專論

新興金融科技遭濫用於犯罪之研究

林繼恆*、楊岳平**、李鎧如***

要　目

DOI：10.6460/CPCP.202112_(30).04

* 恆業法律事務所主持律師，國立政治大學法律研究所博士。
** 國立臺灣大學法律學院副教授，美國哈佛大學法學博士。
*** 恆業法律事務所銀行暨資本市場部主任，美國紐約大學法學院法學碩士。

此外本研究之完成感謝林紘宇律師、洪振騰研究員、謝佳縈律師、簡佑霖律師、鄭淵仲律師、侯少鈞實習律師之大力協助。

摘　要

一、新興金融科技加速支付服務之發展，促使人類的消費或投資經常利用各式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密碼學技術的加持，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，進而本身也規劃中央銀行數位貨幣（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。

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。

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」因屬有價證券而受證券交易法規範，以及洗錢防制法規範外，對於虛擬通貨交易並無其他明文規範，金融監督管理委員會遂以新聞稿方式提醒大眾投資虛擬通貨之風險。本研究團隊透過法院案例分析出虛擬通貨之六大犯罪類型：交易標的型、交付個人資料型、交付虛擬通貨帳戶型、支付工具型、不法所得洗錢型與挖礦竊電型，且發現案件數量持續成長中。

四、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。

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

Research on the Criminality of Fintech Abuse

Ji-Heng Lin* & Yueh-Ping Yang** & Kai-Ju Lee***

Abstract

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' 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 deep impacts on modern ways of payment, and the impact is wider and faster.

Electronic payment instruments, including electronic payments and third-party payments, have five general characteristics, namely, anonymity, speed, difficult tracking, non-

* Managing Partner of Lin and Partners; College of Law, National Chengchi University, Doctor in Law, Taiwan.
** Association Professor of College of Law, National Taiwan University; Doctor in Law, Harvard Law School.
*** Director, Banking and Capital Markets Department, Lin and Partners; New York University School of Law, Master of Laws.

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.

Cryptocurrency itself also witnesses high price fluctuation, resulting in a relatively high investment risk. In addition, in recent years, some fraud cases often collect public money in the name of blockchain and/or cryptocurrency. However, except for Security Token, which is a security regulated by the 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 the potential risks of cryptocurrency investment. In this study, we analyzed all the related court judgements and summarized six major types of crimes related to cryptocurrency, including cryptocurrency as a

medium for transaction, delivey of personal data, delivery of cryptocurrency account, payment instrument, money laundering of illicit income, and theft of electricity for mining. The case number is still growing.

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. This research proposes that investigation authorities may establish communications with competent authorities and report to the latter the businesses that fail to implement AML obligations as observed during the investigation. Based on this information, competent authorities may set the priority businesses for inspection to implement the risk-based approach supervision. Besides, the investigation authorities may further establish a FinTech criminal database that collects investigation data for the analysis of FinTech-related crime. Through the assistance of technology, investigation authorities, with limited supervisory resources, can more comprehensively and timely supervise this complex system and identify the priority businesses for enhanced supervision. 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.

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

壹、研究背景

新興金融科技加速支付服務之發展，促使人類的消費或投資經常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密碼學技術的加持，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，進而本身也規劃中央銀行數位貨幣（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。就「電子支付工具」而言，本研究採較廣義的意義，指涉電子支付機構管理條例第4條第1項各款業務，又可包含狹義的電子支付與第三方支付二種類別，以下分別介紹其定義：

一、狹義的電子支付

狹義的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[1]。目前國內計有5家專營電子支付機構、4家舊法下的電子票證機構及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20億元[2]。常見如：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。

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，合先敘明：

(一)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[3]。常見如：

---

1 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。

2 行政院110年8月18日院臺法字第1100181600號函；金管會，電子支付機構及第三方支付服務業之異同，2015年7月2日，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5條第2項授權規定事項辦法第3條。

3 金管會，行動支付與電子化支付普及之關鍵，臺灣經濟論衡，16卷2期，2018年6月，頁29-30。

Google Pay、Apple Pay、Samsung Pay以及台灣Pay。

(二)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[4]。常見如：台灣Pay「金融卡雲支付」。

(三)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。

三、虛擬通貨

就虛擬通貨而言，本研究所稱的「虛擬通貨」，依我國法下之定義，係指「運用密碼學及分散式帳本技術或其他類似技術，表彰得以數位方式儲存、交換或移轉之價值，且用於支付或投資目的者。」[5]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[6]、涉犯

---

4 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。

5 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。」

6 Lee Michael，剛買瑪莎拉蒂就被捕，桃園警方破獲「比特幣詐騙集

洗錢防制[7]、違反證券交易法[8]或非法吸金[9]等經濟犯罪之案件。依其性質可分為：

(一)支付型代幣

僅單純作為支付用，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。

團」犯罪所得近千萬，2020年6月19日，動區動趨，https://www.blocktempo.com/another-crypto-fraud-being-caught/（最後瀏覽日：2021年6月16日）。

7 張宏業，鑫棧虛擬貨幣工作室盜領泰達幣　8年級首腦涉洗錢遭訴，2021年5月26日，聯合新聞網，https://udn.com/news/story/7321/5486640（最後瀏覽日：2021年6月16日）。

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

9 林欣儀，Q點虛擬貨幣　吸金2.5億9人起訴，2021年4月24日，中時新聞網，https://www.chinatimes.com/newspapers/20210424000443-260106?chdtv（最後瀏覽日：2021年6月16日）。

貳、執法機構查緝新興金融科技相關犯罪之困難

一、電子支付工具相關犯罪之特性

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，已受到包括防制洗錢金融行動工作組織（The Financial Action Task Force，下稱「FATF」）與國際學術研究文獻的重視。本研究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均涉及利用所謂「虛擬帳號」（或稱「虛擬帳戶」）[10]，例如臺北地方法院109年易字

[10] 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

第783號刑事判決、臺北地方法院107年審簡字第643號刑事判決、臺中地方法院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。

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，買方匯入虛擬帳戶的金額才會轉入賣方的實體帳戶；然而由於申設虛擬帳戶實務上僅需身分證字號與實體帳戶等個資即可完成，相對方便容易，故我國犯罪實務上常見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。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，因而具有一定程度的相對匿名性，檢調機關縱使最終追溯到虛擬帳號創建者的真實身分，仍已花費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

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://www.tpp.moj.gov.tw/media/63288/4561672171.pdf?mediaDL=true（最後瀏覽日：2021年8月13日）。

於當次線上交易結束後即失效[11]，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，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得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，需經過進一步調查後方可發現虛擬帳戶持有人的身分，容易造成警方追查犯罪上的延宕與困難。

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。

11 同前註。

(二)多層化特性

電子支付工具的特色之一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。以電子支付與第三方支付為例，用戶申請創建其支付帳戶時，通常會綁定其既有的銀行實體帳戶，而該支付業者本身於銀行亦需設立專戶，因此形成「付款人銀行→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。

支付業者中介金流的直接效果是付款人的銀行與受款人的銀行均僅與支付業者辦理金流，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紀錄勾勒出金流全貌，而必須仰賴扮演中介功能的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電子支付業者合作，因此形成更複雜的支付關係。例如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[12]。於此種情形，電子支

[12] 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

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，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。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

覽日：2021年8月18日）；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年8月18日）。

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，例如臺東地方法院108年原金訴字第47號刑事判決的案件即橫跨2018年至2019年、臺中地方法院108年簡上字第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布可知，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

電子支付工具係仰賴網路系統提供支付服務，故支付機構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，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。

例如竊用他人身分資訊並利用支付平台消費的情形，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扮演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[13]，從而不易辨識消費者實際上並非信用卡持卡人或支付帳戶持有人，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號，犯罪人再將此賣家提供的虛擬帳號傳給被害人指示付款至該虛擬帳號，但犯罪人於取得自己購入的商品後並未出貨給被害人，如此實質上即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

13 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年8月13日）。

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[14]。

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，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

14 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，遊戲點數詐騙，2015年5月6日，https://www.zhonghe.police.ntpc.gov.tw/cp-2450-11749-13.html（最後瀏覽日：2021年8月13日）。

跨境偵查的挑戰。

本研究之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，涉及跨境犯罪者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。由此可知，電子支付工具於我國用於跨境犯罪的案件金額相對龐大，且多為持續一段期間的長期犯罪，所牽涉之境外國家或地區主要為中國大陸，但亦有其他國家例如泰國或韓國，故犯罪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。

二、虛擬通貨相關犯罪之特性

虛擬通貨亦可作為一種數位支付工具，利用區塊鏈網路提供同等支付服務，故虛擬通貨相關犯罪亦可能存在前述五大犯罪特性，且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）[15]等匿名網路，逐漸受到重視，許多非法網站亦開始蓬勃發展。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，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[16]。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。

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）[17]與網路殭屍病毒，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

---

15 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。

16 黃彥鈞，2018 暗網比特幣交易量翻倍，平均每天200萬美元，科技新報，2019年1月22日，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）。

17 https://www.itread01.com/content/1545928942.html（最後瀏覽日：2021年6月7日）。

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資助非法活動，因為此將使查緝更為容易。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。

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[18]。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[19]，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。

---

18 「門羅、DASH、ZEC…」不符合FATF反洗錢方針，OKEx韓國下架「5種隱私幣」，2019年9月17日，BLOCKTEMPO，https://www.Blocktempo.com/okex-korea-fatf-delisting-5-privacy-coins/（最後瀏覽日：2021年6月7日）。

19 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，2018年，頁95。

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，不法份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107年度金上訴字第83號刑事判決）；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。

(二)虛擬通貨之不法所得流向難以掌握

近年因虛擬通貨之跨國交易盛行，且同樣具備前述五大特點，導致不法犯罪份子有利用虛擬通貨遂行洗錢，並且易遭犯罪者利用以規避追查，從典型洗錢行為三階段加以分析，虛擬通貨符合洗錢行為的脈絡，可透過非法資金（處置placement）移轉到其他虛擬通貨錢包地址（層析layering），最終轉移至其他虛擬通貨交易平台或業者購買其他服務、商品甚至法幣（整合

integration），完成洗錢行為，上述多層虛擬通貨之幣流流向通常極為複雜，導致執法機構對於犯罪不法所得流向難以掌握。

然而虛擬貨幣也並不如想像中如此無法可管、無所遁形，原因在於虛擬通貨雖具匿名性（開設虛擬通貨錢包並無實名制要求），然而其另一特點因為所有交易紀錄均記載於區塊鏈分散式帳本中，故具備交易流程之「透明性」，此特性也成為查緝洗錢犯罪及偵查的契機。

我國洗錢防制法於2018年11月7日公布修正法案，依同法第5條第2項規定，虛擬通貨平台及交易業務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。另以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2018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2021年4月7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2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），及非屬於我國洗錢防制法體系下，容有產生洗錢防制體系漏洞之可能，經本研究團隊進行焦點座談瞭解相關虛擬通貨偵查實務，相關金融科技犯罪之不法所得，確有透過上述漏洞進行洗錢或移出不法所得至人頭帳戶，完成不法所得之藏匿，且因現行偵查工具之欠缺，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7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[20]；FATF並於2021年3月發布虛擬通貨業者洗錢防制指引草案[21]（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[22]。FATF發布上述FATF指引草案後（包括Travel Rule），由於對現有

---

20 FATF, *12-month Review Virtual Assets and VASPs*, FATF (June 2020), http://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.])

21 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 (last visited: Oct. 13, 2021).

22 *Id*.

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[23]，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[24]，包括我國本辦法第18條規定：「除第七條由本會

---

23 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 (Apr. 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 (last visited: Oct, 13, 2021).

24 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

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（並未在臺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。

參、電子支付工具犯罪之類型化分析

一、國際發展趨勢分析

經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，本研究發現電子支付工具涉及的犯罪類型主要為詐騙與洗錢[25]，以下簡介之。

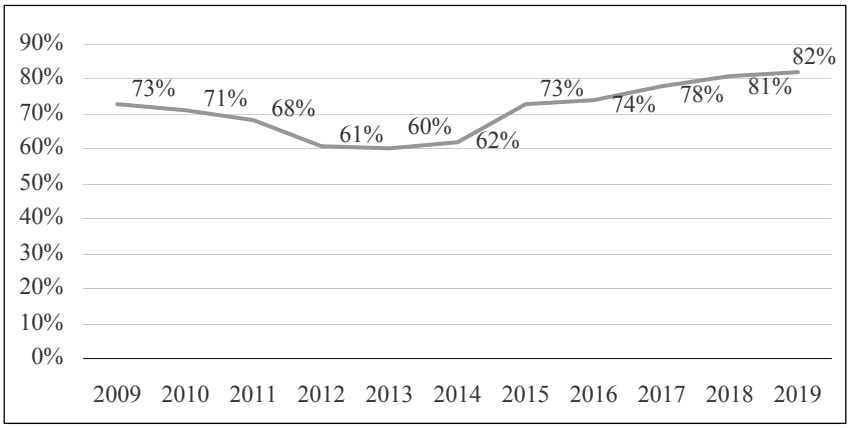
詐騙活動向來是國際商務活動中面臨的主要犯罪類型之一。根據Association for Financial Professionals（AFP）於2020年的研究顯示，B2B交易活動中的詐騙數量在過去五年有明顯的增長，如以下圖1所示，至2018與2019年，已有超過80%的受調查機構表示其曾遭遇詐騙。

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）。

25 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).

圖1

國際商務機構受詐騙的比率（2009~2019）

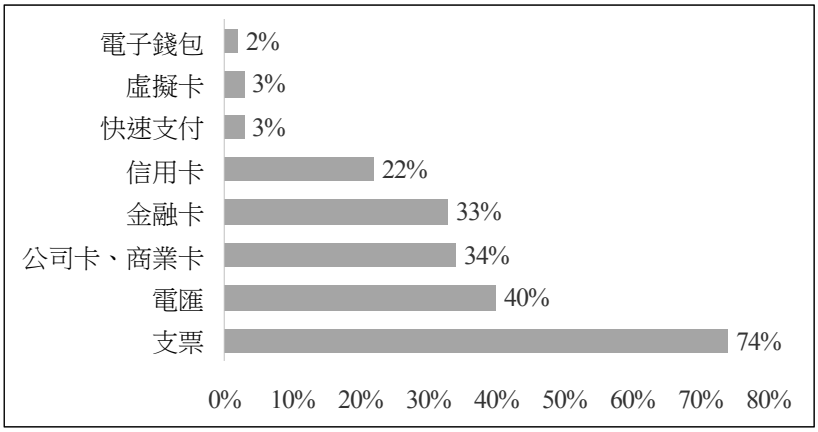


註：2020 AFP Payments Fraud and Control Survey Report: Key Highlights[26]

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2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。

26 *Id*. at 7.

圖2
國際商務機構受詐騙的支付形式（2019）



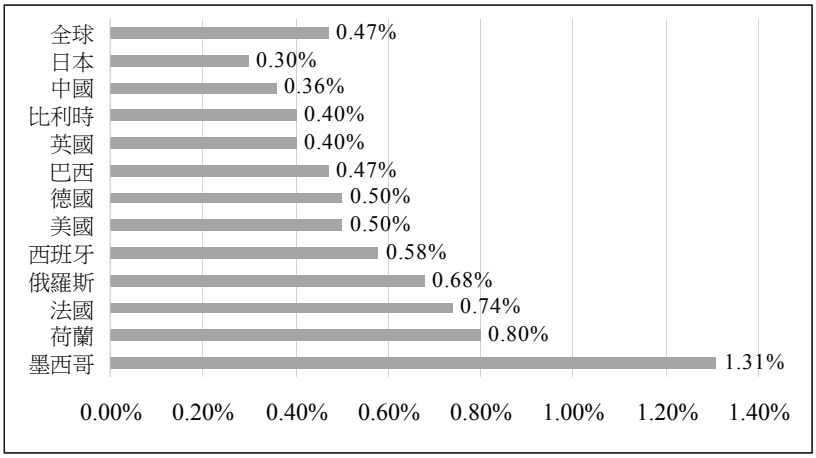
註：2020 AFP Payments Fraud and Control Survey Report: Key Highlights[27]

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占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3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%）。

27 *Id*. at 8.

圖3

主要國家線上支付詐騙率



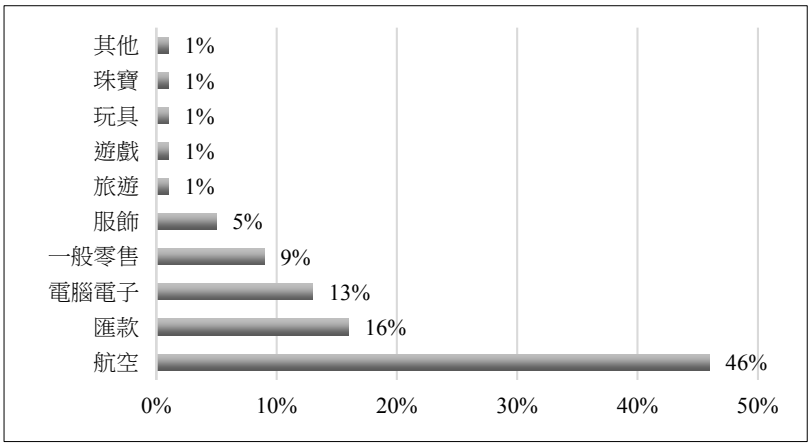
註：Online Payment Fraud Whitepaper 2016-2020[28]

如以產業而言，線上支付詐騙相對集中於若干特定產業。以詐騙交易數量占總體交易數量為基礎，如以下圖4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。

28 Jupiter Research, *Online Payment Fraud Whitepaper 2016-2020*, Experian (Apr. 26, 2021), https://www.experian.com/decision-analytics/identity-and-fraud/juniper-online-fraud-whitepaper (last visited: Oct. 13, 2021).

圖4

主要產業線上支付詐騙交易比例



註：Online Payment Fraud Whitepaper 2016-2020[29]

二、國內支付工具涉及犯罪之統計結果

本研究以司法院之裁判書查詢系統為基礎，使用關鍵字：「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2014年至2021年7月29日間之地方法院刑

[29] *Id*. at 10.

事判決，初步蒐得2,070筆結果。經篩選與支付工具用於犯罪無關之判決後，最終獲得與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，初步觀察得出支付工具於我國主要使用於以下五種犯罪類型，分別為：

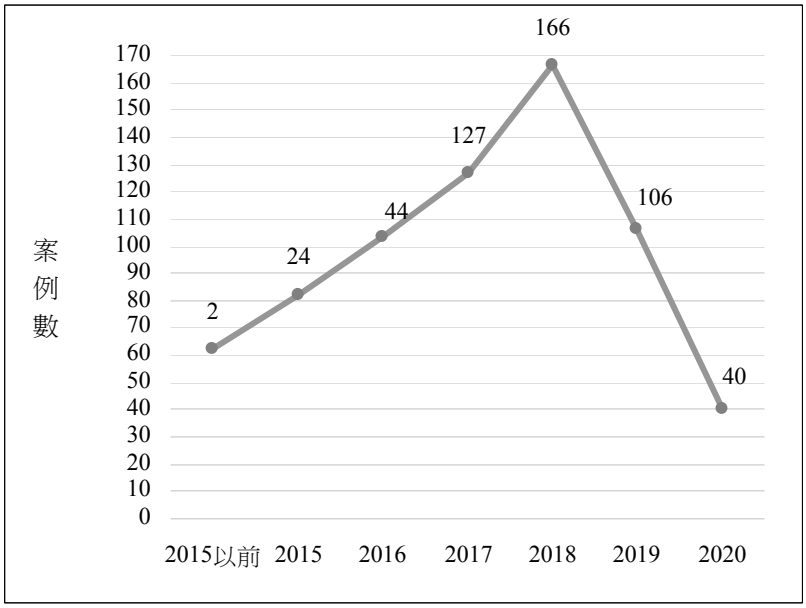
(一)利用支付工具遂行詐騙

本種犯罪之手法多係犯罪集團利用人頭自願提供之資訊，向電子支付業者或第三方支付業者等業者申請設立，或犯罪行為人自有之帳戶，再對被害人施以詐術，使被害人透過超商代收交付款項以遂行詐騙。以下圖5顯示此類犯罪的犯罪行為時點趨勢，至2018年為止均呈現逐年成長之態勢[30]。

30 此處及後續之相類圖表中，為如實反映時間及行為趨勢，故所採取的認定基礎會以自然意義下之一行為作為劃分。因而，可能會出現因為單一案件中有複數行為而有複數時點，導致總行為數與總件數不符之結果，合先敘明。

圖5

支付工具詐騙案件之犯罪行爲時點分布



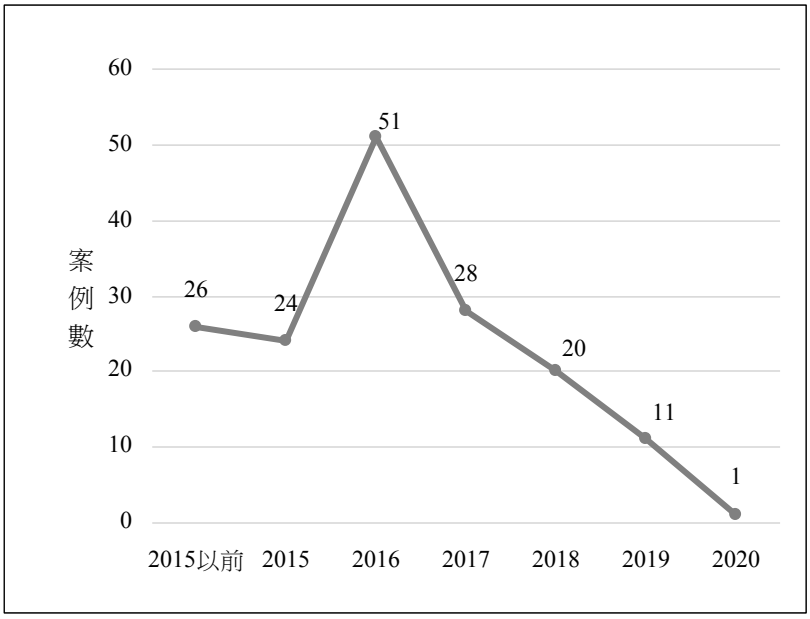
註：研究團隊自製。

(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6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6

網路賭博儲值案件之犯罪行爲時點分布



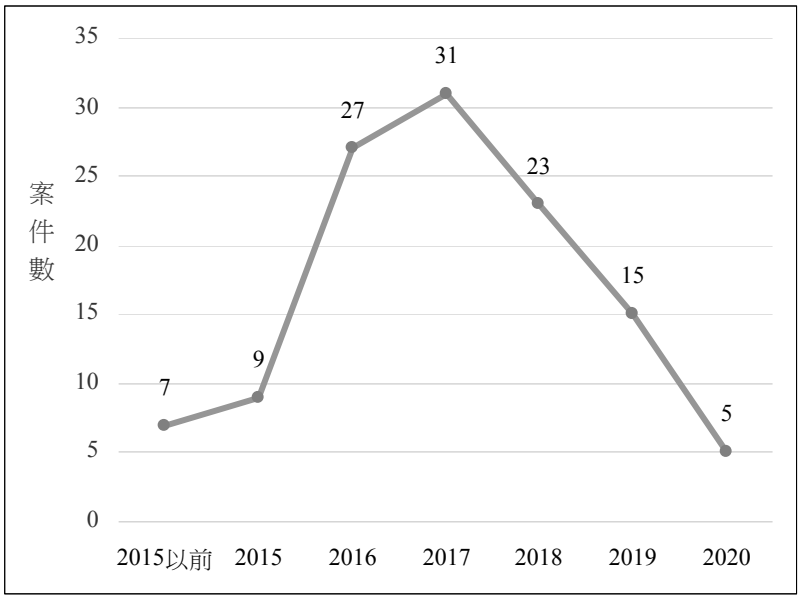
註：研究團隊自製。

(三)竊用他人信用卡或支付帳戶資訊消費

此種犯罪主要以信用卡或支付帳戶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、金融卡或數位帳戶之資訊後，持之於線上透過線上商家提供的支付工具金流服務進行消費。故此種犯罪下，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、支付服務提供者、消費商家、犯罪行為人及被害人。

以下圖7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年至2018年。

圖7
竊用他人資訊消費之犯罪行爲時間點分布



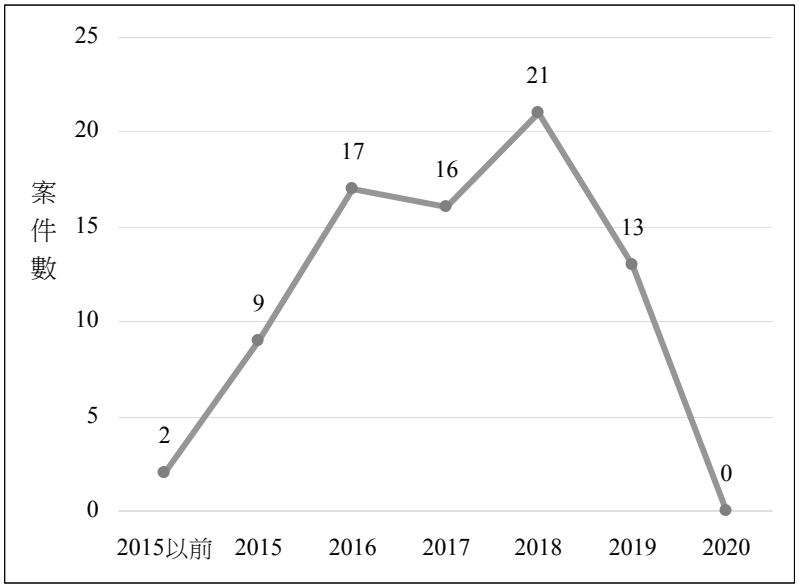
註：研究團隊自製。

(四)盜用他人資訊設定支付帳戶

此種犯罪中，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支付帳戶，並據以進行消費或詐欺等行為。以下圖8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年至2018年。

圖8

盜用他人資訊設定支付帳戶之犯罪行爲時間點分布



註：研究團隊自製。

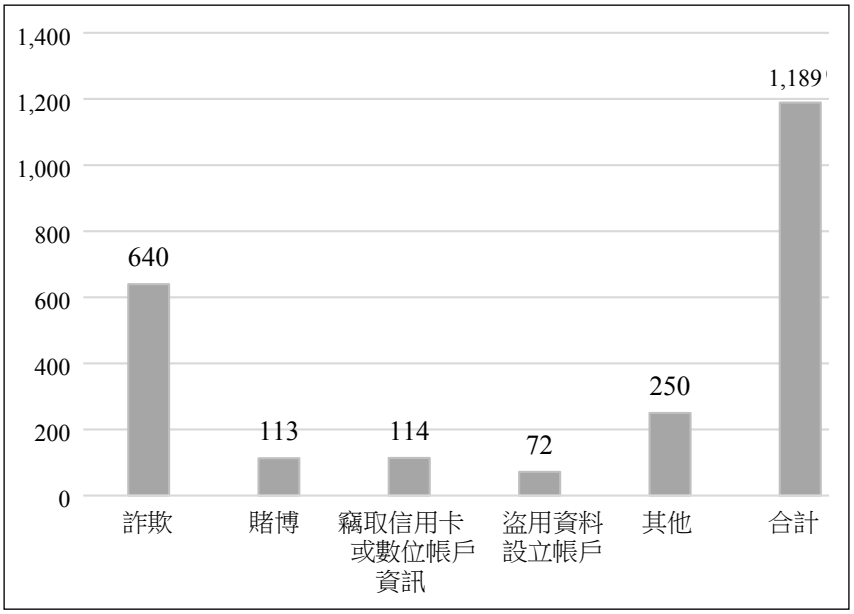
(五)其他犯罪

除上述四種常見的犯罪類型外，本研究亦摘錄部分數量較少但具有一定代表特殊性之犯罪類型供參考，包括違法辦理國內外匯兌、違法經營多層次傳銷、違法經營期貨顧問業等。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，而支付工具的特性或有助此類犯罪的規模擴大與成本降低。綜上，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9[31]所示。相關犯罪類型中，詐騙案件所占比例最高，於本研究蒐集之判決中所記載所占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%）、竊取他人信用卡或數位帳戶資訊消費共114件（約9.5%）、盜用他人資訊設定支付帳戶共72件（約6%）、其他共250件（約21.2%）。

圖9

支付工具涉及犯罪案件類型分布



註：研究團隊自製。

31 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。

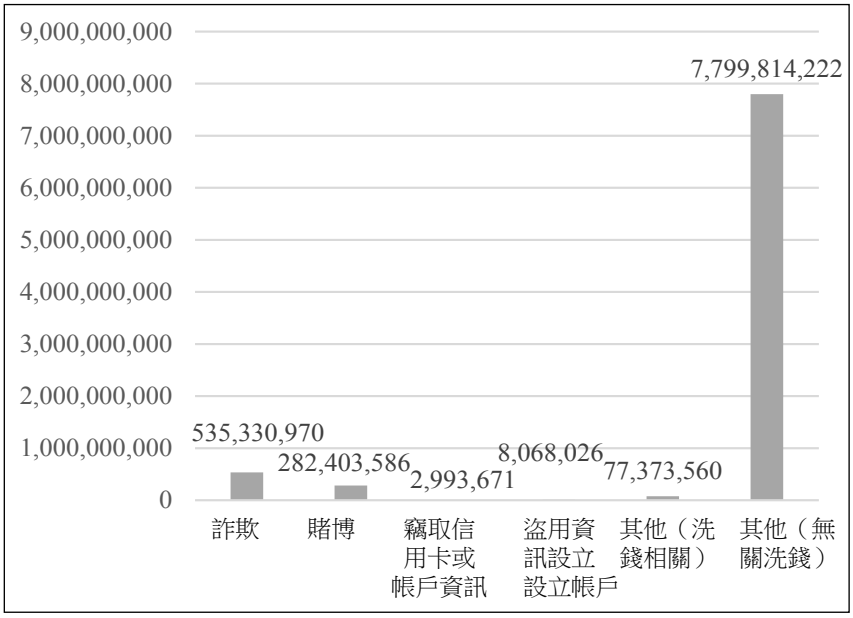
不同支付工具當中，第三方支付與電子支付最常被使用於犯罪，其中常見涉案之支付業者包括綠界（共235件）、歐付寶（共214件）、藍新（共172件）、支付寶（共158件）、紅陽（共54件）等。此外，所蒐得之案件中，共有947件屬於本土為主之案件，約占判決總數之87.8%，涉外案件比例則約為12.2%。於涉外案件中，涉及中國大陸之案件數量最多，共124件，其中多為詐騙集團與違法經營國內外匯兌之案件為主，而所使用之支付工具則多為支付寶。

最後就犯罪金額而言[32]，圖10顯示各類支付工具涉及犯罪的犯罪金額統計。由此圖可知，其他類型案件當中不涉及洗錢罪者雖然數量較少，但涉案金額相當可觀，涉及逾77億元之犯罪金額；相對而言，案件數占比達53.9%的詐騙案件，犯罪總金額約5億3,000萬元的犯罪金額，顯見詐騙案件有數量龐大、但平均每件犯罪金額偏低的特性。

[32] 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10

支付工具涉及犯罪的犯罪金額分布



註：研究團隊自製。

三、小　結

透過上述司法判決實證研究，本研究發現詐欺案件中之詐騙集團多以人頭申請支付帳戶，此外犯罪行為人盜用他人身分或其他資訊創建支付服務帳戶的案件占比亦相當可觀，足見當前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。前開結果將導致面對相關財產犯罪之金流追查困難，並且因為帳戶之申設成本較低，亦可能對犯罪產生相當程度之吸引力。本研究

於後續章節將對此提出相關之政策研究及建議，以期得降低相關犯罪之發生可能。

除詐騙案件外，本研究亦發現，支付工具運用於若干非法金融活動與線上賭博之犯罪金額相較於他犯罪為高，初步推測係與支付工具之「快速性」與「跨境性」之特徵有關，上述特性有助犯罪業者快速且跨境地收取款項，進而有助業者擴大其線上賭博業務範圍至不限於特定地區之人民參與。

最後補充者為，本研究認知到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之限制。

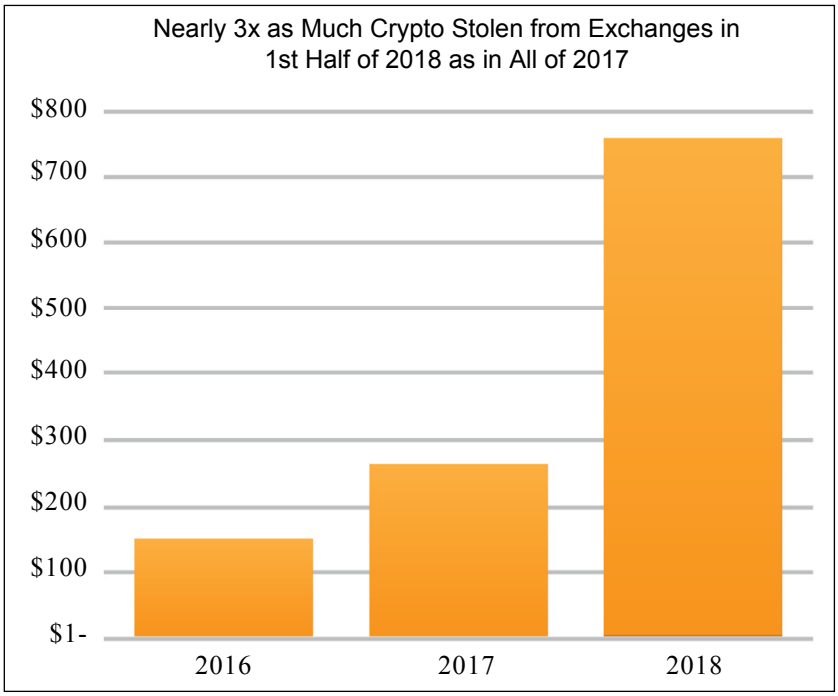
肆、虛擬通貨犯罪之類型化分析

一、國際發展趨勢分析

(一)近年來像比特幣這樣的虛擬通貨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，少數犯罪份子就從虛擬通貨交易所中賺取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。

圖11

2016年至2018年交易所遭盜取之虛擬通貨價值



註：Q2 2018 Cryptocurrency Anti-Money Laundering Report[33]。

(二)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[34]，相比

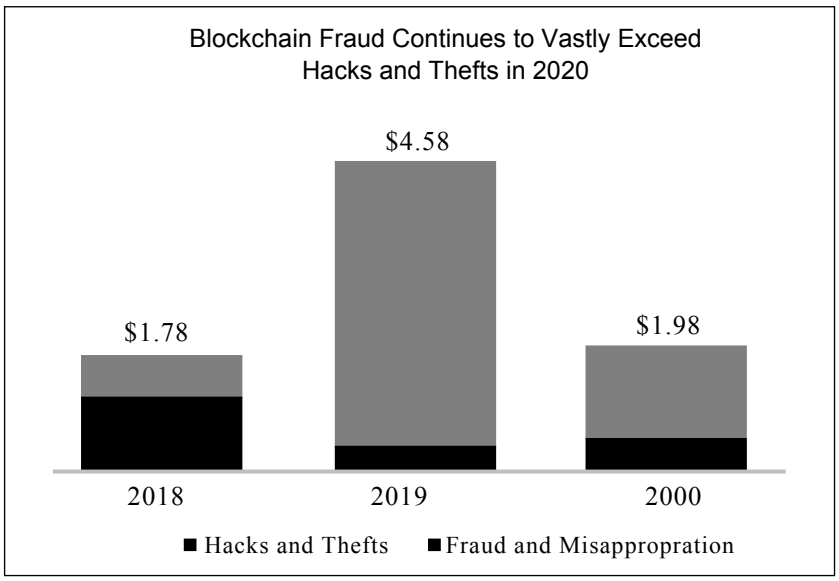
[33] Q2 2018 Cryptocurrency Anti-Money Laundering Report, https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/ (last visited: Oct. 13, 2021).

[34] CIPHERTRACE, *Cryptocurrency Crime and Anti-Money Laundering*

2019年的45億美元卻有顯著的下降。

圖12

2018年至2020年虛擬通貨詐欺與駭客攻擊趨勢



註：Cryptocurrency Crime and Anti-Money Laundering Report, February 2021[35]。

(三)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

*Repor*t (Feb. 2021), CipherTrace, https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/ (last visited: Mar. 5, 2021).

35 *Id*.

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畫，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%。

(四)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[36]。

(五)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[37]，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，虛擬通貨因具有「匿名性」、「經濟價

36 *Id*. at 7.
37 *Id*. at 8.

值載體」及「各國針對虛擬通貨監管法令不健全」等特點，已成為洗錢的溫床，以及部分不法份子手中利用之工具[38]，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。

二、國內虛擬通貨涉及犯罪之統計結果

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[39]，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，可初步可歸納為

38 王心婕，以毒攻毒？虛擬貨幣與反洗錢的棋逢敵手，數位時代，2020年1月29日，https://www.bnext.com.tw/article/56330/bitcoin-money-laundering（最後瀏覽日：2021年2月26日）。

39 目前我國法院判決絕大多數並未針對「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。」之「虛擬通貨」，與其他具有財產價值但並未利用密碼學或分散式帳本技術之虛擬財物（例如：8591虛擬寶物、天堂幣、遊戲鑽石等網路遊戲儲值點數）予以嚴格區分，而係均以「虛擬貨幣」統稱之。本文以下判決統計為凸顯犯罪之趨勢變化故亦包含非利用密碼學或分散式帳本技術者，並配合法院用語均以「虛擬貨幣」統稱之；惟若以下分析內容以「虛擬通貨」描述者，則係指符合上述金管會及FATF所定義之虛擬通貨者而言。

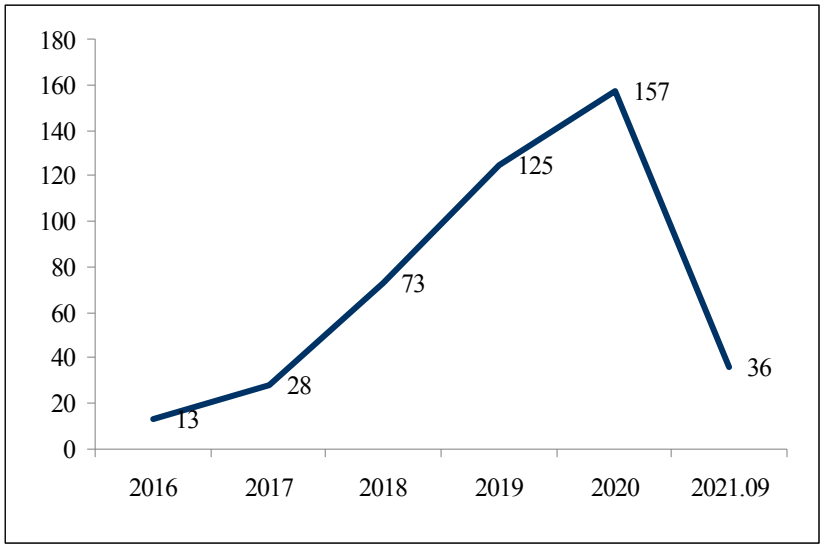
以下六大犯罪類型：

(一)交易標的型

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。此類案件於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13

歷年交易標的型案件數量趨勢圖



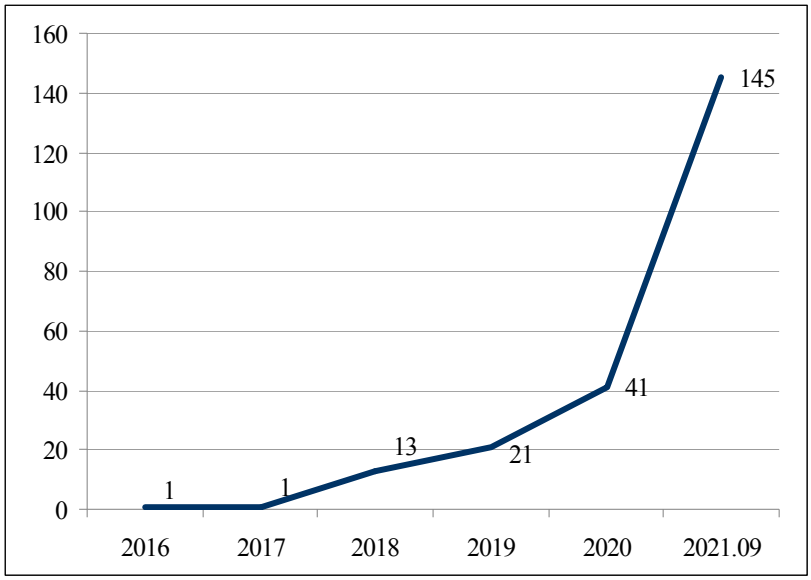
註：研究團隊自製。

(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14

歷年交付個人資料型案件數量趨勢圖

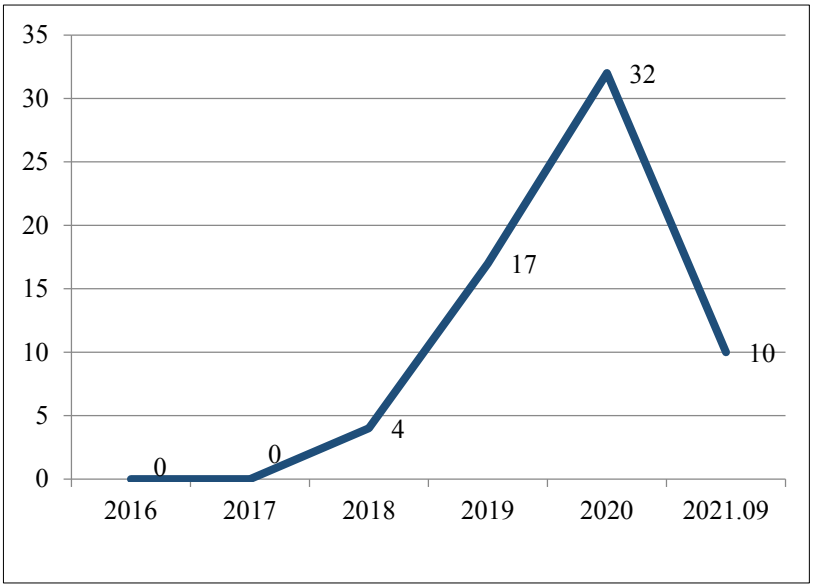


註：研究團隊自製。

(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者，為新興之犯罪類型。此類案件於2018年之前不曾有過，於2018年開始出現，近年並快速成長。此類總計案件數量63件，占所有案件數量之8%。

圖15
歷年交付虛擬通貨帳號型案件數量趨勢圖



註：研究團隊自製。

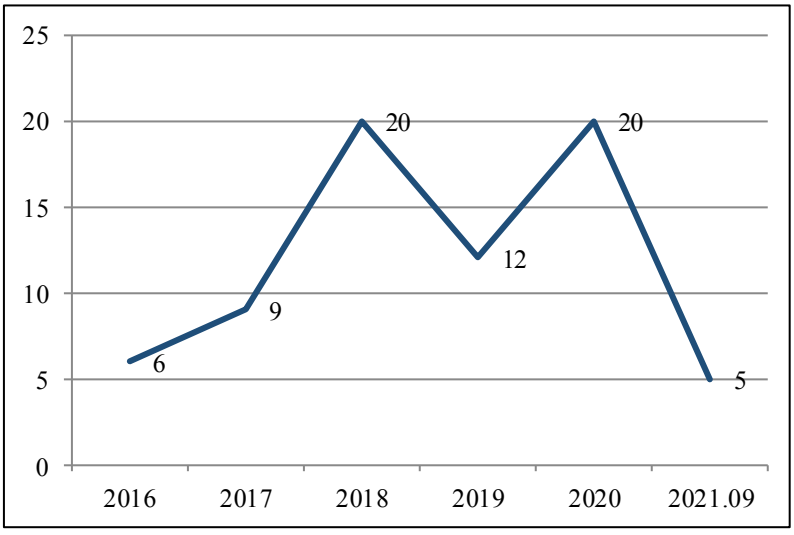
(四)支付對價型

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。

我國法院最早於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。此類總計數量72件，占所有案件數量之9%。

圖16

歷年支付工具型案件數量趨勢圖

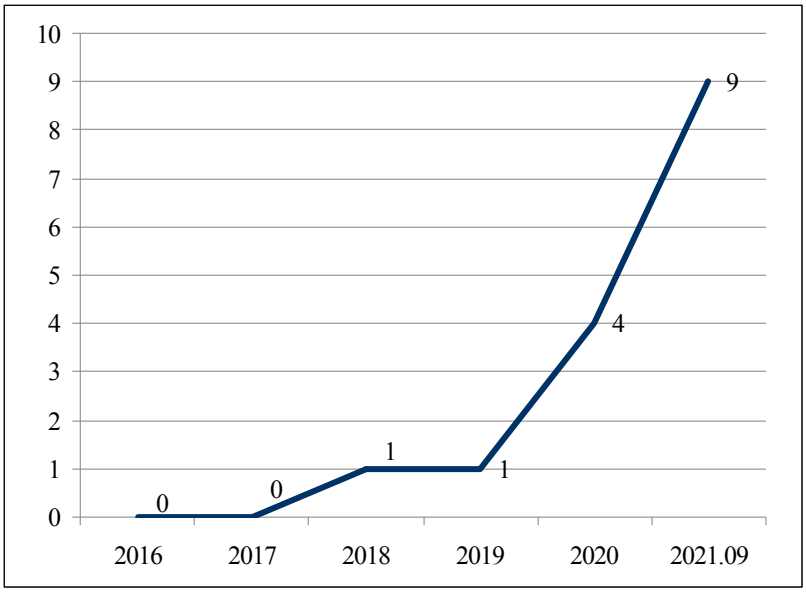


註：研究團隊自製。

(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。基本手法為被告先實施詐騙、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，逃避追緝，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17
歷年不法所得型案件數量趨勢圖



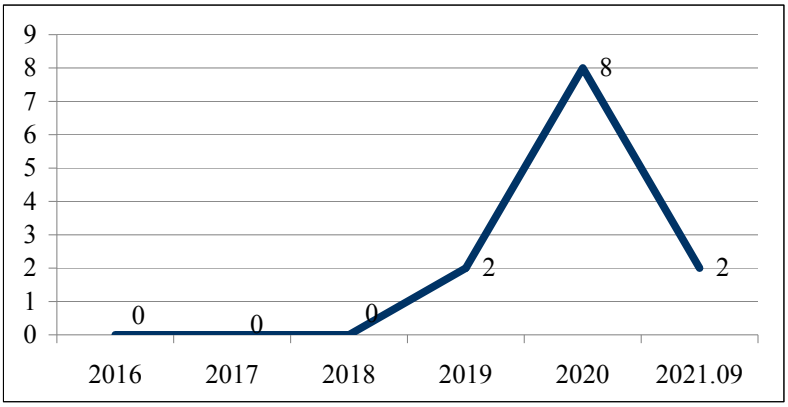
註：研究團隊自製。

(六)挖礦竊電型

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，運算過程須費大量電力。本類型犯罪為被告等設置機房及設備以進行大規模虛擬通貨挖礦，並為供挖礦所需電力，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18

歷年挖礦竊電型案件數量趨勢圖



註：研究團隊自製。

三、小　結

以虛擬貨幣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，為我國涉及虛擬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[40]，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[41]。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貨幣詐欺之「幫助犯」判決。

此外，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[42]，即認為行為人為提供個人比特幣錢包帳戶，或其他類型虛擬通貨之帳戶予詐騙集團，而該錢包位址有不法所得存入者，則原錢包帳戶之使用人，亦將構成洗錢防制法之洗錢罪行為主體。亦即將虛擬通貨之錢包帳戶，定位為類似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，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。

---

40 徐珮菱，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，頁73，2019年4月。

41 Matthew Kien-Meng Ly, *Coining Bitcoins "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J. L. & TECH. 587, 594, 608 (2014).

42 例如：臺灣彰化地方法院109年度金訴字第14號刑事判決。

伍、研究結論及政策建議

一、本研究經分析外國統計資料以及我國司法判決實證研究，發現就電子支付工具而言，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服務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。上開案件當中，有一定比例之案件涉及第三方支付服務提供者及超商代收，搭配前開人頭帳戶的大量創建，導致相關金流追查上出現許多真空地帶而產生偵查上之不易。此外，就虛擬通貨而言，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，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。

二、本研究團隊謹提出具體研究建議如下，以期得降低相關犯罪之發生可能：

(一)監理上落實電子支付工具相關業者的洗錢防制措施：

1. 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

業或人員後，法制上已相對明確電子支付工具相關業者（包括電子支付機構與第三方支付業者）應負洗錢防制義務。下一步之重點即在落實電子支付業者的洗錢防制相關措施，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。此除有賴電子支付工具相關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工具業者應定期與不定期查核其洗錢防制措施落實情形。

2.電子支付工具相關業者當中，電子支付機構目前僅有5家專營業者，故主管機關承擔的監理壓力尚屬可控；但第三方支付業者目前登記在案者有13,113家，主管機關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。除仰賴主管機關的外部監理外，於主管機關監理第三方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電子支付工具相關業者調取相關資料時，如有發現個案業者未確實落實洗錢防制義務者，可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。

(二)建議儘速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7條（旅行規則）之施行日：

1.觀諸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。

2.FATF於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。

3.經查，我國本辦法第7條訂定有「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。

4.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不同虛擬通貨平台間之轉移，尤其是涉及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，故本研究建議於適當時機擇期另訂本辦法第7條之施行日期。

三、為期降低新興金融科技包括電子支付工具與虛擬通貨涉及及犯罪之可能，本研究提出若干政策建議方案如下：

(一)應建立金融科技犯罪相關之資料庫：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相關業者的業務，否則反而會使客戶轉移至更高犯罪風險的服務或管道。本研究團隊因此嘗試透過公開司法判決資料庫進行實證研究，以釐清相關金融科技業者在我國涉及犯罪的情形，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瞭解，目前政府部門相關資料庫並無特別針對電子支付工具與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。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。

(二)應強化犯罪偵查資料數位化及其他監管科技：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。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，監理與犯罪偵查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。

(三)建議新增偽造變造數位支付工具之刑法規定，理由如下：

1.新興支付工具種類更加多元，但並無實體，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、但卻未保護無實體的其他支付工具的真實性，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。

2.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。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。

3.新興的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，因此本研究建議應比照卡式支付工具將無體的新興支付工具亦納入規範中。

4.本研究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201條之2 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。 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。	（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

修正條文	現行條文	說　明
		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205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205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。

參考文獻

一、中文文獻

- Candy Her（2019）。「門羅、DASH、ZEC…」不符合FATF反洗錢方針，OKEx韓國下架「5種隱私幣」。https://www.blocktempo.com/okex-korea-fatf-delisting-5-privacy-coins/
- Lee Michael（2020）。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。https://www.blocktempo.com/another-crypto-fraud-being-caught/
- INSIDE（2020）。是證券不是幣？美國SEC大陣仗起訴瑞波幣母公司！。https://www.inside.com.tw/article/23783-akamai-gaming-2021
- 內政部刑事警察局、海山分局（2015）。遊戲點數詐騙。https://www.zhonghe.police.ntpc.gov.tw/cp-2450-11749-13.html
- 內政部警政署刑事警察局（n. d.）。常見詐騙案例犯罪手法及預防方式一覽表103年12月。https://www.tpp.moj.gov.tw/media/63288/4561672171.pdf?mediaDL=true
- 王心婕（2020）。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
- 金管會（2015）。電子支付機構及第三方支付服務業之異同。https://fscmail.fsc.gov.tw/POP30/
- 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，16*（2），29-37。
- 林欣儀（2021）。Q點虛擬貨幣　吸金2.5億9人起訴。https://www.chinatimes.com/newspapers/20210424000443-260106?chdtv
- 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（n. d.）。http://www.msts.21tw.net/sub_7.html
- 徐珮菱（2019）。洗錢防制法制之研究——以區塊鏈及加密數位

貨幣為中心。*月旦法學雜誌，288*，73-99。http://doi.org/10.3966/102559312019050288006

- 張宏業（2021）。鑫棧虛擬貨幣工作室盜領泰達幣　8年級首腦涉洗錢遭訴。https://udn.com/news/story/7321/5486640
- 黃彥鈞（2019）。2018　暗網比特幣交易量翻倍，平均每天200萬美元。http://technews.tw/2019/01/22/bitcoin-transactions-on-darknet-markets-double-in-2018/
- 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。

二、日文文獻

- 日本金融廳網站（n. d.）。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

三、英文文獻

- CIPHERTRACE (2021). *Cryptocurrency Crime and Anti-Money Laundering Repor*t. https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/
- Emerging Payments Association (2019). *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
- FATF (2020). *12-month Review Virtual Assets and VASPs*. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

➢FATF (2021). *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

➢HM Treasury (2020). *Transposition of the Fifth Money Laundering Directive: response to the consultation*. https://www.blockchainwg.eu/wp-content/uploads/2020/03/5MLD_Consultation_Response-2.pdf

➢Japan Cryptoasset Business Association (2021). *Comments of Japan Cryptoasset Business Association on the draft revised VASP Guidance*. https://cryptocurrency-association.org/cms2017/wp-content/uploads/2021/04/Comments-of-Japan-Cryptoasset-Business-Association-on-the-draft-revised-VASP-Guidance.pdf

➢Jupiter Research (2021). *Online Payment Fraud Whitepaper 2016-2020*, Experian. https://www.experian.com/decision-analytics/identity-and-fraud/juniper-online-fraud-whitepaper

➢Ly, Matthew Kien-Meng (2014). Coining Bitcoins "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies. *Harv. J. L. & Tech., 27*, 587-608. http://www.woodllp.com/Media/Press/pdf/Coining.pdf

➢Morgan, J. P. (2020). 2020 AFP Payments Fraud and Control Survey Report: Key Highlights.

➢Q2 2018 Cryptocurrency Anti-Money Laundering Report (n. d.). https://ciphertrace.com/q2-2018-cryptocurrency-anti-money-laundering-report/