣之監理與法律地位——以日本法為中心〉，《管理評論》，第 36 卷第 4 期。

42. 蔣念祖、戴凡芹(2019)，〈電子支付管理條例修正草案評析〉，《萬國法律》，第 228 期。
43. 鄭文中(2018)，〈淺論歐盟刑事司法合作之歷史發展〉，《台灣國際研究季刊》，第 14 卷第 3 期。
44. 鄭婷嫻(2021)，〈論證券型虛擬通貨引進後證券法規應用與監理機制調適〉，《臺灣財經法學論叢》，第 3 卷第 1 期，。
45. 謝孟珊(2013)，〈第三方支付法制問題研析〉，《科技法律透析》，第 25 卷第 2 期。
46. 謝孟珊(2016)，〈網路代理收付服務於 FATF 及美國之洗錢防制監管規範分析〉，《科技法律透析》，第 28 卷第 2 期。
47. 謝孟珊(2017)，〈電子支付業務管制範疇之比較法研究〉，《月旦法學雜誌》，第 263 期。
48. 鍾欣宜(2019)，〈首次代幣發行(ICO)監理趨勢初探〉，《國家發展研究院經濟研究》，第 19 期。
49. 蘇文杰、李穎、葉永全(2018)，〈毒品交易虛擬金流偵查新模式－以本局與荷蘭警方合作偵查個案為例〉，《107 年毒品犯罪防制工作年報》。
50. Matthew Kien-Meng Ly, Coining Bitcoins “legal-bits”: Examining The Regulatory Framework For Bitcoin And Virtual Currencies, 27 HARV. & Tech 587, 594, 608(2014). 轉引自郭戎晉，網路虛擬貨幣法律爭議之探討，科技法律透析，2014 年 10 月。

二、 網路參考文獻

1. BBC 中文，肺炎疫情：美聯儲緊急降息至零利率 「一次性打完所有彈藥」，2020 年 3 月 16 日，https://www.bbc.com/zhongwen/trad/business-51906250。
2. CTWANT，〈【帳號交易詐個資 5】利用「虛擬帳號」讓受害者儲值　詐騙集團再將錢購點數「銷贓」〉，https://www.ctwant.com/article/31508。
3. ETtoday 新聞雲，〈台灣詐欺犯罪越掃越多？警界有苦難言：

源頭死角太多〉，
https://www.ettoday.net/news/20210211/1917772.htm。
4. Q點虛擬貨幣 吸金2.5億9人起訴，2021/04/24，
https://www.chinatimes.com/newspapers/20210424000443-260106?chdtv。
5. 工商時報（2021/01/21），〈又見三家申設專營電支 首見銀行業與超商結盟〉。
6. 工商時報（2021/03/1），〈五大行動支付 嗶逾4千億〉。
7. 工商時報（2020/08/08），〈台灣超商密度世界第二〉。
8. 工商時報(2019/05/10)，〈金管會：進沙盒有碰錢 就要防洗錢〉。
9. 中央健康保險署新聞稿（05/06/2020），〈不會有連結！口罩進化，小心詐騙也進化〉，https://www.mohw.gov.tw/cp-16-53090-1.html。
10. 中央銀行，比特幣價格大幅波動之說明，
https://www.cbc.gov.tw/tw/cp-1170-128220-09e31-1.html?fbclid=IwAR1Qgs4Vwo1ud_8RZ355t7xnmo6fMiMlhbQ1ynLhnbv5jGuFl-YbcUUL0iw。
11. 中央銀行業務局，金融科技破壞式創新：重塑金融與監管，
file:///C:/Users/CYL/Downloads/C10602508.pdf。
12. 日本加密貨幣交易所遭駭35億日圓一夕消失無蹤，2019-07-12，中央廣播電臺，
https://www.rti.org.tw/news/view/id/2027140。
13. 日本金融庁、消費者庁、警察（2021），暗号資産（仮想通貨）に関するトラブルにご注意ください！，
https://www.fsa.go.jp/news/r2/virtual_currency/20210407_pdf1.pdf。
14. 日本金融庁、消費者庁、警察（2021），暗号資産（仮想通貨）に関するトラブルにご注意ください！，
https://www.fsa.go.jp/news/r2/virtual_currency/20210407_pdf1.

pdf。
15. 比特幣交易平台 Mt.Gox 申請破產保護，BBC 中文網，2014 年 2 月 18 日，http://www.bbc.com/zhongwen/trad/business/2014/02/140228_bitcoin。
16. 比特幣並非貨幣，接受者務注意風險承擔問題，中央銀行 https://www.cbc.gov.tw/public/Attachment/3123016334171.pdf 。
17. 以毒攻毒？虛擬貨幣與反洗錢的棋逢敵手，https://www.bnext.com.tw/article/56330/bitcoin-money-laundering（最後瀏覽日：2021 年 6 月 21 日）。
18. 台灣刑事局破獲 EOS 為賭注的「2020 大選賭博 DApp」，區塊鏈博弈爭議，動區，2019 年 4 月 4 日，https://www.blocktempo.com/taiwan-eos-gamble-bet-president-election-1/?fbclid=IwAR1jlARdLWVKwbs5rs7XzoyUudUbFoxFPj-FiJ25guELZ0ktlMGypNgwmvI。
19. 台灣被捲入洗錢風險？金融犯罪嫌疑者 iFinex，曾是 7 家本土銀行客戶，https://www.cw.com.tw/article/5101992。
20. 台灣經貿網，新加坡銀行業將增加數據分析人才以更準確偵查金融犯罪案件，https://info.taiwantrade.com/biznews/%E6%96%B0%E5%8A%A0%E5%9D%A1%E9%8A%80%E8%A1%8C%E6%A5%AD%E5%B0%87%E5%A2%9E%E5%8A%A0%E6%95%B8%E6%93%9A%E5%88%86%E6%9E%90%E4%BA%BA%E6%89%8D%E4%BB%A5%E6%9B%B4%E6%BA%96%E7%A2%BA%E5%81%B5%E6%9F%A5%E9%87%91%E8%9E%8D%E7%8A%AF%E7%BD%AA%E6%A1%88%E4%BB%B6-1672046.html
21. 全球最大網路黑市「絲綢之路」創始人被判終身監禁，關鍵評論，2015 年 5 月 30 日，

https://www.thenewslens.com/article/17677。
22. 自由時報（2020/02/26），〈虛擬帳戶成詐騙工具 警：個資外流小心成幫助犯〉。
23. 自由時報（2020/03/28），〈網購包裹到家了？恐損失近萬元、「簡訊連結」千萬別點！〉。
24. 自由時報（2020/10/15），〈「全聯」APP 會員贈點活動遭惡意程式詐騙 盜取 1500 萬點數〉。
25. 行政院，加速推動行動支付普及，https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/84ca877a-f946-4684-a19d-732a351dc448。
26. 事務ガイドライン第三分冊：金融会社関係 16・仮想通貨交換業者関係 https://www.fsa.go.jp/common/law/guide/kaisya/16.pdf (最後瀏覽日：2021 年 8 月 15 日)。
27. 国家公安委員会，犯罪収益移転危険度調査書，令和元年 12 月 https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/risk/risk011219.pdf (最後瀏覽日：2021 年 8 月 15 日)。
28. 金管會，虛擬通貨（或稱虛擬資產），https://moneywise.fsc.gov.tw/tabf/FW/FW14_index.html。
29. 金管會，電子支付機構及第三方支付服務業之異同，https://fscmail.fsc.gov.tw/swsfront35/FAQF/FAQDetail.aspx?f=f490e4196e2e39af683286ace2f9c2373a8c2b9874d07219263837a8bb8bd3e2&p=ad9ce81c136bb3a66fffdd0d844dc281f1729de4f28f32541e7233a475eb804e4040a45c7a24799c4afe51824a425576835e00ac075cb6e55207c6a619ce5f6804903e07617d70572744be79568babc299b80592fa6fc6b7d4990ac104084537b7bbbfcfc63cae0ed7ade20d5a47e7259f6e70309de048d2。
30. 金管會再次提醒社會大眾投資比特幣等虛擬商品的風險，

2017-12-19，
https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201712190002&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News。

31. 金管會提醒社會大眾有關虛擬資產的相關風險，2021-04-20，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202104200003&dtable=News。
32. 金管會新聞稿（2021/6/10），110 年 4 月份信用卡、現金卡、電子票證及電子支付機構業務資訊，https://www.banking.gov.tw/ch/home.jsp?id=540&parentpath=0,524,539&mcustomize=news_view.jsp&dataserno=202106100005&dtable=News。
33. 金管會新聞稿預告「虛擬通貨平台及交易業務事業防制洗錢及打擊資恐辦法」草案 https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=202105250007&dtable=News。
34. 金管會對「證券型代幣發行(Security Token Offering, STO) 相關規範」之說明，(2019/06/27)，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News。
35. 金管會網站，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201411250002&toolsflag=Y&dtable=News。
36. 金管會銀行局新聞稿，

https://www.banking.gov.tw/ch/home.jsp?id=540&parentpath=0,524,539&mcustomize=。
37. 金融庁，マネー・ローンダリング及びテロ資金供与対策の現状と課題，https://www.fsa.go.jp/news/r1/20191021amlcft/20191021amlcft-1.pdf。
38. 金融新契機－證券型代幣發行(STO)機會與挑戰，https://www2.deloitte.com/tw/tc/pages/risk/articles/finance-sto-challenge.html。
39. 金融監督管理委員會會於 2019 年 6 月 27 日發布新聞稿，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201906270004&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News。
40. 挖礦 (數位貨幣)，維基百科，https://zh.wikipedia.org/wiki/%E6%8C%96%E7%A4%A6_(%E6%95%B8%E4%BD%8D%E8%B2%A8%E5%B9%A3)。
41. 是證券不是幣？美國 SEC 大陣仗起訴瑞波幣母公司！，2020/12/23，TNL Media，https://www.inside.com.tw/article/23783-akamai-gaming-2021。
42. 科技法律研究所，新加坡國會通過支付服務法修正案，以降低洗錢及犯罪風險，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8622。
43. 科技新報（2021/08/06），〈發送實聯制前先注意，詐騙集團偷換 QR Code 讓民眾傳到高額付費電話〉。
44. 范建得、劉嘉彥，檢視加密貨幣（Cryptocurrency）可能涉及之犯罪問題及其規範，https://blpc.site.nthu.edu.tw/p/406-1390-152227,r7141.php?Lang=zh-tw。
45. 剛買瑪莎拉蒂就被捕，桃園警方破獲「比特幣詐騙集團」犯

罪所得近千萬，2020-06-19，動區動趨，https://www.blocktempo.com/another-crypto-fraud-being-caught/。
46. 財團法人聯合信用卡處理中心網站，https://www.nccc.com.tw/wps/wcm/connect/zh/home/BusinessOperations/BusinessIntroduction/AcquiringBusiness。
47. 勒索軟體頻攻擊科技廠 立委籲政府協力防護，2021/4/21，中央社，https://www.cna.com.tw/news/aipl/202104210115.aspx。
48. 區塊客，《支付服務法》正式上路 新加坡金管局：將促進支付領域的成長和創新，並減輕風險，https://blockcast.it/2020/01/30/sg-payment-service-act-come-into-effect/。
49. 參動區，最大龐氏騙局｜150 億詐騙「OneCoin」主謀的弟弟與投資人和解，逃過 90 年監禁，https://www.blocktempo.com/onecoin-cofounder-agreed-on-a-settlement/。
50. 商工行政資料開放平台，公司登記（依營業項目別）——第三方支付服務業，https://data.gcis.nat.gov.tw/od/detail?oid=12EE0DE2-A3C2-4F68-8455-7A9DE040697A。
51. 國家發展委員會：推動行動支付普及，https://www.ndc.gov.tw/Content_List.aspx?n=0338D970952E63EE。
52. 產業情報研究所，【2020 下半年行動支付大調查】六成消費者常用行動支付 比例首度超越電子票證，2021 年 2 月 3 日，https://mic.iii.org.tw/news.aspx?id=593。
53. 設新創板，請踏著 STO 棺材板前進，數位時代，https://www.bnext.com.tw/article/58696/sto-taiwan。
54. 通保法：Line 資料是警察想調就可以調嗎？，法操，自由評

論網，https://talk.ltn.com.tw/article/breakingnews/2907573。
55. 硬塞科技字典，什麼是監管科技，https://www.inside.com.tw/article/7029-what-is-regtech。
56. 虛擬貨幣：主要定義和潛在的 AML / CFT 風險，https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html。
57. 經濟部 / 駐英國台北代表處經濟組，英國金融科技 FinTech 產業報告之監管框架，https://www.trademag.org.tw/page/newsid1/?id=756172&iz=2。
58. 鉅亨網，2020/09/03，日本央行審議委員：須調降利率減輕企業家計利息負擔 抑制通縮壓力，https://news.cnyes.com/news/id/4520576。
59. 幣寶爭議如何解？虛擬通貨投資的三不管地帶，果殼，動區，https://www.blocktempo.com/crypto-exchange-no-mans-land/。
60. 網絡犯罪再進化：勒索軟件被「挖礦綁架」取代，https://www.thenewslens.com/article/115359。
61. 銀行局，金融機構基本資料查詢——電子支付機構，https://www.banking.gov.tw/ch/home.jsp?id=218&parentpath=0,4,60。
62. 數位時代（12/09/2016），〈別以為透過第三方支付購物就保險，刑事局偵九隊宣佈偵破新型態第三方支付詐欺集團，〉https://www.bnext.com.tw/article/42275/new-third-party-payment-fraud-group。
63. 駐英國台北代表處經濟組，駐英經（109）經字第 102/P200 號（商情文號:第 102 號）：英國央行緊急調降利率以抑制新冠病毒帶來的經濟衝擊(2020/03/12)，https://www.trade.gov.tw/Pages/Detail.aspx?nodeid=45&pid=690749。

64. 聯合報（05/11/2020），〈第三方支付管理鬆成詐騙洗錢管道〉。
65. 識破 ICO 騙局，「拒當韭菜」教戰守則，https://www.bnext.com.tw/article/50799/how-to-avoid-ico-scam (last visited: Jun. 21, 2021).
66. 蘋果日報（11/03/2019），〈防手機掃碼支付成詐騙漏洞　金管會設 3 大控管機制〉。
67. 鑫棧虛擬貨幣工作室盜領泰達幣 8 年級首腦涉洗錢遭訴，聯合報，2021-05-26，https://udn.com/news/story/7321/5486640。
68. 一般社団法人日本暗号資産取引業協会（JVCEA） 役員一覧 2021 年 6 月 25 日更新，https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/jvcea-yakuin.pdf。
69. 公視新聞網，「跨國警破獲史上最大暗網交易 逮捕 150 人、截獲美金 3100 萬」，https://news.pts.org.tw/article/551193，最後瀏覽日：2021/11/1。
70. 號角月報-加拿大版，勁毒狠毒芬太尼，https://www.heraldmonthly.ca/newspaper/web/articleView.php?date=201705&id=5235。
71. 香港經濟日報，【中美貿易戰懶人包】，芬太尼是什麼，為何使中美關係緊張，https://inews.hket.com/article/2491803/%E3%80%90%E4%B8%AD%E7%BE%8E%E8%B2%BF%E6%98%93%E6%88%B0%E6%87%B6%E4%BA%BA%E5%8C%85%E3%80%91%E8%8A%AC%E5%A4%AA%E5%B0%BC%E6%98%AF%E7%94%9A%E9%BA%BC%20%E7%82%BA%E4%BD%95%E4%BD%BF%E4%B8%AD%E7%BE%8E%E9%97%9C%E4%BF%82%E7%B7%8A%E5%BC%B5。
72. 聯合新聞網，美暗網非法交易 助長鴉片類藥物濫用，https://udn.com/news/story/6813/5366613。

三、 外文參考文獻

1. ACCESS, ACCESS rolls out Code of Practice to facilitate application of payment service provider licence under Singapore's Payment Services Act, August 13, 2020, https://www.access.org.sg/blogs/press-release/access-rolls-out-code-of-practice-to-facilitate-application-of-payment-service-provider-licence-under-singapore-s-payment-services-act.
2. Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective, 2020 July, European Financial Reporting Advisory Group, p.35-36.
3. ACIP, Industry Perspectives – Adopting Data Analytics Methods for AML/CFT, https://abs.org.sg/docs/library/acip-working-group-paper---data-analytics-for-aml.pdf.
4. Alex Scroxton, Arrests and indictments made in cyber money laundering ring, https://www.computerweekly.com/news/252490604/Arrests-and-indictments-made-in-cyber-money-laundering-ring.
5. Amanda Macias, Christina Wilkie, U.S. recovers $2.3 million in bitcoin paid in the Colonial Pipeline ransom, CNBC.
6. Angel L. Rodriguez Santiago, New Payment Methods and Insufficiencies in Their Regulatory Scheme, 7 J. L. & CYBER WARFARE 101 (2019).
7. Bank for International (2021), FSI On Policy Implementation No 31 Apr, Supervising Crypto Assets For Anti-Money Laundering, https://www.bis.org/fsi/publ/insights31.pdf.
8. Bank for International Settlements, FSI Insights on policy implementation No 9: Innovative technology in financial supervision (suptech) – the experience of early users, https://www.bis.org/fsi/publ/insights9.pdf.

9. Bank of England, What is the Prudential Regulation Authority (PRA)?, https://www.bankofengland.co.uk/knowledgebank/what-is-the-prudential-regulation-authority-pra.
10. Berkshire Wire, Total Identity Fraud Losses Soar to $56 Billion in 2020, https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020.
11. CFATF Secretariat Research Desk, How can Virtual Assets be used for the commission of Financial Crime? March 24, 2021 P.8, https://www.cfatf-gafic.org/home/cfatf-research-corner/15221-aml-cft-101-how-can-virtual-assets-be-used-for-the-commission-of-financial-crime/file.
12. CGMF, National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding, https://www.sif.admin.ch/dam/sif/en/dokumente/Integrit%C3%A4t%20des%20Finanzplatzes/nra-bericht-krypto-assets-und-crowdfunding.pdf.download.pdf/BC-BEKGGT-d.pdf.
13. Chainalysis, Making Cryptocurrency Part of the Solution to Human Trafficking, https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020.
14. CNA, 51 people under investigation for suspected involvement in scams, including 74-year-old: SPF, https://www.channelnewsasia.com/singapore/scams-spf-251-people-under-investigation-money-mules-412266.
15. CNA, New Inter-Ministry Committee to be set up to combat scams, https://www.channelnewsasia.com/singapore/new-inter-ministry-committee-be-set-combat-scams-768621 (last visited:

Aug 24, 2021).

16. Crypto Crime Report—Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019, https://uploads-ssl.webflow.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda_Chainalysis%20January%202019%20Crypto%20Crime%20Report.pdf.
17. Crypto Crime Report—Decoding increasingly sophisticated hacks, darknet markets, and scams January 2019, https://uploads-ssl.webflow.com/5a9360f88433cb00018022c2/5c4f67ee7deb5948e2941fda_Chainalysis%20January%202019%20Crypto%20Crime%20Report.pdf.
18. Cryptocurrency Anti-Money Laundering Report – Q4 2018, https://ciphertrace.com/cryptocurrency-anti-money-laundering-report-q4-2018/.
19. Cryptocurrency Crime and Anti-Money Laundering Report, Feb. 2021, CipherTrace, p7-8, 16, 21.
20. Cryptocurrency Fraud,https://constantinecannon.com/practice/whistleblower/whistleblower-types/financial-investment-fraud/cryptocurrency-fraud/.
21. CryptoUK, https://cryptouk.io/.
22. CryptoUK, https://cryptouk.io/about/.
23. CryptoUK, https://cryptouk.io/codeofconduct/.
24. Department for Digital, Culture, Media & Sport, UK Digital Strategy: 3. The digital sectors - making the UK the best place to start and grow a digital business, https://www.gov.uk/government/publications/uk-digital-strategy/3-the-digital-sectors-making-the-uk-the-best-place-to-

start-and-grow-a-digital-business.
25. Department of Justice, Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside, Jun. 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.
26. Dominic Low, At Least 21 People in Singapore Fall Prey to Transnational Online Credit Card Fraud Syndicate, The Straits Times (July 28, 2020), https://www.straitstimes.com/singapore/courts-crime/at-least-21-people-in-singapore-fall-prey-to-transnational-online-credit-card.
27. Emerging Payments Association, Facing Up to Financial Crime: Analysis of Payments-Related Financial Crime and How to Minimise Its Impact on the UK 14 (2019).
28. ESMA, Advice: Initial Coin Offerings and Crypto-Assets, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
29. Eurojust, €24 million cryptocurrency theft unraveled with Eurojust's support, €24 million cryptocurrency theft unraveled with Eurojust's support | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu)
30. Eurojust, Digital Criminal Justice, https://www.eurojust.europa.eu/judicial-cooperation/judicial-cooperation-instruments/digital-criminal-justice.
31. Eurojust, Eurojust action days: Financial impact of EUR 2 billion and more than 1 700 arrests, https://www.eurojust.europa.eu/eurojust-action-days-financial-impact-eur-2-billion-and-more-1-700-arrests.

32. Eurojust, Eurojust and EPPO sign Working Arrangement to facilitate cooperation, https://www.eurojust.europa.eu/eurojust-and-eppo-sign-working-arrangement-facilitate-cooperation.
33. Eurojust, Italian and Romanian judicial authorities; with Eurojust's support; dismantle major criminal network in financial fraud; cybercrime and money laundering, https://www.eurojust.europa.eu/italian-and-romanian-judicial-authorities-eurojusts-support-dismantle-major-criminal-network
34. Eurojust, Joint investigation teams, https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams.
35. Eurojust, Who we are, https://www.eurojust.europa.eu/about-us/who-we-are.
36. European Commission, Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690
37. Europol l Convention, Article 3.
38. Europol, 20 Arrests in QQAAZZ Multi-million Money Laundering Case, https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case.
39. Europol, 60 E-Commerce Fraudsters Busted During International Operation, https://www.europol.europa.eu/newsroom/news/60-e-commerce-fraudsters-busted-during-international-operation.
40. Europol, EU Policy Cycle – EMPACT, https://www.europol.europa.eu/empact.

41. Europol, European Financial and Economic Crime Centre, https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc.
42. Europol, Online Scammers Captured After Causing EUR 18 Million of Damage in More Than 35000 Cases, https://www.europol.europa.eu/newsroom/news/online-scammers-captured-after-causing-eur-18-million-of-damage-in-more-35-000-cases.
43. Europol, Payment Fraud, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud.
44. Evan Perez, Zachary Cohen & Alex Marquardt, Jun. 8, 2021, First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers, https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html.
45. EverComplaint, White Paper: How to Prevent Transaction Laundering 7 (2018).
46. Exit scammers run off with $660 million in ICO earnings, https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/.
47. FATF Guidance-Private Sector Information Sharing, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/guidance-information-sharing.html?hf=10&b=0&s=desc(fatf_releasedate).
48. FATF(2018), Financial Flows from Human Trafficking, https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf.
49. FATF, Draft updated Guidance for a risk-based approach to

virtual assets and VASPs, https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf.
50. FATF, FATF Guidance-Private Sector Information Sharing, https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/guidance-information-sharing.html?hf=10&b=0&s=desc(fatf_releasedate).
51. FATF, Guidance For A Risk-Based Approach: Money or Value Transfer Services, february 2016.
52. FATF, Guidance For a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services (2013).
53. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html.
54. FATF, International Standards on Combating Money Laundering And The Financing of Terrorism & Proliferation: the FATF Recommendations 125 (June 2021).
55. FATF, Money Laundering Using New Payment Methods 36 (2010).
56. FCA, About the FCA, https://www.fca.org.uk/about/the-fca.
57. FCA, Cryptoassets: AML / CTF regime, https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime.
58. FCA, Dear CEO Cryptoassets And Financial Crime, https://www.fca.org.uk/publication/correspondence/dear-ceo-letter-cryptoassets-financial-crime.pdf.
59. FCA, Digital regulatory reporting, https://www.fca.org.uk/innovation/regtech/digital-regulatory-

reporting.
60. FCA, Guidance on Cryptoassets Feedback and Final Guidance to CP 19/3, https://www.fca.org.uk/publication/policy/ps19-22.pdf.
61. FCA, Payment Service Providers that repeatedly fail to provide information, https://www.fca.org.uk/firms/financial-crime/payment-service-providers-repeatedly-fail-provide-information.
62. FCA, Regulatory sandbox - cohort 6, https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-6.
63. FCA, Turning technology against financial crime, Turning technology against financial crime.
64. FEDERAL BUREAU OF INVESTIGATION, Incidents of Ransomware on the Rise, April 29, 2016, https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise (last visited: Jun. 21, 2021).
65. Fin CEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions，https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering.
66. Financial Technology Law Review Third Edition, https://www.nkf.ch/app/uploads/2020/06/chapter-23-switzerland-may-2020.pdf.
67. Financier Worldwide Magazine, Financial crimes in Singapore – an overview, https://www.financierworldwide.com/financial-crimes-in-singapore-an-overview#.YQ0Z5tQzY2w.
68. FinCEN, Advisory on Illicit Activity Involving Convertible

Virtual Currency, May 9 2019, https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

69. FinCEN, FinCEN Extends Comment Period for Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions, https://www.fincen.gov/news/news-releases/fincen-extends-comment-period-rule-aimed-closing-anti-money-laundering .
70. FinCEN, FinCEN Recognizes Law Enforcement Cases Significantly Impacted by Bank Secrecy Act Filings ,https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act.
71. Finextra, Singapore police force taps OCBC transaction data to fight financial crime, https://www.finextra.com/pressarticle/79162/singapore-police-force-taps-ocbc-transaction-data-to-fight-financial-crime.
72. FINMA, FINMA publishes ICO guidelines, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.
73. Franzheim, Krimimologene Faktoren der Wirtschaftskriminalitat, Kriminalistik,1980,S. 278 ff..
74. Fumiko Kuribayashi, 18.11 Million Yen Stolen from Japan Post Bank in E-pay Scam, The Asahi Shimbun (Sept. 17, 2020), http://www.asahi.com/ajw/articles/13736152.
75. Global AML and Financial Crime TechSprint, https://www.fca.org.uk/events/techsprints/aml-financial-crime-international-techsprint.
76. Government Office of Science, Distributed Ledger Technology：beyond block chain, https://assets.publishing.service.gov.uk/government/uploads/sys

tem/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

77. Government Office of Science, FinTech Futures: The UK as a World Leader in Financial Technologies, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf.
78. H.R.2613 - Advancing Innovation to Assist Law Enforcement Act, https://www.congress.gov/bill/116th-congress/house-bill/2613/text?r=6&s=1.
79. H.R.56 - Financial Technology Protection Act, https://www.congress.gov/bill/116th-congress/house-bill/56/text?r=4&s=1.
80. HM Treasury, A new approach to financial regulation: building a stronger system, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/81411/consult_newfinancial_regulation170211.pdf.
81. HM Treasury, FCA, Bank of England, Cryptoassets Taskforce: fnal report, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.
82. https://buzzorange.com/techorange/2017/05/16/wanna-cry-why-bitcoin/. https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf
83. https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/#:~:text=Altogether%2C%20over%2050%25%20of%20all,hack%20volume%20was%20virtually%20negligible.

84. https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/.
85. https://ciphertrace.com/q3-2018-cryptocurrency-anti-money-laundering-report/.
86. https://hackernoon.com/the-ultimate-list-of-ico-pools-in-the-bear-market-q4-2018-81ffc4df5a9b (last visited: Jun. 21, 2021).
87. https://www.autonomous.com/.
88. https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/.
89. https://www.blocktempo.com/okex-korea-fatf-delisting-5-privacy-coins/.
90. https://www.blocktempo.com/tokeninsight-mining-report2020/ .
91. https://www.bnext.com.tw/article/56330/bitcoin-money-laundering.
92. https://www.congress.gov/bill/116th-congress/house-bill/2613/text?r=6&s=1.
93. https://www.congress.gov/bill/116th-congress/house-bill/56/text?r=4&s=1.
94. https://www.crowdfundinsider.com/wp-content/uploads/2020/10/DOJ-cryptocurrency_white_paper-10.8.20.pdf.
95. https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/approved_entities_number (last visited: Jun. 21, 2021).
96. https://www.fincen.gov/news/news-releases/fincen-holds-fifth-annual-awards-program-recognize-importance-bank-secrecy-act.
97. https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act.

98. https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.
99. https://www.fincen.gov/what-we-do.
100. https://www.inside.com.tw/article/20437-what-would-twitter-hackers-choose-bitcoin-is-there-a-way-for-hackers-to-escape-the-tracking-of-law-enforcement-agencies.
101. https://www.justice.gov/criminal-ccips/file/872771/download (last visited: Jun. 21, 2021).
102. https://www.keyeinfo.com/depth/depth-hot/45248.html .
103. https://www.mas.gov.sg/news/speeches/2021/payment-services-amendment-bill (last visited: Jun. 21, 2021).
104. https://www.secretservice.gov/investigation/cftf/.
105. https://zh.wikipedia.org/wiki/Bitfinex.
106. ILO says forced labour generates annual profits of US$ 150 billion, May 20 2014, https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_243201/lang--en/index.htm.
107. Insight, How the UK Can Deliver its Digital Policing Vision, https://www.uk.insight.com/en-gb/content-and-resources/2020/articles/how-the-uk-can-deliver-its-digital-policing-vision.
108. International Pet and Animal Transportation Association, Beware: Holiday Pet Scams, IPATA (Nov. 9, 2018), https://www.ipata.org/beware-holiday-pet-scams.
109. International Pet and Animal Transportation Association, https://www.ipata.org/pet-scams.
110. International Pet and Animal Transportation Association, https://theconversation.com/how-to-avoid-scams-when-buying-a-pet-online-153138.
111. IOSCO, Model for Effective Regulation, May 2000, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD110.pdf.

112. J.P. Morgan, 2020 AFP Payments Fraud and Control Survey Report: Key Highlights 7 (2020).
113. Jetpets, Beware of Pet Travel Scams, https://www.jetpets.com.au/pet-scams/.
114. Jupiter Research, Online Payment Fraud Whitepaper 2016-2020 11 (2016).
115. Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment, https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads.
116. Laurence Ingle, Why Build a Sandbox on a Beach? An Analysis of Fintech Regulation in New Zealand, April 4, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3156088.
117. MAS, CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes, https://www.mas.gov.sg/news/media-releases/2017/cad-and-mas-partner-industry-stakeholders-to-fight-financial-crimes.
118. MAS, MAS Establishes Payments Council, https://www.mas.gov.sg/news/media-releases/2017/mas-establishes-payments-council.
119. MAS, Warning on Fraudulent Websites Soliciting "Cryptocurrency" Investments,. https://www.mas.gov.sg/news/media-releases/2019/warning-on-fraudulent-websites-soliciting-cryptocurrency-investments.
120. Ministry of Home Affairs, Association of Banks in Singapore Financial Crime Seminar 2021, "Deepening Partnerships to Combat Financial Crime" – Keynote Address by Mr Desmond Tan, Minister of State, Ministry of Home Affairs and Ministry of Sustainability and the Environment,

https://www.mha.gov.sg/mediaroom/speeches/association-of-banks-in-singapore-financial-crime-seminar-2021-deepening-partnerships-to-combat-financial-crime/.

121. MS-ISAC, RANSOMWARE GUIDE,Sep 2020, p.2, https://www.cisa.gov/sites/default/files/publications/CISA_MSSAC_Ransomware%20Guide_S508C.pdf.

122. NCA, Iranian who ran payment platform for cyber criminals arrested in UK, https://www.nationalcrimeagency.gov.uk/news/iranian-who-ran-payment-platform-for-cyber-criminals-arrested-in-uk.

123. NCA, National Economic Crime Centre, https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre.

124. NCA, What we do, https://www.nationalcrimeagency.gov.uk/what-we-do.

125. North Korean Hackers Accused Of 'Biggest Cryptocurrency Theft Of 2020'—Their Heists Are Now Worth $1.75 Billion"，https://www.forbes.com/sites/thomasbrewster/2021/02/09/north-korean-hackers-accused-of-biggest-cryptocurrency-theft-of-2020-their-heists-are-now-worth-175-billion/?sh=65bb54035b0b.

126. NPCC, Apcc, National Policing Digital Strategy: Digital, Data and Technology Strategy 2020–2030, https://www.apccs.police.uk/media/4886/national-policing-digital-strategy-2020-2030.pdf.

127. Owen, G., & Savage, N.(2015). The Tor Dark Net. Centre for International Governance Innovation.

128. Pablo Iglesias Rodríguez, Towards a New European Financial Supervision Architecture, 16 COLUM. J. EUR. L. ONLINE 1, 3 (2009).

129. Plus Token (PLUS) Scam – Anatomy of a Ponzi, https://boxmining.com/plus-token-ponzi/.
130. PwC, January 2020, 6th Edition ICO/STO report- A Strategic Perspective. https://www.pwc.ch/en/publications/2020/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf.
131. Q2 2018 Cryptocurrency Anti-Money Laundering Report.
132. Q3 2019 Cryptocurrency Anti-Money Laundering Report, https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/.
133. QR Codes Too Easily Misused by Criminals, China Daily (March 2, 2017), http://www.chinadaily.com.cn/opinion/2017-03/02/content_28400890.htm.
134. Rachel Wolfson, Coinbase, Gemini and others join forces to combat human trafficking, Nov. 03, 2020, https://cointelegraph.com/news/coinbase-gemini-and-others-join-forces-to-combat-human-trafficking.
135. Robleh Ali, John Barrdear, Roger Clews and James Southgate, "The economics of digital currencies,"of 2014 Q3, p. 276. Available at: https://www.bankofengland.co.uk/-/media/boe/ files/digital-currencies/the-economics-of-digital-currencies.
136. Security Boulevard, QRL Jacking, https://securityboulevard.com/2018/07/qrl-jacking/.
137. EBA, Crypto-assets: ESAs remind consumers about risks, https://www.eba.europa.eu/financial-innovation-and-fintech/publications-on-financial-innovation/crypto-assets-esas-remind-consumers-about-risks.
138. EPPO, Mission and tasks. https://www.eppo.europa.eu/en/mission-and-tasks.
139. Simmons & Simmons, https://www.simmons-simmons.com/en/publications/ck0bbibrqepe40b59a0g15p8n/100118-esma-and-eba-publications-on-crypto-assets.

140. Singapore Police Force, Man to be Charged For Providing Payment Services Without License Under The Payment Services Act 2019, https://www.police.gov.sg/Media-Room/News/20201105_man_charged_for_providing_payment_servc_wo_licence_under_payment_servc_act_2019.

141. Singapore Police Force, Suspicious Transaction Reporting Office (STRO), https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office.

142. Singapore Police Force, Two Men Charged For Promoting a Multi-level Marketing Scheme Involving Cryptocurrency (ONECOIN), https://www.police.gov.sg/media-room/news/20190410_arrest_two_men_charged_for_promoting_a_mlm_cad.

143. South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin, https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child.

144. The 2021 Crypto Crime Report, Chainanalysis, 2021.2.16, p. 6, https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.

145. The Seven Types of E-commerce Fraud Explained, Information Age (Nov.25, 2019), https://www.information-age.com/seven-types-e-commerce-fraud-explained-123461276.

146. The Strait Times, 17 organisations, 114 people get awards from Commercial Affairs Department for thwarting scams, https://www.straitstimes.com/singapore/courts-crime/17-organisations-114-people-get-awards-from-commercial-affairs-

department-fo.

147. The Strait Times, S'pore police played 'critical role' in Interpol's online financial crime probe; $110m intercepted, https://www.straitstimes.com/singapore/spore-police-played-critical-role-in-interpol-probe-into-online-financial-crimes-us83m.

148. Tookitaki, What is Credit Card Money Laundering and its Schemes?, https://www.tookitaki.ai/compliance_hub/what-is-credit-card-money-laundering-and-its-schemes/.

149. Toronto Centre, FinTech, RegTech and SupTech: What They Mean for Financial Supervision, https://res.torontocentre.org/guidedocs/FinTech%20RegTech%20and%20SupTech%20-%20What%20They%20Mean%20for%20Financial%20Supervision%20FINAL.pdf.

150. U.S. Department of Justice, Cryptocurrency Enforcement Framework, https://www.crowdfundinsider.com/wp-content/uploads/2020/10/DOJ-cryptocurrency_white_paper-10.8.20.pdf.

151. U.S. SEC, Executives Settle ICO Scam Charges, https://www.sec.gov/news/press-release/2018-280.

152. U.S. Secret Service Media Relations, Secret Service Announces the Creation of the Cyber Fraud Task Force, 2020-07-09, https://www.secretservice.gov/newsroom/releases/2020/07/secret-service-announces-creation-cyber-fraud-task-force.

153. U.S.Secret Service Office Of Investigations, Office Of Investigations Strategy Fy2021–2027, https://www.secretservice.gov/sites/default/files/reports/2021-01/inv-strategy-fy21-27.pdf.

154. UCSF Pays $1.14M After NetWalker Ransomware Attack, https://threatpost.com/ucsf-pays-1-14m-after-netwalker-ransomware-attack/157015/
155. UK Finance, FRAUD - THE FACTS 2021, 13 https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf.
156. UK Parliament, AI in policing and security, https://post.parliament.uk/ai-in-policing-and-security/.
157. United States Secret Service, Field Offices, https://www.secretservice.gov/investigation/cftf/.
158. UNSGSA Annual Report to The Secretary-General, September, 2013, https://www.unsgsa.org/sites/default/files/resources-files/2020-09/2013_09_04_F_UNSGSA2013_lowres.pdf.
159. USA.gov, What We Do https://www.fincen.gov/what-we-do.
160. Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF) , https://www.vqf.ch/en/vqf/services.
161. Vincent Fong, With Mobile Payments on the Rise, Creator of QR Codes Thinks It Needs a Security Revamp, FinTech Singapore (Sept. 12, 2019), https://fintechnews.sg/33563/security/qr-payment-security-inventor-masahiro-hara/.
162. Warwick Ashford, WannaCry a signal moment, says NCA, ComputerWeekly.com, https://www.computerweekly.com/news/450421936/WannaCry-a-signal-moment-says-NCA.
163. Yelowitz, A., & Wilson, M. (2015), Characteristics of Bitcoin users: an analysis of Google search data. Applied Economics Letters, 22(13), 1030-1036.