國立臺灣大學法律學院法律學研究所

碩士論文

Graduate Institute of Law

College of Law

National Taiwan University

Master Thesis

加密貨幣之洗錢防制研究

A Study on the Anti-Money Laundering Scheme of Cryptocurrency

李建德

Chien-Te Lee

指導教授：楊岳平 博士

Advisor：Yueh-Ping Yang, S.J.D.

中華民國 107 年 8 月

August, 2018

doi:10.6342/NTU201800740

謝辭

這次能順利完成此論文要感謝的人實在太多，其中天時、地利、人和三要素可說是缺一不可。回首過去充實的一年，我很幸運地遇見了楊岳平老師並有幸能請老師擔任我的論文指導教授。在楊老師的用心教導下，讓從沒想過能準時畢業的我，順利於畢業期限即將屆至的此時完成了論文。楊老師最讓我敬佩的是其開放式的指導方式，因為如此，我才能將我原本以為是天馬行空的想法揮灑在這本論文內。

還記得從小因對於科技產品充滿了興趣，時常獨自研究電腦自學。其後雖然選擇了與興趣相差十萬八千里遠的法律系，但是最初的熱忱還是藏在心中。近年金融科技崛起，其中所涉之法律問題亦逐漸浮現，在得知順利錄取研究所時，我即預計選擇加密貨幣此一主題作為論文題目。起初尚擔心著是否會無緣遇見對金融科技領域著開放想法的老師，擔心即將受傳統法學研究方法所拘束，但現在看來所有的擔憂均是多餘的。非常感謝培養我六年的台大法律系，因為系所提供的良好教學環境，我才非常幸運地得以在對的時間遇見對金融法領域有專精的楊老師。

萬事起頭難，論文尤其是如此，更何況在撰寫的過程中難免會倦怠，若無法一氣呵成，則難免進入持久戰。感謝理律文教基金會所願意讓我於去年底時參與「超國界法律」研究案，使我有機會撰寫出第一篇學術論文，此對我在撰寫這本學位論文時有著莫大的益處。感謝李永芬執行長及審查委員們不吝提供學術研究上的建議，透過研究案我學會了許多做研究必須具有的能力及特質。

感謝願意擔任口試委員的兩位教授。感謝詹德恩教授從實務界觀點為本論文提供許多洗錢防制上的建議，並精闢地點出許多本文尚待精進之處，讓我意識到自己的不足，希望未來能向詹教授多多學習。感謝林盟翔教授用心地對本文進行校正及指出諸多矛盾之處，此篇論文之所以尚堪閱讀，完全是因為有兩位細心的口試委員以及我的指導教授大力地予以訂正及指導。

感謝身旁陪伴過我的人，因為有了你們所以才讓我有了前進的動力。謝謝庭琪還有蔡平，我在學的六年因為有你們的支持與幫助，始得平穩度過每一個關卡。回首過往那些一起抄筆記、占座位及一起補習的回憶，才體悟到於學生時期交一

doi:10.6342/NTU201800740

兩個志同道合好友的重要性。因為你們，我才理解到「出外靠朋友」這句話的真諦。

謝謝工作夥伴的體諒與包容，我撰寫這本論文的期間還必須同時工作，所以有些蠟燭兩頭燒的感覺。不過幸好有正翔、晨齡你們一路的陪伴，讓我覺得早八晚六的工作時間不再那麼辛苦了。特別感謝宜君學姐及慧甄學姐兩位強大前輩的教導，讓初出社會的我得以快速成長。不管是否處於同一個崗位上，帶我入行的這幾個月期間，都是最讓我最難以忘懷的。

最後也是最為重要的感謝，是給一直以來無私奉獻自身的父親與母親，感謝你們用心地栽培讓我有機會走到這一步。若非剛好有你們給我一個幸福且無後顧之憂的家庭，也不會有今日的我。你們是我最重要的親人、隊友，也是因為有你們的支持，我才有機會選擇我走過的路，所有的榮耀屬於你們。

謝謝大家。

2018.08 於臺灣大學

doi:10.6342/NTU201800740

中文摘要

近年來我國逐漸注重洗錢防制的重要性，分別著手對金融機構及指定之非金融事業或人員課予洗錢防制的義務。加密貨幣起初因被我國中央銀行認定為虛擬商品，故缺乏洗錢防制的相關規範。惟主管機關近來已認識到基於區塊鏈運作的加密貨幣因其匿名性及流通性有被洗錢犯罪所利用的疑慮，遂開始規劃如何對其進行監理，初步考慮採取「實名制」及「自律組織」的策略。本文旨在明確化前述策略的應用對象，並提出具體的洗錢防制政策。

本文贊同主管機關所採行之監理策略，爰利用文獻分析法由淺入深，從三種虛擬貨幣匯兌架構出發，定位加密貨幣之性質，再以加密貨幣為論述核心，更深入探討加密貨幣之類型、架構種類、特性以及運作模式以辨識加密貨幣對我國法制可能造成的衝擊以及制訂洗錢防制政策將面臨的難題。

洗錢防制注重以風險為本的監理模式，此不僅是國際趨勢，更是為達有效的監理資源分配所必須。本文爰以風險為基礎分析加密貨幣，發現其會因所採行之架構係屬公鏈或私鏈而有截然不同的洗錢犯罪風險，是以有需要對兩者採行不同的洗錢防制政策。其中採行公鏈架構之全雙向流通性加密貨幣所呈現之洗錢風險最高，採行私鏈架構之加密貨幣相較之下則呈現較低之洗錢風險。

對於公鏈及私鏈之洗錢防制政策適用對象本文參考《FATF 虛擬貨幣風險基礎方法指引》、《美國銀行保密法》及美國金融犯罪稽查局之函釋區分使用者、交換者及發行者三大涉及加密貨幣運用的使用類別。歸納出匯兌業者下之交換者為加密貨幣洗錢防制上最具風險的角色，對其進行態樣分析後再將其細分為場外交易平台、經紀業者及交易所三類。本文藉由特定上述對象以評估加密貨幣與我國之國家洗錢威脅風險間的關聯性，再詳細評估其產業風險及其他風險因素，綜合洗錢風險及產業發展二者對監理策略進行修正，將其進一步具體化，以形成最具效率之洗錢防制政策。

關鍵字：加密貨幣、虛擬貨幣、區塊鏈、金融科技、洗錢防制、FATF、風險基礎方法、化名式匿名、國家風險評估、產業風險評估

doi:10.6342/NTU201800740

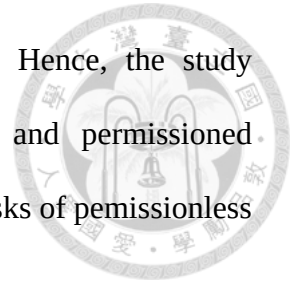
ABSTRACT

In recent years, Taiwan has gradually emphasized the crucial role of Anti-Money Laundering (“AML”) Scheme by obligating Financial Institutions (“FIs”) and Designated Non-Financial Businesses and Professions (“DNFBPs”) to comply with AML regulations. Cryptocurrency is initially deemed by the Central Bank of the Republic of China (Taiwan) as virtual commodity, which lacks appropriate AML measures. However, competent authorities have realized cryptocurrency, which functions based on blockchain, is vulnerable to money launders due to its anonymity and liquidity. Hence, competent authorities have formulated regulatory strategies, such as “Real-Name System” and “Self-Regulatory Organization”. The objectives of this study are defining the subjects to which the aforementioned strategies apply and proposing specific AML policies.

Based on the two strategies proposed by Financial Supervisory Commission (“FSC”), this study applies the Literature Review Method to examine three types of Virtual Currency Schemes, the nature of cryptocurrency, and then the blockchain schemes, properties, and operation model. On the back of the abovementioned analysis, the study identifies the impacts of cryptocurrency on Taiwan’s legal systems and the obstacles in formulating AML policies for cryptocurrency.

Risk-Based Approach (“RBA”) is the foundation of AML scheme. Adopting RBA is not only in line with international trend, but enabling effective allocation of necessary regulatory resources. The study analyze the ML risks of cryptocurrency by applying RBA and identifies a substantial difference in the ML risks stemming from “permissionless blockchain” and “permissioned blockchain”. This study learns that permissionless cryptocurrency featuring bidirectional flow property poses higher ML

doi:10.6342/NTU201800740



risks while permissioned cryptocurrency poses lower ML risks. Hence, the study proposes adopting different AML strategies for pemissionless and permissioned blockchain, and such strategies should be proportionate to the ML risks of pemissionless and permissioned blockchain.

The study refers to “FATF Guidance for a Risk-Based Approach to Virtual Currencies”, “The Bank Secrecy Act” along with the administrative rulings from FinCEN and categorizes the persons engaged in activities related to virtual currencies into User, Exchanger, and Administrator. This study reveals that Exchangers pose the most significant ML risks in the field of cryptocurrency. Based on typology analysis, this study further categorize exchangers featuring the function of money transmittance into “Over-the-Counter Platform”, “Exchange Broker”, and “Exchange Trading Platform”. By identifying the targets above, the study is able to evaluate how cryptocurrency may relate to Taiwan’s National Risk Assessment (“NRA”) and thoroughly assess Taiwan’s Sector Risk (“SRA”) as well as other inherent risks of “Money Transmitters”. The study intends to integrate the above risk assessment findings with cryptocurrency sector developments so as to propose effective and solid AML policies for cryptocurrency, which may be used as references for Taiwan’s AML regulatory strategies.

Keywords: Cryptocurrency, Virtual Currency, Blockchain, Fintech, Anti-Money Laundering, FATF, Risk-Based Approach, Pseudonymity, National Risk Assessment, Sector Risk Assessment

doi:10.6342/NTU201800740

目錄

doi:10.6342/NTU201800740

doi:10.6342/NTU201800740

doi:10.6342/NTU201800740

doi:10.6342/NTU201800740

doi:10.6342/NTU201800740

doi:10.6342/NTU201800740

doi:10.6342/NTU201800740

圖目錄

doi:10.6342/NTU201800740

表目錄

doi:10.6342/NTU201800740

縮寫表

英文簡寫	英文全稱	中文翻譯
AI	Artificial Intelligence	人工智慧
AML	Anti-Money Laundering	防制洗錢
APG	Asia/Pacific Group on Money Laundering	亞太洗錢防制組織
APIs	Application Programming Interfaces	應用程式設計界面
ASIC	Application Specific Integrated Circuit	特殊應用積體電路
BCBS	Basel Committee on Banking Supervision	巴塞爾銀行監理委員會
BIS	Bank for International Settlements	國際清算銀行
BSA	Bank Secrecy Act	美國銀行保密法
BO	Beneficial Owner	實質受益人
CDD	Customer Due Diligence	客戶盡職調查
CFT	Counter Financing Terrorist	打擊資恐
CIP	Customer Identification Program	客戶識別計畫
CPMI	The Committee on Payments and Market Infrastructures	支付及市場基礎設施委員會
CRR	Customer Risk Ratings	客戶風險分級
CTR	Currency Transaction Report	大額通貨交易申報
CUBS	Chinese Underground Banking Systems	中國地下銀行系統
DACs	Decentralized Autonomous Corporations	去中介化自治公司
DAOs	Decentralized Autonomous Organizations	去中介化自治組織
DAPPs	Decentralized Applications	去中介化應用程式
DASs	Decentralized Autonomous Societies	去中介化自治協會
DBU	Domestic Banking Unit	本國銀行
DEA	Drug Enforcement Administration	美國緝毒局
DLTs	Distributed Ledger Technology	分散式帳本技術
DSFI	Directly Supervised Financial Intermediary	直接受監理之金融中介者
DL	Deep Learning	深度學習
DNFBPs	Designated Non-Financial Businesses and Professions	指定非金融事業或人員
DNS	Domain Name System	網域名稱系統
ECDSA	Elliptic Curve Digital Signature Algorithm	橢圓曲線乘法
EDD	Enhanced Due Diligence	加強審查作業程序
FATF	Financial Action Task Force	防制洗錢金融行動工作組織
FinCEN	Financial Crimes Enforcement Network	金融犯罪稽查局
FIs	Financial Institution	金融機構
FSRBs	FATF Style Regional Body	區域性防制洗錢組織

doi:10.6342/NTU201800740

GPU	Graphics Processing Unit	圖形顯示卡
ICO	Initial Coin Offering	首次代幣發行
IMF	International Monetary Fund	國際貨幣基金組織
IP	Internet Protocol	網際網路協定
IPO	Initial Public Offerings	首次公開發行股票
IRA	Institute Risk Assessment	機構風險評估
KYC	Know Your Customer	認識客戶
LCR	Liquidity Coverage Ratio	流動性覆蓋比率
ML	Machine Learning	機器學習
MNO	Mobile Network Operators	行動支付業者或是行動網路經營業者
MSB	Money Services Business	金融服務商
MVCC	Multi-Version Concurrency Control	多版本同作控制
MVTS	Money or Value Transfer Service	金錢或價值移轉服務業
NDD	Normal Due Diligence	中強度盡職調查
NPPS	New Payment Products and Services	新興支付產品及服務
NRA	National Risk Assessment	國家風險評估
OBU	Offshore Banking Unit	國際金融業務分行
OCDD	Ongoing Customer Due Diligence	客戶持續審查
OFAC	Office of Foreign Assets Control	資產控制辦公室之制裁名單
OTC	Over the Counter Trading	場外交易
P2P	Peer-to-Peer	客戶間點對點
PEPs	Politically Exposed Person	重要政治性職務之人
QE	Quantitative Easing	量化寬鬆貨幣政策
SARs	Suspicious Activity Reports	可疑活動報告
SDD	Simplified Due Diligence	低強度盡職調查
SDNs	Specially Designated Nationals List	指定制裁名單
SRA	Sector Risk Assessment	產業風險評估
SRG	Self-Regulatory Guidelines	自律公約
SRO	Self-Regulatory Organization	自律組織
TBML	Trade-Based Money Laundering	貿易洗錢模式
TCOs	Transnational Criminal Organizations	跨國犯罪組織
TFFC	Office of Terrorist Financing and Financial Crimes	恐怖分子資助和金融犯罪辦公室
TFI	Office of Terrorism and Financial Intelligence	恐怖主義和金融情報辦公室
TMS	Transaction Monitoring System	交易監控系統
VCPPS	Virtual Currency Payment Products and Services	虛擬貨幣支付產品與服務
VC	Virtual Currency	虛擬貨幣

doi:10.6342/NTU201800740

第壹章　緒論

第一節　研究動機與研究目的

財產犯罪為我國最常見之犯罪型態，其態樣包括竊盜罪、贓物罪、侵占罪、詐欺罪、背信罪及重利罪等以非暴力違法手段取得他人財產的犯罪行為[1]。根據法務部矯正署歷年統計，財產犯罪占新入監全部刑案受刑人比率約三分之一[2]，可見以錢財作為犯罪動機之案例在我國不在少數。若以西元(下同)2008-2012 年竊盜罪新收案件之人數為例，5 年間一共有 25 萬 442 人係以該罪名而接受偵辦。根據地方法院檢察署偵辦竊盜案件，統計竊盜犯所竊取之標的物，於上述期間以入侵住宅竊盜占 37.4%為最高，其次為汽車、機車等車輛之偷竊占 30.7%，盜取公共設施（如水溝蓋、水閘門、電線、電纜、消防栓等）占 17.4%[3]，其他標的物及農漁牧相關產品和機具則分別占10.8%及3.8%。由上述犯罪人數以及竊取之標的物推論，多數財產犯罪的犯罪標的物應該還是侷限於一般動產。就住宅及車輛兩者因無竊盜標的物價值之數據，難以推論財產犯罪之平均不法所得，惟就盜取公共設施及盜取農漁牧相關產品和機具兩者似可按一般社會通念間接推估所竊取之標的物價值應不至於過於龐大。蓋在如此多的竊盜案中，除非是稀有珠寶、古董、名車，一般動產的價值實在有限，因此較容易透過日常消費將不法所得轉換為得以讓犯罪者自己享受之利益。

惟隨著財產犯罪晉升成為經濟犯罪，其中所涉不法所得金額亦隨之增長，不太容易效仿傳統財產犯罪的方式將不法所得進行轉換。此乃因為經濟犯罪所涉及

---

[1] 林美達（2014），〈新入監財產犯罪受刑人統計分析〉，《矯正統計短文》，頁 1。
[2] 同前註，頁 1。
[3] 陳進步（2013），〈竊盜罪案件統計分析〉，《【專題分析】法律宣導》，頁 1。

doi:10.6342/NTU201800740

之不法性更為重大，從侵犯客體、實施方式、以及偵查難度觀之，均與傳統的財產犯罪不同[4]。對此，學者將其定義為：「犯罪者意圖謀取不法利益，利用法律交往與經濟秩序所允許的經濟活動方式，濫用經濟秩序賴以為存的誠實信用原則，違犯所有直接或間接規範經濟活動之有關之法令，而足以危害正常之經濟活動與干擾經濟生活秩序，甚至於破壞整個經濟結構的財產犯罪或圖利犯罪[5]。」

近年來我國經濟犯罪中又以「電信詐欺」最為聞名[6]。單以台中市 2017 年 1-3 月為例，一共查獲詐欺集團 22 團、機房 4 處、車手 193 名、扣押不法所得約新臺幣 1,118 萬元、攔阻民眾被害金額約新臺幣 2,326 萬元[7]。法務部調查局 2016 年 1 月迄 12 月所偵辦之經濟犯罪及一般犯罪案件共計 945 案，嫌疑人數 2,550 人，涉案之犯罪不法所得金額高達新臺幣 859 億 4,665 萬 3,771 元[8]；其中經法務部調查局移送之經濟犯罪案件共 681 案，嫌疑人 2,105 人，涉案標的新臺幣 856 億 9,958 萬 3,752 元。分析上述數據，經濟犯罪案件所涉之不法所得占調查局所公布之經濟犯罪及一般犯罪案件總涉案金額 99.7%，其中同樣以詐欺犯罪案件為最大宗之經濟犯罪，145 件詐欺犯罪案件占整體經濟犯罪案件 21%，涉詐欺犯罪案件之嫌疑人數為 489 人占整體經濟犯罪嫌疑人數 23.3%，涉案標的共新臺幣 137 億 7,164 萬 26 元占總經濟犯罪涉案標金額 16%。

如此龐大的犯罪所得已經無法透過傳統財產犯罪的處置方式加以轉換，而是

---

[4] 林山田（1987），《經濟犯罪與經濟刑法》，頁 13，台北：三民。
[5] 同前註，頁 13。
[6] 聯合報（2017/06/21），〈台灣詐團全球跑 出國坐牢沒在怕〉，https://theme.udn.com/theme/story/6774/2536427（最後瀏覽日：2018/07/15）
[7] 大紀元（2017/03/27），〈攔阻不法所得破億 中市打擊詐欺領先六都〉，http://www.epochtimes.com/b5/17/3/27/n8972090.htm（最後瀏覽日：2018/07/15）
[8] 法務部調查局（2016），〈經濟犯罪防制工作年報〉，頁 22-29。

doi:10.6342/NTU201800740

必須經過如洗錢防制法第 2 條[9]所述的手法「處置」、「分層化」與「整合」不法所得[10]，才能將其轉換為自己得以享用之利益。為防制犯罪、避免不法所得再次被利用，國家執法者可由此下手管控犯罪者轉換不法所得的管道，並建立金流透明文化，進而達到偵測財產犯罪與預防財產犯罪的效果，此即「洗錢防制」的基本精神[11]。

洗錢相關法制隨著犯罪的組織化及跨國化，已成為各國所關注之重點[12]。洗錢相關法制有二大主要面向，第一面向為如何防制洗錢之發生，第二面向為針對已進入洗錢系統之不法所得，如何請求扣押、沒收、返還及分配，第二面向為第一面向的主要法律效果，兩者間密不可分且相輔相成[13]。聯合國於 1988 年通過《聯合國反毒公約》[14]、2000 年通過《打擊跨國組織犯罪公約》[15]，再就貪腐問題於 2003 年通過《反貪腐公約》[16]，其目的在處理第二面向不法所得的議題。我國經過多年努力，針對不法所得議題亦分別於 2015 年通過沒收新制[17]和於 2016 年通過沒收

---

[9] 本法所稱洗錢，指下列行為：
一、意圖掩飾或隱匿特定犯罪所得來源，或使他人逃避刑事追訴，而移轉或變更特定犯罪所得。
二、掩飾或隱匿特定犯罪所得之本質、來源、去向、所在、所有權、處分權或其他權益者。
三、收受、持有或使用他人之特定犯罪所得。

[10] 黃士元（2017），〈偵查中保全扣押犯罪所得〉，《司法新聲》，123 期，頁 13。

[11] 洗錢防制辦公室（2017），〈洗錢防制辦公室新聞稿〉。載於：https://www.ey.gov.tw/File/AD5A3CDBD5F63C71?A=C（最後瀏覽日：2018/07/15）

[12] *FATF Members and Observers*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/pages/aboutus/membersandobservers/ (last visited July 15, 2018).

[13] 蘋果日報（2016/11/15），〈林鈺雄：洗錢擴大沒收才能正本清源〉，http://www.appledaily.com.tw/realtimenews/article/new/20161115/988896/（最後瀏覽日：2018/07/15）

[14] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, U.N. Doc. E/Conf. 82/16 (Dec. 19, 1988), *reprinted in* 28 I.L.M. 493 (1989) [hereinafter *UN Convention against Illicit Traffic*].

[15] United Nations Convention against Transnational Organized Crime, G.A. Res. 55/25, U.N. Doc. A/RES/55/25 (Jan. 8, 2001).

[16] United Nations Convention Against Corruption, G.A. Res. 58/4, U.N. Doc, A/58/4 (Dec. 9, 2003).

[17] 104 年 12 月 30 日修正公佈之中華民國刑法（以下簡稱刑法）增訂第五章之一「沒收」，明定沒收為刑罰及保安處分以外之法律效果，具有獨立性，而非從刑。沒收之範圍擴大至犯罪行為人所有之犯罪所得，並及於犯罪行為人以外之自然人、法人或非法人團體，且因事實上或法律上原因未能追訴犯罪行為人之犯罪或判決有罪者，亦得單獨宣告沒收。

doi:10.6342/NTU201800740

程序法新制[18]，以符合「防制洗錢金融行動工作組織」（Financial Action Task Force, FATF）所列之四十項反洗錢國際規範要求[19]，進而與國際標準接軌，貫徹打擊洗錢犯罪的效果。

我國立法者與學者在研究如何對於已進入洗錢系統之不法所得，如何請求扣押、沒收、返還及分配相關制度上的努力值得讚賞[20]，惟洗錢第一面向的議題—亦即「防制洗錢」—應亦有同等之重要性，特別在金融犯罪態樣日新月異之今日更是如此。有論者將現代金融犯罪分成三種類行，分別是以金融體系為犯罪工具的犯罪行為；攻擊金融體系的犯罪行為；發生在金融體系內部的犯罪行為[21]。隨著金融科技的衝擊，洗錢模式逐漸由傳統模式升級，特別是利用「區塊鏈」此一主要的金融科技結晶，藉由其獨有的特性透過匯兌業者與金融體系相連結，以達成洗錢的犯罪態樣—亦即以金融體系為犯罪工具的犯罪行為。

加密貨幣如同早年網際網路發達後成為犯罪者洗錢慣用的工具[22]，已開始為犯罪者所採用。例如知名暗網網站「絲路」[23]，即係利用加密貨幣「比特幣」及其採用的「公鏈」[24]區塊鏈技術，交易違禁品以達成洗錢的目的，其所用於交易之加密貨幣—比特幣，亦隨著其獨有之加密特性，逐漸地受到欲匿名交易之大眾所接

---

[18]為因應 104 年 12 月 30 日修正公布之「中華民國刑法」關於沒收制度之重大變革，並完備扣押之相關程序，關於沒收程序部分，增訂第 7 編之 2「沒收特別程序」專編，同時配合修正第 1 編「總則」第 1 章「法例」、第 2 編「第一審」第 1 章「公訴」、第 8 編「執行」等相關條文，並增訂保全追徵之扣押規定及建構扣押相關程序之規範。此次修正重點在於建構刑法新增剝奪被告以外第三人財產及擴大單獨聲請宣告沒收之適用範圍，所應恪遵之正當程序，並設置專庭、專股來辦理羈押、搜索、扣押等強制處分事件，以降低預斷與先入為主發生之可能性。

[19] 詳細論述，參照：本文第四章第一節。

[20] 詳細論述，參照：本文第三章第一節第二項「洗錢防制之沒收架構」。

[21] 詹德恩（2013），〈我國金融犯罪特性與抗制難題〉，《中正財經法學》，第 7 期，2013 年 7 月，頁 165-166。

[22] JEAN-LOUP RICHET, LAUNDERING MONEY ONLINE: A REVIEW OF CYBERCRIMINALS' METHODS (2013), https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf.

[23] 詳細論述，參照：本文第三章第二節第七項「加密貨幣與網路犯罪的關聯」。

[24] 公鏈為區塊鏈組織設定之一種，參與者可自由加入區塊鏈，且無從審查，故得保有高度隱密性。詳細論述，參照：本文第二章第二節第三項「加密貨幣之架構種類」。

doi:10.6342/NTU201800740

受，比特幣之價值因此逐漸得到承認，其所代表之價值甚至超越黃金[25]。有鑒於比特幣所代表之價值及其背後龐大之交易市場，我國民眾近年來亦開始跟隨國際趨勢，盛行「挖礦」賺取比特幣或他種「有利可圖」的加密貨幣[26]並交易之，更有甚者，甚至直接將加密貨幣列為付款方式之一[27]。在如此迅速的發展趨勢下，加密貨幣伴隨的洗錢隱憂亦逐步浮現：化名式匿名的加密貨幣世界，有無可能發展成為另一個被財產犯罪者所利用的洗錢工具？現行洗錢防制相關規定，是否足以因應金融科技帶來的挑戰？

自 2009 年比特幣首次發行後，諸多加密貨幣如雨後春筍般湧現，隨著全球大量「礦工」投入挖掘加密貨幣，加密貨幣總市值已超過 2000 億美元[28]，而形成不可小覷的產業。隨著加密貨幣的市值逐漸攀升，此一新興科技自然容易為洗錢犯罪所利用，這類透過加密貨幣洗錢的案例，在我國已屢次發生。本文認為造成加密貨幣逐漸演變成為洗錢媒介之原因在於其具備的隱匿性、高價值、易流通、易交易等性質[29]。傳統洗錢模式所使用的交易媒介，常為貴重礦石、金屬、無記名有價證券等實體物品，惟此等利用實體物品洗錢之方式，勢必提高交易過程中所涉之風險以及成本，故於網路金融發達後，現代洗錢模式有逐漸朝向以跨國金流匯兌或公司法人格與海外空殼公司交易等不具實體性的貿易洗錢模式(Trade-Based Money Laundering, TBML)的趨勢[30]，此即科技之進步必然伴隨而來的犯罪手法升

---

[25] 財經新報（2017/07/10），〈比特幣是「新黃金」，價格飆將飆至 5.5 萬美元？〉，https://finance.technews.tw/2017/07/10/bitcoin-new-gold（最後瀏覽日：2018/06/20）

[26] 如：萊特幣、以太幣、狗狗幣等具收益價值之虛擬貨幣。

[27] 蘋果日報（2017/10/16），〈全台第一家　用比特幣也能喝咖啡買麵包〉，http://www.appledaily.com.tw/realtimenews/article/new/20171016/1223378/（最後瀏覽日：2018/06/20）

[28] *All Cryptocurrencies*, COINMARKETCAP, https://coinmarketcap.com/all/views/all/ (last visited June 20, 2018).

[29] 參閱相同見解：謝建國（2016），《洗錢犯罪防制對策之研究》，中央警察大學警察政策研究所博士論文，頁 35-37。

[30] RENA S. MILLER, LIANA W. ROSEN & JAMES K. JACKSON, CONGRESSIONAL RESEARCH SERVICE,

doi:10.6342/NTU201800740

級，而有正視的必要。

惟具體應如何有效規範加密貨幣的洗錢防制問題？為回應此問題尚須從加密貨幣所應用的區塊鏈技術著手，瞭解此技術的特性與運作模式後始能對症下藥，尋求最適當的解決方案。區塊鏈技術的創新之處，在於其獨有之分散式帳本技術（Distributed Ledger Technology, DLT），賦予了加密貨幣隱匿性、易流通、易交易的特性[31]，此種技術特性，可與金融服務相結合，例如使銀行體系從現有之 FinTech 1.0 升級成 FinTech 2.0[32]，達成客戶間點對點（Peer-to-Peer, P2P）交易、國內外銀行間結算機制的創新、證券商交割機制的創新等[33]。另一方面，由於區塊鏈的上述特性，應用區塊鏈技術的加密貨幣亦因此具備了所有洗錢媒介須具備之特質，甚至更便利、更隱密、更不易為執法機關所察覺[34]。未來隨著區塊鏈技術更廣泛的應用與加密貨幣的市場需求，必然會需要更多相對應之具體規範以監理其伴隨

TRADE-BASED MONEY LAUNDERING: OVERVIEW AND POLICY ISSUES (2016), http://goodtimesweb.org/industrial-policy/2016/R44541.pdf.

[31] EVANGELOS BENOS, ROD GARRATT & PEDRO GURROLA-PEREZ, THE ECONOMICS OF DISTRIBUTED LEDGER TECHNOLOGY FOR SECURITIES SETTLEMENT 5-7 (2017), https://www.philadelphiafed.org/-/media/bank-resources/supervision-and-regulation/events/2017/fintech/resources/economics-distributed-ledger-technology-for-securities-settlement.pdf?la=en.

[32] Ye Guo & Chen Liang, *Blockchain Application and Outlook in The Banking Industry*, 2:24 FIN. INNOVATION 1, 5 (2016), https://jfin-swufe.springeropen.com/track/pdf/10.1186/s40854-016-0034-9；Fintech 世代的定義尚處於討論階段，學界對於世代上的劃分各有不同見解，本文參照前揭著作再參酌：郭戎晉(2015)，〈從國際趨勢談金融科技(FinTech)與 Bank 4.0 推動策略〉。載於：http://www.tfsr.org.tw/Uploads/files/201511%20從國際趨勢談金融科技(FinTech)與 Bank%204_0 推動策略_郭戎晉組長.pdf 一文簡介之英國政府科技辦公室（Government Office for Science）提出未來 10 年願景，金融科技推展上極為重要的四大關鍵領域：

1. 機器學習（Machine Learning）及認知計算（Cognitive Computing）。
2. 數位貨幣（Digital Currency）及區塊鏈（Blockchain）相關技術。
3. 巨量資料分析（Big Data Analytics）、數據優化及組合相關技術。
4. 分散式系統（Distributed System）、行動支付（Mobile Payment）與 P2P 應用（Peer-to-Peer Applications）。

綜合上述文獻，初步選擇採取之見解為：Fintech 1.0 為以網際網路達成數位金融(Internet Finance Businesses)；Fintech 2.0 為後續科技與金融整合上再次突破，如：區塊鏈結合金融業或其他以上新型金融技術之整合。

[33] 李智仁（2017），〈會發亮的不一定都是金子──Fintech 發展的光與影〉，《月旦會計實務研究》，創刊號，頁 72-74。

[34] Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network*, 13 NW. J. TECK. & INTELL. PROP. 37, 60 (2015).

doi:10.6342/NTU201800740

的洗錢防制議題。前中央銀行總裁彭淮南同本文見解，亦公開表示加密貨幣如比特幣等有納入洗錢申報管控的必要[35]。

本研究擬剖析加密貨幣，從技術層面著手，更深入探討公鏈型及私鏈型加密貨幣現實上可能涉及的洗錢風險，以及我國是否及如何將加密貨幣納入洗錢防制之範圍。按我國近年來致力於打擊跨國洗錢及金融犯罪，為此特別訂立諸多專法和法規命令如「洗錢防制法」、「銀行業防制洗錢及打擊資恐注意事項」、「證券期貨業防制洗錢及打擊資恐內部控制要點」及「保險業防制洗錢及打擊資恐內部控制要點」、「銀行業及電子支付機構電子票證發行機構防制洗錢及打擊資恐內部控制要點」、「資恐防制法」、「電子支付機構防制洗錢及打擊資助恐怖主義注意事項範本」等，更於 2017 年 6 月 28 日新訂「金融機構防制洗錢辦法」以落實充分認識客戶（Know Your Customer, KYC）、客戶盡職調查（Customer Due Diligence, CDD）等與 FATF 接軌所必須之措施；惟在我國對金融機構採取上述洗錢防制措施前，在加密貨幣洗錢防制議題上，諸多歐美先進國家如澳洲、英國、加拿大、美國均已針對加密貨幣之匯兌及運用作出相對應的法規範[36]。我國洗錢防制主管機關法務部與相關部會亦不落人後，於 2018 年 6 月份初步達成共識，將加密貨幣匯兌業者歸類為洗錢防制法第 5 條 3 項 5 款所稱之「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」[37]，目前因尚未有專門規範的辦法，是以現行之計為增設限制，使比特幣等加密貨幣匯兌業者不得開戶，或是有銀行會接受開戶但會將

---

[35] 中央社（2017/10/25），〈彭淮南：比特幣應納洗錢防制管理〉，http://www.cna.com.tw/news/afe/201710250340-1.aspx（最後瀏覽日：2018/06/24）

[36] Connor Gamble, *The Legality and Regulatory Challenges of Decentralised Crypto-Currency: A Western Perspective*, 20 INT'L TRADE & BUS. L. REV. 346, 361 (2017).

[37] 經濟日報（2018/06/04），〈比特幣納管 設三防線〉，https://money.udn.com/money/story/5613/3178180（最後瀏覽日：2018/06/21）

doi:10.6342/NTU201800740

其列為「高風險客戶」，禁止其進行網路銀行等相關業務[38]，故實有必要深究如何加強我國洗錢防制的規範，以面對未來發展金融科技伴隨的監理衝擊。

以美國為例，金錢服務業者為洗錢防制的規範重心。只要符合金融服務商之定義，即應受銀行保密法所規範。「匯兌業者」(Money Transmitter) 為金錢服務業者下所涵蓋的六大規範主體之一，故應如何定位匯兌業者則為下一步應探究之問題。匯兌業者按美國法的定義為：「從事資金移轉或提供匯兌業務之人」[39]。而匯兌業務則係：「透過任何方式接受貨幣或其他相當於貨幣之有價物，並將之從一人移轉至另一人或其他地點」[40]。加密貨幣的買賣從定義上無疑符合了匯兌業務的內容。但若所有從事加密貨幣買賣之人均被列為匯兌業者而應受美國銀行保密法之規範，則將過度限縮金融市場，且與金融自由化及擴大金融市場規模等基本政策背道而馳。故應如何在加密貨幣匯兌的市場內重新定義匯兌業者並將不同交易態樣細分為不同之規範主體，似可做為我國未來立法之參考。

我國欲防制洗錢、沒收不法所得之決心有目共睹。未來我國須面臨之問題已不只是政策推行力度不足，更包括如何與各國洗錢防制相關規定相調和。有鑒於此，本文擬先檢視我國現行洗錢防制制度，再以 FATF 所提出之建議及導入該建議並且以實施有年之美國為主要觀察對象，希冀能透過研習其主管部門所採行之監理模式，了解我國現行洗錢防制制度在監理加密貨幣上不足之處，進而提出修改建議，促使我國儘速立法澄清現行法的模糊地帶，以提升我國金融體系下的法安定性，並與國際防制洗錢及打擊資恐實務接軌。

---

[38] 聯合報（2018/01/23），〈比特幣交易商列高風險 且不能從事網銀業務〉，https://money.udn.com/money/story/5641/2945930（最後瀏覽日：2018/06/14）

[39] 31 CFR § 1010.100(ff)(5)(i)(A)(2015).

[40] *Id.*

doi:10.6342/NTU201800740

第二節　研究方法

本研究所採用之方法，將以「比較研究法」及「文獻回顧分析法」進行之。以下簡要說明之：

第一項 比較研究法

為提出具體可行且與國際接軌的法規建議，本研究將蒐集國內外相關文獻及案例，將之綜合整理、歸納分析並比較之，以確實掌握國內外相關法規的規範內容與具體適用情形，對照比較國外與我國之利弊得失，以為規劃建議之依據。

第二項 文獻回顧分析法

本文除上述研究方法外，另視各部份之需要，轉以文獻回顧分析法進行論證。如在我國洗錢防制法之解釋論上，仍依照傳統的法律解釋為主要依據，但又因立法過程大量參考國際組織 FATF 之建議，是以會需要蒐集國內外相關文獻資料進行綜合分析、歸納整理，以探究立法意旨。

第三節　研究架構

本研究分為六章，第一章交代研究動機與目的、研究方法、研究範圍等基本問題。第二章介紹網路虛擬貨幣之概念及其分類，從虛擬貨幣的交易架構分析其是否存在容易被洗錢犯罪利用的風險，以利於後續檢討其下位概念—加密貨幣時，藉由整合虛擬貨幣架構之風險以及加密貨幣具有之風險辨識較高風險之交易模式。第三章介紹加密貨幣於我國洗錢防制法規範架構上可能面臨之問題，並分析洗錢防制對於我國管制層面及執行層面可能造成之衝擊。第四章以美國法及 FATF 所提出的建議為借鏡對象，試圖從中探尋足以應用至我國之建議並加以歸納。第五章承前章所分析之建議及改善方式，從我國所具備之國家風險出發，試圖尋找我國可能用於監理公鏈型及私鏈型加密貨幣的洗錢防制策略。經由加密貨幣匯兌產業

doi:10.6342/NTU201800740

的風險評估，預估產業於我國可能具有之風險等級。最後再整合洗錢風險及交換者自身可能具有的風險，歸納出能讓洗錢防制策略得以實施的洗錢防制政策。第六章整合上述並歸納出結論。

第四節　研究範圍及限制

本研究主要對象為加密貨幣，此種用於表徵價值的技術近來廣受爭論，各界看法不一。故本文將從洗錢防制的角度切入，探討如何監理加密貨幣始能達成有效的洗錢防制目的，主要研究範圍將以公鏈型加密貨幣中的貨幣型加密貨幣為對象，透過分析防制洗錢金融行動工作組織與外國立法例探尋貨幣型加密貨幣於我國最妥適的監理方式。

礙於加密貨幣牽涉過多技術層面的問題，本研究收集各學者及專家對加密貨幣之文獻與論述，併同國內外加密貨幣匯兌業者之實務概況，期待達成最貼近真實的加密貨幣交易模型。惟過程中礙於加密貨幣存在大量的技術性細節專業，從而在研究相對應之規範方式上，不排除可能與實際加密貨幣之運作模式稍有落差，此為本研究可能的限制。

doi:10.6342/NTU201800740

第貳章　網路虛擬貨幣概念

第一節　虛擬貨幣的介紹

第一項 虛擬貨幣之意義

自 2008 年比特幣出現後，虛擬貨幣（Virtual Currency）或是加密貨幣（Cryptocurrency）等相關詞彙逐漸進入大眾的日常生活圈內，並逐漸受重視，此由 2017 年 5 月 22 日「比特幣」一詞的搜尋數量暴增至 Google 搜尋排行榜第 5 名，「乙太坊」一詞排行第 18 名可知[41]。

加密貨幣和虛擬貨幣雖常被視為同義詞，但不管從字義上去解讀或是根據國際貨幣基金組織(International Monetary Fund, IMF)所給予的定義觀之，兩者間仍存在著些許不同。若從字義上解讀「加密貨幣」一詞，所謂的「加密」指的是貨幣本質—即所使用的區塊鏈技術，因為區塊鏈在運作的過程中往往需要經過演算法的加密及解密[42]方能更動公開帳本上的數據[43]。反觀「虛擬貨幣」一詞中的「虛擬」二字則非常貼切地形容了此貨幣的性質，不管背後所運用的技術為何，只要是無法以實體呈現的貨幣均屬此類。因此，不少學者在解說比特幣時會使用「虛擬貨幣」一詞[44]。

本文首先將虛擬貨幣和電子貨幣相區別，再細部針對全雙向流通性虛擬貨幣架構的下位概念「加密貨幣」進行討論。為釐清相關概念，本文製作簡圖如下，

---

[41] William Suberg, *Bitcoin Enters Top 5 Google Searches, Ethereum at 18*, COINTELEGRAPH (May 23, 2017), https://cointelegraph.com/news/bitcoin-enters-top-5-google-searches-ethereum-at-18.

[42] Yicheng（2017），〈區塊鏈運作原理〉。載於：https://easonwang01.gitbooks.io/blockchain/content/block.html（最後瀏覽日：2018/06/14）

[43] 詳細論述，參照：本文第二章第二節以下。

[44] Matt Egan, *What is the Dark Web, What is the Deep Web, and How Can You Access It?*, TECH ADVISOR (Apr. 6, 2018), https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/.

doi:10.6342/NTU201800740

說明各名詞間的相互關係。以下逐一說明之。

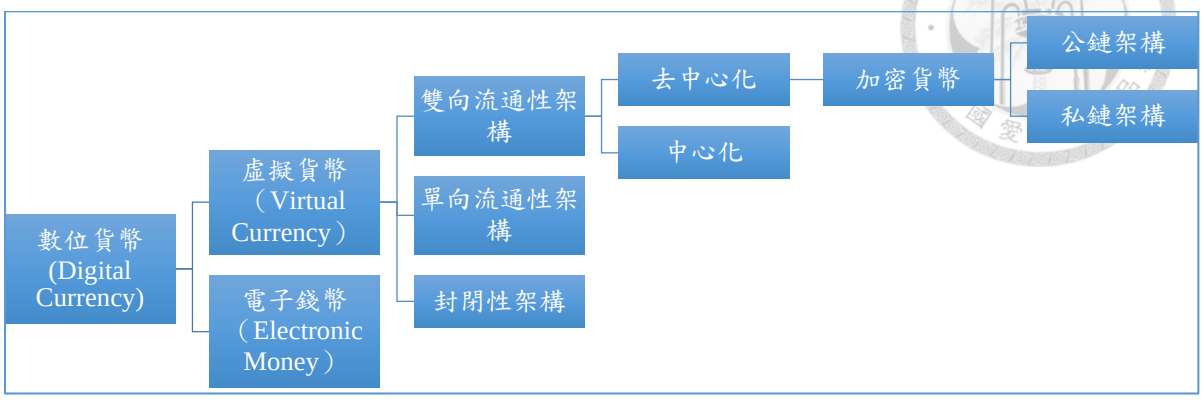


圖 一：虛擬貨幣之分類

第一款 數位貨幣

在具體說明何謂「虛擬貨幣」以前，需先說明「數位貨幣」的概念。根據 IMF 研究團隊[45]，所有經數位化的貨幣均可被稱為數位貨幣(Digital Currency)；我國中央銀行則稱之為數位通貨[46]。數位貨幣是指以數位形式呈現其價值的統稱，該價值又可按具法償性質以及不具法償性質，再細分為「電子貨幣」和「虛擬貨幣」[47]。

第二款 電子貨幣

所謂的「電子貨幣」，是一種現金的替代制度，其將具法償性質的現實貨幣數位化，進而轉換成為在開放性網路的數位世界中，以電子形式的「現金」直接進行交易，如同實體世界中的現金[48]。有學者以「電子貨幣係指利用電子資金移轉方式，交易時由一方下達轉帳的命令，將資金由己方移轉至另一方」加以定義[49]。

---

[45] DONG HE ET AL., VIRTUAL CURRENCIES AND BEYOND: INITIAL CONSIDERATIONS 5-9 (International Monetary Fund ed. 2016), http://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

[46] 中央銀行（2016/03/24），〈央行理監事會後記者會參考資料〉。載於：https://www.cbc.gov.tw/public/Attachment/632510582671.pdf（最後瀏覽日：2018/07/15）

[47] 同前註，頁 3。

[48] 李榮謙、方耀（2001），〈電子支付系統與電子貨幣：發展、影響及適當的管理架構〉，《中央銀行季刊》，第 23 卷第 3 期，頁 16。

[49] 同前註，頁 17。

doi:10.6342/NTU201800740

歐洲議會與歐盟理事會所正式發佈的行政指令，更進一步認為這種另類存在於電子世界的「現金」應符合下列要件[50]：

1. 電子貨幣須儲存於電子裝置；
2. 其所發行的價值須不低於消費者使用傳統貨幣所購買的價值；
3. 須為發行機構之外的第三人所接受。

由此觀之，電子貨幣雖非實體貨幣，但經由獨立的支付系統即能達成金錢價值的移轉，在使用上較傳統的簽帳卡、信用卡、轉帳卡、ATM 卡、電子支票等通路產品更為便利，交易成本也相對低廉。我國為降低大量小額交易的交易成本訂有「電子票證發行管理條例」，該條例第 3 條的第 1 款及第 5 款分別對應歐盟 2000/46/EC 號行政命令的要件，第 1 條亦以因應電子科技之發展、便利民眾為主要的立法目的。綜合以上特徵，目前依法發行的電子票證例如悠遊卡、一卡通應屬電子貨幣的具體應用。理想的電子貨幣應擁有下列四種特性：可信賴的貨幣價值及價值標準、可移轉性、匿名性、便利性[51]。惟現實上因為電子貨幣受限於《電子票證發行管理條例》的規範，所以無法完全達到理想上的將現實貨幣完全電子化。

第三款 虛擬貨幣

為因應理想上電子貨幣應具備的諸多特性，虛擬貨幣因而問世。歐洲中央銀行(European Central Bank, ECB)於 2012 年 10 月 29 日所提出的《虛擬貨幣架構報告》(Virtual Currency Schemes)指出，虛擬貨幣是一種由開發者發行、控制，且不受監

---

[50] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the Taking Up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions 2000/46/EC, 2000 O.J. (L 275) 39, 40, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0046&from=EN.

[51] 李榮謙、方耀（2001），同前揭註 48，頁 25-26。

doi:10.6342/NTU201800740

理的數位錢幣[52]。同時，此種數位錢幣的價值在一定程度內需被某一團體認可[53]。本文認為虛擬貨幣本身因不存在實體，僅是由數位形式呈現的一段數據，其本身的價值仍取決於某一團體或是大眾所付予之評價，故認同歐洲中央銀行 2012 年就「虛擬貨幣需在一定程度內需被某一團體認可」的定義。惟本文並不認為虛擬貨幣會因「受監理與否」而影響其本質，因為近來眾多國家已開始立法監理虛擬貨幣，但此並不會促使虛擬貨幣轉換為電子錢幣。綜合論述下，虛擬貨幣應可被定義為是一種由開發者發行及控制且其價值在一定程度內需被某一團體認可的數位錢幣。

如前所述，虛擬貨幣不具法償效力，是一種由非官方發行的貨幣，故而離達成理想電子貨幣所應具備的「可信賴的貨幣價值及價值標準」此一特性尚有一段距離。但除此之外，虛擬貨幣能運用技術在其他特性方面彌補市場上的需求，且隨著時間的流逝，一些虛擬貨幣逐漸具備了購買力和基本的價值標準[54]。種種因素

---

[52] EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES 13-16 (Oct. 2012), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[53] 惟該定義隨著虛擬貨幣的發展及各國政府相繼著手規範而備受挑戰，是以歐洲中央銀行隨後於 2015 年 2 月所提出的《虛擬貨幣架構—深入分析》報告即對 2012 年虛擬貨幣的定義進行修正，主要針對貨幣(Money)、不受監管、一定程度內需被某一團體認可等三項定義。從歐洲中央銀行對虛擬貨幣進行的分析觀之，無論從經濟面向(Economic Perspective)或是法律面向(Legal Perspective)解釋虛擬貨幣，均欠缺些許能與傳統貨幣比肩的要素。歐洲中央銀行認為虛擬貨幣因欠缺貨幣經濟學可做為交易媒介、可做為記帳單位、可做為儲存價值的三要件故不具備貨幣的功能；同時因虛擬貨幣欠缺法律觀點上貨幣需為「廣泛被交易的匯兌單位」(widely to exchange value in transactions)，故法律上亦難稱之為貨幣。再者，因各國及國際組織相繼針對虛擬貨幣進行監理及提出規範上的建議，且考慮到用客觀團體是否認可虛擬貨幣可能導致過度限縮虛擬貨幣一詞的適用，因而認為「不受監理」及「需被某一團體認可」用於定義虛擬貨幣已不妥當，將其從定義內容刪除。是故目前按歐洲中央銀行對於虛擬貨幣的定義應為：「非由中央銀行、信用機構或是電子貨幣機構發行，卻在某些情形下能用於替代貨幣，且以數位形式呈現的價值」。本文在此因主題及篇幅上之限制，並不會深入探究歐洲中央銀行 2012 年與 2015 年就「是否需被某一團體認可」之議題，惟因本文所探討之議題為加密貨幣與洗錢防制，而加密貨幣又屬於虛擬貨幣，若採歐洲中央銀行 2015 年之定義恐將過度限縮虛擬貨幣之定義，故本文暫不採歐洲中央銀行 2015 年之見解刪除「需被某一團體認可」的定義。

參考：EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES - A FURTHER ANALYSIS 23-25 (2015), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf。

[54] Jonas Chokun, *Who Accepts Bitcoins As Payment? List of Companies*, 99 BITCOINS (June 18, 2018, 5:12 PM), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.

doi:10.6342/NTU201800740

可能導致未來虛擬貨幣的定義再度改變，如未來當虛擬貨幣已具備「廣泛被交易的匯兌單位」時，歐洲中央銀行對於虛擬貨幣所提出的法律面向分析可能須再度與時俱進，做出新的修正。

虛擬貨幣之所以逐漸受到重視的原因，或許是因為電子貨幣無法滿足特定使用者的需求，因此虛擬貨幣的價值得以獲得體現。但背後更深層的原因，在於其所採用的技術能讓使用者在極為自由的環境下進行交易，較不易受執法機關的監理。此點對極度追求移轉性、匿名性、便利性的使用者特別具有吸引力。

第二項 虛擬貨幣之架構

虛擬貨幣其按所採行的兌換架構，又可細分為封閉性虛擬貨幣架構、單向流通性虛擬貨幣架構、以及雙向流通性虛擬貨幣架構（又稱開放性架構）。目前耳熟能詳的「加密貨幣」所採行的架構多半准許使用者自由地將加密貨幣與現實貨幣進行兌換，因此應歸類為採行雙向流通性虛擬貨幣架構的虛擬貨幣。

歐洲中央銀行將虛擬貨幣細分成三種架構[55]，分別是：

1. 封閉性虛擬貨幣架構[56]：封閉性虛擬貨幣又稱「遊戲內」架構，其發行的目的僅在提供特定虛擬空間需要的支付需求，通常是依照使用者的某種表現來取決發行的數量。此架構原則上與現實世界的經濟脫勾，自成一經濟體系。

2. 單向流通性虛擬貨幣架構[57]：單向流通性虛擬貨幣係指架構的設計上僅准許現實世界中的法定貨幣經一定的匯兌程序流入虛擬世界的經濟體系。法定貨幣經過虛擬貨幣的發行公司或發行人兌換成虛擬貨幣後，即得用於購買虛擬空間中所提供之虛擬商品及服務，但一經兌換的虛擬貨幣即無法再兌換回原先用來取得

---

55 EUROPEAN CENTRAL BANK, *supra* note 52, at 13-16.
56 *Id.* at 13.
57 *Id.* at 14.

doi:10.6342/NTU201800740

的法定貨幣。

3. 雙向流通性虛擬貨幣架構[58]：雙向流通性虛擬貨幣在自由匯兌的特性上與現實中可互相匯兌的貨幣相同，導致採行此架構之虛擬貨幣有著最似於現實貨幣所具有之風險屬性。在此種架構下，虛擬貨幣可依照匯率與現實社會中之各種法定貨幣兌換，使用者得以現實存在的貨幣買入虛擬貨幣，亦可賣出虛擬貨幣換取現實貨幣，猶如各國法定貨幣間之匯兌。也因此，虛擬貨幣不僅得用以購買虛擬世界中之商品與服務外，經匯兌後，亦能在現實社會中達到同等的效果。

虛擬貨幣架構種類的區分，有助立法者在制訂法規範時應採行何種洗錢防制模式，蓋不同架構種類的虛擬貨幣對社會經濟影響的程度不盡相同。例如封閉性虛擬貨幣架構幾乎與現實社會脫勾，法定貨幣與虛擬貨幣之間並無必然的連結，故無須過多的監管。惟本文對於虛擬貨幣可否截然按法定貨幣匯兌虛擬貨幣的方向來區分抱持著保留的態度。虛擬貨幣與法定貨幣的流向是需受重視的一個因素，但同時應考慮到貨幣系統的設計架構，以及有無明顯可替換的匯兌方式以規避當初設計者預先希望採取或禁止之貨幣匯兌方向。以下為本文對於歐洲中央銀行所提出之三種虛擬貨幣架構保持保留態度的理由。

第一款 封閉性虛擬貨幣架構

此架構原本的構思為自創一個獨立的經濟體系，故在設計上應避免與現實社會所流通的法定貨幣掛勾。欲達成此目的，封閉性虛擬貨幣架構至少需要有兩項設計：首先，開發者在設計上應封閉虛擬貨幣匯兌平台的匯兌可行性。倘若開發者不如此作為，此架構內的虛擬貨幣將可用於交易，例如約定出賣人轉讓一定虛

---

[58] *Id.*

doi:10.6342/NTU201800740

擬貨幣與買受人，並約定買受人於虛擬貨幣轉讓成功後，給付現實貨幣予出賣人。其次，在完全封閉的架構下，開發者應禁止用戶間轉讓帳戶，為達此目的應禁止虛擬貨幣於不同帳戶間互相轉讓及自由更改 ID 或是用於登入之電子郵件地址。蓋若准許單一用戶的帳號能自由地透過更改 ID 或是電子郵件地址，則不啻於變向准許用戶在現實世界中先訂定買賣契約後，再進入封閉式的虛擬貨幣架構內進行交易，無法達到真正原先預期的封閉效果。以歐洲中央銀行所舉之遊戲—魔獸世界(World of Warcraft, WoW)為例，原先的遊戲開發者明文禁止玩家私下轉售 WoW 黃金，但是因為私下轉讓無法禁止、黑市甚難消除之故，該遊戲現今已准許玩家於遊戲商城內透過法定貨幣購買遊戲代幣以換取 WoW 黃金[59]。原因可歸咎於原先魔獸世界內所使用的虛擬貨幣架構無法嚇阻轉場外交易，在封閉性上有明顯的漏洞，使得虛擬貨幣得以變相地和真實貨幣相互匯兌，故應不得認為其係完全封閉性的虛擬貨幣架構。

真實的封閉性虛擬貨幣架構，可以 Yahoo 奇摩知識+內所使用的「知識點數」為例。所謂知識點數，是一個用來吸引大眾回答問題的虛擬貨幣。有問題的使用者得以類似懸賞的方式發佈問題，並以知識點數做為報酬。知識點數主要取得的方式為參與社群的討論，取得之點數既無法於使用者間移轉，亦無法直接以法定貨幣購買[60]。在此完全封閉的架構下，使用者除按開發者的原意賺取虛擬貨幣外，別無他法。本文因此認為採行完全封閉性虛擬貨幣架構之虛擬貨幣被洗錢犯罪所利用的風險最低，洗錢防制需求亦同。相對地，若開發者准許使用者在封閉的架

---

[59] 魔獸世界（2018/04/29），〈魔獸代幣 - 問答集〉。載於：https://worldofwarcraft.com/zh-tw/news/18141101/introducing-the-wow-token（最後瀏覽日：2018/07/15）

[60] Yahoo 奇摩知識+，〈點數與等級〉。載於：https://tw.answers.yahoo.com/info/scoring_system（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

構內自由轉讓虛擬貨幣，雖表面上無法與現實世界的法定貨幣相連結，但仍無法避免場外交易，故應稱之為「半封閉性虛擬貨幣架構」。本文考量其架構上不准許虛擬貨幣與現實貨幣間的直接匯兌，僅准許虛擬貨幣帳戶間的價值讓與，認為其被洗錢犯罪所利用的風險僅略高於完全封閉性虛擬貨幣架構，至多僅有中低風險等級。

茲將本文以上概念區分整理如下表：

表 一：封閉性虛擬貨幣架構

架構特色 / 架構分類	開發者是否准許虛擬貨幣與現實貨幣間的直接匯兌？	開發者是否准許虛擬貨幣帳戶間的價值讓與？
完全封閉性虛擬貨幣架構	否	否
半封閉性虛擬貨幣架構	否	是

第二款 單向流通性虛擬貨幣架構

單向流通性虛擬貨幣架構，同樣可再細分為「完全單向流通性虛擬貨幣架構」以及「半單向流通性虛擬貨幣架構」。完全單向流通性虛擬貨幣架構於使用現實貨幣購買後即轉換為虛擬貨幣，虛擬貨幣不得轉讓，亦不得再兌換回現實貨幣。此種架構能有效避免使用者間相互約定為場外交易，金流清楚透明，被洗錢犯罪所利用的風險雖較封閉性架構高，整體而言風險仍得歸類為中風險屬性。例如國立臺灣大學計算中心所發放及銷售的影印點數和月旦法學知識庫所銷售之點數均為採行此架構的案例。

反觀半單向流通性虛擬貨幣架構的特色在於：架構設計者雖不提供將虛擬貨幣兌換回現實貨幣的方式，但准許使用者間相互移轉虛擬貨幣。如此設計將使使

doi:10.6342/NTU201800740

用者間得透過場外交易的方式，變相達成匯兌虛擬貨幣與現實貨幣的目的。例如國內知名的伊莉論壇積分即准許私下轉讓，導致不乏在拍賣網站上販賣積分的行為出現。又例如 Line 代幣，其於購買後雖然不准許用戶移轉代幣，但並不禁止以贈送禮物的方式將虛擬貨幣轉換後移轉他人，導致許多銷售 Line 貼圖的商家，以變相贈送禮物的方式，再將虛擬貨幣兌換回真實貨幣。由此觀之，半單向流通性虛擬貨幣架構因准許虛擬貨幣帳戶間的價值讓與，故被洗錢犯罪所利用的風險屬性應較完全單向流通性虛擬貨幣架構來得高，本文評價為中高風險。

茲將本文以上概念區分整理如下表：

表 二：單向流通性虛擬貨幣架構

架構特色 / 架構分類	開發者是否准許虛擬貨幣與現實貨幣間的直接匯兌？	開發者是否准許虛擬貨幣帳戶間的價值讓與？
完全單向流通性虛擬貨幣架構	是(僅單向)	否
半單向流通性虛擬貨幣架構	是(僅單向)	是

第三款 雙向流通性虛擬貨幣架構

雙向流通性虛擬貨幣架構的開發者並未對所發行的虛擬貨幣做出任何匯兌上的規範，故使用者能自由買賣、移轉所取得的虛擬貨幣，現下於加密貨幣市場被廣為交易的加密貨幣多屬於此類型。在此種架構下，貨幣的流通性優先被考量，此為原則，與封閉性、單向流通性虛擬貨幣架構的原則為限制虛擬貨幣與現實貨幣間之匯兌不同。

準此，倘若某虛擬貨幣在架構設計上，僅准許虛擬貨幣與現實貨幣之間的匯

doi:10.6342/NTU201800740

兌，但卻同時禁止虛擬貨幣帳戶之間的移轉，則可認為係「半雙向流通性虛擬貨幣架構」，為雙向流通性虛擬貨幣架構的例外。半雙向流通性虛擬貨幣架構的或可用於避險或是冷儲存。例如在動盪的國家內，因人民不夠信任該政府的中央銀行，所以決定與第三方虛擬貨幣公司訂定定期的消費借貸契約，約定以一定匯率先將現實貨幣轉換為虛擬貨幣，由虛擬貨幣公司代為保管，待有需要時，再以匯兌的方式換回原本的現實貨幣或是其他類別的法定貨幣。本文觀察目前市面上之加密貨幣，尚未發現採行半雙向流通性虛擬貨幣架構之加密貨幣，惟未來隨著科技的演進，不排除會產生此類尚處於理論階段的加密貨幣。相對而言，全雙向流通性虛擬貨幣架構則在設計上完全不受任何帳戶間或是與法定貨幣匯兌上的限制；觀察其具有之匯兌流通性，最似於能自由流通之法定貨幣，被洗錢犯罪所利用之風險應高於所有目前已知的虛擬貨幣架構。

茲將本文以上概念區分整理如下表：

表 三：雙向流通性虛擬貨幣架構

架構特色 / 架構分類	開發者是否准許虛擬貨幣與現實貨幣間的直接匯兌？	開發者是否准許虛擬貨幣帳戶間的價值讓與？
全雙向流通性虛擬貨幣架構	是	是
半雙向流通性虛擬貨幣架構	是	否

第四款 虛擬貨幣架構與洗錢防制的關聯

本文認為上述虛擬貨幣架構分析可從「開發者是否准許虛擬貨幣與現實貨幣間的直接匯兌」及「開發者是否准許虛擬貨幣帳戶間的價值讓與」兩方面作為評估洗錢風險的要素。從架構開發者是否准許虛擬貨幣與現實貨幣間的直接匯兌出

doi:10.6342/NTU201800740

發，因架構的開放性是金錢匯兌的基礎，是以越是開放的架構將會吸引越多的金錢匯兌業者及使用者,在此環境下金錢及價值移轉的盛行將有助於掩飾不法金流，創造易處置、多層化、整合的環境，因此洗錢風險會隨著匯兌業者的盛行而升高。我國近來完成的產業風險評估亦呈現此趨勢[61]，例如從產業及部門弱點評等表可以察覺不具直接匯兌能力的信用卡公司、非人壽保險公司被歸類為「低風險」等級；電子支付機構、證券金融事業因尚須與金融機構合作才得以完全發揮功能，但因已具典型的價值轉換功能故風險評估為「中」；郵政機構、農業金融機構因已具有匯兌能力故評估為「高風險」；最後銀行及國際金融業務分行(Offshore Banking Unit, OBU) 因除具有本國的匯兌能力外尚具有跨國匯兌的能力，是以評估的風險等級為「非常高」。

同理，完全封閉性虛擬貨幣架構及半封閉性虛擬貨幣架構因原先架構設計上不具有對外匯兌的可能性，是以本文認為應無法構成易吸引匯兌業者的環境，此類環境的欠缺將導致洗錢犯罪實施上的困難，故對洗錢犯罪較不具吸引力，風險等級較低。完全單向流通性虛擬貨幣架構及半單向流通性虛擬貨幣架構雖容許以現實貨幣與虛擬貨幣間的單向匯兌，惟欲利用此種架構進行洗錢將會面臨「整合」不法資金上的困難，特別是涉及欲迅速將鉅額不法所得整合至合法的所得時。

儘管如此，採行單向流通性虛擬貨幣架構之虛擬貨幣仍不排除被洗錢犯罪所利用的可能，蓋洗錢犯罪所涉之不法所得的轉換並非以匯兌回現實貨幣為要件，將虛擬貨幣用於享有架構內的服務或是兌換成其他虛擬貨幣亦有可能構成洗錢。例如單向流通性虛擬貨幣架構雖是以開發者是否准許虛擬貨幣與現實貨幣間的單向匯兌為區分標準，本文又以開發者是否准許虛擬貨幣帳戶間的價值讓與區分成

[61] 詳細論述，參照：本文第五章第一節。

doi:10.6342/NTU201800740

不准許帳戶間價值讓與的全單向流通性虛擬貨幣架構及准許帳戶間價值讓與的半單向流通性虛擬貨幣架構；惟以上區分並未考量「是否准許虛擬貨幣與虛擬貨幣間相互匯兌」的情形。假若單向流通性虛擬貨幣架構出現准許以虛擬貨幣匯兌虛擬貨幣的架構，則不免會衍生出將原先「不准許與現實匯兌的虛擬貨幣」匯兌為「准許與現實貨幣匯兌的虛擬貨幣」[62]後再利用全雙向流通性虛擬貨幣架構兌換為現實貨幣。本文認為此類僅准許現實貨幣與虛擬貨幣單向流通卻准許虛擬貨幣與虛擬貨幣之間相互匯兌的虛擬貨幣架構應加上「可轉換」的標籤，所謂可轉換意旨虛擬貨幣與虛擬貨幣間的直接匯兌。例如一種由發行者發行僅能使用現實貨幣購買的 A 幣，A 幣雖不能讓與其他用戶亦不能匯兌回現實貨幣，但卻能購買發行者所發行的商品 B 幣，B 幣是資產型代幣，持有 B 幣代表著能享有 B 虛擬貨幣基金的受益權，且發行者准許 B 幣持有者販售 B 幣以換取現實貨幣，此時的 A 幣所採行之架構即能稱之為「可轉換全單向流通性虛擬貨幣架構」。類似邏輯能套用至本文所介紹之他種虛擬貨幣架構，同時亦顯示了並非僅全雙向流通性虛擬貨幣架構始有被洗錢犯罪所利用的風險。

單向流通性虛擬貨幣架構雖於整合不法所得上相較雙向流通性虛擬貨幣架構較不易整合鉅額的不法所得，惟加上前述「可轉換」的特性，則將大幅降低洗錢的難度。更何況不具虛擬貨幣轉換性的單向流通性虛擬貨幣架構若並不執著於將虛擬貨幣匯兌回現實貨幣，而是欲享有虛擬貨幣所帶來的直接利益，則仍有被洗錢犯罪利用的可能。但不能否認的是：單向流通性虛擬貨幣架構的架構構成上因僅准許現實貨幣與虛擬貨幣間的單向匯兌，是以風險評級應會介於准許現實貨幣與虛擬貨幣間雙向匯兌的雙向流通性虛擬貨幣架構及不准許現實貨幣與虛擬貨幣

[62] 實務用語通常稱此類虛擬貨幣與虛擬貨幣之間的交易為幣幣交易。

doi:10.6342/NTU201800740

相互匯兌的封閉性虛擬貨幣架構之間，風險評級應介於中度風險或是中高風險。本文認為半單向流通性虛擬貨幣架構欲成功將已兌換成虛擬貨幣之不法所得再匯兌回現實貨幣尚能依賴「開發者准許虛擬貨幣帳戶間的價值讓與」要素，是故被洗錢犯罪所利用的風險應會較否準虛擬貨幣帳戶間價值讓與的全單向流通性虛擬貨幣來得高，因此評估為中高風險。

全單向流通性虛擬貨幣架構雖較封閉性虛擬貨幣架構為高，但整體評估上因不准許虛擬貨幣帳戶間的價值讓與，故被洗錢犯罪所利用之風險會較半單向流通性虛擬貨幣架構低，至多僅能認為有中度被利用的風險。全雙向流通性虛擬貨幣架構則因為架構的設計上完全容許虛擬貨幣與現實貨幣間的相互匯兌，具備高度的匯兌功能，最容易吸引匯兌業者成為中間人賺取利潤，匯兌業者的激增將有助於處置、多層化、整合不法所得，讓不法金流隱匿於合法金流之中，從而造就容易被洗錢犯罪所利用的環境，風險等級評估上應為三種架構中最高，本文評級為非常高風險。半雙向流通性虛擬貨幣架構則因為不准許虛擬貨幣帳戶間的價值讓與故對於洗錢犯罪而言較全雙向流通性虛擬貨幣架構來得不便，是以整體風險會略低於全雙向流通性虛擬貨幣架構，因此本文將此類虛擬貨幣架構評價為高風險等級。

上述封閉性、單向流通性、雙向流通性虛擬貨幣架構之風險評級主要是隨著「是否准許虛擬貨幣與現實貨幣間的直接匯兌」而遞增，依序可排列成低風險、中風險、高風險。初步以能否直接達成匯兌目的進行風險評估後，後續可再依「開發者是否准許虛擬貨幣帳戶間的價值讓與」就能否間接達成匯兌目的進行第二層的風險評估。如採行的虛擬貨幣架構准許於架構內自由轉讓虛擬貨幣，將有助於洗錢「多層化」階段的實現，評估上可再將風險層級調高，但不應超過原先第一

doi:10.6342/NTU201800740

層就「是否准許虛擬貨幣與現實貨幣間的直接匯兌」評估出來的風險等級，因為間接匯兌能造成的洗錢風險不會高於直接匯兌所能造成的洗錢風險。按此脈絡，虛擬貨幣架構的洗錢風險等級評估似可呈現如下圖：

圖 二：虛擬貨幣架構依洗錢風險排序的遞增圖

建構出初步虛擬貨幣架構可能涉及之風險後，主管機關即得參照防制洗錢金融行動工作組織(FATF)之建議，採取以風險為基礎的洗錢防制模式，對於被歸類為低度洗錢及資恐(Terrorist Financing, TF)[63]風險的項目，可決定不採行某些「建議」中要求金融機構及指定之非金融事業或人員應採取之措施，以將珍貴的執法資源有效地分配予採行高風險虛擬貨幣架構的虛擬貨幣。就識別為高風險或非常高風險的虛擬貨幣服務，洗錢防制上則可參考「FATF 虛擬貨幣風險基礎方法指引」著手進行規範，詳如第四章。

[63] 資恐防制法第 1 條將資恐定義為：「恐怖活動、組織、分子之資助行為」。

doi:10.6342/NTU201800740

第三項 虛擬貨幣之功能

虛擬貨幣於 2008 年金融海嘯前即已存在，但是在架構的運用上並無特別突出，直至金融海嘯過後，一位自稱「中本聰」之人提出了一種採用密碼學的分散式帳本虛擬貨幣支付系統[64]，始讓往後 10 年來的虛擬貨幣逐漸由原本的封閉性虛擬貨幣架構及單向流通性虛擬貨幣架構，朝著全雙向流通性虛擬貨幣架構的方向發展。虛擬貨幣作為一種不被任何政府認可的「貨幣」，不具有法償效力，故現實上能發揮其價值之處，主要還是來自於願意接受該虛擬貨幣的社群。倘若該虛擬貨幣社群足夠龐大，可能形成直接使用虛擬貨幣即可進行交易的環境，例如暗網(Deep Web)上均使用屬於虛擬貨幣概念的加密貨幣進行交易。

但去除虛擬貨幣本身技術所能帶來的技術應用與功能不談，單就虛擬貨幣經濟學的角度觀察廣義的虛擬貨幣，即不難發現導致虛擬貨幣崛起的另一種原因。目前所盛行的諸多加密貨幣，都是從 2008 年金融海嘯以後始開始得到重視及取得經濟價值，主要原因或許是因為部分民眾不願再將所有的資產交付與一個中心機構。2008 年金融海嘯爆發後，各國紛紛推行量化寬鬆貨幣政策(Quantitative Easing, QE)，透過中央銀行運用大量購買公債以及長期債券的方式，向銀行體系注入資金[65]，期待透過將如此大量超額的資金注入銀行體系，使長短期利率處於低水平，迫使銀行在較低的貸款利率下對外放貸，進而增加整個經濟體系的貨幣供給，從而達到促進消費、經濟增長、帶來高流動性的積極推動作用[66]。在此背景下，市場資金轉而流向黃金、房地產等保值商品，其中採行加密技術的虛擬貨幣—加密貨

---

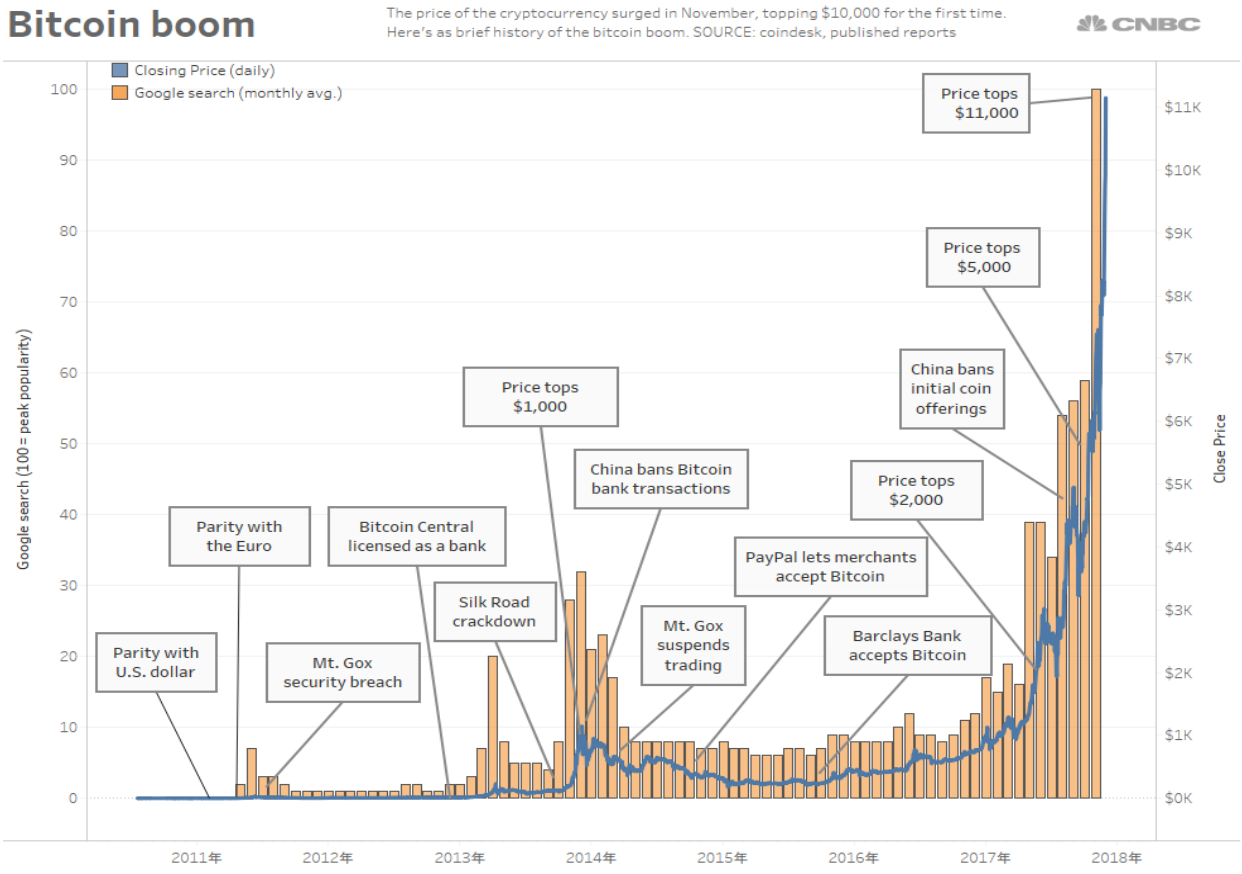
64 SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, https://bitcoin.org/bitcoin.pdf (last visited July 16, 2018).

65 耿群（2006），〈日本結束量化寬鬆貨幣政策的影響分析〉，《國際金融研究》，第 5 期，頁 4-7。

66 中央銀行（2013/12/26），〈量化寬鬆貨幣政策〉。載於：https://www.cbc.gov.tw/public/Attachment/41161474471.pdf（最後瀏覽日：2018/07/15）

doi:10.6342/NTU201800740

幣因其隱密性、便利性、且又有固定的發行總量（以比特幣為例是 2100 萬顆為挖礦上限），自然地成為投資人的選擇之一[67]。下圖為自 2011 年起比特幣的價格走勢以及 Google 的平均搜尋次數，可見虛擬貨幣的價格走勢整體而言是上升的，且有越來越受到眾人矚目的趨勢。



圖片來源：CNBC[68]

圖 三：比特幣的價格走勢以及 Google 的平均搜尋次數

許多虛擬貨幣的投資者將所得投入虛擬貨幣市場，除尋求一個無中心機構、不受中央政府監理的投資功能外，有學者另指出虛擬貨幣尚有補足實體經濟的功能，似能用於解釋為何一些加密貨幣能在金融海嘯過後崛起。經濟學家愛德華・

[67] 自由時報（2017/12/13），〈《財經觀測站》比特幣的崛起與風險〉， http://news.ltn.com.tw/news/business/paper/1159808（最後瀏覽日：2018/02/15）

[68] John W. Schoen, *This Chart Shows Bitcoin's Meteoric Rise over the Last 6 Years*, CNBC (Nov. 29, 2017) https://www.cnbc.com/2017/11/29/this-chart-show-bitcoins-meteoric-rise-over-the-last-6-years.html.

doi:10.6342/NTU201800740

卡斯特羅諾瓦（Edward Castronova）指出虛擬貨幣的另一功能在於補足實體經濟體系內較不容易補足的缺陷。其認為在虛擬貨幣的經濟體系內，持有者較不會感到焦慮也不會覺得事事都在自己的掌控外，因此較不會有無助感，而且相較現實貨幣提供了更多的獨立性與自主性。在此較低成本的體系內，虛擬貨幣還是同實體經濟體系，具備著「提供人們更大的快樂」的功能，因為虛擬貨幣雖然與現實貨幣不同，但卻同樣能造成「快樂水車」（Hedonic Treadmill）的效果，即一種永不滿足的忌妒心態，就如同上癮的狀況，永遠不嫌錢多，永遠需要獲得更多的金錢才能達到相同程度的喜悅。

按此脈絡理解，在虛擬貨幣的經濟體系內，由於資訊透明，獲取更多「金錢」的規則較明確，較不會有一些隱性的規則阻撓獲取「金錢」的過程，所以參與者能自主決定要透過何種管道獲取更多的「金錢」來尋求快樂。就如同遊戲世界中的虛擬貨幣一般，每個人都清楚獲取虛擬報酬的規則，道路及目標是明確的，玩家擁有完全的自主權如何操控既有的財富，且在這過程中不會感到焦慮或是擔心因為外部環境的變動而導致所投入的金錢化為烏有[69]。

第四項 小結

本文綜合歐洲中央銀行對虛擬貨幣的定義及現今的發展趨勢，認為採取全雙向流通性虛擬貨幣架構的加密貨幣最需要加以規範。中央銀行總裁楊金龍曾表示：「如果虛擬通貨廣泛運用在大眾的日常生活中，將可能取代法定貨幣，對準備金供需、貨幣乘數、貨幣流通速度都可能帶來影響，最後會影響到中央銀行貨幣政

---

[69] 愛德華・卡斯特羅諾瓦（2018），《《虛擬貨幣經濟學》：實體經濟有三大缺陷，虛擬貨幣讓人更快樂 》。載於：https://www.thenewslens.com/article/89423（最後瀏覽日：2018/06/14）；*See generally* EDWARD CASTRONOVA, WILDCAT CURRENCY: HOW THE VIRTUAL MONEY REVOLUTION IS TRANSFORMING THE ECONOMY (2015).

doi:10.6342/NTU201800740

策的執行。」此外，「虛擬通貨具備交易速度快、成本低及匿名的特性，能夠繞過銀行支付系統，取代現行以法定貨幣的跨境移轉，進而規避外匯及資本管制[70]。」由此可知，虛擬貨幣的發展，或可能左右國家對於既有貨幣所制訂的相關貨幣政策，亦可能對經濟體系造成難以規範的法律黑洞。

第二節　加密貨幣的介紹

第一項 加密貨幣之意義

目前許多網路文獻將虛擬貨幣一詞與「加密貨幣」互相通用，惟本文討論的主體為基於區塊鏈運作之加密貨幣，故統一使用加密貨幣一詞以特定運用此類去中心化技術的虛擬貨幣。另外為了將本文欲討論的加密貨幣細緻化，本文認為只要符合下述五要件，即應認為是加密貨幣：1.無人或政權願擔保此貨幣的價值；2.其價值完全繫諸於社會大眾；3.未經實體發行或未表徵已發行的法定貨幣；4.擁有獨立的支付系統且利用分散式帳本技術來達成用交易雙方間的去信任基礎；5.其價值在一定程度內被某一團體認可[71]。加密貨幣作為虛擬貨幣的下位概念，理論上具備所有虛擬貨幣的性質，僅是在運作上運用了區塊鏈技術而達成貨幣本身運作上及交易過程上的加密，為與傳統遊戲代幣相區分，故稱之為加密貨幣。加密貨幣因為非實體貨幣，其在現實世界上僅是一段電磁紀錄，所以在理解上可將其當成是一段有價值的電磁紀錄，基於區塊鏈而產生及變更。在此前提下，加密貨幣的性質、功能、種類均取決其所寄託的區塊鏈之上，亦即加密貨幣完全是按照區塊鏈的規範來運行的。是以加密貨幣的功能以及所表彰的有價物，亦會隨著區塊

---

[70] 蘋果日報（2018/01/10），〈比特幣改變世界　楊金龍：正評估發行法定數位貨幣優點及挑戰〉，https://tw.appledaily.com/new/realtime/20180110/1275886/（最後瀏覽日：2018/06/14）

[71] COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, DIGITAL CURRENCIES 13-20 (2015), https://www.bis.org/cpmi/publ/d137.pdf.

doi:10.6342/NTU201800740

鏈的功能提升而改變。

以比特幣為例，作為第一種採行區塊鏈技術的加密貨幣，所使用的第一代區塊鏈技術(Blockchain 1.0)也是最為簡單且直接的[72]。第一代區塊鏈是分散式帳本技術進化過後的一種資料結構，在結合加密特性與去中心化的特性後，第一代區塊鏈形成了一種匿名、安全、無中心機構，且一經共識決即能迅速變更資料的帳本技術。而虛擬貨幣作為極具經濟價值的一種應用方式，也就非常自然地成為這種全新帳本技術的一種應用，第一種為眾人所知的加密貨幣—比特幣即由此而生。

隨著區塊鏈技術的改良，越來越多更為繁雜的資料可透過區塊鏈的帳本技術處理，第二代(Blockchain 2.0)、第三代(Blockchain 3.0)、第四代(Blockchain 4.0)區塊鏈的概念油然而生。這些不同的區塊鏈技術世代，代表著應用層面的擴張，但是不管應用形態為何，只要是以區塊鏈為基礎的帳本架構，就不免會涉及服務或是價值移轉的交易，是以未來不管進入第幾區塊鏈世代，加密貨幣的概念還是會一直存在，只不過所表彰的價值形態不同而已。以下將簡單介紹加密貨幣於不同區塊鏈世代所帶來的功能。

第二項 加密貨幣之功能

加密貨幣隨著不同的區塊鏈世代的升級而越趨於複雜，涉及的洗錢議題可能不再是以加密貨幣為洗錢的客體，而是利用智能契約或是區塊鏈平台上的應用從事有價證券或是其他服務形態的洗錢。本文所討論的加密貨幣洗錢防制議題係以第一代區塊鏈為基礎的加密貨幣—比特幣為例，不會牽涉到以智能契約提供的價值服務，故本文所研究之成果對於不同世代的加密貨幣並不一定能適用。惟基於

---

[72] *Blockchain Evolution: from 1.0 to 4.0*, MEDIUM (Dec. 7, 2017), https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666.

doi:10.6342/NTU201800740

學術研究，在此舉例些許未來可能出現的加密貨幣類型，供未來制定洗錢防制政策參考。以下所區分的加密貨幣類型並非學界內的共識，目前除貨幣型加密貨幣應較無爭議外，其他類型的加密貨幣因尚在發展中，因此加密貨幣的類型並無法截然劃分，尚存在著同時符合兩種加密貨幣類型的可能，茲參考多數網路媒體說法區分如下[73]：

第一款 貨幣型加密貨幣

貨幣型加密貨幣(Currency Cryptocurrencies)又被稱為匯兌型加密貨幣(Transactional Cryptocurrencies)，是基於第一代區塊鏈技術的基礎應用，所表彰的是區塊鏈內部的價值單位，亦為本文重點討論對象。作為最基本的加密貨幣形態，貨幣型加密貨幣具備著分散式、去中心化、高度公開透明、時序性編排資料庫等特性，詳如後述[74]。

第二款 功能型加密貨幣

功能型加密貨幣(Utility Cryptocurrencies)的作用是透過區塊鏈的平台，在加密貨幣發行的時點提供特定的功能，例如提供存取應用程式或服務的數位化存取權限。若按如此廣義的敘述看來，以下之平台型及程式型加密貨幣均會因為提供特定功能而符合功能型加密貨幣的論述，創造此一概念應無特別存在的價值。因此本文認為似可將功能型加密貨幣理解成脫離貨幣型加密貨幣，但尚未轉型成為平台型及程式型加密貨幣的一個階段。功能型加密貨幣與貨幣型加密貨幣最顯著的不同在於其提供了除移轉「公眾賦予其所表彰的價值」以外的功能。此不同來自

---

[73] Cryptomaniac, *4 Categories of Cryptocurrency You Should Know*, CRYPTOVERZE.COM (Apr. 2018) https://cryptoverze.com/cryptocurrency-categories/.

[74] CHRISTIAN MULLER & DALMIR HASIC, BLOCKCHAIN: TECHNOLOGY AND APPLICATIONS 6-7 (2016), http://www.softwareresearch.net/fileadmin/src/docs/teaching/SS16/Seminar/Seminar_Paper_Hasic_Mueller.pdf.

doi:10.6342/NTU201800740

於功能型加密貨幣新增了初步的電腦語言功能，使得「智能契約」(Smart Contract)得以實現。如此觀之，功能型加密貨幣是基於第二代區塊鏈技術的應用，與第一代不同之處在於除了表彰公眾所賦予之價值外，尚加入了使程式自行達成協議的功能。因此功能型加密貨幣在保有貨幣型加密貨幣的所有優點下，更加擴增了其應用範圍。此種加密貨幣依循各種代表著「條款與條件」(Terms and Conditions)的自動執行程式碼移轉，換取服務。例如在一個買賣的智能契約中，出賣人能預先在區塊鏈平台上利用程式碼訂定支付 A 價錢就取得 A 服務、B 價錢就能取得 B 服務的自動化執行契約，欲取得 B 服務的買受人就必須支付相對應的加密貨幣來滿足程式內預設的條件，當條件成就後，預設的執行程序就會被啟動以履行債務[75]。整個程序能在交易的一瞬間完成，且享有區塊鏈所帶來的優點—即成本低、交易迅速、去中心化、去中介化、交易資訊透明、高安全性、化名式匿名所帶來的隱私等等。

第三款 平台型加密貨幣

功能型加密貨幣因受惠於第二代區塊鏈技術，故加密貨幣不再只有相互移轉的功能。但若要將其達成協議的功能進一步加以應用則不免需要一個程式平台協助同時達成協議的履行及價值的移轉。因此，本文認為平台型加密貨幣(Platform Cryptocurrencies)除了應具有全雙向流通性虛擬貨幣架構的相互匯兌的功能外，更具有在可程式化(Programmable)的平台內流通的功能。例如以太坊(Ethereum)即提供了一個具有智能契約功能的區塊鏈技術平台，所運用的加密貨幣為以太幣(Ether)。在此平台上除了貨幣傳輸的功能外，理論上尚可將所有動產、不動產、智慧財產、

[75] 陳恭（2017），〈區塊鏈與金融科技之發展及應用〉，《財金資訊季刊》，第 90 期，頁 35-38。

doi:10.6342/NTU201800740

有價證券、各種產權證明等等在現實上能表徵價值的財產虛擬化，並且透過履行智能契約的方式移轉[76]。此外若干「去中介化應用程式」(Decentralized Applications, DAPPs)、「去中介化自治組織」(Decentralized Autonomous Organizations, DAOs)、「去中介化自治公司」(Decentralized Autonomous Corporations, DACs,)「去中介化自治協會」(Decentralized Autonomous Societies, DASs)，亦能在此種平台上成立並且募資。以以太坊 2016 年所成立的去中介化自治組織－The DAO 為例，可說是存在於區塊鏈上的一間電子公司(Digital Company)，想要投資的投資人可以注入資金投資，但這間公司並不會有負責人、董事長、董事會、及員工[77]，更遑論現行洗錢防制法所強調應辨識之「實質受益人」。

未來若此類型電子公司得以廣泛設立，將會衍生複雜的法律議題。如 The DAO 在 2016 年 6 月 18 號就因為被駭而造成價值 360 萬個以太幣—當時價值約 5000 萬美元折合新臺幣 15 億元被移轉[78]。當時因為損失規模甚大，所以多數決定以硬分岔的方式另起爐灶，但是若類似情形再次發生，在難以竄改的區塊鏈架構的前提下，除了動搖區塊鏈的基礎架構造成分岔外，實在難以有任何有效作為。若類似犯罪發生如何處理投資者的賠償問題？投資者的權益如何被保障？司法管轄權究應如何歸屬？洗錢防制法如何處理此種機構？如何規範？種種尚待解決的議題仍圍繞著加密貨幣及後續的進階應用，如何處理貨幣型加密之洗錢防制問題以及未來更進階的加密貨幣類型應用上所面臨的立法及監理難題恐怕只增不減。

---

[76] MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 21–22 (2015).
[77] Ian Allison, *Ethereum Reinvents Companies with Launch of The DAO*, INT'L BUS. TIMES UK (Apr. 30, 2016, 8:49 PM), https://www.ibtimes.co.uk/ethereum-reinvents-companies-launch-dao-1557576.
[78] Michael Castillo, *The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*, COINDESK (June 17, 2016, 2:00 PM), https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/.

doi:10.6342/NTU201800740

第四款 程式型加密貨幣

程式型加密貨幣(Application Cryptocurrencies)所表徵的價值，可能已超出財產的範疇，而進入到一個較為抽象的領域—例如跟自由、司法管轄、網路審查、監理科技、人權保障相關聯的應用，Institute for Blockchain Studies 的創辦人 Melanie Swan 稱此階段為區塊鏈 3.0－治理應用階段(Justice Applications)[79]。此階段各類區塊鏈應用已發展成熟，所以將出現更多整合應用型態(Coordination Applications)，如整合就醫紀錄、病歷資料以及就醫費用的健康幣(Healthcoin)、將 DNA 資料庫公開的基因幣(Genomecoin)以及紀錄網路域名，使之能夠以去中心化的方式驗證[80]網域名稱系統(Domain Name System, DNS)的姓名幣(Namecoin)[81]。因此本文認為程式型加密貨幣會是平台型加密貨幣更進階的一種應用，其透過在區塊鏈平台上建置複雜的程式，並且將加密貨幣設計成能用於享有此類應用程式的某種服務或功能，已超越功能型加密貨幣僅提供履行簡單的條款與條件或是平台型加密貨幣准許在平台上履行條款並移轉所表徵的價值之範疇。

第三項 加密貨幣之架構種類

加密貨幣在流通性上享有極高的自由度，任何人只要通過區塊鏈密碼學的驗證，即會被認為是所有權人，可以隨意移轉經證明為具有所有權範圍內的加密貨幣。由於此種架構下的移轉非常自由，或許可理解為「內部自由」，前文所提及之全雙向流通性虛擬貨幣架構、半雙向流通性虛擬貨幣架構及半封閉性虛擬貨幣架構即為擁有此種自由的虛擬貨幣架構，本文以下將稱之為「加密貨幣流通自由」。

---

[79] SWAN, *supra* note 76, at 27-33.
[80] *Id.* at 69-79.
[81] David Gilson, *What are Namecoins and .bit Domains?* COINDESK (June 18, 2013), http://www.coindesk.com/what-are-namecoins-and-bit-domains.

doi:10.6342/NTU201800740

但良好的加密貨幣架構除流通自由外，尚須有移轉的對象，始能完成貨幣移轉的交易。若交易人無法輕易進入加密貨幣的區塊鏈內成為其中一員，則內部流通性再自由亦屬枉然。此種須獲得准許始能成為交易對象的自由，或可稱之為「外部自由」或是「參與自由」。

加密貨幣的架構種類在建置上，會因為參與自由的不同而區分為不同的架構，架構不同會造成洗錢防制難度的不同及應用上的不同，可謂洗錢防制必須考量之重要因素之一。以下將就加密貨幣可能所採行的三種架構：公鏈架構(Permissionless Blockchain)、半私鏈架構(Permissioned Public Blockchain)及全私鏈架構(Permissioned Private Blockchain)進行介紹。

第一款 公鏈架構

公鏈架構為最開放的區塊鏈架構，採行此架構的加密貨幣不僅有著無限制的內部流通自由，在外部參與自由上亦完全不受任何限制。採行此架構的加密貨幣其參與自由完全不受限制，而且每個參與者均能檢視其中的資訊並加入共識演算法，驗證每一筆交易以提高信任機制，因此在高自由度、高透明度、高信賴度的吸引下，參與的社群人數最容易快速增長。

以比特幣為例，只要有網際網路，就能下載從創始區塊迄今為止的所有交易訊息，並且獲得一組在區塊鏈上的地址—俗稱「錢包」。參與者能經由參與共識演算法的過程來獲取加密貨幣，也能透過以現實貨幣向已經擁有比特幣的人購買。目前多數加密貨幣均採此架構。

第二款 半私鏈架構

此架構與公鏈的不同之處，在於並非所有人都能自由選擇加入該區塊鏈，從而成為其中的節點，必須滿足平台所設立的某種條件、或是獲得准許後始能加入。

doi:10.6342/NTU201800740

所謂的節點是分散式帳本結構中存有一份完整帳本資訊且利用分散式網路同步帳本的電子計算機[82]。半私鏈架構與全私鏈架構不同之處，在於未被准許之人雖然不能將資訊寫入區塊鏈內，但卻可以讀取儲存在區塊鏈上的資料[83]，在兼顧管控使用者的同時達成資訊公開透明的目的，可說是公鏈與私鏈間的折衷方案。因為此架構介於公鏈與私鏈之間，所以又被稱為「混合鏈」，不僅模糊了公鏈與私鏈中間的界線，並且還具有結合兩者各自優點的功能。

在半私鏈架構的持續開發下，其與全私鏈架構的區分標準可能更趨於模糊，未來或許不能僅依參與自由者及公開透明度作為區分標準。例如當一區塊鏈架構能賦予每個節點(參與者)不同檢視權限或是參與權限時，因為各個節點分工的事項不同，也許能限制部分節點只能檢視與自身功能有關聯的資訊，而僅少數節點始能下載完整的區塊鏈數據[84]。此情形下，因為部分資訊能夠被選擇性地公開或不公開，所以若要以公開區塊鏈內的資料與否區分全私鏈或是半私鏈，似有相當程度的困難。較簡易且方便的區分方式，應可從功能面向出發，先查看在參與自由方面是否受限，以區隔公鏈與私鏈，再觀察區塊鏈本身於運作上是否較偏向以開發者自身用途為主、或是否接受來自外部的檢視等因素，綜合判斷是否採行半私鏈架構或是全私鏈架構。

目前採取此種架構的區塊鏈，以 Ripple Labs 所開發的 Ripple 平台為代表，所發行的加密貨幣為瑞波幣(XRP)。瑞波幣目前所設立的加入條件相當寬鬆，容易讓

---

[82] WORK BANK, DISTRIBUTED LEDGER TECHNOLOGY (DLT) AND BLOCKCHAIN 1-2 (2017), http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.

[83] CHARLES BRENNAN & WILLIAM LUNN, BLOCKCHAIN THE TRUST DISRUPTER 41 (2016), https://www.finextra.com/finextra-downloads/newsdocs/document-1063851711.pdf.

[84] 聯合報（2018/01/16），〈財經觀點／加速金融革新 應善用「混合鏈」〉， https://udn.com/news/story/11316/2933722（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

持有者感受不到其實其已脫離公鏈的範圍。但從技術面剖析 Ripple，欲加入 Ripple 的區塊鏈，需先找到一個願意轉帳給自己 20 個瑞波幣的使用者，當有一筆大於 20 個瑞波幣的款項轉入到一個不存在的帳戶時，一個新的 Account Root 節點才會新增至公共帳本中，完成所謂的開戶程序[85]。在上述交易架構中，接收 20 個瑞波幣是作為加入區塊鏈的條件，若未滿足該條件，則無法成為節點的一員，享有發送、接收加密貨幣等權限。此例所設定的條件雖極為寬鬆，但未來在洗錢防制政策的推行下，加密貨幣發行者為因應相關確認客戶身分的法規範，得輕鬆更該加入條件，以符合主管機關的要求。

第三款 全私鏈架構

採行全私鏈架構的區塊鏈，通常是為了追求區塊鏈的某種特性而私下建構的區塊鏈，所以無論是要成為節點、或是讀取其中的資料，都必須經過授權。在此架構內，理論上因參與之節點已通過身分認證，所以在交易時可免除認證的繁複手續，提高資訊處理的速度。

全私鏈架構較適合應用於企業內部，蓋企業內部應用上較無須顧慮到公開透明的問題，且在一個控制環境中，每個節點及參予的使用著都是能輕易驗證的，故全私鏈又常被稱為「企業鏈」（Enterprise Blockchain）[86]。也因為每個節點都是受信任的，所以較諸於公鏈，全私鏈能簡化一些認證機制，達成與公鏈相比較快的運算速度，此為其優點；但缺點也就是開放性不足，以致不如公鏈來得公開透

---

[85] Frederik Armknecht et al., *Ripple: Overview and Outlook*, *in* 9229 TRUST AND TRUSTWORTHY COMPUTING: 8TH INTERNATIONAL CONFERENCE, TRUST 2015, HERAKLION, GREECE, AUGUST 24-26, 2015, PROCEEDINGS 163, 163-80 (Mauro Conti, Matthias Schunter & Ioannis Askoxylakis eds. 2015), http://dx.doi.org/10.1007/978-3-319-22846-4_10.

[86] 安菲（2018），〈不可不知 區塊鏈的三種基本形態〉，《區塊客》。載於：http://blockcast.it/2018/02/19/public-enterprise-hybrid-blockchain/（最後瀏覽日：2018/05/14）

doi:10.6342/NTU201800740

明[87]。

第四款 小結

綜合以上分析可知，加密貨幣的流通性與區塊鏈所採行的帳本架構息息相關。在流通自由上，因為區塊鏈的運作方式不同於一般的帳本架構，所以能達成去中心化的效果。去中心化代表著並沒有一個中心機構會妨礙加密貨幣的流通自由，是以在流通自由上，加密貨幣理論上會優於採行傳統中心化帳本技術的貨幣系統。而公鏈與私鏈雖然理論上擁有同等的自由，但是因為私鏈的驗證節點通常都是由開發者控制，再加上區塊鏈上的資訊或許有部分需要權限才能讀取，導致資訊不夠公開透明，所以可能較容易讓參與者對於「是否與擁有與公鏈相同的流通性」感到疑慮。

在參與自由上，公鏈因為完全對外開放，欲參與者都能下載一份帳本並且參與共識決的過程，所以在帳本數目上及讀取權限上均無任何限制。但如此運作模式亦將導致各個參與共識演算法的礦工毫無限制地增加，當很多礦工相爭解決同一個數學謎題時，謎題的難度就會大幅提升，導致礦工必須投入更多算力(Hash Power)來增加工作量證明(Proof of Work)，進而導致運算成本的過度付出，所以並非最具經濟效益的區塊鏈架構，但是相對於成本上的缺點，其優點為高安全性、去中心化程度最高。

至於全私鏈架構與半私鏈架構的區塊鏈，與公鏈最大的不同在於帳本的參與者在被賦予權限前是受限的，而有文獻指出前者除有讀取上的限制外，尚有寫入

[87] iThome（2017/11/24），〈工研院資通所所長闕志克：真正區塊鏈應用還太少，未來區塊鏈發展方向將朝向混合鏈〉， https://www.ithome.com.tw/news/118522（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

上的限制，而後者則採不開放資料寫入、但公眾卻可以自由讀取區塊鏈上的資料[88]。兩者的架構在規劃上已經考量到未來參與者並非毫無限制，是以演算法及驗證過程所需時間及運算成本都會較公鏈來得低。此優點附隨而來的缺點，即為安全性及透明度上會不如公鏈，但這些缺點都能很容易地透過其他方式加以補足，所以就長遠來看，私鏈或許會是未來金融體系或是其他企業內部較偏好的區塊鏈架構[89]。

不同種類的架構除參與自由及參與後所擁有之權外，於辨識參與者之難易度亦各不相同。因公鏈架構准許任何人成為參與者，參與自由最高，所以欲辨識參與者之身分資訊的成本亦最高，若未有強大的監理科技(RegTech)及嚴密的法律規範，破除公鏈架構之匿名性的難度相當大，而匿名性破除的難度與被洗錢犯罪所利用的風險成正比，具高度匿名性及高風險的公鏈型加密貨幣因此成為本文主要欲討論之對象。反觀私鏈架構因需先被核准後始能被加入區塊鏈的網絡中，事先審查每個欲成為節點的參與者應非難事，較容易進行確認客戶身分程序，匿名性相對較低，可能被洗錢犯罪所利用的風險亦較低。

---

[88] CHARLES BRENNAN & WILLIAM LUNN *supra* note 83, at 40-42.

[89] Jon Southurst, *Only Permissioned Blockchains Can Transform Finance, Says Chain's Ludwin*, BITCOINIST.COM (Oct. 26, 2016, 04:37 AM), http://bitcoinist.com/permissioned-blockchains-finance-ludwin/.

doi:10.6342/NTU201800740

表 四：集中式架構、全私鏈架構、半私鏈架構、公鏈架構於運作上及功能上之異同

Ledger	Mechanics						Function		
	Level	*Copies*	*Readers*	*Writers*	*Incentive*	*Token*	*Cost*	*Security*	*Centralisation*
Traditional	Centralised	One	One	One	-	Off-ledger $	Average	Worst	Worst
Permissioned Private	De-centralised	Multiple	Multiple	Multiple	Stake	Off-ledger $	Best	Average	Average
Permissioned Public	De-centralised	Multiple	Unlimited	Multiple	Stake	On-ledger	Best	Average	Average
Unpermissioned Public	Distributed	Unlimited	Unlimited	Unlimited	Rewards $	On-ledger ₿	Worst	Best	Best

Source: Credit Suisse Research; On Distributed Communications Networks by Paul Baran, 1962

表格來源：Credit Suisse

第四項 從分散式帳本技術到區塊鏈

經過上述分析可知，目前最受眾所矚目的加密貨幣應該都屬於在公鏈上運作且採行「全雙向流通性虛擬貨幣架構」，惟不管採行何種架構，加密貨幣的運作都與所採行的分散式帳本技術（Distributed Ledger Technology, DLTs）脫離不了關係。現在耳熟能詳區塊鏈（Blockchain）就是一種分散式帳本的資料結構（Data Structure）[90]，而比特幣則是運用區塊鏈技術的一種具體化應用。

分散式帳本技術是一種儲存資料庫的方式，資料庫原則上是是分散在各個節點、且可公開供檢視。分散在各個國家、機構的紀錄，是透過連續性的記帳方式保存，若要將新的資料加入帳本，則需先驗證（Validate）交易（Transaction）資

[90] *The Ultimate Guide to Understanding Blockchain Technology*, BLOCKCHAIN TECHNOLOGIES, https://www.blockchaintechnologies.com/blockchain-technology/ (last visited Aug. 12, 2018).

doi:10.6342/NTU201800740

料的正確性。一旦通過驗證，該筆資料將被系統視為正確有效的一筆紀錄，分散在各地的帳本亦會將該筆紀錄納入原本的帳本，成為帳本的一部份[91]。像這種透過點對點網路（Peer-to-Peer Network）和共識的演算法(Consensus Algorithms)所新增的資料，即具有高度的正確性、難以竄改性、安全性、及容錯性[92]。

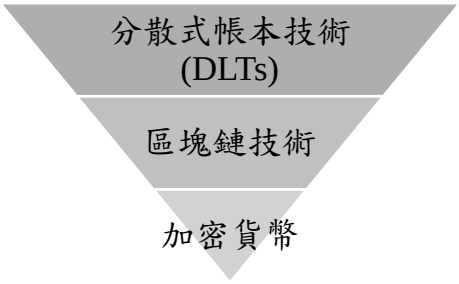


圖 四：分散式帳本、區塊鏈、加密貨幣技術階層關係圖[93]

第一款 中心式帳本技術

分散式帳本技術的主要目的是達成去中心化。此種近於破壞式創新的帳本儲存技術，讓傳統的中心式帳本面臨了前所未有的挑戰，堪稱是新一代的電子技術革命。

傳統的中心式帳本儲存技術，是將每天所產生的交易加以彙整成資料庫，並由單一機構維護、保管、儲存。如此的交易彙整技術必須通過正確性(Validity)和完整性(Integrity)的檢驗，才能稱得上是一種理想的帳本儲存方式[94]。為了達成最基

---

[91] UK GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 56-62 (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[92] CLAUDIO SCARDOVI, RESTRUCTURING AND INNOVATION IN BANKING 36-37 (2016).

[93] CHARTERED ACCT. AUSTRALIA & NEW ZEALAND, THE FUTURE OF BLOCKCHAIN: APPLICATIONS AND IMPLICATIONS OF DISTRIBUTED LEDGER TECHNOLOGY 8 (2017), https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-future-inc-caanz-blockchain-010217.pdf.

[94] Gareth W. Peters & Efstathios Panayi, *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, *in* BANKING BEYOND BANKS AND MONEY: A GUIDE TO BANKING SERVICES IN THE TWENTY-FIRST CENTURY, 239, 10-12 (Paolo Tasca, Tomaso Aste, Loriana Pelizzon & Nicolas Perony eds., 2015).

doi:10.6342/NTU201800740

本的兩項檢驗，所有的交易均必須經過人工的處理和驗證，方能保證最基本的運作。在確保交易的正確性和資料庫的完整性的同時，尚須考慮數據中心的維護成本、內部資料庫對外的共識性、安全性等因素。這些因素均會間接地增加中心式帳本的維護費用。

除了技術風險外尚有人為風險，蓋中心化的帳本須由人來維護，尚無法排除帳本被人為竄改或是操作不當導致資料損毀的風險[95]。為了消除各種可能會威脅中心式帳本的因素，各大銀行紛紛提高維護帳本所需之費用[96]。以美國銀行(Bank of America)為例，其 2015 年花費在資訊安全高達 4 億美元。摩根大通亦不落人後，其資安預算已從 2.5 億美元提高至 5 億美元[97]。研究預計在 2019 年時，資安被駭所造成的損失可能高達 2 兆美元，是 2015 年的 4 倍[98]。因所造成的損失是如此的巨大，故全球的資安市場在 2015 年時已高達 750 億美元[99]，且預計於 2020 年升至 1700 億美元[100]。由此觀之，採行中心式帳本技術的資料庫從建置到後續的維護，均離不開隱藏的資安風險。而越重要的資料能承受的資安風險就越小，為了縮小此風險，系統維護的成本勢必就會隨之提升。這也是為何大型的金融業者會越來越注重資料庫的維護的原因，蓋系統一旦被有心人士入侵，所造成的損害通常都

---

[95] Greeshma R. Nair & Shoney Sebastian, *BlockChain Technology Centralised Ledger to Distributed Ledger*, 4 INT'L RES. J. ENG'G & TECH. 2823, 2823-27 (2017), https://www.irjet.net/archives/V4/i3/IRJET-V4I3711.pdf.

[96] Harry Terris, *Banks to Spend More on Tech in 2016 - Especially Security*, AMERICAN BANKER (Oct. 15 2015, 10:00 P.M), https://www.americanbanker.com/news/banks-to-spend-more-on-tech-in-2016-especially-security.

[97] Steve Morgan, *Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers*, FORBES (Jan. 27, 2016), https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#68d0c7a3264c.

[98] *Cybercrime Will Cost Businesses Over $2 Trillion By 2019*, JUNEIPER RESEARCH, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion (last visited Nov. 14, 2017).

[99] *Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015*, GARTNER (Sept. 23, 2015), https://www.gartner.com/newsroom/id/3135617.

[100] *World Cybersecurity Market Will Grow by $100B in Five Years*, RT INTERNATIONAL (Sept. 12, 2015), https://www.rt.com/usa/315147-cybersecurity-market-growth-boom/.

doi:10.6342/NTU201800740

是難以估計的。

第二款 分散式帳本技術

針對中心式帳本所附隨的維護成本日益漸增的問題，分散式帳本誕生了。分散式帳本最初的構思，是為了優化單一且龐大資料庫所面臨的存取上限和運算瓶頸的問題。假設一採行中心式帳本技術的金融機構，每天需處理的平均交易數量為 1000 筆，若以 1000 筆交易資訊為建置資料庫的考量，該金融機構僅需支付相當的費用於剛好能處理若干筆交易資訊的硬體上。惟使用者的使用習慣時常無法以平均值來計算，以過年訂車票為例，該訂票系統在整點訂票系統開放時，會湧入比平時高數倍的交易資訊，導致系統負荷不了而無法服務全體客群。但如專門為了應付一年之中少數幾次會暴增的交易時段而提升硬體的性能，不過是浪費平時閒置的效能而已，徒增建置成本與開銷。

分散式帳本在某種程度上為上開問題提供瞭解決方案。若能將資料庫複製多份至不同的伺服器供使用者存取，將能大大提升資料的可靠性和有效性、整體吞吐量和效能、以及可拓展性 [101]。此係因資料庫數目的提升將連帶提升連接數，同時也會增加資料的冗餘度(Redundancy)，這樣一來單一資料庫毀損時不至於影響整體系統的運作。

惟如何使所有資料庫間的資料得以保持一致和同步，即成為問題，此涉及資料庫如何配置，不同的配置方式將導致不同的同步的方式。在採行分散式帳本技術的資料庫中，可按「是否將完整的資料庫分散至各個節點」區分為「完整複製型的全鏡像分散式」 (Fully Replicated Distributed Database)的資料庫、「完全差異

[101] BANK FOR INT'L SETTLEMENTS, DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENT, CLEARING AND SETTLEMENT: AN ANALYTICAL FRAMEWORK 9-14 (2017), https://www.bis.org/cpmi/publ/d157.pdf.

doi:10.6342/NTU201800740

型的無冗餘分散式」(Non-Redundant Allocation)資料庫、和介於兩者之間的「半複製型」(Partial Replication)資料庫[102]。本文所欲討論的對象—分散式帳本技術下的區塊鏈—係採取全鏡像分散式的資料庫，故僅就此部分予以細述。

所謂的全鏡像分散式資料庫，係指所有的節點均存有一份完整的資料庫。因所有資料庫間的資料都會互相複製、同步，就如同鏡子一般，故所有被同步的子資料庫又稱之為資料庫鏡像(Database Mirroring)[103]。此種形式的分散式資料庫，通常會透過「主從架構」(Master-Slave Relationship)來保持資料庫之間的資料傳遞(Propagate)，亦即要先由一個最上位的主資料庫更新成最新的資料後，再將欲更新的資料向下傳遞，以達成所有分散在外的資料庫的一致性。惟對於每秒數萬筆交易的金融機構而言，如此形式的資料庫更新方式較諸於中心式資料庫並未顯得更有效率，蓋帳本的交易效率很大因素還是取決於最上位的主帳本。主要問題還是來自於採取分散式帳本技術的資料庫，對於資料的「讀取」雖有顯著的優化效果，但是一旦要將一筆資料「寫入」帳本時，即會面臨同時也有可能會有另一筆相衝突的資料在同一時間被寫入的問題。目前較簡易預防資料衝突問題的技術，就是如上所述的「主從架構」，但若是一味依靠主資料庫的更新來帶動從資料庫的更新的話，又與中心式帳本相去不遠，無法解決頻寬的瓶頸(Bottleneck)、可靠性(Reliability)、延遲(Latency)等問題。

為解決採取「主從架構」的分散式資料庫通常會面臨與中心式資料庫相同的上述問題，各種資料庫廠商分別發展出所謂的多主複製型(Multi-Master Replication)的分散式帳本技術。顧名思義，在採行多主複製型的資料庫中存在著多個主資料

---

[102] RAMEZ ELMASRI & SHAM NAVATHE, FUNDAMENTALS OF DATABASE SYSTEMS 887-97 (2010).
[103] *Database Mirroring and Replication (SQL Server)*, MICROSOFT DOCS (Mar. 14, 2017), https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/database-mirroring-and-replication-sql-server.

doi:10.6342/NTU201800740

庫，所有想被寫入的資料均可自由地向各個主資料庫進行寫入。當一主資料庫接收到寫入資料時，就會透過對等式網路(Peer-to-Peer)的方式通知其他的主資料庫更新資料，以達成真正意義上的資料相互同步。惟採取此種型態的資料庫固然能呈現分散式資料庫的優點，卻無法完整解決同時寫入的資料有可能相互衝突的問題[104]。如金融業者採取此種形式的資料庫更新方式，即無法避免同一時間執行兩筆支出交易，被不同的主資料庫接收到，導致最後資料庫同步時不知究竟應該採用哪一筆資料的問題。針對此問題有提出「多版本同作控制(Multi-Version Concurrency Control, MVCC)」的解決方案，提供多種遇見資料衝突時的處理方式[105]，包括：1.事務隔離 2.明確鎖定 3.應用層的數據完整性檢查 4.鎖和索引等[106]，對此本文不會一一探究。須注意的是「多版本同作控制」仍須人力的涉入，無法透過資料庫本身的機制來決定最後應採用哪一筆交易，因此到目前為止，無一金融機構會使用全鏡像分散式帳本架構為基礎來建構客戶的交易資料庫；既然連記錄交易資料的帳本均構成問題，更遑論更深層的應用至電子貨幣或是加密貨幣了。

第三款 基於區塊鏈的加密貨幣

2008 年比特幣的誕生，打破了上述的技術性僵局。比特幣之所以能成為目前最熱門的加密貨幣、且受網路黑市愛好者們的喜愛，主要原因還是因為背後所帶來的新型分散式帳本架構—區塊鏈。傳統的分散式帳本資料結構無法安全地用於儲存客戶的金融資料，蓋金融體系講究穩定，無法容忍帳面上出現錯誤。

---

[104] Gideon Greenspan, *Ending The Bitcoin vs Blockchain Debate: Is there any Value in a Blockchain without a Cryptocurrency?* MULTICHAIN (July 19, 2015), https://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/.

[105] *MySQL 5.7 Reference Manual 21.6.11 NDB Cluster Replication Conflict Resolution*, MYSQL, https://dev.mysql.com/doc/refman/5.7/en/mysql-cluster-replication-conflict-resolution.html (last visited June 14, 2018).

[106] 郭朝益（2007/02/08），〈同作控制(Concurrency Control) - 簡介〉。載於：http://postgresql-chinese.blogspot.tw/2007/02/concurrency-control.html（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

區塊鏈的出現,某程度解決了多版本同作控制(下稱 MVCC)在多主複製型的分散式帳本無法妥善處理的資料衝突問題。不僅如此，在解決前述問題後，區塊鏈擴充了分散式帳本技術的運用，讓帳本能脫離資料庫的形態，進而走入一個以網絡(Network)所呈現的全新形態。此係因為區塊鏈跳脫了以資料庫為形式的記帳模式，而改採一種新興的紀錄模式。

在區塊鏈出現前，傳統資料庫是利用寫入資料來達成變更內部資料的方式。在傳統帳本模式下，任何對帳本的寫入動作均會導致帳本內的資料變動，每一種變動都是一筆新的交易。在單一資料庫、單一帳本的情形下，不會有交易衝突的問題。但若是在多個資料庫間，資料互相分散的情形下，同時對於需變更的資料做出完全相反交易時，就會暴露傳統以資料庫形式帳本的短處[107]。

區塊鏈出現後，帳本有了以網絡相互串聯的概念。其較傳統帳本的優勢在於能複製無上限的帳本，並且確保帳本間的資料保持一致性，不會有資料衝突的狀況產生。加密貨幣作為新式帳本內的一種資料，首先被應用至虛擬貨幣，經檢視加密貨幣運作以來的新聞，尚未有任何雙重支付(Double Spending)或是帳本出現錯誤而毀損的案例，可見區塊鏈於處理多個資料庫間資料相衝突的機制，確實較傳統帳本來得有效。以下將以比特幣為例深入探討加密貨幣的運作及如何達成去中心化。

第五項 加密貨幣的運作模式—以比特幣為例

在瞭解如何防制比特幣為洗錢犯罪所利用,需先瞭解其運作模式及交易架構，以便對症下藥，從癥結點開始治理。

---

[107] RAGHU RAMAKRISHNAN & JOHANNES GEHRKE, DATABASE MANAGEMENT SYSTEMS 484-88 (2d. ed. 2003).

doi:10.6342/NTU201800740

第一款 加密貨幣的交易架構

觀察市場上的加密貨幣流向，能得知有一方為供應方、另一方則為需求方。供應方負責生產和提供加密貨幣，需求方則扮演著「活化」加密貨幣的角色。需求方負責使用現實貨幣向供應方購買加密貨幣，其主要目的除了為了投資或是利用買賣賺取價差外，多半是為了利用加密貨幣所具備的諸多特性，如：可移轉性、匿名性、便利性等等。目前市面上提供以加密貨幣作為付款方式的商家尚不普及，往往需經兌換後才能利用其具有的價值進行消費，從而又多出了仲介者的角色。

加密貨幣的交易架構先由供應者提供加密貨幣予加密貨幣仲介者，再由需要使用加密貨幣之人擔任消費者向仲介者購買的三方關係。供應者早期為提供運算能力的「礦工」。但隨著加密貨幣的普及，單由礦工提供算力並由系統自動產生加密貨幣做為報酬以支撐整個支付體系已非易事，如何推廣新發表的加密貨幣更是問題。因此後期開發的加密貨幣較偏向由加密貨幣發行業者本身直接對外發售以獲取資金。如 Ripple Lab 所發行的瑞波幣、Telegram 公司所發行的 TON 代幣[108]，均非屬開採式的貨幣，而是由加密貨幣發行人逕自在建置貨幣系統時先予以發行並用於募資。

加密貨幣的消費者是需要虛擬貨幣的客群，越多消費者願意以實體貨幣購買該款加密貨幣，代表該加密貨幣的需求度越高，流動率、接受度和變現度也就相對提高。比特幣作為首先發行的加密貨幣，目前在買/賣價格上居首，遠超越他種加密貨幣。造成此結果的原因即是因為使用客群最為廣泛。據 2017 年 11 月所統計的一份資料，比特幣佔有加密貨幣總市佔率的 58%，每天平均有超過 4 億 9 千

[108] Jon Russell, *Telegram has Raised an Initial $850M for its Billion-Dollar,* ICO TECHCRUNCH (Feb. 17, 2018), https://techcrunch.com/2018/02/16/telegram-ico-850-million/.

doi:10.6342/NTU201800740

萬美元的交易量，且有 32 萬 6 千筆交易被確認。該統計顯示每天平均有 71 萬 5 千個活躍的比特幣帳戶（地址），且單就 Blockchain.info 所擁有的 1 千 8 百多萬個比特幣帳戶來看，願意使用或是接受比特幣的潛在客群還是不在少數[109]。其次，比特幣也是最廣為接受的加密貨幣，據 Statista.com 統計自 2016 年 1 月至 2018 年 8 月之數據，全球已累計 3,461 台比特幣 ATM[110]。上述數據顯示加密貨幣會因願意接受其作為交易對價的群體的增加而普及。

加密貨幣的買賣與外匯買賣的差異在於仲介者。消費者欲買賣外國貨幣時，因較能信任由政府核准設立的金融業者，故平時外匯的買賣可不臨櫃辦理、而直接在金融業者的系統進行買賣交易。消費者於交易後能放心地將換取後的外幣直接存放於金融業者提供的外幣帳戶，不用擔憂被竊取或是挪用，在交易便利性上再增一層穩定的誘因。此係因放置在銀行的存款均受存款保險的保障[111]，存保公司負有賠付存款餘額之責，保障範圍包含「外幣存款」和「存款利息」[112]，以網路開立的數位存款帳戶亦享有保障[113]，單一金融機構的總額賠償上限目前為新臺幣 300 萬元[114]。

反觀加密貨幣的買賣，由於買賣加密貨幣的行為不受法律規範，故許多態樣的仲介業者紛紛加入此自由度、獲利程度均極高的行業。扮演貨幣買賣角色的仲

---

[109] Kai Sedgwick, *Bitcoin by Numbers: 21 Statistics That Reveal Growing Demand for the Cryptocurrency*, BITCOIN.COM (Nov. 11, 2017), https://news.bitcoin.com/bitcoin-numbers-21-statistics-reveal-growing-demand-cryptocurrency/.

[110] *Bitcoin - Statistics & Facts*, STATISTA.COM, https://www.statista.com/topics/2308/bitcoin/ (last visited Aug. 15, 2018).

[111] 按存款保險條例第 10 條：「凡經依法核准收受存款…具保本保息之代為確定用途信託資金之金融機構，應向存保公司申請參加存款保險，經存保公司審核許可後為要保機構。」又按同條例第 28 條：「要保機構經主管機關或農業金融中央主管機關勒令停業時，存保公司應依下列方式履行保險責任：一、根據停業要保機構帳冊紀錄及存款人提出之存款餘額證明，將賠付金額以現金、匯款、轉帳或其他撥付方式支付。」

[112] 《存款保險條例》第 12 條。

[113] 惟不包括銀行所設之國際金融業務分行（OBU）收受之存款。

[114] 《存款保險條例》第 13 條。

doi:10.6342/NTU201800740

介者，在法律規範上又被稱為「交換者」，具體可區分成：場外交易平台、經紀業者以及交易所，以上採行的交易方式又可按隱密性、風險、交易費用、交易自由等因素進行選擇，詳如第五章第三節第二項。

第二款 加密貨幣表彰的權利

比特幣是加密貨幣的一種，本身只存在於電子世界中，其留存在現實世界中者僅為一段程式碼、一段電磁紀錄。惟此紀錄有助逆推比特幣的整個運作模式，故在理解比特幣的交易架構後，接著需理解比特幣的交易和持有究竟代表什麼意義？

持有比特幣代表於區塊鏈帳本上查詢持有人的地址時，將發現存在且尚未變成輸入交易之紀錄[115]。此定義意指比特幣是：1.存在於分散式帳本內的紀錄；2.該紀錄尚未因為「交易」而更新。舉例來說，每個人都有「年齡」的時間紀錄，隨著時間的流逝（即比特幣內的「交易」），年齡就會隨之增長，而此增長是不可逆的。一個人的年齡會按照時間的流速增長，目前增長的單位為「年」（即比特幣內的「區塊」），每增長 1 年即代表老了 1 歲。如要計算目前的年齡，當然要先知道自己的出生年/月/日後，再計算已經流逝的時間，方能得出目前的年齡。例如：欲計算一個人是否具備完全行為能力，需從該人出生之日起算 20 年。計算的過程是累計的，累計的過程亦不可與時間軸相衝突，否則計算出來的年齡就沒有意義。例如：從 16 歲到 17 歲相差 365 日，計算始日必須從 16 歲的第 1 日的第 1 秒開始起算，任何起算時間的錯置均會導致年齡計算的錯誤。

比特幣就如同上述例子中的年齡，是一個虛無飄渺，但卻又富有意義的一項

---

[115] Yicheng（2017），同前揭註 42。

doi:10.6342/NTU201800740

紀錄。目前各個虛擬貨幣交易所所交易的虛擬貨幣，均係一個「尚未因為交易而更改的紀錄」。只要所持有的紀錄尚未因為新加入的區塊而變更，那所持有的比特幣就不會有帳目上的更改。當使用者欲交易比特幣時（也可想成是推動時間的流動），其需先完成三項條件：1.得知接收者的錢包地址；2.發送者的私鑰；3.足夠的比特幣及手續費。接收者的錢包地址是先經過該地址的私鑰，經由橢圓曲線乘法（Elliptic Curve Digital Signature Algorithm, ECDSA--SECP256K1）轉換為公鑰，再將公鑰透過一系列的加密演算法後，形成由 Base58 編碼的結果，也就是錢包地址[116]。錢包地址由英數字混和而組成[117]，並無法從當中得出任何錢包持有者的訊息。是故，使用者在接收比特幣時，僅需提供錢包地址，即可接收比特幣。但是單持有錢包地址的效果只有接收，不包括發送，因錢包地址是由公鑰及私鑰一同組成，從地址能演算出公鑰，公鑰卻因非對稱式加密的結果，無法得出私鑰。滿足上述三項條件，才能移轉比特幣。如前所述，比特幣係「尚未因為交易而更改的紀錄」，所以欲交易比特幣，必須擁有更改紀錄的權限，若無此權限則難謂擁有比特幣。權限的有無則取決私鑰，發送者在交易前首先會向每個節點發佈三樣訊息[118]：1.發送者取得比特幣之前手的公鑰，及用相對應的私鑰所為之簽名，證明自己確實擁有移轉此筆紀錄的權限；2.欲發送多少比特幣；3.接收者的地址。上開交易的訊息會與其他的交易訊息一同被打包成一個區塊，等候「礦工」的驗證。

礦工是一群利用電腦、礦機來提供算力的區塊鏈驗證者。所謂的「算力」就是推動區塊鏈持續運作的力量，無論：1.驗證發送者對於從前手取得的公鑰的簽名

---

[116] Yicheng（2017），〈BITCOIN 原理與實作〉。載於：https://easonwang01.gitbooks.io/blockchain/content/chapter1.html（最後瀏覽日：2018/07/15）

[117] 例如：1KN44ET8TUfYd54q2TGvYFgsd367HoLHva

[118] *How Bitcoin Transactions Work*, BITCOIN.COM (June 8, 2017), https://www.bitcoin.com/info/how-bitcoin-transactions-work; *How Do Bitcoin Transactions Work?* COINDESK (Jan. 29, 2018), https://www.coindesk.com/information/how-do-bitcoin-transactions-work/.

doi:10.6342/NTU201800740

是否正確；2.將每筆交易資訊彙整成一個區塊；3.算出新區塊的 Hash 值以便將其納入區塊鏈內；4.解出數學謎題以獲得工作量證明（Proof of Work, PoW），均需要礦工提供算力來支撐整個虛擬貨幣架構的運作 [119]。比特幣的產生與工作量證明息息相關，只有第一個解出數學謎題的礦工能將新的區塊納入區塊鏈中。工作量證明的原理是利用嘗試錯誤法(Trial and Error)的方式重複運算，直至找出一個對的答案，亦即一個能與數學謎題(由梅克爾樹（Merkle Tree）加上前區塊的 Hash 值)相結合後，且能符合該區塊 Block Header[120]的 Hash 值(運用 SHA 256 雜湊演算法所算出)所得出的一個符合的值 [121]。這個值又稱為 Nonce[122]，是一個隨機值，他只要能與數學謎題結合後，運用 SHA 256 雜湊演算法(Hash Function)能得出在與 Block Header 的 Hash 值同樣有著規定數量的零(Zero)，即能成功驗證該區塊 [123]，謎題的難度就是透過規定必須產生多少個零來決定的，零的數量越多代表著能符合條件的 Nonce 值越少，要投入更多的算力才能找到符合條件的值。在算出能符合 Block Header Hash 值的 Nonce 後，該值就會被廣播到全部的節點，讓各個節點親自驗證到底所找到的 Nonce 值是否正確。這個驗證程序非常快，因為只要將謎題加上 Nonce 經過 SHA 256 雜湊演算法演算出符合 Block Header 的一定條件後，就算通過驗證，無須再透過嘗試錯誤法(Trial and Error)的方式重複運算。這裡提出的 Nonce 值就是該運算節點的工作量證明(Proof of Work)，能提出這個證明並且獲得所有節

---

[119] Noelle Acheson, *How Bitcoin Mining Works*? COINDESK (Jan. 29, 2018), https://www.coindesk.com/information/how-bitcoin-mining-works/.

[120] Block Header 是透過結合 Version, Previous Block Hash, Merkle Root, Timestamp, Difficulty Bits, Nonce 等因素組成。

[121] Kiran Vaidya, *Decoding the Enigma of Bitcoin*, MINING MEDIUM (Dec. 15, 2016), https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2.

[122] iThome（2016/04/23），〈區塊鏈運作原理大剖析：5 大關鍵技術〉，https://www.ithome.com.tw/news/105374（最後瀏覽日：2018/06/14）

[123] Michael Scott, *The Essence of the Blockchain*, MIRACL, https://www.miracl.com/press/the-essence-of-the-blockchain (last visited July 15, 2018).

doi:10.6342/NTU201800740

點的認同後，區塊才算經過驗證，被驗證的區塊才能被鏈入區塊鏈當中，成為難以竄改的一部份。同時能提出正確 Nonce 值的節點也才能因為有效的工作量證明而獲得工作的報酬—比特幣 [124]。比特幣作為解開數學謎題的獎勵，會自動分配予第一位正確 Nonce 值之人，惟近來因挖礦難度大幅提升，由礦工獨自以自組之電腦設備透過圖形顯示卡(Graphics Processing Unit, GPU)進行挖礦已不符合成本效益，是以大部分的礦工要不是將本身的設備連入「礦池」[125](Mining Pool)要不就是集資投資專門運算 Hash 值的 ASIC 礦機 [126]共同組成「礦場」[127]投入爭取成為第一位解出數學謎題之人。當挖礦競爭的對手從個別的節點演變成各礦場及礦池之間的競爭時，仍期待以獨自挖礦而賺取比特幣的可能性即變得微乎其微，有論者即稱現在進行挖礦之人在玩類似樂透的遊戲 [128]。為避免投入之資本成為玩樂透的門票，大部分的礦工採取以礦池的方式分工計算 Nonce 值，利用此種方式將各礦工的設備串連起來分別運算以達到計算能力的最大化。礦池以各礦工所付出的工作量證明為分配比例，當一人解出 Nonce 值獲得比特幣後，該比特幣即會按礦工所付出的工作量證明為比例分配，降低挖礦的射悻性 [129]。

比特幣只能透過「交易」（Transaction）來移轉。交易的方式分為兩種，分別是原始取得式交易（Coin-Base Transaction）和繼受取得式交易(Regular Transaction)。

---

[124] MULLER & HASIC, *supra* note 74, at 21; *What is Mining?* ANTMINER DISTRIBUTION EUROPE B.V., https://www.antminerdistribution.com/what-is-bitcoin-mining/ (last visited Aug. 12, 2018).

[125] Ofir Beigel, *What is Bitcoin Mining and is it Profitable in 2018?* 99BITCOINS, (Aug. 8, 2018, 5:18 PM), https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/.

[126] 特殊應用積體電路（Application Specific Integrated Circuit, ASIC）晶片，是一種專門為某種特定用途(如計算 Hash 值)所設計的電子電路晶片，因其提供的算力高、耗能低，故現已取代以往 GPU 的挖礦模式。

[127] 經濟日報（2018/04/05），〈比特幣礦場直擊 20 坪機房月賺 60 萬〉， https://money.udn.com/money/story/5612/3070186（最後瀏覽日：2018/07/08）

[128] Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L.J. 139, 145 (2016).

[129] ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 211-13 (2015).

doi:10.6342/NTU201800740

原始取得式交易並無交易相對人，以此種方式取得的比特幣，在交易成功前是不存在的，因此當然也就無跡可尋。礦工們透過提供算力而獲取的比特幣即屬此種方式。繼受取得式交易又稱普通交易，所交易的標的是已經被持有的比特幣，目前各大加密貨幣仲介業者所交易的加密貨幣均屬此類。透過此種交易方式而取得的比特幣因有跡可尋，故較容易受到主管機關的關注[130]。

在交易比特幣的過程中，一定會產生一個或多個輸入交易和輸出交易。所謂「輸入交易」(Transaction Input)，係比對即將執行的交易資料與該交易在分散式帳本中的前一筆交易資料之間有無違誤。唯有透過和既存在帳本內的資料比對過後，始能發現 1.交易者確實擁有其所稱擁有的比特幣；以及 2.交易者擁有更改該數額比特幣在分散式帳本上的權限[131]。上述比對的過程又稱為驗證(Validation)，前文已略有提及。利用私鑰和公鑰所為之簽名若經礦工驗證為正確時，即代表著同時符合擁有正確數額並有權執行該筆交易的兩項要件，此筆交易才會正式被加入分散式帳本中，具體過程是將所有通過驗證的交易資訊彙整成一個區塊，然後和之前已經通過驗證的區塊相結合，形成一條區塊鏈。而所謂的「輸出交易」(Transaction Output)則代表著交易者欲交易的對象和數額[132]。當輸入交易通過礦工的「驗證」後，輸出交易才會被執行。交易經執行後，比特幣的所有紀錄即隨之變更，且此變更甚難因為錯誤而撤銷。這是因為所有經驗證後的紀錄都會形成一個又一個「區塊」，每個區塊會按驗證的順序排列先後順序，形成一條「區塊鏈」，任何未經驗證的變動都將會導致區塊之間的 Hash 值不一致。但有時新區塊產生時，不代表交

---

[130] KRZYSZTOF OKUPSKI, BITCOIN DEVELOPER REFERENCE: WORKING PAPER 5-14 (July 30, 2016), https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.
[131] *Id.* at 17-19.
[132] *Transaction*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Transaction (last updated Aug. 7, 2018).

doi:10.6342/NTU201800740

易已經執行，所以一些有經驗的幣民會等待區塊完成、並且再接上至少 5 至 6 個新的區塊後，才會認同交易已經執行完成。蓋在極少數的時候，有些節點會同時找出 Nonce 的數值解開數學謎題，這時候各該節點就會同時向各個節點發布已經完成的工作證明，請求其他節點予以驗證，當其他節點驗證無誤後，就會將通過驗證的區塊更新至自己的帳本內。但是在完成此流程的同時，倘若也有另一個取得正確 Nonce 數值的區塊正在與其他節點進行驗證工作，而且也有部分節點認同驗證數值，所以將另一個區塊鏈入自身帳本，將導致部分節點接受到的區塊不一致的情況—亦即區塊鏈上的分岔(Forks)。在此情形，因為同時通過驗證的節點都會認為自己更新的區塊才是正確的區塊，所以就會無視之後無法自動延伸既有區塊鏈的區塊。解決的方式就是等待下一個先行找出新區塊的 Nonce 並解開數學謎題的節點出現，並且廣播給所有節點，經所有節點驗證後，先找出新區塊的那一條分支就會成為新的唯一一條區塊鏈，分岔的另一條分支就會跟隨新區塊鏈，而捨棄與新區塊鏈相衝突的區塊，改而採行與新區塊鏈完全相同的區塊[133]。這也是為何一個區塊的完成並不表示內含的交易資訊已經被執行。

須注意者為，分岔不表示區塊鏈內含的資訊被竄改，因為被捨棄的區塊中那些尚未被執行的交易，還會是會再次與其他待認證的交易重新被打包成一個新的、等待通過驗證的區塊。因此，因修復分岔而被捨棄的交易資訊並未被遺忘，只是優先順序被調整，其交易資訊自始未被真正執行，當然也就沒有竄改區塊鏈的說法。這樣的驗證機制能確保就算有多個節點同時解開數學謎題，並且各自將不同的區塊鏈入自己的分支，也不會造成雙重支付(Double-Spending)的問題，因為最後

[133] JOHN P. PODOLANKO ET AL., COUNTERING DOUBLE-SPEND ATTACKS ON BITCOIN FAST-PAY TRANSACTIONS (2017), http://www.ieee-security.org/TC/SPW2017/ConPro/papers/podolanko-conpro17.pdf.

doi:10.6342/NTU201800740

還是以下一個最先解開數學謎題並且讓所有節點認可的最長區塊鏈為主，其餘分支的交易會等到後續再行執行。而當執行上發現同一筆交易其實已經執行過、且餘額不足時，該筆交易就不會通過驗證，當然亦不會被整個區塊鏈群體所接受[134]。

上述機制的運作，理論上能有效避免雙重支付及被竄改的可能性，但是前提是沒有某些人士或是礦池掌握多於 50%的算力，擁有如此之多的算力而開啟的攻擊被稱之為 51%攻擊(51% Attack)。此種攻擊模式代表著有一個節點在機率上能比其他節點優先找出 Nonce 值，通過數學謎題，並且讓其他節點優先驗證錯誤的交易資訊。當然只有攻擊一個區塊是不夠的，因為有可能在所有節點通過驗證前，會有其他的節點同樣發現 Nonce 值，通過數學謎題，造成分岔。是以要確保錯誤的交易訊息被保留，除了需要有超過 50%的算力，尚須具備持續提供這些算力的能力，以確保有錯誤交易訊息的區塊鏈分支一直保持著領先的狀態[135]。歷史上曾有礦池的算力一度超過 50%，而導致使用者的憂慮，進而要求礦池為了降低公眾的顧慮而轉讓持有的算力[136]，但時至今日，各個礦池所持有的算力趨於平均，所以理論上會出現 51%攻擊的機率極低[137]。

第六項 比特幣的特性

大致分析比特幣背後的技術原理後，可以得出比特幣擁有的特性，列舉如下[138]：

---

[134] *Id.* at 2-3.
[135] MARTIJN BASTIAAN, PREVENTING THE 51%-ATTACK: A STOCHASTIC ANALYSIS OF TWO PHASE PROOF OF WORK IN BITCOIN 1-3 (2015), https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf.
[136] Pete Rizzo, *Ghash.io: We Will Never Launch a 51% Attack Against Bitcoin*, COINDESK (June 17, 2014, 11:22 AM), https://www.coindesk.com/ghash-io-never-launch-51-attack/.
[137] *Pool Distribution (calulate by blocks) Pool Stats*, BTC.COM, https://btc.com/stats/pool?pool_mode=all (last visited July 15, 2018).
[138] 林弘斌、鄧介銘（2017），〈淺談區塊鏈技術與金融區塊鏈實作驗證〉，《財金資訊季刊》，第 90

doi:10.6342/NTU201800740

1. 去中心化—比特幣的產生、分配、移轉，均完全按照程式預先所設定的藍圖運行，而推動程式運作之人，則為分散在全世界的礦工。只要有網路的地方就可能有礦工的存在，此即採用分散式帳本技術最大的特點，造就了無中心機構的虛擬貨幣架構。

2. 高流通性[139]—比特幣屬全雙向流通性虛擬貨幣，採行此種架構的虛擬貨幣除在使用者間無移轉限制，在架構的規範上更不存在如同現實貨幣匯兌的限制。比特幣同時具備易移轉、易匯兌兩種性質，再加上虛擬貨幣的無實體性質，讓使用者在全世界有網路的地方均能輕易地移轉比特幣。

3. 所有權專屬性—比特幣的移轉其實只是更改帳本上既有的資料，僅有無體財產權的變動，而非實體物的移轉，法律性質上應可理解為係一「準物權行為」。在這個準物權行為關係中，私鑰是驗證處分權有無的必要條件，取得私鑰才能等同取得移轉對應在公共帳本上的比特幣的權利，因此只要持有私鑰的比特幣所有權人不將私鑰交與或託付與他人，在此前提下，比特幣的所有權就是絕對專屬的，任何政府機構或是國際組織均無權也無法執行比特幣的所有權。

4. 帳本公開性—比特幣所採行的公鏈[140](Permissionless)區塊鏈技術，讓每個欲參與驗證過程的使用者均能下載一份從創始區塊至今的帳本。這是因為驗證區塊的完整性需要知道前一筆交易的正確性，所以唯有將完整的交易紀錄歷史公開，才能達到准許每個人自由參與的結果。載至 2018 年 6 月，全世界已累

期，頁 22。

[139] *What is Cryptocurrency: Everything You Need To Know [Ultimate Guide]*, BLOCKGEEKS, https://blockgeeks.com/guides/what-is-cryptocurrency/ (last visited July 11, 2018).

[140] Ramesh Gopinath, *Checking the Ledger: Permissioned vs. Permissionless Blockchains*, IBM (July 28, 2016), https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-blockchains/.

doi:10.6342/NTU201800740

計的帳本資料量已達 173 千兆位元組[141] (173 GB)，任何人均能下載並檢視自始至今的所有交易紀錄。

5. 匿名性—雖然因為公鏈的緣故，使得交易紀錄與帳本公開化，但是使用者並不會因此完全喪失隱私，暴露在公眾的眼裡。比特幣利用「去連結」的方式，讓使用者在一定程度內達成半匿名的效果，其缺失是一旦建立「身分連結」，則過往的交易紀錄將無所遁形，故此種半匿名性的交易又被理解為「化名性匿名」(Pseudonymity)。欲建立身分連結，本文於後文有提倡從交換者著手，建立加密貨幣錢包對應真人的資料庫，再對於接受使用加密貨幣付款的商家進由發放許可的方式取得國內加密貨幣最終可能流入的對象。藉由監理科技整合上述兩項訊息將有可能將加密貨幣的使用者及所移轉的對象進行連結，追蹤金流。

第七項 加密貨幣與網路犯罪的關聯

比特幣由於採取全雙向流通性虛擬貨幣架構，因此現實貨幣能自由地與虛擬貨幣匯兌。在虛擬貨幣的洗錢防制架構尚未健全的今日，如何避免虛擬貨幣被濫用以及如何配置相對應的配套措施，即成為國際關注的議題。貝萊德集團的執行長勞倫斯•芬克曾表示:「比特幣的湧現讓我們看清了到底有多少洗錢的需求[142]。」英國財政部根據英國國家犯罪調查局的研究亦指出：「不排除透過小額大量匯兌虛擬貨幣的方式洗錢[143]」，肯認了虛擬貨幣對於洗錢犯罪的助益。

---

[141] *Size of the Bitcoin blockchain from 2010 to 2018*, STATISTA.COM, https://www.statista.com/topics/2308/bitcoin/ (last visited Aug. 15, 2018).

[142] Fred Imbert, *Blackrock Ceo Larry Fink Calls Bitcoin an 'Index Of Money Laundering'*, CNBC (Oct. 13, 2017), https://www.cnbc.com/2017/10/13/blackrock-ceo-larry-fink-calls-bitcoin-an-index-of-money-laundering.html.

[143] Jon Buck, *Bitcoin Low Risk for Money Laundering, High For Cybercrime: UK Treasury*, COINTELEGRAPH (Oct. 29, 2017), https://cointelegraph.com/news/bitcoin-low-risk-for-money-laundering-

doi:10.6342/NTU201800740

以比特幣為例，因為其同時具備隱密性、便捷性、缺乏中心機構的監理等特質，所以不乏犯罪者利用其作為勒索取贖的對價。如烏克蘭於 2016 年 12 月 26 日所發生的一宗綁架案即要求被害人支付價值一百萬美元的比特幣作為贖款[144]。該起事件的綁架犯後來雖依約放人，但目前仍未有任何關於案情的後續發展。又如 2017 年 5 月開始發酵的 WannaCry 勒索病毒，亦是以比特幣作為取贖的方式[145]，比特幣獨特的高度化名性、傳輸便捷性的特性，使駭客得以大量、制式化的方式向中了勒索病毒的受害者要求支付贖金。第一波的攻擊總共累積了 52.2 BTC，當時價值美金約 14 萬美金 ，但各國執法機構卻無法有任何作為，更遑論對該筆款項進行沒收[146]。如今造成該次全球性的駭客仍未落網，且就技術上而言，犯罪者只要避免將比特幣與現實貨幣相互連結，就不太可能被追蹤到其真實的身分。又或著駭客能等到法律追訴期經過後再行轉換該筆贓款，以規避主管機關的查緝[147]。

除多元的網路犯罪態樣外，比特幣還是暗網交易的通用貨幣。所謂暗網，係指透過特殊加密程序，使搜尋引擎無法查詢的網路。暗網隱藏在日常網路使用者接觸的網路範圍之外，使用者需透過特殊的網路協定才能進行訪問。暗網與一般網站最大的不同，在於其隱密性，因為在暗網裡廣泛使用的 Tor 協定技術，讓一般

---

high-for-cybercrime-uk-treasury.

144 Matthias Williams, *Ukraine Kidnappers Free Bitcoin Analyst After $1 Million Ransom Paid*, REUTERS (Dec. 30, 2017), https://www.reuters.com/article/us-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-mln-ransom-paid-idUSKBN1EN1QB.

145 *What You Need to Know about the WannaCry Ransomware*, SYMANTEC (Oct. 23, 2017), https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack; *WannaCry Ransomware Bitcoins Move from Online Wallets*, BBC (Aug. 3, 2017), http://www.bbc.com/news/technology-40811972.

146 Ryan Browne, *Hackers Have Cashed Out on $143,000 of Bitcoin From the Massive Wannacry Ransomware Attack*, CNBC (Aug. 3, 2017, 11:09 AM), https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-bitcoin-from-the-massive-wannacry-ransomware-attack.html.

147 若不考慮特別法或是國際公約的情況下，我國刑法對於網路勒索最有可能涉及之條文，為刑法第 346 條第 1 項之恐嚇取財罪以及第 359 條之妨害電腦使用罪。兩罪均為五年以下有期徒刑之罪，按刑法第 80 條第 2 項之規定，追訴權於二十年內未起訴而消滅。

doi:10.6342/NTU201800740

執法機構就算知道違法交易平台的存在，卻不具備找出背後始作俑者的能力。

著名暗網網站「絲路」即利用暗網的隱密性公開地兜售毒品，交易所使用的貨幣多為易移轉但又不會暴露買受人及出賣人身分的比特幣[148]。該網站曾在 2013 年 10 月 2 日被美國聯邦調查局(Federal Bureau of Investigation, FBI)以打擊犯罪為由封網，並逮捕創始人 Ross William Ulbricht[149]。但該網站的 2.0 版本於 2013 年 11 月重新上線，同樣公開地販售大量毒品、違禁物、非法服務等等。2014 年 10 月 6 日聯邦調查局和歐盟聯合再次關閉其 2.0 版本，但是 3.0 版本隨後再次上線，一直到今日仍無法杜絕[150]。此種以暗網為基礎的網路交易平台提供了犯罪者一個安全、便利、多客源的交易環境。而比特幣可以說是間接促使暗網交易的幕後黑手，蓋其所提供的化名式匿名，使買受人能輕鬆支付欲購買的服務，無須擔心執法單位循金錢流向反查到自己。出賣人更喜歡使用比特幣作為支付的價金，因為比特幣較無被執法單位中途查緝、沒收、或是被同行在交易過程中反搶的問題。

第八項 加密貨幣與洗錢的關聯

美國緝毒局(Drug Enforcement Administration, DEA)2017 年 10 月所公布的國家毒品威脅評估報告中，對於比特幣洗錢的議題顯得相當重視。該報告指出全美毒品的販賣所得為 640 億美金，占全美國總不法所得 3000 億美金的百分之二十一，而這些錢大多數都是以現金形式呈現，因此要如何才能有效運用如此大量的現金，

---

[148] Axel Bugge, *Dark Web Drug Market Growing Rapidly in Europe: Report*, REUTERS (Nov. 29, 2017), https://www.reuters.com/article/us-europe-drugs-darkweb/dark-web-drug-market-growing-rapidly-in-europe-report-idUSKBN1DS28A.

[149] Greenspan, *supra* note 104.

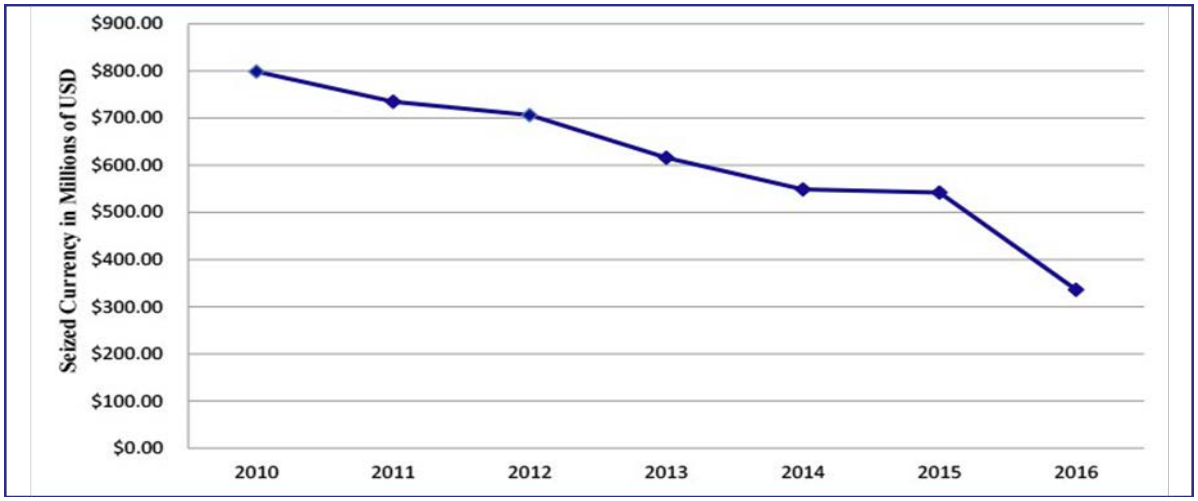
[150] James Cook, *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*, BUSINESS INSIDER (Nov. 6, 2014, 10:56 AM), https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11.

doi:10.6342/NTU201800740

即成為一個現實問題[151]。跨國犯罪組織(Transnational Criminal Organizations, TCOs)為了將現金移轉，可能採取任何以下的方式：

1. 將不法所得以現金的方式從 A 地點夾帶至 B 地點；
2. 將不法所得注入銀行系統，利用其進行洗錢；
3. 利用空殼公司或其他手法將不法所得偽裝成合法的所得。

犯罪組織以往慣用的手法為第一種方式，即利用大量來往美國的旅客夾帶不法所得出境。蓋此種方式較為簡便，無須過多的技術及規劃，即可規避美國金融犯罪稽查局(FinCEN)所訂定之超過一萬美元[152]即應申報的手續[153]。但是因為歷年來查緝技術、手段的升級，運輸現金的風險越來越大，一旦被查獲則將面臨全數不法所得被沒收的風險。



圖片來源：El Paso Intelligence Center/ National Seizure System

圖 五：美國 2010-2016 年所查緝之現金數額

上圖顯示美國歷年查緝的金錢數目，從 2010 年至 2016 年止，每年被海關所

[151] U.S. DEP'T JUST., DRUG ENF'T ADMIN., 2017 NATIONAL DRUG THREAT ASSESSMENT DEA-DCT-DIR-040-17 (2017), https://www.dea.gov/sites/default/files/docs/DIR-040-17_2017-NDTA.pdf.

[152] *Currency and Monetary Instruments - Amount That Can be Brought into or Leave the U.S.*, U.S. CUSTOMS AND BORDER PROTECTION (June 16, 2016), https://help.cbp.gov/app/answers/detail/a_id/195/.

[153] 31 U.S.C. 5316 and Treasury Department regulations (31 CFR Chapter X).

doi:10.6342/NTU201800740

查獲的不法所得，基本上呈現遞減的狀態。造成此現象的主因並非毒梟藏匿不法所得的手法提升，使得執法單位無法再像以前一樣沒收應申報而未申報的現金；而是毒梟已經開始減少運用傳統的方式將不法所得攜帶出境[154]。報告指出，近來洗錢手法的精進，使得毒梟開始運用金錢或價值移轉服務(Money Value Transfer System, MVTS)、貿易洗錢(Trade-Based Money Laundering, TBML)、傳統銀行(Formal Banking System)和虛擬貨幣進行洗錢[155]。因此，最傳統的金錢運輸方式漸漸顯得多餘、費時且不可靠。從 2010 年至 2016 年間所查獲的現金數額觀之，六年間查獲的現金數額減少了一半以上[156]。假設這六年來美國海關及邊境保衛局並無任何經費短少、懈怠、裁員等情形，此數據顯示六年間毒梟已逐漸揚棄攜帶現金闖關的洗錢模式，至少有二分之一以上的不法所得已經透過他種類的管道進行洗錢。

根據美國緝毒局的觀察，由於目前僅少數先進國家有針對虛擬貨幣制定法律規範，多數國家尚未著手立法，使得犯罪組織有機會利用監管漏洞進行洗錢，因此跨國犯罪組織有將貿易洗錢與比特幣洗錢相結合的趨勢。美墨跨國犯罪組織(下稱 TCOs)以往所使用的傳統貿易洗錢模式，是先由 TCOs 向中國商人購買大量中國製造的產品，通常會以電匯或是現金付款，而購買來的貨物則會運送至墨西哥或是南美洲的商人手上轉賣變現[157]。如下圖：

---

154 U.S. DEP'T JUS., DRUG ENF'T ADMIN., *supra* note 151, at 125.
155 *Id.*
156 *Id.* at 126.
157 *Id.* at 130.

doi:10.6342/NTU201800740

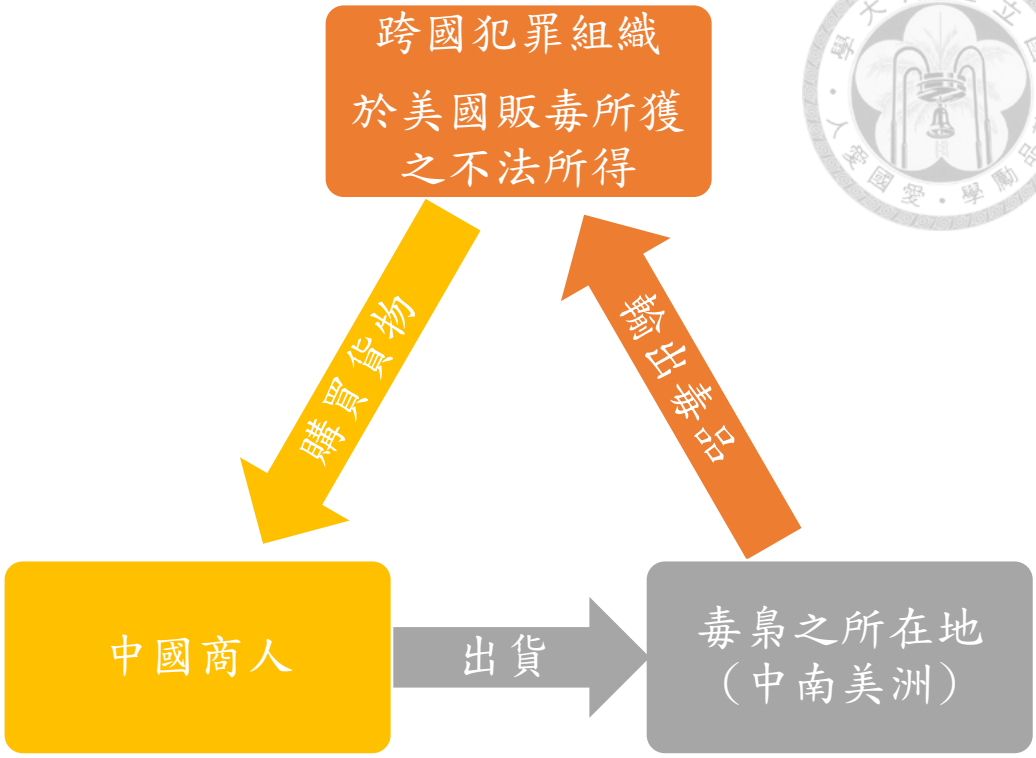


圖 六：跨國犯罪組織所使用的傳統貿易洗錢模式

但是越來越多的中國商人喜歡以比特幣作為購買貨物的對價[158]，因為比特幣的匿名性和便利性，使得中國商人更容易規避政府當局的貨幣政策，從而使得賺取的貨幣能更輕鬆地在各國間移轉、取用，如此一來無異使得 TCOs 更容易洗錢，兩者一拍即合。原先 TCOs 尚須面臨如何規避主管機關的稽查、以利用電匯的方式將美元移轉至位於中國的出口商手中。現在 TCOs 僅需向有牌照的虛擬貨幣匯兌業者[159]購買比特幣，或是更有甚者，直接向礦工購買比特幣後，再利用比特幣向中國商人進行交易，完全規避主管機關的監察[160]。交易架構如下：

---

158 *Id.*
159 金融服務商的一種。詳細論述，參照：本文第四章二節三項立法解釋以下之論述。
160 U.S. DEP'T JUS., DRUG ENF'T ADMIN., *supra* note 151, at 130.

doi:10.6342/NTU201800740

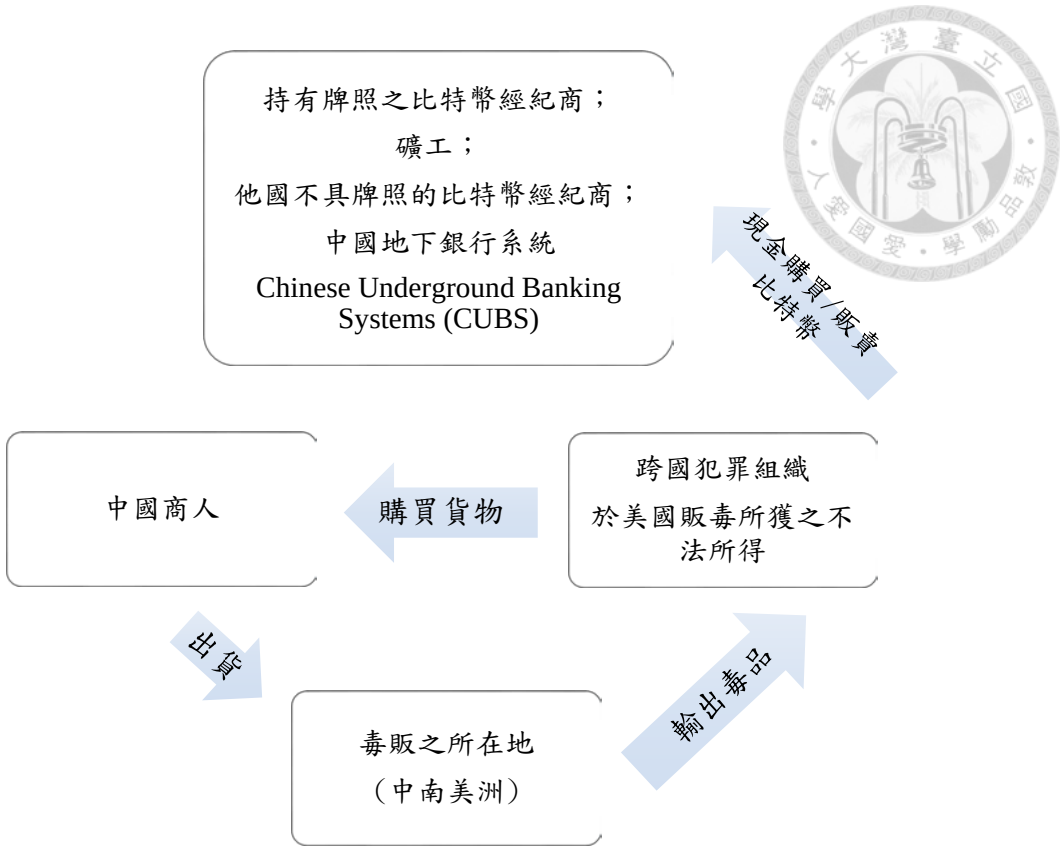


圖 七：跨國犯罪組織所使用的加密貨幣混合貿易洗錢模式

在此種新式的洗錢結構中，跨國犯罪組織能更輕易地利用比特幣搭配以往的貿易洗錢模式，使得執法機關更不易查緝。TCOs 除了選擇用銀行轉帳的方式與有牌照的經紀商交易外，更有可能選擇私自販售比特幣的礦工、不具牌照的比特幣經紀商以及所謂的中國地下銀行系統(Chinese Underground Banking Systems, CUBS)。之所以不傾向與有牌照的比特幣經紀商進行交易，是因為該等經紀商已受政府的監管，必須依照主管機關的指示去瞭解是誰在匯兌虛擬貨幣(KYC)和盡職調查(CDD)，多少會有不必要的風險存在。但若是轉向私自販售比特幣的礦工，或是主機並非設立在美國的比特幣經紀商或交換商交易比特幣的話，則可規避被執法機關察覺有多少現金被轉換成比特幣的風險[161]。

[161] *Id.*

doi:10.6342/NTU201800740

最後一種中國地下銀行系統(CUBS)推測會是最受中國商人歡迎的方式，因為中國國民受限於政策因素，導致外匯上有周轉問題，若是先讓中國境內的礦場生產比特幣，透過與 CUBS 合作的方式，即可順利將比特幣賣予位於美國的 TCOs。CUBS 於美國收受大量無法利用正常管道匯出的美金，即能與位於中國但想移轉資產至海外的商人合作，僅需在中國境內支付相對應的人民幣或是比特幣，位於美國的現金即能立刻放行 [162]，將在中國境內的金錢移轉至海外。此服務如此便利，可想而知，對於想移民至美國的中國人，或是想赴美留學的華人具有特別的吸引力。

綜上所述，比特幣洗錢和貿易洗錢結合能達成的效果有二：1. 將大量位於中國的資產移轉至國外；2.將不易移轉的現金透過轉換成比特幣的方式移轉。

第三節　小結

本章從數位貨幣著手，分別探討電子貨幣及虛擬貨幣兩項子類別，兩者最主要的區別在於「電子貨幣」，是一種現金的替代制度，其將具法償性質的現實貨幣數位化，進而轉換成為在開放性網路的數位世界中，以電子形式的「現金」直接進行交易，如同在實體世界中的現金；虛擬貨幣則不具法償功能。虛擬貨幣為非由中央銀行、信用機構或是電子貨幣機構發行，由某一團體認可，且在某些情形下能用於替代貨幣，且以數位形式呈現的價值。其又可按准許與現實貨幣兌換的架構細分為封閉性虛擬貨幣架構、單向流通性虛擬貨幣架構、以及雙向流通性虛擬貨幣架構。本文認為每種架構又可按「是否准許於架構內流通」細分為半封閉、半單向、半雙向流通性虛擬貨幣架構，區分實益在於將每種架構按照可能被洗錢

[162] *Id.*

doi:10.6342/NTU201800740

犯罪所利用的風險加以排列，將能落實 FATF 以風險為基礎的洗錢防制政策，對於較低風險之虛擬貨幣架構如完全封閉性、半封閉性、全單向流通性虛擬貨幣架構採行低度或是完全無需採行洗錢防制的政策；對較高風險之虛擬貨幣架構如半單向流通性虛擬貨幣架構、半雙向流通性虛擬貨幣架構、全雙向流通性虛擬貨幣架構則可按被洗錢犯罪所利用的潛在風險排列。本文亦舉例說明上述架構尚有可能再以准許虛擬貨幣與虛擬貨幣間相互匯兌以規避原先架構上之限制，是以對此類架構特別加上「可轉換」的標籤。具可轉換性質的匯兌架構在洗錢風險的評定上會較採行同類虛擬貨幣之匯兌架構來得高。最終本文認為全雙向流通性虛擬貨幣架構被洗錢犯罪所利用的風險最高，故接下來以採行此類匯兌架構之虛擬貨幣為主要探討對象。

全雙向流通性虛擬貨幣架構之虛擬貨幣於規範上又以採行區塊鏈技術的加密貨幣為本文欲關注的對象，主要原因在於其所採行的區塊鏈屬於分散式帳本的一種資料結構，但透過特殊的密碼學及演算法，能達成去中心化、去中介化、化名式匿名等難以規範且為洗錢犯罪或其他犯罪所喜愛的特性。惟並非所有類型的加密貨幣均有可能被洗錢犯罪所利用，是以本文從區塊鏈技術的世代為分界線，依據不同世代的區塊鏈所產生不同種類應用的加密貨幣為論述對象，試圖縮小本文欲討論之加密貨幣範圍。本文將採行第一代區塊鏈技術之加密貨幣稱為貨幣型加密貨幣，因其屬區塊鏈技術最基礎的應用，最主要之功能為記帳，故最容易被用於移轉價值。有鑒於價值移轉服務被洗錢犯罪所利用的風險較高，後續爰以貨幣型加密貨幣為主要探討對象。貨幣型加密貨幣又可按所採行之區塊鏈架構細分為公鏈架構、全私鏈架構與半私鏈架構，因不同種類的架構對於參與者能成為節點的自由度及參與後具有的帳本存取權限各不相同，爰於分析三種區塊鏈架構後以

doi:10.6342/NTU201800740

最具參與自由、最難破除匿名性、洗錢風險相對高之公鏈型加密貨幣為主要研究對象。職是之故，本文隨後以公鏈型加密貨幣之最佳代表—比特幣為例，介紹加密貨幣運作之方式及可能被洗錢犯罪所利用之特性，以建立加密貨幣與洗錢之間的關聯性。最後結果顯示，目前加密貨幣實務上已有與貿易洗錢整合之例。對此類因金融科技的發展所興起之新興洗錢手法，我國洗錢防制法是否具備處罰能力？是否能對此類利用加密貨幣進行洗錢犯罪之犯罪所得沒收？若加密貨幣因故滅失能否追徵替代物或是價額？若法律操作上可行，實務操作是否亦可行？管制層面及執行層面是否有對應之措施使得洗錢防制法得以落實？以上僅就種種加密貨幣對我國洗錢防制法可能造成的問題與衝擊稍作舉例，惟加密貨幣所涉及之法律議題並非止步於洗錢防制議題。例如美國法上執掌金融犯罪之主管機關—金融犯罪稽查局(FinCEN)從洗錢防制之觀點出發，將加密貨幣認定為交易媒介(medium of exchange)而納入銀行保密法加以規範[163]；美國證券交易委員會(SEC)曾於 SEC v. Shavers 一案中表明「加密貨幣是貨幣或是金錢的一種型態[164]」；美國商品期貨交易委員會(CFTC)則將加密貨幣認定為是一種商品或是有價證券[165]；美國聯邦選舉委員會(FEC)另將加密貨幣當成是一種捐款[166]；美國國家稅務局(IRS)則是將加密貨幣當成是須課稅的客體[167]。美國之例顯示了各監理機關均從所執掌項目出發，分別對於加密貨幣採行不同的定性與管制模式。本文為深入探究加密貨幣之洗錢防制議題，爰參考美國之定性方式，暫且將加密貨幣作為有價值之交易媒介看待，並於第三章探討此種交易媒介對於我國洗錢防制法所造成之衝擊。

---

[163] 詳細論述，參照：本文第四章第二節第三項。
[164] Laura D. Pond, *Schrödinger's Currency: How Virtual Currencies Complicate the RIC and REIT Qualification Requirements*, 9 Colum. J. Tax L. 229, 240-241 (2018).
[165] *Id.* at 240.
[166] *Id.*
[167] *Id.*

doi:10.6342/NTU201800740

第參章　加密貨幣的洗錢防制問題

第一節　洗錢防制的規範架構

第一項 洗錢防制之罪刑架構

我國於 2016 年 12 月 28 日所修正之洗錢防制法，主要係參酌防制洗錢金融行動工作組織（Financial Action Task Force，以下簡稱 FATF）於 2012 年發布之防制洗錢及打擊資助恐怖主義與武器擴散國際標準的四十項建議（以下簡稱 FATF 四十項建議）[168]與巴勒摩公約 (the Palermo Convention)[169]，旨在重建金流秩序，特別是落實公、私部門在洗錢防制之相關作為，以強化我國洗錢防制體質，並增進國際合作，從而達到阻斷罪犯之不法金流，徹底杜絕犯罪的目標[170]。

為達上述目標，我國新洗錢防制法除擴大洗錢防制法之適用範圍、增加刑度外，更是增加沒收犯罪所得之範圍[171]、要求有更嚴格的紀錄保存規定[172]、針對重要政治性職務之人(Politically Exposed Person, PEPs)及關係人進行加強審查[173]、針對來自高風險國家之客戶或金融機構採取有效的風險防制措施[174]、遵守保密與申報義務[175]、針對指定非金融事業或人員(DNFBPs)進行盡職調查[176]、針對現金攜帶

---

[168] 行政院洗錢防制辦公室（2016），〈洗錢防制法修正條文對照表修正說明〉，http://www.amlo.moj.gov.tw/HitCounter.asp?xItem=467286&ixCuAttach=161358（最後瀏覽日：2018/06/24）

[169] Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Nov. 15, 2000, S. Treaty Doc. No. 108-16 (2004), 2237 U.N.T.S. 319, http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

[170] 立法院法律系統，〈洗錢防制法現行法異動條文及理由〉。載於，http://lis.ly.gov.tw/lglawc/lglawkm（最後瀏覽日：2018/06/24）

[171] FATF 建議 3。

[172] FATF 建議 11。

[173] FATF 建議 12。

[174] FATF 建議 19。

[175] FATF 建議 21。

[176] FATF 建議 22。

doi:10.6342/NTU201800740

之申報或違反揭露義務者做出規範[177]。就加密貨幣初期會面臨之主要洗錢防制問題，與如何適用洗錢防制法、如何沒收、加密貨幣服務商(MSB)於洗錢防制法上之定位等問題有關，是以本章擬先就洗錢防制法欲處罰之態樣以及洗錢防制法之沒收加以分析，以便檢視加密貨幣對於我國洗錢防制法會造成何種衝擊？以及有無適用上之問題？

我國現行洗錢防制法所欲處罰的態樣約略可區分為以下類型[178]：

1. 為自己特定犯罪而洗錢(洗錢防制法§§2、3⑬、14)；
2. 為他人特定犯罪而洗錢(洗錢防制法§§2、3、14)；
3. 資助恐怖活動(洗錢防制法§§2、3、14；資恐防制法§9)；
4. 持有來源不明的財產(洗錢防制法§15)。

就上述洗錢態樣，又可依構成要件進一步區分為一般洗錢罪與特殊洗錢罪[179]。就一般洗錢罪而言，洗錢防制法第 2 條先定義了洗錢行為，再按 FATF 四十項建議中的第 3 項建議，於第 3 條 1 項 1 款降低特定犯罪之概括門檻，並於其後款項列舉其餘會構成洗錢行為的前置特定犯罪。而所謂的特殊洗錢罪，則係於洗錢防制法第 2 條所設之洗錢行為以外，另於第 15 條訂定特別犯罪構成要件。以下分述之：

第一款 一般洗錢罪

洗錢此一行為的定義，係規定於洗錢防制法第 2 條，共分 3 款。第 1 款為洗錢罪之意圖犯，該款規定一方面參酌維也納公約第 3 條第 1 項第 b 款第 i 目所列舉之「移轉財產」態樣[180]，將刑事不法所得移轉予他人列為客觀要件，一方面增添

---

[177] FATF 建議 32。

[178] 王皇玉（2103），〈洗錢罪之研究—從實然面到規範面之檢驗〉，《政大法學評論》，第 132 期，頁 225-232；古承宗（2017），〈洗錢刑法的正當性依據──兼論當代刑事政策的變異〉，《犯罪、資恐與洗錢：如何有效訴追犯罪？》，頁 263-308。

[179] 古承宗，同前註，頁 267。

[180] The conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with subparagraph a) of this paragraph, or from an act of participation

doi:10.6342/NTU201800740

「意圖」的主觀特殊構成要件，使得犯罪構成要件更為寬鬆，不待達成隱匿效果的洗錢目的，即可構成洗錢罪[181]。所謂意圖洗錢罪中之意圖，為特別構成要件，按新古典暨目的論之犯罪體系理論之觀點，故意與意圖要素均被定位為犯罪構成要件之階層[182]，兩者同屬主觀構成要件要素。而對於像第 1 款之意圖洗錢罪，僅有洗錢故意無法成罪，尚須同時具備洗錢故意與意圖始構成洗錢犯罪。至於意圖之定義，我國有學者認為是：「行為人出於特定之犯罪目的，而努力謀求構成要件之實現，或希求構成要件所預定之結果發生，以達其犯罪目的之主觀心態[183]。」行為人祇要基於特定犯罪目的，而著手實行客觀之構成犯罪事實者，即有意圖之存在，至於行為人所意圖之內容，亦即其所追求之犯罪目的能否實現，則在所不問；我國實務亦採此見解，認為某些特殊犯罪之構成要件如明文以「意圖」為其成立要件，除須在著手時認知到有犯罪構成事實，且仍決定為其行為之意思外，尚須滿足有此不法動機—亦即法定之不法意圖—的要件，始能加以論罪[184]。洗錢防制法於第 2 條第 1 款增訂意圖的特殊主觀要件，雖然限縮了積極的直接故意要件，但實際上較舊法之打擊範圍更為廣泛，蓋其不以受有利益的結果犯作為定罪要件，而改以處罰意圖犯的方式來遏止洗錢犯罪。

洗錢防制法第 2 條第 2 款亦參酌維也納公約第 3 條第 1 項第 b 款第 ii 目[185]規

---

in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions.

[181] 洗錢防制法第 2 條第 1 款：「意圖掩飾或隱匿特定犯罪所得來源，或使他人逃避刑事追訴，而移轉或變更特定犯罪所得者。」

[182] 吳致勳（2015），《財產犯罪主觀要件之研究》，東吳大學法學院法律學系碩士論文，頁 20-25。

[183] 林山田（2008），《刑法通論（上）》，作者自版，2008 年 1 月十版，頁 281-282。

[184] 93 台上 4798 號判決

[185] The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with subparagraph a) of this paragraph or from an act of participation in such an offence or offences.

doi:10.6342/NTU201800740

定，將洗錢態樣增訂為包含「隱匿或掩飾特定犯罪所得之本質、來源、所在地、處置、轉移、相關的權利或所有權」等犯罪行為，並且同樣去除舊法規定必須「受有利益」之要件，亦即不待受有利益亦可處罰之。由此可見，如今新法已將洗錢罪從過往的結果犯立法模式，徹底轉換為行為犯的立法模式；亦即犯罪行為一經著手實行，於其行為完成時其所犯之罪即告成立，並不待任何結果發生。

洗錢防制法第 2 條第 3 款則是參考聯合國禁止非法販運麻醉藥品和精神藥物公約[186]第 3 條第 1 項第 c 款[187]之規定，針對主觀上明知或可得而知所收受、持有或使用之標的為特定犯罪之所得加以處罰，從而將可能輔助洗錢的專業人士或是關係人納入洗錢犯罪的框架內，以便在最大的程度內警醒受益人。

洗錢防制法第 3 條另外詳細列舉了該法所欲規範洗錢活動的「特定犯罪」。新法參考 FATF 四十項建議之第 3 項建議，保留門檻式規範，並按照 FATF 將門檻大幅降低至最低標準應至少採取最重本刑為 1 年以上有期徒刑之罪或最輕本刑為 6 個月以上有期徒刑之罪的建議，從當中較嚴格者。現行洗錢防制法第 3 條第 1 項已明定最輕本刑為 6 個月以上有期徒刑以上之刑之罪，即屬第 2 條所稱之特定犯罪。除此之外，同法第 14 條亦明文將第 2 條各款之罪之未遂犯加以入刑，綜合觀察可知我國立法者欲擴大洗錢行為之決心。

---

[186] UN Convention against Illicit Traffic, *supra* note 14.

[187] c) Subject to its constitutional principles and the basic concepts of its legal system: i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from an offence or offences established in accordance with subparagraph a) of this paragraph or from an act of participation in such offence or offences; ii) The possession of equipment or materials or substances listed in Table I and Table II, knowing that they are being or are to be used in or for the illicit cultivation, production or iii) Publicly inciting or inducing others, by any means, to commit any of the offences established in accordance with this article or to use narcotic drugs or psychotropic substances illicitly; iv) Participation in, association or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

doi:10.6342/NTU201800740

第二款 特殊洗錢罪

洗錢防制法第 15 條[188]不同於第 2 條[189]普通洗錢罪之處，在於少了前置犯罪（Predicate Offense）的要件，亦即不以犯現行條文第 3 條[190]所定之特定犯罪為前提。

一般洗錢罪之構成要件，原則上以犯第 3 條所列舉之特定犯罪為前提，以合理化洗錢犯罪之入罪。此一要件在幾次修法後，門檻已大幅降低，進而擴大了適用範圍，且第 2 條所稱之洗錢行為並不以第 3 條之前置犯罪已經有罪判決確定為必要，僅需有證據證明洗錢行為與特定犯罪有所連結即可。

惟即便如此，建立特定犯罪與洗錢行為有所關聯仍非易事，蓋「從犯罪者之

---

[188] 洗錢防制法第 15 條（罰則）
收受、持有或使用之財物或財產上利益，有下列情形之一，而無合理來源且與收入顯不相當者，處六月以上五年以下有期徒刑，得併科新臺幣五百萬元以下罰金：
一、冒名或以假名向金融機構申請開立帳戶。
二、以不正方法取得他人向金融機構申請開立之帳戶。
三、規避第七條至第十條所定洗錢防制程序。
前項之未遂犯罰之

[189] 第 2 條（洗錢之定義）
本法所稱洗錢，指下列行為：
一、意圖掩飾或隱匿特定犯罪所得來源，或使他人逃避刑事追訴，而移轉或變更特定犯罪所得。
二、掩飾或隱匿特定犯罪所得之本質、來源、去向、所在、所有權、處分權或其他權益者。
三、收受、持有或使用他人之特定犯罪所得。

[190] 第 3 條（特定犯罪）
本法所稱特定犯罪，指下列各款之罪：
一、最輕本刑為六月以上有期徒刑以上之刑之罪。
二、刑法第一百二十一條第一項、第一百二十三條、第二百零一條之一第二項、第二百六十八條、第三百三十九條、第三百三十九條之三、第三百四十二條、第三百四十四條、第三百四十九條之罪。
三、懲治走私條例第二條第一項、第三條第一項之罪。
四、破產法第一百五十四條、第一百五十五條之罪。
五、商標法第九十五條、第九十六條之罪。
六、廢棄物清理法第四十五條第一項後段、第四十七條之罪。
七、稅捐稽徵法第四十一條、第四十二條及第四十三條第一項、第二項之罪。
八、政府採購法第八十七條第三項、第五項、第六項、第八十九條、第九十一條第一項、第三項之罪。
九、電子支付機構管理條例第四十四條第二項、第三項、第四十五條之罪。
十、證券交易法第一百七十二條第一項、第二項之罪。
十一、期貨交易法第一百十三條第一項、第二項之罪。
十二、資恐防制法第八條、第九條之罪。
十三、本法第十四條之罪。

doi:10.6342/NTU201800740

角度觀察，犯罪行為人為避免犯行遭查獲，會盡全力滅證，但對於犯罪之成果即犯罪所得，反而會盡全力維護[191]」。是以，特殊洗錢罪之作用在於輔助執法機關，當其無法透過偵查的方式將不法金流與特定犯罪相互連結時，仍有法律明文規定，准許其以洗錢罪之「前前置」行為為構成要件，不再討論已識別之不法金流之前置特定犯罪為何，而是以第 15 條所列舉之 3 款已明顯與洗錢防制規定相悖且有意規避洗錢防制之行為為構成要件，以便處罰刻意規避洗錢防制規定而取得不明財產之人。

第二項 洗錢防制之沒收架構

洗錢防制法之沒收架規範於第 18 條，第 1 項修正理由參照 FATF 四十項建議之第 4 項應「允許沒收洗錢犯罪行為人洗錢行為標的之財產」的建議，此擴張了較舊法下的沒收客體，不再限於僅能對「犯罪所得財物或財產上利益」而為沒收。洗錢防制法第 18 條 2 項則參考 2014 年歐盟沒收指令第 5 條、德國刑法第 73d 條及第 261 條、奧地利刑法第 20b 條第 2 項及第 165 條等規定，引進擴大沒收制度。第 18 條 3 項則基於平等互惠原則，當外國政府、機構或國際組織依第 21 條所簽訂之條約或協定請求我國扣押或沒收之案件符合第 3 條所列之罪時，即使我國並未偵查或審判該案件，亦得為沒收。上述洗錢防制法 18 條第 1 款及第 2 款為規範於洗錢防制法的沒收規定，惟另有刑法第 38 條及第 38-1 相競合的問題。我國學者對洗錢防制法與刑法的沒收規定已多有討論[192]，以下僅就加密貨幣可能涉及之沒收規定簡單介紹：

洗錢犯罪過程中可能涉及之金錢、財產流通依學說分類可區分成三類，其中

---

[191] 洗錢防制法第 15 條修正說明。

[192] 楊雲驊、林麗瑩（2017），〈洗錢犯罪不法所得之沒收〉，《新洗錢防制法─法令遵循實務分析》，頁 60。

doi:10.6342/NTU201800740

「洗錢行為客體」和「洗錢的對價報酬」兩類分別規定於第 18 條第 1 項，另一類「其他不明財產」則規範於第 18 條第 2 項。[193]

第一款 洗錢行為客體

洗錢防制法第 18 條第 1 項前段謂：「犯第 14 條之罪，其所移轉、變更、掩飾、隱匿、收受、取得、持有、使用之財物或財產上利益，沒收之」。此項即一般洗錢罪的沒收規定，只要符合第 2 條各款洗錢行為，即該當第 14 條之罪，即可沒收。洗錢防制法第 18 條 1 項後段謂：「犯第 15 條之罪，其所收受、持有、使用之財物或財產上利益，亦同」。表明了犯罪者只須符合特殊洗錢罪以下三款要件：冒名或以假名向金融機構申請開立帳戶、以不正方法取得他人向金融機構申請開立之帳戶、以及規避第 7 條至第 10 條所定洗錢防制程序，再加上無法證明財物或財產上利益之來源或是證明與收入相當，即可沒收。

按第 18 條 1 項前後段宣告沒收之意旨，沒收之對象均為「洗錢行為客體」，又稱之為「洗錢行為標的」[194]。所謂洗錢行為客體，係指犯罪行為人透過前置犯罪所取得之犯罪所得，其後滿足第 14 條及第 15 條所謂之洗錢行為的構成要件。該洗錢行為客體，按一般洗錢罪與特殊洗錢罪的構成要件不同，分別以第 18 條 1 項前段與後段予以沒收。

第二款 洗錢的對價報酬

至於第二類「洗錢的對價報酬」，有學者認為這類的對價報酬通常發生在第三人協助前置犯罪行為人洗錢的過程中，屬觸犯洗錢罪的犯罪所得，為因應刑法沒

---

[193] 許恒達（2017），〈洗錢防制法新修正沒收規定之檢討〉，《犯罪、資恐與洗錢：如何有效訴追犯罪？》，頁 228。

[194] 薛智仁（2017），〈評析洗錢罪之沒收規定〉，《犯罪、資恐與洗錢：如何有效訴追犯罪？》，頁 315。

doi:10.6342/NTU201800740

收專章的修正，故不另行於洗錢防制法中予以規定，直接回歸適用刑法[195]。此類「洗錢的對價報酬」因非洗錢犯罪主要欲掩飾之對象，而是做為誘因，使他人願意幫助或是從事洗錢犯罪，對於此類充作報酬之不法所得亦應予沒收，若原物已滅失，則應追徵其價額。蓋無論沒收之性質係採取刑罰說、保安處分說、獨立刑事制裁手段說、準不當得利的衡平措施說、二元說－刑罰兼保安處分性質說等[196]，從沒收的最大公因數切入，種種學說皆不樂見因犯罪而享有利益(Crime should not pay) ，此為沒收制度起初欲避免之基本原則[197]。

為達成最有效之沒收規定適用，「洗錢的對價報酬」除洗錢防制法之沒收規定，尚有可能與刑法沒收相競合之餘地。倘若洗錢的對價報酬為不法所得，參考洗錢防制法第 2 條 3 款謂「收受他人之特定犯罪所得」之規定以及洗錢防制法第 3 條關於特定犯罪的各款，收受者似乎會因幫助洗錢收受對價報酬而另外成立洗錢罪，並且同樣適用洗錢防制法關於沒收之規定。就此意義而言，似有兩種沒收方向，只不過洗錢防制法關於「洗錢的對價報酬」沒收，是取決於收受者是否因犯洗錢防制法第 3 條之各款犯罪而成立第 2 條之洗錢行為，進而構成第 14 條之一般洗錢罪，而可依第 18 條 1 項予以沒收，故適用範圍較窄；而另一種方向則是回歸刑法第 38-1 條，按收受洗錢對價之人是否構成犯罪行為人而可依第 1 項沒收，或是認其不構成犯罪時，依第 2 項之第三人沒收。

由上述分析可知，洗錢的對價報酬可能有犯罪所得沒收之競合難題。就此問題，有學者提出考慮賦予法院針對洗錢行為標的為「裁量沒收」的建議，於同一

---

195 許恒達（2017），同前揭註 193，頁 229。
196 曾淑瑜（2016），〈論修正前後沒收轉型之爭議〉，《司法新聲》，第 120 期，頁 10-12。
197 GUY STESSENS, MONEY LAUNDERING: A NEW INTERNATIONAL LAW ENFORCEMENT MODEL 51-56 (2008).

doi:10.6342/NTU201800740

行為同時觸犯兩種沒收時，由法院選擇較為妥適的沒收方式[198]。

兩種沒收方式的區別實益，主要在於洗錢客體的性質。洗錢罪的洗錢客體並不屬於新修正刑法沒收標的中之違禁物、犯罪工具(及犯罪所生之物)與犯罪所得的任何一項，而是屬於「關聯客體」(Beziehungsgegenstand) [199]。這與洗錢罪的處罰目的有關，洗錢罪欲處罰者，係對前置犯罪利得的掩飾或隱匿行為，蓋此等行為嚴重戕害國家金流秩序，影響金融市場及民生經濟。從一般洗錢罪的構成要件觀察，行為人需先具有「特定犯罪所得」，始能進入洗錢階段，是以前置犯罪所得是後階段洗錢罪的關聯客體[200]。

區分洗錢客體之性質在於能否適用刑法第 38 條 1、2 項及第 38-1 條 2、3、4 項以下的沒收規定來追徵價額，或擴及犯罪所得之範圍及於財產上利益或是孳息。有學者認為刑法第 38 條 2 項但書及第 38-1 條但書謂：「有特別規定者，依其規定」係授權允許沒收關聯客體的特別法—即洗錢防制法得回歸適用刑法之規定。按此邏輯，關聯客體之沒收必須以「有特別規定」為前提，原則上不會回歸刑法第 38 條之犯罪物沒收或是刑法第 38-1 條之犯罪所得沒收；若「特別規定」已授權可以沒收關聯客體卻漏未規定細部之沒收規定如：處理追徵、孳息等問題時，則得回歸適用刑法關於沒收之規範，蓋刑法第 38 條 2 項但書及第 38-1 條但書已開放特別

---

198 薛智仁（2017），同前揭註 194，頁 318。

199 許恆達（2017），同前揭註 193，頁 231；「關聯客體」之定義可參 106 年度台上字第 1374 號裁判要旨：「另在客觀要件上，應區分該供犯罪所用之物，是否為實現犯罪構成要件的事實前提，即欠缺該物品則無由成立犯罪，此類物品又稱為關聯客體，該關聯客體本身並不具促成、推進構成要件實現的輔助功能，故非供犯罪所用之物，其沒收必須有特別規定方得為之。例如不能安全駕駛罪，行為人所駕駛之汽車或機車即為構成該罪之事實前提，僅屬該罪之關聯客體，而不具促成、推進犯罪實現的效用，即非屬供犯罪所用而得行沒收之。至於犯罪加重構成要件中若有特別工具，例如攜帶兇器竊盜罪、利用駕駛供不特定人運輸之交通工具之機會犯強制性交罪，該兇器、交通工具屬於犯罪行為人者，分別對於基本構成要件之普通竊盜罪、強制性交罪而言，仍具有促成、推進功能，即屬於供犯罪所用之物，而在得沒收之列。」

200 許恆達，同前註，頁 232。

doi:10.6342/NTU201800740

規定回歸適用，能為特別規定所涵蓋。亦即，洗錢防制法之沒收特別規定，可因刑法第 38 條 2 項但書及第 38-1 條但書之特別授權，取代原本之第 38 條 2 項及第 38-1 條 1 項，從而同條其他款項接著連動，依據已經准許沒收關聯客體的第 38 條 2 項及第 38-1 條 1 項，發揮各自的效用[201]。惟另有學者認為既然特別法已另行規定洗錢罪所欲沒收之客體，且性質屬「關聯客體」，則應無再將其套回適用刑法第 38 條 2 項及第 38-1 條 1 項以下各款規定的空間，蓋刑法但書中所謂的「特別規定」是限定適用於「犯罪工具產物及犯罪所得」的特別規定，並不包含關聯客體，又因為沒收與追徵均屬於國家對人民財產權的干預，不得准許類推適用，結果就是洗錢罪行為客體不論是犯罪物、犯罪所得之替代品或孳息，均無法分別透過刑法第 38 條 4 項及第 38-1 條 4 項追徵其替代價值[202]。

若採前者見解認為洗錢防制法得回歸適用刑法之規定追徵犯罪物、犯罪所得之替代品或孳息，即有可能追徵將現實貨幣兌換為加密貨幣進行洗錢，卻因交易所被駭客攻擊而滅失之加密貨幣；亦可追徵因加密貨幣匯率巨幅變動而產生之巨大孳息。若採後者見解則因為「特別規定」限定適用於犯罪工具產物或犯罪所得，「關聯客體」非屬之，故會推導出不得沒收洗錢行為標的之孳息，亦不得追徵其價額之結果。

第三款 其他不明財產

至於第三類應被沒收的客體「其他不明財產」，則規範於洗錢防制法第 18 條 2 項：「以集團性或常習性方式犯第 14 條或第 15 條之罪，有事實足以證明行為人所得支配之前項規定以外之財物或財產上利益，係取自其他違法行為所得者，沒收

[201] 同前註，頁 233。
[202] 薛智仁（2017），同前揭註 194，頁 315。

doi:10.6342/NTU201800740

之」。修法理由參照外國法，將此項稱之為「擴大沒收」，以因應司法實務上，於查獲時發現與本案無關、但與其他違法行為有關聯，且行為人缺乏足夠佐證證明該財產與犯罪並無關聯時，允許法院得以沒收之，以杜絕犯罪行為、彰顯我國對於金流秩序公平正義之重視。本項被沒收的客體，本質上與洗錢偵辦過程中所發現的不法所得無關，但是為了杜絕集團性犯罪及不法金流橫行，是以在洗錢防制法第 18 條第 2 項擴大沒收(erweiterter Verfall)範圍。有學者認為此項規定本質上屬於特別的利得沒收規範，因為此款的沒收範圍並非針對洗錢罪的連結客體，而是在洗錢客體之外另行沒收「未確定罪名的犯罪所得」[203]。

第三項 洗錢防制法之規範主體

新修正洗錢防制法除第5條第1項沿用了舊法所列舉的共18款金融機構外[204]，尚參考 FATF 四十項建議之第 22 項建議，於第 3 項新增「指定之非金融事業或人員」[205]，此二者為洗錢防制法主要規範之主體。

---

[203] 許恆達（2017），同前揭註 193，頁 243。

[204] 本法所稱金融機構，包括下列機構：
一、銀行。
二、信託投資公司。
三、信用合作社。
四、農會信用部。
五、漁會信用部。
六、全國農業金庫。
七、辦理儲金匯兌之郵政機構。
八、票券金融公司。
九、信用卡公司。
十、保險公司。
十一、證券商。
十二、證券投資信託事業。
十三、證券金融事業。
十四、證券投資顧問事業。
十五、證券集中保管事業。
十六、期貨商。
十七、信託業。
十八、其他經目的事業主管機關指定之金融機構。

[205] 本法所稱指定之非金融事業或人員，係指從事下列交易之事業或人員：

doi:10.6342/NTU201800740

按 FATF 第 22 項建議，指定之非金融事業或人員在符合一定狀況時應遵循 FATF『第 10 項建議』客戶審查要求、『第 11 項建議』交易紀錄保存要求、『第 12 項建議』擔任重要政治性職務人士相關要求、『第 15 項建議』、新科技運用相關要求及『第 17 項建議』依賴第三方相關要求。我國新修洗錢防制法在第 7 條即參考上述建議，要求金融機構(Financial Institution, FIs)及指定非金融事業或人員(Designated Non-Financial Businesses and Professions, DNFBPs)應於特定場合進行確認客戶身分程序。確認程序應以風險為基礎確認客戶身分，若由代理人辦理者，應確實查證代理之事實、且應涵蓋實質受益人(Beneficial Owner, BO)之審查、國內外政府或國際組織重要政治性職務之客戶(PEPs)審查等，細節另規範於「金融機構防制洗錢辦法」。洗錢防制法第 8 條、第 9 條及第 10 條同樣對金融機構及指定非金融事業或人員的交易紀錄保存、一定金額以上之通貨交易申報，以及未依法向法務部調查局申報的後果做出規範。

由上可知，洗錢防制法對於金融機構及指定之非金融事業或人員兩大規範主體，均有課予洗錢防制的義務。單就洗錢防制法所明訂之上位規範，除罰責以外，唯一就兩者作出區別待遇的規範位於第 6 條，該條第 1 項強制規定金融機構應訂

一、銀樓業。
二、地政士及不動產經紀業從事與不動產買賣交易有關之行為。
三、律師、公證人、會計師為客戶準備或進行下列交易時：
（一）買賣不動產。
（二）管理金錢、證券或其他資產。
（三）管理銀行、儲蓄或證券帳戶。
（四）提供公司設立、營運或管理服務。
（五）法人或法律協議之設立、營運或管理以及買賣事業體。
四、信託及公司服務提供業為客戶準備或進行下列交易時：
（一）擔任法人之名義代表人。
（二）擔任或安排他人擔任公司董事或秘書、合夥人或在其他法人組織之類似職位。
（三）提供公司、合夥或其他型態商業經註冊之辦公室、營業地址、居住所、通訊或管理地址。
（四）擔任或安排他人擔任信託或其他類似契約性質之受託人或其他相同角色。
（五）擔任或安排他人擔任實質持股股東。
五、其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員。

doi:10.6342/NTU201800740

定防制洗錢注意事項，就特定事項報請中央目的事業主管機關備查；而非金融事業或人員之防制洗錢注意事項，則「得」由中央目的事業主管機關訂定。茲將兩者規範的差異繪表如下：

表 五：金融機構與指定非金融事業或人員之異同

	金融機構	指定非金融事業或人員
洗錢防制法第 6 條	應訂定防制洗錢注意事項，報請中央目的事業主管機關備查。目前已訂定「金融機構防制洗錢辦法」。	防制洗錢注意事項，得由中央目的事業主管機關訂定之，目前相關規範如表二。
	規避、拒絕或妨礙查核者，由中央目的事業主管機關處新臺幣五十萬元以上五百萬元以下罰鍰。	規避、拒絕或妨礙查核者，由中央目的事業主管機關處新臺幣五萬元以上五十萬元以下罰鍰。
洗錢防制法第 7 條	1. 應以風險為基礎進行確認客戶身分程序並保留資料五年。 2. 針對現任或曾任國內外政府或國際組織重要政治性職務之客戶或受益人與其家庭成員及有密切關係之人，以風險為基礎，執行加強客戶審查程序。	
	違反所定辦法者，由中央目的事業主管機關處金融機構新臺幣五十萬元以上一千萬元以下罰鍰。	違反所定辦法者，由中央目的事業主管機關處指定之非金融事業或人員新臺幣五萬元以上一百萬元以下罰鍰。
洗錢防制法第 8 條	因執行業務而辦理國內外交易，自交易完成時起，應至少保存五年。	
	違反者，由中央目的事業主管機關處金融機構新臺幣五十萬元以上一千萬元以下罰鍰。	違反者，由中央目的事業主管機關處指定之非金融事業或人員新臺幣五萬元以上一百萬元以下罰鍰。
洗錢防制法第 9 條	達一定金額以上之通貨交易，除本法另有規定外，應向法務部調查局申報。	
	一定金額為新臺幣五十萬元。	一定金額參照表二之個別辦法： 銀樓業：對新臺幣五十萬元以上之現金交易，應於交易後五個營業日內，向法務部調查局申報。 公證人：公證費用或交易金額

doi:10.6342/NTU201800740

		高於新臺幣五十萬元。 律師、記帳士、記帳及報稅代理人、會計師：對於客戶交易酬金或交易金額高於新臺幣五十萬元。 外幣收兌處：收兌之各種外幣現鈔與旅行支票，每筆結售金額達等值新臺幣五十萬元以上時，應以「收兌處外幣收入」性質申報。
	違反者由中央目的事業主管機關處金融機構新臺幣五十萬元以上一千萬元以下罰鍰。	違反者由中央目的事業主管機關處指定之非金融事業或人員新臺幣五萬元以上一百萬元以下罰鍰。
洗錢防制法第10條	對疑似犯第十四條、第十五條之罪之交易，應向法務部調查局申報，依規定為申報者，免除其業務上應保守秘密之義務。	
	違反者由中央目的事業主管機關處金融機構新臺幣五十萬元以上一千萬元以下罰鍰。	違反者由中央目的事業主管機關處指定之非金融事業或人員新臺幣五萬元以上一百萬元以下罰鍰。

表 六：指定非金融事業或人員之對應的法律規範

銀樓業	1. 銀樓業防制洗錢與打擊資恐施行及申報辦法 2. 銀樓業防制洗錢及打擊資恐注意事項
地政士及不動產經紀業	1. 地政士及不動產經紀業防制洗錢辦法 2. 地政士及不動產經紀業防制洗錢及打擊資恐注意事項
律師	1. 律師辦理防制洗錢確認身份保存交易紀錄申報可疑交易作業辦法 2. 律師辦理洗錢防制作業應行注意事項
公證人	1. 公證人辦理防制洗錢確認身份保存交易紀錄及申報可疑交易作業辦法 2. 公證人辦理防制洗錢作業應行注意事項
會計師	1. 會計師防制洗錢辦法 2. 會計師防制洗錢注意事項
記帳士、記帳及報稅代理人	1. 記帳士暨記帳及報稅代理人防制洗錢辦法 2. 記帳士暨記帳及報稅代理人防制洗錢應行注意事項
其他業務特性或交易型	1. 外幣收兌處設置及管理辦法 2. 臺灣銀行股份有限公司指定外幣收兌處設置及收兌外幣注

doi:10.6342/NTU201800740

態易為洗錢犯罪利用之事業或從業人員	意事項

由上表可知，洗錢防制法除刑責不同外，就指定非金融事業或人員與金融機構的洗錢防制要求似趨於一致，惟實際所課予之洗錢防制義務尚須各別檢視細部辦法加以分析，詳如後述。目前除「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」概括條款外，就非金融事業或人員的相關規範亦已完成。新洗錢防制法課予了金融機構與非金融機構多種義務，如第 6 條應遵守洗錢防制注意事項及受主管機關查核之義務；第 7 條課予應審查客戶及其密切關係人之身分的義務；第 8 條課予保存紀錄的義務；第 9 條課予申報大額交易的義務；第 10 條課予申報疑似洗錢犯罪之義務等是。

現行洗錢防制法若欲在未修法的前提下，將加密貨幣業者納入洗錢防制的範疇，僅能將該產業列入洗錢防制法第 5 條 3 項 5 款所謂之「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」，惟並非所有與加密貨幣相關聯的產業或是應用均會產生「易洗錢」的特性，此部分待第五章時再予詳述。以下將介紹加密貨幣納入我國洗錢防制法後有可能會造成的衝擊。

第二節　加密貨幣對洗錢防制規範的衝擊

隨著加密貨幣在各國開始普及，各種衍生的議題如洗錢防制、消費者保護，以及資訊安全即隨之浮現。以南韓 Youbit 為例，該加密貨幣交易所遭駭客攻擊損

doi:10.6342/NTU201800740

失達總資產 17%因此宣佈關門停業，並聲請破產[206]。因類似事件一再重演，有時甚至不排除交易所本身高層涉嫌侵占[207]，造成各國開始明確規範加密貨幣[208]。

對於加密貨幣可能涉及之洗錢議題，我國亦開始採取較積極的態度進行規範，經法務部、中央銀行、經濟部、金融監督管理委員會、內政部警政署，及法務部調查局等主管機關，共同研討現有法令規定，分別從管制層面及執法層面進行研討，各方均初步贊同有必要將虛擬貨幣納入現有的洗錢防制體系加以管制[209]，近期亦決定將虛擬貨幣納入洗錢防制法第 5 條 3 項 5 款所稱之「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」加以管制。本文同主管機關立場，認為有必要對部分「高風險」加密貨幣匯兌業務進行管制，以下將分別從管制層面及執法層面討論現今我國主管機關可能面臨的難題。

第一項 管制層面

從管制層面觀看加密貨幣，似乎可再區分成「欲管制的對象」以及「欲管制的交易型態」。所謂「欲管制的對象」從最廣義的角度解釋，可以是經手加密貨幣之人或團體；但也可以再行進一步限縮，以風險為基礎，使用「欲管制的交易型態」限縮「欲管制的對象」。若參考美國金融犯罪稽查局[210]的規範方式，是先將從事加密貨幣之業者因觸及「欲管制的交易型態」，亦即「匯兌服務」而被主管機關

---

[206] 許家華（2017/12/21），〈北韓駭客搞的鬼？南韓比特幣交易所 YOUBIT 二度遭駭聲請破產〉。載於：鉅亨網，https://news.cnyes.com/news/id/3995934（最後瀏覽日：2018/06/14）

[207] 中央社（2018/04/05），〈疑涉侵占 南韓拘留加密貨幣交易所高層〉，https://news.rti.org.tw/news/view/id/404104（最後瀏覽日：2018/06/14）

[208] 中央社（2018/04/05），〈打擊炒作 南韓出重手管制虛擬貨幣交易〉，http://www.cna.com.tw/news/afe/201712280264-1.aspx（最後瀏覽日：2018/06/14）

[209] iThome（2018/04/12），〈各國紛紛祭出禁令防制虛擬貨幣洗錢犯罪，臺灣即將跟進，法務部擬把虛擬貨幣納入洗錢防制體系〉，https://www.ithome.com.tw/news/122370（最後瀏覽日：2018/06/14）

[210] 名詞翻譯參考：詹德恩（2016/08/29），〈從檢察官進駐兆豐金談起〉，《天下雜誌》。載於：https://opinion.cw.com.tw/blog/profile/52/article/4714（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

判定為匯兌業者。主管機關接著再按觸及「匯兌服務」之「欲管制的對象」將其區分成三種類型，分別為：使用者(User)、交換者(Exchanger)、以及發行者(Administrator)，具體的區分方式將於第四章說明之。

我國若欲將加密貨幣業納入洗錢防制法，首要面臨的問題即如上述，必須處理如何將參與加密貨幣的各個角色類型化、明確化，以使規範對象知悉自己所從事的業務是受管制業務。惟在類型化各加密貨幣參與者的角色以前，似需先區辨何種角色將以何種交易型態經手加密貨幣，以針對最具風險性值的交易型態下手，從根本上達到洗錢防制的效果。

欲辨識在眾多加密貨幣交易態樣中何者最具備洗錢風險，應回顧加密貨幣以區塊鏈技術為基礎的交易架構，從中識別主管機關最有可能就哪個環節進行有效的洗錢防制。蓋在金融科技的創新下，以區塊鏈為基礎的加密貨幣因為「去中心化」的因素，已非如同過去任何金融商品，可以輕鬆就發行機構或是經手機構進行管制。一言以蔽之，我國主管機關所面臨最大的監理困境，應為如何在不妨礙金融科技發展的前提下，又可同時兼顧洗錢防制、維護金融秩序。

從第二章及第三章所討論的虛擬貨幣種類和加密貨幣的交易架構，綜合觀察現今加密貨幣於我國的交易模式，可得出以下幾點發展方向：

1. 加密貨幣在我國正以全雙向流通性的架構進行交易；
2. 少數商家正接受以加密貨幣直接購買商品或服務；
3. 我國已有運用加密貨幣吸金[211]、詐騙[212]、洗錢[213]，甚至劫持加密貨幣[214]；

---

[211] 同前揭註 7。

[212] 自由時報（2018/03/02），〈投資比特幣週 20％回饋？ 警：股神都做不到別被騙！〉，http://news.ltn.com.tw/news/society/breakingnews/2354226（最後瀏覽日：2018/03/30）

[213] 自由時報（2017/06/30），〈破比特幣洗錢中心 上億贓款被漂白〉，http://news.ltn.com.tw/news/society/paper/1114873（最後瀏覽日：2018/06/14）

[214] 自由時報（2018/02/22），〈劫比特幣轉匯中國 藏鏡人疑跨國指揮〉， http://news.ltn.com.tw/news/society/paper/1178123（最後瀏覽日：2018/06/14）；自由時報（2018/02/22），〈虛擬商品隱密性高常用於洗錢難追查〉，http://news.ltn.com.tw/news/society/paper/1178124（最後瀏覽日：

doi:10.6342/NTU201800740

4. 我國正朝向實名制及加強審查與加密貨幣「高風險帳戶」[215]；
5. 我國區塊鏈業者正擬定組成聯合自律組織，積極與政府溝通並制定產業標準[216]。

從以上時序的流程可看出，先有加密貨幣的交易，才逐漸體現出其具備的價值，之後才進而衍生出許多濫用加密貨幣的情形發生；而當政府欲積極介入管制時，既有的區塊鏈相關從業人員們始開始共同擬組聯合自律組織(Self-Regulatory Organization, SRO)，為了「讓政府拿出正確的態度來面對產業現況」。再後續的發展就須由自律組織、金融業者以及各相關政府部會共同討論會計與法律等議題。國內知名加密貨幣匯兌業者 MaiCoin 執行長 Alex Liu 先生即表示：「自律對於相關部會的影響力深遠，眼下最重要的是，在確認客戶身份程序作業(KYC)的合規、反洗錢(Anti-Money Laundering, AML)和稅收上有必要盡速管理[217]。」另一加密貨幣匯兌業者幣託(BitoEX)執行長鄭光泰亦附和道：「必須從現在碰到的問題來解決，稅收、防洗錢、業者自律、帳務透明，要做到讓人能信任[218]。」可見我國產業界已做好準備，只等政府部會明確將加密貨幣產業納入洗錢防制法的相關規範，即可立即配合相關反洗錢措施。

既然加密貨幣匯兌業者亦認為洗錢防制人人有責，等於管制層面上已提供主管機關一個明確的規範對象。惟主管機關在訂定專門辦法時，仍應以風險為基礎，要求加密貨幣匯兌業者將監控資源優先分配予高風險客戶，並建立類似金融機構的一系列反洗錢機制。誠然，國內一些加密貨幣匯兌業者已致力於建立信任機制，

2018/05/14）

[215] 中時電子報（2018/04/23），〈買賣比特幣就是高風險帳戶？金管會：視交易資金狀況〉，http://www.chinatimes.com/realtimenews/20180423002367-260410（最後瀏覽日：2018/06/14）

[216] Steve Jr Lin（2018/04/27），〈【監管第一步】台灣區塊鏈業者擬組聯合自律聯盟，欲積極與政府溝通並制定產業標準〉。載於：https://www.blocktempo.com/taiwan-regulation-first-step-blockchain-industry-4/（最後瀏覽日：2018/06/14）

[217] 同前註。

[218] 同前註。

doi:10.6342/NTU201800740

但若洗錢防制僅要求在認識客戶程序上(KYC)嚴格把關，恐仍稍有不足，因此本文認為更深層的管制面向，應從交易的開啟(Initiation)著手。

加密貨幣的移轉不同於通常銀行間的匯款，不存在「退匯」一詞、或是於SWIFT(環球銀行金融電信協會的一種結算系統)系統被駭時還可以追回被竊取之款項[219]。其最主要的原因，係因加密貨幣的移轉並不透過任何中心機構，每一筆交易的完成訊息都將成為區塊鏈中的一個區塊，是難以被修正或是竄改的。是以加密貨幣的洗錢防制管理，必須在洗錢三階段的「處置」(Placement)階段時盡力阻止，蓋一旦犯罪者順利將不法所得兌換成加密貨幣，以我國目前的執法技術而言，已無法再對後續的流向及移轉繼續進行有效的監控。

惟要在管制面避免不法所得進入「處置」階段，意味著要非常注重於認識客戶的程序以及執行交易的程序上。此二者若採取極度嚴格的措施，除不利於我國加密貨幣產業的發展，更將開啟我國幣民「海外大逃亡」的時代，屆時將因諸多客戶選擇匯款至國外交易加密貨幣，反而增加我國主管機關查緝上的困難、資本流出以及我國用戶無法獲得應有的保障等問題。

第二項 執行層面

從執行層面分析加密貨幣可能對洗錢防制帶來的衝擊，可從不同階段觀察，本文擬分別從「辨識的執行」、「規範的執行」及「落實的執行」分別論述。

第一款 辨識的執行

首先，「辨識的執行」涉及加密貨幣的規範主體。如同前文所述，SRO 的成立，

---

[219] 金融監督管理委員會（2017/12/15），〈遠東國際商業銀行 SWIFT 系統遭駭重大偶發事件所涉缺失，違反銀行法第 45 條之 1 第 1 項規定，核處新臺幣 800 萬元罰鍰〉。載於：https://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=201712180001&toolsflag=Y&dtable=Penalty（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

有助於辨識規範主體，但是就算沒有 SRO，檯面上的加密貨幣商也勢必將受規範，是以更具實益的作法，應是進一步辨識其他不容易被察覺、卻又是主管機關欲規範的類型，例如日前發生的達斯幣(Dascoin)吸金一案[220]，並不適用《銀行法》、《多層次傳銷管理法》、《證券投資信託及顧問法》，蓋我國中央銀行目前尚不認為加密貨幣能與貨幣、有價證券或是受益憑證等同視之，規範上目前仍是將其以「虛擬商品」看待[221]，再加上加密貨幣時常透過網站買賣，機房不一定位於我國，是以如欲規範加密貨幣的規範主體，較適合的方式也許是以涉及洗錢的高風險態樣來規範。此問題應該是我國在面對如何就加密貨幣為洗錢防制規範時最先會遇見的衝擊。

第二款 規範的執行

當我國主管機關克服辨識的難題後，第二層的衝擊就是「規範的執行」。主管機關於辨識規範客體後，或許會希望按 FATF 所制定的洗錢防制規範來制定其它指定非金融事業或人員的相關規範。但是因為加密貨幣具備的特性以及時常浮動的價值，將會導致所訂定的規範在執行上面臨更進一步的衝擊。此階段的挑戰較著重於規範的擬定與現實面的結合，若規範的範圍過於廣大，甚至已經超出「落實的執行」的範圍，則不僅規範策略失敗，成效低落，現實面的執行亦無法落實。例如 FATF 重要政治性職務人士指引文件中，就第 12 項建議及第 22 項建議應如何

---

[220] 大紀元（2018/04/03），〈新興網路犯罪「虛擬貨幣老鼠會」恐吸金 3 億 警方要查〉，http://www.epochtimes.com/b5/18/4/3/n10274122.htm（最後瀏覽日：2018/06/21）；「達斯幣」其背後 Netleaders 公司在新加坡登記為 CL SINGAPORE PTE.LTD，利用 LINE、微信等通訊軟體招攬下線，在台灣發展組織並宣稱有 4000%投報率，強調投資達斯幣可於日後幣值上升時獲利。該公司採取以比特幣付款購買達斯幣的「幣幣交易」方式收取台灣會員的資金；據追查，該組織恐在台已吸金直逼 3 億元，但我國執法單位尚束手無策。

[221] 中央銀行、金融監督管理委員會（2013/12/30），〈比特幣並非貨幣，接受者務請注意風險承擔問題〉。載於：中華民國中央銀行全球資訊網，https://www.cbc.gov.tw/ct.asp?xItem=43531&ctNode=302（最後瀏覽日：2018/06/22）

doi:10.6342/NTU201800740

分別適用於金融機構及指定之非金融事業或人員做出說明，其中建議第 12 項亦適用於 PEPs 之家庭成員及有密切關係之人，惟建議並未定義家庭成員及有密切關係之人一詞之範圍。原因是因為 PEPs 的密切關係之人與所在國之社會經濟與文化架構有關，各國之種族、文化、宗教連結的程度不盡相同，所以 FATF 的建議內僅用最概括的方式來論述「規範的執行」，指引第 47 條則建議各國將有密切關係之人與家庭成員的作定義或提供釋例時「不應做過度狹義或廣義的解釋」。我國參考 FATF 所提供之建議，並按《洗錢防制法》第 7 條 4 項後段訂定了《重要政治性職務之人與其家庭成員及有密切關係之人範圍認定標準》，其中第 7 條所列舉之判斷基準，如：第 2 款具密切關係之人擴及於同一公司之董事、監察人、或高級主管；第 4 款擴及受僱人或僱用人；卻不列舉與重要政治性職務之人同一政黨、社團、或工會之重要成員，即被批評為「抓小放大」不符經驗法則，故有論者建議將第 2 款連同其他超越各國實踐標準之範圍刪除，並新增第 13 款納入「其他一客觀情勢或一般社會之通念，認與重要政治性職務之人維持非比尋常密切關係之人」[222]。

以上舉例，均體現制定規範之時需考量此規範能否被有效地執行，所以就算於第一階段已辨識出有可能涉及加密貨幣洗錢的團體、組織或態樣，在研擬規範時，尚須將是否真有規範的必要、規範對於防制加密貨幣洗錢所能產生之效益、規範的實施可能性、規範對於被規範者可能產生的影響、規範對於整體產業的影響等等納入規範的考量，如此始得有效落實洗錢政策的執行。但如何就我國國情制定一套既能符合國際反洗錢需求、同時又能讓我國各加密貨幣商業機構及主管機關能有效遵循的規範，即是現今有可能面臨的衝擊。

---

[222] 錢世傑（2017），〈重要政治性職務之人(PEP)規定之合理性及其適用〉，《洗錢防制法律與政策研討會學術論文集》，頁 103。

doi:10.6342/NTU201800740

第三款 落實的執行

第三階段「落實的執行」，係指實質意義上的執行。在順利完成加密貨幣洗錢態樣的辨識、及採納國際化且實際的規範方式後，剩下要面臨的是實際上如何落實加密貨幣的洗錢防制。誠如前述，加密貨幣背後的區塊鏈技術是金融科技重大的創新，新的技術所帶來的各種去中心化、隱密性、安全性、便捷性都是洗錢防制上的難題，從事加密貨幣產業的業者們雖可被歸類為洗錢防制法內「指定之非金融事業或人員」，但是若欲落實反洗錢的政策加以管制，卻須耗費更多的研究資源以尋求相對應的規範模式。

以下就以實質受益人的辨識能否獲得有效落實為例。我國《洗錢防制法》第 7 條 1 項明文：「金融機構及指定之非金融事業或人員確認客戶身份程序應以風險為基礎，並應包括實質受益人[223]之審查」。審查實質受益人時，按《金融機構防制洗錢辦法》第 3 條 7 款第 1 目第 1 小目明定：「為辨識實質受益人，須瞭解具控制權之最終自然人身份，包括直接、間接持有法人股份或資本超過百分之二十五者」；金融機構得請客戶提供股東名冊或其他文件（如聲明書等）協助完成辨識。若無法按前述方式完成辨識，則按第 2 及第 3 小目，應先辨識有無透過其他方式對客戶行使控制權之自然人；若無，始辨識高階管理人員之身份。上述規定係參考 FATF 四十項建議之第 10 項第 10 款及第 24 項建議，透過客戶身分確認作業程序 (Customer Identification Program, CIP)辨識實質受益人。我國雖於第一階段辨識出「實質受益人為洗錢防制應規範的對象」，並於第二階段擬定具體規範導入我國法，將國際準則明文化，但於第三階段卻遇到阻礙，讓辨識實質受益人的目標難以確

[223] 金融機構防制洗錢辦法第 2 條將實質受益人定義為：「對客戶具最終所有權或控制權之自然人，或由他人代理交易之自然人本人，包括對法人或法律協議具最終有效控制權之自然人」。

doi:10.6342/NTU201800740

切得到落實。由此可見，落實法規範確實存在執行上的困難。

本例中辨識實質受益人的主要目的，除驗證其身份外，尚有讓資金來源、去向透明化的效果，為達成此效果，僅要求新開戶之客戶須經過身分確認作業程序是不足的，尚須將既有龐大的客戶群逐一辨識，直至辨識出實質受益人。就此，洗錢防制法尚未制訂出一套足以將法規範落實的措施，導致現行實務作業上雖有規範、且金融業者均已開始遵守[224]，卻無法達成原本預期的成效。原預期能依靠新修正之公司法第 22-1 條[225]第 6 項及第 7 項賦予主管機關裁罰權限、嚴重者甚至得廢止公司登記的方式，來得到妥善的解決[226]。惟因第 3 項對於實質受益人之定義係參考證券交易法第 25 條第 1 項規定，故訂定出與 FATF 第 24 項建議和我國金融機構防制洗錢辦法第 3 條 7 款 1 目相左的定義。蓋目前國際趨勢對於構成實質受益人的股權數是採行 25%，由洗錢防制相關法規均訂定「直接或間接持有該公司 25%以上的已發行股份」可知。而行政院版公司法第 22-1 條雖於修法理由提及為因應 FATF 之建議而引進實質受益人之規定[227]，卻又於辨識方法上參考我國證

---

[224] 同前揭註 6。

[225] 行政院於 106 年 12 月 21 日通過之「公司法修正草案」第二十二條之一

I 公司應於每月十五日前，將實質受益人資料以電子方式申報至中央主管機關建置之資訊平臺。但符合一定條件之公司，不適用之。

II 前項資料，中央主管機關應定期查核。

III 第一項所稱實質受益人，指董事、監察人、經理人及持有已發行股份總數或資本總額超過百分之十之股東。

IV 第一項申報資料，應包含實質受益人姓名、國籍、出生年月日或設立登記之年月日、身分證明文件號碼、持股數或出資額及其他中央主管機關指定之事項。

V 第一項資訊平臺之建置、資料之申報格式、一定條件公司之範圍、資料之蒐集、處理及利用，第二項之查核程序、方式，第三項經理人之範圍，前項指定事項之內容及其他應遵行事項之辦法，由中央主管機關會同法務部定之。

VI 未依第一項規定申報 或申報之資料不實，經中央主管機關限期通知改正，屆期未改正者，處代表公司之董事新臺幣五萬元以上五十萬元以下罰鍰。經再限期通知改正仍未改正者，按次處新臺幣五十萬元以上五百萬元以下罰鍰。其情節重大者，得廢止公司登記。

VII 前項情形，應於第一項之資訊平臺依次註記裁處情形。

VIII 中央主管機關得就第一項之業務，委託具公信力之機關（構）或團體辦理。

[226] 2017 年 12 月 21 日公司法部分條文修正草案條文對照表。

[227] 行政院於 106 年 12 月 21 日通過之「公司法修正草案」第二十二條之一第一項修法理由：「(一)

doi:10.6342/NTU201800740

券交易法，從而以 10%的股權數為基準，從修正草案第 3 項「指董事、監察人、經理人及持有已發行股份總數或資本總額超過百分之十之股東。」可知。若採取草案內對於實質受益人之定義，不僅將於我國法成立兩套實質受益人的判斷基準[228]，更有可能促使實際持有 10%以上股權之股東，透過法人持股分散持有股權，而規避公司法第 22-1 條可能被申報之情形[229]。因此有學者即指出行政院版公司法所出現的「實質受益人」字樣，因僅揭露第一層直接持股對象，經行政部門聘請的外國顧問評估，未達到通過年底 APG 評鑑所需要的中等以上標準，不符合國際防制洗錢規範，是以對於我國年底即將面對的 APG 防制洗錢評鑑的幫助不大[230]。對於外界的質疑，我國主管機關日前亦達成共識將最後將把「實質受益人」一詞自法條中刪除，但揭露程度仍不變[231]，最新於 2018 年 7 月 6 日三讀通過之公司法亦再次確認公司法第 22-1 條無「實質受益人」字眼，且按條文公司應每年以電子方式申報董事、監察人、經理人及持股超過 10%股東資料，若有變動者於變動後

為落實建構以風險分析為基礎之跨國洗錢防制制度，並有助於我國通過西元二 O 一八年亞太洗錢防制組織(Asia/Pacific Group on Money Laundering，以下簡稱 APG)第三輪相互評鑑，爰參照「防制洗錢金融行動工作組織」(Financial Action Task Force, 以下簡稱 FATF)第二十四項關於實質受益權之建議，引進實質受益人之規定。

（二)依前揭 FATF 建議，要求政府應有效掌握公司實質受益人資料，並應有一定機制確保該資料之正確性與及時性，爰明定由中央主管機關建置資訊平臺，供公司以電子方式申報實質受益人資料，並參照證券交易法第二十五條第二項規定，要求公司應於每月十五日前申報。」

[228] 按 FATF 對於實質受益人之定義，多係指對公司具最終所有權或控制權之自然人依前小目規定未發現具控制權之自然人。我國金融機構防制洗錢辦法第 3 條 7 款 1 目參考國際標準於前條第 2 小目對於無法由第 1 小目辨識出直接、間接持有該法人股份或資本超過百分之二十五時，或對具控制權自然人是否為實質受益人有所懷疑時，規定應辨識有無透過其他方式對客戶行使控制權之自然人。依前二小目規定均未發現具控制權之自然人時，金融機構應按同條第 3 小目辨識高階管理人員之之身分。

[229] 何嘉容（2018），〈誰是實質受益人？ 公司法修法與洗錢防制〉，《會計研究月刊》，第 391 期，頁 88。

[230] 自由時報（2018/05/16），〈公司法實質受益人漏洞 學者：恐無法通過洗錢評鑑〉，http://news.ltn.com.tw/news/business/breakingnews/2427180（最後瀏覽日：2018/06/23）

[231] 中時電子報（2018/06/11），〈行政院版公司法 刪除實質受益人字眼〉， http://www.chinatimes.com/newspapers/20180611000204-260202（最後瀏覽日：2018/06/23）

doi:10.6342/NTU201800740

15 日內申報[232]。

近期立法院三讀通過公司法修正案針對《公司法》新增訂第 22-1 條，經濟部次長王美花表示：「經濟部必須在 2 個月內訂出相關子法，包括洗錢防制條文後續申報程序及細節，訂出申報格式，並且規畫最簡易操作方式，供企業申報」。並透露：「第 22-1 修正案最快會先在 8 月生效，其餘條文預訂明年 1 月 1 日上路」[233]。如此觀之，我國仍欠缺能落實金融機構防制洗錢辦法第 3 條 7 款 1 目所稱之「實質受益人」的強制性規範，公司法第 22-1 條雖然強制規定公司每年以電子方式申報董事、監察人、經理人及持股超過 10%股東資料，但誠如前述，如此規範將有可能促使實際持有 10%以上股權之股東，透過法人持股分散持有股權，而規避公司法第 22-1 條之可能。雖從持股比例難以妥當地辨識最終實質受益人，然此「透明條款」仍對於建置全台公司持股比例資料庫有著極為巨大的助益。未來我國主管機關即可透過專門軟體，將公司或高階負責人互相持股之數額清楚以圖像顯現，雖無法立即辨識出最終實質受益人，但從持股連結的複雜程度觀之，實已足夠引起調查人員的注意。類似以系統方式偵測持股比例異動的方式，同樣有助於洗錢防制及打擊資恐，雖目前僅是構想，有效性亦尚待評估，但可以肯定本次公司法第 22-1 條之增訂，將成為日後我國欲落實國際標準揭露實質受益人不可或缺的一塊基石。

第三節　我國目前的加密貨幣洗錢防制規範政策

有鑒於加密貨幣於我國日漸盛行，近來所衍生的投資糾紛及負面新聞均不在

---

[232] 聯合新聞網（2018/07/06），〈力拚洗錢防制評鑑 公司申報最快 8 月生效〉， https://udn.com/news/story/7238/3238629（最後瀏覽日：2018/07/08）

[233] 聯合新聞網（2018/07/06），〈公司法三讀後 69 萬家公司快做這件事 公司法三讀通過〉，https://udn.com/news/story/7238/3239049（最後瀏覽日：2018/07/07）

doi:10.6342/NTU201800740

少數[234]，對此我國前任中央銀行總裁彭淮南、現任中央銀行總裁楊金龍及現任法務部長邱太三均認為應立法納管[235]。立法院於 2018 年 5 月所舉辦的「健全加密貨幣洗錢防制」公聽會，邀請法律學者、立法委員、科技公司執行長、銀行局副局長及洗錢防制辦公室執行秘書共同討論未來的規劃方向，初步結果亦均認為應將加密貨幣納入管制[236]。

管制的第一步除了推行加密貨幣實名制外，尚有應如何定位加密的問題。本文為了深入探討洗錢防制議題故於前文將加密貨幣的定位為一種交易媒介。惟加密貨幣涵蓋的範圍甚廣，例如由首次代幣發行(ICO)所發行的「代幣」本質上亦屬於加密貨幣。中央銀行總裁楊金龍認為由科技公司經由首次代幣發行的加密貨幣，性質上應只能叫「代幣」，蓋加密貨幣是「經由電腦進行找尋、媒合出的一連串編碼所組成，然後經過人為的定義及定價而出現價值」，無論從概念上理解或是形成的方式來理解均和實體貨幣相去甚遠，完全不等同於「貨幣」[237]。就此以觀，廣義的加密貨幣洗錢防制尚會牽涉到加密貨幣產生的方式。

首次貨幣(代幣)發行（Initial Coin Offering, ICO）是近來興起的新型融資方式，類似首次公開發行股票（Initial Public Offerings, IPO）[238]，因 ICO 所發行的加密貨幣(下稱代幣)所具備之功能與所表徵的價值可能具有多重性質，相較於傳統的貨幣型加密貨幣更為複雜，因篇幅上的限制，本文不會深入討論 ICO 可能涉及的洗錢

---

[234] 信傳媒（2018/05/07），〈麻吉大哥的秘銀幣捲入侵占爭議 台灣虛擬貨幣確定走向管制派〉，https://www.cmmedia.com.tw/home/articles/9775（最後瀏覽日：2018/06/14）

[235] 自由時報（2018/04/20），〈虛擬貨幣納管達共識！邱太三：將對比特幣做相當管制〉，http://news.ltn.com.tw/news/politics/breakingnews/2401194（最後瀏覽日：2018/06/14）

[236] 科技新報（2018/05/02），〈加密貨幣洗錢防制，實名制是共識〉，http://technews.tw/2018/05/02/cryptocurrency-money-control/（最後瀏覽日：2018/06/14）

[237] 工商時報（2018/05/07），〈法源不明 央行擬正名代幣解套〉， http://www.chinatimes.com/newspapers/20180507000176-260202（最後瀏覽日：2018/06/14）

[238] iThome（2017/09/11），〈報告：ICO 吸金能力大過創投、知名眾籌平台〉，https://www.ithome.com.tw/news/116786（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

議題；但可預見的是未來我國仍須另外針對 ICO 研擬代幣的洗錢防制政策，原因在於 ICO 與本文前述採取公鏈架構的加密貨幣有著明顯不同。

ICO 是直接讓投資人以現實貨幣購買稱為代幣（Token）的加密貨幣，而不是由提供算力的礦工透過「挖礦」來競爭新產生的加密貨幣。此不同之處會造成採行 ICO 方式所發行的加密貨幣，於數量控制上不若公鏈型加密貨幣，因為發行人可以自由控制欲產生的代幣、並且銷售予願意購買的投資者以募取資金。在此種以銷售代幣為主要獲利管道的經營模型下，較難期待初始發行人會遵守某一固定發行數量的承諾，更何況部分不肖 ICO 業者主要目的僅是為了募取投資者的資金，而非欲真實發行具有實際功用的加密貨幣。因此，ICO 近來常出現加密貨幣詐騙案，如 LoopX 一個月內成功籌集了近 450 萬美元後，其 Facebook、Telegram 及 YouTube 賬戶均被刪除，負責人從此消失；又如 Miroskii 即利用虛構的技術宣稱自己是「沒有銀行家的銀行」，造假程度誇張，但發起人依然成功籌得 83 萬美元後消失無蹤 [239]。此現象持續發燒，根本沒在運作的「殭屍專案」也在今年初大幅增加。根據 Bitcoin.com 統計，去年共 902 件 ICO 專案中，有 46%都以失敗告終；其中，142 件專案在籌資前就已經宣告失敗，還有另外 276 件則在募完錢就消失，完全沒有推出任何產品 [240]。如此高風險的籌資行為，讓 ICO 成為有心人士吸金的良好工具，現行眾多負責人均位於海外或是根本無從得知其真實身分，若有心吸金後潛逃根本無從制止。

在 ICO 籌資的案例中，因加密貨幣是投資者給付價金的對價，且該款加密貨

---

[239] Elliott Leung（2018/03/07），〈影帝都賣虛擬貨幣？再有虛擬貨幣眾籌騙局〉，https://unwire.pro/2018/03/07/miroskii-fake-cryptocurrency-ico/news/（最後瀏覽日：2018/07/15）

[240] 張庭瑜（2018/02/26），〈投資 ICO 致富夢一場，調查：去年近半數專案宣告失敗〉，https://www.bnext.com.tw/article/48305/46-last-years-icos-failed（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

幣僅能在開發者所制定的架構內流通，或是做為支付某些服務的對價，是以能與現實貨幣互相兌換的自由度會較公鏈架構的加密貨幣低，匯兌成本即隨之升高。類似採取私鏈架構的加密貨幣，在性質上與比特幣相較更趨近於商品或是證券，端視該款發行之加密貨幣是否表彰一定價值，以及投資者能否持代幣向發行者兌換經濟上權利。

分析上述採行公鏈架構的比特幣以及多數採行私鏈架構以向大眾募資的首次貨幣(代幣)發行的加密貨幣，可得知名稱上的「加密貨幣」在細分下卻有著與現實貨幣完全不同的關聯性。我國相關部會所著重的「實名制」，主要應是針對採取公鏈架構之加密貨幣，蓋公鏈型加密貨幣始得稱之為真正意義上的去中心化，也因此才能成就難以破解的安全性以及讓各國主管機關困擾的化名式匿名。公鏈型加密貨幣因設計上較趨向於「錢」，所以在規範上可以參照指定之非金融事業或人員來管制規範客體。至於私鏈型加密貨幣因為性質上較偏向於商品或是證券，再加上發行機構與投資人兩者均不難辨識，所以主管機關對此類加密貨幣的規範方向應是消費者保護。

確實，加密貨幣在未有任何政權的支持下，因缺乏法令的支持促使其成為合法通貨的貨幣，所以其購買力當然也得不到確保，無法與傳統由國家發行的貨幣相比。但是當比特幣這種既採行公鏈區塊鏈技術、又同時具備雙向流通虛擬貨幣架構的加密貨幣，得到廣泛的用戶支持，其支付能力及變現能力將呈現與法定貨幣相距不遠的狀態。JPMorgan 的執行長 Jaime Dimon 曾說比特幣是專門為洗錢犯罪與毒品交易而生詐騙工具，但其後已表示對此發言深感遺憾，且會在未來發展

doi:10.6342/NTU201800740

一套類似結算所的平台以參與加密貨幣市場[241]。Goldman Sachs 亦在一份 9 頁的報告中直言「比特幣就是錢」[242]。如此看來，比特幣雖非貨幣，但是至少在支付或是匯兌上，具有即時變成貨幣的功能。

第四節　小結

本章先從洗錢防制法罪刑架構出發，區分一般洗錢罪及特殊洗錢罪，前者規定於《洗錢防制法》第 2 條共三項，前提是須符合第 3 條所稱之特定犯罪；後者則規定於《洗錢防制法》第 15 條，與普通洗錢罪不同之處，在於少了前置犯罪的要件，亦即不以犯現行條文第 3 條所定之特定犯罪為前提。區分完洗錢罪之基本刑罰架構後，本文從犯罪後的獨立法律效果—沒收為主要討論對象，就洗錢犯罪過程中可能涉及之金錢、財產流通，依學說分述其中「洗錢行為客體」、「洗錢的對價報酬」及「其他不明財產」三類，希冀能透過檢視現行刑法沒收章節與洗錢防制法之沒收章節探詢較適合為加密貨幣應用之沒收制度。論述之下，發現洗錢防制法之沒收似可認為是刑法沒收之特別規定，依學說見解，洗錢犯罪因犯罪客體並非犯罪工具，蓋被洗的錢是構成要件實行的前提，欲漂白之金錢一旦欠缺該物品自然亦欠缺促成犯罪構成要件實現的效果，故不能徑認定為犯罪工具而應認其為關聯客體[243]。就關聯客體能否回歸適用刑法第 38 條 1、2 項及第 38-1 條 2、3、4 項以下的沒收規定追徵價額、或是擴及犯罪所得之範圍及於財產上利益或是孳息須視刑法第 38 條 2 項但書及第 38-1 條但書謂：「有特別規定者，依其規定」如何解釋。本文贊同刑法第 38 條 2 項但書及第 38-1 條但書已開放特別規定回歸適用刑

---

[241] Kenneth Rapoza, *Goldman Sachs Caves: Bitcoin is Money,* FORBES (Jan. 10, 2018, 11:15 AM), https://www.forbes.com/sites/kenrapoza/2018/01/10/goldman-sachs-caves-bitcoin-is-money/.
[242] *Id.*
[243] 許恆達（2017），同前揭註 193，頁 231。

doi:10.6342/NTU201800740

法之學說，認為洗錢防制法之沒收特別規定，可因刑法第 38 條 2 項但書及第 38-1 條但書之特別授權，取代原本之第 38 條 2 項及第 38-1 條 1 項，因同條其他款項接著連動，故能補充特別法之沒收未能處理之追徵、孳息等問題[244]。如此一來對於收取加密貨幣作為洗錢犯罪之對價但卻又因故滅失者，或是因利用加密貨幣作為洗錢客體卻因幣值變動而產生之孳息等問題，均能妥善以現行法處理，不失一個對現有洗錢防制法及刑法沒收章節競合妥善的解釋。惟本文亦同意反對學說之見解，現行洗錢防制法對於行為客體的沒收缺乏通盤規劃，於放寬對第三人洗錢行為客體之同時，卻疏未規定洗錢行為客體之追徵價額條款，長遠妥適之作法似可明文增訂準用條款，明文有特別法規定許可或應予沒收關聯客體者，準用第 38 條 2 項至 4 項[245]及準用第 38-1 條 3 項至 5 項以消除洗錢防制法之沒收能否回歸適用刑法沒收之模糊地帶。現行法律適用上雖得以按照上述方式進行操作，理論上對我國洗錢防制法的規範主體進行規範，將被歸類為指定之非金融事業之加密貨幣進行沒收，達成理論上沒收加密貨幣的效果，惟加密貨幣於現實上造成的種種影響卻是現行洗錢防制法及刑法中所規範的罰則及沒收制度無法解決的。例如從管制層面觀察加密貨幣，何機關應適用何種標準並使用何種方式對利用加密貨幣洗錢之人的關聯客體進行沒收？如有上述標準，於執行層面是否有辦法落實？本文認為欲解決管制層面上的問題,應回顧加密貨幣以區塊鏈技術為基礎的交易架構，從中識別主管機關最有可能就哪個環節進行有效的洗錢防制，爰於下一章先參考外國立法例，以辨識須管制之對象，提出潛在的規範方式。就執行面上，本文從「辨識的執行」、「規範的執行」及「落實的執行」三種面項討論除建構監管政策

[244] 同前註，頁 233。
[245] 薛智仁（2017），同前揭註 194，頁 316。

doi:10.6342/NTU201800740

外，尚須考量執行面能否有效執行，避免過高的期待卻得不到預期的落實，最終落於空談。就「辨識的執行」本文認為透過 SRO 對檯面上的加密貨幣匯兌業者先行整合，探討何種交易模式風險屬性最高，共同辨識應優先規範之對象。就「規範的執行」，本文呼籲在研擬規範時須將是否真有規範的必要、規範對於防制加密貨幣洗錢所能產生之效益、規範的實施可能性、規範對於被規範者可能產生的影響、規範對於整體產業的影響等等納入規範的考量，以規範的擬定與現實面確實能落實的可能性為主要考量。最後本文論及「落實的執行」，以實質受益人搭配目前新法的方向，說明為何要確實落實 FATF 之建議確實有其困難，除因法規制定上欠缺能落實之對應規範，更須實務運作上能配合並落實法律所課予之義務。同理，我國相關部會所著重的應是加密貨幣之「實名制」，以落實加密貨幣之洗錢防制，惟採行公鏈架構之加密貨幣，因架構上已達成真正意義上的去中心化，也因此成就難以破解的安全性以及讓各國主管機關困擾的化名式匿名。為解決管制層面、執行層面之種種難題以讓洗錢防制法之相關刑罰及沒收規定有適用之餘地，本文擬於第四章深入參考 FATF 國際組織及美國法，以探詢較適合適用於我國之加密貨幣管制方式及相對應之落實之策。

doi:10.6342/NTU201800740

第肆章　加密貨幣之洗錢防制方向

第一節　國際組織對於加密貨幣的政策—以防制洗錢金融行動工作組織為例

我國新修正之洗錢防制法主要係參考防制洗錢金融行動工作組織（FATF）所發布之「評鑑方法論」。FATF 亦曾針對虛擬貨幣發表「風險基礎方法指引」，指引內臚列多項建議供主管機關參考，如主管機關欲著手規範加密貨幣，此指引勢將成為訂定專法中不可或缺的參考對象。關於該指引的細節部分，本文不擬逐一敘述，僅分析此份國際組織對於規範加密貨幣所提出之建議，並將其簡化以明確我國未來加密貨幣之洗錢防制方向。

FATF 就加密貨幣所發表之指引，主要規範對象為「虛擬貨幣支付產品與服務」（Virtual Currency Payment Products and Services, VCPPS 以下統一稱之），指引內所提及之虛擬貨幣，主要係針對採行公鏈區塊鏈技術且基於全雙向流通性虛擬貨幣架構的狹義虛擬貨幣[246]，亦即本文所稱的加密貨幣。以下將就 FATF 所提出之建議，按第三章所舉例的三點對我國洗錢防制法最大的衝擊—辨識、規範、落實，分別區分並敘述之。

第一項 辨識規範客體的建議

「FATF 虛擬貨幣風險基礎方法指引」[247](下稱「指引」)在辨識的執行上，基

---

[246] 指引第 10 條：「此指引的重點放在可轉換、屬於提供受管制的金融體系門徑的交叉點的虛擬貨幣兌換方（可轉換的 VC 活動與受管制的法定貨幣金融體系交叉處）。不處理 VC 支付機制所產生的非防制洗錢／打擊資恐的法規議題（如：消費者保護、嚴謹的安全性與健全性、稅務、反詐欺問題以及網絡 IT 安全標準等）。也不處理 VC 的非支付用途（如：基於儲蓄或投資目的儲存具有價值的產品，如：衍生品、商品和證券產品）或 VC 活動 5 的貨幣政策面向。」

[247] FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL CURRENCIES (June

doi:10.6342/NTU201800740

本亦採行以風險為基礎的識別方式來辨識虛擬貨幣是否可能被利用為洗錢工具。就最初的風險評估，指引第 13 條認為目前可能存在洗錢或資恐風險的虛擬貨幣，「只有可用於將價值移進和移出法定貨幣以及受管制金融體系的可轉換虛擬貨幣 」，此與前文分析之採行雙向流通虛擬貨幣架構之加密貨幣，應屬同一類重點規範對象。而就最容易進行洗錢防制的環節，指引的政策與美國 FinCEN 政策相同，建議應管制可轉換虛擬貨幣與金融體系門徑的交叉點—即交換者，而不是透過虛擬貨幣購買商品或服務的使用者。

既然現實貨幣與虛擬貨幣之間的匯兌為管制的重點，則下一項應辨識的規範對象，即為從事匯兌的金融機構方及 VCPPS 方。金融機構一方的辨識較不具困難[248]，較需注意的是倘若一機構並非金融機構，則需辨識其是否構成「金錢或價值移轉服務業」(Money or Value Transfer Service, MVTS)。MVTS 就如同美國法上的匯兌業務，由於涉及的行業非常廣泛，無法如金融機構一般以列舉方式明訂於條文內，而須視個案所執行的業務是否有可能觸及「金錢或價值移轉」服務。

例如行動支付業者或是行動網路經營業者(Mobile Network Operators, MNO)，也許會透過新興支付產品及服務（New Payment Products and Services, NPPS）允許多種充值或交易的資金提供方式或是預付卡方案，進而允許資金在個人與個人間移轉，此即可能構成 MVTS。又如網路支付服務提供者所提供的服務若允許個人

2015), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[248] FATF 對金融機構之定義：金融機構係指任何自然人或法人代表客戶從事下列一項或多項活動或作業為其業務者稱之：1. 接受一般民眾存款及其他附償還式資金。2. 借貸。3. 金融租賃。4. 金錢或價值移轉服務。5. 發行並管理支付工具（如：信用卡、現金卡、支票、旅行支票、匯票及銀行本票、電子貨幣等）。6. 金融擔保與承約。7. 執行下列交易： (a) 貨幣市場工具（支票、票據、存單、衍生商品等）；(b) 外幣兌換；(c) 匯率、利率及指數商品；(d) 可轉讓證券；(e) 商品期貨交易。8. 參與證券發行及提供相關金融服務。9. 個別及集體投資組合管理。10. 代表他人保管與經營現金或流通性證券。11. 代表他人從事其他投資、經營或管理資金或金錢。12. 壽險及其他與投資型保單之核保與發行。13. 金錢與貨幣的兌換。

doi:10.6342/NTU201800740

與個人間的價值移轉，亦有可能因此成為 MVTS[249]；以目前當紅的網路直播為例，若直播主於直播時所得到的「贊助」(通常是虛擬貨幣形式)能全數歸類為直播主的收入[250]，即代表著有心洗錢的人士能透過人頭帳戶購買虛擬貨幣，並於直播主直播時打賞(贈送)，直播主於節目結束後再以所獲得的虛擬貨幣(也許是鮮花、愛心等形式)向傳播公司請求相對的「酬勞」，即能輕鬆完成 A 至 B 的金錢移轉，且 B 之所得為合法勞務所得。實務上因直播成本低廉又較不引人矚目，所以就連年僅 6 歲的直播主都能年收入破千萬美金[251]。當然其中或許大多數均為合法經營的直播主，但根據中國的一項直播統計，2,100 名直播主即能在一個月達到 3.1 億人民幣的收入。其中進入「十月主播收入總榜 TOP 30」的直播主中，其中一位直播主的金幣收入達 708,860,000 折合人民幣 3,420,860 元、但卻只有 25 位粉絲，另有一名同樣入榜的直播主收入月達人民幣 1,217,081 元、卻只有 1 位粉絲[252]。擁有大量類似直播主的網路平台或是公司，極有可能涉及 MVTS，而 MVTS 在洗錢防制的重要性與 VCPPS 相似，規範上至少應受如同指定之非金融事業等級的管制。

VCPPS 相較於 MVTS 在辨識上並不困難，只要於我國有設立公司、並且使用虛擬貨幣與金融機構及 MVTS 從事跟現實貨幣有關之業務即屬之。惟須注意，在風險基礎方法下，VCPPS 在辨識上亦須區分風險等級，以強化對於較高風險情況的要求，而非一概將有涉及虛擬貨幣業務者均視為高風險。對此，指引第 23 條同本文看法，建議在評估可轉換虛擬貨幣的洗錢／資恐風險時，應考量虛擬貨幣所

---

[249] 參照：法務部調查局（2013），〈洗錢防制工作年報〉，頁 70-80。

[250] 蘋果日報（2018/02/02），〈館長爆實況主收入「直播電玩可賺 50 萬」〉，https://tw.appledaily.com/new/realtime/20180202/1290788/（最後瀏覽日：2018/06/14）

[251] 鉅亨網新聞中心（2017/12/12），〈網紅經濟有多賺？6 歲網紅直播主年收入破千萬美金〉，https://news.cnyes.com/news/id/3987511（最後瀏覽日：2018/06/14）

[252] 恒豐國際娛樂平台（2017）〈《直播職業 10 月陳述》直播收入榜發佈：花椒主播最掙錢〉，http://www.hzhonghao.com/news/gsxw/15.html（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

採行的架構，蓋一般而言「可轉換的去中心化 VCPPS 因其匿名性質以及不易辨識參與者的身份，故應可視為具備較高的洗錢／資恐風險，因此需要應用強化的客戶審查措施」，由此可知，辨識虛擬貨幣是採集中式抑或是分散式的帳本技術，在風險分級上是一個需要考量的重要因素，若無法辨識虛擬貨幣的性質及架構，後續勢必會產生規範上的困難。

成功辨識與 VCPPS 來往之金融機構及 MVTS 後，下一步應辨識的對象即為與 VCPPS 往來的客戶。指引第 23 條內的建議一即建議「可靠地辨識並確認客戶」，並運用風險基礎方法，評估虛擬貨幣可能涉及洗錢／資恐風險的活動。評估進行中，應按指引第 49 條參考 FATF 第 20 項建議，在虛擬貨幣交易可能涉及犯罪活動所得、或可能和資恐有關時，記錄與通報可疑活動。

第二項 規範客體的規範建議

FATF 指引就各國如何規範虛擬貨幣洗錢，於指引第 20 條提出了整體法律框架的規範，各國應先參考虛擬貨幣在該國的盛行度(Intensity)與市場佔有率(Volume)，再參考 FATF 的建議及以風險為基礎，制定合於國內虛擬貨幣匯兌業者及其他充當虛擬貨幣節點的法規範。此類金融科技上的創新—特別是運用虛擬貨幣科技的新興產品與服務，參考指引第 24 條，似可由公私部門間相互合作來達成規範共識。例如第三章提及的自律組織(SRO)與權責機關相互討論防制洗錢的對策即屬之。

國內監理者在結合公私部門達成共識後，規範上應參照指引第 14 條建議，參考國際標準規定，「鎖定可轉換虛擬貨幣的節點—亦即：規範現實貨幣與虛擬貨幣中間的交叉點」，而非試圖管制透過虛擬貨幣購買商品或服務的使用者。此規範建議如同美國規範政策，不管是發行者(Administrator)或是交換者(Exchanger)，只要是提供現實貨幣與虛擬貨幣之間的匯兌服務，都是指引所述的高風險管制對象。

doi:10.6342/NTU201800740

若再進一步深入規範，則參照指引第 15 條建議，似可在風險基礎方法下，管制「不提供虛擬和法定貨幣之間的交易或兌現服務」、但卻提供「金融機構寄送、接收和儲存虛擬貨幣的指定之非金融事業或人員」。此處所指稱的服務，應是前述的 MVTS，只不過移轉標的較為限縮，但是擴大了規範主體，納入了寄送、接收及儲存虛擬貨幣的非金融事業或人員。若我國欲採此建議，則必須在辨識階段加強，將科技公司、虛擬貨幣投資公司、以及提供虛擬貨幣作為支付管道的商家納入規範的範圍。指引就第 15 條的建議，明白說明除了直接從事虛擬貨幣及現實貨幣交易的 VCPPS，其餘涉及虛擬貨幣周邊的非金融事業或人員，均不在指引欲防制的虛擬貨幣洗錢之範圍內。就此觀察，我國於初期建構虛擬貨幣相關規範時，應可區分為與金融機構及 MVTS 來往的 VCPPS、及虛擬貨幣周邊的非金融事業或人員；前者可作為規範的主要對象，先以專法或專章訂定之，後者則可視前者的規範結果及對產業的衝擊，再另行考慮應否對其為專門規範，如此才能最大程度的兼顧我國金融科技產業的發展及國際組織就虛擬貨幣所建立的規範指引。

而就 VCPPS 的規範而言，可先從許可制著手。指引第 21 條即建議各國權責機關可以參考防制洗錢金融行動工作組織就虛擬貨幣所作出的特定建議，運用至自身法體系內，以識別及降低虛擬貨幣所具備的風險，其中一項建議即要求各國權責機關就 VCPPS 的營業制定相關的「執照／註冊規範」，以實施有效監管。如此觀之，VCPPS 必須符合洗錢防制的要求，始可被准許營業。指引第 40 條進一步就權責機關如何擬定細部規範，列舉許多規範上可考慮採行的方式：包括運用風險基礎方法（FATF(下同)建議 1）、客戶審查（CDD）（建議 10）、紀錄保存（建議 11）、針對金錢或價值移轉服務制定註冊或申請執照的要求（建議 14）、找出並減緩與新科技有關的風險（建議 15）、要求制訂防制洗錢／打擊資恐計畫（建議 18）

doi:10.6342/NTU201800740

以及報告疑似洗錢或資恐交易（建議 20）等。

第三項 建議的落實與政策執行

指引於第四節臚列了一些可供執法機關參考的建議，以下將簡述並分析指引內的建議是否可完全於我國落實，以及實際執行上將面臨何種困難。

第一款 風險基礎方法與規範基礎方法

指引第 41 條建議為了降低(Mitigate)金融機構以及指定之非金融事業或人員洗錢／資恐風險，應運用風險基礎方法；此代表著不管是金融或非金融的服務提供者，均應花費人力進行風險評估，而非在未經評估下即自動或全盤拒絕提供 VCPPS 或相關服務。我國新修正之洗錢防制法及金融機構防制洗錢辦法爰參酌 FATF 所建議運用之風險基礎方法，如金融機構防制洗錢辦法第 2 條立法說明即謂該辦法係參酌 FATF 所發佈之銀行業風險基礎方法指引第 9 段及第 24 段所訂定。所謂的風險基礎方法，理論上應是以「最適當且有效之方法」達成服務提供機構有效配置資源的目的 [253]，分配較多資源予高風險客戶的監控，對中風險或是低風險的客戶則相對無須耗費過多的監控資源。惟欲落實風險基礎方法，在辨識洗錢／資恐風險時，勢必不能全然以「規範為基礎」制定出一套能被簡易遵循的辨識程序。

有見解因此指出，法律制定上，以規範為基礎的思考模式應退讓，如此才能順應國際潮流；具體執行上應先參考我國實際產業狀況（即交易習慣），識別出有可能構成洗錢或資恐的行為類別，再由該類別去辨識出可能參與其中的洗錢／資

[253] 金融機構防制洗錢辦法第 2 條第 8 項將風險基礎方法定義為：指金融機構應確認、評估及瞭解其暴露之洗錢及資恐風險，並採取適當防制洗錢及打擊資恐措施，以有效降低此類風險。依該方法，金融機構對於較高風險情形應採取加強措施，對於較低風險情形，則可採取相對簡化措施，以有效分配資源，並以最適當且有效之方法，降低經其確認之洗錢及資恐風險。

doi:10.6342/NTU201800740

恐行業，進而按該行業的特性，就風險類型及如何發現風險訂定自律規範[254]。上述見解從 FATF 建議一的解釋文出發，認為「風險評估的本質與內容必須要跟義務人的營業性質與規模相襯[255]」[256]，是以應透過民間機構自我落實為核心。各該行業就各自的特性及風險類型訂定自律規範的作法，對於擁有獨立工會、既有法律明確規定身分之非金融事業或人員確實不失一個良好的洗錢防制落實方案。

但就虛擬貨幣產業而言，目前雖然有 SRO 初步形成之勢，但就整體產業的大小、行業特性、交易類型的風險觀之，要完全依賴 VCPPS 自律規範，恐尚缺乏期待可能性。單就虛擬貨幣產業規模而言，就無法與金融機構相比；從自律架構觀之，亦無法與其他非金融事業或人員如律師、會計師等擁有公會之組織相比；若再從交易涉及的複雜程度、及自律機構如欲親自施行風險為基礎的洗錢防制措施而言，所需之法遵成本更是難以估計。因此綜觀各面向觀察，要落實 VCPPS 自行以風險為基礎的規範模式，尚有一定的難度，初期規範還是可能須以「規範為基礎」來輔助該產業建構一套至少符合 FATF 的洗錢防制標準，待產業風險明確化、自制組織或是公會成形後，再依據實際交易情形研擬細部風險分級的方法。

於此期間內，似可先參照指引第 25 條建議，由各主管機關協同評估虛擬貨幣產品或服務（例如：匯兌服務、貨幣付款機制、虛擬貨幣 ATM、商品、證券等）可能具有之風險，以使相關機關瞭解特定虛擬貨幣產品或服務在洗錢防制／打擊資恐方面，可能如何影響該機關所職掌的職務及相關法規範。先透過此種跨部會

---

[254] 謝昆峯（2017），〈洗錢防制法第七條「以風險為基礎」之意旨及執行之本土化〉，《洗錢防制法律與政策研討會學術論文集》，頁 67。

[255] The nature and extent of any assessment of money laundering and terrorist financing risks should be appropriate to the nature and size of the business.

[256] FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 31 (Feb. 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

doi:10.6342/NTU201800740

的自我評估，有效於各方面—例如犯罪防制、金融市場、稅務等方面—辨識虛擬貨幣可能具有之風險，才能先制定關於虛擬貨幣的基礎規範，待日後產業漸漸茁壯後，再課予業者以「風險為基礎」辨識潛在的洗錢／資恐對象的義務。如此方式既能確保產業發展初期不至於因課與過重的洗錢防制義務而增加法令遵循的成本，又能在產業茁壯期間學習有效的風險分級方法。

第二款 客戶盡職調查

惟不管是初期的以規範為基礎、或是其後漸進實現的以風險為基礎，最初步驟還是須從認識客戶等與實際交易有關的環節開始做起，如此才有足夠訊息判斷客戶風險及交易風險。FATF 就規範初期如何落實 VCPPS 洗錢防制／打擊資恐，於指引第 42 條至 54 條提出規範面的建議規範。如指引 42 條即建議參考 FATF 建議 10，課予 VCPPS 踐行客戶盡職調查(Customer Due Diligence, CDD)的義務，不論是對新客戶或是既有的客戶，均應執行此盡職調查義務。準此，與新客戶建立商業關係時，在客戶識別計畫(Customer Identification Program, CIP）後應利用可靠的、具獨立來源的文件、資料或資訊，完成盡職調查，若屬高風險客戶則再進行加強客戶調查（Enhanced Due Diligence, EDD），以完成整體的認識客戶程序 (Know Your Customer, KYC)。

我國現行規範下，VCPPS 如幣託及 MaiCoin 在對新客戶採取 KYC 程序時，確實會要求客戶提供身分證，有些甚至會要求提供台灣手機的帳單[257]，但通常不會對發出購買交易的帳號做出限制，導致無驗證的帳號亦可進行購買、發送及接

[257] Maicoin（2018），〈帳號及交易安全〉。載於：https://www.maicoin.com/zh-TW/faq/security（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

收虛擬貨幣[258]。因此現行 VCPPS 的驗證機制，尚無法完全瞭解客戶，不知名的客戶仍有可能透過大量購買虛擬貨幣的方式將現金轉換並移轉至國外。有鑒於此，若欲達成全面瞭解客戶的目標，指引第 44 條針對「非當面進行身份辨識與驗證」，建議參照 2013 年 6 月新型支付產品與服務指引與第三方資料庫或其他可靠來源的資訊進行確認，就如同現行金融機構能透過「內政部國民身分證領補換資料查詢系統」、財團法人金融聯合徵信中心下的「Z21 國民身分證領補換資料系統」以及透過「金融機構向戶政機關查詢國民身分證資料作業程序[259]」，逕向戶政機關查詢身分證資料以確保真實性。惟如此驗證尚無法確認身分證是否為遺失證、或完全排除被冒用的可能性。

本文建議參考指引第 45 條建議，鼓勵可轉換虛擬貨幣匯兌業者利用「多重技術」(Multiple Techniques)，於合理範圍內驗證客戶身分。利用多重技術進行認識客戶程序的另一個優點，就是較容易執行與風險相對應的盡職調查方式進行客戶驗證程序，實現以風險為基礎的評估方式。針對高風險客戶，可採行多重技術認證程序，加強客戶調查；針對中風險或是低風險的客戶，則無需執行多道認證程序，而可於線上驗證程序時效仿第一類數位存款帳戶的認證程序，加入視訊及自然人憑證 IC 卡的驗證[260]或是生物辨識技術（Biometric）。如就高風險客戶或是欲開啟超乎平均值的交易權限時，要求本人透過視訊或是親自完成驗證程序、並留下生物跡證(如手機指紋辨識或是至具有指靜脈功能之 ATM)，如此便能確保日後的每一筆交易均是本人為之，除了以科技實現每筆交易的確認客戶程序，又可杜絕人

---

[258] 惟近來有從嚴的趨勢，詳細論述，參照：第五章第三節第二項關於交換者之論述。

[259] 98 年 4 月 29 日金管銀（一）字第 09800164640 號函訂定；金融監督管理委員會 103 年 9 月 11 日金管銀法字第 10300245231 號修訂

[260] 聯合報（2018/01/10），〈第 3 類數位帳戶不能轉帳 王道銀批荒謬〉，https://udn.com/news/story/7239/2922933（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

頭帳戶的問題。倘若原本屬較低風險等級的客戶，日後發現其風險等級已升高為高風險客戶，則可採取暫時停止其交易權限，待通過多重技術認證後再行開啟其交易功能，以利完成既有客戶識別審查，持續追蹤客戶，完成真正意義上的實名制。

如採取以上方式，尚可同時建置「大額交易驗證程序」，如 VCPPS 之客戶欲開啟超過新臺幣 50 萬元之交易、或是當日交易金額逾新臺幣 50 萬元時，自動連線至自然人憑證驗證系統，以便在重複驗證客戶身分程序的同時詢問交易目的，若有可疑之處亦可自動回報專責主管機關(如現行金融機構就大額通貨申報的申報機關為法務部調查局)。除此之外，指引第 44 條尚建議未來可應用至 VCPPS 加強客戶調查的作業程序，例如在進行可疑交易時自動追查客戶的網際網路協定（IP）地址，並在網路上搜尋由該 IP 地址所發起的歷次交易活動資訊，與現在客戶的交易資料相比對，以比對交易模式是否相吻合，但前提是資料的蒐集過程必需符合國內關於資料蒐集或是個人資料保護的規定。

指引第 53 條建議指出，上述由第三方建構的數位身份系統，可與 VCPPS 更緊密結合，以達成防制洗錢／打擊資恐的國際標準。當然，若這些身分驗證系統非由政府所設，可能牽涉第三方身份資訊保管機構及其他相關機構，這些有權審查、監督、驗證客戶並維護數位身份的第三方機構亦應受管制，以確保身份／確認過程的信賴度。

第三款 交易管控

落實認識客戶程序後，落實交易管控的困難度將減少許多。指引第 47 條指出能利用 NPPS 的「多重簽章技術」(Multi-sig)，與去中心化 VCPPS 相整合，以降低交易上的風險。多重簽章技術能提供 VCPPS 限制交易執行的能力，如透過在欲

doi:10.6342/NTU201800740

限制的錢包載入一個總交易上限，限制可移轉之價值以及交易的執行速度。即便如此，以上限制也只適用於本地端 VCPPS 發送虛擬貨幣時，至於發送後的虛擬貨幣移轉至何地、或是做於何種用途，均非現在科技所能限制的範圍。

第四款 法律遵循科技

最後，為盡速克服去中心化可轉換虛擬貨幣在法律遵循以及執法方面帶來的挑戰，上述身份上及交易上的辨識與驗證刻不容緩，指引第 51 條即指出金融機構、指定之非金融事業或人員、開發方、投資人以及在 VC 領域內的各方人員，均應努力開發有助於提升法律遵循的科技。

對此，我國似可建立一負責統籌區塊鏈技術與應用的國家級研究中心，以利公私部門間的整合及溝通。以中國為例，其先從民間開始帶動加密貨幣與區塊鏈之相關產業應用，政府政策方慢慢跟上。如中國人民銀行於 2016 年 1 月召開數字貨幣研討會，對外宣布正在研發數字人民幣，並於 11 月開始就其轄下研究單位，開始招聘金融科技與區塊鏈領域專才；又如，中國工信部信息化和軟件服務業司發布之《中國區塊鏈技術和應用發展白皮書（2016）》，文件詳細列出區塊鏈標準建立工作的時程表，其後於 2017 年 5 月已由「中國區塊鏈技術和產業發展論壇」公佈了《區塊鏈和分散式帳本技術參考架構》標準，成為首個政府指導下之區塊鏈基礎標準[261]。

區塊鏈應用研究中心的建置不僅有助快速達成指引第 51 條之建議，更可同時達成指引第 54 條之建議，讓金融機構與指定之非金融事業或人員可參與有助於客戶身份辨識／確認、交易監督系統的開發過程，進而擬定一個能被眾 VCPPS 機構

[261] 劉柏定（2017），〈區塊鏈技術與應用在中國大陸之發展近況〉，《經濟前瞻》，172 期，頁 72-76。

doi:10.6342/NTU201800740

所接受的共同規範框架和標準。透過制定一個產業的標準化規範，更能凝聚所有虛擬貨幣機構，促使機構間的交易資訊相互流通，如此更有便於辨識金流來源及流向，共同打造一個強化防制洗錢／打擊資恐的企業文化。

第四項 重新評估加密貨幣之建議

本文參照 2015 年 FATF 所發布之「FATF 虛擬貨幣風險基礎方法指引」整理以上建議，惟虛擬資產如加密貨幣隨著科技急速發展，時至今日，3 年前的建議能否有效規範目前快速發展的產業環境不無疑問。2018 年 7 月在阿根廷舉行二十國集團布宜諾斯艾利斯峰會（2018 G20 Buenos Aires Summit）所發表的第 10 點聲明即稱加密資產(Crypto-Assets)具有「造福廣大金融體系及經濟環境的能力」但同時亦有「消費者/投資者保護、市場安定性、逃稅、防制洗錢、打擊資恐」等議題亟需討論，故仍須保持警惕並持續關注 [262]。

FATF 於上述峰會期間向財長和央行行長會議提出的最新報告書(FATF Report to the G20 Finance Ministers and Central Bank Governor，下稱報告書)第 7 點陳稱虛擬貨幣/加密資產因具有極佳的存取性，使其能讓使用者輕易地在世界各地取得，從而使其引來欲移轉或儲存價值之人、洗錢犯罪者、資助恐怖主義者的關注；第 8 點亦確認虛擬貨幣/加密資產除已被販毒、詐騙犯罪所利用外，從趨勢觀之，更是投洗錢犯罪的前置犯罪者之所好，是故將虛擬貨幣/加密資產充作洗錢犯罪的客體近來有增長的趨勢 [263]。

有鑒於此，FATF 已重新對 G20 各國及其他先進國家對於加密貨幣的洗錢防制

---

[262] G20 FINANCE MINISTERS & CENTRAL BANK GOVERNORS MEETING, COMMUNIQUÉ (July 21, 2018), https://g20.org/sites/default/files/media/communique-_fmcbg_july.pdf.

[263] FIN. ACTION TASK FORCE, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS 1-4 (July 2018), http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.

doi:10.6342/NTU201800740

政策進行盤點，約略可分成採取完全禁止式的洗錢防制政策、套用洗錢防制法式的洗錢防制政策及概括式的洗錢防制政策。簡述如下：

1. 完全禁止式的洗錢防制政策[264]
   此類政策的洗錢防制方向是以完全禁止虛擬貨幣/加密資產在國內進行交易為主。按 FATF 可再行區分成完全禁止虛擬貨幣/加密資產於國內使用的「完全禁止」型以及僅禁止虛擬貨幣/加密資產與金融機構有任何往來的「半禁止」型模式。

2. 套用洗錢防制法式的洗錢防制政策[265]
   此類政策的洗錢防制方向是將虛擬貨幣/加密資產納入防制洗錢與打擊資恐的法規範內，實行方式之一可能是透過對於現行的洗錢防制法進行解釋，將從事虛擬貨幣/加密資產的匯兌業者解釋成如同價值移轉服務、銀行或其他支付機構，而有著套用洗錢防制法的空間。

3. 概括式的洗錢防制政策[266]
   此類政策的洗錢防制方向較為簡略，其未有專門用於規範虛擬貨幣/加密資產的專法，但是有概括式的規範要求金融機構必須通報可疑交易。所謂的可疑交易涵蓋範圍非常廣泛，其中除與金融機構間之交易，尚包括與虛擬貨幣/加密資產有關的任何交易。更有甚者會將既有僅適用金融機構的通報規範直接套用至虛擬貨幣/加密資產匯兌業者，令其履行通報義務。

上述洗錢防制政策均有國家採行，另外有尚未明確採行何種洗錢防制政策但是正積極立法，擬定相關法規範的國家。FATF 爰整理繪表如下:

表 七：G20 各國對虛擬貨幣/加密資產之洗錢防制政策

目前所採行的洗錢防制方式	國家
完全禁止式的洗錢防制政策	中國、印度、印度尼西亞
套用洗錢防制法式的洗錢防制政策	澳大利亞、法國、德國、意大利、日本、瑞士、美國
概括式的洗錢防制政策	阿根廷、南非
立法中國家	巴西、加拿大、歐盟、墨西哥、荷蘭、俄羅斯、沙烏地阿拉伯、韓國、西班牙、土耳其、英國

資料來源：FATF Report to the G20 Finance Ministers and Central Bank Governors

264 *Id.* at 2.
265 *Id.*
266 *Id.*

doi:10.6342/NTU201800740

根據上表可知目前各國對虛擬貨幣/加密資產所採行之洗錢防制政策各不相同，且並非各國均已著手規劃如何處理加密貨幣之洗錢防制議題。FATF 於報告書第 11 點即稱虛擬貨幣/加密資產的洗錢防制環境正面臨前所未有的轉變，在此科技日新月異所造就的易變環境下，因各國的步調未必相同，所以也就導致洗錢防制的一致性難以達成。當各國各自採取不同方向的洗錢防制政策，將有可能使得虛擬貨幣/加密資產匯兌業者面臨不同的洗錢防制標準，為將利益最大化，其將有可能透過法規套利(Regulatory Arbitrage)的方式選擇洗錢防制力度相對較低的國家作為設立地點的首要考量，以讓具高流通性的加密貨幣產業能以較低的成本取得對外的合法性。

FATF 報告書第 12 點已表示將於 2018 年 9 月休會期間開會討論 FATF 如何將現有的防制洗錢及打擊資恐標準應用至虛擬貨幣/加密資產上，另於 2018 年 10 月將會評估為因應虛擬貨幣/加密資產因其使用之技術所生之特性，是否有需要將現行的 40 項建議予以更新，以確保現有建議的各個面向包括：客戶盡職調查、金錢及價值移轉服務、電匯、監理與執法等議題均能有效套用至虛擬貨幣/加密資產上。報告書第 14 點更進一步揭示將會以協助公部門及私部門持續降低洗錢的風險為目標，重新審視本文所引用之 2015 年「FATF 虛擬貨幣風險基礎方法指引」。有鑒於此，本文所提及的 FATF 建議很有可能即將再度進行最新的檢視，屆時也許會有更新的資訊尚待補充。

第五項 小結

虛擬貨幣支付產品與服務商(VCPPS)起初在規範上確實需要投入許多的研究及規劃，從識別應規範的對象為何，即須灌注許多的研究資源。本文粗略以 FATF 虛擬貨幣風險基礎方法指引為鑒，認為除了 VCPPS 外，尚應辨識和 VCPPS 建立

doi:10.6342/NTU201800740

業務往來的金融機構、與虛擬貨幣相關的金錢與價值移轉服務(MVTS)及新興支付產品及服務（NPPS）。成功辨識以後，再結合公私部門，達成規範時程上的共識，以漸進式的規範要求上述業者須得到營業許可，首要規範對象應是提供可轉換虛擬貨幣的節點—亦即現實貨幣與虛擬貨幣中間的匯兌窗口，次要規範對象則是管制「不提供虛擬和法定貨幣之間的交易或兌現服務」但卻提供「金融機構寄送、接收和儲存 VC 的指定之非金融事業或人員」，至於使用虛擬貨幣購買商品或服務的使用者，則得斟酌是否須納入規範範圍內。

至於如何真正落實規範，仍應回歸運用風險基礎方法來辨識風險，起初似可先以規範為基礎作為引導，既不會對新創科技公司課予過大的法令遵循成本，又可實際觀察我國虛擬貨幣產業的高風險族群，以利往後制定專門的應對措施。是以在規範上，可先參考指引所提供的諸多建議，如利用多重技術辨識及驗證客戶身分、成立研究中心、公私部門結合共同開發有助於提升法律遵循的科技、成立虛擬貨幣公會、制定標準化作業模式以及建構一個有利於公部門於各工會成員間追查金流來源及流向的資訊共享平台。在完成以上基礎規範的建置與落實後，我國始能按指引第 39 條所建議的，有效率且有效地和國際合作，協助其他國家對抗洗錢(FATF(下同)建議 40)－包括司法互助（建議 37）；協助辨識、凍結、扣押並沒收可能以虛擬貨幣形式取得的犯罪所得及犯罪工具（建議 38）；並於發現虛擬貨幣相關的罪行時提供有效的引渡協助（建議 39）。

本節解析 FATF 訂定之虛擬貨幣洗錢防制的相關建議，辨識出首要規範對象為提供可轉換虛擬貨幣的節點，惟此概念仍然過於模糊，尚需將其定義以更細緻化的分類方式加以區分。本文爰參考較具加密貨幣洗錢防制經驗之美國法為例，特定 FATF 所指稱之匯兌加密貨幣與現實貨幣之間的「節點」。

doi:10.6342/NTU201800740

第二節　以美國為例

第一項 主管機關

金融犯罪稽查局(Financial Crimes Enforcement Network, FinCEN)係美國負責金融犯罪之主管機關，其上級機關為恐怖主義和金融情報辦公室(Office of Terrorism and Financial Intelligence, TFI)，隸屬美國財政部[267]。美國尚有其他與金融相關之執法部門，例如主管財政情報與分析之情報及分析辦公室[268]（Office of Intelligence and Analysis, OIA）與財政部恐怖分子資助和金融犯罪辦公室[269]（Office of Terrorist Financing and Financial Crimes, TFFC）等是。

第二項 適用法規

美國最主要涉及洗錢的法案，有 2001 年通過之愛國者法案(USA PATRIOT Act)和銀行保密法[270]（Bank Secrecy Act, BSA）。銀行保密法也稱為貨幣和對外交易報告法（Currency and Foreign Transactions Reporting Act of 1970 (31 U.S.C. 5311 et seq.)）。該法案主要可分為金融紀錄的保存與貨幣和外匯交易報告兩個部份[271]。前者主要授權財政部制定一系列的金融紀錄規範，如通貨交易申報(Currency Transaction Reports, CTRs) 和可疑活動報告(Suspicious Activity Reports, SARs)[272]，

---

[267] *Terrorism and Financial Intelligence*, U.S. DEP'T TREASURY, https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx (last updated May 23, 2018).

[268] *Office of Intelligence and Analysis*, DEP'T HOMELAND SECURITY (July 13, 2018), https://www.dhs.gov/office-intelligence-and-analysis.

[269] *Terrorist Financing and Financial Crimes*, U.S. DEP'T TREASURY, https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorist-Financing-and-Financial-Crimes.aspx (last updated Dec. 2, 2010).

[270] 張漢宜（2011），〈美國反洗錢，衝擊全球金融〉，《天下雜誌》，373 期。載於：https://www.cw.com.tw/article/article.action?id=5003762（最後瀏覽日：2018/04/14）

[271] FED. DEPOSIT INS. CORPORATION, BANK SECRECY ACT, ANTI-MONEY LAUNDERING, AND OFFICE OF FOREIGN ASSETS CONTROL SECTION 8.1, https://www.fdic.gov/regulations/safety/manual/section8-1.pdf (last visited July 21, 2018).

[272] *Id.* at 1.；我國對此原先有另外制定「金融機構對達一定金額以上通貨交易及疑似洗錢交易申報

doi:10.6342/NTU201800740

以利主管機關於偵查有無逃稅或在發生洗錢、詐騙案時，能迅速透過相關資訊建立有利於起訴的證據。後者則較偏向規範各種超過免申報數額(1 萬美金)的交易型態[273]。

第三項 立法解釋

根據美國金融犯罪稽查局自 2011 年至 2014 年針對虛擬貨幣所做出的一系列函釋，能得出加密貨幣之重點洗錢防制對象並非從持有者著手規範[274]。原因在於比特幣採取全雙向流通性虛擬貨幣架構與公鏈的區塊鏈技術，導致任何人均能隨時參與比特幣的交易。如此便利的取得模式將使虛擬貨幣持有者的基數難以掌控，而且虛擬貨幣本身存有化名性的特性，根本無法透過現有的執法技術對一般的使用者作出有效的規範。

第一款 以行為態樣為主的規範模式

如前述，欲規範虛擬貨幣，需考量時間、成本等諸多因素，以取得最有效之洗錢防制效果與洗錢防制成本之間的平衡。為達成此目標，FinCEN 改採以行為態樣為其規範重點，先著重於解釋 31 CFR § 1010.100(ff)之「金融服務商」(Money Services Business, MSB)。根據 ff 段，MSB 的涵蓋範圍包括所列舉的 7 種項目，只要有分支機構在美國領地內從事所列舉之行為，不管係臨時或永久從事，均受規範所及。其中與虛擬貨幣關係最密切的規定，位於 MSB 所列舉的第五個項目—匯兌業者(Money Transmitter)。根據 31 CFR § 1010.100(ff)(5)(i)(A)，匯兌業者係從事資金移轉或提供匯兌服務(Money Transmission Services)之人。所謂「匯兌服務」，

辦法」，惟該法規現已由主管機關另外訂入為規範各別對象所訂定之「防制洗錢與打擊資恐施行及申報辦法」。

[273] *Id.*

[274] *Administrative Rulings*, FINCEN, U.S. DEP'T TREASURY, https://www.fincen.gov/resources/statutes-regulations/administrative-rulings (last visited July 15, 2018).

doi:10.6342/NTU201800740

指的是：「透過任何方式接受貨幣、資金、或其他相當於貨幣之有價物，並將之從一人移轉至另一人或其他地點」。根據上開定義，匯兌業者所提供之匯兌服務並不區分虛擬貨幣或是法定貨幣，只要所提供的服務是用於匯兌「相當於貨幣之有價物」即該當匯兌服務[275]。

由上可知，FinCEN 對於於金融服務商(MSB)的定義相當廣泛，因此給予主管機關非常大的管轄空間與權限，此為美國法以行為態樣為規範對象之優點。美國法若無金融服務商此一概念，則將與我國一樣，面臨僅能對法定貨幣適用金融相關法規，一旦規範之對象未經定義，即面臨無從管制之窘境。以下詳述之。

依美國聯邦法規(The Code of Federal Regulations, CFR)及 FinCEN 對貨幣之定義，所謂「貨幣」，係指流通且習慣上使用(circulates and is customarily used)、具法償性質(legal tender)、由國家發行、且被接受為交易媒介(accepted as a medium of exchange)。符合上述條件之貨幣，有美國銀幣憑證—即「銀券」(U.S. Silver Certificates)、美國國幣(U.S. Notes)、聯邦儲備鈔券(Federal Reserve notes)及由其他國家官方所承認並且於流通上、習慣上當成交易媒介使用的鈔券[276]。貨幣交易如構成結構性交易，有相關的申報義務。所謂「結構性交易」，依美國法下之定義，係指任何人或團體試圖進行單筆或數筆、不論金額多寡、不論係經由單家或數家金融機構、任何時間點內、以任何方式所為之貨幣交易行為[277]。上述交易行為按

---

[275] FIN. CRIMES EN'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[276] FIN. CRIMES ENF'T NETWORK, FINCEN FORM 105 - CURRENCY AND OTHER MONETARY INSTRUMENTS REPORT (2011), https://www.fincen.gov/sites/default/files/administrative_ruling/fin-2011-r001.pdf; 31 CFR § 1010.100(m); 31 CFR§ 103.11(h).

[277] 31 CFR § 1010.100(xx) a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose

doi:10.6342/NTU201800740

31 CFR §§ 1010.311, 1010.313, 1020.315, 1021.311, 1021.313 各部分的子部分規定，有貨幣交易申報之義務，如有人或團體於單日總和的交易數額超過$10,000 美元之申報門檻，即須通報。但虛擬貨幣因無法被解釋成 31 CFR § 1010.100(m)之貨幣，故也無庸遵循 31 CFR § 1010.100(xx)關於結構性交易(Structure)之定義及衍生之法律效果。

但因為美國法存在金融服務商的概念，所以美國法在解釋虛擬貨幣時有了許多轉圜空間，無須考量虛擬貨幣的法律定性，僅需符合所規範的行為態樣，即可利用匯兌業者條款予以規範。因而相較於現實的「貨幣」，FinCEN 即能將一個作用近似貨幣且在某種環境下有著與貨幣相去不遠性質、卻又不完全具有所有貨幣應有功能[278]之交易媒介—亦即虛擬貨幣[279]—逕行適用 31 CFR § 1010.100(ff)(5)以下關於匯兌業者(金融服務商的一種)之規定。蓋虛擬貨幣不具法償性質，但其下位概念「加密貨幣」卻又具有可轉換的性質，在全雙向流通性虛擬貨幣架構下，此類加密貨幣多數具備與現實貨幣匯兌的能力，或是在功用運作上似於現實貨幣。

第二款 虛擬貨幣匯兌的規範

上述解釋雖然使得規範虛擬貨幣有了法源依據，然符合「匯兌」的服務態樣繁多，光靠如此模糊的定義仍無法讓大眾知悉在何種情形下始受銀行保密法的法效所及。為此，FinCEN 於 2013 年發佈《金融犯罪稽查應用至虛擬貨幣發行者、交換者或使用者(指導)規範》，將創造、取得、分配、交換、接收、匯兌虛擬貨幣

---

of evading the reporting requirements…

[278] 依據傳統貨幣銀行學，貨幣必須具備「交易媒介」、「計價單位」、「價值儲藏」及「延期支付」四大功能。

[279] FIN. CRIMES ENF'T NETWORK, *supra* note 275, at 1. ("Virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.)

doi:10.6342/NTU201800740

之人逐一分類成以下三種：

1. 使用者(User)[280]：
指以取得虛擬貨幣為主並將其用於購買貨品或服務之人。普通民眾如以虛擬貨幣用於消費或是單純買來投資，待增值後再行轉賣亦屬之。

2. 交換者(Exchanger)[281]：
指以商業為目的從事虛擬貨幣與真實貨幣交換或與其他虛擬貨幣交換之人。此類型的業者又可以細分為場外交易平台、虛擬貨幣經紀業者、交易所三類，共同之處在於均從事匯兌服務，詳如第五章第三節。

3. 發行者(Administrator)[282]：
指以商業為目的發行（投入市場）虛擬貨幣並且有權力贖回（退出市場）虛擬貨幣之人。最典型模式為首次代幣發行，若發行的「代幣」於分類或性質上能用於支付或是變相匯兌相當於貨幣之有價物時，代幣發行人即會構成 FinCEN 欲規範之發行者。

以下說明之。

第一目　使用者

使用者能透過各種方式取得虛擬貨幣，例如：賺取、收割、挖掘、創造、自動取得、生產、或購買等方式，但使用者如何取得虛擬貨幣並非 FinCEN 關注之重點[283]。FinCEN 所關注的是虛擬貨幣被使用的方式以及為誰的利益而使用。蓋從定義上而言，難認使用者有從事「匯兌業務」的行為，因此使用者並不屬於 MSB，無需遵守 FinCEN 針對 MSB 所制定關於註冊取得牌照、通報可疑交易、檔案保存等一系列的規範。

具體而言，FinCEN 於 2014 年 1 月所公布之「FinCEN 適用於虛擬貨幣挖礦作

---

[280] FIN. CRIMES ENF'T NETWORK, FIN-2014-R012, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY PAYMENT SYSTEM (2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf.
[281] *Id.* at 2.
[282] *Id.*
[283] *Id.*

doi:10.6342/NTU201800740

業規範」[284]針對挖礦公司可否以其生產之虛擬貨幣用於購買貨品或服務以及用於購買現實貨幣做出說明。首先，FinCEN 並不認為個人挖礦與法人挖礦應做區分，亦不認為將所挖掘到的虛擬貨幣用於購置物品、服務、清償債務、盈餘分派會影響使用者的本質。FinCEN 係以行為目的為規範主體，只要使用者係基於個人用途來使用虛擬貨幣，而非為他人的利益來使用虛擬貨幣，使用者就不會誤入「接受」和「匯兌」虛擬貨幣的範圍[285]。FinCEN 在此所指的是匯兌虛擬貨幣不能單純觀察虛擬貨幣的流向，而是需要從使用虛擬貨幣之人「欲將虛擬貨幣用於何種用途」以及「欲基於誰的利益使用虛擬貨幣」兩點來綜合判斷。例如礦工獲得虛擬貨幣後將其轉送至他人換取服務或是物資，因為是基於個人利益用於購買個人所需之物品，所以不會構成匯兌服務。FinCEN 表示若有公司完全是基於公司投資的需求從事投資所必須的活動，如買賣可轉換的虛擬貨幣或是利用可轉換的虛擬貨幣收付帳款，因用途上是屬於個人用途且是以投資為目的而進行買賣可轉換虛擬貨幣的行為，故不構成匯兌服務，無須遵守銀行保密法的規範。

按 FinCEN 對於使用者的解釋，挖礦公司在生產虛擬貨幣、使用虛擬貨幣換取貨物及服務的範圍內，無須向主管機關註冊或受銀行保密法的規範。惟須注意，當使用者使用虛擬貨幣向賣方購買貨品時，不得約定使用者向第三方支付虛擬貨幣，否則將違反「基於個人用途且不得為他人之利益使用虛擬貨幣」的規範目的。由此可見，使用者不得透過利益第三人契約來規避只能與相對人交易的規定。另外，為了達成「基於個人用途」所需之交易，使用者只能在此範圍內將虛擬貨幣轉換成現實貨幣的形式，或是將一種虛擬貨幣轉換成另外一種虛擬貨幣。按此邏

---

[284] FIN. CRIMES ENF'T NETWORK, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY 1-5 (2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf..

[285] *Id.*

doi:10.6342/NTU201800740

輯，使用者當然也可以以自我投資為目的，將所有的虛擬貨幣資產轉換成現實資產或是他種類的虛擬貨幣[286]。

第二目　交換者

FinCEN 於 2013 年發布之《金融犯罪稽查應用至虛擬貨幣發行者、交換者或使用者(指導)規範》[287]，是第一份針對提供虛擬貨幣服務的金融服務商(MSB)進行進一步角色區分的官方指引。按此指引，交換者與發行者因存在大量共通之處，包括接受或匯兌可轉換之虛擬貨幣、及買賣可轉換之虛擬貨幣，在功能上可輕易用於移轉金錢或是價值，是以 FinCEN 在法律定位上將其歸類為提供金融服務之匯兌業者(Money Transmitter)。

金融服務商按美國聯邦規則彙編(CFR)31 篇（Title），B 章（Subtitle），X 節（Chapter），1010 部分（Part），A 子部分（Subpart）100 小節（Section）ff 段可分為：外匯經紀商(Dealer in Foreign Exchange)、票據支付商(Check Casher)、旅行支票或匯票之發行業者或是承銷商(Issuer or Seller of Traveler's Checks or Money Orders)、預付服務供應商(Provider of Prepaid Access)、匯兌業者(Money Transmitter)、美國郵政(U.S. Postal Service)及預付服務承銷商(Seller of Prepaid Access)等 7 類。虛擬貨幣之使用者並不會被歸類為匯兌業者，因其並非從事資金移轉或提供匯兌業務(Money Transmission Services)之人。反觀交換者因符合匯兌業務「透過任何方式接受貨幣、資金、或其他相當於貨幣之有價物，並將之從一人移轉至另一人或其他地點」之定義，故須受銀行保密法所拘束。交換者原則上雖受拘束，但美國法另有一套排除匯兌業務之制度，若符合其規範則無庸被歸類為交換者而受 FinCEN

[286] *Id.*
[287] FIN. CRIMES ENF'T NETWORK, *supra* note 275, at 1-5.

doi:10.6342/NTU201800740

之監管。本文於討論例外排除法則前，擬先介紹 FinCEN 所認為原則上可能構成交換者及發行者的三種可轉換虛擬貨幣交易態樣(Convertible Virtual Currency Activity)：從事電子貨幣和電子稀有金屬交易之經紀商和交易商(E-Currencies and E-Precious Metals)、中心式之虛擬貨幣(Centralized Virtual Currencies)、去中化之虛擬貨幣(De-Centralized Virtual Currencies)。

一、電子貨幣和電子稀有金屬交易之經紀商和交易商

FinCEN 於 2008 年所發布的《套用匯兌業者定義至從事貨幣和商品交易之經紀商和交易商指引》[288]指出若經紀商(Broker)和交易商(Dealer)從事收受和匯兌資金之行為完全是基於善意，其與客戶或是為了與客戶進行商品或貨幣的買賣，不會被認為從事貨幣匯兌業務(engaged as a business in the transfer of funds)，從而不會構成匯兌業者。所謂「從事貨幣匯兌業務」，依 31 C.F.R. § 103.11(uu)(5)(i)[289]所述，係指透過任何方式接受貨幣或貨幣形式呈現之資金、或使用各式金融機構(如美國聯邦儲備銀行)、電匯網路、或利用其他從事貨幣匯兌業務之人匯兌貨幣、資金或其他相當於貨幣和資金之有價物。若要被認為非「從事貨幣匯兌業務」，所接收或是所匯兌之資金必須是非以執行或是交割該筆資金為主要目的；申言之，必須是附隨於主要交易目的所為之資金移轉，始得將其從「從事貨幣匯兌業務」加以排除[290]。例如 31 C.F.R. § 103.11(uu)(5)(ii)即將證券交易和不動產交易交易商排除在「從事貨幣匯兌業務」者外，蓋於所列舉之案例中，匯兌資金之行為完全是基於

---

[288] FIN. CRIMES ENF'T NETWORK , FIN-2008-G008 USA PATRIOT ACT, APPLICATION OF THE DEFINITION OF MONEY TRANSMITTER TO BROKERS AND DEALERS IN CURRENCY AND OTHER COMMODITIES (2008), https://www.fincen.gov/sites/default/files/guidance/fin-2008-g008.pdf.

[289] FinCEN 原文文獻中的 31 CFR § 103 因條文修正之故已於 2011 年 3 月 1 日起移至 31 CFR Chapter X，故此後所呈現的 31 CFR § 103.11 其實即是對應到現行法 31 CFR § 1010.100。因此 31 CFR § 103.11(uu)(5)(i)會對應到現行法 31 CFR § 1010.100(ff)(5)(i)，在此合先敘明。

[290] Generally, the acceptance and transmission of funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself.

doi:10.6342/NTU201800740

善意，與客戶之間之所以有貨幣匯兌是為了買賣證券或是不動產，故不會構成(uu)(5)(i)所稱之「從事貨幣匯兌業務」之人。

依上所述，欲構成排除事由，須經紀商和交易商在善意的情況下讓資金附隨於貨幣或是商品所進行之交易，讓資金的流動看起來是基於履行一個已成立的契約所生之義務。加密貨幣的匯兌若非基於善意或非為履行某種契約上義務，該匯兌行為很自然地將不會是實際履行契約時的必要因素(Fundamental Element)，從而其將構成「從事匯兌業務」，而使交易商被歸類為匯兌業者，須遵守銀行保密法對於洗錢防制的相關規範。如此解釋，即能說明為何礦工使用加密貨幣購買商品的行為並不會構成「交換者」、反而被 FinCEN 歸類為「使用者」，無需特別課與其洗錢防制的義務。另須注意的是，一旦加密貨幣持有人並非以履行某種契約上義務為目的直接移轉加密貨幣予契約相對人，所牽涉之第三人極有可能會構成「交換者」。例如由第三人負責匯兌各個客戶帳戶之間的資金、或是准許第三人和客戶之間有直接的資金往來（如由第三人直接將資金轉至客戶的帳戶內等）。

綜上所述，匯兌業者客觀上須有接受貨幣、資金、或其他相當於貨幣之有價物，並將其從一人移轉至另一人或其他地點的外觀，此外尚須認定其有「從事匯兌業務」。具體的判斷方式為檢視匯兌貨幣之人是否係為履行一個已成立契約所生之義務而匯兌貨幣。若貨幣移轉僅發生於契約兩造當事人，則可認為兩者均屬於「使用者」；若有契約當事人以外之人參與貨幣的匯兌，協助當事人移轉貨幣或是相當於貨幣的有價物，該第三人即可能構成符合電子貨幣和電子稀有金屬交易態樣的「交換者」。又因為匯兌業者所匯兌的標的可為任何可能相當於貨幣之有價物，故以上區分加密貨幣匯兌之經紀商和交易商之方式，可完全適用於加密貨幣或是他種虛擬貨幣。

doi:10.6342/NTU201800740

二、中心式之虛擬貨幣

採行中心式可轉換虛擬貨幣交易態樣的交換者，顧名思義有著集中式的儲存庫(Repository)，控制人通常也會是虛擬貨幣的發行人。FinCEN 認為發行人所建立的架構若准許所發行的虛擬貨幣自由在使用者帳戶間進行移轉，具有控制權之發行人同時會構成交換者 [291]。由此可見，本文第二章所述及之「是否容許虛擬貨幣於帳戶間移轉」有其區別實益。採行半單向流通性架構之虛擬貨幣，雖不容許現實貨幣與虛擬貨幣間的匯兌，但因貨幣發行人容許貨幣於其設計的交易環境內互相移轉，是以發行者將會因其設立之交易系統，而間接充當交換者角色，此為非直接從事不同貨幣間的匯兌，卻因容許使用者間的貨幣移轉，而成為交換者之例。

倘若中心式虛擬貨幣的發行者採行全雙向流通性架構，就現實貨幣與虛擬貨幣之間的匯兌因涉及 1.發行者發行虛擬貨幣及 2.利用虛擬貨幣為對價交換現實貨幣，從而同時兼有發行者及交換者的角色。FinCEN 於定義匯兌業者時，亦考慮此類交換者與發行者的競合關係，涵攝上先將新發行的加密貨幣解釋為「可替代的有價物」，再將加密貨幣移轉至交易相對人所開立之虛擬貨幣帳戶解釋為「匯兌有價物至其他地點」，以符合匯兌業者之定義，成功適用銀行保密法。以買受人持現實貨幣向出賣人購買加密貨幣為例，案例內的出賣人由發行者與交換者同時兼任；虛擬貨幣所採行之架構會傾向於中心式虛擬貨幣架構，因為在此種架構內發行之虛擬貨幣數額或是移轉之虛擬貨幣完全取決於發行者，其具備著帳本紀錄的直接更改權限，無須如去中心化架構經各個節點驗證獲得工作量證明後始得確認交易資訊為有效且已經被執行。

有論者可能主張上述「以現實貨幣購買虛擬貨幣」之案例中，可將提供虛擬

---

[291] FIN. CRIMES ENF'T NETWORK, *supra* note 275, at 5.

doi:10.6342/NTU201800740

貨幣匯兌服務之人解釋成「商品或服務」的仲介者，亦即在出賣人(發行者)與買受人(使用者)所訂定之買賣契約中，將交換者認為是幫助使用者與發行者成立並且履行商品買賣義務之履行輔助人，進而將虛擬貨幣匯兌行為認定為是履行一個已成立的契約所生之義務，所以符合前文所述之「從事貨幣匯兌業務」之例外。對此問題，FinCEN 認為當買賣標的為貨幣、虛擬貨幣或是相當之有價物時，會構成「附隨於主要交易目的所為之資金移轉例外」之例外，在此種情形仍應受銀行保密法的規範[292]。

三、去中化之虛擬貨幣

最後，涉及去中心式可轉換虛擬貨幣交易態樣的虛擬貨幣，為同時符合「欠缺集中式儲存庫和管理者」以及「能夠透過自身的計算能力獲取虛擬貨幣」兩項表徵之虛擬貨幣。FinCEN 認為運用此類虛擬貨幣購買商品或服務因僅構成使用者，故不會構成匯兌業者，惟一旦運用此類貨幣以換取現實貨幣或相當於貨幣之有價物為代價而售予他人時，則會構成匯兌業者，須受銀行保密法的規範。

第三目　發行者

發行者為最明顯應受管制之業者，蓋其透過發行虛擬貨幣，並且以營利為目的來販售所發行的虛擬貨幣。發行者也可以理解成交換者的上位類型，兩者之間的差別在於發行者本身即為虛擬貨幣的來源，無須另行建構一套媒合系統，促成交易者之間成立虛擬貨幣的交易。發行者並非無償發行虛擬貨幣，當其將所創造的虛擬貨幣基於營利(獲取貨幣或相當於貨幣之有價物)之目的轉讓予他人時，因任何有買賣可轉換虛擬貨幣以換取現實貨幣之情事即構成匯兌服務，故從事人員會被歸類為金融服務商下的匯兌業者，應遵守銀行保密法以及受到 FinCEN 的監管。

---

[292] FIN. CRIMES ENF'T NETWORK, *supra* note 275, at 4-5.

doi:10.6342/NTU201800740

目前第三大虛擬貨幣瑞波幣的發行公司 Ripple—即為曾因違反監管法令而受裁罰的發行者。以下說明該案例[293]：

Ripple Labs 是一家在德拉瓦州註冊、總部位於加州的公司。子公司 XRP Fund II, LLC 於 2013 年成立，設於加州；後於 2014 年 6 月更名為 XRP II, LLC。Ripple Labs 是一家提供匯兌虛擬貨幣為主要業務的公司，其所發行之虛擬貨幣 XRP，是一種既存的虛擬貨幣，無須像它種虛擬貨幣需透過「挖礦」的方式來產生。Ripple Labs 曾向法院宣示其主要業務包括提供虛擬貨幣的匯兌、即時性的虛擬貨幣交易和資金調度業務、和提供以虛擬貨幣代替現實貨幣為帳面上交易的服務[294]。

Ripple Labs 自 2013 年 3 月 6 日開始販售其所生產的瑞波幣(XRP)，當時並未向美國金融犯罪稽查局(FinCEN)註冊成為金融服務商。FinCEN 隨後於 2013 年 3 月 18 日公佈《金融犯罪稽查應用至虛擬貨幣發行者、交換者或使用者(指導)規範》[295]明確定義何者會構成匯兌業者而應受銀行保密法的規範。

Ripple Labs 於 FinCEN 公佈規範虛擬貨幣的函釋後，仍繼續販售瑞波幣以換取法定貨幣，且在販售的過程中並未聘雇任何與洗錢防制相關的專業人員來幫助公司遵循銀行保密法的相關規範。

經 FinCEN 調查，Ripple Labs 的子公司 XRP II, LLC 是母公司特別成立從事虛擬貨幣販售及匯兌業務的子公司，換句話說，是由子公司代母公司進行關於虛擬貨幣的所有交易。子公司雖於 2013 年 9 月 4 日依法向 FinCEN 註冊成為金融服務商，卻未依法擬訂一套有效率的洗錢防制計畫(Anti-Money Laundering

---

[293] Ripple Labs, Inc. v. Lacore Enterprises, LLC, Motion for Preliminary Injunction, 13-cv-5974-RS/KAW (N.D. Cal. 2013).
[294] FIN. ACTION TASK FORCE, ATTACHMENT A: STATEMENT OF FACTS AND VIOLATIONS (2014), https://www.fincen.gov/sites/default/files/shared/Ripple_Facts.pdf.
[295] FIN. CRIMES ENF'T NETWORK, *supra* note 275, at 4-5.

doi:10.6342/NTU201800740

("AML")Program)[296]、未依法向主管機關提出可疑活動報告(Suspicious Activity Reports, SARs)[297]、未按資金匯兌規則(Funds Transfer Rule)[298]的規定針對相當於或大於 3000 美金的交易進行驗證、保存和收集交易資訊、亦未按資金流通規則(Funds Travel Rule)[299]，針對相當於或大於 3000 美金的交易進行交易資訊的彙整並傳遞給下一個金融中間機構或是接收資金的金融機構。

XRP II 除未在時間內遵循匯兌業者應遵循的法律規定外，更是知法犯法。FinCEN 於對外公佈之 Ripple Facts 報告中敘明一例。當買家開出欲以 25 萬美金購買瑞波幣時，XRP II 屈服於買家，而忽略銀行保密法於客戶確認身分程序(Know Your Customer, KYC)應盡之義務。隨後經主管機關調查，始得知該買家曾犯有三項和郵寄爆裂物有關的重罪[300]。基於 XRP II 多次忽視應遵循的法律規定，FinCEN 最終對該公司處以 70 萬美金的罰鍰。

Ripple 案顯示了美國當局對於虛擬貨幣洗錢防制的決心。FinCEN 透過函釋，將匯兌業者進一步區分為使用者、交換者、發行者三種類型，除了非以營利為目的的使用者外，其他有收取手續費的平台均會構成交換者，更遑論以獲利為目的發行虛擬貨幣的發行者了。FinCEN 最新實務見解顯示，其認為現行各個虛擬貨幣交易網站以及欲透過首次代幣發行(Initial Coin Offering, ICO)銷售虛擬貨幣的發行者，在構成發行者或是交換者的前提下，應構成從事匯兌服務的匯兌業者，而匯兌業者因屬金融服務商下的一種態樣，故須受美國銀行保密法所規範[301]。前述見

---

296 31 U.S.C. §§5318(a)(2) and 5318(h); 31 C.F.R. § 1022.210.
297 31 C.F.R. § 1022.320(a)(2).
298 31 C.F.R. § 1010.410(e).
299 31 C.F.R. § 1010.410(f).
300 United States v. Roger Ver, CR 1-20127-JF (N.D. Cal.2002)
301 FIN. CRIMES ENF'T NETWORK, *FinCEN's Letter to U.S. Senator Ron Wyden*, COINCENTER.ORG, (Feb. 13, 2018) https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf.

doi:10.6342/NTU201800740

解來自於 FinCEN 法律事務助理秘書 Drew Maloney 寄給美國參議員 Ron Wyden 的信，信中認同性質似於加密貨幣的貨幣型代幣因可用於兌換其他貨幣或相當於貨幣之有價物，故應遵守 AML/CFT 的相關規範[302]，但其後於信中亦同意並非所有以首次代幣發行的代幣均會受銀行保密法的監管，尚需判斷代幣的性質，個別判斷是否適用；同時亦已與美國證券交易委員會(Securities and Exchange Commission, SEC)與商品期貨交易委員會(Commodity Futures Trading Commission, CFTC)共同研究對於 ICO 應如何分配 AML/CFT 的職權[303]。當職權釐清後，FinCEN 有可能會正式公告 ICO 應適用銀行保密法的規範標準，之後若有業者被歸類為加密貨幣、代幣的交換者或是發行者則須遵守銀行保密法的相關規範，如同 Ripple 裁罰一案 FinCEN 要求 XRP II 公司採取之一系列洗錢防制措施，始不會被開罰。

第四項 例外不適用銀行保密法之情形

第一款 附隨性例外

附隨性例外(Integral Service Exemption)於前文已有提及，為將其明確化爰參考 FinCEN 對此項例外的解釋整理如下[304]：

1. 匯兌服務必須是附隨於以履行某種債之關係為主要目的(如為獲取服務或

---

[302] Generally, under existing regulations and interpretations, a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency is a money transmitter and must comply with AML/CFT requirements that apply to this type of MSB [money services business]. An exchange that sells ICO coins or tokens, or exchanges them for other virtual currency, fiat currency, or other value that substitutes for currency, would typically also be a money transmitter.

[303] "FinCEN is working closely with the [SEC] and the [CFTC] to clarify and enforce the AML/CFT obligations of businesses engaged in ICOs activities that implicate the regulatory authorities of these agencies. The application of AML/CFT obligations to participants in ICOs will depend on the nature of the financial activity involved in any particular ICO. This is the matter of the facts and circumstances of each case."

[304] FIN. CRIMES ENF'T NETWORK, *supra* note 280, at 3-5.

a) The money transmission component must be part of the provision of goods or services distinct from money transmission itself; b) The exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission; c) The money transmission component must be integral (that is, necessary) for the provision of the goods or services.

doi:10.6342/NTU201800740

是貨物)；換言之，單獨為匯兌貨幣而匯兌之並不能構成此項例外要件，因為其匯兌的目的不具附隨性，無法與「以匯兌為主要目的」截然分割，構成獨立於「以匯兌為主要目的」以外，為履行某種債之關係始發生例外不受規範的匯兌服務。

2. 上述例外要件只能由履行某種債之關係的直接當事人所主張。
3. 其匯兌貨幣之目的須是用於履行債之關係所必需的義務，亦即若無此項附隨於履行債務時所必須完成之義務，則無從履行債務。

FinCEN 表示必須同時達成上述 3 項要件始有可能通過「附隨性例外」的基本門檻，從「從事匯兌服務」的態樣中排除，至於是否真的符合例外則需由主管機關進一步認定之。

第二款 支付處理者例外

支付處理者(Payment Processor Exemption)例外整理如下[305]：

1. 提供服務之一方必須便利購置物品、服務之結帳程序。
2. 當事人所運行的結算及交割系統必須符合銀行保密法。
3. 當事人之服務須與書面所聲明的相一致。
4. 當事人同意為債權人或債務人所處理之款項與前兩者所提供之物或服務相當[306]。

若有業者同樣符合上述四項例外，其所從事之業務將會被認定為「並未從事匯兌服務而非匯兌業者」，因而從金融服務商下列的 7 種應受規範的項目中排除，毋庸受銀行保密法所規範。探討此例外的實益在於 FinCEN 曾對「代付商」作出的解釋。按 FinCEN 的見解，當一業者做為支付處理者，一方面接受債務人的現實貨幣，卻於另一方面支付相當價值的加密貨幣予債權人，則不會構成匯兌業者的例外。理由在於該結算系統並不符合第二項例外要件，蓋不管接收現實貨幣端的結算系

---

[305] FIN. CRIMES ENF'T NETWORK, *supra* note 280, at 3-5.

[306] 31 CFR § 1010.100(ff)(5)(ii)

(a) the entity providing the service must facilitate the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself); (b) the entity must operate through clearance and settlement systems that admit only BSA-regulated financial institutions; (c) the entity must provide the service pursuant to a formal agreement; and (d) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds.

doi:10.6342/NTU201800740

統是否符合銀行保密法的規範，只要另外一端的支付系統是藉由加密貨幣為之，則該部分當然不會構成被銀行保密法所認可的結算系統，因此不會構成支付處理者的例外。

第五項 適用銀行保密法之法律效果

透過以上論述可知只要從事匯兌服務就會被歸類為匯兌商而成為管制的對象，交換者及發行者均屬此類。被歸類為匯兌商後需遵循銀行保密法而需遵守下列法規所課予的義務[307]：

1. 必須向 FinCEN 註冊。
2. 實施全面性的洗錢弱點風險評估。
3. 基於以上的風險評估實施防制洗錢計畫。
4. 遵循 31 CFR § 1010, 1022 部分以下關於資料保存、上呈機制、交易監控等義務。例如：31 CFR § 1022.310 之大額通貨交易申報、31 CFR § 1022.320 可疑交易案件申報、31 CFR § 1010.410 資料保存與維護以及 31 CFR § 1010.415 流通性證券之交易資料保存。
5. 若有符合 31 CFR § 1010.100(ddd)資金移轉(Transmittal of Funds)的情形，則為完全遵循 FinCEN 的規範，尚有 31 CFR § 1010.410(e)資金匯款規則（Funds Transfer Rule）及 31 CFR § 1010.410(f) 資金流通規則(Funds Travel Rule) 的適用。

上述法律效果基本上與防制洗錢金融行動工作組織(Financial Action Task Force, FATF)所提出的建議相同。以資金匯款規則及資金流通規則為例，前者主要目的在留存能協助主管機關能偵測、調查洗錢犯罪及其他金融犯罪的資金匯款紀錄[308]；後者則是要求金融機構於匯款及解款時將在機構間所流通的資金透過不同程度的辨識以認識該筆流通款項背後的客戶資訊。如資金流通規則需匯款行辨識匯款人

---

[307] FIN. CRIMES ENF'T NETWORK, *supra* note 280, at 5.

[308] FIN. ACTION TASK FORCE, FUNDS "TRAVEL" REGULATIONS: QUESTIONS & ANSWERS (1997), https://www.sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf. (The funds transfer rules are designed to help law enforcement agencies detect, investigate and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through funds transfer systems.)

doi:10.6342/NTU201800740

姓名、匯款帳號、匯款人之地址、匯款人所使用的金融機構、匯款金額、匯款日期、收款人所使用之金融機構[309]，而解款行則需辨識收款人姓名、收款人地址、收款人帳號及其他有助於辨識收款人的特定訊息[310]。其中為客戶進行匯款及收款時應進行的客戶盡職調查程序（CDD）及紀錄留存，分別與 FATF 建議 10 及建議 11 相對應。

第六項 美國紐約州法對於虛擬貨幣所採之具體措施

美國紐約州於 2015 年 6 月將 FinCEN 從 2013 至 2014 年對於虛擬貨幣匯兌業者所作出的分類再行特別立法—訂定所謂的「虛擬貨幣許可規範架構」(BitLicense Regulatory Framework)[311]，並同時參考 FATF 的建議將洗錢防制義務明確化、細節化，在 Part 200 以下列出 22 個小節，分別是：200.1 說明、200.2 定義、200.3 發放許可、200.4 申請程序、200.5 申請費用、200.6 申請機關的措施、200.7 法令遵循、200.8 資本規範、200.9 客戶的資本保障、200.10 所營事業有重大變革、200.11 控制權人變更或併購、200.12 紀錄保存、200.13 查核、200.14 報告及資訊公開、200.15 制定洗錢防制計畫、200.16 制定資訊安全計畫、200.17 事業遭致災難的復原計畫及持續運作計畫、200.18 廣告和行銷、200.19 消費者(客戶)保護、200.20 申訴管道、

---

[309] All transmittor's financial institutions must include and send the following in the transmittal order:
The name of the transmittor,
The account number of the transmittor, if used,
The address of the transmittor,
The identity of the transmittor's financial institution,
The amount of the transmittal order,
The execution date of the transmittal order, and
The identity of the recipient's financial institution;

[310] and, if received:
The name of the recipient,
The address of the recipient,
The account number of the recipient, and
Any other specific identifier of the recipient.

[311] *BitLicense Regulatory Framework*, NY DEP'T FIN. SERV., https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm (last visited June 21, 2018).

doi:10.6342/NTU201800740

200.21 過渡期間、200.22 本法的可分割性[312]。

紐約州專門立法 Part 200 主要是為了規範交換者。首先於定義上，200.2(d)明確將匯兌服務(Exchange Service)定義為從事法定貨幣與虛擬貨幣的兌換服務、從事虛擬貨幣與法定貨幣的兌換服務、從事虛擬貨幣與虛擬貨幣的兌換服務[313]；200.2(p)次將虛擬貨幣定義為任何數位單位能用於儲存價值或是成為價值轉換的媒介，細節上承接聯邦法的規定應該做廣義的解釋，包含前述有著集中式儲存庫及管理者的中心式虛擬貨幣、去中心化且不具集中式儲存庫及管理者的去中心式虛擬貨幣、或是透過運算或是生產所產生的虛擬貨幣[314]；200.2(q)再將從事虛擬貨幣商業活動(Virtual Currency Business Activity)列舉共 5 種應被列入管制的活動，分別是 1.為了匯兌虛擬貨幣而接收虛擬貨幣，但如是符合「附隨於主要交易目的所為之資金移轉例外」或是僅匯兌「象徵式、微不足道」的虛擬貨幣，則屬於例外不受規範的範圍 2.為他人儲存、持有、保有、控制虛擬貨幣 3.從事商業類型的虛擬貨幣買賣 4.從事商業類型的匯兌服務 5.控制、管理或是發行虛擬貨幣[315]。Part 200.2 (q)所列舉的 5 種受規範的態樣，除了最後一種是針對發行者外，其餘 4 種均是交換者無

---

312 N.Y. Comp. Codes R. & Regs. tit. 23

313 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.2(d) (2015). Exchange Service means the conversion or exchange of Fiat Currency or other value into Virtual Currency, the conversion or exchange of Virtual Currency into Fiat Currency or other value, or the conversion or exchange of one form of Virtual Currency into another form of Virtual Currency

314 *Id.* § 200.2(p) Virtual Currency means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.

315 *Id.* § 200.2 (q) Virtual Currency Business Activity means the conduct of any one of the following types of activities involving New York or a New York Resident:
(1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;
(2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;
(3) buying and selling Virtual Currency as a customer business;
(4) performing Exchange Services as a customer business; or
(5) controlling, administering, or issuing a Virtual Currency.

doi:10.6342/NTU201800740

法避免的活動。而 Part 200.3 主要發放許可的對象即是從事上述虛擬貨幣商業活動的業者，若無 NYDFS 發放許可，則不許在紐約州內從事與虛擬貨幣業務相關的商業活動，由此可證紐約州為落實聯邦法而擬訂的虛擬貨幣規範主要還是以與匯兌業務相關的交換者為主要規範對象[316]。

與洗錢防制最相關的 Part 200.15 詳細地勾勒出具體從嚴管控虛擬貨幣行業以達到避免虛擬貨幣被洗錢犯罪所利用的法律規範模式。Part 200.15 (b)要求被許可人對自身機構所從事的業務及可能有往來的客群，進行一系列的地域風險、客戶風險、產品及服務管道風險並且進行風險評估，每年應進行一次，並將評估結果導入洗錢防制計畫中應用。Part 200.15 (c)將洗錢防制計畫的最低基準加以列舉：分別是內部控制的具體章程及流程、洗錢防制計畫的獨立測試、合格的法令遵循人員、及持續的教育訓練。Part 200.15 (e)為洗錢防制計畫訂定詳細的資料保存規範、監督及通報可疑交易報告的門檻、時效、流程，如當一人於一天內交易金額累計超過 1 萬美元，持有執照之匯兌業者應於 24 小時內申報之。Part 200.15 (h)明確規範業者應訂定客戶確認作業程序(Customer Identification Program, CIP)於有新客戶往來時對客戶所提供的各種資訊進行驗證，過程包括比對財政部資產控制辦公室（Office of Foreign Assets Control, OFAC）之指定制裁名單（Specially Designated Nationals List, SDNs）、區分本國籍及外國籍客戶，以便對非美國公民進行加強審查作業程序(Enhanced Due Diligence, EDD)。Part 200.15 (i)要求被許可的匯兌業者須有一套客戶風險分級(Customer Risk Ratings, CRR)的機制，以風險基礎方法管理客戶群，使得 OFAC 的相關規範亦能同時被遵循。Part 200.15 (j)說明匯兌業者應建

316 *Id.* § 200.3 (a) License required. No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity

doi:10.6342/NTU201800740

立一套機制以拒絕或中止有可能違反聯邦法或州法的交易。最後 Part 200.15 (k)要求被匯兌業者指定完備上述所有規範與機制之人應善盡管理責任，確保每項要求是以「日」為基礎(Day-to-Day Basis)進行。

觀察 Part 200 的細部規範及要求業者所負之洗錢防制義務，可知美國紐約州已使用金融機構等級的規範措施加諸於虛擬貨幣匯兌服務，對加密貨幣的規範之嚴堪稱世界之最[317]。截至 2018 年 7 月，紐約州僅發放 10 張虛擬貨幣許可證(BitLicense)[318]。其中 Genesis Global Trading 稱其早於 2015 年 8 月就向紐約州金融服務廳(NYDFS)申請許可，且還是 26 家早於 2016 年 6 月以前就提出申請的業者之一，卻等了近 3 年的時間始獲得許可，所以其估算以 3 年審核 5 張虛擬貨幣營業許的的速度來看，目前待許可的業者最遲可能要等到 2027 年才會知道是否會獲得許可[319]。因此一些加密貨幣匯兌業者的 CEO 稱虛擬貨幣許可證就是個失敗的產物，應盡早廢除此種許可制度[320]。

第三節　我國之洗錢防制方向

第一項 指定之非金融事業洗錢防制方向

我國法務部、金融監督管理委員會、中央銀行、經濟部等部會於 2018 年 6 月已初步達成將虛擬貨幣匯兌業者歸類為洗錢防制法第 5 條 3 項 5 款所稱之「其他

---

[317] Gabriela Barkho, *Why a Top Cryptocurrency Exchange is Technically Illegal in New York City*, INVERSE (Jan. 17, 2018), https://www.inverse.com/article/40144-binance-bitlicense-bitcoin-cryptocurrency-exchange-new-york-city.

[318] *DFS Grants Virtual Currency License to Bitpay*, NY DEP'T FIN. SERV., (July 16, 2018) https://www.dfs.ny.gov/about/press/pr1807161.htm; 十家業者分別是 BitPay Inc., Square, Inc., Xapo, Inc., Genesis Global Trading Inc., bitFlyer USA, Coinbase Inc., XRP II, Circle Internet Financial, Gemini Trust Company, Paxos。

[319] Robert Hackett, Jeff John Roberts & Jen Wieczner, *The Ledger: Is New York's BitLicense an 'Absolute Failure?'*, FORTUNE (May 25, 2018), http://fortune.com/2018/05/25/the-ledger-cryptocurrency-bitlicense/.

[320] *Id.*

doi:10.6342/NTU201800740

業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」[321]，惟就加密貨幣之洗錢防制應由何機關執掌尚未定案，仍待行政院指定未來的目的事業主管機關[322]。

從各部會討論出的初步結論，似將虛擬貨幣匯兌業者歸類為洗錢防制法第 5 條 3 項之「指定之非金融事業或人員」而非第 5 條 1 項 18 款之「其他經目的事業主管機關指定之金融機構」。由此規範方向似可合理預期未來主管機關可能推出之「虛擬貨幣匯兌業防制洗錢與打擊資恐施行及申報辦法」應該會呈現與現行其他「指定之非金融事業或人員」相距不遠的規範方式，不至於過苛。蓋若規範強度如美國紐約州般使用幾近於金融業者的規範方式則不免過於嚴苛，同時亦失去將虛擬貨幣匯兌業歸類為「指定之非金融事業或人員」的初衷。

本文試圖統整既有對「指定之非金融事業」訂定的「防制洗錢辦法」並進行比較，以評估未來「虛擬貨幣匯兌業」的防制洗錢規範可能會受何種程度的規範。爰將目前僅有的兩種「指定之非金融事業」亦即銀樓業及不動產經紀業的相關辦法予以比較。另因專業人士如律師、公證人、會計師屬於「指定之非金融人員」故不在比較之列。整理共同之處如下表：

表 八：洗錢防制法第 5 條 3 項「指定之非金融事業」之規範比較

基本原則	課予之義務	銀樓業防制洗錢與打擊資恐施行及申報辦法(107.03.23)	地政士及不動產經紀業防制洗錢辦法(106.06.28)
新客戶審別識	確認客戶身分，及留存或紀錄其身分資料。	第 3 條 1 項 1 款	第 4 條 1 項 1 款
	確認法人客戶身分，及留存或紀錄	無	第 4 條 1 項 2 款

[321] 同前揭註 38。

[322] 經濟日報（2018/06/04），〈比特幣納管主管機關...待政院指定〉， https://udn.com/news/story/7239/3178182（最後瀏覽日：2018/07/01）

doi:10.6342/NTU201800740

	其身分資料。		
	由客戶代理人為交易者，應確認代理人身分資料，並留存或紀錄之外，應確認其代理權之真實性。	第 3 條 1 項 2 款	第 4 條 2 項
	客戶為法人者應確認實質受益人身分資料，並留存或紀錄。	無	第 4 條 3 項
客戶姓名檢核* *為客戶盡職調查 (CDD)的一環	確認客戶是否屬法務部依資恐防制法規定公告制裁名單，或其他國家、國際組織認定或追查，與恐怖主義或恐怖活動有關之個人、法人或團體。若查證相符則應拒絕與其交易並通報調查局。	第 8 條 1 項 1 款	第 8 條 1 項 1 款
		資恐防制法第 7 條共同適用	
加強客戶審查 (EDD)	應採取合理措施辨識現任或曾任國內外政府或國際組織重要政治性職務之客戶或受益人與其家庭成員及有密切關係之人，並對其加強身分審查及瞭解資金來源。	第 4 條	第 5 條
紀錄留存	留存交易紀錄至少 5 年。	第 3 條 3 項 第 7 條 2 項 第 8 條 2 項	第 4 條 6 項 第 7 條 2 項 第 9 條 2 項
申報可疑/大額交易	可疑交易及其他規定之情事應於 10 個營業日內申報調查局。	第 6 條 第 7 條 1 項 第 8 條 1 項 2 款	第 8 條 第 9 條 2 項
	對新臺幣 50 萬元（含等值外幣）以上之現金交易於交易後 5 個營業日內申報調查局	第 5 條	無
	對明顯重大緊急之疑似洗錢交易案件，應立即以傳真或其他可行方式儘速辦理申報。	第 7 條 1 項 2 款 第 8 條 1 項 2 款	無

從上表可知，目前主管機關對「指定之非金融事業」主要著重的還是確認客

doi:10.6342/NTU201800740

戶身分，要求面對新客戶時至少需辨識身分證明文件，若由代理人代理交易則需辨識代理人之身分。其中銀樓業採取相較於不動產經紀業為寬鬆的做法，無須確認法人客戶之身分及確認其實質受益人之身分資料，此應為行業特性使然，蓋與銀樓交易通常是由自然人前往交易，法人難以持現金進行交易，確認以現金進行交易之自然人身分因此成為《銀樓業防制洗錢與打擊資恐施行及申報辦法》第 3 條的主要目的。

於確認客戶身分後，我國主管機關要求「指定之非金融事業」採取合理措施辨識「現任或曾任國內外政府或國際組織重要政治性職務之客戶或受益人與其家庭成員及有密切關係之人」(PEPs)，並對其加強身分審查及瞭解資金來源。對於何謂「合理措施」並無明確的參考標準，但應是一個以行業能力所出發的相對概念。如具備較多能力的金融機構即於《金融機構防制洗錢辦法》第 10 條被強制性要求應利用自行建置之資料庫或外部之資訊來源來確認客戶及其實質受益人、高階管理人員是否為現任或曾任國內外政府或國際組織之重要政治性職務人士，該法並未使用「合理措施」的用語。相較之下可知「合理措施」應與措施的施行人本身的能力相關，若施行人本身不具有採行相對應措施的能力，則要求其採取超出能力範圍的措施即難謂「合理」。惟如此一來認定施行人是否具備採行相對應措施的能力即成為關鍵的判定因素，須由主管機關從客觀上認定，若認為已採行「合理措施」即屬合規；反之，若認為並未採行「合理措施」則可能會因違反《洗錢防制法》第 7 條 5 項所稱之「前項所定辦法」而被處以新臺幣五萬元以上一百萬元以下罰鍰(指定之非金融事業)。就此不明確性可能須待未來相關裁罰案例或是函釋公布後始能進行更進一步的分析。

「指定之非金融事業」除須辨識重要政治性職務人士外，尚有被課予比對往

doi:10.6342/NTU201800740

來的客戶是否為依《資恐防制法》第 4 條及第 5 條規定公告之制裁名單，或其他國家、國際組織認定或追查與恐怖主義或恐怖活動有關之個人、法人或團體。此項義務對於「指定之非金融事業」的影響可大可小，若僅依法務部調查局所公布之名單進行檢核，單憑人工即可完成；但若是要將涵蓋的範圍擴增至「其他國家、國際組織認定或追查與恐怖主義或恐怖活動有關之個人、法人或團體」則可能須購買價值不斐的姓名檢核資料庫 [323]。目前尚未有更細部辦法敘明「指定之非金融事業」要如何始能完成除法務部調查局以外的姓名檢核，但若以產業規模以觀，資本額較低的銀樓業或不動產經紀業若缺乏主管機關的強制性規定，應該也不會希望投資大量成本購置資料庫進行姓名檢核。蓋此類產業所面對的客戶大多均屬本國客戶，較不若金融業者般擁有跨國界的客戶進行匯款交易，是以實務應用上完全導入主管機關規範之標準的期待可能性較低。虛擬貨幣匯兌產業於初期規劃時，雖可效法銀樓業或不動產經紀業將「其他國家、國際組織認定或追查與恐怖主義或恐怖活動有關之個人、法人或團體」訂入辦法中，但主管機關於落實辦法中的相關規定時，或許可待公司營運至一定規模時再於實際運作上強制公司落實姓名檢核的工作。類似明定條文但卻不逐一落實的現象，對於近期加速落實洗錢防制的我國來說是一個較為無解的狀況，但為因應即將到來的 APG 防制洗錢評鑑，僅能先以一種過度形式進行先求有再求好立法模式。未來於訂定相關辦法時還是需要評估產業規模及實務運作上能否達成規定，以達成全面性的法律遵循，避免規範上及落實上的差距過大。

最後，「指定之非金融事業」尚有紀錄留存與申報調查局兩種義務。留存的紀錄觀察銀樓業及不動產經紀業的相關規定，主要是任何與確認客戶身分及與交易

[323] 如 Thomson Reuters World-Check、Dow Jones Factiva、Lexis Nexis World Compliance。

doi:10.6342/NTU201800740

相關的紀錄，任何與此二項相關的紀錄應至少留存 5 年。至於依法須向調查局申報者又可細分為大額通貨交易申報(Currency Transaction Report, CTR)及可疑交易案件申報兩種，前者主要申報的對象為任何新臺幣五十萬元（含等值外幣）以上之現金交易，而後者的申報對象則為疑似洗錢交易案件[324]。銀樓業及不動產經紀業應各自向法務部調查局申報的行為雖非完全相同，但概括而言，指定之非金融事業具有申報疑似洗錢交易或資恐情事的義務。對於履行此項義務，指定之非金融事業必須對每一筆交易進行審查，視是否符合可疑態樣而決定是否需申報予調查局。此項申報義務對於金融機構及指定之非金融事業或人員均有適用，合理推定未來即將被納管的虛擬貨幣匯兌行業應同樣會被課予申報可疑交易及大額通貨的義務。此項義務對於其他指定之非金融事業或人員可能負擔相對較小，蓋就交

---

[324] 《銀樓業防制洗錢與打擊資恐施行及申報辦法》第 6 條
交易有下列情形之一者，銀樓業應確認客戶身分，留存客戶身分資料及交易紀錄，並應向法務部調查局為疑似洗錢交易之申報：
一、客戶有不尋常之交易，且該交易與客戶身分、收入顯不相當或與其營業性質無關。
二、客戶連續以略低於新臺幣五十萬元進行現金交易。
三、交易完成後，對有存疑之客戶予以確認時，發現客戶否認該交易、無該客戶存在或其他有相當之證據或事實，確信該客戶名稱係被他人所冒用。
四、電視、報章雜誌或網際網路及其他相關媒體報導之重大特殊案件之涉案人之交易。
五、客戶為法務部調查局所公告之恐怖分子或組織；或國際洗錢防制組織認定或追查之恐怖組織。
六、其他經認定有疑似洗錢交易情形。
交易未完成者，應申報客戶特徵及交易過程。

《地政士及不動產經紀業防制洗錢辦法》第 8 條
地政士及不動產經紀業從事與不動產買賣交易有關之行為時，發現下列各款情事之一者，應向法務部調查局申報：
一、客戶屬法務部依資恐防制法規定公告制裁名單，或其他國家、國際組織認定或追查，與恐怖主義或恐怖活動有關之個人、法人或團體。
二、交易金額源自於國際防制洗錢組織所公告防制洗錢及打擊資恐有嚴重缺失，或其他未遵循、未充分遵循國際防制洗錢組織建議之國家或地區，或支付予該國家或地區之帳戶或人員，且疑似與恐怖活動、恐怖組織或資恐有關聯。
三、客戶拒絕或無故拖延提供相關身分資料、使用假名、假冒他人名義或偽變造身分證件。
四、交易金額與客戶年齡、身分或收入顯不相當，或以現鈔支付定金以外各期價款，且無合理說明資金來源。
五、客戶要求將不動產權利登記予第三人，未能提出任何關聯或拒絕說明。
六、不動產成交價格明顯高於市場行情且要求在相關契約文件以較低價紀錄。
七、其他疑似洗錢交易或資恐情事。

doi:10.6342/NTU201800740

易型態而言，他種產業於進行交易時毋須以全電子自動化的形式進行。目前洗錢防制法第 5 條 3 項之指定之非金融事業或人員的交易型態尚能使用人工辨識的方式逐筆審查交易，但若虛擬貨幣匯兌事業加入此行列，將有可能成為第一個需要效仿金融機構引進專業的交易監控系統(Transaction Monitoring System, TMS)，以自動化設備與軟體協助辨識及申報大額通貨及可疑交易的指定之非金融事業或人員。原因在於虛擬貨幣匯兌事業的交易型態與銀行業相近，不管是對於內部虛擬貨幣的移轉或是利用虛擬貨幣 ATM 提領現金，均能一定程度上套用現實貨幣可能發生的疑似洗錢態樣。例如利用未經驗證或是人頭之虛擬貨幣帳號以低於金融機構申報門檻的金額小額多次購入虛擬貨幣，累計至一定金額再進行移轉的洗錢態樣，若非利用專業的軟體設定參數以自動化的方式產生警示，光是以人工的方式實難想像如何從成千上萬筆的電磁紀錄中辨識出需申報與調查局的可疑交易。綜合上述，本文認為未來虛擬貨幣被納管成為指定之非金融事業中的一員時，業者最有可能面臨的問題會是如何對用戶進行姓名檢核作業以及識別可疑交易與申報可疑交易案件。

第二項 指定之非金融事業與金融機構洗錢防制方向之差距

我國主管機關對於金融機構及指定之非金融事業或人員採取不同強度的監管措施，如建置重要政治性職務人士之資料庫即為一例，前文稍有述及。以下擬將我國主管機關課予金融機構的一些義務與指定之非金融事業機構相比較，以較為宏觀的角度觀察目前主管機關對於新興金融科技產業與傳統金融產業所為之區別規範，進而探究未來政策的推行會較偏向目前的金融機構規範方式抑或是力度較低卻能平衡洗錢防制與產業發展的折衷型規範模式。

doi:10.6342/NTU201800740

第一款 確認客戶身分程序繁瑣程度不同

指定之非金融事業的相關防制洗錢辦法於確認客戶身分程序時明文須留存或記錄其身分資料[325]，地政士及不動產經紀業之確認範圍較銀樓業廣，其擴及的範圍包含至法人、代理人、第一層實質受益人(持有該法人股份或資本超過百分之二十五之自然人)，若未能確認則應確認其董事、監察人或相當職位之自然人身分資料[326]。金融機構除須確認上述資料外，就確認實質受益人的身分部分，除需於第一層：辨識直接、間接持有該法人股份或資本超過百分之二十五之人外；於無法完成辨識時，則需加深辨識至第二層：進一步辨識「有無透過其他方式對客戶行使控制權之自然人」；於未能發現行使實質控制權之人時，則繼續第三層之辨識：繼續辨識高階管理人員之身分[327]。

由此可知指定之非金融事業若有被課予辨識實質受益人之義務，實際辨識程度上至少會較金融機構為簡便，且並無強制性規範要求須以合理措施驗證其身分，包括使用可靠來源之資料或資訊。綜觀銀樓業及地政士及不動產經紀業之相關防制洗錢辦法，兩項辦法內均未提及「驗證」一詞，反觀《金融機構防制洗錢辦法》「驗證」一詞出現 17 次，大多緊接於「辨識」一詞。可見金融機構於確認客戶身分時，除要求客戶提供資訊外，尚須另尋可靠、獨立來源之文件、資料或資訊，辨識及驗證客戶身分，對資訊正確性的要求程度明顯高於指定之非金融事業。且前開辦法第 7 條將整套的「確認客戶身分作業」程序當成是金融機構的義務，若

---

325 《地政士及不動產經紀業防制洗錢辦法》第 4 條 1 項
一、客戶為自然人者，應檢視其國民身分證、健保卡、護照、居留證或其他可資證明身分之證明文件，留存或紀錄其姓名、出生年月日、地址及統一編號等身分資料，並徵詢其職業及聯絡電話號碼紀錄之。
二、客戶為法人或團體者，應確認其名稱、負責人姓名、登記住址、統一編號、主營業所或主事務所地址、電話號碼及資格證明文件等資料，並留存或紀錄之。

326 《地政士及不動產經紀業防制洗錢辦法》第 4 條 2 項。

327 《金融機構防制洗錢辦法》第 3 條 7 款 1 目。

doi:10.6342/NTU201800740

仰賴第三方執行辨識及驗證客戶本人身分、代理人身分、實質受益人身分，該依賴第三方之金融機構仍應負確認客戶身分之最終責任[328]。

從上可知，因未明文規範要求須以合理措施驗證由客戶識別審查程序而取得之資訊，讓指定之非金融事業毋須向第三方進行客戶資料的驗證，於確認客戶身分程序中較金融機構為寬鬆，所需耗費的洗錢防制成本亦較低。

第二款 持續審查客戶的規範不同

我國《金融機構防制洗錢辦法》第 5 條謂：「確認客戶身分措施，應包括對客戶身分之持續審查」，可見確認客戶身分(KYC)程序並不止於同辦法第 3 條、第 4 條所規範的徵求客戶個人資料、辨識及驗證客戶身分，尚包括後續的「持續審查」。由此推論，我國洗錢防制法對於確認客戶身分程序應不限對新客戶所進行之確認作業程序(CIP)，尚包含後續的客戶持續審查(Ongoing Customer Due Diligence, OCDD)。客戶識別審查（CIP）通常用於識別新客戶[329]，亦是整個確認客戶身分程序的第一個步驟，主要目的為以風險為基礎的程序收集、辨識、驗證客戶資訊，如以風險為基礎綜合考慮客戶所開設的帳戶權限、開戶管道來判斷進行識別審查時應辨識及驗證的程度[330]，《金融機構防制洗錢辦法》第 3 條、第 4 條即是在規範應辨識、審查、驗證的項目及何種情況下應予以婉拒建立業務關係。其後第 5 條則參考 FATF 評鑑方法論之評鑑準則第 10-7 點，明定於確認客戶身分措施，應包

---

[328] 金融機構防制洗錢辦法第 7 條：
「金融機構確認客戶身分作業應自行辦理，如法令或本會另有規定金融機構得依賴第三方執行辨識及驗證客戶本人身分、代理人身分、實質受益人身分或業務關係之目的及性質時，該依賴第三方之金融機構仍應負確認客戶身分之最終責任。」

[329] 31 C.F.R. § 103.121(a)(3)(i)(A)；但仍有例外情形非於新開戶時進行 CIP 程序，詳見 31 C.F.R. § 103.121(b)(2)(ii)(C)。

[330] *Description: Frequently Asked Questions (updated): Final Customer Identification Program Rule*, OFF. COMPTROLLER CURRENCY, U.S. DEP'T TREASURY (Apr. 28, 2005), https://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-16.html.

doi:10.6342/NTU201800740

括對客戶身分之持續審查，並細緻地將應進行持續審查的時機做出更進一步的規範。我國法雖並未對客戶持續審查作出明確的定義，但若參考有明確定義客戶持續審查的澳洲洗錢防制主管機關 AUSTRAC 對 CIP 程序及 OCDD 程序所進行的區辨，可知前者程序是被規劃成在提供任何服務前必須經過的程序，內容包含收集與驗證客戶資訊；反觀後者的主要目的在於反制洗錢及資恐犯罪，運用持續審查客戶的方式讓機構能於客戶識別審查程序結束後，辨識及反制提供予既有客戶之服務所可能導致的洗錢及資恐風險 [331]。因此，客戶持續審查程序是於客戶開戶後即有適用，不因是否已進行過客戶盡職調查(CDD)或是加強盡職調查(EDD)程序而有所不同。根據澳洲洗錢防制法，客戶持續審查程序是由下列 3 項要件所構成的：1.收集並且驗證除了現有客戶的 KYC 資訊、2.監控系統、3. 加強盡職調查的計畫(EDD Program)[332]。綜上所述，金融機構被課予持續審查客戶的義務不可謂不大，此為指定之非金融事業所無的義務。舉例而言，《金融機構防制洗錢辦法》第 5 條 2 款要求金融機構對客戶進行持續審查，對業務關係中之交易進行詳細審視，以確保所進行之交易與客戶及其業務、風險相符，必要時並應瞭解其資金來源。為因應此項義務，面對成千上萬名客戶的金融機構須建置資料庫並購置洗錢防制系統並將其與現有的電子交易系統整合並調整一定參數始能有效率地審視業務關係中所進行之交易。又同辦法第 5 條 3 款要求金融機構應「定期檢視其辨識客戶及實質受益人身分所取得之資訊是否足夠，並確保該等資訊之更新，特別是高風險客戶，金融機構應至少每年檢視一次」，按現行銀行實務作業，實質受益人之身分資料及高風險客戶的持續審查均是透過人工所進行，期間所花費的法遵成本亦相當

[331] AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE, ONGOING CUSTOMER DUE DILIGENCE (OCDD), http://www.austrac.gov.au/sites/default/files/documents/ongoing_customer_due_diligence_1.pdf (last visited July 4, 2018).
[332] *Id.*at 2.

doi:10.6342/NTU201800740

可觀。現行指定之非金融事業除客戶識別審查外毋須進行後續的持續審查，相較於金融機構在審查作業上輕鬆許多，因此亦無需另訂專法規範應建置何種標準之法律遵循部門，詳如下述。

第三款 法遵人力配置上的不同

我國金融監督管理委員會於 2018 年 3 月 31 完成並公布新修訂《金融控股公司及銀行業內部控制及稽核制度實施辦法》(下稱銀行業內控稽核辦法)。表示本次修正旨在強化法遵與風險控管機制及建置資安專責制度，並推動金融機構應建立內部檢舉人保護制度，爰一共修正 6 條，增訂 3 條條文[333]。新修正之《銀行業內控稽核辦法》第 32、34、38-1 條及新增訂之第 34-1 條主要規範對象為「金融控股公司及銀行業之總機構」之法遵與風險控管機制。所謂銀行業，按《銀行業內控稽核辦法》第 2 條包括銀行機構、信用合作社、票券商及信託業；金融控股公司則係指《金融控股公司法》第 4 條之金融控股公司。《銀行業內控稽核辦法》第四節主要規範法令遵循制度，按前述辦法，前一年度經會計師查核簽證之資產總額達新臺幣一兆元以上之銀行業應設置專責之法令遵循單位。該單位主要職掌第 34 條所列舉之各項事項[334]，並得兼辦防制洗錢及打擊資恐相關事項。另外新增定之

---

[333] 金融監督管理委員會（2018），修正「金融控股公司及銀行業內部控制及稽核制度實施辦法」部分條文，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201803200002&toolsflag=Y&dtable=News（最後瀏覽日：2018/07/04）

[334] 《金融控股公司及銀行業內部控制及稽核制度實施辦法》第 34 條
法令遵循單位應辦理下列事項：
一、建立清楚適當之法令規章傳達、諮詢、協調與溝通系統。
二、確認各項作業及管理規章均配合相關法規適時更新，使各項營運活動符合法令規定。
三、於銀行業推出各項新商品、服務及向主管機關申請開辦新種業務前，法令遵循主管應出具符合法令及內部規範之意見並簽署負責。
四、訂定法令遵循之評估內容與程序，及督導各單位定期自行評估執行情形，並對各單位法令遵循自行評估作業成效加以考核，經簽報總經理後，作為單位考評之參考依據。
五、對各單位人員施以適當合宜之法規訓練。
六、應督導各單位法令遵循主管落實執行相關內部規範之導入、建置與實施。

doi:10.6342/NTU201800740

34-1條乃參考2005巴塞爾銀行監理委員會(Basel Committee on Banking Supervision, BCBS)所發布之銀行的法遵和法遵功能文件(Compliance and the Compliance Function in Banks)所提出銀行法令遵循之十點原則[335]，內提及法遵主要權責規範包括建立全行法遵風險管理架構、獨立法令遵循組織及權責、及落實法令遵循效能報告及監督訂定[336]。為落實上述規範內容，因此法遵單位須具備應有之「法遵功能」(Compliance Function)以實現辨識、評估、監控、測試及報告法遵風險。如BCBS指引原則五即著重於銀行法遵功能的獨立性，訂定人員之職務應防範利益衝突，且應定期向決策單位報告等管理機制[337]。

上述僅是銀行業等金融機構須建置之法令遵循制度，該辦法內另有就內部控制稽核制度及資安專責制度訂定細部規範。主管機關考量前揭辦法內所述及之落實成本，故參考2008年美國聯邦準備委員會(Federal Reserve Board, FRB)對銀行發出之「大型銀行複雜法遵風險管理架構及監控」行政函釋[338]，訂定1兆新臺幣的監理門檻[339]。指定之非金融事業機構未如同大型銀行擁有龐大的資本額、金融客群、實體匯兌通路，亦不具備落實完整之法遵功能及制定內部控制制度的能力，主管機關或許衡量現下其對金融體系的影響力及尚處於產業萌芽時期，爰從資本額為一分界線，將被認定為尚非屬大型金融機構之業者排除，以免對該產業造成

---

335 金融監督管理委員會(2018)，〈金融控股公司及銀行業內部控制及稽核制度實施辦法 條文對照表〉。載於：http://law.fsc.gov.tw/law/LawContent.aspx?id=FL049894（最後瀏覽日：2018/07/04）

336 *See generally* BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS (2005), https://www.bis.org/publ/bcbs113.pdf.

337《金融控股公司及銀行業內部控制及稽核制度實施辦法》第34-1立法理由；孫欣、章友馨(2018)，〈金融機構法令遵循風險評估與法規資料庫〉。載於：https://home.kpmg.com/tw/zh/home/insights/2018/01/law-compliance-risk-assessment-and-regulations-database.html（最後瀏覽日：2018/07/04）

338 函中係以總資產規模在500億美元($50 billion相當新臺幣1.5兆元)以上之銀行為來建構符合所揭示之複雜法遵風險管理及監控架構的分界線。

339 BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8 / CA 08-11: COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES (2008), https://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.

doi:10.6342/NTU201800740

過大的法令遵循負擔。

第四節　小結

本節從抽象至具體探討目前去中心化加密貨幣之洗錢防制方向，FATF 於大方向建議監理機關課予虛擬貨幣支付產品及服務(VCPPS)對新客戶踐行客戶識別計畫(CIP）之義務，並且不論是對新客戶或是既有的客戶均應施行盡職調查(CDD)，以可靠的、具獨立來源的文件、資料或資訊，完成驗證客戶資訊，若屬高風險客戶則再進行加強客戶調查（EDD)，完成整體的認識客戶程序 (KYC)。FATF 另於《虛擬貨幣風險基礎方法指引》第 51 條至第 54 條建議中提出虛擬貨幣於法令遵循上可能面臨的挑戰及潛在的解決方案,如開發有助於提升法令遵從性的科技(如：提供客戶身份辨識資訊的應用程式設計界面（Application Programming Interfaces, APIs)、第三方數位認證身份系統以及考慮成立一個包含接受過主管機關審核的虛擬貨幣自律組織產並制定組織會員應遵守的政策及自律規範(如：妥適的客戶盡職調查程序及交易監控機制等)。

其後本文以較具有虛擬貨幣規範經驗的美國為例，從具體的銀行保密法觀察聯邦層級的主管機關 FinCEN 如何規範 FATF 於指引內建議納管之虛擬貨幣支付產品及服務。FinCEN 之建議係以從事匯兌業務之客觀態樣為出發點，輔以使用者、交換者、發行者各自具備之客觀型態為區辨方式，限縮構成匯兌業務的虛擬貨幣交易型態(如：以自身投資為目的買賣虛擬貨幣將構成使用者)。若最後確定從事虛擬貨幣交易之態樣符合交換者、發行者之定義，則須受銀行保密法之規範，遵守相關洗錢防制規定。更具體之虛擬貨幣洗錢防制規範方式可見美國紐約州金融廳(NYDFS) Part 200，該法詳細列出欲取得虛擬貨幣營業執照之 22 個小節，其中第 15 小節即列舉欲取得許可執照應遵循之洗錢防制作業，如進行地域風險、客戶風

doi:10.6342/NTU201800740

險、產品及服務管道風險評估；訂定內部控制具體章程及流程、洗錢防制計畫的獨立測試、聘僱合格的法令遵循人員、持續的教育訓練、訂定詳細的資料保存規範、監督及通報可疑交易報告的門檻、時效、流程；訂定客戶確認作業程序、比對 OFAC 指定制裁名單、建置客戶風險分級機制等。

比較 FATF《虛擬貨幣風險基礎方法指引》與美國銀行保密法及更細部的紐約州 Part 200 所訂定之規範，可知目前美國已訂定一套如何區辨應受管制之虛擬貨幣匯兌業者之機制，從抽象至具體，逐一辨識應被納管之對象並課予其極高的防制洗錢及打擊資恐義務，整體規範方向偏嚴。

反觀我國，因經濟規模或是貨幣通用性上均遜色於美國[340]，新臺幣亦不同於美元，並非各國主要兌換幣別[341]，是否有必要完全採行與美國相同之洗錢防制措施即值得研究。本文先參考最新立法動態，並以主管機關目前的初步規劃出發，分析目前我國就指定之非金融事業採行何種規範標準，具體要求遵循之法規範為何。本文以指定之非金融事業[342]銀樓業、地政士及不動產經紀業為比較對象，綜合比較兩者並從嚴推論未來虛擬貨幣匯兌業可能面臨之法規範。經比較，指定之非金融事業主要被課予之義務有對新客戶進行識別審查程序（CIP），程序內至少包含確認客戶身分，若由客戶代理人為交易者，應確認代理人身分資料及留存或記錄其身分資料兩項(如銀樓業僅此二項)；較嚴謹的規範尚會增加確認法人客戶身分及其實質受益人之身分資料(如地政士及不動產經紀業即要求確認至第一層之實

---

340 *Country Comparison Taiwan vs United States 2018*, COUNTRYECONOMY.COM, https://countryeconomy.com/countries/compare/taiwan/usa (last visited July 15, 2018).

341 Kimberly Amadeo, *Strength and Power of the US Dollar---3 Reasons Why the U.S. Dollar is So Powerful*, THE BALANCE.COM (Feb. 19, 2018), https://www.thebalance.com/power-of-the-u-s-dollar-3306267.

342 《洗錢防制法》第 5 條 3 項統稱除金機構以外之事業及對象為「指定之非金融事業或人員」，本文因討論對象為加密貨幣匯兌事業，故以「指定之非金融事業」為參考對象，不包括「指定之非金融人員」。

doi:10.6342/NTU201800740

質受益人，若無法取得資訊尚可退而求董監事之資料)。除前述程序對於確認客戶身分之嚴謹度較低外，尚有較為簡易之名單檢核義務、僅就重要政治性職務人士及實質受益人執行加強客戶審查(EDD)之義務、以及紀錄留存、申報可疑/大額交易之義務。

欲知於我國上述義務相較金融機構之規範強度孰强孰弱，即須與金融機構之相關規定相互比較。本文觀察《金融機構防制洗錢辦法》與《金融控股公司及銀行業內部控制及稽核制度實施辦法》並重點節錄確認客戶身分程序、持續審查客戶以及設置具備法遵功能之法遵部門三項課予金融機構或具一定資本額之金融機構之義務，將其與指定之非金融事業相互對照，發現指定之非金融事業毋庸進行驗證、持續審查客戶、當然也無須建置具法遵功能之法遵部門，規範密度遠低於機構。綜上分析，將虛擬貨幣匯兌業歸類為指定之非金融事業所導致之洗錢防制義務上的差距是否妥適？又是否合乎我國國家風險？若有未合是否有較為具體之建議？即為下章欲討論之主題。

doi:10.6342/NTU201800740

第伍章　加密貨幣於我國未來之洗錢防制與推行

隨著各國開始著手立法防止加密貨幣被洗錢犯罪所利用，我國在未來亦不免面臨應如何處理加密貨幣洗錢防制的議題。此議題攸關我國未來於金融科技產業的發展、國家競爭力、金融業之繁衰。若立法適宜，不僅能促使我國成為亞太金融重鎮，領先全球、提升我國就業率自不在話下。惟若立法不當，造成產業政策錯誤，不僅錯失以金融科技一躍成為世界金融重鎮之契機，更可能使我國變成洗錢犯罪的天堂，不可不慎。從而，如何在金融科技的發展及洗錢防制兩者間取得平衡,使我國能盡速利用獨步於全球的金融監理沙盒來打造一個繁榮的經濟重鎮，即為本章欲拋磚引玉之目的，期待能集思廣益，討論出一個適合國家前進的法制規劃方向。

加密貨幣必須遵守洗錢防制相關規範已經是各界所達成之共識，完全不受任何管控的加密貨幣就如同脫韁之野馬，必定會有部分人士將其非法利用，造成金融體系的傷害,前章已介紹先進國家及國際組織均著手立法監管加密貨幣之方式。我國為因應 2018 年 11 月的亞太防制洗錢組織(Asia/Pacific Group on Money Laundering, APG)第三輪相互評鑑，近幾年來已提高執法力道，從 2016 年分別修正之「洗錢防制法」及「資恐防制法」和後續公布之一系列「防制洗錢辦法」、「內部控制要點」、「注意事項」、「申報辦法」可知主管機關已開始密切關注洗錢防制的議題。

惟除了加密貨幣對洗錢防制規範的衝擊，尚有其他因素驅使著各國主管機關紛紛針對加密貨幣做出規範。主要原因在於加密貨幣之特性除了易造就洗錢的犯罪環境外，亦將使得透過加密貨幣所犯之財產犯罪較容易開脫。例如因犯毒品危

doi:10.6342/NTU201800740

害防制條例而獲得大量不法所得，此時因前置犯罪所獲之不法所得有時須快速匯至第三國家，犯罪者因此可能面臨地下通匯的抽成及匯率的問題，加密貨幣的問世，可能解決犯罪者上述問題，因此易成為幫助洗錢犯罪得以實施的關聯客體，或著是一種新型態的不法所得移轉方式。另外，加密貨幣亦可能衍生各種型態的網路犯罪，包括刑法第 320 條（普通竊盜罪竊）、刑法第 339 條(詐欺取財得利罪)、刑法第 346 條(恐嚇取財罪)、刑法第 358 條（入侵電腦或其相關設備罪）、第 359 條（破壞電磁紀錄罪）、第 360 條（干擾電腦或其相關設備罪）等犯罪。

為避免加密貨幣造就更多難以追查的洗錢前置犯罪，故有遵循洗錢防制相關規範之必要。洗錢防制的重點主要在於確認客戶身分，破除加密貨幣本身具有之匿名性。首要須受洗錢防制管控之對象為從事加密貨幣與現實貨幣之間的匯兌業者(Money Transmitter—美國法中所謂的交換者“Exchanger”與發行者“Administrator”即屬此類。)，蓋其扮演著替存在於虛擬世界的匿名者兌換現實貨幣的角色，若要破除匿名性從而落實洗錢防制，將無可避免地必須由此下手以追尋可疑金流來源。以下將從我國《國家洗錢及資恐風險評估報告》出發，分析加密貨幣潛在的國家風險(National Risk Assessment, NRA)及產業風險(Sector Risk Assessment, SRA)，以風險為基礎個別探討加密貨幣未來的洗錢防制推行方向。

第一節　國家策略及國家風險評估

國家策略主導著主管機關將採行之洗錢防制模式，是以在探討應採行何種洗錢防制模式之前，應先探究我國可能採行的方針以將加密貨幣的負面影響降至最低，並將加密貨幣於我國金融發展的益處最大化。又因國家策略之制定須考量的面相甚廣，故本文以下將以洗錢防制為中心加以論述。

我國為 APG 之會員，為遵循相關建議及要求，近來大幅加強洗錢防制之力度，

doi:10.6342/NTU201800740

以 FATF 40 項建議為標準，建構防制洗錢與打擊資恐策略之架構，是以本文於前章除美國法外，再以《FATF 虛擬貨幣風險基礎方法指引》為鑒，希冀為較缺乏洗錢防制經驗之我國提出一個可行的洗錢防制架構。

在制定風險策略上，我國未曾進行過國家層級洗錢及資恐風險評估，故對於 FATF 建議採行之風險評估方法論與程序之進行較為陌生。所幸於 2017 年在政府高層及各界支持下，正式成立行政院洗錢防制辦公室 [343]。該機構負責統籌洗錢與資恐風險評估作業、評鑑宣導與教育、有效運用資源，將國內防制洗錢的政治決心具體反映至實際運作層面。執行成果也是有目共睹，在歷經 2017 年 6 月至 2018 年 3 月間共達 4 次的大型國家風險評估會議，與無數次由各不同部門機關參與之小型會議，期間參與之公部門機關部會高達 37 個 [344]、私部門公會及機構亦達 31 個 [345]，終於成功辨識出對我國最具威脅的 8 大類型，包含毒品販運、詐欺、組織犯罪、貪污賄賂、走私、證券犯罪、第三方洗錢、稅務犯罪等類型。

---

[343] 行政院洗錢防制辦公室成立背景：http://www.amlo.moj.gov.tw/ct.asp?xItem=464864&CtNode=45705&mp=8004（最後瀏覽日：2018/04/15）

[344] 公部門機關部會包括：包括：國家安全局、司法院民事廳、司法院刑事廳、外交部、國防部、教育部、法務部、經濟部、勞動部、衛生福利部、金融監督管理委員會、行政院環境保護署、文化部、行政院大陸委員會、行政院海洋委員會海巡署、中央銀行、國家通訊傳播委員會、內政部警政署、內政部移民署、內政部地政司、內政部民政司、內政部合作及人民團體司籌備處、財政部賦稅署、財政部關務署、財政部國際財政司、交通部航港局、法務部調查局、法務部行政執行署、法務部廉政署、經濟部國際貿易局、行政院農業委員會農業金融局、金融監督管理委員會銀行局、金融監督管理委員會證券期貨局、金融監督管理委員會保險局、金融監督管理委員會檢查局、行政院國土安全辦公室及洗錢防制辦公室等。

[345] 私部門公會機構包括：中華民國銀行商業同業公會全國聯合會、中華郵政、全國農業金庫、中華民國信用合作社聯合社、中華民國票券金融商業同業公會、中華民國人壽保險商業同業公會、中華民國產物保險商業同業公會、財團法人保險事業發展中心、財團法人保險犯罪防制中心、中華民國證券商業同業公會、中華民國證券投資信託暨顧問商業同業公會、臺灣集中保管結算所股份有限公司、中華民國期貨業商業同業公會、中華民國信託業商業同業公會、中華民國保險經紀人商業同業公會、中華民國保險代理人商業同業公會、中華民國地政士公會全國聯合會、中華民國不動產仲介經紀商業同業公會全國聯合會、中華民國不動產代銷經紀商業同業公會全國聯合會、中華民國律師公會全國聯合會、中華民國會計師公會全國聯合會、臺灣證券交易所股份有限公司、財團法人中華民國證券櫃檯買賣中心、臺灣期貨交易所股份有限公司、財團法人臺灣金融研訓院、中華民國金銀珠寶商業同業公會全國聯合會、社團法人中華民國記帳及報稅代理人公會全國聯合會、中華民國記帳士公會全國聯合會及社團法人臺北市記帳、報稅代理人公會、臺北市租賃商業同業公會及外幣收兌處等。

doi:10.6342/NTU201800740

表 九：國家風險評估—洗錢威脅辨識結果一覽表

洗錢及資恐評等表			
低	中	高	非常高
1.人口販運 Trafficking In Human Beings (Migrant Smuggling)	1.非法販運武器 Illicit Arms Trafficking	1.仿冒、盜版、侵害營業秘密 Counterfeiting and Piracy of Product, IPR Crime	1.毒品販運 Drug Trafficking
2.性剝削(含兒童) Sexual Exploitation	2.贓物 Illicit Trafficking In Stolen and Other Goods		2.詐欺 Fraud
3.偽造貨幣 Counterfeiting Currency	3.竊盜 Theft		3.走私 Smuggling
4.殺人、重傷害 Murder,grievous Bodily Injury	4.綁架、拘禁等妨害自由 Kidnapping,illegal Restrain		4.稅務犯罪 Tax Crimes
5.搶奪 Robbery	5.環保犯罪 Environmental Crime		5.組織犯罪 Organized Crime
6.勒贖 Extortion	6.偽造文書 Forgery		6.證券犯罪 Securities Crime
7.海盜 Piracy			7.貪污賄賂 Corruption And Bribery
8.恐怖主義、資恐 Terrorism(TF)			8.第三方洗錢 Third-party ML

表格來源：洗錢防制辦公室國家風險評估報告

上表所使用的，係以 FATF 40 項建議中的詞彙表(Glossary)所列舉的 22 項特定犯罪類型(Designated Categories of Offences) 為評估標的，經由分析犯罪者能力[346]、洗錢的規模[347]和估算不法所得[348]等 3 項風險因子分級而成。其中屬於非常高的風險評等項目，幾乎都可以使用加密貨幣進行後續洗錢作業，舉例言之，近年執法

[346] 犯罪者能力係指犯罪者展現的洗錢犯罪知識、技巧、專業、網絡與資源（特別是金融、貿易、法律、資訊科技、知悉反洗錢及管制措施），以運用該知識規避主管機關查緝。

[347] 洗錢規模係衡量犯罪者利用金融機構、指定之非金融事業或人員及其他產業洗錢之程度(犯罪所得)。

[348] 不法所得係指單項前置犯罪或專業洗錢產生之不法所得價值。

doi:10.6342/NTU201800740

機關即發現有以加密貨幣如比特幣支付毒品交易款項之情形，且以大麻最多[349]。在此交易架構中，購毒者係直接以加密貨幣進行交易，在交易前已為販毒者完成洗錢當中的「處置」階段，於成功移轉加密貨幣後，更在雙方交易完成時結束了「多層化」階段，販毒者能輕易將加密貨幣於不同的錢包中無限數次且分拆金額的移轉，以進行後續更深層的「多層化」作業，只待最後兌換成現實貨幣的「整合」程序。如此簡易的洗錢方式，卻讓執法機關面臨著極大的執法困境，不難瞭解為何我國主管機關迫切的想將加密貨幣納入洗錢防制的規範內。

加密貨幣在國家風險層級上具有良好的整合功能，能非常簡易地與每項列入「非常高」的前置犯罪相結合，透過其高度複雜性、廣泛的流通規模，能輕易地放大犯罪者的洗錢能力及洗錢規模，且根據其浮動的價值，讓犯罪所得難以估計。因加密貨幣對於上述新型洗錢模式有著良好的輔助特性，本文擬就國家策略層面著手，探詢應以何種國家層級的策略，降低加密貨幣對於現行已辨識出的高風險洗錢的威脅。

第一項 科技面相與洗錢防制

有著智慧島嶼美稱的我國向來以資訊產業聞名，科技人才輩出，有專門之產學研究中心研究區塊鏈技術[350]，故在科技面實現加密貨幣的 KYC 並不困難。期待在符合國際反洗錢的相關規範下，給予加密貨幣於我國足夠的發展空間，提升我國金融環境的同時亦能提升我國競爭力，吸引海外投資。

雖然如此，但洗錢防制的成本以及難度，會隨著加密貨幣所採行之技術係屬公鏈或是私鏈而有所不同，此為策略考量之要素之一。且加密貨幣可能用於洗錢

---

[349] 行政院洗錢防制辦公室（2018），同前揭註 387，頁 19。

[350] 如籌備中的國立臺灣大學金融科技暨區塊鏈中心及運作中的政治大學金融科技研究中心等是。

doi:10.6342/NTU201800740

犯罪的風險與破除匿名性的難易度有著直接的關連，破除匿名性的難易度則與加密貨幣究竟採行公鏈或是私鏈相關連。誠如第二章所述，公鏈因採行自由參與的開放性架構，任何人皆能加入網絡而成為其中的節點以發布交易訊息進行交易，故認識客戶程序僅能間接要求由主管機關列管之匯兌業者確認交易個體，且確認對象僅限於透過匯兌業者進行交易之人，現行非透過匯兌業者或是交易所進行匯兌之對象(如場外交易平台)尚無法進行確認客戶身分的程序。採行私鏈架構之加密貨幣為讓發行者有效控制寫入及讀取權限，主要之驗證節點通常屬於同一機構，使得主管機關得以透過對該機構進行監管達成全面防制該款採行私鏈架構之加密貨幣被洗錢犯罪所利用的目的，從而破除匿名性。

上述因素皆屬監管加密貨幣尚須考量的要素，並且綜合加密貨幣之特性與經濟效益加以評估。是以本文認為加密貨幣之洗錢防制策略，須按採行公鏈技術或是私鏈技術的加密貨幣有所不同。

第二項 公鏈之洗錢防制策略

第一款 具吸引力的法律規範策略

比特幣係採行公鏈的一種加密貨幣，只要係此類型的加密貨幣，洗錢防制措施上即必須面對無中心機構、無法管控的節點、化名式匿名等問題，以致主管機關就算有心監管，也很難全面性的監管到除了交換業者以外之人。對於採行此種技術的加密貨幣，較適合提供誘因，促使使用者以自身資訊來換取。欲達成此一前提，主管機關必須規劃出一個能提供安定性、安全性的平台，若有基本保障，即能吸引大量合法使用者加入由政府所主導的平台，孤立違法的使用者，使違法使用者手中的加密貨幣難以流通，進而達成洗錢防制的目的。

我國的加密貨幣投資者除私下相約面交外，欲購買或是出售加密貨幣，必然

doi:10.6342/NTU201800740

須經由場外交易平台、加密貨幣經紀業者及加密貨幣交易所。場外交易平台因僅負責撮合欲交易之雙方，並不會深入瞭解客戶資訊，再加上這類平台業者通常會將網站架設在國外，因此欠缺洗錢防制上的可行性。欲解決民眾透過場外交易平台進行交易，應先加強加密貨幣經紀業者及加密貨幣交易所的吸引力。惟在不經由政府補貼業者的前提下，若要在法律規範上提升我國加密貨幣經紀業者及加密貨幣交易所對於使用者的吸引力應可從兩方面著手。本文一方面參考近期因空前的「洗錢防制總動員」對金融機構的客戶所產生的困擾[351]，認為不可過度苛求加密貨幣經紀業者及加密貨幣交易所對客戶進行過嚴密的審查，另一方面似可從法律規範上強制要求經紀業者及交易所就可能發生的駭客事件進行投保、成立類似存款保險的基金、準備一定數額之準備金、以及專門適用於加密貨幣匯兌業的流動性覆蓋比率(Liquidity Coverage Ratio, LCR)規範等。

就法規策略上，避免課予經紀業者及交易所過於苛求的審查義務，將能增加客戶使用我國本土服務之便利性，進而吸引客戶選擇使用本土之交易服務。此為法規為避免過於嚴苛的確認客戶程序，導致如同金融機構一般出現的擾民現象於加密貨幣經紀業者上再次重演，所需施行的消極法規策略。本文建議以前文所分析的「指定非金融事業」之規範為參考對象，最多不宜超過前揭標準。積極法規策略則除如同上述參考金融機構之作法成立存款保險基金及對資安事件進行投保外，本文認為有必要針對經紀業者之資訊安控方面，訂定類似於金融機構之《金融機構辦理電子銀行業務安全控管作業基準》。蓋近來加密貨幣經紀業者及交易所

[351] 工商時報（2017/04/19），〈洗錢防制 矯枉過正反擾民〉，https://m.ctee.com.tw/album/ab438efa-d245-4a92-b786-11a2cbb976ee/800282（最後瀏覽日：2018/07/08）；自由時報（2017/03/23），〈洗錢防制擾民？立委爆：結婚 50 萬禮金銀行拒收〉，http://ec.ltn.com.tw/article/breakingnews/2010097（最後瀏覽日：2018/07/08）

doi:10.6342/NTU201800740

被駭客入侵之案件頻傳，如從今年 1 月開始，日本最大的加密貨幣交易所之一 Coincheck 因平台遭駭客入侵導致全部約 5.26 億個新經幣 [352]（New Economy Movement Coin, 簡稱 NEM(XEM)幣）被非法轉移。據估算，這批丟失的新經幣價值 5.23 億美金 [353]（約為台幣 152 億元）。2018 年 6 月 10 日南韓國內排名第 7 的虛擬貨幣交易平台 Coinrail 遭駭，造成價值約 400 億韓元（約新臺幣 11 億元）之虛擬貨幣失竊，約略等同於該交易所買賣虛擬貨幣的 30% [354]。其後於 2018 年 6 月 20 日全球第 6、南韓第 1 大的虛擬貨幣交易平台 Bithumb 傳出遭到駭客入侵，被駭走價值 350 億韓元（約新臺幣 10 億元）的虛擬貨幣；南韓資安公司 Hauri 指出：「雖然 Bithumb 在資安方面付出相當多的投資，但是與法律上有強制規範安全標準的金融公司相比，水準還差一大截」[355]。前車之鑑，後車之師，本文前文雖認為於確認客戶資訊等洗錢防制所帶來之義務上可採去與金融業相較之下較為消極之法規策略，毋庸超出現有之「指定之非金融事業」；惟本文認為加密貨幣匯兌業因行業特性使然，為提供使用者穩定、安全的環境，資安控管、加密貨幣存款保險、準備金制度等有助於吸引本土使用者使用為於我國服務之法規範，應採積極之立法策略，訂定明確標準，特別是資安控管上，其標準可能須至少趨近於金融機構之標準或是達到同等標準。

最後本文所提及的專門適用於加密貨幣匯兌業的流動性覆蓋比率(Liquidity

---

[352] 截至 2018 年 7 月 NEM (XEM)幣市值約 1,687,023,000 美元，加密貨幣世界排名第 16 名；*NEM (XEM) Price, Charts, Market Cap, and Other Metrics*, COINMARKETCAP, https://coinmarketcap.com/currencies/nem/ (last visited July 8, 2018).

[353] 科技橘報（2018/01/29），〈【整個平台被盜光光】史上最大虛擬貨幣被駭案，日本交易所損失 124 億台幣〉，https://buzzorange.com/techorange/2018/01/29/japan-coincheck-hacked-all-money-gone/（最後瀏覽日：2018/07/08）

[354] 經濟日報（2018/06/12），〈比特幣又被駭 引發拋售潮〉， https://udn.com/news/story/6811/3193368（最後瀏覽日：2018/07/08）

[355] 自由時報（2018/06/22），〈BITHUMB 遭駭價值 10 億元虛擬貨幣 韓警展開調查〉，http://ec.ltn.com.tw/article/breakingnews/2466635（最後瀏覽日：2018/07/08）

doi:10.6342/NTU201800740

Coverage Ratio, LCR)規範，同樣是以穩定、安全的產業基礎為出發點，主要適用之對象為自身從事匯兌業務的經紀業者，因此類業者非如場外交易平台及交易所主要提供居間的功能，而係以自身之儲備金及加密貨幣從事匯兌業務，為避免過大的加密貨幣產業事件產生加密貨幣瘋狂擠兌及提領，促使經紀業者臨時「停機維修」，故有必要針對流動性風險設置基本的規範措施。參考《銀行流動性覆蓋比率實施標準》第 2 條及巴塞爾銀行監理委員會於 2013 年 1 月發布之「巴塞爾資本協定三：流動性覆蓋比率與流動性風險監控工具」（Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools）所謂流動性覆蓋比率係指合格高品質流動性資產總額除以未來三十個日曆日內之淨現金流出總額，主要目的為強化銀行短期流動性之復原能力，衡量銀行於壓力情境下是否具備足夠之合格高品質流動性資產，以因應未來三十日之現金流出需求[356]。本文認為欲將此標準套用至經紀業者，則需將標準大幅降低，參考加密貨幣匯兌行業之貨幣漲跌特性大幅縮短因應未來現金流出需求的期間。原因在於我國主管機關將加密貨幣認定為一種資產，此由我國中央銀行自 2013 年即稱呼虛擬通貨為「虛擬商品」可知。中央銀行總裁楊金龍於 2018 年 8 月 7 日「2018 金融科技生態系領袖峰會」發表之「虛擬貨幣與數位經濟」演講更是重申：「虛擬通貨充其量只是加密資產，而非貨幣，無法取代法定貨幣」並且點出 7 大問題包括：「1.貨幣供應量無法調節；2.價格波動大；3.效率低；4.耗能；5.硬分叉；6.無求償管道；7.易被不法人士利用」[357]。因加密貨幣並非貨幣，且在我國亦未能被市場普遍信任，是以本文認為用於規範現實貨幣的方式不宜逕行套用至加密貨幣。於參酌規範現實貨幣之作法前尚應考量加密貨

[356] 銀行流動性覆蓋比率實施標準總說明。

[357] 楊金龍（2018/08/07），〈虛擬貨幣與數位經濟與數位經濟：央行在數位時代的角色〉。載於：中央銀行，https://www.cbc.gov.tw/public/Attachment/888144602.pdf（最後瀏覽日：2018/08/10）

doi:10.6342/NTU201800740

幣本質上造成其難以成為貨幣的問題，並將欲套用之規範內容加以稀釋。此類做法亦符合以風險為基礎的規範模式，蓋性質越似於現實貨幣，理論上其被洗錢犯罪所利用之風險則越大；同理可證，性質上離現實貨幣越遠，其理論上被洗錢犯罪所利用之風險則越低。我國主管機關目前將加密貨幣定位為非貨幣，故本文同樣提倡以非貨幣的規範模式。在此所提倡之流動性覆蓋比率規範方式旨在提供加密貨幣之消費者一種保護措施，促成一個既對消費者友善且賦予國內之加密貨幣交易所及經紀業者較場外交易平台更具吸引力的環境。惟具體是否應採行此種保障措施？又應套入何種標準？尚待專業學者及各界先進研究。

除制定上述消極法規策略及積極法規策略外，尚有將完整達到積極法規策略之經紀業者及交易所納入由官方認證的機制，以證明該機構確實有達到我國政府為促進穩定、健全之加密貨幣交易環境之目的所訂定之法規範或是標準。認證機制可與執照機制相互配套，如完成主管機關所規範之種種需求並經認證後始授予與認證相對應的營業許可。一言以蔽之，按法規範所制訂之標準分別給予認證，再按認證賦予相對應的營業許可，如此一套由政府背書且明確的制度，方能吸引公鏈型加密貨幣之使用者。惟此牌照初始的發放標準不宜過嚴，蓋政府的初期目標應是達成一個具有良性競爭力的加密貨幣匯兌環境，此一環境內必須要有眾多業者參與，才能達成一個「手續費」及「交易匯率」不致偏離世界各大交易所的交易行情。也因此我國近期已出現主打零手續費之加密貨幣交易平台[358]。若能造就此一環境，相關部門即較無須擔憂會有投資客將現實貨幣匯往國外購買加密貨幣。此乃因本國自有的競爭環境有著不遜色於外國交易所的交易匯率，且具有牌

[358] COBINHOOD 會收取多少交易手續費？載於：https://cobinhood.zendesk.com/hc/zh-tw/articles/360001593431-COBINHOOD-會收取多少交易手續費-（最後瀏覽日：2018/07/08）

doi:10.6342/NTU201800740

照之加密貨幣匯兌業者均符合政府所訂定之相關規範，較有保障，相較於國外交易商出事時「求償無門」的機率偏低，更何況能免去外匯匯差的成本，又能以本國貨幣進行交易，實難想像如此優渥的環境不吸引本國的加密貨幣投資者。

在成功達成上述吸引加密貨幣投資者的環境後，能確保任何向我國加密貨幣匯兌業者購買加密貨幣之現實貨幣不會因為兌換為外匯而外流，此其一。更重要的是，主管機關後續僅須針對加密貨幣匯兌業者的牌照予以定期審查，即能促使此一行業充分遵守主管機關之規範；其中確保客戶身分資訊、掌握疑似洗錢金流、確保匯兌業者於限定範圍內持有一定數量之現實貨幣及加密貨幣等，均非難事。

至於發放許可執照的相關規範，則似可參考上述重點及第四章之分析，就洗錢防制部分，按照目前主管機關對「指定之非金融事業」所採行之洗錢防制標準即可，取目前洗錢防制規範的最大公因數，先避免苛求業者制定一系列的洗錢防制方法論、進行繁瑣的驗證程序及持續審查客戶(OEDD)及設置專門法遵部門。就增加行業安全性及穩定性部分，則得以資安控管、加密貨幣存款保險、準備金制度、專門適用於加密貨幣匯兌業的流動性覆蓋比率等有助於吸引本土使用者使用位於我國服務之法規範。

上述制度除洗錢防制規範至少需以現行之「指定之非金融事業」為最低標準，其他積極性的立法措施似可按被主管機關認證的水平，進行執照等級上的區分，回歸按法規範所制訂之標準分別給予認證，再按認證賦予相對應的營業許可的指標。所發放之許可執照應設置較短的許可期限，如 2 年至 3 年，屆期再以更新執照的方式獲得繼續營業之許可，以利主管機關持續為服務使用者把關，確保如資安等相關的法規範均有實際落實。

另外按本文所建議的發放方式，初步許可執照之發放邏輯為將許可執照區分

doi:10.6342/NTU201800740

為一級、二級、三級，並且分別給予授權許可之項目；當然，隨著授權許可項目的遞增，主管機關伴隨之監管力道亦會隨之提升。本文認為一級許可執照之授權經營項目，應可涵蓋所有加密貨幣之匯兌業務、發行加密貨幣期貨、證券、指數型證券投資信託基金等金融商品以及承銷首次加密貨幣發行之業務、所屬客戶從金融機構轉入款項及匯出款項不設限制等。二級許可執照授權之範圍，則僅涵蓋加密貨幣之匯兌業務、或加密貨幣與支付相關的代理業務，不會涵蓋至其他加密貨幣金融商品、另外此類執照業者所屬之客戶從金融機構轉入款項及匯出款項將設置一定限制等。三級許可為管制最寬鬆之加密貨幣許可執照，此類執照僅容許從事商業行為之人接收加密貨幣，如接受加密貨幣作為付款之商家。本文除一級、二級許可外，尚建議設立第三級許可之原因，在於未來當加密貨幣不再需要經過匯兌業者兌換回現實貨幣方能使用之時，因一切交易行為不會透過由主管機關監控之匯兌業者，將使得不法金流無從識別起。但如果將接收加密貨幣做為直接服務對價之商家納入資料庫，至少能從數據識別上順藤摸瓜，從商家之錢包逆向追查加密貨幣之來源，若發現源自於被列入警示之錢包地址，則該筆用於支付之加密貨幣將有可能是經過「多層化」後之不法所得，將能調閱店家監視器提供檢調獲得更多使用加密貨幣之人之線索。此類許可因僅是幫助主管機關有機會能辨識直接使用加密貨幣進行交易之使用者，故無需付出任何系統建置成本或遵循成本。茲將上述規範邏輯繪表如下：

doi:10.6342/NTU201800740

表 十：加密貨幣許可執照相對應之法律遵循規範

規範項目 / 許可等級	洗錢防制規範	資訊安控規範	類加密貨幣存款保險	準備金比率	流動性覆蓋比率
一級許可	以指定之非金融事業為最低標準	金融機構等級或趨近於金融機構等級	保額較高	比率較高	標準較高
二級許可			保額較低	比率較低	毋庸適用或是較低之標準
三級許可	無（至多手機簡訊認證）	僅需將交易地址回報	無		

第二款 由主管機關輔助成立自律組織

主委顧立雄指出：「未來使用者在作數位貨幣與法定貨幣要交換時要『實名制』，而且比特幣業者要有自律組織[359]」。可見主管機關於初步規劃上認為法規範僅占洗錢防制的一部分，另外很大一部分應由業者透過組成自律組織，「發展出一套本身必須做的查核動作」[360]。成立自律組織的功能在於有效統合產業的需求，並集合產業意見向主管機關溝通應如何規範才能同時達成主管機關的需求及產業內部的良好發展。目前主管機關僅明確表示的需求僅是希望加密貨幣匯兌業者從事加密貨幣與法定貨幣之間的匯兌時需要「實名制」，至於應達到何種程度的實名制並未說明。本文於第四章已舉銀樓業及地政士及不動產經紀業為例，推測被歸類為「指定之非金融事業」將可能需遵循之認識客戶義務，前者僅需確認客戶身分，及留存或記錄其身分資料，如由代理人代理則須確認代理人身分資料、並將其留存或記錄外，確認其代理權之真實性；後者則須進一步就法人客戶及實質受益人等身分資料進行確認。此時若主管機關若對應否兼採行後者措施有疑慮，則得與加密貨幣匯

[359] 中時電子報（2018/05/29），〈比特幣納管 顧立雄：要實名制與自律組織！〉，http://www.chinatimes.com/realtimenews/20180529001913-260410（最後瀏覽日：2018/07/09）

[360] 同前註。

doi:10.6342/NTU201800740

兌業之自律機構進行討論，詢問實務上是否准許法人進行加密貨幣之交易，若現行實務上均須由自然人本人之身分資料及帳戶始得進行交易，且自律組織亦表示未來不會接受法人客戶，則無需就法人及實質受益人相關部分進行規範。類似協調之案例，亦可套用至本文所建議之規範項目，如自律組織一致認為無需共同建置類似存款保險的加密貨幣存款保險制度，認為準備金之比率應向下調整，或是制定流動性覆蓋比率將會過於嚴苛，均得敘明理由及可能達成同等安全、穩定目標之替代方案與主管機關討論，隨時更動許可執照的發放標準與應達到之標準。藉由此種產業內部的交流，統一意見與需求，再和主管機關討論如何始能達成監管欲達成之目的，始能協助主管機關訂定出一套具有規範上實益且能具體落實與執行的法律規範，避免空具法律條文規定卻又因立法過苛而導致「說一套，做一套」的情勢發生。

自律組織既然有著統合意見與協助主管機關訂定法規範之效果，理應於產業發展初期盡速產生，主管機關此時能給予之助力在於官方上予以許可，並承認自律組織擁有代表該產業的話語權，將其公告於眾，以助自律組織有要成立。瑞士主管機關 FINMA 的作法更是進一步將前款法律規範與自律組織相結合，創造許可制上的雙軌制。在瑞士，欲成為受許可之加密貨幣匯兌業者有兩項途徑，其一是直接向主管機關申請許可，核准後發予許可執照，當局稱此類業者為受直接受監理之金融中介者(Directly Supervised Financial Intermediary, DSFI)[361]；其二是加入由官方所認許之自律組織(SRO)[362]。瑞士之自律組織因在自治規範上須符合主管機關所訂定之規範，且獲得官方的授權許可，故有權力及義務要求旗下成員遵循主管

[361] Kevin Helms, *How Bitcoin Companies Can Legally Operate in Switzerland*, BITCOIN NEWS (Feb. 1, 2017), https://news.bitcoin.com/bitcoin-companies-legally-operate-switzerland/.
[362] *Id.*

doi:10.6342/NTU201800740

機關所制定的相關規範，並於偵查到違反之情事時做出懲處，等於由自律組織透過真正實質意義上之自我規範落實由主管機關制定的相關規範[363]。繪圖如下：

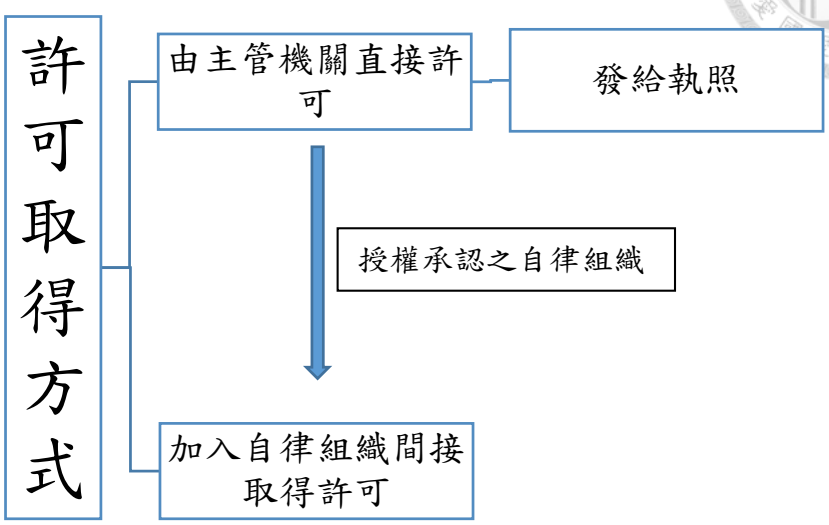


圖 八：以雙軌制發放許可執照

是否賦予加入自律組織具有間接之許可營業權，端視主管機關如何取捨，惟於自律組織成立初期，最為重要的還是彙整產業內的需求及凝聚共識。若要採行如瑞士的雙軌併行制，則自律組織內部勢必須成立負責督導與裁罰的委員會，以對內部成員開罰。惟於組織成立初期，可能會產生無一成員能完整遵循主管機關所訂定之相關規範的狀況，能否期待自律組織所組成的委員會對己課予公正的罰鍰？若真課予罰鍰，是否會因此而影響初期加入自律組織成員間的和諧，最終導致自律組織自行瓦解？本文認為較保守的作法應是先由主管機關和輔助成立之自律組織相互協調，或由自律組織先行訂定自律規範，再向主管機關共同討論應採行之規範標準。例如 2018 年 8 月 10 日「亞太區塊鏈發展協會」所發佈之「虛擬通貨交易所會員自律公約」(Self-Regulatory Guidelines, SRG) 即於第 1 條開宗明義指出「建立與主管機關雙向充分互信監理溝通管道」的重要性「藉以排除障礙（例

363 *Id.*

doi:10.6342/NTU201800740

如信託機制、KYC 權限等），即時共同研擬對策[364]」。

第三款 監理科技

監理科技(RegTech)同金融科技(FinTech)一詞，皆是由英文翻譯組合而成的新名詞。國際金融協會(Institute of International Finance, IIF)將監理科技定義為：「使用新科技以更有效及更具效率的方式滿足監理及遵法之需求[365]」。英國金融監督管理局（或稱金融行為監管局 Financial Conduct Authority, FCA)則稱監理科技為：「協助金融服務合乎規範的新科技[366]」。我國 2016 年 5 月公布的「金融科技發展策略白皮書」則將監理科技稱為法遵科技，是一種「利用資訊科技，廣泛蒐集各國金融監理制度與法規要求，提供分析與管理的工具，自動協助金融機構遵守法規要求，以降低作業風險，相關工具包括法律/監理差距分析、全球法規遵循、資訊管理、合規性健診、監管報告、交易報告、培訓、活動監控、風險資料倉儲、案例管理等工具」[367]。

上述三種定義皆有著共通之處，亦即將此種新科技用作取代舊式之監理、遵法、合規模式。雖然監理科技的發展尚處於萌芽的階段，但若觀察金融科技之例，現正邁向數位金融 4.0（亦稱 Bank 4.0）之我國，透過互聯網、行動銀行及理財機器人所提供的自動化金融服務，已逐漸取代舊式以人工為主的服務，此為全球銀行業之趨勢。在此趨勢下，傳統銀行漸進式地將資源轉移到網路銀行服務，如位

---

[364] 林盟翔（2018/08/16），〈虛擬通貨分級監理 產業自律探路〉， https://m.ctee.com.tw/expert/289f93d0/10190（最後瀏覽日：2018/08/17）

[365] INST. INT'L FIN., REGTECH IN FINANCIAL SERVICES: TECHNOLOGY SOLUTIONS FOR COMPLIANCE AND REPORTING 2 (2016), https://www.iif.com/system/files/regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf. ("Regtech" is "the use of new technologies to solve regulatory and compliance requirements more effectively and efficiently.)

[366] *RegTech*, FCA UK, https://www.fca.org.uk/firms/regtech (last updated June 28, 2018). (RegTech applies to new technologies developed to help overcome regulatory challenges in financial services.)

[367] 金融監督管理委員會（2016），《金融科技發展策略白皮書》， https://www.fsc.gov.tw/uploaddowndoc?file=news%2F201605181357350.pdf（最後瀏覽日：2018/07/10）

doi:10.6342/NTU201800740

居美國第 2 大的美國銀行，在近 2 年內關閉本土逾 500 家分行；又如法國第 3 大的興業銀行，計畫在 2020 年前關閉本土分行達 400 家。其他如英國匯豐、渣打、美國摩根大通…等跨國銀行，亦都有大規模關閉分行及裁員的計畫，以便大步跨進「去實體分行」（De Banked）的 Bank 4.0 時代[368]

金融科技的興起伴隨而生的問題之一，是如何於經數位化的海量交易資訊之中進行監理。蓋金融科技的推行將導致部分舊式的監理模式不再如以往般適宜；於是乎，本文亦認同監理科技做為金融科技下的一子項目[369]，未來將會取代舊式的監管工具（Tools）成為新型的監理媒介。在歷經此轉換的過程中，主管機關的監理模式為跟上金融科技的發展及監管工具的淘汰，即須從舊式的賦權式監理模式（Empowering Regulation）進化成新型態的賦能式監理模式（Enabling Regulation）[370]。有論者稱科技賦能指的是「運用科技幫助人類超越極限，做到過去無法完成的事情，並迎向未來挑戰[371]」。結合賦能及監理兩者，可得出所謂賦能式監理應是利用監理科技賦予監理機關足以監理的能力，亦即對監理機關做科技賦能[372]。學者指出：「不管是 ICO 或者是加密貨幣都是創新的新興科技議題，不管哪個單位作為監理機關，該機關是否有能力因應，是非常重要的關鍵。」並且建議應該要讓監理機關勇於做新的嘗試與探索，畢竟「現在傳統金融與區塊鏈金融的發展，就

---

368 工商時報（2015/10/22），〈Bank 4.0「去實體分行」浪潮的挑戰〉，http://www.chinatimes.com/newspapers/20151022000050-260202（最後瀏覽日：2018/07/10）

369 彰化銀行（2017），〈監理科技〉，《彰銀資料》，第 66 卷 11 期，2017 年 11 月。

370 郭秋榮（2018），〈全球金融科技之監理對我國之啟示（上）〉，〈證券服務〉，第 664 期，頁 71-72。(文章著者整理自 2016/11 臧正運「金融科技的治理與監管」簡報)。

371 商業周刊（2017/11/27），〈2017 IBM Forum 科技賦能--擅用科技，助人類超越極限〉，https://www.businessweekly.com.tw/article.aspx?id=34037&type=Indep（最後瀏覽日：2018/07/10）

372 iThome（2018/05/30），〈ICO 比照創櫃板群募規則？立委要求金管會一個月內提出研商結果〉，https://www.ithome.com.tw/news/123517（最後瀏覽日：2018/07/09）

doi:10.6342/NTU201800740

像是在三萬英呎高空更換飛機引擎，對監理機關都是很大的挑戰[373]。」

本文贊同前揭見解，認為主管機關於監理科技的發展上，扮演著舉足輕重的角色，蓋監理科技的發展與監理規範相輔相成，如同共生關係。主管機關須先有相應之科技能力，始能瞭解並充分擬定與監理內容相關的標準。例如能適用監理科技監理之內容可能包括資本額、組織設立型態、強制信託保護資金、實地或表報查核、消費者保護、個資隱私、防制洗錢與打擊資恐等[374]，惟當主管機關欲以加密貨幣為防制洗錢與打擊資恐之監理對象時，主管機關本身是否瞭解加密貨幣之性質？是否已做足科技賦能？若具備科技賦能，能否將其應用於監理上最終形成防制洗錢之監理科技？

公鏈型加密貨幣因其性質，已難以單純利用舊式的賦權式監理模式進行監理，確認客戶身分相關之法律規範及制定資訊安全標準僅能以加密貨幣匯兌業者為規範對象達成部分的加密貨幣監理。使用者若非使用經本國核可之加密貨幣匯兌業者，如利用場外交易平台私下交易或是外國之加密貨幣匯兌業者進行交易，則會因為未經過被監理之對象而不受監理形成監理漏洞。

因此本文認為公鏈型加密貨幣之監理策略，除了上述法規建置及成立自律組織並讓兩者相互配合協調外，未來尚須發展一套適用於加密貨幣之監理科技，以補足監理漏洞，這是發展金融科技必須面對的問題。有論者認為監理科技跟金融科技是並行的，如果要做更多的創新發展與開放，必須用新的、更有效的監理科技來協助監管[375]。本文從其論點，從金融科技一直汰舊換新向前邁進之例可知，

---

373 同前註。
374 郭秋榮（2018），同前揭註 370，頁 72。
375 姜統掌（2018/04/02），〈FinTech 核心：普惠金融、監理科技〉，http://www.ecf.com.tw/tw/article/show.aspx?num=149（最後瀏覽日：2018/07/09）

doi:10.6342/NTU201800740

金融與監理的發展如同逆水行舟，不進則退，一但起了頭，若不願被趨勢所淘汰，只能繼續跟隨，與之共同發展。可預見的，監理科技將會追隨金融科技發展的腳步，此為科技不斷向前邁進下所使然；例如貨幣型加密貨幣發展至今日，就監理加密貨幣之監理科技雛型，已有論者提出分析：進出於比特幣中繼節點的封包(交易訊息)來判斷發起交易的初始節點，進而推測比特幣發送、接收地址的網際網路協定位址(Internet Protocol, IP)，且此偵測方式並不因加密貨幣經由混幣服務[376](Mixing Service)而受影響[377]。

賦權式監理模式轉換成成新型態的賦能式監理模式，是未來我國欲致力發展金融科技所不可迴避的問題，但在現階段加密貨幣之監理規範尚未明確以前，可能還須先以賦權式監理模式為努力目標，待日後我國主管機關達到充分的科技賦能後再利用監理科技補齊加密貨幣監管上的灰色地帶[378]。

第三項 私鏈之洗錢防制策略

私鏈區塊鏈技術擁有非常可觀的應用價值。採行此類型的加密貨幣，洗錢防制難度相較於採行公鏈之加密貨幣低上許多。主要原因在於發行者對所發行的加密貨幣具有較多控制權限[379]，只要能有效監管該加密貨幣發行業者，就能相當程度地防制存在於私鏈上的加密貨幣被洗錢犯罪所利用。因私鏈運用層面極廣，故

---

[376] 混幣服務的運作模式是由服務提供者接收加密貨幣後，透過大量、密集發送隨機數量的比特幣至無數個受控制的加密貨幣帳戶內，讓加密貨幣看起來像是在流通。上述過程會一直重複，直到客戶提供的加密貨幣全部發回至預定接收方的地址。

[377] Philip Koshy et al., *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, 8437 FIN. CRYPTOGRAPHY & DATA SEC. 469, 469-85 (2014).

[378] 工商時報（2018/02/05），〈金管會迎戰金融科技 將增聘監理科技人才〉，http://www.chinatimes.com/newspapers/20180205000219-260202（最後瀏覽日：2018/07/10）

[379] Justin O'Connell, *What Are the Use Cases for Private Blockchains? The Experts Weigh In*, BITCOIN MAG. (June 20, 2016), https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/; Wendy（2016），〈區塊鏈大牛們居然是這麼評價私鏈的〉。載於：巴比特資訊，http://www.8btc.com/experts-private-blockchains（最後瀏覽日：2018/06/15）

doi:10.6342/NTU201800740

在細部規範上可能更為複雜，但從洗錢防制的本質觀察，涉及加密貨幣及現實貨幣匯兌的私鏈應是首要規範對象，其次則為牽涉到消費者保護議題的私鏈。前者較有可能涉及洗錢或是構成易於洗錢的前置犯罪行為，故為本文重點討論之對象。

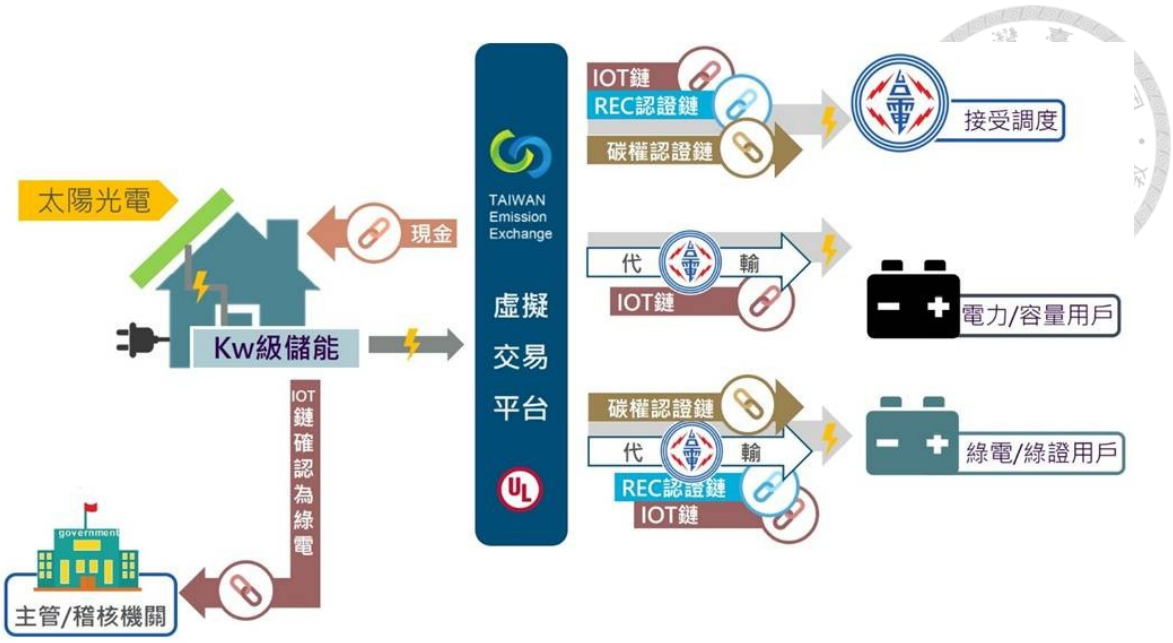
第一款 非審慎監理策略

私鏈於結構上如前文所述，可再區分成半私鏈架構及全私鏈架構，而較有可能涉及加密貨幣洗錢的架構為半私鏈架構，因為採行該架構的加密貨幣能在保有一定程度的帳本公開性之下，由發行者制定更多有關加密貨幣的性質，例如發行數量、貨幣功能、貨幣用途等等。舉例言之，台灣碳交易公司（TWEE）與工研院合作合作開發之「區塊鏈再生能源調度交易平台」，即透過混合一共 4 條採行私鏈架構之區塊鏈[380]，進行數位再生能源憑證與數位碳權的發行，不僅如此，發電者也能直接透過區塊鏈進行交易，包含獲得儲能獎勵、數位再生能源憑證與數位碳權的交易。此例體現了私鏈架構的發行者所發行的每個單位的加密貨幣，是可以經過政府認證的，政府也有能力監管此架構下所發行的加密貨幣；此例另外也體現了私鏈架構能經由多條區塊鏈相互認證，加密貨幣調度平台能控制綠色能源幣和碳權幣的發行數量及匯率、制定貨幣的功能、就不同貨幣區分不同用途等等；此例甚至體現了發行者就私鏈所享有的資訊控制程度，如：達成對主管機關公開區塊鏈上所有機構各自所賺取的綠色能源幣和碳權幣，但各機構卻只能查詢各自從歷史以來所進行的交易資訊。

---

[380] 第一是用來儲存發電紀錄、確保為純綠電的 IOT 鏈，第二是頒發再生能源憑證的 REC 鏈，第三是回饋綠能獎勵的以太坊，第四則是碳權認證鏈。

doi:10.6342/NTU201800740



圖片來源：台灣碳交易

圖 九：私鏈理論上可由政府機關輕易監管之案例

上述案例的加密貨幣較貼近產業上的應用，且願意將資訊公開予政府機關，現實貨幣與加密貨幣之間的金流來源均有跡可循，參與用戶理論上皆須通過實名制，故其可能用於洗錢的疑慮，遠低於公鏈型加密貨幣。規範上應可採行寬鬆審查的方式，例如採取申報生效制，規定機構應先申請主管機關核予加密貨幣發行許可執照，若主管機關於一定期限內未附理由予以否准，則視為同意。準此，私鏈的監管策略尚包含著由主管機關部分介入，惟不宜超過「指定之非金融事業」防制洗錢與打擊資恐之標準。

主管機關對於上述標準最關注的，應仍是如何破除匿名性及落實通報機制。就匿名性而言，因採行全私鏈及半私鏈架構之加密貨幣所運作的節點具有被控制的可能性，是以要遵循確認客戶身分並不困難。又因為採行私鏈架構之加密貨幣僅依賴一定數量的節點完成共識決，故可被操控的可能性上遠高於公鏈，已被移轉的加密貨幣或許能經由各節點達成共識而再次被移轉，或是利用分岔的方式孤

doi:10.6342/NTU201800740

立被盜取的加密貨幣[381]，是以較公鏈架構之加密貨幣更不容易被當成是洗錢犯罪的犯罪客體。如此一來，似可以「非審慎監理」(Non prudential Regulation, Conduct of Business Regulation，亦稱為「業務行為」監理)為監理策略。有論者參照微型金融之例，舉出通常會選擇採行非審慎監理的三個主要目的：1.保護金融服務的消費者；2.使各種機構可以提供多種恰當的產品及服務；3.提供政府制定經濟、金融和刑事執法策略所需的資訊[382]。

本文參照上述三項主要目的，認為採行私鏈架構之產業亦有上述三項需求，且能進行套用。以保護金融服務的消費者及便利機構提供服務出發，套用至私鏈型加密貨幣產業，即是為確保開發私鏈區塊鏈之金融科技業者不至於因過嚴苛的立法及規範而導致業者望之卻步，同時亦是希望業者因為較低的產業門檻而將所降低的成本回饋予消費者，使得消費者更容易能享受到採行私鏈架構之加密貨幣所帶來之便利性，保障消費者的權益。就配合制定經濟、金融和刑事執法策略而言，則以避免將繁瑣的審慎監理用於非審慎目的為原則[383]，於不影響私鏈產業的範圍內僅就需審慎監理之事項進行必要的監理，例如最基本的認識客戶程序以達成防制洗錢及打擊資恐之目的。為同時達到最低程度的干預及金融和刑事執法策略上的需求，本文以下就採行私鏈架構之加密貨幣提出審計節點的監理科技，期待能兼顧產業發展與監理，在非審慎監理的監理密度下達到對部分資訊審慎監理的目的。

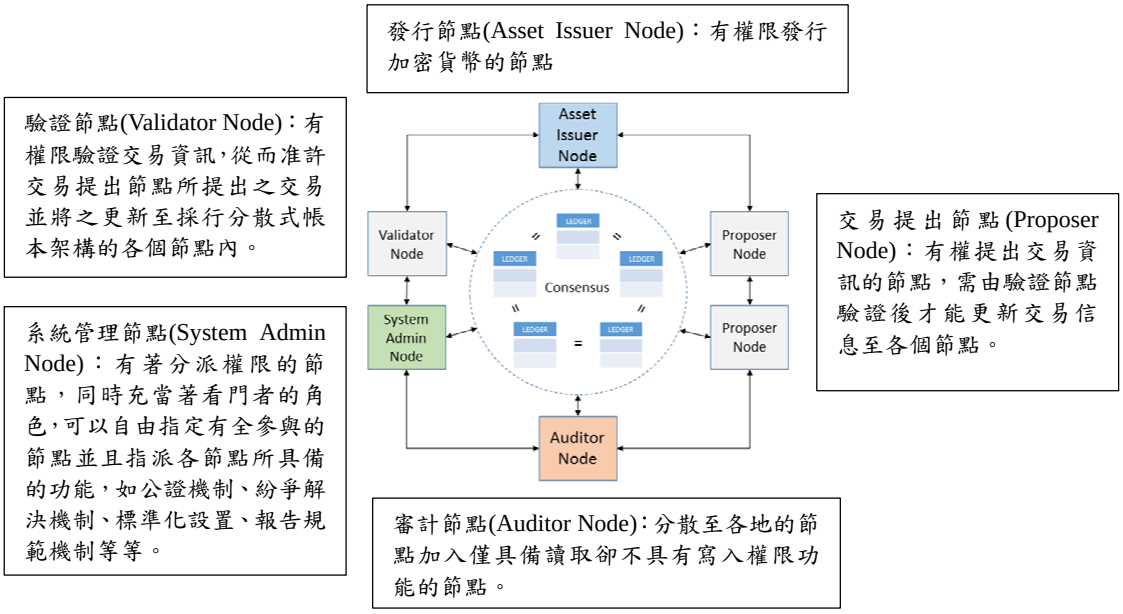
---

[381] 如本文第二章第二節第二項第三款所提及的 DAO 事件。
[382] 林盟翔（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 42-44。
[383] 同前註，頁 42。

doi:10.6342/NTU201800740

第二款 審計節點

審計節點的建置是國際清算銀行(Bank for International Settlements, BIS)之支付及市場基礎設施委員會(The Committee on Payments and Market Infrastructures, CPMI)所提出的一個可能採行之監管架構，亦即在分散至各地的節點加入僅具備讀取卻不具有寫入權限功能的節點。有論者提出為追蹤採行分散式帳本技術之加密貨幣金流之流向，可建置「審計節點」(Auditor Node)，讓區塊鏈上的交易資料具有「可審計與可追溯性」，以利主管機關審核、追蹤與監控區塊鏈上之交易歷程[384]。審計節點的運行方式如下圖所示：



圖片來源：CPMI, Distributed Ledger Technology in Payment, Clearing and Settlement.

圖 十：私鏈型加密貨幣的運作架構及可能採行之洗錢防制方式

從上圖所表述之架構可知，審計節點的權限別於其他種類的節點，更有所謂的系統管理節點，該節點有著分配權限的權限，所以才能限制審計節點僅能讀取而不能寫入。由此觀之，具有審計節點的區塊鏈架構多半不會是採用公鏈的交易

384 臧正運（2017），〈區塊鏈運用對金融監理之啟示與挑戰〉，《月旦法學雜誌》，267 期，頁 142。

doi:10.6342/NTU201800740

架構，蓋節點權限的分派牽涉到能主導整個帳本運行的管理者，此角色的存在對於完全開放的公鏈是一個足以影響「去中心」、「去信任」機制的問題，因為前述的機制之所以能夠確信能被實踐，就是因為依賴共識演算法所產生的共識決，並不會有一個能主導各節點權限設定的管理者出面操控干涉。職是之故，目前存在於交易市場的加密貨幣不會有所謂的「審計節點」，也不見有所謂的管理節點，存在的僅有交易提出節點及驗證節點。是以於實行面上，公鏈型加密貨幣無法如私鏈型貨幣加入審計節點，最終可能採行之方式即如同 FATF 虛擬貨幣指引內所述 VCPPS 為主要規範對象。

惟採行私鏈架構之加密貨幣，並無如同公鏈架構之加密貨幣在實行面上面臨難以加入審計節點的問題。蓋如前所述，私鏈架構內的驗證節點及具備功能其他功能的節點多半是由可識別的業者所控制，主管機關理論上僅需增訂能加入審計節點的規範即能安插審計節點至業者所控制的私有鏈內，監控所有交易內容。至於審計節點應具有何種權限，端視業者與主管機關協調之結果，例如法務部調查局有一套針對金融機構疑似洗錢或資恐交易態樣的可疑表徵判斷表[385]及達到大額申報門檻即必須申報的法規範。若未來對加密貨幣業者所制定之規範內容亦包括可疑態樣及達特定交易金額即須申報之規範，為以最小程度之干預達成最大程度之法令遵循，以監理科技之方式建置審計節點，並將所有欲偵測的態樣及申報門檻以程式化的方式編寫進節點之中，設定觸發一定情境時即自動通報法務部調查局，似為可供參考的洗錢防制方式。長遠而言，審計節點內更可更進一步加入讓電子計算機深度學習(Deep Learning, DL)可疑交易態樣的功能作為機器學習

[385] 法務部調查局（2018），〈疑似洗錢或資恐交易態樣簡稱對照表(含新舊態樣對照表)107/3/1 後適用〉。載於：https://www.mjib.gov.tw/userfiles/files/35-洗錢防制處/files/可疑交易申報專/check_list.pdf（最後瀏覽日：2018/07/11）

doi:10.6342/NTU201800740

(Machine Learning, ML)的基石，以促成研發具備自主判斷可疑交易態樣的人工智慧（Artificial Intelligence, AI）為最終目標[386]，在落實監理科技的同時亦降低洗錢防制及法令遵循的成本，最大程度上成就非審慎監理之目標。

[386] Michael Copeland, *The Difference Between AI, Machine Learning, and Deep Learning?*, NVIDIA (July 29, 2016), https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/.

doi:10.6342/NTU201800740

第二節　產業風險評估

我國風險評估報告經過分析共 31 個行業及部門的地域風險、客戶風險、產品及服務管道風險並且進行評級，就其中每個產業分別檢視其行業特性、產品及業務特性、客戶關係、地理範圍、服務管道等各項因子進行檢視[387]，最終繪表如下[388]：

表 十：產業及部門風險評估—洗錢威脅辨識結果一覽表

產業及部門弱點評等表			
低	中	高	非常高
1.期貨經理事業 Managed futures enterprises	1.信用合作社 Credit cooperatives	1.國際證券業務分公司 Offshore Securities Unit	1.國際金融業務分行 Offshore Banking Unit
2.信用卡公司 Credit card companies	2.證券投顧事業 Securities investment consulting enterprises	2.外國銀行在臺分行 Branches of foreign banks	2.本國銀行 Domestic banks
3.非人壽保險公司 Non-Life Insurance companies	3.地政士 Land administration agents	3.郵政機構 The postal institution	
4.外幣收兌處 Foreign exchange counters	4.證券金融事業 Securities finance enterprises	4.證券商 Securities firms	
5.證券集中保管事業 Centralized securities depository enterprises	5.融資性租賃事業 Financial Leasing enterprises	5.國際保險業務分公司 Offshore Insurance Unit	
	6.期貨商 Futures commission merchants	6.銀樓業 Jewelry retail businesses	
	7.保險代理人及經紀人公司 Insurance agents and brokers	7.會計師 Accountants	
	8.記帳士暨記帳及報稅代理人 Certified Public Bookkeepers, Bookkeeper and Tax Return Filing Agents	8.律師 Lawyers	
	9.電子支付機構 Electronic payment institutions	9.不動產經紀業 Real estate brokers	
	10.第三方支付服務業 Third-party payment enterprises	10.農業金融機構 Credit departments of agriculture and fishery associations, Agricultural Bank of Taiwan	
	11.票券金融公司 Bills finance companies	11.人壽保險公司 Life Insurance companies	
	12.公證人 Notaries	12.證券投信 Securities investment trust enterprises	
註：電子票證業雖未納入國家風險評估程序會議之評級範圍，惟已依洗錢防制法指定納入洗錢防制及打擊資恐體系			

[387] 行政院洗錢防制辦公室（2018），〈國家洗錢及資恐風險評估報告「金流透明 世界好評+」〉。載於：https://drive.google.com/open?id=1EaQgIeUG-M8eLkcfNbLqJho-SlRpMtD1（最後瀏覽日：2018/06/20）

[388] 同前註，頁 42。

doi:10.6342/NTU201800740

表格來源：行政院洗錢防制辦公室

觀察上表可知，被評估為非常高風險族群的兩類產業--本國銀行（Domestic Banking Unit, DBU）及國際金融業務分行（Offshore Banking Unit, OBU）[389]均具備能與法定貨幣直接往來的特點。至於其他被評定為高風險之產業，則基本上不具備能直接移轉資金的能力，專業人士如會計師、律師、地政士等之所以被評定為高風險產業，係因其所具備的高度專業知識與能力，故「能透過相關金融稅務、不動產實務及相關法規，以創設複雜的公司架構、安排營運或透過不實財務簽證或信託，或居間仲介，協助犯罪者隱匿或移轉不法所得」[390]。惟具有專業知識、或是本身專業即對洗錢犯罪具有高度吸引力，雖有助洗錢犯罪將結構複雜化，規避執法機關查緝，但終究還是需要面臨金錢及價值移轉的問題。蓋洗錢本質上就是一門牽涉到價值移轉、變更、掩飾、隱匿、收受持有他人不法所得的犯罪，價值再如何移轉，如欲移轉至國外，必須面臨異國貨幣匯兌的轉換；如欲在我國使用不法所得，則必須面臨洗錢最終階段—即價值上的「整合」。不管何者，均無法規避與法定貨幣有直接或間接的匯兌往來，所以一如產業風險評估所呈現的產業風險趨勢所示，與法定貨幣直接匯兌越相關的產業，其具有的洗錢威脅就越高，風險分數當然也會越高，反之亦然。

若按上述的脈絡，提供加密貨幣與法定貨幣間的匯兌產業、以及提供代幣作為價值移轉的產業，因直接涉及與法定貨幣或是價值交換的往來，應被歸類為「非常高風險」的產業加以列管。惟如此推論似嫌過於速斷，故本文參考行政院洗錢

[389] 參照金管會「金融業納入示範區問答集」，OBU 係指銀行依《國際金融業務條例》設立會計獨立之「國際金融業務分行」，以境外個人、境外法人及境內金融機構為主要客戶，提供外幣相關金融服務及商品。而 DBU 為指定辦理外匯業務銀行，以本國人、本國公司、在我國境內有住所之外國人及外國公司在我國之據點等為主要客戶，提供新臺幣及外幣之相關服務，故通常會以 DBU 泛指國內銀行及其分行，和主要辦理國際金融業務之 OBU 有所區別。

[390] 同前註，頁 25。

doi:10.6342/NTU201800740

防制辦公室就非常高風險產業所使用的評估標準，分析涉及金錢匯兌及價值交換的產業是否應被歸類為具高風險洗錢威脅的產業。

第一項 行業固有特性

行業固有特性代表的是該行業在國內經濟中具有的重要性，以及其結構和營運地點是否支持資金的迅速移轉，應綜合考量的因素包括：行業規模、行業業務結構之複雜度、與其他行業之整合程度以及行業的營運地點四要素[391]。欲將加密貨幣相關產業列入高風險產業，至少需分別達到上述四要素，亦即行業規模的交易量和資產規模均屬大額、行業結構複雜，且與其他行業整合良好，營運地點普遍存在於國內和國際上的程度。倘具備上述要素，該行業可被客戶廣泛地使用於移轉資金，呈現顯著的金錢及價值移轉能力(MVTS 通常都具備此種特性)，故風險評級應為「非常高」。

加密貨幣及代幣產業若涉及金錢匯兌及價值移轉，按上述要素，其產業規模及交易量須達到均屬大額的地步。目前因缺少台灣本土加密貨幣產業交易資料，尚難估計是否已達到大額的規模，惟透過全世界比特幣的總市值與世界首富之一比爾蓋茲的資產和世界黃金的總市值相比較，即發現比爾蓋茲一人所擁有的資產比加密貨幣多了一倍不止，黃金的總市值更是比特幣總市值的 200 倍以上[392]。從世界觀的角度觀看目前最具價值的加密貨幣—比特幣，尚難認為加密貨幣已達到具規模的交易量、或是達到能被認為是大額的程度。

再分析加密貨幣的結構複雜程度及是否允許與其他行業進行一定程度上的整合要素，本文認為就本項而言，加密貨幣已達到複雜的產業結構及具備高度與其

---

391 同前註，頁 82。

392 Raul, *The Bitcoin Economy, in Perspective*, HOWMUCH.NET (June 21, 2017), https://howmuch.net/articles/worlds-money-in-perspective.

doi:10.6342/NTU201800740

他行業整合的能力。惟加密貨幣雖具有上述潛在能力，在實際整合上卻尚難一蓋而論。因各國風土民情各不相同，對於加密貨幣之接受程度亦不盡相同，或許他國存有許多服務供應商及網路買賣願意接受以加密貨幣作為付款選項[393]，惟觀察我國實際上的加密貨幣交易環境，似難認為其已達到「整合良好」的程度。是以本文認為，加密貨幣之技術層面確實極為複雜，造成執法機關在追查金流上諸多不便，可認為其結構之複雜度、與其他產業相較已達「極其複雜」的程度，風險評級上應可評價為非常高風險。惟就加密貨幣與產業「整合良好」的程度，從目前加密貨幣於我國的發展觀之，似未達到符合非常高風險的要素，本文認為至多僅能評估為高風險，但較為妥適的風險評級應為中風險。

最後評估加密貨幣營運地點的普遍程度，所謂的營運地點概念，對加密貨幣基本上並不適用，因為加密貨幣運作於去中心化的架構上，營運地點遍及全球，有網路的地方就能使用存在於世界各地的節點驗證交易訊息，完成交易。以加密貨幣就科技面的普及率(Accessibility)來說，已經達到有網路的地方即能從事交易的地步；但在應用面可能還不如法定貨幣來得方便，蓋接受加密貨幣付款的商家相較現實貨幣還是遠遠不及，由此觀之，加密貨幣似缺乏整合程度。本文認為雖然加密貨幣的直接交易能力尚不及法定貨幣，但若其具備隨時兌換成法定貨幣的能力，仍可間接達成如同法定貨幣的便利性，利用加密貨幣進行支付的普及率即可能大增。

例如知名的訂票網站 Expedia 即與加密貨幣匯兌業者 Coinbase 合作，讓客戶能在購票時以匯兌業者的匯率支付相當於票券價值的加密貨幣，加密貨幣匯兌業

---

[393] Elise Moreau, *13 Major Retailers and Services That Accept Bitcoin*, LIFEWIRE (Aug. 6, 2018), https://www.lifewire.com/big-sites-that-accept-bitcoin-payments-3485965.

doi:10.6342/NTU201800740

者會再以自身制定的匯率,向票券公司支付相當於原票券銷售金額的現實貨幣[394]。票券公司在此種交易架構內，看似接受加密貨幣作為其販售票券之對價，但實際上並非如此，其僅是開放第三方(加密貨幣匯兌業者)介入，使客戶得以直接在訂票程序時以加密貨幣作為支付方式，經由匯兌業者的即時匯兌轉換為現實貨幣以作為支付票券之對價。加密貨幣匯兌業者有無限可能從事類似的代支付程序，其雖非向使用者提供直接性的加密貨幣/法定貨幣之間的匯兌業務，但於輔助交易履行的過程中，藉由自身匯兌轉換加密貨幣後再向提供服務/商品的第三方支付價金，不啻提供了加密貨幣近似於法定貨幣的支付能力，有鑒於此，雖加密貨幣匯兌業者目前於我國並未提供類似的服務，但未來該行業具有許多被客戶廣泛使用的特質，並具備顯著的資金移轉能力與支付能力，現在或許還不至於列為非常高風險的等級，僅能賦予其至多高風險之評級，但未來仍應視其於我國之發展狀況決定是否調整評價為非常高的風險等級。

第二項 行業提供之產品及服務性質

產品及服務性質的不同，關係到固有弱點的不同，所以在評估一個產業可能具有之風險時，應該探知被評估的產業所提供的產品或是服務是否與通常被評估為洗錢及資恐弱點之產品和服務相關聯。通常被評估具有洗錢及資恐弱點之產品和服務包括：具有現金支付和貨幣工具可能性的產品和服務、私人銀行、貿易融資服務、使用新興科技的產品和服務、包括電子資金轉帳在內之可跨境移轉資金的服務或商品、涉及高價值商品、以及其他尚在調查之商品及服務[395]。若要達到非常高風險的產業類別，須該產業提供大量易受利用的產品服務，且該服務構成

---

[394] *Bitcoin Terms & Conditions*, EXPEDIA, https://www.expedia.com/Checkout/BitcoinTermsAndConditions (last visited July 15, 2018).

[395] 行政院洗錢防制辦公室（2018），同前揭註 387，頁 84。

doi:10.6342/NTU201800740

該行業整體業務營運的顯著部分；除此之外尚須易受利用的產品服務的交易量、使用頻率是偏高，且很多一部分可能都是有涉(調查)案之案件。

目前蓬勃發展的加密貨幣產業，可對應至前文所述之「貨幣型加密貨幣」是基於區塊鏈 1.0 最基礎的應用。此類加密貨幣產業因所發行的加密貨幣功能上尚無法跨及除金錢及價值移轉以外之應用，故其產品及服務性質本質上係以提供價值移轉等較易被洗錢犯罪所利用的服務為主，且勢必構成產業營運的顯著部分。即使加密貨幣未來加入智能契約而演進至區塊鏈 2.0 之階段，仍難以避免主要產品服務與提供價值相關的交易脫鉤。因智能契約加入的是讓交易能按特定的條件履行特定的義務。至於履行之義務為何，仍無法避免是具有價值的服務或是資產，因為有價值之物或是所表徵的服務才最有需要且有被程式碼自動履行，達到避免由人經手的「去信任」實益。也因此，本文認為此類運用分散式帳本技術的新興科技在應用上估計會按產業對於「去信任」的需求而逐漸地被應用。金錢及價值移轉服務因涉及的不僅是高價值商品的移轉，其更涉及到如何在安全、保密、跨境、低成本的情形下完成服務。是以，加密貨幣產業在未來估計仍會有一段時間因其被運用至的服務，而被列為「易受(洗錢)利用」的產品和服務，在行業所提供之產品及服務性質上被列為「非常高風險」產業。惟若在更遙遠的未來，加密貨幣已發展至能基於區塊鏈 3.0 技術而被廣泛地應用至各個產業；屆時，也許僅「貨幣型」加密貨幣須被列為非常高風險至高風險產業的類別，其餘如「平台型」或「功能型」加密貨幣則能按屆時所提供的服務，再次進行產業的風險評估。

第三項 與客戶業務關係之性質

洗錢防制中的「防制」是為了防止潛在的風險客戶從事洗錢犯罪，若產業內的大多數客戶均由高風險客戶所組成，可合理推論潛在的風險因子會隨之遞增，

doi:10.6342/NTU201800740

產業所涉及的洗錢風險亦會隨之提升；因此客戶所從事的業務及相關資料(Clientele)的辨識及取得即顯得相當的重要。此項評等旨在瞭解與該行業客戶資料相關的固有弱點，考慮範圍包括：與客戶之間的業務性質，亦即辨識該產業內的客戶是否大多數會涉及交易，「直接、間接、持續性交易」及「交易關係」均屬之；客戶身分，亦即在瞭解客戶身分的同時，檢視客戶之身分是否屬重要政治性職務之人或是與其家庭成員有密切關係之人、是否屬國際制裁對象或已被列入黑名單、是否被列入負面新聞、及該客戶在產業中是否具一定的重要性，透過認識客戶程序進而判斷客戶群具有的風險屬性；客戶的職業及客戶所從事的業務，亦即從客戶群中辨識潛在易被洗錢/資恐犯罪所利用的活動族群，用來辨識弱點的因素包括高淨資產人士的比例、現金密集業務、實質受益人結構的複雜程度及辨識的難易度等等[396]。

將上述因素帶入加密貨幣匯兌產業逐一檢視，從與客戶之間的業務性質觀之，加密貨幣於區塊鏈 1.0 主要的應用即為價值移轉的交易，且既直接又間接；實體科技層面的移轉是極為直接且具有強制力的，此可歸功於分散式帳本具有的不可竄改性及共同記憶的機制，有學者將此特性稱之為「不可竄改之共同記憶」[397]。之所以又說「間接」是因為交易雙方所採行的區塊鏈交易架構，透過區塊鏈的加密程序進行義務上的履行，雙方無須提供任何個人資訊即可進行交易，因此對於採行公鏈型架構的加密貨幣，其化名式匿名促使交易雙方在不同空間下間接地達成原本只有面對面交易才能獲得的信任。如此吸引人的交易環境再加上原意即為提供匯兌業務的加密貨幣匯兌產業，合理推論產業內的客戶大多數均會涉及交易，

396 行政院洗錢防制辦公室（2018），同前揭註 387，頁 86。
397 臧正運（2017），同前揭註 384，頁 136-152。

doi:10.6342/NTU201800740

形成一個龐大的交易社群。當一個產業內部結構是由如此大量的交易群體結合而成時，交易被利用的程度隨即提升，形成易被洗錢犯罪所利用的高風險產業。

至於客戶身分與客戶的職業及客戶所從事的業務兩類，加密貨幣的產業評估上將面臨著如何辨識、取得及驗證客戶資料的困境。若無法取得上述兩類資料，即無法估算客戶群體內是否存在高風險客戶，當然也就無法評估產業所隱含的風險。本文認為加密貨幣匯兌產業因產業固有的業務特性，故大部分客戶間的業務應無法與「直接、間接、持續性交易」等交易脫鉤，業務關係上呈現高風險，又若無法達到正確辨識客戶身分、職業或行業別，亦無法客觀地將產業內所涉及的風險加以辨識。在欠缺足以識別風險的情況下，為確保國內金融秩序之安定，本文認似能採行「大膽假設、小心求證」的策略，暫時將產業以中高風險來對待，待觀察發現所涉及之客戶身分及所從事的業務活動較不易成為洗錢之弱點後再降低其風險，似屬較為保守的取向。

第四項 行業活動之地理範圍

考量行業所可能涉及的地理範圍，有助於縮小洗錢防制所關注的範圍，並就所涉及的範圍評估服務可能被利用的風險。舉例而言，行業活動的地理範圍也許會橫跨各個司法管轄區，當行業活動擴及至一些可能已被聯合國、美國財政部海外資產控制辦公室（Office of Foreign Assets Control, OFAC）、防制洗錢金融行動工作組織(FATF)、各區域性防制洗錢組織(FATF Style Regional Body, FSRBs)列為高風險司法管轄區時，主管機關即需提高注意。又如行業拓展的範圍牽涉到金融監理制度不健全的國家或是當地的金融活動非以銀行業為主流，鑒於位於此類高風險管轄區的行業較容易被洗錢犯罪所利用，故而應對涉及之行業採取較頻繁且持續

doi:10.6342/NTU201800740

監控措施，特別是當位於高風險地區的業務佔據了主要往來的業務比例時[398]。

加密貨幣匯兌行業可執行的交易約略可分成以加密貨幣兌換法定貨幣的「法幣交易」、加密貨幣兌換加密貨幣的「幣幣交易」以及場外平台交易(OTC 交易)。法幣交易在判定地域範圍上較為簡易且明確，由於牽涉到法定貨幣資金上的移轉，通常會由交易所位於兌換幣別的國家予以支付或是匯款。例如交易所同時於 A 國及 B 國設有交易據點，A 國通用貨幣為美金、B 國通用貨幣為新臺幣，若位於 C 國之 X 欲將交易所內的加密貨幣分別兌換美元現鈔以及以新臺幣形式匯款給 D 國之第三人，可能採取之方式之一即親自拜訪 A 國交易所的據點領取美金。惟若欲以匯款形式使第三人取得法定貨幣(本例為 C 國之 X 欲將 B 國之通用新臺幣以匯款形式匯給 D 國之第三人)，交易所及提領者至少須滿足各自角色兩項條件(交易所為 1、2，提領者為 3、4)中的一項條件；1.必須交易所於法定貨幣提領國設有據點(如 B 國)，並且該據點具有透過該國之金融機構或是貨幣移轉服務將貨幣移轉至他國的能力；2.交易所須於非法定貨幣發行之國家(如 D 國)，具有透過以買匯的方式取得外匯後再匯至予客戶或是客戶指定之第三人的能力；3.必須提領者於貨幣提領國(如 D 國)有開設金融機構之帳戶，亦即接收帳款的能力；4.必須提領者或是接收者於他國開設能接收外幣匯入之帳戶(如雖未於 D 國開設帳戶但於 E 國設有帳戶)，且須容許外匯解款後以相同幣別於外匯帳戶間進行移轉。

如此觀之，涉及法幣交易的加密貨幣行業因提供「出金」的服務，較易受出金據點之地域風險所影響。若出金地區之洗錢防制法規較不嚴謹，但位於執行洗錢防制法規較嚴謹之國家之加密貨幣匯兌行業卻同時於兩國間從事加密貨幣交易所之業務，依據業務種類的繁雜程度，很有可能會成為行業運作上的弱點，較易

[398] 行政院洗錢防制辦公室（2018），同前揭註 387，頁 87。

doi:10.6342/NTU201800740

被洗錢犯罪所利用。以我國目前法規為例，若將加密貨幣之性質定位為商品，客戶能先購買與法定貨幣同等價值的加密貨幣商品後，再將加密貨幣以「出售」之方式販售與交易所，由交易所位於其他地區之據點支付當地法定貨幣作為對價。此時即能有效規避《管理外匯條例》第 6-1 條關於新臺幣五十萬元以上之等值外匯收支或交易應申報之規定與《銀行法》第 29 條非銀行不得經營收受存款或辦理國內外匯兌業務之規定，蓋加密貨幣非法定貨幣，並不構成《銀行法》第 5 條之 1 之「收受存款」；再者，《管理外匯條例》第 2 條所稱之外匯係指外國貨幣、票據及有價證券，加密貨幣並不在管制範圍內，無法以同條例第 22 條「非法買賣外匯為常業者」進行管制，形成類似場外交易平台或是地下通匯的移轉機制。於上述交易架構下，判斷交易所是否提供能達到類似外匯移轉的功能，以及交易所的分支據點是否位於較低洗錢風險的地域，即能判斷該交易所之地域風險，若判斷入金及出金國家有一方係洗錢高風險國家，可能即須針對經常性從事與該國交易之客戶，進行加強客戶審查（EDD）瞭解其金流來源及去向，避免因業務活動涉及地域風險較高的國家連帶影響我國的風險評級。

第五項 服務管道之性質

服務管道（Delivery Channels）指的是服務提供者與客戶之間互動的方式，通常越直接的管道，所面臨的風險會越低[399]。以銀行開戶程序為例，於開通服務管道之時，客戶必須提供第一證明文件及第二證明文件，前項第一證明文件就自然人而言限於國民身分證，對法人而言則尚須提供主管機關登記證照或核准成立或備案之文件，暨負責人之身分證及確認實質受益人之身分(如持有 25%以上自然人

[399] 同前註，頁 88。

doi:10.6342/NTU201800740

股東/出資人及高階管理人等身分證明文件)[400]。除驗證身分證明文件外，尚須經過確認客戶身份程序，瞭解開戶動機與目的等事項，並評估開戶合理性，如為自然人開戶另須拍照留存影像檔。以上程序均是透過面對面程序完成，因為與客戶有著實際上的接觸，所以若於驗證身分證明文件時發現可疑或是開戶動機不單純，銀行行員能及時發覺，有助於弱化服務被用於洗錢犯罪的風險。

現行金融機構除須臨櫃開立之實體帳戶外，尚有所謂的「數位帳戶」[401]，所謂數位帳戶，是為推動「打造數位化金融環境 3.0」計畫，自 2015 年起開始推行的便民服務 [402]主要授權依據是《銀行受理客戶以網路方式開立數位存款帳戶作業範本》(下稱開立數位帳戶作業範本)。按立法的先後順序觀察，該存款帳戶作業範本 [403]應係參考《電子支付機構管理條例》第 15 條 4 項、第 24 條 3 項、第 25 條 3 項等法授權訂定之《電子支付機構使用者身份確認機制及交易限額管理辦法》(下稱支付機構限額管理辦法)[404]第 6 條細分之第一類、第二類、第三類電子支付帳戶之開戶作業程序，不同之處在於按數位帳戶作業範本所開立的數位存款帳戶並未如支付機構限額管理辦法明訂電子支付機構應按帳戶開立的類型而區分使用額度上的限制，而是以驗證程度來訂定可進行的交易權限。

按開立數位帳戶作業範本第 2 條，數位存款帳戶係指銀行以網路方式受理客

---

400 台灣銀行，〈如何開戶往來〉。載於：http://www.bot.com.tw/business/deposit/generaldeposit/pages/tb3114.aspx（最後瀏覽日：2018/06/14）

401 數位帳戶通常主打較高的存款利息，國內各大銀行均有類似帳戶：如華南銀行之 SnY、台新銀行之 Richart、國泰銀行之 KOKO、兆豐銀行之 Mega Lite 等是。

402 金融監督管理委員會（2015），〈未來民眾開立存款帳戶，可以直接透過網路線上申辦〉。載於：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0%2C2&mcustomize=news_view.jsp&dataserno=201510270006&aplistdn=ou&toolsflag=Y&dtable=News（最後瀏覽日：2018/06/26）

403 中華民國 104 年 10 月 27 日金融監督管理委員會金管銀法字第 10400243620 號 函訂定發布全文 12 條。

404 中華民國 104 年 4 月 27 日金融監督管理委員會金管銀票字第 10400077770 號 令訂定發布全文 23 條，並自 104 年 5 月 3 日施行。

doi:10.6342/NTU201800740

戶申請所開立之新臺幣及外匯活期存款帳戶。此類帳戶並不需要以面對面方式開戶，故於交易權限上有按身分驗證的完整度來進行區分。如第一類數位存款帳戶於完成存款帳戶作業範本第 4 條 1 項 1 款第 2 目所規定之「經第三方認證確保金鑰儲存安全之儲存私鑰之載具」(如自然人憑證)及第 3 目所規定之「建立客戶影像檔」前，按第 4 目規定，其帳戶限「適用於非電子轉帳交易指示類[405]，及電子轉帳交易指示類之低風險交易[406]且不得提高非約定轉入帳戶之轉帳限額」，惟一旦完

[405] 按中華民國 107 年 3 月 14 日金融監督管理委員會金管銀國字第 10702029320 號函洽悉修正發布之《金融機構辦理電子銀行業務安全控管作業基準》第 4 條 2 款非電子轉帳及交易指示類係指與資金轉移無關或不直接影響客戶權益之服務項目，其服務項目舉例如下：
註: 中華民國銀行商業同業公會全國聯合會用語中似因每條下僅有一項，故僅以(款)來接續(條)，並無(項)的使用。

非電子轉帳及交易指示類	服務項目
查詢	１、帳務類查詢： 存放款餘額查詢、交易明細查詢、額度查詢、歸戶查詢、託收票據查詢、匯入匯款查詢、信用狀查詢等交易。 ２、非帳務類查詢： 匯率查詢、利率查詢、共同基金查詢、金融法規查詢、股市行情查詢、投資理財資訊查詢、業務簡介查詢等交易。 ３、個人資料查詢
通知	入扣帳通知、存款不足通知、存放款到期通知、放款繳息通知、託收票據狀況通知、消費通知等交易。

[406] 按《金融機構辦理電子銀行業務安全控管作業基準》第 4 條第 1 款(二)：低風險性之交易係指該訊息執行結果對客戶權益無重大影響之各類電子轉帳及交易指示，內容包括下列各項：
１、 辦理上述申請指示類之服務。
２、 辦理 ATM 存提款之服務。
３、 依法令規定應為照會、認識客戶作業。
４、 辦理約定轉入帳戶之轉帳。
５、 辦理客戶直接向金融機構或間接透過金融資訊服務事業、票據交換所等平台，進行概括約定繳稅費及限定性繳款之扣款約定及扣款服務。
６、 設定約定轉入帳戶，惟設定非同一統一編號帳戶者須先
臨櫃申請後才能透過線上新增；其交易限額同１０之(２)要求，若配合採用各種嚴密之技術防護措施，提供客戶確認交易內容並能 防止或偵測交易內容被竄改，其限額可由個別金融機構 視其風險承擔之能力斟酌予以適當提高。
７、 同一統一編號帳戶間轉帳。
８、 貸款撥款至同一統一編號帳戶或學校之就學貸款指定帳戶。
９、 客戶非直接獲取金融機構之服務且需其人工確認客戶身分與指示內容之申請指示類。
１０、非約定轉入帳戶
(１)ATM、POS 等之低風險性交易，其限額應符合現行 ATM 作業及 POS 作業相關規定。

doi:10.6342/NTU201800740

成前兩目所稱之驗證後即可取得數位存款帳戶最完整的權限[407]。實務上通稱通過自然人驗證加視訊的新開戶客戶為 1A 客戶，若僅持自然人憑證開戶則稱為 1B 客戶[408]。

第二類數位存款帳戶是銀行受理於本行(即既有客戶)已開立存款帳戶之舊客戶採用連結本人之自行金融支付工具，依據安控基準之介面安全設計進行身分驗證所開立的數位帳戶[409]。所謂的「自行金融支付工具」可以是存款帳戶、信用卡或其他經主管機關認可之金融支付工具,但不包含未以臨櫃方式開立之存款帳戶；經此程序驗證後即可取得適用安控基準非電子轉帳交易指示類，及電子轉帳交易指示類之低風險交易權限。

第三類數位存款帳戶是銀行受理於他行(即他行客戶)已開立存款帳戶之舊客戶採用連結本人之金融支付工具，依據安控基準之介面安全設計進行身分驗證所開立的數位帳戶[410]。例如 A 銀行客戶利用 A 行發出的信用卡和金融卡至 B 銀行開設數位存款帳戶即為一例。因透過此類驗證方式所開設之數位帳戶是仰賴其他機構所驗證的金融支付工具來驗證客戶身分，故從開戶銀行角度觀之，此類帳戶的安全等級最低，賦予的帳戶使用權限亦僅限於「同一統一編號之安控基準非電子

---

(2)網際網路之低風險性交易，以每一帳戶每筆不超過等值新臺幣五萬元、每天累積不超過等值新臺幣十萬元、每月累積不超過等值新臺幣二十萬元為限。
(3)透過網站、行動 APP、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經金融機構人工確認客戶身分與指示內容者，其交易限額同(2)要求。
(4)配合採用各種嚴密之技術防護措施(如簡訊簡碼回傳)，提供客戶確認交易內容並能防止身分確認資料與交易內容被竄改者，其非約定轉入帳戶之轉帳限額，可由個別金融機構視其風險承擔之能力斟酌予以適當提高，最高不超過當日累計等值新臺幣二佰萬元為限;若經客戶事先申請且由金融機構人工與客戶確認其指定人員之身分與指示內容者(如電話照會)，其交易限額不在此限。
１１、個人資料異動。

[407] 適用《金融機構辦理電子銀行業務安全控管作業基準》非電子轉帳交易指示類，及電子轉帳交易指示類之高風險及低風險交易。
[408] 同前揭註 260。
[409] 《銀行受理客戶以網路方式開立數位存款帳戶作業範本》第 4 條 2 款
[410] 《銀行受理客戶以網路方式開立數位存款帳戶作業範本》第 4 條 3 款

doi:10.6342/NTU201800740

轉帳交易指示類及電子轉帳交易指示類之低風險交易」。所謂同一統一編號即是同一身分證字號，是以使用第三類數位存款帳戶之客戶只能做「自我交易」；即開戶後，只能幫「自己」做交易，例如轉帳至自己於他行開設之帳戶或是繳納稅賦、公共事業費用等，但就是不具備「匯兌」之功能。

有銀行即將上述三類帳戶按權限的大小區分成超級帳戶、進階帳戶、完整帳戶、基本帳戶並納入自身之數位存款帳戶特別約定條。繪表如下：

表 十一：數位存款帳戶類型所對應之驗證方式及交易權限[411]

帳戶類型	身分驗證	使用範圍
第一類(1-1 類) (超級帳戶)	採用經第三方認證確保金鑰儲存安全之憑證簽章進行身分驗證，並透過視訊等方式建立存戶影像檔。	適用金融機構辦理電子銀行業務安全控管作業基準(以下簡稱安控基準)非電子轉帳交易指示類，及電子轉帳交易指示類之高風險及低風險交易。
第一類(1-2 類) (進階帳戶)	採用憑證簽章進行身分驗證。	適用安控基準非電子轉帳交易指示類，及電子轉帳交易指示類之低風險交易且不得提高非約定轉入帳戶之轉帳限額。
第二類 (完整帳戶)	受理已開立存款帳戶之舊戶開立第二類帳戶，採用連結本人之自行金融支付工具(以存款帳戶、信用卡或其他經主管機關認定之金融支付工具為限，但不包含未以臨櫃方式開立之存款帳戶)進行身分驗證。	適用安控基準非電子轉帳交易指示類及電子轉帳交易指示類之低風險交易。
第三類 (基本帳戶)	採用連結本人之金融支付工具(以存款帳戶、信用卡(須持有逾 180 天(含)以上)或其他經主管機關認定之金融支付工具為限，但不包含未以臨櫃方式開立之	適用安控基準非電子轉帳交易指示類及電子轉帳交易指示類之低風險交易，惟排除非同一統一編號之約定及非約定轉入帳戶之帳務交易。

411 國泰世華（2017），〈數位存款帳戶帳戶類型--國泰世華商業銀行數位存款帳戶特別約定條款〉。載於：https://www.kokobank.com/KOKO/Content/HTML/dsa_term.html（最後瀏覽日：2018/06/27）

doi:10.6342/NTU201800740

	存款帳戶)或透過存款帳戶(須含統一編號)進行身分驗證。	

表格來源：國泰世華商業銀行數位存款帳戶特別約定條款

前述三類帳戶類型之區別實益雖係按服務管道之性質作出區別待遇，惟最核心的理念仍是按確認客戶身分的強度來評估客戶所具有的風險。客戶所能提供的資訊越是完整、越容易受到驗證，對開戶銀行而言越容易對客戶採行相對應的風險措施。認識客戶(KYC)在此之中所扮演的角色即不言可喻，蓋對於新客戶—尤其是以非面對面管道而接受開戶之新客戶，在執行第一階段的客戶識別計畫(CIP)時僅能以科技的方式協助辨識客戶的基本資訊，為確保客戶提供的資訊的正確性，開立數位帳戶作業範本第 3 條 2 款及 3 款即規定除取得身分基本資料及國民身分證正反面影像檔及具辨識力之第二身分證明文件影像檔外，尚須向經認證第三方機構驗證所取得的資訊是否屬實,因此第三方資訊是否足以信賴及是否能被驗證，即成為開戶銀行關注之重點。對此，開立數位帳戶作業範本第 3 條 4 款規定銀行受理開立帳戶時應查詢財團法人金融聯合徵信中心「Z21 國民身分證領補換資料查詢驗證」、「Z22 通報案件紀錄及補充註記資訊」、查詢並確認客戶之「受監護或輔助宣告」狀態並留存電子申請紀錄以供備查[412]。

金融機構成功取得並驗證客戶資訊後始得就所提供的產品、地域、交易型態

412 《銀行受理客戶以網路方式開立數位存款帳戶作業範本》雖未提及外籍人士提供居留證資料者能否開設數位存款帳戶，但參考《電子支付機構使用者身分確認機制及交易限額管理辦法》第 8 條內容，我國國民開立第一類電子支付帳戶須確認使用者提供之行動電話號碼及國民身分證，於驗證國民身分證並應向內政部或財團法人金融聯合徵信中心查證資料之真實性;提供居留證資料者，應向內政部查詢資料之真實性以觀。若未有法規禁止外籍人士開設數位存款帳戶，對於欲用居留證資料開戶者，理應向內政部查詢資料以驗證客戶資料的真實性。但就實務運作觀之，目前銀行的做法似直接將數位存款的存戶限縮至「具有本國國籍之成年自然人」(如國泰之 KOKO 的數位存款帳戶特別約定條款)，禁止非本國籍人士開立數位存款帳戶。類似作法可以理解，蓋非本國籍的人士較難向經認證之第三方驗證資訊，風險亦較難評估，禁止其透過非面對面方式開戶尚合乎以風險為基礎的開戶方式。

doi:10.6342/NTU201800740

等風險因子進行評估，導入客戶風險評等模型(CRR)計算客戶風險等級[413]，再依「風險評估」的結果，執行不同強度的「客戶盡職調查」(CDD)程序，例如高風險客戶應進行高強度盡職調查（Enhanced Due Diligence, EDD），並應取得管理階層主管之核准，方得開戶或交易；一般風險客戶進行中強度盡職調查（Normal Due Diligence, NDD）；而低風險客戶則進行低強度盡職調查（Simplified Due Diligence, SDD）即可[414]。

從上述實例可知，隨著驗證強度的增加，越有可能得知使用者的真實身份，賦予的權限也會隨之增加。此類以驗證身分的完整度來區分使用者的權限亦是以風險為基礎方法的具體實現。以數位帳戶為例，因其單月交易限額與可提領的金額上限均受有限制[415]，故開戶程序較傳統帳戶來得簡便。此類數位帳戶於進行客戶識別計畫(CIP)時透過系統自動導入風險評等模型(CRR)以資料的可驗證性與完整程度計算客戶風險等級，提供之資料完整程度與風險程度呈反比。如前述舉例，第一類數位帳戶因透過拍攝真人照片及經第三方驗證的個人資訊(自然人憑證)，是以不明確性較低，風險平等較低。但如第三類數位帳戶因欠缺可供銀行驗證的直接資訊，故風險評級為「高風險」，在未能完成高強度盡職調查(EDD)前僅能於同一統一編號之約定及非約定轉入帳戶進行適用安控基準之非電子轉帳交易指示類及電子轉帳交易指示類之低風險交易。

同理，本文認為加密貨幣於評估服務管道之性質時可效法如數位存款帳戶之

---

413 張兆順，劉書甯採訪、撰文（2017），〈國銀談法遵經驗--因應美國監理重點兆豐啟動法遵再造工程〉，《台灣銀行家》，93 期，頁 12。

414 中時電子報（2015/01/15），〈勤業眾信法務專欄－國際洗錢防制管理制度新思維〉，http://www.chinatimes.com/newspapers/20150115000172-260205（最後瀏覽日：2018/06/30）

415 如按《國泰世華商業銀行數位存款帳戶特別約定條款(106.8)》第一類(1-1 類)帳戶，統一編號歸戶限額為單筆 10 萬/單日 10 萬/單月 20 萬。存戶可自訂限額為單筆 1~50 萬/單日 1~50 萬/單月 1~100 萬。

doi:10.6342/NTU201800740

例，按行業就數位開戶所採行的資料蒐集及可驗證性進行評估，給予要求客戶須經被認證之第三方驗證的業者「低風險」的風險評級；給予要求客戶須使用第三方佐證資訊驗證的業者「中風險」的風險評級；給予僅要求客戶使用自身所提供之資訊即能開戶的業者「高風險」的風險評級。

惟上述方確認客戶及驗證客戶措施若僅由行業集體組成之自律組織(SRO)執行的話，在無法接觸到實體身分證明文件的情形下，實無法有效驗證客戶資訊之真偽，是以產業除須致力於降低服務管道間的匿名性外，尚須國家機關的介入，幫助驗證往來客戶之身分，本文於前文論及就國家如何降低國家風險時已有提及。

另外以上所預估之風險評級，僅是初始進行客戶識別計畫時給予之評級，後續若有發現客戶屬於重要政治性人物或是被列入負面新聞名單，則系統自動導入之風險評等模型(CRR)應將該客戶之風險等級調升。最後本文認為除上所述之低、中、高三級以外，應給予未能按客戶所提供之資訊完整度及可驗證性而調整客戶所能使用的服務權限之業者「非常高風險」的風險評級。理由在於加密貨幣服務提供業者原可採行上述以風險為基礎的客戶分類方式以辨識客戶身分的完整度，降低因服務性質及交易客體之匿名性所造成的行業固有風險等風險，但卻捨而不為，故有非常高的風險被洗錢犯罪所利用。

第三節　風險之控制及應對

經過上述分析，包括行業固有特性、行業產品及服務性質、行業活動之地理範圍及服務管道之性質後，加密貨幣行業似可暫時被認定具有非常高被利用的風險：其中行業與客戶關係之性質因無相關參考數據，似可暫列為具有中高度被利用的風險。

doi:10.6342/NTU201800740

惟不管風險等級如何，會影響者主要是規範方向與應對措施上的不同，不應因行業本身的固有特性而制定全面性的打壓策略，封殺具有如此多元發展可能性的產業。誠如 FATF 虛擬貨幣風險基礎方法指引第 28 條所述，當各國完成風險評估後，各國仍有自由決定如何管制可轉換的虛擬貨幣與法定貨幣之間的兌換平台（亦即本文所述的加密貨幣匯兌業者、VCPPS）蓋國家作為擁有獨立主權之國際法人 [416]，可能因各自的國家法規環境或是策略目標的不同（如：消費者保護、安全性與健全性、貨幣政策等）而選擇應對 VCPPS 採取相對應的洗錢防制政策。但是於考慮應採取何種洗錢防制措施時應將該措施可能遭成當地和全球洗錢、資恐風險等級之衝擊納入考量因素。如一概禁止 VCPPS 之活動，可能有一定機率迫使原先進行之交易活動地下化，讓這些被迫地下化之活動因欠缺防制洗錢、打擊資恐的相關監督與管控措施，更容易被洗錢犯罪所利用。

本文贊同 FATF 之建議。由於區塊鏈目前最為成熟的應用比特幣，自 2008 年迄今為止，包含我國在內，已有多數使用者持有並且投資相當金額於加密貨幣產業，根據 Bitcoinity.org 提供的交易訊息的統計，比特幣在 2016 年 11 月的交易量創下新高紀錄，總共交易了 1.747 億枚比特幣，至 11 月為止交易總額達更高達 1,370 億美元即體現了加密貨幣增長的趨勢 [417]，迄今雖未有超過當年的交易量，但就市場資本(Market Capitalization)言已達約 1094 億美元 [418]。若我國有計畫將加密貨幣納入洗錢防制法之管制，行業面上似可先考慮以影響社會層面最大、最廣的公鏈

---

[416] 《國家權利義務宣言草案》第一條規定：「各國有獨立權，因而有權自由行使一切合法權力，包括其政體之選擇，不接受其他任何國家之命令。」

[417] 聯合新聞網（2016/12/29），〈石油爭霸底定 「新貨幣戰」開打！〉， https://fund.udn.com/fund/story/7488/2198963（最後瀏覽日：2018/06/30）

[418] 以 6,414.03 BTC/USD 乘上 17.1M Bitcoins 會有約 109,476,830,708 USD 的市場資本；*Bitcoin Trading Volume*, BITCOINITY.ORG, https://data.bitcoinity.org/markets/volume/5y?c=e (last visited June 30, 2018).

doi:10.6342/NTU201800740

型加密貨幣匯兌行業擬定規範計畫，其次為首次代幣發行(ICO)所發行的支付型代幣及資產型代幣。以下將以二起國內比特幣案例為例，試圖分析加密貨幣被洗錢犯罪利用之方式，尋找公鏈交易架構中最適合規範並且有效降低洗錢風險之環節。

第一項 公鏈型加密貨幣匯兌行業之風險

案例一

比特幣交易所假藉駭客入侵，詐騙客戶比特幣案：

「○○比特股份有限公司」董事長何○○涉嫌於 104 年 1 月間掏空公司資產及詐騙客戶比特幣，臺灣臺中地方法院檢察署（光股）廖檢察官梅君指揮刑事警察局電信偵查大隊與臺中市政府警察局第二分局組成專案小組進行偵辦，調查中發現犯嫌何○○擔任比特幣交易平臺「○○比特股份有限公司」董事長，該公司主要業務是在網路上媒合比特幣買賣，曾經是國內前三大比特幣交易所，103 年期間何嫌因積欠地下錢莊債務，急需大量資金週轉，所以對外謊稱該公司有 VIP 客戶高價收購比特幣，實際上卻是私下調高公司比特幣收購價格，吸引民眾至其他比特幣交易平臺購買比特幣至該公司變賣，民眾為賺取價差大量「搬磚」，但實際上卻是他本人私下變更該公司電腦伺服器後臺設定，將公司及客戶比特幣打入自己私人比特幣錢包，再對外宣稱該公司比特幣遭駭客入侵，致使公司蒙受鉅額損失結束營業，被害人及股東求助無門，向地檢署提出告訴[419]。

案例二

偵破陳○○為首之比特幣洗錢中心案

本案調查犯嫌陳○○原為「偽造銀聯卡提領集團」旗下車手之一，後轉型擔任洗錢機房主謀，並自行上網學習比特幣相關知識，後續招募共犯游○○、潘○○及蔣○○等 3 人共同成立比特幣洗錢中心，專門協助電信詐騙集團贓款洗錢，以避免遭到銀行凍結，近期更發現該機房製作教學指南準備擴大營運而招募時，取得先機順利破獲。由於比特幣係屬新興虛擬貨幣，犯嫌採取虛實混合的複雜洗錢模式，以網路銀行 U 盾結合比特幣帳戶交易，透過偽造大陸身分證及人頭配合視訊演出來騙過大陸比特幣交易平臺實名身分認證機制，避免日後身分遭到追查，由於所使用的金流超過 5 層洗錢，不僅能防止帳戶贓款遭到凍結風險，更順利將款項轉匯回銀聯卡然後交由車手提領；因此該集團從 105 年 4 月迄今，已經成功轉帳超過上百

[419] 內政部警政署 (2016/05/16)，〈比特幣交易所假藉駭客入侵，詐騙客戶比特幣案〉載於：https://www.ruifang.police.ntpc.gov.tw/cp-2366-24183-25.html（最後瀏覽日：2018/05/15）

doi:10.6342/NTU201800740

萬人民幣，全案經本局電信偵查大隊事前完整蒐證及犯罪現場電腦、手機端數位鑑識，終於突破嫌犯心防坦承犯罪，並查扣犯罪工具及比特幣帳號，有效遏止詐騙集團持續洗錢犯罪，避免更多人受害。[420]

圖片來源：蘋果日報[421]

圖 十一：比特幣洗錢中心犯罪流程圖

雖案例一及案例二犯罪情狀不盡相同，但分別可得知，現下比特幣已逐漸成為網路世界的新興產物，故已有不法份子利用國內尚無政府單位及相對應之洗錢防制機制，使用加密貨幣為犯罪工具，獲取不法所得。目前公鏈型加密貨幣最易被利用之方向即吸金犯罪和洗錢犯罪，分別為案例一及案例二所呈現。案例一雖難謂構成洗錢犯罪，惟涉及之 VCPPS 與案例二相同均屬洗錢防制之重點，又因詐騙手法係先以吸收加密貨幣為主，再以「假被駭」、「真侵占」之手法易持有為所

[420] 內政部警政署 (2016/05/11)，〈偵破陳○○為首之比特幣洗錢中心案〉。載於：http://www.hlpb.gov.tw/circulatedview.php?menu=2428&typeid=2453&circulated_id=60364（最後瀏覽日：2018/05/15）

[421] 蘋果日報（2016/05/04），〈詐騙集團車手 利用比特幣洗錢〉，http://www.appledaily.com.tw/realtimenews/article/new/20160504/852962/（最後瀏覽日：2017/01/15）

doi:10.6342/NTU201800740

有，於涉犯洗錢犯罪的前置犯罪時即已預先完成「處置」不法所得的階段，讓後續「多層化」的洗錢階段能輕易地被實施。類似透過加密貨幣所犯之前置犯罪，不僅難以查緝，更難於成功查緝後以刑法或洗錢防制法之沒收章節將犯罪所得與以沒收。因為如前所述，加密貨幣並非實體財產，其本質上還是存在於分散式帳本內的一筆電磁紀錄，任何擁有私鑰之人均有權更改自有「錢包」(即地址)內之紀錄。此紀錄因竄改難度及成本極高，一經移轉且經各節點驗證後，加密貨幣之所有權即隨之移轉，是以欲「沒收」經處置成為加密貨幣之不法所得，須搶先於持有人移轉加密貨幣以前，或是於移轉後獲取被移轉地址之私鑰，才算是真正地將犯罪所得沒收。如案例二中，警方因達成即時性的逮捕並且查扣犯罪工具及比特幣帳號，僅須犯嫌願意供出密碼，即能有效沒收不法所得。惟若犯嫌不願意供出能存取加密貨幣於區塊鏈上之私鑰，法院即便欲沒收比特幣亦無從執行。

案例二為使用加密貨幣之匿名性而從事洗錢犯罪之態樣。上圖之第一層至第二層為「處置」不法所得的階段、第二層至第四層為洗錢「多層化」的階段、第四層至第五層為「整合」的階段。本案之所以能順利偵破，係循現金軌跡，順著車手等人之蹤跡而破獲此洗錢集團，並非基於第一層至第五層的洗錢階段偵測異常而開啟之偵查，主要原因在於加密貨幣本身移轉上的化名式匿名及實體貨幣金流與加密貨幣金流互不干涉之故。就加密貨幣之隱匿性質而言，案例二之洗錢中心首先是使用法定貨幣購買加密貨幣，成功購買後再將加密貨幣從交易所內的地址移轉至自有之地址。

之所以須於第二層後再進行第三層之移轉作業有兩種主要原因：其一，完成購買後之加密貨幣雖帳面上屬於買受人所有，但是實際上買受人看到的僅是交易所系統上顯示的「IOU」信息，表示著買受人對於出賣人隨時得主張給付之加密貨

doi:10.6342/NTU201800740

幣。買受人實際得到所購買之交易貨幣的時點，其實是向交易所要求移轉帳戶內之加密貨幣至自有之錢包之時。蓋於交易所開立之錢包地址，該地址之私鑰並不歸屬於帳戶所有人，交易所保有能動用加密貨幣之私鑰，所以當執法機關函文要求凍結某一筆帳戶之貨幣時，能輕易地被實現。此亦係為何當交易所被駭時，所有客戶存放於交易所之加密貨幣會連同被盜之原因。所以為了確保正在進行洗錢的不法所得不會被輕易凍結，利用加密貨幣之洗錢犯罪通常會於購買後盡速移轉加密貨幣至冷錢包[422]，或是由自己控制私鑰之錢包。另一層原因在於透過全新的錢包地址達成去識別化的效果。公鏈型加密貨幣雖然本身即具有化名式匿名的功能，惟如案例二之第二層所示，買受人若進行的是「法幣交易」，須以實體帳戶(人頭帳戶)進行入金的動作，尚無法保證日後追查金流來源時不會順藤摸瓜找到犯罪集團。因此，將加密貨幣移轉至其他地址或是分流至無數個不同之地址，再行交錯複雜之移轉，很容易混淆金流來源，造成追查金流上之困難—此是尚能於公有鏈上查詢金流移轉情形的比特幣。

近來經改良並且加強隱私性之加密貨幣，如門羅幣(Monero，縮寫：XMR)及Zcash，更是因其特有之屬性而受到洗錢犯罪者的喜愛[423]。以門羅幣為例：該款加密貨幣會在區塊鏈上加密收件人的位址，並創造一個假的寄件人位址加以混淆。是以不僅無從得知加密貨幣持有人之真實身分，更無從追查資金來源。再以門羅幣主要的競爭對手 Zcash 為例，該款加密貨幣同樣採行公鏈型區塊鏈技術，同樣注

---

422 鑒於使用者於加密貨幣交易所開設之帳戶並不保有私鑰，或是交易所可能存在各種漏洞及被駭的風險，有廠商遂將加密貨幣地址等訊息燒綠於一個離線裝置，並讓使用者自訂能存取私鑰之方式，使得使用者欲移轉加密貨幣時必須透過該離線裝置始得順利完成交易。此種借用硬體設備達成加密貨幣之私鑰（密碼）和網際網路保持分離的硬體錢包又被稱為「冷錢包」。

423 Olga Kharif, *The Criminal Underworld Is Dropping Bitcoin for Another Currency*, BLOOMBERG.COM (Jan. 3, 2018, 4:20 AM), https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

doi:10.6342/NTU201800740

重使用者之隱私。相較比特幣有辦法得知發送者及接收者之地址，Zcash 會將真的位址加密，讓真實位址更難找出來。不過據報導，普林斯頓大學的研究人員最近在開發一款工具，可一定程度上分析 Zcash，不過對於門羅幣還未能有有效破解地址加密以追蹤貨幣來源之方法。Coinfirm—一家專門就區塊鏈提供洗錢諮詢及法律諮詢的公司的執行長就表示，新型的加密貨幣所表露之技術太過於強大，以致於幾乎所有兌換成門羅幣或是由門羅幣兌換出來的其他資產，都被標記為具高違法風險。相較之下，比特幣被標示為具高違法風險的比例只有 10%，蓋「過度匿名的資金來源所呈現的風險屬性就越高，因為你如何證明這些資金的來源並非非法的？」。[424]利用新型加密貨幣或是比特幣，層層轉址後，最後再匯入如案例二內第四層的交易所錢包內，以販售予交易所之方式兌換回法定貨幣，此時已難以追查金流來源。可見要從加密貨幣的金流上查緝疑似洗錢之態樣實屬不易。

為有效杜絕上述兩類洗錢態樣，最為關鍵的部分還是如何始能有效地讓使用加密貨幣匯兌服務之使用者心甘情願地揭露自身資訊。誠如上述，具高匿名度的加密貨幣，追查金流尚屬不易，若再無從得知交易者或是被交易者之身份資訊，洗錢防制將無從做起。是以理想上若行業內之客戶均樂意以較為繁雜之方式進行驗證，則行業內涉及加密貨幣匯兌部分之業務的匿名性就會降低，一旦匿名性降低，追查金流的複雜程度亦會隨之降低，將會有助於主管機關追查可疑之金流及金流背後之人。此匿名人的追蹤難易度才是決定服務管道風險屬性的關鍵。

第二項 規範公鏈型加密貨幣交易之主體—以交換者為中心

交換者為虛擬貨幣支付產品與服務(VCPPS)底下的一個子類別，是除了發行者

---

[424] 科技新報（2018/01/05），〈罪犯不再熱愛比特幣，門羅幣成新寵〉，https://technews.tw/2018/01/05/criminal-drop-bitcoin-to-monero/（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

以外最需被注意的服務提供者。因發行者(Administrator)通常存在於私鏈型的加密貨幣架構內，故於討論公鏈型加密貨幣時暫時先以交換者為主要討論對象。

按美國法，交換者是以商業為目的從事虛擬貨幣與真實貨幣之交換(即法幣交易)或與其他虛擬貨幣交換(即幣幣交易)之人或是法人[425]，FATF 則將此種行業稱為「於金融體系門徑的交叉點提供可轉換的虛擬貨幣兌換方」[426]。兩者均是在表述進行價值轉換之行業，並且均從規範此行業為出發點，期待達成加密貨幣洗錢防制之目標。觀察目前網路上提供「加密貨幣匯兌服務」之交換者，約略可以分成代客戶媒合的場外交易平台(OTC)、制定買賣匯率向客戶購買及販售虛擬貨幣的虛擬貨幣經紀業者以及虛擬貨幣交易所三種[427]，風險程度及規範難度各不相同。考慮到此後所論及之交換者或許不僅提供加密貨幣之匯兌服務，故以下分述之交易所涉及之交易標的將以虛擬貨幣稱之。

第一款 場外交易平台

場外交易(Over the Counter Trading, OTC 又稱 Direct Trading)平台，以類似民法第 565 條所規定之「報告居間」型式運作。平台受賣方委託，為其尋找可與其訂約之他方相對人，以提供訂約之機會，如因其報告而訂約成功者，報告之居間商即得請求報酬。惟 OTC 平台通常還會加進履約保證的機制，以提高相對人的保障，已逸脫傳統居間契約僅介紹買賣雙方促成交易的態樣，形成了一種新型的混合契約。

場外交易的運作方式與虛擬貨幣交易所最大的不同，在於信用基礎、價格形

---

425 FIN. CRIMES ENF'T NETWORK, *supra* note 275, at 3.
426 FIN. ACTION TASK FORCE, *supra* note 247, at 4.
427 Nelson Wells et al., *Best Cryptocurrency Exchanges: The Ultimate Guide*, BLOCKGEEKS, https://blockgeeks.com/guides/best-cryptocurrency-exchanges/ (last visited July 11, 2018).

doi:10.6342/NTU201800740

成的機制以及清算方式。此種交易平台類似於拍賣網站或是 Facebook 上的拍賣社團，主要目的是提供一個讓買受人和出賣人能自己尋找交易對象、並且私下相約交易的環境。此種平台最吸引人之處在於能最大程度的保有匿名性，因為平台不會主動要求交易雙方提供個人資料，亦不會蒐集個人的訊息，所以若是使用此平台進行虛擬貨幣洗錢的交易，將能最大程度地降低被查緝的風險。但有利就有弊，因為平台在交易的過程中扮演著協調者的角色，所以要促成一筆交易需要雙方強烈的信任為基礎。

第一目　信用基礎

以 LocalBitcoins.com 為例，該網站為一提供比特幣場外交易的平台，交易者僅需提供用戶名稱、電子郵件、密碼，即能迅速成為一個場外交易平台的交易者[428]，交易者隨後即可以 1%交易額當成是成交手續費開始進行交易，不受任何限制[429]。至於是否與一個完全匿名的交易者交易，則完全取決於雙方對於交易所需之信任。對此，平台開放交易者制定個人的交易條款，交易者可以制定需要進行身分認證或是存摺圖檔才能進行交易的條款，若無法接受該交易者的條款，則可以自由選擇不與該交易者進行交易[430]。

在如此自由開放的市場中，若是要求交易者進行 KYC 的賬號驗證，將會降低欲交易之一方被選擇的機會，因為還是有許多擁有良好交易評價的買家/賣家提供更簡便的交易手續。在此環境下，反而會形成以交易量、評價、交易速度、註冊時間長短來判定是否為良好的交易對象，而不是一張透過掃描上傳的證件照來判

[428] *How to Sell Bitcoins?* LOCALBITCOINS.COM, https://localbitcoins.com/guides/how-to-sell-bitcoins (last visited July 11, 2018).
[429] *LocalBitcoins Fees?* LOCALBITCOINS.COM, https://localbitcoins.com/fees (last visited July 11, 2018).
[430] *How to Buy Bitcoins?* LOCALBITCOINS.COM, https://localbitcoins.com/guides/how-to-buy-bitcoins (last visited July 11, 2018).

doi:10.6342/NTU201800740

斷。退步言之，若有用戶係以強烈的信任基礎為交易前提的話，也不會選擇此種交易平台進行交易。蓋虛擬貨幣交易所及虛擬貨幣經紀業者完全能提供更良好的信任基礎，但卻會收取較高的手續費，如何取捨完全視用戶的需求而定。

綜上所述，場外交易平台主要係以匿名、簡便、低手續費，來吸引願意由交易雙方自行承擔信用風險的用戶。於此環境，交易雙方均需建立雙邊授信後才可進行交易；相較而言，採行場內交易機制的交易所及經紀業者，則係以交易雙方對交易所的信任為基礎，以較高的交易價格來換取由交易所承擔匿名交易者可能產生的信用風險。

第二目　價格形成的機制

場外交易平台顧名思義，就是因為交易雙方保有撮合的自由，無須透過一套既定的交易程序來購買虛擬貨幣。場外交易的價格係基於買賣雙方的雙邊詢價形成；場內交易則基於程式設計和演算法撮合而成。

以 LocalBitcoins.com 為例，該網站呈現交易的方式趨於廣告，讓刊登者自由選擇交易地區、時間、匯率、條件、收款方式等選項。之後網站會將刊登者所制定的條件分類、整理、排序，以利交易者按自己的喜好選擇，若是有不滿意之處還可以直接聯繫刊登者，透過談判的方式取得一個共同可接受的交易方案[431]。如此多元化且難受監管的成交機制，也是吸引眾多交易者選擇場外交易的原因。

第三目　清算方式不同

場外交易與場內交易不同的另一因素為交易的清算方式。交易平台除提供最簡便的保障外，買賣雙方須自行安排資金和虛擬代幣的清算。其清算方式係由買

[431] *Setting Up Advertisements to Buy and Sell Bitcoins*, LOCALBITCOINS.COM, https://localbitcoins.com/guides/how-to-sell-bitcoins-online (last visited June 30, 2018).

doi:10.6342/NTU201800740

受人先向出賣人發起交易，於交易成立後，交易平台會從出賣人的帳戶餘額中，先扣除相對應的金額作為履約保證，一直到買受人透過約定的方式支付出賣人現實貨幣並由出賣人確認無誤後，才會將該筆虛擬貨幣放行[432]。在此清算機制中，買受人能在一定程度內降低出賣人不履約的信用風險。但是交易平台畢竟未經手現實貨幣，所以在處理糾紛時，僅能依買受人所提供的證據來判定一方是否履約，徒增交易的不便利性。

場外交易最常發生的糾紛不外乎下列狀況[433]：

1. 買受人透過轉帳方式付款，要求出賣人放行履約保證帳戶的虛擬貨幣，出賣人查詢後發現表面帳戶有金額入帳，故予放行，履行後才發現實際款項未到。
2. 買受人未透過轉帳方式付款，但是提供假冒的交易紀錄，要求出賣人放行履約保證帳戶的虛擬貨幣。
3. 買受人透過轉帳方式付款，要求出賣人放行履約保證帳戶的虛擬貨幣，出賣人以銀行帳戶被銀行帳戶被凍結為由拒絕履約。

場外交易平台在上述三種情形發生時，均無法有效地確認事實真偽，因為沒有一個獨立的清算機制可供參考或是執行。在 1 和 2 的情形中，出賣人都是因「並未實際收到款項但卻已經履約」而蒙受損害，交易平台對此除了關閉詐騙帳戶外，無法追回已經轉出的虛擬貨幣。第 3 種情形更是撲朔迷離，難辨真偽，蓋交易平台並非金融機構，無法判斷究竟買受人是否利用非法戶頭轉帳導致出賣人的戶頭連帶被凍結，抑或是金融主管機關查覺到出賣人的戶頭交易量異常而與以凍結。場外交易因為上述優缺點，促使了他種採取場內交易平台進行集中清算的交換業

---

[432] *Id.*

[433] 此三類型為筆者搜尋 https://localbitcoins.com/forums/#!/?fraud 觀察該場外交易平台時常出現有買/賣家被詐騙而張貼的資訊所歸納而成。

doi:10.6342/NTU201800740

者。

第二款 加密貨幣經紀業者

加密貨幣經紀業者(Exchange Brokers)旨在提供交易者一個風險較低的交易環境。平台業者自身作為交易主體，理論上將能全權領導交易的進行，即時地處理訂單，給予交易者更多的信賴與保障。此類交易業者外觀上收取交易相對人之現實貨幣後再以一定之匯率將現實貨幣轉換為加密貨幣後返還予交易相對人，模式類似民法第 576 條之行紀，蓋經紀業者「以自己之名義，為他人(加密貨幣交易相對人)之計算，為動產之買賣或其他商業上之交易，而受報酬(匯差)之營業」。但本文觀察此類加密貨幣交易態樣，似較接近民法第 345 條之買賣契約，原因在於此類經紀業者本身為買賣交易之一方的同時亦扮演著交易平台的角色。換句話說，此類業者因未以自己之名義為他人計算，而是以自動化設備訂定加密貨幣的出售與收購價格，並以高出市場匯率的價格賺取利潤。若如此解釋，交易雙方於進行匯兌行為時，會是先由發起交易之當事人(所服務之客戶)約定由其移轉加密貨幣或是現實貨幣予經紀業者；而作為買賣對價，再由經紀業者支付相當之現實貨幣或是加密貨幣予交易當事人，綜合觀察此契約性質似較趨近於買賣契約。

此類交換者通常是公司法人，擁有網站、匯率、註冊機制、客戶服務及申訴管道等等，其因做為公開且固定的交易相對人，為保護其名譽，與其交易會出現違約不履行的風險較低。若以本國之經紀業者 Bito EX 及 MaiCoin 為例，其除了具備上述優點外，尚提供了 24 小時匯兌服務、以簡便親民的方式(如超商)購買加密貨幣等附加服務。

當然在降低交易者所需承擔的風險同時，交易成本也會隨之升高。例如經紀業者通常會訂定高於市場的賣價，或是低於一般市售價格的買價，以便從交易的

doi:10.6342/NTU201800740

過程中賺取利潤。以我國目前較知名的兩家加密貨幣經紀業者 MaiCoin 及幣託(BitoEx)為例，其所提供的買賣價差通常高達 10%左右，買賣價格則是以均價加減 5%以賺取價差 [434]。近來因為價格波動幅度增大，截至 2018 年 1 月止，買賣差價已高達 20%[435]。由此可見，經紀業者較適合長期投資的交易者，並不適合用於從事短線交易。

第三款 加密貨幣交易所

加密貨幣交易所(Exchange Trading Platforms)運作的形式類似民法第 565 條所謂之「媒介居間」，居間商受契約當事人雙方之委託，斡旋於雙方當事人間，以促成雙方訂立契約 [436]。惟加密貨幣交易所從事的媒介居間並非僅單純促成雙方訂立契約，在交易當事人掛單前，需先提撥交易貨幣/金額至交易所的強制履約帳戶，存放在履約帳戶的貨幣/金額會於交易條件成就時自動扣除並轉換為所交易之項目。知名加密貨幣交易所如：幣安(Binance)、火幣、Bitfinex、Bitstamp，均提供交易者以加密貨幣匯兌加密貨幣或是現實貨幣兌換加密貨幣的方式掛單，再由交易所提供的交易平台自動為符合需求的訂單進行撮合，從中收取交易費。整體觀之，在交易所進行交易，能避免交易者承受如場外交易平台被相對人債務不履行的風險，亦無需屈就於加密貨幣匯兌業的固定匯率，同時實現低風險、高自由的交易需求，對於欲投資加密貨幣之人有相當大的吸引力。

從上述交易架構中可知，交易所與經紀業者間最大的不同之處在於前者並不

---

[434] LocalBitcoin vs BitoEx（幣託）的要價比較，參閱：比特台灣 (2017)。載於：http://www.bitcoin-tw.com/localbitcoins-vs-bitoex.html（最後瀏覽日：2018/06/14）

[435] BitoEX 比特幣(BTC)價格紀錄（2018），〈BitoEX 價格紀錄表〉，https://www.e04.info/（最後瀏覽日：2018/06/14）

[436] 杜怡靜（2010），〈關於居間人之報酬請求權／98 台上 1591 決〉，《台灣法學雜誌》，第 155 期，頁 157-160。

doi:10.6342/NTU201800740

會以自身擁有的加密貨幣作為交易標的,被交易之標的完全是由交易雙方所提供；後者則是自身擁有一定儲備的加密貨幣與現實貨幣，待交易相對人出現再以較時價略高的價錢買入或賣出賺取利潤。架構的不同導致獲利方式亦不相同，蓋交易所收取的是成交手續費，通常是成交金額的一定百分比；反觀經紀業者所賺取的利潤則來自加密貨幣買價與賣價之間的匯差。因此誠如前述，經紀業者於加密貨幣市價起伏較大之時，買價及賣價之間的差距將會呈現巨大的落差，一來降低大量用戶一窩蜂將暫時存放於經紀業者所提供的加密貨幣帳戶中出售加密貨幣，導致流動性風險，二來若真有交易能順利進行，經紀業者也並無損失，蓋原本之買/賣價就較均價高。交易所無法如經紀業者須經由操作匯率來賺取利益，在交易所的交易架構下，因買家及賣家能各自制定想買入及賣出的匯率，利用市場自由競爭的機制來達成交易媒合，是故利用交易所作為交易平台之人較能以貼近市場價格的價錢完成交易目的。

第四款 交換者之間的比較

若比較上述三種型態的交換者，應可按隱密性、風險、交易費用、交易自由來分類交換者。繪表如下：

表 十二：交換者間就隱密性、風險、交易費用、交易自由之比較

特色 / 交換者種類	隱密性	風險	交易費用	交易自由
場外交易平台	高	高	低	高
經紀業者	中	中	高	低
交易所	低	低	中	中

場外交易平台為三種交換者種類中，最具隱密性的類型，主要原因還是因為平台准許當事人享有交易形成的自由，相互信任即可進行交易。平台在其中扮演

doi:10.6342/NTU201800740

著報告居間的角色，故不會積極地介入雙方糾紛，亦不會花費成本在洗錢防制、盡職調查、及認識客戶，所以交易費用低廉，普遍僅收成交數額的 1%或更低的廣告費用 [437]，但也因鬆散的管制機制導致相對高的風險。經紀業者和交易所相比，具有更高的風險。風險來源來自於經紀業者本身，因為經紀業者同時扮演著加密貨幣錢包的角色。此現象在經紀業者和交易所當中非常常見，亦為資安專家們所詬病 [438]，詳如交換者所具備之風險。

經紀業者在交易隱密性和交易風險兩方面，均介於場外交易平台與交易所之間。本文認為經紀業者較交易所隱密的原因約略可分為「審查動機」以及「管轄制約」兩點。經紀業者與交易所最大的不同在於前者乃做為交易之一方，與其交易將有助於公司獲利，故利害關係較大；後者做為居間商，僅負責撮合交易雙方地訂單，並從中收取手續費，故利害關係較小。本文認為利害關係的不同與客戶審查密度的嚴謹有直接的關聯。以下說明之。

第一目　審查動機

國內知名經紀業者幣託和 MaiCoin 各有一套客戶審查程序，幣託將身分驗證分為 A、B、C 三個等級 [439]，各有不同權限。MaiCoin 則將驗證程序分為新手、老將兩種等級 [440]。各自擁有的權限繪表如下：

---

[437] 簡書（2017），〈LocalBitcoins 費用〉，https://www.jianshu.com/p/7c271a096db8（最後瀏覽日：2018/06/14）

[438] Qin Chen, *This is How You Can Protect Your Cryptocurrencies from Hackers*, CNBC (Nov. 3, 2017), https://www.cnbc.com/2017/11/02/heres-how-to-protect-your-bitcoin-and-ethereum-from-hacking.html.

[439] 幣託，〈身份驗證與功能限制〉載於，https://www.bitoex.com/constrains?locale=zh-tw（最後瀏覽日：2018/06/30）

[440] 同前揭註 257。

doi:10.6342/NTU201800740

表 十三：國內交易商間之使用權限對照表—以幣託及 MaiCoin 為例

	幣託			MaiCoin	
等級	C	B	A	新手	老將
超商購買加密貨幣	不可	可	可	可	可
收發加密貨幣	可	可	可	可	可
提領現金	不可	可	可	不可	可
銀行匯款購買比特幣	不可	不可	可	不可	可

幣託要開啟等級 C 的權限僅需 email 和手機認證[441]、maicoin 則對新手無任何身分驗證要求[442]。原先幣託及 MaiCoin 利用超商購買加密貨幣和收發加密貨幣的帳戶是無需身分驗證的。但幣託已於 2018 年 6 月 19 日公布於同月 21 日以後 C 級帳戶需通過基本身分驗證後始得利用超商購買加密貨幣[443]，大幅度地增加了驗證門檻，結果是往後匿名人士不得再未經驗證的狀態下將不明所得至超商購買比特幣的方式購買比特幣。幣託對於等級 B 和 A 的區別在於前者要求客戶上傳身分證圖檔和存簿影本[444]，後者則要求上傳身分證圖檔和通過銀行帳號驗證(綁定金融卡)，以便日後入帳或是扣款[445]。目前 MaiCoin 老手等級除增加上傳電話帳單圖檔外，其餘均與幣託舊制相同[446]，亦即未經驗證的用戶仍擁有透過萊爾富支付現金購買

---

441 同前揭註 439。

442 同前揭註 257。

443 幣託（2018），〈【官方公告：請提升至 B 級用戶才能到全家購買比特幣】〉。載於：https://www.facebook.com/bitoex/posts/2089049798037354（最後瀏覽日：2018/06/30）
各位愛用幣託的會員您好，幣託在 2015 年率先透過全家便利商店提供最便利的比特幣購買服務，感謝用戶長期以來的支持。為了讓台灣的數位貨幣能夠更完善，符合比特幣業者自律條規並保護用戶購買權益，幣託將於 2018/06/21 中午 12 點，全面變更規定成用戶需通過『B 級驗證』才能透過全家購買比特幣。請 C 級用戶進行等級升級，才能到享受 24/7 購買服務。
BitoEX 營運團隊

444 同前揭註 439。

445 同前揭註 257。

446 同前註。

doi:10.6342/NTU201800740

加密貨幣、發送及接收加密貨幣、出售加密貨幣的功能[447]。

雖然 MaiCoin 於 2018 年 6 月底尚未如同幣託對超商入金的身分驗證採取較嚴格的驗證措施(目前對於未驗證的用戶仍可於一日內購買累計等同於新臺幣 50 萬元的加密貨幣)，但已於 2018 年 06 月 25 日公告「為與銀行端及檢調單位合作，一同聯手防堵詐騙人頭帳戶，近期將會建置新的功能及驗證機制，且此功能及機制將於近期正式啟用」整理繪表如下：

[447] MaiCoin 2018 年尚未改制以前的權限彙整表

層級	身份驗證要求	開放功能	限額
新手	無	萊爾富支付購買 發送 & 接收 出售開啟	萊爾富支付購買: 新台幣 $20,000 (單次限額與 $20 手續費) 出售: 無上限
老將	照片證件 + 手機帳單驗證	萊爾富支付購買 ATM 或銀行轉帳購買 & 賣出 發送 & 接收 出售開啟	萊爾富支付購買: 新台幣 $20,000 (單次限額與 $20 手續費) 銀行 & ATM 轉帳購買: 日限額新台幣 $500,000 (如要增額, 請聯繫 info@maicoin.com) 出售: 無上限

doi:10.6342/NTU201800740

表 十四：MaiCoin 表示即將上線的驗證機制權限彙整表[448]

驗證階段	Tier 1 鐵級用戶	Tier 2 銅級用戶	Tier 3 (文件驗證) 銀級用戶	Tier 4 (文件驗證+銀行驗證) 金級用戶
功能	萊爾富現金購買額度 新台幣5000元/筆 每日購買額度 新台幣 50萬 接收加密貨幣	萊爾富現金購買額度 新台幣5000元/筆 每日購買額度 新台幣 50萬 接收加密貨幣 出售	萊爾富現金購買額度 新台幣20000元/筆 每日購買額度 新台幣 50萬 接收加密貨幣 出售 傳送加密貨幣	萊爾富現金購買額度 新台幣20000元/筆 每日購買額度 新台幣 50萬 接收加密貨幣 出售 傳送加密貨幣 銀行轉帳購買
必備要件	綁定email 綁定手機號碼	綁定email 綁定手機號碼 銀行資料	綁定email 綁定手機號碼 銀行資料 基本資料 上傳身分證、手機帳單	綁定email 綁定手機號碼 銀行資料 基本資料 上傳身分證、手機帳單 綁定本人銀行資料

表格來源：MaiCoin

上表為未來 MaiCoin 可能採取的驗證措施與相對應所賦予的權限。從該表及近來幣託及 MaiCoin 所採行的策略可知原先為吸引客戶購買加密貨幣而採取不對購買之客戶進行審查的動機已逐漸被近年來甦醒的洗錢防制意識所影響。

原先分析的結果顯示，因購買、收發加密貨幣此兩種有利經紀業者的行為是有助於業者獲利的，故完全不受身分限制，僅當用戶有需要從經紀業者取得實體貨幣時，才需經過基本的身分驗證。如此驗證機制的設定，雖然便於用戶購買加密貨幣，以圖利自身，卻也為有心洗錢的人士開了一條後門。例如：如何防制犯罪者利用超商購買加密貨幣的方式處置(Placement)不法所得？蓋目前加密貨幣具有高度匿名性和欠缺管制，一旦不法所得進入洗錢的第一階段「處置」後，後續

[448] MaiCoin（2018），〈2018/06/25 MAICOIN 數位資產交易平台 公告〉。載於：https://maicoin2.freshdesk.com/zh-TW/support/solutions/articles/32000023973-2018-06-25-maicoin-數位資產交易平台-公告（最後瀏覽日：2018/06/30）

doi:10.6342/NTU201800740

多層化（Layering）、整合（Integration）的階段將非常不利主管機關的追查[449]。但上述為便利客戶入金而降低認識客戶的審查動機，因主管機關已明言需採實名制，是以已有顯著的改善，要不具名從超商購買加密貨幣並移轉加密貨幣已較以往困難許多。

另一方面，交易所因為必須顧及交易雙方的交易安全，所以會對每一筆交易做更細緻的審查。蓋假若因交易所的過失，導致有一方已經履約，卻無法對另一方強制執行的話，交易所將需承擔系統出錯所造成之損害。進一步言之，欲成為交易所的用戶，交易雙方的金融訊息一定會經手交易所，所以交易所能更輕易地達成認識自己的客戶(KYC)的要求，因此隱密性最低。下圖將簡略論述何以交易所能認識到交易雙方的金融訊息：

圖 十二：交易所藉由入金、出金程序確認客戶身分

如上圖所示，買受人欲藉由交易所購買加密貨幣，必須先將用於購買之資金以匯款方式交予交易所的履約保證專戶保管，交易所於接收這筆資金時，即可得知買受人所使用的金融機構，故加密貨幣所謂的「化名式匿名」在此已破功，執法單位可從實體金融單位得知買受人的訊息。反過來說，出賣人欲向交易所提領販售所得，亦必須向交易所提供實體金融帳戶，交易所即能即時記錄金流的流向。

---

[449] 蔡佩玲（2017），〈國際洗錢防制發展趨勢與我國洗錢防制新法－兼論刑事政策變革〉，《刑事政策與犯罪防治研究專刊》，14 期，頁 3-12。

doi:10.6342/NTU201800740

第二目　管轄制約

管轄制約是指交易所會因為所服務的客群、現實貨幣、地域，而必須提升自我的審查義務。解釋為何會因為「管轄」的因素而受制約前應認識到：交易所主要係由「交易成交量」的抽成來獲利，越多交易者代表著越多的獲利。有此認識後即不難理解為何各大交易所均建置不同語言的網頁、開放 VISA 及電匯等付款方式，以吸收來自全世界欲買賣加密貨幣的交易者。交易所欲達成交易量最大化的目標，必須透過通用貨幣(歐元或美元)以及和各國所屬的金融機構合作，使得分散至各國的交易者們能更方便的匯款和提款。如此一來將使得交易所成為理論上隱密性最低的一種交易模式。

第五款 交換者所具備之風險因素

交換者除因交易客體—加密貨幣本身特性所具備之洗錢風險，自身之營運模式亦具有產生他種風險的可能。本文大方向於建議加密貨幣之防制洗錢及打擊資恐政策時亦參酌以下各種風險，並擬於最後提出如何具體利用此發現來完善本文就我國加密貨幣匯兌產業於洗錢防制與打擊資恐規範議題上所提出之建議。

交換者如前所述可區分為場外交易平台、經紀業者、交易所三類，且因場外交易平台與後二者之信用基礎、價格形成機制、清算方式各不相同，使得業者本身所面臨之最大風險還是來自於加密貨幣用於洗錢之風險。本文以下將撇除場外交易平台，著重於經紀業者及交易所二類除洗錢以外可能具有之風險，為用語上方便，將以「交換者」為經紀業者及交易所的通稱。

交易者所具備除洗錢以外之風險主要來自於加密貨幣本身的性質以及買賣加密貨幣之大眾投資者欠缺資安意識兩種因素。舉加密貨幣為例，就其本身之性質而言，因其僅是一項存在於區塊鏈內某一地址中尚未被更改的電磁紀錄，所以若

doi:10.6342/NTU201800740

要聲稱對該筆紀錄具有所有權，須向區塊鏈內的眾多節點證明自己擁有「私鑰」，私鑰是唯一能證明自己並且賦予自己移轉加密貨幣的憑證。以比特幣為例，其私鑰其實是一長串使用 SHA-256 生成 32 bytes 位元（256 bits）的隨機亂數[450]。要記得一長串隨機的亂數作為密碼對大眾使用者而言無疑是非常困難的一件事，況且一般民眾亦不具有以自身為節點，親自進行區塊鏈上交易的能力。因此，經紀業者和交易所的產生不僅提供了簡潔且容易操作的圖形使用者介面（Graphical User Interface, GUI）、手機 APP、更同時提供了匯兌及交易服務，以吸引更多客戶前往交易。

惟上述簡便化所導致的結果，即是與經紀業者和交易所交易之客戶不再利用完全由自己控制私鑰的帳戶與經紀業者和交易所進行交易，而是先至經紀業者或交易所註冊後，再利用註冊後由經紀業者和交易所所提供的地址進行入金或是出金的交易。以向經紀業者購買加密貨幣的流程(入金)為例，客戶須先至經紀業者註冊帳戶，通過驗證後會獲得一組加密貨幣的錢包地址。其後藉由信用卡、電匯等金融匯款方式將現實貨幣匯至經紀業者之金融帳戶，經經紀業者確認收款後再移轉相當價值之加密貨幣至客戶於註冊時所獲取之錢包地址。以出售加密貨幣的流程(出金)為例，客戶須先移轉欲出售的加密貨幣至於經紀業者註冊時所獲得之錢包地址，待移轉完成後始得利用經紀業者所提供的圖形使用者介面進行出售加密貨幣的交易。

---

[450] MORDECHAI GURI, BEATCOIN: LEAKING PRIVATE KEYS FROM AIR-GAPPED CRYPTOCURRENCY WALLETS, BEN-GURION UNIVERSITY OF THE NEGEV (Apr. 23, 2018), https://arxiv.org/pdf/1804.08714.pdf;
私鑰呈現的方式：
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262
Base 58 WIF 私鑰則呈現如：
5Kb8kLf9zgWQnogidDA76MPL6TsZZY36hWXMssSzNydYXYB9KF

doi:10.6342/NTU201800740

於上述無論入金或出金之時，均須先將現實貨幣或加密貨幣移轉予交換者(經紀業者及交易所)的情況下，將會有數種衍生的問題產生，分別是 1.雙重帳本；2.資訊安全；3.資金沉澱。

第一目　雙重帳本

雙重帳本言下之義有兩套帳本，分別是交換者自己一套供客戶閱覽的帳本以及真正存在於區塊鏈上的帳本。供客戶閱覽的帳本會透過交換者所提供的圖形使用者介面顯示與客戶，讓客戶瞭解交易細節，但此帳本並非真正存在於區塊鏈上的帳本，不具備所有區塊鏈帳本所擁有的優點，亦即並非安全且不可竄改的；顯示在此帳本上的加密貨幣數量亦非真正所擁有的加密貨幣數量，除非客戶至區塊鏈的交易資訊上確認所擁有的錢包地址有交易訊息產生，要不然呈現在交換者所提供的帳本上的加密貨幣至多僅能稱之為「隨時對交換業者請求給付加密貨幣之請求權」。

本文以實證研究的方式，檢視曾經於透過便利商店入金向我國經紀業者購買比特幣的交易紀錄，再將經紀業者所提供的地址與區塊鏈上該地址所存在的交易紀錄相比對；本文發現[451]：筆者於 2016 年第一次透過便利商店購買之比特幣並未紀錄於區塊鏈上，但於經紀業者的交易紀錄卻有該筆紀錄。其後筆者透過交易介面將該筆比特幣移轉至另一個地址，從區塊鏈上的紀錄發現，是由第三人的比特幣地址(可能為經紀業者所控制)移轉筆者所指定的加密貨幣予筆者的交易相對人，交付方式類似民法第 761 條 3 項之指示交付，不同之處在於筆者無法將名義上所擁有，但實際上類似[452]民法第 602 條 1 項消費寄託[453]於經紀業者之加密貨幣，藉

[451] 以下敘述之案例將以「筆者」為作者本人之稱謂。

[452] 81 年台上字第 2166 號指出：民法第 602 條規定之消費寄託契約以移轉寄託物所有權於受寄人

doi:10.6342/NTU201800740

由讓與民法第 478 條[454]消費借貸返還請求權予交易第三人，蓋還是須由筆者自己操作，經紀業者始會從其他帳戶向筆者之交易相對人支付。本文認為在上述雙重帳本之情形，因客戶之帳戶交易並未實際出現在區塊鏈帳本上，實難認為客戶擁有經紀業者所聲稱擁有之加密貨幣；對於並未實際擁有之加密貨幣所為之後續處置似屬於「不真正第三人利益契約」。蓋利益第三人契約，按民法第 269 條 1 項謂：要約人（或稱債權人）與債務人約定，使債務人向第三人給付，且「第三人對於債務人，有直接請求給付之權」。惟本案情形是筆者欲指示經紀業者向第三人為給付，且因為操作上僅能由擁有「隨時對交換業者請求給付加密貨幣之請求權」的筆者為之，契約存在寄託人與受寄人之間，第三人無權直接向受寄人行使消費寄託物返還請求權，理由是寄託人於技術上亦無從讓與該權利。實際上所發生之契約關係為由寄託人(筆者)向受寄人(經紀業者)請求其向契約外之第三人為給付，第三人對於受寄人無任何請求權亦非契約當事人，故判斷在雙重帳本的交易下，客戶與經紀業者間的契約關係似為寄託(蓋就算經紀業者將加密貨幣實際移轉至客戶註冊時所附贈之帳戶，客戶因未保有私鑰，故難謂實際上擁有)，將加密貨幣移轉之債之關係應最似「不真正第三人利益契約」。

第二目　資金沉澱

資金沉澱的現象與後續所論及之資安風險息息相關，蓋所謂資金沉澱的「資金」來自於暫存於交換者所提供之錢包內之加密貨幣。本文認為資金沉澱的現象

為約之成立要件，但此時筆者之帳戶因實際於區塊鏈帳本上自始未有加密貨幣的交付，故難成立消費寄託契約。

[453] 民法第 602 條:「寄託物為代替物時，如約定寄託物之所有權移轉於受寄人，並由受寄人以種類、品質、數量相同之物返還者，為消費寄託。自受寄人受領該物時起，準用關於消費借貸之規定。消費寄託，如寄託物之返還，定有期限者，寄託人非有不得已之事由，不得於期限屆滿前請求返還。前項規定，如商業上另有習慣者，不適用之。」

[454] 民法第 478 條：「借用人應於約定期限內，返還與借用物種類、品質、數量相同之物，未定返還期限者，借用人得隨時返還，貸與人亦得定一個月以上之相當期限，催告返還。」

doi:10.6342/NTU201800740

與資安風險提升的原因在於，一般客戶或是投資者於注資購買加密貨幣後，往往抱持著「放著等以後升值」的心態來看待帳戶所呈現的餘額，且因缺乏資訊安全上的認知，加上再度移轉加密貨幣需要花費手續費作為移轉的成本，因此大部分小額採購加密貨幣之用戶不會選擇於交易後將加密貨幣移轉至私人實際控制的地址或冷錢包。隨著客戶數目的增加，暫存或是直接選擇以經紀業者或交易所所提供的錢包為儲存媒介之客戶亦會隨之增加，導致沉澱於經紀業者或交易所的加密貨幣與日俱增，最終達到一個可觀的數額。此時只要駭客攻破上述交換業者的資安防線即能達成大收割的結果，一次盜取鉅額之加密貨幣。

第三目　資訊安全

誠如上述，經紀業者及交易所因實務作業上可能存在雙重帳本的問題，或是有實際同步帳本，且所有客戶之帳戶於區塊鏈上的私鑰均由經紀業者及交易所所掌握。如此情形將使得上述業者容易成為被駭客攻擊之目標，面臨非常大的資安風險。本文前述即以近來韓國及日本發生的駭客事件為例，凸顯大型加密貨幣交易所被駭客攻擊的機率及所損失的鉅額加密貨幣。

第四目　流動性風險

流動性風險的產生源自於使用經紀業者或是交易所所提供的錢包，蓋利用前述之錢包代表著無法掌控自己的私鑰，以至於並非用戶隨時想轉讓加密貨幣就可以轉讓。同理，加密貨幣的價格波動瞬息萬變，用戶欲將加密貨幣提現時，亦將有可能於現金提領時遭遇流動性風險，因業者可能不具有充分的流動性資產給付大量出售的加密貨幣，故有可能會將買賣價格修改成遠高/低於市價的水準、臨時

doi:10.6342/NTU201800740

關閉網站，對外宣稱維修中或系統異常或是將一定時間內已成立的交易取消[455]，來防範「資不抵債」的流動性風險。

第三項 交換者之防制洗錢及打擊資恐政策

政策（Policy）是一個與策略（Strategy）相關，卻又不盡相同的名詞。有論者認為兩者的思考流程始於目標（Objectives），將目標明確化後擬定策略，策略即是達到特定目標之方向、時機與程度。策略擬定後，下一步即是擬訂更具體的行動方針與投入相對應的資源，此即政策制定的環節，政策在此扮演著載具（Carrier）的角色，乘載著前往該目標的工具與方法。一言以蔽之，政策即是達成預設目標之工具與使用之方法[456]。我國近來大力推行洗錢防制，所欲達成的目標是維持人的秩序及「錢的秩序」，並塑造洗錢防制之觀念及文化[457]。加密貨幣匯兌產業欲達成上述目標，即須訂定相對應的策略方針，本文參考 FATF 及美國法分別提供的建議及具體採行之規範方式，認為採行公鏈架構之加密貨幣與採行私鏈架構之加密貨幣應按其性質的不同在制定洗錢防制策略上而有所區別。

先擬訂洗錢防制策略經風險評估後再制訂政策的優點在於能客制化出最適於我國使用之洗錢防制政策，而非一概參照外國法將其規範引進並進行直接適用。未經分析以前，國家對於區塊鏈究應採何種洗錢防制措施？洗錢防制力度是強是弱？大方針為何？尚屬不明確的狀態。若我國欲以促進金融科技發展為目標，那麼策略上應採取相對寬鬆的措施。惟相對寬鬆並不代表政府可以毫無作為，仍應

---

[455] Bitoex 幣託（2017），〈「因海外交易所發生異常報價，須重新尋找基準」〉。載於：https://www.facebook.com/bitoex/posts/1997881620487506（最後瀏覽日：2018/06/14）

[456] 科技產業資訊室（2008），〈政策與政策流程思考〉。載於 http://cdnet.stpi.narl.org.tw/techroom/analysis/2008/pat_08_A019.htm（最後瀏覽日：2018/07/12）

[457] 外交國防法務處（2017），〈防制洗錢 國家向前－我國防制洗錢策略與未來展望〉。載於：https://www.ey.gov.tw/Page/448DE008087A1971/907324a2-38db-4d75-80b9-402009242f62（最後瀏覽日：2018/07/12）

doi:10.6342/NTU201800740

擬訂大方向之洗錢防制策略及具體之洗錢防制政策，蓋國家應以公共利益、民眾福祉民眾為依歸，摒棄偏私與壓力，確實推動行政工作，此乃人民至上原則之表現。

現今區塊鏈技術在公鏈之應用上以趨近成熟，又因其應用甚廣，僅需網路連線即可線上交易，故外國政府已經著手制定規範區塊鏈在加密貨幣應用上的方針，我國亦不落人於後，於近日已開始擬定規範策略，殊值讚許。

下表為 2016 年中央銀行就各國對於虛擬通貨之監管態度。從中可發現一共通點，亦即於專法訂定前，大多數國家均有適用現行法規之機制。

表 十五：各國政府對加密貨幣之監管態度

國家	AML/CFT[24]：適用(或修正)現行法規或提出警示	稅務處理	對消費者警示	經營虛擬通貨交易平台須經特許或註冊	對金融業警示或禁止其從事虛擬通貨業務	禁止發行或使用
阿根廷	警示可能涉及洗錢及資助恐怖分子風險		警示		對申報個體提出警示	
玻利維亞						禁止
加拿大	修訂現行法規	課稅	諮詢			
中國大陸					禁止	
法國	適用現行法規	課稅	警示			
德國	適用現行法規					
義大利			警示		警示	
日本	擬提出新法規		警示	擬提出新法規		
俄羅斯	適用現行法規		警示			禁止(已提草案)
新加坡	擬提出新法規	課稅	警示			
南非			警示			
英國	適用現行法規	課稅				
美國*	適用現行法規(聯邦法)	課稅(聯邦稅)	警示	州政府許可制(如紐約 BitLicense)		

* 美國商品期貨交易委員會(CFTC)已將比特幣等虛擬貨幣正式歸類為大宗商品，虛擬貨幣選擇權交易與原油或小麥等衍生性商品交易一樣，須受 CFTC 的監管。
資料來源：IMF (2016), "Virtual Currencies and Beyond: Initial Considerations," *IMF Staff Discussion Notes*, No. 16/3。

表格來源：中央銀行 2016/03/24 央行理監事會後記者會參考資料

我國於修正洗錢防制法後於該法第 5 條 3 項 5 款增訂「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」，已為有必須適用洗錢防制法之「其他事業」增訂一概括條款，讓處於立法過渡期之我國能有法可循。惟因第 5 款之條款實在過為概括，解釋上存在著非常大的空間，空泛將加密貨幣產業適用洗錢防

doi:10.6342/NTU201800740

制法第 5 條 3 項 5 款所稱之「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」並非長遠之計，至多僅能以該款為授權依據，另行訂定更具體之相關遵循規範。

是以近日政府部門亦表態將加密貨幣產業業務應受規範，先將加密貨幣產業解釋屬於洗錢防制法第 5 條 3 項 5 款所稱之「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」，再制訂防制洗錢相關的法規範納管，欲朝實名制與自律組織方向前進[458]。惟所納管之加密貨幣應為採行公鏈架構之貨幣型加密貨幣，不可一概而論。蓋加密貨幣產業應用規模甚大，不應僅因涉及「加密貨幣」，即被冠上「高風險」、「易洗錢」的標籤，尚須由交易程序、技術等面向，綜合評估該業務型態是否具有「易為洗錢犯罪所利用」之特性；若無，則無需以過嚴格的標準來審視該業務，如此始得在建立洗錢防制文化的同時亦兼顧我國金融科技發展的發展。

因加密貨幣產業是一個尚未開發完全的產業，產業資訊較少，故有評估上的困難。從而在定位此一「指定非金融事業或人員(Designated Non-Financial Business Professions, DNFBPs)」的風險等級是否屬於屬於洗錢防制法第 5 條 3 項 5 款所稱之「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」時，在資訊有缺漏而致以風險為基礎之判斷方式難以評估的前提下，似有必要暫時以較高風險等級的處置方式予以對待。至於進行風險評估方法時，可參酌巴塞爾銀行監理委員會「Sound Management of Risks Related to Money Laundering and Financing of Terrorism」附錄四所列舉之下列因素以綜合判斷該服務之風險等級。

1. 產品和服務之性質(Nature of Products and Services)

---

[458] 同前揭註 359。

doi:10.6342/NTU201800740

2. 客戶業務關係之性質(Nature of Business Relationship)
3. 地理範圍(Geographic Reach)
4. 服務管道之性質(Nature of Delivery Channels)

另外在評估程序中，可參酌防制洗錢金融行動工作組織（FATF）於 2014 年 6 月發佈之「虛擬貨幣的重要定義與潛在的防制洗錢／打擊資恐風險報告」(2014 年 6 月 VC 報告)、FATF 後來於 2015 年 6 月所增訂之「虛擬貨幣風險基礎方法指引」[459]及「FATF 評鑑方法論」[460]對於虛擬貨幣支付產品與服務（VCPPS）所提出之建議，前文已有述及。

職是之故，FATF 及美國 FinCEN 綜合交易程序、技術等面向，評估現下最易被利用於洗錢之加密貨幣業務型態應屬「交換者」，蓋兩者不約而同均提出管制現實貨幣與虛擬貨幣間的交換者為主要規範方式，期待能減少匿名性，讓金流更加透明。主要原因應在於加密貨幣與現實貨幣的兌換過程中，除非是以現金交易之形式直接交易，多數須經由交換者之手，故而以規範交換者為重點。交換者又如前文分析能細分成場外交易平台、加密貨幣經紀業者、以及加密貨幣交易所。匯兌過程中又能以公鏈加密貨幣、私鏈加密貨幣、本國匯兌、跨國匯兌而有洗錢風險的不同。

本文所討論之交換者共分三類，且交易客體多屬於採取公鏈架構之加密貨幣。利用加密貨幣從事洗錢犯罪相較於其他洗錢方式更具技術層面的複雜性，且於查緝後若不立即保全扣押相關犯罪所得，將可能導致區塊鏈紀錄更改後，被「脫產」之加密貨幣無從執行的窘境。加密貨幣因不具實體，亦不如他種以價值移轉作為

---

[459] 法務部調查局（2017），〈虛擬貨幣風險基礎方法指引〉。載於：http://www.amlo.moj.gov.tw/HitCounter.asp?xItem=491315&ixCuAttach=173792 最後瀏覽日：2018/07/15）

[460] 調查局（2017），〈FATF 評鑑方法論(中文)〉。載於：http://www.amlo.moj.gov.tw/HitCounter.asp?xItem=491310&ixCuAttach=173787（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

洗錢犯罪的態樣，能從實體物品追緝洗錢犯罪。較為高明的加密貨幣洗錢犯罪會減少與實體金錢接觸之機會，以降低若車手被逮將有可能暴露集團組織的風險。

綜上所述，未來加密貨幣洗錢態樣有可能會向白領金融犯罪領域的方向發展，且新型態主打匿名性的加密貨幣如：門羅幣及 ZCash，將一定程度上帶動此發展趨勢。蓋主打匿名性的加密貨幣將大幅增加加密貨幣金流追蹤上的困難度，使交易所即便採取實名制後，仍無法透過分析公鏈上的公開資訊追尋接收貨幣之人。種種因素均加劇了加密貨幣之洗錢風險，並提供了專業洗錢犯罪利用此新型態的洗錢防制弱點的機會，未來將可能見到以販售加密貨幣之資金購買金融商品之案例。類似案例會利用販售加密貨幣之資金(看似合法)，再混合他種金融商品，以增加「多層化」及「整合」階段的完善程度。為有效反制上述新型態之洗錢方式，本文擬就位於我國之交換者進行分析，旨在利用產業風險評估回顧前文大方向對於公鏈之洗錢防制策略，探詢對交換者可採行之政策，以政策具作為載具（Carrier），將公鏈型加密貨幣之洗錢防制策略更具體化，提出一個較明確的前進方向。

第一款 場外交易平台

首先以場外交易平台為例，因交易平台本身係以近於報告居間的模式搓合交易者，其並不會強制客戶提供身分資訊以供驗證。驗證客戶資訊雖是提升客戶信用的管道之一，但是交易實際取決的因素，並非交易對象是否有通過手機驗證或是證件驗證等驗證程序。蓋場外交易平台並不會如同金融機構嚴格進行客戶審查，且若進行客戶審查也會因成本過高不利於競爭，而面臨客戶流失的風險。因此大多數場外交易平台之客戶反而會選擇以評價、成功成交數量、平均完成交易時間等因素，來判斷是否應與該名買家/賣家進行交易。一言以蔽之，此類交換者是以犧牲「信任」換取「匿名性」為主的平台，規範上非常不易。本文認為此類交換

doi:10.6342/NTU201800740

者平台之行業固有特性及服務性質均屬非常容易為洗錢犯罪所利用之類型，呈現非常高風險的狀態；另外就「行業活動之地理範圍」而言，因業者實際架設主機之所在地並非處於我國，且亦無從得知加密貨幣之來例及去向，種種未知及不確定性導致無從評估風險等級；但就「與客戶業務關係之性質」及「服務管道之性質」兩者可以從前文的敘述得知並不會真的做到「認識客戶」的程度，蓋平台提供的僅是一種認識其他交易者的管道，並不會過度介入客戶間所約定的契約，所以亦無從期待其會在提供服務的管道上進行分級制度或以相對應的風險賦予使用服務上的權限，風險等級因此可謂「非常高」。

此類交換者在五項風險評估中有四項被歸類為「非常高」風險，理應嚴加控管，但因為此類業者僅靠平台即可運轉(通常平台的主機位於外國)，且因實際交易僅發生在交易雙方，故無論從司法管轄權或是規範可能性以觀，並無具體可實行之政策，策略上僅能對其他交換者施行「具吸引力的法律規範策略」試圖推行其他較易監控之交換者類型，加強其他交換者對於我國交易者的吸引力，以減少使用此類交易管道的使用者族群。

第二款 加密貨幣經紀業者及交易所

此類交換者的規範政策可朝兩種方向進行，一種方向是欲同時達到規範場外交易平台且降低此類交換者所可能隱藏的其他風險如資訊安全、資金沉澱、流動性風險等；另一種政策方向則僅是管控被用於洗錢的風險。上述兩種政策方向中如採行前者可讓法規範一步到位，在降低交換者整體行業被洗錢犯罪所利用的風險同時，亦可就消費者保護這一部分做出充分的法規範，預防類似南韓及日本之大型交換者遭駭客入侵，而導致多數消費者求償無門，徒增對加密貨幣產業的不信任。若主管機關採行後者政策，欲先於今年 APG 評鑑以前完成加密貨幣產業的

doi:10.6342/NTU201800740

洗錢防制規範，本文認為先以「指定之非金融事業」進行管控，不失為一良好的暫時性規範政策。原因在於目前我國加密貨幣產業尚處於初期發展的階段，直接課予負擔過重的洗錢防制義務，不啻於宣布退出金融科技 ABCD 中的區塊鏈技術(Blockchain)[461]，蓋在產業未發展成熟前，過於強硬的洗錢防制義務將導致法遵成本大幅提高，而業者將間接轉嫁此類成本予消費者，從而促使我國消費者轉向國外的交換者進行交易。若我國連第一代區塊鏈技術的應用(Blockchain 1.0)都無法完善地規劃，欲發展後續第二代整合智能契約的區塊鏈技術只會更加困難。

僅就洗錢防制為規範的政策應會偏向於實名制的推行，推行過程中，督促平台進行客戶審查(Customer Due Diligence, CDD)是認識客戶(KYC)環節不可或缺的。若按防制洗錢金融行動工作組織(FATF)金融機構應實施之標準 [462]，應禁止客戶保有匿名帳戶或使用虛構化名之帳戶(此原則不管是金融業者或是非金融業者均通用)，並於執行審查客戶時採取下列步驟：

1. 透過可靠、獨立之原始文件、資料或資訊（身分資料）確認客戶身分，查證客戶提供資料之真實性。
2. 辨識實質受益人身分，及採取適當措施並運用相關資訊或從可靠來源加以確認，俾瞭解實質受益人為何者。(若政策執行上未准許法人客戶則無需採行此步驟)
3. 取得業務關係之目的及業務性質等資訊。

以上程序的實施，並無法完全杜絕利用加密貨幣之洗錢犯罪，蓋新型加密貨幣如門羅幣及 ZCash 有著更強大的匿名性，針對利用此種加密貨幣進行洗錢之犯罪者，雖其貨幣來歷極其可疑，惟若缺乏明確證據能積極證明其所得為犯罪所得

---

[461] Mr.Fintech（2017），〈金融科技 ABCD 技術知多少?〉。載於：http://www.thinkfintech.tw/Article?q=ART171129001(最後瀏覽日：2018/06/14)；金融科技 ABCD 分別為 A：人工智慧(Artificial Intelligence)；B：區塊鏈技術(Blockchain)；C：雲端計算(Cloud Computing)；D：大數據(Big Data)。

[462] FATF 建議 10。

doi:10.6342/NTU201800740

的話，基於罪刑法定主義原則，無法將其所有之加密貨幣一概沒收。此問題若係發生在私鏈型加密貨幣，或許有辦法以審計節點的方式予以追查金流，掌握金流流向，惟公鏈型加密貨幣既如前文所述，加入審計節點在現實上有一定的困難度，以致金流的追蹤不甚容易，更遑論讓主管機關主動追查金流背後之匿名人。

是以就洗錢防制的中程政策發展上，本文亦肯認應成立由官方認許之自律組織，此自律組織不應虛有其表，更應該對其成員有實質性的影響力。大原則為寧願由自律組織內部自我協調，相互規範，也不要由主管機關主動裁罰。原因在於由主管機關主動裁罰較容易對投資者發出此一產業的洗錢防制密度較嚴的警訊，此為對外部之不良影響。對內而言，由主管機關為主動裁罰即表示自律組織無法有效對內部成員形成有效規範，運作與溝通上尚欠缺有效的管理及自律，仍未形成能真正自律之自律組織。

長遠的洗錢防制政策為回歸規範全數交換者，欲達此目標，則不能僅將洗錢的風險納入考量，蓋欲規範場外交易平台尚須降低加密貨幣經紀業者及交易所兩者可能隱藏的其他風險如資訊安全、資金沉澱、流動性風險等，以促成一個對於消費者較有保障的環境。一旦形成此具吸引力且以客戶為中心的環境，客戶自願提供自身(金流)資料的意願即會增加，更勝一概以法律明文規定，採取過為強硬的限制措施。政策下具體可採行之計畫，可由政府介入建立一個類似存款保險之制度，讓欲享有政府提供的保護傘之客戶有意願放棄部分匿名性，以換取安定性及安全性。更進一步尚可推行監理科技，利用監理科技破除匿名性。若採取此種政策，未來我國執法機關將有辦法掌握一個慣用加密貨幣交易使用者之資料庫。該資料庫將不再侷限於從事「法幣交易」的客戶，更可涵蓋大多數以加密貨幣購買加密貨幣，即進行「幣幣交易」之客戶。屆時，若有大額加密貨幣款項以完全匿

doi:10.6342/NTU201800740

名的形式，層層轉手至某一客戶之帳戶中，將會顯得非比尋常，因為大部分之客戶均已習慣與具有保險、保障之相對人進行交易，若非有相當大之誘因，一般不會選擇與未經社群驗證之人進行交易。此機制有助於廣納合法使用者，增長合法使用者之族群，並鼓勵多數本國之使用者採用主要據點位於本國的加密貨幣匯兌業者，以利主管機關在有效掌握客戶群體資訊時，促進本國金融科技產業之發展。換個角度觀之，若合法之使用者族群得以增長，屆時主要目的為利用加密貨幣進行洗錢之群體將會被孤立，或是迫於避免與我國之加密貨幣匯兌業者來往，因為一旦建立業務關係，不免須揭露自身之身份訊息，若不加以揭露，又會被列為高風險客戶加以監控，得不償失。

第四節　小結

本文從國家風險評估報告出發參考報告內「洗錢威脅辨識結果」中對我國最具威脅的 8 大類型，包含毒品販運、詐欺、組織犯罪、貪污賄賂、走私、證券犯罪、第三方洗錢、稅務犯罪等，並將加密貨幣可能用於與上述威脅結合之可能性。結果顯示因加密貨幣運作上採行全雙向流通性虛擬貨幣架構，再加上目前我國及是其他多數國家均欠缺對於加密貨幣匯兌業者的一套明確且完整的法規範，是以不難達成與現實貨幣相互匯兌的結果。簡易匯兌的性質加上加密貨幣與生俱來的匿名性等特性，導致加密貨幣在國家風險層級上具有良好的整合功能，能非常簡易地與每項列入「非常高」的前置犯罪相結合，透過其高度複雜性、廣泛的流通規模，輕易地放大犯罪者的洗錢能力及洗錢規模，且根據其浮動的價值，讓犯罪所得難以估計。綜合上述，本文認為有擬定洗錢防制策略之必要。

洗錢防制策略是達成防制洗錢目標之指引方向，本文討論之主軸為如何達成「防制加密貨幣用於洗錢」之目標，為達成此最終目標，制定洗錢防制策略即成

doi:10.6342/NTU201800740

為首要探究對象。採取公鏈架構之貨幣型加密貨幣與採行私鏈架構之貨幣型加密貨幣因運行模式相差甚遠，是以本文於擬定洗錢防制策略時亦就兩者之差異處分別提出不同方向的策略。就公鏈型加密貨幣本文認為目前主管機關準備以「指定之非金融事業」的標準制定適用於加密貨幣產業的洗錢防制規範，是妥適的洗錢防制策略，惟其他如資安、消費者保護等議題尚欠缺妥適的策略方向；對此，本文亦提出如：加密貨幣的存款保險、準備金比率、流動性覆蓋比率、自律組織、監理科技等大致可再朝具體政策發展的洗錢防制策略。就私鏈型加密貨幣，因節點具有控管可能性，在結點的權限限制上及參與上均能被貨幣發行人有效管控，是以本文建議除最基本的確認客戶身分洗錢防制義務不得省略外，可採取「非審慎監理」的策略，併同監理科技—審計節點以最便捷、省時、省力的方式達成自動偵測並申報的結果。

擬定策略後，本文就加密貨幣產業進行風險評估，以評估上述策略是否能有效降低產業內的地域風險、客戶風險、產品及服務管道風險。為進行風險評級，本文分別檢視加密貨幣匯兌行業之固有特性、產品及業務特性、客戶業務關係之性質、行業活動之地理範圍、服務管道之性質等因子，發現如下：固有特性風險評級應為「非常高」；行業所提供之產品及服務性質應為「非常高風險」產業；至於客戶身分與客戶的職業及客戶所從事的業務兩類，加密貨幣的產業評估上將面臨著如何辨識、取得及驗證客戶資料的困境。目前因無法取得上述兩類資料，即無法估算客戶群體內是否存在高風險客戶，當然也就無法評估產業所隱含的風險，現暫時將產業以「中高風險」來對待；地域風險的評等取決於交易所之分支據點是否位於較低洗錢風險的地域，因目前尚無技術能準確判斷於區塊鏈上所移轉之加密貨幣被發送至之地域位於何處，僅能以交換者之營業地域進行判斷，就此以

doi:10.6342/NTU201800740

觀，目前位於我國之交換者之地域風險應為「低」至多評估為「中」。最後就服務管道之性質，本文參酌數位存款帳戶之例，發現驗證過程的繁瑣程度影響著客戶資訊取得的完整度，而客戶資訊越完整，能被驗證的程度亦越高。是以，本文認為加密貨幣於評估服務管道之性質時可效法如數位存款帳戶之例，按資料蒐集的完整度及可驗證性進行評估，給予要求客戶須經被認證之第三方驗證的業者「低風險」的風險評級；給予要求客戶須使用第三方佐證資訊驗證的業者「中風險」的風險評級；給予僅要求客戶使用自身所提供之資訊即能開戶的業者「高風險」的風險評級；給予未能按客戶所提供之資訊完整度及可驗證性而調整客戶所能使用的服務權限之業者「非常高風險」的風險評級。

辨識並評估上述加密貨幣匯兌行業之各種風險後，本文參酌 FATF 之建議及美國法，將行業內從事匯兌業務之業者稱之為交換者，並以其作為規範公鏈型加密貨幣首要應被管制之對象，並將其細分為場外交易平台、加密貨幣經紀業者、加密貨幣交易所三類，並對三者之交易架構進行比較，以探詢規範方式是否應加以區別。三者相較之下，場外交易雖然交易風險最高，但勝在交易方式最自由、交易費用最低廉、以及最高度的匿名性。經紀業者就交易費用而言雖為三者中最高，且交易自由為三者中最低，但卻能吸引願意用中等程度的交易風險以保有中等程度匿名性之客戶。交易所則反其道而行，以最低程度的交易風險吸引願意以最低度的匿名性進行交易之客戶，並同時提供三者中較為中庸的交易費用及交易自由。

交易架構間的不同是造就上述差異之處的主要原因，但是當本文更進一步檢視經紀業者及交易所兩者之交易架構，即發現兩者雖非如場外交易平台需要交易雙方付出大量的信任以彌補債務不履行的風險，卻存有其他不可忽視的風險。因

doi:10.6342/NTU201800740

此本文將經紀業者及交易所可能因交易架構本身而產生之風險因素再細分為雙重帳本、資金沉澱、資訊安全及流動性風險。

最後，本文利用產業風險評估回顧前文大方向對於公鏈之洗錢防制策略，探詢對交換者可採行之政策。場外交易平台目前尚無有效之直接性洗錢防制政策，但是本文認為有可能透過消除前述「經紀業者及交易所可能因交易架構本身而產生之風險因素」而讓經紀業者及交易所更具吸引力，減少交易者使用場外交易平台的誘因。至於經紀業者及交易所之洗錢防制政策又可分為採行能同時防制場外交易平台被洗錢犯罪所利用之「一次到位」規範方式以及「漸進式」的規範方式。因我國即將接受 APG 評鑑，似短期內無法一次到位，併同消費者保護的議題完全研究透徹並納入規範，是以本文僅說明漸進式的政策進行方式，並區分短期、中期、長期能執行的政策。短期政策應會偏向於對經紀業者及交易所實施實名制，並先行以「指定之非金融事業」作為洗錢防制的標準；中期政策則會偏向由政府輔導並成立一個被認許的自律組織，由自律組織推行主管機關所訂定的法規範，力求達成實質意義上之「自律」；長期政策則講求推行能將規範場外交易平台納入規範，較簡易的實行方法之一為減少「經紀業者及交易所可能因交易架構本身而產生之風險因素」，亦即須對經紀業者及交易所進行除洗錢風險以外的風險進行監理，監理方式除以法律明文作為助力外，另有較須開發成本的方式—即開發監理科技，利用技術來連結未納入加密貨幣身分資料庫的交易者。

doi:10.6342/NTU201800740

第陸章　結語

加密貨幣近年來價格波動幅度極大，以比特幣為例，有紀錄曾顯示一單位創下超過 7000 美元的匯兌價格，因此不僅易被認為是新型的投資工具，更有可能因其後導入智能契約而有商業上的應用價值。加密貨幣在如此璀璨的前景下，近來卻因涉及吸金、洗錢、被駭客入侵等犯罪議題而蒙上一層陰影。本文認為加密貨幣作為新興金融科技下的產物，如同互聯網一樣，無可避免於發展初期時被犯罪人士所利用，惟若因此而將技術本身視為犯罪工具進而嚴加管制則不免過於可惜。蓋若採此種策略，不僅將不利我國金融科技的發展，更將使得合法使用加密貨幣之人承擔少數人的不法行為，有違公允。本文遂以加密貨幣之洗錢防制為題，針對加密貨幣洗錢議題進行深度的探討，旨在扶持產業發展的同時壓抑犯罪的產生，希冀能利用最低限度的法規範，於降加密貨幣用於洗錢風險的同時促使該產業蓬勃發展。

本文於第二章首先區分數位貨幣、電子貨幣及虛擬貨幣的概念，以利辨識加密貨幣係屬何者。研究發現加密貨幣作為虛擬貨幣的下位概念，除承繼虛擬貨幣能以數位形式呈現價值的特性外，尚具有去中心化、高流通性、所有權專屬性、帳本公開性、及匿名性等特性。上述特性對於價值移轉服務具有極大的吸引力，故為金融業所關注，卻也吸引了洗錢犯罪。進一步深入探究其原因，發現並非所有加密貨幣均能被洗錢犯罪所利用，理由在於加密貨幣具有吸引洗錢犯罪之特性會隨著所採行之虛擬貨幣架構及區塊鏈架構而有所不同，其中又以採行公鏈區塊鏈技術的全雙向流通性虛擬貨幣架構最易為洗錢犯罪所利用。

本文於第三章先以洗錢防制法的角度切入，探討加密貨幣若作為一種用於洗

doi:10.6342/NTU201800740

錢的犯罪客體是否有與現行洗錢防制法直接關聯的問題。本文發現欲達成防制加密貨幣用於洗錢，法律面應先有可行的規範依據，是以就其是否能被沒收、不法所得及孳息的追徵等議題進行討論。經本文分析發現現行法在未修法下，加密貨幣作為洗錢防制法欲規範的洗錢客體，性質應屬於「關聯客體」。對於關聯客體的沒收於洗錢防制法第 18 條已有特別規定，惟該條並未就關聯客體變得之物或財產上利益及其孳息不能沒收或不宜執行沒收時能否追徵其價額進行規範。對此本文參考學說見解認為刑法第 38 條 2 項但書及第 38-1 條但書已開放「特別規定」回歸適用刑法，以解決法律面能否沒收的問題。其後本文就法律「欲管制的交易型態」以及「欲管制的對象」為法律管制層面分析，從美國法上從事匯兌服務的交易型態區分出三種對象，分別是：使用者、交換者、以及發行者，其中使用者因並不構成「欲管制的交易型態」故不列入「欲管制的對象」。管制型態與對象確立後，本文接著按執行層面的不同階段論接著論述「辨識的執行」、「規範的執行」及「落實的執行」，試圖以主管機關的角度看待實務執行上會遇見的「斷層」，即欲將死板的洗錢防制法規範活化並套用至加密貨幣時將面臨的衝擊。

本文於第四章從抽象至具體，先就 FATF 所提供的建議進行簡化及歸納，發現「虛擬貨幣支付產品與服務」及「金錢或價值移轉服務業」為洗錢防制重點，須透過風險基礎方法由各主管機關協同評估虛擬貨幣產品或服務可能具有之風險。具體實行措施包括以多重驗證技術、第三方驗證系統等方式踐行客戶識別計畫、客戶盡職調查、加強客戶調查等確認客戶身分程序。美國法則以金融服務商下的「匯兌業者」定位 FATF 所述的「虛擬貨幣支付產品與服務」，蓋從事此類服務之加密貨幣經紀業者符合匯兌服務的交易態樣，因此受美國銀行保密法所規範。符合匯兌業者之人僅有交換者以及發行者兩者，本文就交換者更進一步深入探究，

doi:10.6342/NTU201800740

參考紐約州法 Part 200 對虛擬貨幣匯兌服務所訂定之義務，發現僅就 Part 200.15 所規定的洗錢防制義務已不下於我國課予金融機構應遵守之洗錢防制義務。為探詢我國主管機關未來的洗錢防制方向究竟是朝審慎監理抑或是非審慎監理之洗錢防制模式，最後本章以有限的資訊綜合其他「指定之非金融事業」的法規範，預估加密貨幣將來的規範方向及具體有可能採行的措施，並得出對加密貨幣匯兌行業所採行之洗錢防制措施以不超過「指定之非金融事業」的程度為當。

本文於第五章參考國家風險評估報告得出加密貨幣較容易與已識別的洗錢威脅相結合，因此認為有擬定洗錢防制策略之必要。對公鏈，本文提出以具吸引力的法律規範、由主管機關輔助成立自律組織、監理科技三種策略；對於私鏈，則提出非審慎監理、審計節點兩種策略。惟應用上述策略時尚需經過以風險為基礎方法的評估過程，是以先進行加密貨幣匯兌產業的風險評級，再利用風險評級後的結果，針對採行公鏈架構之貨幣型加密貨幣之匯兌業者擬定洗錢防制政策。最終本文對於場外交易平台採取不直接課予洗錢防制義務的政策；另建議對加密貨幣經紀業者及加密貨幣交易所二者採取短期實施實名制、中期成立一個被認許的自律組織、長期開發監理科技的洗錢防制政策。

doi:10.6342/NTU201800740

參考文獻

一、 中文部分

(一)、 書籍

1. 林山田（2008），《刑法通論（上）》，10 版，作者自版，2008 年 1 月。
2. 林山田（1987），《經濟犯罪與經濟刑法》，台北：三民書局，1987 年 5 月。

(二)、 專書論文

1. 古承宗（2017），〈洗錢刑法的正當性依據──兼論當代刑事政策的變異〉，《犯罪、資恐與洗錢：如何有效訴追犯罪？》，頁 263-307，台北：新學林，2017 年 8 月。
2. 許恒達（2017），〈洗錢防制法新修正沒收規定之檢討〉，《犯罪、資恐與洗錢：如何有效訴追犯罪？》，頁 215-262，台北：新學林，2017 年 8 月。
3. 楊雲驊、林麗瑩（2017），〈洗錢犯罪不法所得之沒收〉，《新洗錢防制法─法令遵循實務分析》，頁 51-80，台北：元照，2017 年 8 月。
4. 薛智仁（2017），〈評析洗錢罪之沒收規定〉，《犯罪、資恐與洗錢：如何有效訴追犯罪？》，頁 309-343，台北：新學林，2017 年 8 月。

(三)、 期刊

1. 王皇玉（2103），〈洗錢罪之研究—從實然面到規範面之檢驗〉，《政大法學評論》，132 期，2013 年 4 月，頁 215-260。
2. 何嘉容（2018），〈誰是實質受益人？公司法修法與洗錢防制〉，《會計研究月刊》，391 期，2018 年 6 月，頁 88。
3. 李智仁（2017），〈會發亮的不一定都是金子—FINTECH 發展的光與影〉，《月旦會計實務研究》，創刊號，2017 年 11 月，頁 70-76。
4. 李榮謙、方耀（2001），〈電子支付系統與電子貨幣：發展、影響及適當的管理架構〉，《中央銀行季刊》，23 卷 3 期，2001 年 12 月，頁 7-50。
5. 林弘斌、鄧介銘（2017），〈淺談區塊鏈技術與金融區塊鏈實作驗證〉，《財金資訊季刊》，90 期，2017 年 10 月，頁 19-27。
6. 林盟翔（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》，267 期，2017 年 7 月，頁 30-75。
7. 耿群（2006），〈日本結束量化寬鬆貨幣政策的影響分析〉，《國際金融研究》，第 5 期，2006 年 5 月，頁 4-7。

doi:10.6342/NTU201800740

8. 張兆順(由劉書甯採訪、撰文)（2017），〈國銀談法遵經驗--因應美國監理重點兆豐啟動法遵再造工程〉，《台灣銀行家》，93 期，2017 年 9 月，頁 12-15。
9. 郭秋榮（2018），〈全球金融科技之監理對我國之啟示（上）〉，《證券服務》，664 期，107 年 4 月，頁 67-80。
10. 陳恭（2017），〈區塊鏈與金融科技之發展及應用〉，《財金資訊季刊》，90 期，2017 年 10 月，頁 2-7。
11. 曾淑瑜（2016），〈論修正前後沒收轉型之爭議〉，《司法新聲》，120 期，2017 年 10 月，頁 9-27。
12. 黃士元（2017），〈偵查中保全扣押犯罪所得〉，《司法新聲》，123 期，2017 年 7 月，頁 7-39。
13. 詹德恩（2013），〈我國金融犯罪特性與抗制難題〉，《中正財經法學》，第 7 期，2013 年 7 月，頁 159-220。
14. 彰化銀行（2017），〈監理科技〉，《彰銀資料》，第 66 卷 11 期，2017 年 11 月，頁 4-7。
15. 臧正運（2017），〈區塊鏈運用對金融監理之啟示與挑戰〉，《月旦法學雜誌》，267 期，2017 年 8 月，頁 136-152。
16. 劉柏定（2017），〈區塊鏈技術與應用在中國大陸之發展近況〉，《經濟前瞻》，172 期，2017 年 7 月，頁 72-76。
17. 蔡佩玲（2017），〈國際洗錢防制發展趨勢與我國洗錢防制新法－兼論刑事政策變革〉，《刑事政策與犯罪防治研究專刊》，14 期，2017 年 10 月，頁 3-12。

(四)、 學位論文

1. 吳致勳（2015），《財產犯罪主觀要件之研究》，東吳大學法學院法律學系碩士論文，2016 年。
2. 謝建國（2016），《洗錢犯罪防制對策之研究》，中央警察大學警察政策研究所博士論文，2016 年。

(五)、 學術研討會論文集

1. 錢世傑（2017），《重要政治性職務之人(PEP)規定之合理性及其適用，洗錢防制法律與政策研討會學術論文集》，2017 年 11 月，頁 75-105。
2. 謝昆峯（2017），《洗錢防制法第七條「以風險為基礎」之意旨及執行之本土化，洗錢防制法律與政策研討會學術論文集》，2017 年 11 月，頁 51-72。

doi:10.6342/NTU201800740

(六)、 政府出版品

1. 林美達（2014），〈新入監財產犯罪受刑人統計分析〉，《矯正統計短文》，103 年 6 月，頁 1-4。
2. 法務部調查局（2013），〈洗錢防制工作年報〉，102 年，頁 1-358。
3. 法務部調查局（2016），〈經濟犯罪防制工作年報〉，105 年，頁 1-379。
4. 陳進步（2013），〈竊盜罪案件統計分析〉，《【專題分析】法律宣導》，102 年 6 月，頁 1-3。

(七)、 法院判決

1. 最高法院 81 年台上字第 2166 號判決
2. 最高法院 93 年台上 4798 號判決
3. 最高法院 93 年度台上字第 2103 號判決

(八)、 網路文獻

1. BitoEX 比特幣(BTC)價格紀錄（2018），〈BitoEX 價格紀錄表〉，https://www.e04.info/（最後瀏覽日：2018/06/14）
2. Bitoex 幣託（2017），〈「因海外交易所發生異常報價，須重新尋找基準」〉。載於：https://www.facebook.com/bitoex/posts/1997881620487506（最後瀏覽日：2018/06/14）
3. COBINHOOD 會收取多少交易手續費？載於：https://cobinhood.zendesk.com/hc/zh-tw/articles/360001593431-COBINHOOD-會收取多少交易手續費-（最後瀏覽日：2018/07/08）
4. Elliott Leung（2018/03/07），〈影帝都賣虛擬貨幣？再有虛擬貨幣眾籌騙局〉，https://unwire.pro/2018/03/07/miroskii-fake-cryptocurrency-ico/news/（最後瀏覽日：2018/07/15）
5. iThome（2016/04/23），〈區塊鏈運作原理大剖析：5 大關鍵技術〉，https://www.ithome.com.tw/news/105374（最後瀏覽日：2018/06/14）
6. iThome（2017/09/11），〈報告：ICO 吸金能力大過創投、知名眾籌平台〉，https://www.ithome.com.tw/news/116786（最後瀏覽日：2018/06/14）
7. iThome（2017/11/24），〈工研院資通所所長闕志克：真正區塊鏈應用還太少，未來區塊鏈發展方向將朝向混合鏈〉，https://www.ithome.com.tw/news/118522（最後瀏覽日：2018/06/14）
8. iThome（2018/04/12），〈各國紛紛祭出禁令防制虛擬貨幣洗錢犯罪，臺灣即將跟進，法務部擬把虛擬貨幣納入洗錢防制體系〉，https://www.ithome.com.tw/news/122370（最後瀏覽日：2018/06/14）

doi:10.6342/NTU201800740

9. iThome（2018/05/30），〈ICO 比照創櫃板群募規則？立委要求金管會一個月內提出研商結果〉，https://www.ithome.com.tw/news/123517（最後瀏覽日：2018/07/09）
10. LocalBitcoin vs BitoEx（幣託）的要價比較，參閱：比特台灣 (2017)。載於：http://www.bitcoin-tw.com/localbitcoins-vs-bitoex.html（最後瀏覽日：2018/07/15）
11. MaiCoin（2018），〈2018/06/25 MaiCoin 數位資產交易平台 公告〉。載於：https://maicoin2.freshdesk.com/zh-TW/support/solutions/articles/32000023973-2018-06-25-maicoin-數位資產交易平台-公告（最後瀏覽日：2018/06/30）
12. Maicoin（2018），〈帳號及交易安全〉。載於：https://www.maicoin.com/zh-TW/faq/security（最後瀏覽日：2018/06/14）
13. Mr.Fintech（2017），〈金融科技 ABCD 技術知多少?〉。載於：http://www.thinkfintech.tw/Article?q=ART171129001（最後瀏覽日：2018/06/14）
14. Steve Jr Lin（2018），〈【監管第一步】台灣區塊鏈業者擬組聯合自律聯盟，欲積極與政府溝通並制定產業標準〉。載於：https://www.blocktempo.com/taiwan-regulation-first-step-blockchain-industry-4/（最後瀏覽日：2018/07/15）
15. Wendy（2016），〈區塊鏈大牛們居然是這麼評價私鏈的〉。載於：巴比特資訊， http://www.8btc.com/experts-private-blockchains（最後瀏覽日：2018/06/15）
16. Yahoo 奇摩知識+，〈點數與等級〉。載於：https://tw.answers.yahoo.com/info/scoring_system（最後瀏覽日：2018/06/14）
17. Yicheng（2017），〈BITCOIN 原理與實作〉。載於：https://easonwang01.gitbooks.io/blockchain/content/chapter1.html 最後瀏覽日：2018/07/15）
18. Yicheng（2017），〈區塊鏈運作原理〉。載於：https://easonwang01.gitbooks.io/blockchain/content/block.html（最後瀏覽日：2018/07/15）
19. 三立新聞網（2016/05/04），〈虛擬換真錢！詐騙集團洗錢新招 利用「比特幣」撈 5 千多萬〉，http://www.setn.com/News.aspx?NewsID=143726（最後瀏覽日：2018/06/24）
20. 大紀元（2017/03/27），〈攔阻不法所得破億 中市打擊詐欺領先六都〉，http://www.epochtimes.com/b5/17/3/27/n8972090.htm（最後瀏覽日：2018/07/15）
21. 大紀元（2018/04/03），〈新興網路犯罪「虛擬貨幣老鼠會」恐吸金 3 億 警方要查〉， http://www.epochtimes.com/b5/18/4/3/n10274122.htm（最後瀏覽日：2018/06/21）
22. 工商時報（2015/10/22），〈Bank 4.0「去實體分行」浪潮的挑戰〉，http://www.chinatimes.com/newspapers/20151022000050-260202（最後瀏覽日：2018/07/10）
23. 工商時報（2017/04/19），〈洗錢防制 矯枉過正反擾民〉，https://m.ctee.com.tw/album/ab438efa-d245-4a92-b786-11a2cbb976ee/800282（最後瀏覽日：2018/07/08）
24. 工商時報（2018/02/05），〈金管會迎戰金融科技 將增聘監理科技人才〉，http://www.chinatimes.com/newspapers/20180205000219-260202（最後瀏覽日：2018/07/10）

doi:10.6342/NTU201800740

25. 工商時報（2018/05/07），〈法源不明 央行擬正名代幣解套〉，http://www.chinatimes.com/newspapers/20180507000176-260202（最後瀏覽日：2018/06/14）
26. 中央社（2017/10/25），〈彭淮南：比特幣應納洗錢防制管理〉，http://www.cna.com.tw/news/afe/201710250340-1.aspx（最後瀏覽日：2018/06/24）
27. 中央社（2018/04/05），〈打擊炒作 南韓出重手管制虛擬貨幣交易〉，http://www.cna.com.tw/news/afe/201712280264-1.aspx（最後瀏覽日：2018/06/14）
28. 中央社（2018/04/05），〈疑涉侵占 南韓拘留加密貨幣交易所高層〉，https://news.rti.org.tw/news/view/id/404104（最後瀏覽日：2018/06/14）
29. 中央銀行（2013/12/26），〈量化寬鬆貨幣政策〉。載於：https://www.cbc.gov.tw/public/Attachment/41161474471.pdf（最後瀏覽日：2018/07/15）
30. 中央銀行（2016/03/24），〈央行理監事會後記者會參考資料〉。載於：https://www.cbc.gov.tw/public/Attachment/632510582671.pdf（最後瀏覽日：2018/07/15）
31. 中央銀行、金融監督管理委員會（2013/12/30），〈比特幣並非貨幣，接受者務請注意風險承擔問題〉。載於：中華民國中央銀行全球資訊網，https://www.cbc.gov.tw/ct.asp?xItem=43531&ctNode=302（最後瀏覽日：2018/06/22）
32. 中時電子報（2015/01/15），〈勤業眾信法務專欄－國際洗錢防制管理制度新思維〉，http://www.chinatimes.com/newspapers/20150115000172-260205（最後瀏覽日：2018/06/30）
33. 中時電子報（2018/04/23），〈買賣比特幣就是高風險帳戶？金管會：視交易資金狀況〉，http://www.chinatimes.com/realtimenews/20180423002367-260410（最後瀏覽日：2018/06/14）
34. 中時電子報（2018/05/29），〈比特幣納管 顧立雄：要實名制與自律組織！〉，http://www.chinatimes.com/realtimenews/20180529001913-260410（最後瀏覽日：2018/07/09）
35. 中時電子報（2018/06/11），〈行政院版公司法 刪除實質受益人字眼〉，http://www.chinatimes.com/newspapers/20180611000204-260202（最後瀏覽日：2018/06/23）
36. 內政部警政署 (2016/05/11)，〈偵破陳○○為首之比特幣洗錢中心案〉。載於：http://www.hlpb.gov.tw/circulatedview.php?menu=2428&typeid=2453&circulated_id=60364（最後瀏覽日：2018/05/15）
37. 內政部警政署 (2016/05/16)，〈比特幣交易所假藉駭客入侵，詐騙客戶比特幣案〉載於：https://www.ruifang.police.ntpc.gov.tw/cp-2366-24183-25.html（最後瀏覽日：2018/05/15）
38. 王儷玲（2018），〈善用監理科技保護消費者〉。載於：遠見雜誌，https://www.gvm.com.tw/article.html?id=43093 .
39. 台灣銀行，〈如何開戶往來〉。載於：http://www.bot.com.tw/business/deposit/generaldeposit/pages/tb3114.aspx（最後瀏覽日：2018/06/14）.
40. 外交國防法務處（2017），〈防制洗錢 國家向前－我國防制洗錢策略與未來展望〉。載於：

doi:10.6342/NTU201800740

https://www.ey.gov.tw/Page/448DE008087A1971/907324a2-38db-4d75-80b9-402009242f62（最後瀏覽日：2018/07/12）
41. 安菲（2018），〈不可不知 區塊鏈的三種基本形態〉，《區塊客》。載於：http://blockcast.it/2018/02/19/public-enterprise-hybrid-blockchain/（最後瀏覽日：2018/05/14）
42. 自由時報（2016/05/04），〈比特幣成詐騙集團洗錢工具 月洗 5000 萬元〉，http://news.ltn.com.tw/news/society/breakingnews/1685234（最後瀏覽日：2018/06/24）
43. 自由時報（2017/03/23），〈洗錢防制擾民？立委爆：結婚 50 萬禮金銀行拒收〉，http://ec.ltn.com.tw/article/breakingnews/2010097（最後瀏覽日：2018/07/08）
44. 自由時報（2017/06/30），〈破比特幣洗錢中心 上億贓款被漂白〉，http://news.ltn.com.tw/news/society/paper/1114873（最後瀏覽日：2018/06/14）
45. 自由時報（2017/12/13），〈《財經觀測站》比特幣的崛起與風險〉，http://news.ltn.com.tw/news/business/paper/1159808（最後瀏覽日：2018/02/15）
46. 自由時報（2018/02/22），〈劫比特幣轉匯中國 藏鏡人疑跨國指揮〉，http://news.ltn.com.tw/news/society/paper/1178123（最後瀏覽日：2018/06/14）
47. 自由時報（2018/02/22），〈虛擬商品隱密性高 常用於洗錢難追查〉，http://news.ltn.com.tw/news/society/paper/1178124（最後瀏覽日：2018/05/14）
48. 自由時報（2018/03/02），〈投資比特幣週 20%回饋？ 警：股神都做不到別被騙！〉， http://news.ltn.com.tw/news/society/breakingnews/2354226（最後瀏覽日：2018/03/30）
49. 自由時報（2018/04/20），〈虛擬貨幣納管達共識！邱太三：將對比特幣做相當管制〉， http://news.ltn.com.tw/news/politics/breakingnews/2401194（最後瀏覽日：2018/06/14）
50. 自由時報（2018/05/16），〈公司法實質受益人漏洞 學者：恐無法通過洗錢評鑑〉， http://news.ltn.com.tw/news/business/breakingnews/2427180（最後瀏覽日：2018/06/23）
51. 自由時報（2018/06/22），〈Bithumb 遭駭價值 10 億元虛擬貨幣 韓警展開調查〉，http://ec.ltn.com.tw/article/breakingnews/2466635（最後瀏覽日：2018/07/08）
52. 行政院洗錢防制辦公室（2016），〈洗錢防制法修正條文對照表修正說明〉，http://www.amlo.moj.gov.tw/HitCounter.asp?xItem=467286&ixCuAttach=161358（最後瀏覽日：2018/06/24）
53. 行政院洗錢防制辦公室（2018），〈國家洗錢及資恐風險評估報告「金流透明 世界好評+」〉。載於：https://drive.google.com/open?id=1EaQgIeUG-M8eLkcfNbLqJho-SlRpMtD1（最後瀏覽日：2018/06/20）
54. 行政院洗錢防制辦公室成立背景：http://www.amlo.moj.gov.tw/ct.asp?xItem=464864&CtNode=45705&mp=8004（最後瀏覽日：2018/04/15）
55. 行政院洗錢防制辦公室新聞稿（2017/12/28），〈籌備工作，好還要更好〉，https://www.ey.gov.tw/File/AD5A3CDBD5F63C71?A=C（最後瀏覽日：2018/07/15）
56. 林盟翔（2018/08/16），〈虛擬通貨分級監理 產業自律探路〉，https://m.ctee.com.tw/expert/289f93d0/10190（最後瀏覽日：2018/08/17）

doi:10.6342/NTU201800740

57. 法務部調查局（2017），〈工作項目〉，https://www.mjib.gov.tw/EditPage/?PageID=cb9c3a93-6c70-4b68-bedd-4b2537dcbd27（最後瀏覽日：2018/06/09）
58. 法務部調查局（2017），〈虛擬貨幣風險基礎方法指引〉。載於：http://www.amlo.moj.gov.tw/HitCounter.asp?xItem=491315&ixCuAttach=173792（最後瀏覽日：2018/07/15）
59. 法務部調查局（2018），〈疑似洗錢或資恐交易態樣簡稱對照表(含新舊態樣對照表)107/3/1 後適用〉。載於：https://www.mjib.gov.tw/userfiles/files/35-洗錢防制處/files/可疑交易申報專區/check_list.pdf（最後瀏覽日：2018/07/11）
60. 金融監督管理委員會（2015），〈未來民眾開立存款帳戶，可以直接透過網路線上申辦〉。載於：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0%2C2&mcustomize=news_view.jsp&dataserno=201510270006&aplistdn=ou&toolsflag=Y&dtable=News（最後瀏覽日：2018/06/26）
61. 金融監督管理委員會（2016），《金融科技發展策略白皮書》，https://www.fsc.gov.tw/uploaddowndoc?file=news%2F201605181357350.pdf（最後瀏覽日：2018/07/10）
62. 金融監督管理委員會（2017），〈金管會再次提醒社會大眾投資比特幣等虛擬商品的風險〉。載於：https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0%2C2&mcustomize=news_view.jsp&dataserno=201712190002&aplistdn=ou&dtable=News（最後瀏覽日：2018/06/14）
63. 金融監督管理委員會（2017），〈遠東國際商業銀行 SWIFT 系統遭駭重大偶發事件所涉缺失，違反銀行法第 45 條之 1 第 1 項規定，核處新臺幣 800 萬元罰鍰〉。載於：https://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2&mcustomize=multimessage_view.jsp&dataserno=201712180001&toolsflag=Y&dtable=Penalty（最後瀏覽日：2018/06/14）
64. 金融監督管理委員會（2018），〈金融控股公司及銀行業內部控制及稽核制度實施辦法 條文對照表〉。載於：http://law.fsc.gov.tw/law/LawContent.aspx?id=FL049894（最後瀏覽日：2018/07/04）
65. 金融監督管理委員會（2018），〈修正「金融控股公司及銀行業內部控制及稽核制度實施辦法」部分條文〉，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201803200002&toolsflag=Y&dtable=News（最後瀏覽日：2018/07/04）
66. 信傳媒（2018/05/07），〈麻吉大哥的秘銀幣捲入侵占爭議 台灣虛擬貨幣確定走向管制派〉，https://www.cmmedia.com.tw/home/articles/9775（最後瀏覽日：2018/06/14）
67. 姜統掌（2018/04/02），〈FinTech 核心：普惠金融、監理科技〉，http://www.ecf.com.tw/tw/article/show.aspx?num=149（最後瀏覽日：2018/07/09）

doi:10.6342/NTU201800740

68. 恒豐國際娛樂平台（2017）〈《直播職業 10 月陳述》直播收入榜發佈：花椒主播最掙錢〉，http://www.hzhonghao.com/news/gsxw/15.html（最後瀏覽日：2018/06/14）
69. 科技產業資訊室（2008），〈政策與政策流程思考〉。載於 http://cdnet.stpi.narl.org.tw/techroom/analysis/2008/pat_08_A019.htm（最後瀏覽日：2018/07/12）
70. 科技新報（2018/01/05），〈罪犯不再熱愛比特幣，門羅幣成新寵〉，https://technews.tw/2018/01/05/criminal-drop-bitcoin-to-monero/（最後瀏覽日：2018/06/14）
71. 科技新報（2018/05/02），〈加密貨幣洗錢防制，實名制是共識〉，http://technews.tw/2018/05/02/cryptocurrency-money-control/（最後瀏覽日：2018/06/14）
72. 科技橘報（2018/01/29），〈【整個平台被盜光光】史上最大虛擬貨幣被駭案，日本交易所損失 124 億台幣〉，https://buzzorange.com/techorange/2018/01/29/japan-coincheck-hacked-all-money-gone/（最後瀏覽日：2018/07/08）
73. 孫欣、章友馨（2018），〈金融機構法令遵循風險評估與法規資料庫〉。載於：https://home.kpmg.com/tw/zh/home/insights/2018/01/law-compliance-risk-assessment-and-regulations-database.html（最後瀏覽日：2018/07/04）
74. 財經新報（2017/07 月 10 日），〈比特幣是「新黃金」，價格飆將飆至 5.5 萬美元？〉，https://finance.technews.tw/2017/07/10/bitcoin-new-gold（最後瀏覽日：2018/06/20）
75. 商業周刊（2017/11/27），〈2017 IBM Forum 科技賦能--擅用科技，助人類超越極限〉，https://www.businessweekly.com.tw/article.aspx?id=34037&type=Indep（最後瀏覽日：2018/07/10）
76. 國泰世華（2017），〈數位存款帳戶帳戶類型--國泰世華商業銀行數位存款帳戶特別約定條款〉。載於：https://www.kokobank.com/KOKO/Content/HTML/dsa_term.html(最後瀏覽日：2018/06/27）
77. 張庭瑜（2018/02/26），〈投資 ICO 致富夢一場，調查：去年近半數專案宣告失敗〉， https://www.bnext.com.tw/article/48305/46-last-years-icos-failed（最後瀏覽日：2018/06/14）
78. 張漢宜（2011），〈美國反洗錢，衝擊全球金融〉，《天下雜誌》，373 期。載於：https://www.cw.com.tw/article/article.action?id=5003762（最後瀏覽日：2018/04/14）
79. 許家華(2017)，〈北韓駭客搞的鬼？南韓比特幣交易所 YOUBIT 二度遭駭 聲請破產〉。載於：鉅亨網，https://news.cnyes.com/news/id/3995934（最後瀏覽日：2018/06/14）
80. 郭戎晉(2015)，〈從國際趨勢談金融科技(FinTech)與 Bank 4.0 推動策略〉。載於：http://www.tfsr.org.tw/Uploads/files/201511%20 從國際趨勢談金融科技(FinTech)與 Bank%204_0 推動策略_郭戎晉組長.pdf（最後瀏覽日：2018/08/05）

doi:10.6342/NTU201800740

81. 郭朝益（2007/07/08），〈同作控制(Concurrency Control) - 簡介〉。載於：http://postgresql-chinese.blogspot.tw/2007/02/concurrency-control.html（最後瀏覽日：2018/06/14）
82. 愛德華・卡斯特羅諾瓦（2018），《《虛擬貨幣經濟學》：實體經濟有三大缺陷，虛擬貨幣讓人更快樂 》。載於：https://www.thenewslens.com/article/89423（最後瀏覽日：2018/06/14）
83. 楊金龍（2018/08/07），〈虛擬貨幣與數位經濟與數位經濟：央行在數位時代的角色〉。載於：中央銀行，https://www.cbc.gov.tw/public/Attachment/888144602.pdf（最後瀏覽日：2018/08/10）
84. 經濟日報（2018/06/04），〈比特幣納管 設三防線〉，https://money.udn.com/money/story/5613/3178180（最後瀏覽日：2018/06/21）
85. 經濟日報（2018/06/04），〈比特幣納管主管機關...待政院指定〉，https://udn.com/news/story/7239/3178182（最後瀏覽日：2018/07/01）
86. 經濟日報（2018/06/12），〈比特幣又被駭 引發拋售潮〉，https://udn.com/news/story/6811/3193368（最後瀏覽日：2018/07/08）
87. 鉅亨網新聞中心（2017/12/12），〈網紅經濟有多賺？6 歲網紅直播主年收入破千萬美金〉， https://news.cnyes.com/news/id/3987511（最後瀏覽日：2018/06/14）
88. 幣託(2018)，〈【官方公告：請提升至 B 級用戶才能到全家購買比特幣】〉。載於： https://www.facebook.com/bitoex/posts/2089049798037354(最後瀏覽日：2018/06/30）
89. 幣託，〈身份驗證與功能限制〉載於，https://www.bitoex.com/constrains?locale=zh-tw（最後瀏覽日：2018/06/30）
90. 數位時代（2018/01/12），〈韓國大媽要哭了，南韓政府將立法禁止虛擬貨幣交易〉，https://www.bnext.com.tw/article/47776/south-korea-ban-bitcoin-cryptocurrency-trading-2018（最後瀏覽日：2018/07/15）
91. 調查局（2017），〈FATF 評鑑方法論(中文)〉。載於：http://www.amlo.moj.gov.tw/HitCounter.asp?xItem=491310&ixCuAttach=173787（最後瀏覽日：2018/06/14）
92. 聯合報（2017/06/21），〈台灣詐團全球跑 出國坐牢沒在怕〉，https://theme.udn.com/theme/story/6774/2536427（最後瀏覽日：2018/07/15）
93. 聯合報（2018/01/10），〈第 3 類數位帳戶不能轉帳 王道銀批荒謬〉，，https://udn.com/news/story/7239/2922933（最後瀏覽日：2018/06/14）
94. 聯合報（2018/01/16），〈財經觀點／加速金融革新 應善用「混合鏈」 〉，https://udn.com/news/story/11316/2933722（最後瀏覽日：2018/06/14）
95. 聯合報（2018/01/23），〈比特幣交易商列高風險 且不能從事網銀業務〉，https://money.udn.com/money/story/5641/2945930（最後瀏覽日：2018/06/14）
96. 聯合新聞網（2016/12/29），〈石油爭霸底定 「新貨幣戰」開打！〉，https://fund.udn.com/fund/story/7488/2198963（最後瀏覽日：2018/06/30）
97. 聯合新聞網（2018/07/06），〈力拚洗錢防制評鑑 公司申報最快 8 月生效〉，https://udn.com/news/story/7238/3238629（最後瀏覽日：2018/07/08）
98. 聯合新聞網（2018/07/06），〈公司法三讀後 69 萬家公司快做這件事 公司法三讀通過〉， https://udn.com/news/story/7238/3239049(最後瀏覽日：2018/07/07）

doi:10.6342/NTU201800740

99. 簡書（2017），〈LocalBitcoins 費用〉，https://www.jianshu.com/p/7c271a096db8（最後瀏覽日：2018/07/15）
100. 蘋果日報（2016/11/15），〈林鈺雄：洗錢擴大沒收才能正本清源〉，http://www.appledaily.com.tw/realtimenews/article/new/20161115/988896/（最後瀏覽日：2018/07/15）
101. 蘋果日報（2017/10/16），〈全台第一家　用比特幣也能喝咖啡買麵包〉，http://www.appledaily.com.tw/realtimenews/article/new/20171016/1223378/（最後瀏覽日：2018/06/20）
102. 蘋果日報（2018/01/10），〈比特幣改變世界　楊金龍：正評估發行法定數位貨幣優點及挑戰〉，https://tw.appledaily.com/new/realtime/20180110/1275886/（最後瀏覽日：2018/06/14）
103. 蘋果日報（2018/02/02），〈館長爆實況主收入「直播電玩可賺 50 萬」〉，https://tw.appledaily.com/new/realtime/20180202/1290788/（最後瀏覽日：2018/06/14）
104. 魔獸世界（2018/04/29），〈魔獸代幣 - 問答集〉。載於：https://worldofwarcraft.com/zh-tw/news/18141101/introducing-the-wow-token（最後瀏覽日：2018/07/15）

doi:10.6342/NTU201800740

二、 英文部分

(一)、 Cases

1. Ripple Labs, Inc. v. Lacore Enterprises, LLC, Motion for Preliminary Injunction, 13-cv-5974-RS/KAW (N.D. Cal. 2013).
2. United States v. Roger Ver, CR 1-20127-JF (N.D. Cal.2002).

(二)、 Books, Reports, and Other Nonperiodic Materials

1. ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES (2015).
2. AUSTRALIAN TRANSACTION REPORTS AND ANALYSIS CENTRE, ONGOING CUSTOMER DUE DILIGENCE (OCDD), http://www.austrac.gov.au/sites/default/files/documents/ongoing_customer_due_diligence_1.pdf. (last visited July 4, 2018).
3. BANK FOR INT'L SETTLEMENTS, DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENT, CLEARING AND SETTLEMENT: AN ANALYTICAL FRAMEWORK (2017), https://www.bis.org/cpmi/publ/d157.pdf.
4. BASEL COMM. ON BANKING SUPERVISION, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS (2005), https://www.bis.org/publ/bcbs113.pdf.
5. BD. OF GOVERNORS OF THE FED. RESERVE SYS., SR 08-8 / CA 08-11: COMPLIANCE RISK MANAGEMENT PROGRAMS AND OVERSIGHT AT LARGE BANKING ORGANIZATIONS WITH COMPLEX COMPLIANCE PROFILES (2008), https://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.
6. CHARLES BRENNAN & WILLIAM LUNN, BLOCKCHAIN THE TRUST DISRUPTER (2016), https://www.finextra.com/finextra-downloads/newsdocs/document-1063851711.pdf.
7. CHARTERED ACCT. AUSTRALIA & NEW ZEALAND, THE FUTURE OF BLOCKCHAIN: APPLICATIONS AND IMPLICATIONS OF DISTRIBUTED LEDGER TECHNOLOGY (2017), https://www2.deloitte.com/content/dam/Deloitte/au/Documents/Economics/deloitte-au-economics-future-inc-caanz-blockchain-010217.pdf.
8. CHRISTIAN MULLER & DALMIR HASIC, BLOCKCHAIN: TECHNOLOGY AND APPLICATIONS (2016), http://www.softwareresearch.net/fileadmin/src/docs/teaching/SS16/Seminar/Seminar_Paper_Hasic_Mueller.pdf.
9. CLAUDIO SCARDOVI, RESTRUCTURING AND INNOVATION IN BANKING (2016).
10. COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, DIGITAL CURRENCIES (2015), https://www.bis.org/cpmi/publ/d137.pdf.
11. DONG HE ET AL., VIRTUAL CURRENCIES AND BEYOND: INITIAL CONSIDERATIONS (International Monetary Fund ed. 2016), http://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.
12. EDWARD CASTRONOVA, WILDCAT CURRENCY: HOW THE VIRTUAL MONEY REVOLUTION IS TRANSFORMING THE ECONOMY (2015).
13. EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES (Oct. 2012), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.
14. EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES - A FURTHER ANALYSIS (2015), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.
15. EVANGELOS BENOS, ROD GARRATT & PEDRO GURROLA-PEREZ, THE ECONOMICS OF DISTRIBUTED LEDGER TECHNOLOGY FOR SECURITIES SETTLEMENT (2017), https://www.philadelphiafed.org/-/media/bank-resources/supervision-and-regulatio

doi:10.6342/NTU201800740

n/events/2017/fintech/resources/economics-distributed-ledger-technology-for-securities-settlement.pdf?la=en.
16. FED. DEPOSIT INS. CORPORATION, BANK SECRECY ACT, ANTI-MONEY LAUNDERING, AND OFFICE OF FOREIGN ASSETS CONTROL SECTION 8.1, https://www.fdic.gov/regulations/safety/manual/section8-1.pdf (last visited July 21, 2018).
17. Frederik Armknecht et al., *Ripple: Overview and Outlook, in* 9229 TRUST AND TRUSTWORTHY COMPUTING: 8TH INTERNATIONAL CONFERENCE, TRUST 2015, HERAKLION, GREECE, AUGUST 24-26, 2015, PROCEEDINGS 163, 163-80 (Mauro Conti, Matthias Schunter & Ioannis Askoxylakis eds. 2015), http://dx.doi.org/10.1007/978-3-319-22846-4_10.
18. FIN. ACTION TASK FORCE, ATTACHMENT A: STATEMENT OF FACTS AND VIOLATIONS (2014), https://www.fincen.gov/sites/default/files/shared/Ripple_Facts.pdf.
19. FIN. ACTION TASK FORCE, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS (July 2018), http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf.
20. FIN. CRIMES ENF'T NETWORK , FIN-2008-G008 USA PATRIOT ACT, APPLICATION OF THE DEFINITION OF MONEY TRANSMITTER TO BROKERS AND DEALERS IN CURRENCY AND OTHER COMMODITIES (2008), https://www.fincen.gov/sites/default/files/guidance/fin-2008-g008.pdf.
21. FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
22. FIN. CRIMES ENF'T NETWORK, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY (2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf.
23. FIN. CRIMES ENF'T NETWORK, FIN-2014-R012, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY PAYMENT SYSTEM (2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf.
24. FIN. CRIMES ENF'T NETWORK, *FinCEN's Letter to U.S. Senator Ron Wyden*, COINCENTER.ORG, (Feb. 13, 2018) https://coincenter.org/files/2018-03/fincen-ico-letter-march-2018-coin-center.pdf.
25. FIN. CRIMES ENF'T NETWORK, FINCEN FORM 105 - CURRENCY AND OTHER MONETARY INSTRUMENTS REPORT (2011), https://www.fincen.gov/sites/default/files/administrative_ruling/fin-2011-r001.pdf.
26. FIN. ACTION TASK FORCE, FUNDS "TRAVEL" REGULATIONS: QUESTIONS & ANSWERS (1997), https://www.sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf.
27. FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL CURRENCIES (June 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.
28. FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION (Feb. 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

doi:10.6342/NTU201800740

29. G20 FIN. MINISTERS & CENT. BANK GOVERNORS MEETING, COMMUNIQUÉ (July 21, 2018), https://g20.org/sites/default/files/media/communique-_fmcbg_july.pdf.
30. Gareth W. Peters & Efstathios Panayi, *Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, *in* BANKING BEYOND BANKS AND MONEY: A GUIDE TO BANKING SERVICES IN THE TWENTY-FIRST CENTURY, 239 (Paolo Tasca, Tomaso Aste, Loriana Pelizzon & Nicolas Perony eds., 2015).
31. GUY STESSENS, MONEY LAUNDERING: A NEW INTERNATIONAL LAW ENFORCEMENT MODEL (2008).
32. INST. INT'L FIN., REGTECH IN FINANCIAL SERVICES: TECHNOLOGY SOLUTIONS FOR COMPLIANCE AND REPORTING (2016), https://www.iif.com/system/files/regtech_in_financial_services_-_solutions_for_compliance_and_reporting.pdf.
33. JEAN-LOUP RICHET, LAUNDERING MONEY ONLINE: A REVIEW OF CYBERCRIMINALS' METHODS (2013), https://arxiv.org/ftp/arxiv/papers/1310/1310.2368.pdf.
34. JOHN P. PODOLANKO ET AL., COUNTERING DOUBLE-SPEND ATTACKS ON BITCOIN FAST-PAY TRANSACTIONS (2017), http://www.ieee-security.org/TC/SPW2017/ConPro/papers/podolanko-conpro17.pdf.
35. KRZYSZTOF OKUPSKI, BITCOIN DEVELOPER REFERENCE: WORKING PAPER (2016), https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf.
36. MARTIJN BASTIAAN, PREVENTING THE 51%-ATTACK: A STOCHASTIC ANALYSIS OF TWO PHASE PROOF OF WORK IN BITCOIN (2015), https://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf.
37. MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (2015).
38. MORDECHAI GURI, BEATCOIN: LEAKING PRIVATE KEYS FROM AIR-GAPPED CRYPTOCURRENCY WALLETS, BEN-GURION UNIVERSITY OF THE NEGEV (Apr. 23, 2018), https://arxiv.org/pdf/1804.08714.pdf.
39. RAGHU RAMAKRISHNAN & JOHANNES GEHRKE, DATABASE MANAGEMENT SYSTEMS (2d. ed. 2003).
40. RAMEZ ELMASRI & SHAM NAVATHE, FUNDAMENTALS OF DATABASE SYSTEMS (2010).
41. RENA S. MILLER, LIANA W. ROSEN & JAMES K. JACKSON, CONGRESSIONAL RESEARCH SERVICE, TRADE-BASED MONEY LAUNDERING: OVERVIEW AND POLICY ISSUES (2016), http://goodtimesweb.org/industrial-policy/2016/R44541.pdf.
42. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, https://bitcoin.org/bitcoin.pdf (last visited July 16, 2018).
43. UK GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.
44. U.S. DEP'T JUST., DRUG ENF'T ADMIN., 2017 NATIONAL DRUG THREAT ASSESSMENT DEA-DCT-DIR-040-17 (2017), https://www.dea.gov/sites/default/files/docs/DIR-040-17_2017-NDTA.pdf.
45. WORK BANK, DISTRIBUTED LEDGER TECHNOLOGY (DLT) AND BLOCKCHAIN (2017), http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf.

doi:10.6342/NTU201800740

(三)、 Periodical Materials

1. Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L.J. 139, 145 (2016).
2. Connor Gamble, *The Legality and Regulatory Challenges of Decentralised Crypto-Currency: A Western Perspective*, 20 INT'L TRADE & BUS. L. REV. 346 (2017).
3. Greeshma R. Nair & Shoney Sebastian, *BlockChain Technology Centralised Ledger to Distributed Ledger*, 4 INT'L RES. J. ENG'G & TECH. 2823 (2017), https://www.irjet.net/archives/V4/i3/IRJET-V4I3711.pdf.
4. Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network*, 13 NW. J. TECK. & INTELL. PROP. 37 (2015).
5. Laura D. Pond, *Schrödinger's Currency: How Virtual Currencies Complicate the RIC and REIT Qualification Requirements*, 9 Colum. J. Tax L. 229, 240-241 (2018).
6. Philip Koshy et al., *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, 8437 FIN. CRYPTOGRAPHY & DATA SEC. 469 (2014).
7. Ye Guo & Chen Liang, *Blockchain Application and Outlook in The Banking Industry*, 2:24 FIN. INNOVATION 1 (2016), https://jfin-swufe.springeropen.com/track/pdf/10.1186/s40854-016-0034-9.

(四)、 International Materials

1. Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the Taking Up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions 2000/46/EC, 2000 O.J. (L 275) 39, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0046&from=EN.
2. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Nov. 15, 2000, S. Treaty Doc. No. 108-16 (2004), 2237 U.N.T.S. 319, http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.
3. United Nations Convention against Corruption, G.A. Res. 58/4, U.N. Doc, A/58/4 (Dec. 9, 2003).
4. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, U.N. Doc. E/Conf. 82/16 (Dec. 19, 1988), *reprinted in* 28 I.L.M. 493 (1989).
5. United Nations Convention against Transnational Organized Crime, G.A. Res. 55/25, U.N. Doc. A/RES/55/25 (Jan. 8, 2001).

(五)、 Internet Resources

1. *Administrative Rulings*, FINCEN, U.S. DEP'T TREASURY, https://www.fincen.gov/resources/statutes-regulations/administrative-rulings (last visited July 15, 2018).
2. *All Cryptocurrencies*, COINMARKETCAP, https://coinmarketcap.com/all/views/all/ (last visited June 20, 2018).

doi:10.6342/NTU201800740

3. Axel Bugge, *Dark Web Drug Market Growing Rapidly in Europe: Report*, REUTERS (Nov. 29, 2017), https://www.reuters.com/article/us-europe-drugs-darkweb/dark-web-drug-market-growing-rapidly-in-europe-report-idUSKBN1DS28A.
4. *Bitcoin - Statistics & Facts*, STATISTA.COM, https://www.statista.com/topics/2308/bitcoin/ (last visited July 15, 2018).
5. *Bitcoin Terms & Conditions*, EXPEDIA, https://www.expedia.com/Checkout/BitcoinTermsAndConditions (last visited July 15, 2018).
6. *Bitcoin Trading Volume*, BITCOINITY.ORG, https://data.bitcoinity.org/markets/volume/5y?c=e (last visited June 30, 2018).
7. *BitLicense Regulatory Framework*, NY DEP'T FIN. SERV., https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm. (last visited June 21, 2018).
8. *Blockchain Evolution: from 1.0 to 4.0*, MEDIUM (Dec. 7, 2017), https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666.
9. *Country Comparison Taiwan vs United States 2018*, COUNTRYECONOMY.COM, https://countryeconomy.com/countries/compare/taiwan/usa (last visited July 15, 2018).
10. Cryptomaniac, *4 Categories of Cryptocurrency You Should Know*, CRYPTOVERZE.COM (Apr. 2018) https://cryptoverze.com/cryptocurrency-categories/.
11. *Currency and Monetary Instruments - Amount That Can be Brought into or Leave the U.S.*, U.S. CUSTOMS AND BORDER PROTECTION (June 16, 2016), https://help.cbp.gov/app/answers/detail/a_id/195/.
12. *Cybercrime Will Cost Businesses Over $2 Trillion By 2019*, JUNEIPER RESEARCH, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion (last visited Nov. 14, 2017).
13. *Database Mirroring and Replication (SQL Server)*, MICROSOFT DOCS (Mar. 14, 2017), https://docs.microsoft.com/en-us/sql/database-engine/database-mirroring/database-mirroring-and-replication-sql-server.
14. David Gilson, *What are Namecoins and .bit Domains?* COINDESK (June 18, 2013), http://www.coindesk.com/what-are-namecoins-and-bit-domains.
15. *Description: Frequently Asked Questions (updated): Final Customer Identification Program Rule*, OFF. COMPTROLLER CURRENCY, U.S. DEP'T TREASURY (Apr. 28, 2005), https://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-16.html.
16. *DFS Grants Virtual Currency License to Bitpay*, NY DEP'T FIN. SERV., (July 16, 2018), https://www.dfs.ny.gov/about/press/pr1807161.htm.
17. Elise Moreau, *13 Major Retailers and Services That Accept Bitcoin*, LIFEWIRE (Aug. 6, 2018), https://www.lifewire.com/big-sites-that-accept-bitcoin-payments-3485965.
18. Fred Imbert, *Blackrock Ceo Larry Fink Calls Bitcoin an 'Index Of Money Laundering'*, CNBC (Oct. 13, 2017), https://www.cnbc.com/2017/10/13/blackrock-ceo-larry-fink-calls-bitcoin-an-index-of-money-laundering.html.
19. Gabriela Barkho, *Why a Top Cryptocurrency Exchange is Technically Illegal in New York City*, INVERSE (Jan. 17, 2018),

doi:10.6342/NTU201800740

https://www.inverse.com/article/40144-binance-bitlicense-bitcoin-cryptocurrency-exchange-new-york-city.
20. *Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015*, GARTNER (Sept. 23, 2015), https://www.gartner.com/newsroom/id/3135617.
21. Gideon Greenspan, *Ending The Bitcoin vs Blockchain Debate: Is there any Value in a Blockchain without a Cryptocurrency?* MULTICHAIN (July 19, 2015), https://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/.
22. Harry Terris, *Banks to Spend More on Tech in 2016 - Especially Security*, AMERICAN BANKER (Oct. 15 2015, 10:00 P.M), https://www.americanbanker.com/news/banks-to-spend-more-on-tech-in-2016-especially-security.
23. *How Bitcoin Transactions Work*, BITCOIN.COM (June 8, 2017), https://www.bitcoin.com/info/how-bitcoin-transactions-work.
24. *How Do Bitcoin Transactions Work?* COINDESK (Jan. 29, 2018), https://www.coindesk.com/information/how-do-bitcoin-transactions-work/.
25. *How to Buy Bitcoins?* LOCALBITCOINS.COM, https://localbitcoins.com/guides/how-to-buy-bitcoins (last visited July 11, 2018).
26. *How to Sell Bitcoins?* LOCALBITCOINS.COM, https://localbitcoins.com/guides/how-to-sell-bitcoins (last visited July 11, 2018).
27. Ian Allison, *Ethereum Reinvents Companies with Launch of The DAO*, INT'L BUS. TIMES UK (Apr. 30, 2016, 8:49 PM), https://www.ibtimes.co.uk/ethereum-reinvents-companies-launch-dao-1557576.
28. James Cook, *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*, BUSINESS INSIDER (Nov. 6, 2014, 10:56 AM), http://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11.
29. John W. Schoen, *This Chart Shows Bitcoin's Meteoric Rise over the Last 6 Years*, CNBC (Nov. 29, 2017) https://www.cnbc.com/2017/11/29/this-chart-show-bitcoins-meteoric-rise-over-the-last-6-years.html.
30. Jon Buck, *Bitcoin Low Risk for Money Laundering, High For Cybercrime: UK Treasury*, COINTELEGRAPH (Oct. 29, 2017), https://cointelegraph.com/news/bitcoin-low-risk-for-money-laundering-high-for-cybercrime-uk-treasury.
31. Jon Russell, *Telegram has Raised an Initial $850M for its Billion-Dollar,* ICO TECHCRUNCH (Feb. 17, 2018), https://techcrunch.com/2018/02/16/telegram-ico-850-million/.
32. Jon Southurst, *Only Permissioned Blockchains Can Transform Finance, Says Chain's Ludwin*, BITCOINIST.COM (Oct. 26, 2016, 04:37 AM), http://bitcoinist.com/permissioned-blockchains-finance-ludwin/.
33. Jonas Chokun, *Who Accepts Bitcoins As Payment? List of Companies*, 99 BITCOINS (June 18, 2018, 5:12 PM), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.
34. Justin O'Connell, *What Are the Use Cases for Private Blockchains? The Experts Weigh In*, BITCOIN MAG. (June 20, 2016), https://bitcoinmagazine.com/articles/what-are-the-use-cases-for-private-blockchains-the-experts-weigh-in-1466440884/.
35. Kai Sedgwick, *Bitcoin by Numbers: 21 Statistics That Reveal Growing Demand for the Cryptocurrency*, BITCOIN.COM (Nov. 11, 2017),

doi:10.6342/NTU201800740

https://news.bitcoin.com/bitcoin-numbers-21-statistics-reveal-growing-demand-cryptocurrency/.
36. Kenneth Rapoza, *Goldman Sachs Caves: Bitcoin is Money*, FORBES (Jan. 10, 2018, 11:15 AM), https://www.forbes.com/sites/kenrapoza/2018/01/10/goldman-sachs-caves-bitcoin-is-money/.
37. Kevin Helms, *How Bitcoin Companies Can Legally Operate in Switzerland*, BITCOIN NEWS (Feb. 1, 2017), https://news.bitcoin.com/bitcoin-companies-legally-operate-switzerland/.
38. Kimberly Amadeo, *Strength and Power of the US Dollar---3 Reasons Why the U.S. Dollar is So Powerful*, THE BALANCE.COM (Feb. 19, 2018), https://www.thebalance.com/power-of-the-u-s-dollar-3306267.
39. Kiran Vaidya, *Decoding the Enigma of Bitcoin*, MINING MEDIUM (Dec. 15, 2016), https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2.
40. *LocalBitcoins Fees?* LOCALBITCOINS.COM, https://localbitcoins.com/fees (last visited July 11, 2018).
41. Matt Egan, *What is the Dark Web, What is the Deep Web, and How Can You Access It?*, TECH ADVISOR (Apr. 6, 2018), https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/.
42. Matthias Williams, *Ukraine Kidnappers Free Bitcoin Analyst After $1 Million Ransom Paid*, REUTERS (Dec. 30, 2017), https://www.reuters.com/article/us-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-mln-ransom-paid-idUSKBN1EN1QB.
43. Michael Castillo, *The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*, COINDESK (June 17, 2016, 2:00 PM), https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/.
44. Michael Copeland, *The Difference Between AI, Machine Learning, and Deep Learning?*, NVIDIA (July 29, 2016), https://blogs.nvidia.com/blog/2016/07/29/whats-difference-artificial-intelligence-machine-learning-deep-learning-ai/.
45. Michael Scott, *The Essence of the Blockchain*, MIRACL, https://www.miracl.com/press/the-essence-of-the-blockchain (last visited July 15, 2018).
46. *MySQL 5.7 Reference Manual 21.6.11 NDB Cluster Replication Conflict Resolution*, MYSQL, https://dev.mysql.com/doc/refman/5.7/en/mysql-cluster-replication-conflict-resolution.html (last visited June 14, 2018).
47. Nelson Wells et al., *Best Cryptocurrency Exchanges: The Ultimate Guide*, BLOCKGEEKS, https://blockgeeks.com/guides/best-cryptocurrency-exchanges/ (last visited July 11, 2018).
48. *NEM (XEM) Price, Charts, Market Cap, and Other Metrics*, COINMARKETCAP, https://coinmarketcap.com/currencies/nem/ (last visited July 8, 2018).
49. Noelle Acheson, *How Bitcoin Mining Works*? COINDESK (Jan. 29, 2018), https://www.coindesk.com/information/how-bitcoin-mining-works/.
50. *Office of Intelligence and Analysis*, DEP'T HOMELAND SEC. (July 13, 2018), https://www.dhs.gov/office-intelligence-and-analysis.
51. Ofir Beigel, *What is Bitcoin Mining and is it Profitable in 2018?* 99BITCOINS, (Aug. 8, 2018, 5:18 PM), https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/.
52. Olga Kharif, *The Criminal Underworld Is Dropping Bitcoin for Another Currency*, BLOOMBERG.COM (Jan. 3, 2018, 4:20 AM),

doi:10.6342/NTU201800740

https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.
53. Pete Rizzo, *Ghash.io: We Will Never Launch a 51% Attack Against Bitcoin*, COINDESK (June 17, 2014, 11:22 AM), https://www.coindesk.com/ghash-io-never-launch-51-attack/.
54. *Pool Distribution (calulate by blocks) Pool Stats*, BTC.COM, https://btc.com/stats/pool?pool_mode=all (last visited July 15, 2018).
55. Qin Chen, *This is How You Can Protect Your Cryptocurrencies from Hackers*, CNBC (Nov. 3, 2017), https://www.cnbc.com/2017/11/02/heres-how-to-protect-your-bitcoin-and-ethereum-from-hacking.html.
56. Ramesh Gopinath, *Checking the Ledger: Permissioned vs. Permissionless Blockchains*, IBM (July 28, 2016), https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-blockchains/.
57. Raul, *The Bitcoin Economy, in Perspective*, HOWMUCH.NET (June 21, 2017), https://howmuch.net/articles/worlds-money-in-perspective.
58. *RegTech*, FCA UK, https://www.fca.org.uk/firms/regtech (last updated June 28, 2018).
59. Robert Hackett, Jeff John Roberts & Jen Wieczner, *The Ledger: Is New York's BitLicense an 'Absolute Failure?'*, FORTUNE (May 25, 2018), http://fortune.com/2018/05/25/the-ledger-cryptocurrency-bitlicense/.
60. Ryan Browne, *Hackers Have Cashed Out on $143,000 of Bitcoin From the Massive Wannacry Ransomware Attack*, CNBC (Aug. 3, 2017, 11:09 AM), https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-bitcoin-from-the-massive-wannacry-ransomware-attack.html
61. *Setting Up Advertisements to Buy and Sell Bitcoins*, LOCALBITCOINS.COM, https://localbitcoins.com/guides/how-to-sell-bitcoins-online (last visited June 30, 2018).
62. *Size of the Bitcoin blockchain from 2010 to 2018*, STATISTA.COM, https://www.statista.com/topics/2308/bitcoin/ (last visited Aug. 15, 2018).
63. Steve Morgan, *Bank of America's Unlimited Cybersecurity Budget Sums Up Spending Plans In A War Against Hackers*, FORBES (Jan. 27, 2016), https://www.forbes.com/sites/stevemorgan/2016/01/27/bank-of-americas-unlimited-cybersecurity-budget-sums-up-spending-plans-in-a-war-against-hackers/#68d0c7a3264c.
64. *Terrorism and Financial Intelligence*, U.S. DEP'T TREASURY, https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx (last updated Dec. 2, 2010).
65. *The Ultimate Guide to Understanding Blockchain Technology*, BLOCKCHAIN TECHNOLOGIES, https://www.blockchaintechnologies.com/blockchain-technology/ (last visited Aug. 12, 2018).
66. *Transaction*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Transaction (last updated Aug. 7, 2018).
67. *WannaCry Ransomware Bitcoins Move from Online Wallets*, BBC (Aug. 3, 2017), http://www.bbc.com/news/technology-40811972.
68. *What is Cryptocurrency: Everything You Need To Know [Ultimate Guide]*, BLOCKGEEKS, https://blockgeeks.com/guides/what-is-cryptocurrency/ (last visited July 11, 2018).

doi:10.6342/NTU201800740

69. *What is Mining?* ANTMINER DISTRIBUTION EUROPE B.V., https://www.antminerdistribution.com/what-is-bitcoin-mining/ (last visited Aug. 12, 2018).
70. *What You Need to Know about the WannaCry Ransomware*, SYMANTEC (Oct. 23, 2017), https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.
71. William Suberg, *Bitcoin Enters Top 5 Google Searches, Ethereum at 18*, COINTELEGRAPH (May 23, 2017), https://cointelegraph.com/news/bitcoin-enters-top-5-google-searches-ethereum-at-18.
72. *World Cybersecurity Market Will Grow by $100B in Five Years*, RT INTERNATIONAL (Sept. 12, 2015), https://www.rt.com/usa/315147-cybersecurity-market-growth-boom/.

doi:10.6342/NTU201800740