國立臺灣大學進修推廣學院事業經營法務碩士在職學位學程

碩士論文

Professional Master's Program of Law in Business Administration School of Professional Education and Continuing Studies

National Taiwan University

Master Thesis

論金融機構洗錢防制與資訊共享法制—以區塊鏈技術的應用為中心

The Anti-Money Laundering and Information Sharing Laws for Financial Institutions: Focusing on Blockchain Applications

林智強

Chih-Chiang Lin

指導教授：楊岳平 博士

Advisor: Yueh-Ping Yang, S.J.D

中華民國 111 年 7 月

July 2022

doi:10.6342/NTU202202035

誌謝

首先要萬分感謝指導教授楊岳平老師，願意允收為徒，在我的論文撰寫過程中，不斷的指導並修正我的觀念及想法，讓我能以更宏觀的角度，更嚴謹態度闡述資訊共享的問題探討；楊老師是金融科技的專家，對於金融科技的相關應用相當熟悉，也因如此，才能包容資訊工程背景出身的我完成此篇論文，更讓我佩服的是楊老師對於資訊科技的鑽研之深，已非三言兩語可以形容；資訊共享的議題，牽扯到科技的應用、國際法規的思考，以及法律層面的配合，我很慶幸可以得到楊老師的指點與提攜，讓我在論文的寫作過程，能更深入的探討資訊共享相關的法律議題。

同時，我也要感謝臺灣大學進修推廣學院事業經營法務碩士在職學位學程的主任李茂生教授，很榮幸可以在李教授退休之前入學就讀，事業經營法務碩士在職學位學程是少數跨領域結合商管及法律的課程，雖然我之前沒有相關的背景，但在這兩年紮實的課程之下，雖然學習過程艱苦，而享受的果實異常的美好，帶著滿滿的知識繼續往人生下個階段前進。

另外，我也要感謝我們班上玫蓉、靜雯、詠心、琦慧、音孜、沁蓉、子瑜、書良、秉森及怡利這些在金融業服務的同學，像音孜、書良在外銀從事法令遵循和洗錢防制多年，靜雯是消費金融的內控專家，詠心是證券業法務專家，其餘同學也都是金融業翹楚，有幸能認識這些同學共同完成兩年的學業，在我論文寫作的過程，這些同學在金融業多年的經驗，提供給

我相當多寶貴的意見，也讓我的論文也能盡量貼近金融從業人員的想法及需求，更加具有實務的操作性。

也要萬分感謝陳肇鴻教授以及林育延教授願意擔任我的口試委員，兩位老師在百忙之中能抽空指導及指正我的論文，協助我能更精進，更全方位的思考資訊共享議題，由衷感激老師們的大力協助，以及溫暖的鼓勵，深表感謝。

我很慶幸可以在知天命之年紀，完成此論文，也讓我對於人生下半場的路，能有我充足的知識大步走下去，取之於社會，用之於社會，也自我期許未能對社會有更多的貢獻，謝謝所有幫助過我的人，由衷感謝。

林智強 謹誌

2022.07

于 臺灣大學進修推廣學院

doi:10.6342/NTU202202035

摘要

本文係以技術角度切入，探討區塊鏈去中心化技術，是否可以應用在金融機構洗錢防制資訊共享議題。本文首先分析我國在 APG 之後金融機構洗錢防制現況及面臨的困境，再探討美國、澳洲及新加坡在金融機構資訊共享的發展，由此開始探討我國在制度面與架構面的可能設計，以及區塊鏈技術之於資訊共享應用的好處；本文接著並分析區塊鏈中的公有鏈、聯盟鏈以及私有鏈之異同，探討究竟何者較適合本文的應用；此外區塊鏈的安全性也是本文討論的重點，包含資料加密以及傳輸加密，確保資料的安全性；本文最後分析應用區塊鏈技術辦理資訊共享可能涉及的法律問題，包括個人資料保護法、銀行法、金融控股法等相關規定，以及提出主管機關對於金融機構間基於洗錢防制的資訊共享可著重的未來發展方向。

關鍵詞：區塊鏈、資訊共享、資料加密、傳輸加密、洗錢防制、資恐防制

doi:10.6342/NTU202202035

ABSTRACT

This thesis adopts a technological view to discuss whether the decentralization technology of blockchain can be applied to the issue of money laundering prevention and information sharing among financial institutions. The thesis firstly analyzes the current situation of money laundering prevention in Taiwan and the associated difficulties faced with by Taiwan's financial institutions after the APG evaluation in 2018. The thesis then discusses the development of information sharing in the United States, Australia, and Singapore and the benefits of information sharing. Following these analyses, the thesis then discusses public chain, consortium chain, and private chain and evaluates which type of chain is more suitable for introducing the information sharing among financial institutions in Taiwan. The thesis also points out the importance of blockchain security, including the issues of data encryption and transmission encryption, in ensuring data security. Finally, the thesis explores the legal issues associated with information sharing among financial institutions for the purpose of anti-money laundering, including the Personal Data Protection Act, Banking Act, Financial Holding Company Act, and propose directions for the future development of information sharing laws by Taiwan's financial regulator.

Keywords: blockchain, information sharing, data encryption, transmission encryption, anti-money laundering, combatting the financing of terrorism.

doi:10.6342/NTU202202035

目次

doi:10.6342/NTU202202035

doi:10.6342/NTU202202035

doi:10.6342/NTU202202035

圖次

doi:10.6342/NTU202202035

表次

doi:10.6342/NTU202202035

第一章 緒論

第一節　研究動機及目的

民國（下同）100 年，因為銀行客戶的需求，我開始接觸反洗錢的領域，當時我國的金融機構反洗錢的作業，大部份以外匯電文黑名單掃描以及大額申報為主。之後我國自民國 96 年間亞太防制洗錢組織（下稱「APG」）第二輪相互評鑑程序的「一般追蹤名單」於 100 年間落入加強追蹤名單，持續至 103 年間第二輪相互評鑑程序結束時，仍與不丹、馬爾地夫、巴基斯坦、巴布紐亞幾內亞、菲律賓、阿富汗、 寮國、越南、汶萊等國同列過渡追蹤程序之追蹤國家。之後考量我國金流秩序不佳，不僅誘發犯罪誘因與犯罪發生，更影響金、商業發展及國際聲譽，故法務部自 104 年起先行推動刑法沒收新制， 並於 105 年制定資恐防制法並修正洗錢防制法，其中洗錢防制法部分，因涉及各金融機構與非金融機構之事業或人員，故由金融監督管理委員會、內政部、經濟部、財政部等各部會分別配合修正相關子法與實務規定[1]，撼動我國的銀行高層，故我國開始正視洗錢防制作業的重要性，開

[1] 法務部新聞（7/26/2017），<我國已脫離亞太防制洗錢組織(APG)第二輪評鑑之過渡追蹤程序，繼續爭取第三輪評鑑佳>，https://www.moj.gov.tw/media/14504/772619593112.pdf?mediaDL=true (最後瀏覽日：7/13/2022)。

doi:10.6342/NTU202202035

始投入大量的人力物力，最終也讓我國在第三輪的相互評鑑獲得一般追蹤名單的好成績。

但好成績的背後，是金融機構花費龐大的合規成本所達成，甚至矯枉過正，造成開戶的不便，也造成金融科技的發展受阻，此外又因個人資料保護法、銀行法與金融控股法的保密義務等規定，導致金融機構認識客戶（KYC）的結果，無法彼此共同分享，亦無法共同打擊犯罪。由此以觀，以洗錢防制為目的之資訊共享，勢在必行，也符合國外的趨勢，而各銀行的客戶 KYC 資訊目前只屬於銀行及客戶本身所有，但倘若統一集中在某個地方，除資訊安全面向需考量外，可能也不符合效益。如能運用區塊鏈技術的優勢-包括去中心化、不可竄改性、可追蹤性以及加密安全性，或許在資訊共享上可以發揮更大的效益，故本論文期待由實務現況、技術觀點以及法規層面加以分析區塊鏈技術是否可以應用在資訊共享，以及相關須留意的法規配套措施。

第二節　研究對象與範圍

依洗錢防制法第五條規定，本法所稱金融機構，包括銀行、信託、保險、證券公司等等，故上述金融機構都需要對客戶進行實質審查以及可疑交易監控，其中洗

doi:10.6342/NTU202202035

錢最重要的金流主要發生在銀行，故銀行也因此負擔最大的洗錢防制責任，面臨的罰款風險也最重，所以銀行也是花費最多精力在做洗錢防制相關工作的金融機構。故本論文的研究對象將主要針對臺灣的銀行同業進行研究。

依目前洗錢防制法規定，銀行有關洗錢防制的日常作業，包含名單檢核、風險評級、持續盡職調查、交易監控、可疑報告，其關係如以下圖 1 所示：

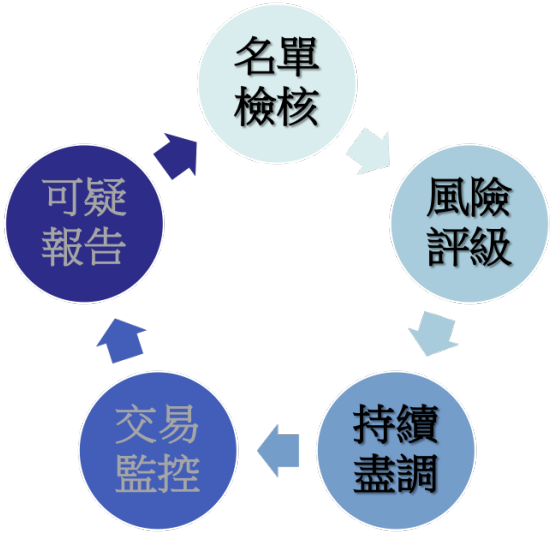

圖 1 洗錢防制日常作業（資料來源：作者自製）

尤其是第一關的名單檢核，依照金融機構防制洗錢辦法第三條第九項「金融機構完成確認客戶身分措施前，不得與該客戶建立業務關係或進行臨時性交易」之規定，以及第十條「金融機構於確認客戶身分時，應運用適當之風險管理機制，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」之規定，故銀行需要利用 Dowjones 或是 Worldcheck 名單

doi:10.6342/NTU202202035

資料庫（以下稱第三方名單資料庫），並搭配智慧型比對的姓名掃描軟體，即時辨識客戶身份是否為禁制名單上的人或所謂重要政治性職務人士（下稱「PEP」）。但現實的狀況是，第三方名單資料庫動輒幾百萬筆，且為求名單的豐富性，所以收錄的 PEP 名單或負面新聞名單 ，很多資訊其實都不太足，造成疑似案件產生（例如姓名相似的情形），也無法進一步識別其身份，進而影響之後的風險評級或以風險為本的交易監控。

為了加強金融機構在執行洗錢防制作業的 KYC 品質，以及聯合打擊犯罪的目的，金融機構間的資訊共享勢在必行，而本論文的研究對象會針對洗錢防制工作最重的銀行業為主，研究我國金融機構間資訊共享如何在符合國情、監管，及合規下進行以區塊鏈技術為基礎的資訊共享目的。

第三節　研究方法

筆者在業界多年，長期與銀行客戶交流溝通，了解也能理解洗錢防制工作對於金融機構的重擔及壓力，以及執行上的困難與挑戰。資訊共享在很多國家已施行多年，也證明對於洗錢防制作業的效率能有所提升，並有聯合打擊犯罪的優勢。每個國家的洗錢防制工作架構不同，所以資訊共享也有不同的設計方式，我國因部門組織權責問題，不一定能像其它國家提出資訊共享的解決方案；但隨著科技的進步與

doi:10.6342/NTU202202035

發展，尤其是區塊鏈已開始被接受為一種安全的資訊分享架構，所以本文會以下列方法，進行研究分析，區塊鏈是否適合我國作為資訊共享的平台。

第一項 文獻分析法

本文將蒐集及研究各國的洗錢防制現況及未來的發展，並針對跟我國國情比較相近的美國、澳洲及新加坡三個國家，分析其資訊共享的執行方式、現況及成果，並以這三國的洗錢防制工作框架為基礎分析其資訊共享的組織架構，以及主管機關對於金融機構的監管權力。

第二項 比較分析法

本文將參考美國、澳洲、新加坡的洗錢防制資訊共享的相關文獻，雖然這三個國家的資訊共享都是以中心化的方式進行，而考量到我國因國情及洗錢防制工作架構的綜合因素，本文會嘗試提出以有彈性的去中心方式進行資訊共享，針對中心化及去中心化的資訊分享方式進行優缺點比較，探討有彈性的去中心方式是否適合我國的資訊共享。

doi:10.6342/NTU202202035

第四節　研究架構

本論文總共有五章，第一章為緒論，先說明本文的研究動機及目的，研究對象與範圍、研究方法以及研究架構。第二章將闡述 APG 之後我國金融機構洗錢防制的現況，包括我國的金融機構執行狀況、困境以及資訊共享的可能性，再針對美國、澳洲以及新加坡說明其資訊共享的發展現況。

第三章將探討資訊共享之方法與問題探討，其中第一節將比較中心化與去中心化之資訊共享方法，第二節將針對去中心化的方法即區塊鏈進行探討，第三節再說明區塊鏈之安全性問題，第四節再以若干應用區塊鏈技術的資訊共享案例，包括環球貿易共享區塊鏈與保險業理賠聯盟鏈。

第四章將重點討論銀行間資訊共享之法律問題，包括銀行法、個人資料保護法、金融控股公司法以及洗錢防制法之相關規定。最後第五章再整理各章結論並提出可行建議。

doi:10.6342/NTU202202035

第二章 APG 之後臺灣金融機構洗錢防制現況

第一節　金融機構洗錢防制執行現況

第一項 目前執行狀況

根據金融機構防制洗錢辦法第八條第一項規定，金融機構應依據風險基礎方法，建立客戶及交易有關對象之姓名及名稱檢核政策及程序，以偵測、比對、篩檢客戶、客戶之高階管理人員、實質受益人或交易有關對象是否為資恐防制法指定制裁之個人、法人或團體，以及外國政府或國際組織認定或追查之恐怖分子或團體。第八條第二項進一步要求金融機構之客戶及交易有關對象之姓名及名稱檢核政策及程序，至少應包括比對與篩檢邏輯、檢核作業之執行程序，以及檢視標準，並將其書面化。第九條第二項則規定金融機構應依據風險基礎方法，建立帳戶或交易監控政策與程序，並利用資訊系統，輔助發現疑似洗錢或資恐交易。

筆者於 2010 年開始接觸反洗錢系統，在 2016 年兆豐紐約銀行天價罰款[2]以及因應 2018 年 APG 第三輪評鑑之需求，筆者協助超過十五家我國銀行建置符合洗

[2] 陳一姍（08/21/2016），<兆豐銀為何被罰 57 億>，《天下雜誌》，https://www.cw.com.tw/article/5077992，（最後瀏覽日：07/13/2022）。

doi:10.6342/NTU202202035

錢防制相關法規之洗錢防制系統，故根據筆者之觀察，幾乎所有銀行都已經全部導入或部分導入洗錢防制系統，並以資訊系統輔助日常洗錢防制的各項工作，且已編製適當的人力以及建立符合洗錢防制流程的各項監控工作，這也是為什麼我們可以在 APG 第三輪評鑑獲得好成績的原因。

第二項 執行困境

但好成績的背後代價，是銀行需每年花費龐大的合規成本。至於我國銀行的狀況，根據筆者就近觀察，銀行在洗錢防制的合規成本主要包括以下幾項的基本支出：

1. 反洗錢系統軟體建置費用，第一年大約在新台幣 1000 萬到 1 億元不等，依銀行規模大小而有所差異，之後每年需再支付 200 萬到 500 萬的年維護費用。

doi:10.6342/NTU202202035

2. 名單資料庫，比如 Dow jones[3]或是 Refinitiv World-check[4]，費用大約是每年兩百萬到五百萬的使用費，依銀行規模大小而有所差異。

3. 系統軟硬體，包含伺服器主機、網路設備、儲存設備、資料庫、備援軟體、備份軟體等等，費用大約是 1000 萬到 3000 萬不等，依銀行規模大小而有所差異，之後每年需再支付 100 萬到 400 萬的年維護費用。

4. 洗錢防制專責部門，編制大約為十人到百人不等，每人年薪再加上每年費用大約為 1000 萬到 1 億元，依銀行規模大小而有所差異。

以上，如以大型銀行來說，初期建置就需花費約 2 億 3 千 5 百萬，之後每年固定需花費 1 億 1 千 4 百萬，上述計算，還不包含銀行的作業流程因反洗錢原因而增加的成本，所以反洗錢的日常作業，對於銀行的營利影響不小。

---

[3] Dow Jones, https://www.dowjones.com/professional/risk/Dow Jones Risk & Compliance（last visited July 13, 2022）.

[4] Refinitiv World Check Risk Intelligence, https://solutions.refinitiv.com/world-check-kyc-screening?utm_content=Refinitiv%20Brand%20Product-OTHER-APAC-G-EN-Exact&utm_medium=cpc&utm_source=google&utm_campaign=581061_WorldCheckRIPaidSearchBAU&elqCampaignId=17078&utm_term=refinitiv%20world%20check&gclid=CjwKCAjwoMSWBhAdEiwAVJ2ndhdDD_d5CUj_mPaSTm1VWLSijyvsWSGZfrkRs4pynblwzGXvDjfLhBoCIhMQAvD_BwE&gclsrc=aw.ds（last visited July 13, 2022）.

doi:10.6342/NTU202202035

除了合規成本之外，目前銀行仰賴的第三名單資料庫，例如上述提到的 Dow jones 或是 Refinitiv World-check，由於名單資料庫數量龐大，動輒超過數百筆，且都只能收錄公開資訊，所以部份的資訊實際上並不詳細，再加上名字拚寫變化複雜，每天會產生數百筆的警示案件，故洗錢防制專責人員很難用已知的資訊識別出客戶的真實身份，甚至無法確認其洗錢風險，所以目前的作業方式雖然可以達成洗錢防制的相關規定，但非常沒有效率，倘若同一人或企業，在不同的銀行開戶交易，每家銀行都需要做一樣沒有效率的工作，不只浪費時間，且對未來的金融科技發展可能影響更大。

第三項 金融機構間資料共享

2017 年 11 月的 FATF Guidance : Private Sector Information Sharing 也說明了金融機構資料共享的重要性：「有效且運作良好的資訊共享是 AML/CFT 架構的基礎之一」[5]，而且對於聯合打擊犯罪更是很效的方法：「資訊共享對於打擊洗錢、恐怖主義融資和武器擴散融資至關重要，跨國洗錢不分國界，資訊共享的障

[5] FATF, *FATF Guidance-Private Sector Information Sharing* (Nov. 2017), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf（last visited July 13, 2022）.

doi:10.6342/NTU202202035

礙可能會對 AML/CFT 工作的有效性產生負面影響，相對的，也會無意中促進此類犯罪網絡的運作，這也證明在國家和全球範圍內，能快速、有意義和全面地共享來自各種來源資訊的重要性。」[6]

綜上，如果金融機構間可以有條件地共享有洗錢可疑的資訊，不只可以減輕個別銀行洗錢防制的工作，且可以更有效率地提前發現金融犯罪的發生，以下即以美國、澳洲、新加坡這三個國家為例說明可能的資訊共享作法。

第二節　國外現況與資訊共享未來發展

第一項 美國

美國的洗錢防制主管機關財政部金融犯罪執法網（Financial Crimes Enforcement Network，下稱「FinCEN」）在 2020 年 12 月發佈關於「美國愛國者法案」314(b)規定，取代之前 2016 年 11 月的指引[7]；根據此規定，金融機構可以在安全港（safe harbor）條款下，在識別及申報有洗錢及資恐活動的可疑交易的

[6] *Id*.

[7] FinCEN, *Section 314(b) Fact Sheet* (Dec. 2020) , https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf (last visited July 13, 2022).

doi:10.6342/NTU202202035

前提下，進行資訊的相互共享；儘管 314（b）的資訊共享是自願性質，但 FinCEN 強烈鼓勵金融機構參與[8]。

儘管金融機構按照 314（b）條進行信息共享是自願的，但它可以幫助金融機構增強對洗錢和恐怖防制要求的合規性，尤其是在蒐集可能涉及洗錢或資恐的客戶或交易資訊，包括未知的帳戶、金流活動或相關實體或個人等等時，資訊共享可以幫助金融機構更清楚地了解整個金流軌跡，特別是當金流很複雜時，例如涉及多個金融機構、實體和司法管轄區之間時，資訊共享可以對可能涉及洗錢或資的客戶活動建立更加全面和準確的調查，以便在盡職調查和交易監測中作出更精準的決策。

資訊共享也能提醒其他金融機構留意以前可能不知道有可疑活動的客戶。加強其識別和協助發現洗錢和資恐的手法。促進更有效的可疑交易申報——例如當金融機構通過自願資訊共享程序獲得更完整的金流活動時，有可能將原本不需申報的可疑交易，改正為必需辦理可疑交易申報的決定。

[8] *Id*。

doi:10.6342/NTU202202035

FinCEN 在 2009 年發佈 section 314(b)指引[9]，但 2020 年 12 月發佈的 314（b）條規定廢止了 2009 年指引、2012 年行政命令以及 2016 年 11 月發布的前一版 314（b）簡報[10]。依此規定，金融機構或金融機構協會可以就有關個人、實體、組織以及國家的資訊進行資訊共享，以便識別並適時申報可能涉及的潛在的恐怖主義活動或洗錢的活動。

金融機構間的資訊共享對於識別、報告及防止犯罪至關重要。具體而言，根據 314（b）設立的安全港條款進行資訊共享的金融機構或金融機構協會，可以共享與其懷疑可能涉及潛在資恐或洗錢的活動有關的資訊。例如金融機構或金融機構協會可共享涉及一項或多項美國法典（U.S.C.）第 18 卷第 1956 節及 1957 節所述特定非法活動（SUA）收益的特定交易資訊。本節列出了適用洗錢犯罪的各類上游犯罪，其列出的特定非法活動，包括一系列詐欺和其他犯罪活動，包括針對個人、組織或政府的詐欺、電腦詐欺和濫用以及其他犯罪。[11]

---

[9] FinCEN, *Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act* （June 16, 2009）, https://www.fincen.gov/resources/advisories/fincen-guidance-fin-2009-g002（last visited July 13, 2022）.

[10] FinCEN, *supra* note 7.

[11] FinCEN, *supra* note 9.

doi:10.6342/NTU202202035

參考 314（b）資訊共享解析（Information Sharing Insights），其中有關參與者的報告[12]，截至 2019 年為止，美國共有 8,400 家金融相關機構參與 FinCEN 的 314（b）資訊共享計劃，包含存款機構、賭場、證券商、期貨公司、信託公司、保險公司、貸款或金融、貨幣兌換業、房貸公司及基金公司，其比例如以下圖 2 所示：

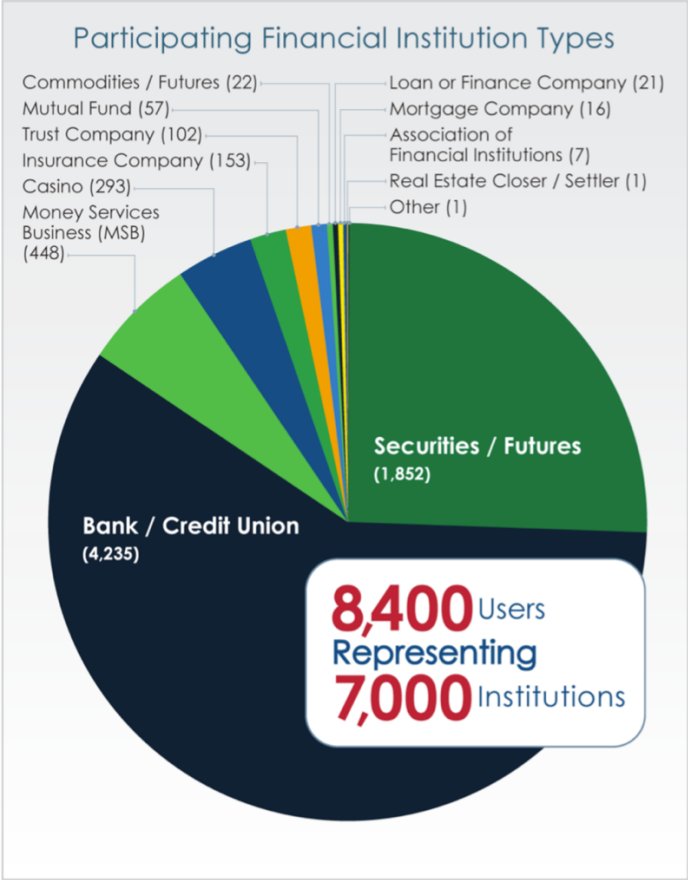

圖 2 金融機構類型（資料來源：FinCEN）

[12] FinCEN, *Information Sharing Insights-314(b) Participation and Reporting* (2019), https://www.fincen.gov/sites/default/files/shared/314bparticipationinfo.pdf (last visited July 13, 2022).

doi:10.6342/NTU202202035

而這些參加 314（b）的金融機構的可疑交易申報案件，也從 2017 年開始在二年內增加 19.7%，如下圖：

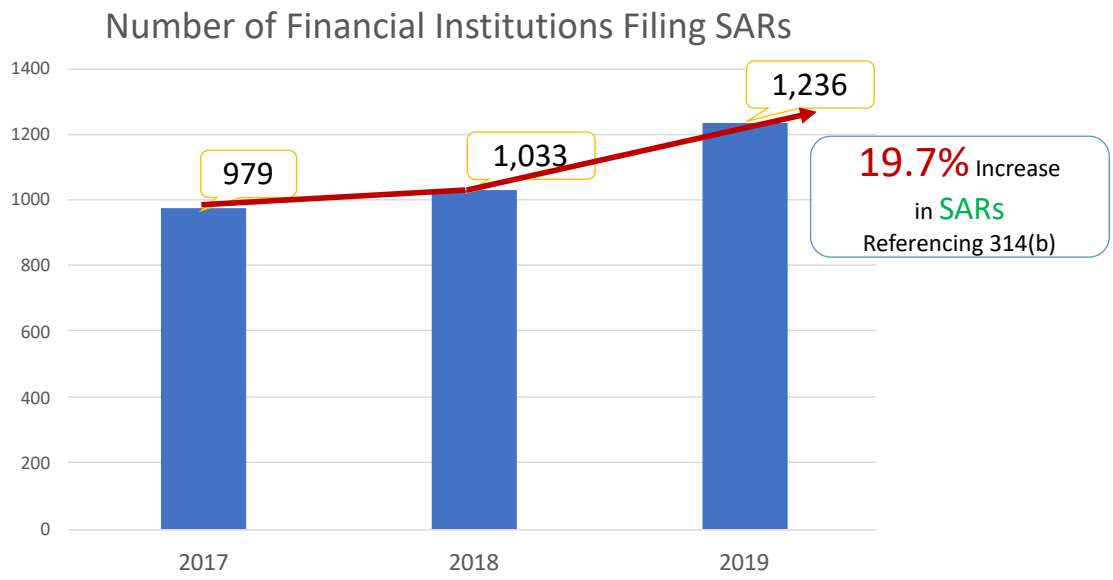

圖 3 金融機構申報數量（資料來源：FinCEN）

在 FinCEN 資源中心解析中也指出，可疑交易申報（SAR）的數量，也因 314（b）的關係，申報數量逐年增加，如下圖，由此可見，314（b）下的資訊共享達到的聯合打擊犯罪的成效相當有效。

doi:10.6342/NTU202202035

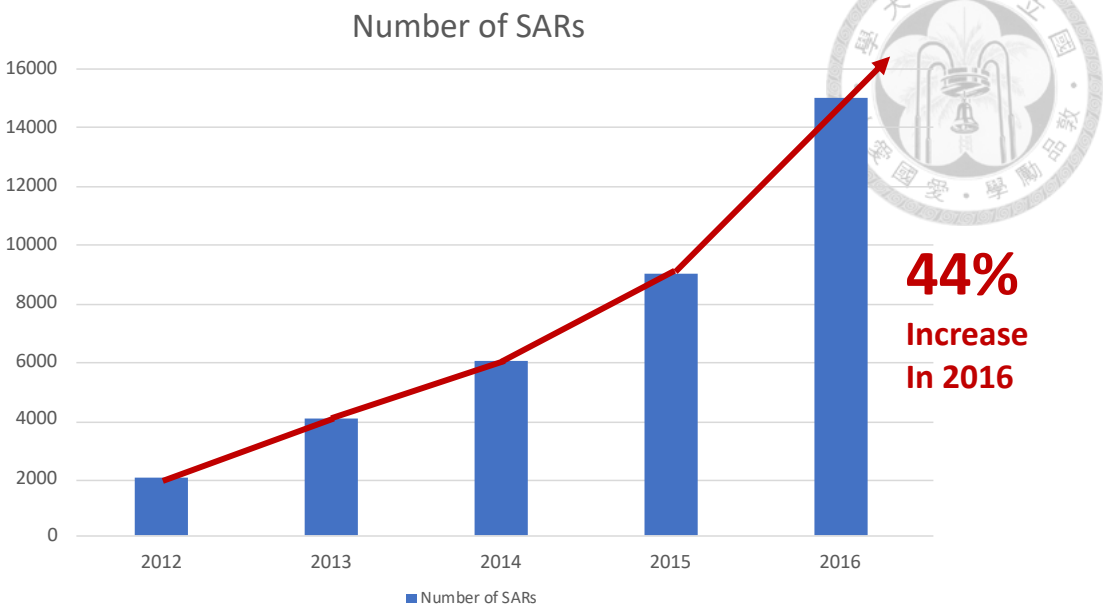

圖 4 申報總數量統計（資料來源：FinCEN）

第二項 澳洲

Fintel Alliance 是澳洲交易報告與分析中心（Australian Transaction Reports and Analysis Centre，簡稱「AUSTRAC」）於 2017 年所成立，目的是要提高金融部門對犯罪的預防能力，並支援對嚴重犯罪和國家安全事務的執法調查。Fintel Alliance 也是世界上第一個基於公私部門合作夥伴關係成立的犯罪防制機構[13]，其匯集了打擊洗錢、恐怖主義融資和其他嚴重犯罪的專家。Fintel Alliance 的合作夥伴包括主要銀行、匯款服務商和博彩運營商，以及來自澳洲和海外的執法和安全機構，公私

[13] AUSTRAC, https://www.austrac.gov.au/about-us/fintel-alliance（last visited July 13, 2022）.

doi:10.6342/NTU202202035

部門攜手合作，開發共享情報的平台並提供創新解決方案，以檢測、破壞和預防嚴重犯罪。[14]

Fintel Alliance 建立資訊分享計劃[15]，以使政府、執法部門以及金融機構能夠就運營事宜進行有效溝通。其中建立了一個安全的資訊共享平台，使合作夥伴能夠通過視頻、聊天和共同創作機密情報產品進行即時合作。此資訊共享的好處甚至已超越 Fintel 聯盟本身，而擴展到加強政府與政府之間以及政府與行業之間的合作，成為一個綜合性的交流平台，繼續支持和提高 Fintel Alliance 在瞄準、破壞和預防金融犯罪方面的有效性。[16]

具體運作上，Fintel Alliance 首先會先擬定工作計劃，針對優先主題例如針對最脆弱的社區成員的犯罪、利用政府收入、破壞專業洗錢與犯罪以及對澳洲國內或

[14] *Id*.

[15] AUSTRAC, *Fintel Alliance extract 2020-21 AUSTRAC Annual Report-Information sharing project*, （2021）, https://www.austrac.gov.au/sites/default/files/2021-11/FintelAlliance_PerformanceReport20-21_v5_Web.pdf（last visited July 13, 2022）.

[16] *Id*.

doi:10.6342/NTU202202035

國際利益的威脅。Fintel Alliance 的合作夥伴會在 AUSTRAC 位於雪梨和墨爾本的辦事處共同合作，共享和分析金融情報，以調查和破壞犯罪或恐怖活動。[17]

其次，Fintel Alliance 另外再分成營運中心（Operations Hub）以及創新中心（Innovation Hub），其中運營中心將合作夥伴聚集在同一個地方，即時交換和分析金融情報，並將來自個別金融機構的數據結合追蹤工具及最佳實踐方法相結合；至於創新中心內的合作夥伴則會共同設計和測試有助於在運營層面蒐集與分析金融情報的新的創新的技術解決方案，包括評估區塊鏈或數字資產（例如密碼資產）等新興技術的影響。[18]

第三項 新加坡

於 2021 年 10 月，新加坡金融管理局（Monetary Authority of Singapore，下稱「MAS」）公佈其將使用新的數位資訊共享平台打擊洗錢及資恐活動，而創設名為 COSMIC（Collaborative Sharing of ML/TF Information & Cases）的新平台，供金

[17] AUSTRAC, *supra* note 13.

[18] *Id*.

doi:10.6342/NTU202202035

融機構安全地分享客戶或交易的資訊，這樣的資訊共享機制，將有助於金融機構識別及擾亂非法網絡，從而有助於保護新加坡金融中心。[19]

COSMIC 平台是由 MAS 及六家主要的商業銀行共同創建，這六家銀行分別是 DBS、OCBC、UOB、SCB、Citibank 以及 HSBC[20]，COSMIC 平台有強大的安全功能，以防止未經授權的存取，並將由 MAS 負責系統運作。MAS 將會在合法的狀態下，允許金融機構在以防制洗錢、資恐以及武擴的前提下共享資訊；MAS 還將要求所有 COSMIC 參與者實施強有力的保全措施，以防止 COSMIC 的資訊未經授權而被使用和揭露； MAS 將監督金融機構遵守這些要求，並對有疏失的金融機構採取行動。[21]

MAS 目前計劃在 2023 年上半年推出 COSMIC 平台。COSMIC 最初會將重點放在商業銀行常涉及的三個主要金融犯罪風險，即濫用空殼公司、非法目的濫用貿易融資以及武器擴散。參與 COSMIC 發展的六家銀行是新加坡商業銀行中的領

---

[19] MAS, *MAS and Financial Industry to Use New Digital Platform to Fight Money Laundering*（Oct. 2021）, https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering（last visited July 13, 2022）.

[20] *Id*.

[21] *Id*.

doi:10.6342/NTU202202035

先者，其將在初始階段參與並被允許在 COSMIC 中共享資訊。 MAS 計劃逐步將 COSMIC 的覆蓋範圍擴大到更多的金融機構和重點領域，並強制共享特定方面的資訊[22]。

COSMIC 平台共享風險資訊的目的是為防止非法行為者利用金融機構之間的資訊落差，但同時也保護了個人的利益與隱私，盡量減少資訊共享給個人帶來的不便；因此，COSMIC 平台僅允許以下類型的共享資訊：

1. 解決關鍵風險領域中潛在的洗錢、資恐或武擴問題。[23]

2. 如果客戶的行為和交易活動出現多個超越風險門檻的危險信號，有可能發生潛在的金融犯罪。[24]

3. 採用 MAS 指定的數據格式，以便僅共享相關的風險信息。[25]

---

[22] MAS, *Consultation Paper on the FI-FI Information Sharing Platform for AML/CFT*（October 2021）, https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf（last visited July 13, 2022）.

[23] *Id.* at5-6。

[24] *Id.*

[25] *Id.*

doi:10.6342/NTU202202035

4. 通過 MAS 的安全數位平台所分享的洗錢、資恐或武擴資訊和案例都會被命名為「Collaborative Sharing of ML/TF Information & Cases」，簡稱 COSMIC。[26]

依據 MAS 的規劃，金融機構可以通過 COSMIC 平台，以三種方式進行資訊共享：

1. 請求（Request）：如果客戶出現危險信號，並且金融機構需要更多風險資訊來評估客戶是否參與非法活動，它可能會請求其他金融機構提供有關該客戶的風險資訊與活動。[27]

2. 提供（Provide）：如果客戶的異常交易活動超過了更高的門檻，表示客戶參與風險更大的非法活動，此時金融機構必須主動向其他金融機構提供與客戶活動相關的風險資訊。[28]

---

[26] *Id.*

[27] *Id.* at9-10.

[28] *Id.*

doi:10.6342/NTU202202035

3. 警示（Alert）：如果客戶的活動表現出較高的危險信號閾值，且金融機構提交客戶的可疑交易報告並決定終止關係，此時金融機構應在 COSMIC 平台上的「觀察名單」中對該客戶發出警報。[29]

關於 COSMIC 平台上資訊共享的法律依據，相關法律架構將在由新加坡的金融服管理者協會（Financial Services Association，FSMA）規定之。 它將規定金融機構之間出於防制洗錢或打擊資恐目的共享的風險資訊，以及要求金融機構就獲得的資訊的使用和保密採取相關保障措施。

至於金融機構的民事責任而言，如果金融機構採取了合理的謹慎措施並基於善意行事，MAS 規劃賦予參與 COSMIC 平台的金融機構就其向 COSMIC 提供的資訊享有一定的民事責任的法定保護。這將有助於保護參與的金融機構免於受到因參與 COSMIC 平台而引起的不當法律控訴。它將使參與的金融機構得以相信其為風險客戶及其相關非法活動而進行的合法資訊共享不會使他們面臨民事訴訟。

有關 COSMIC 的系統架構，金融機構可以透過以下兩種介面共享資訊：

[29] *Id.*

doi:10.6342/NTU202202035

1. 網頁為基礎的使用者介面（Web-based User Interface）：金融機構可以透過網頁介面連線 COSMIC，辦理線上填表或文件的上傳或下載，進而與其它金融機構共享可疑資訊。[30]

2. 自動化資訊交換管道（automated information exchange channels）：也就是我們熟知的應用程式介面（Application Programming Interface，簡稱「API」或安全檔案傳送協定（Secure File Transfer Protocol，簡稱「SFTPS」），可以透過自動化方式串接金融機構與 COSMIC 系統。[31]

第三節　小結

由以上三個國家的經驗可知，防制洗錢及打擊資恐工作，不能只依賴個別的金融機構依照法規或仰賴系統獨立作業，而需透過資訊共享方式，聯合打擊犯罪行為。美國的 314(b)在 2016 年就已訂出相關的規定，並在 2020 年 11 月發佈新規定的情況說明書（Fact Sheet），更詳細規定如何辦理資訊共享，以鼓勵金融機構、賭場、證券商、期貨公司、信託公司、保險公司等等參加共享自身的可疑資訊，聯合打擊犯罪；而澳洲更是在 2017 年成立世界第一個公部門-私部門合作夥伴的資訊共

[30] *Id*. at 21-22.

[31] *Id*.

doi:10.6342/NTU202202035

享聯盟 Fintel Alliance，合作夥伴包括主要銀行、匯款服務商和博彩運營商，以及來自澳洲和海外的執法和安全機構，並集中在 AUSTRAC 位於雪梨和墨爾本的辦事處共同合作，分享資訊並研究新的方法來預防及打擊犯罪；跟我國地緣及國情更相近的國家-新加坡，也在 2021 年 10 月公布成立 COSMIC 平台，如同美國及澳洲一樣，都是聯合民間的金融機構，並利用更先進的數位平台，以共同打擊犯罪為目的做相當程度的資訊共享；以 FinCEN Resource Center Insights 的報告也指出，資訊共享造成可疑交易申報-File SAR 的數量逐年增加，可見資訊共享對於聯合打擊犯罪的重要性。

我國的金融機構為了因應 2018 年 APG 第三輪評鑑，已花費龐大的經費建置自己的洗錢防制系統，也編制有大量人力處理洗錢防制的日常工作，但每個金融機構都受限於自身享有的資訊流及金流，而只能以「盡職調查」為原則，此係由於因金融機構並非公部門，沒有對外調查的權利，故如判斷交易可疑自然就申報可疑交易，但如個案交易的資訊不足且在本行的交易不頻繁，也只能輕輕放過，但這讓有心人提供了一個破口，可利用我國家數眾多的銀行，從事洗錢犯罪的行為。

倘若我國能效法美國、澳洲，甚至新加坡，提供數位平台，讓金融機構可以透過資訊共享平台，詢問並分享自己的資訊，並讓公部門執法機關可以在第一時間介

doi:10.6342/NTU202202035

入調查，如此一來，金融機構可以更有效率地執行洗錢防制及打擊資恐的相關工作，公部門亦可以更快速進行調查，市民大眾也可以有更快速的金融服務品質，加速金融科技的相關運用，共創三贏的局面。由此可知資訊共享的重要性。

不過先前探討的美國、澳洲、新加坡，這三個國家都是採取中心化架構的方式，由公部門設置資訊共享機構或平台。反觀我國目前似乎是先訂定指引，規範金融機構得共享資訊之法令相關規定，讓金融機構可以在法令規定下自行辦理資訊共享，這也延伸出另一個問題，資訊共享是否一定要由公部門以集中方式也就是所謂的中心化架構運作？有無可能利用去中心化的架構達成資訊共享的目的？畢竟金融機構各自所屬的資料，並非那一個公部門可以擁有，如果以去中心化的方式，比如區塊鏈技術，是否會更符合？以下就中心化及去中心化的資訊架構分析其優缺點，更進一步分析區塊鏈是否可以適用在資訊共享。

doi:10.6342/NTU202202035

第三章 資訊共享之方法與問題探討

以打擊犯罪為目的的資訊共享，已是各國洗錢與資恐防制的重要手段，而每個國家因為自身組織架構以及法律條件的不同，亦有不同的資訊共享規劃。以上述舉例的三個國家而言，看來似乎都是以中心化的技術，由一個公部門的主管機關負責資訊共享架構。

但洗錢或資恐防制所需共享的資訊，理論上不應屬於某個機關或單位所有。而隨著科技的進步，特別是區塊鏈技術近幾年的盛行，去中心化（decentralization）技術是否可以運用在以打擊犯罪為目的的資訊共享？本章將先分析我國與其它國家的洗錢防制組織架構差異後，接著探討中心化與去中心化的做法及優缺點，進而評估我國的資訊共享較適合採用中心化技術或去中心化技術作法。

第一節 我國與他國的洗錢防制工作架構比較

依防制洗錢金融行動工作組織（Financial Action Task Force on Money Laundering ，簡稱「FATF」）的四十項建議[32]第 20 項建議指出：「金融機構有合

[32] FATF, *International Standards on Combating Money Laundering and The financing of Terrorism & Proliferation-20 Reporting of suspicious transactions: The FATF Recommendations*（March 2022）.

doi:10.6342/NTU202202035

理依據懷疑資金係犯罪收益或與提供恐怖活動有關時，應儘速直接依法令所定之義務向金融情報中心提出申報」[33]；此外第 29 項建議：「各國應設立金融情報中心作為全國性統一受理、分析可疑交易報告及其它有關洗錢、相關前置犯罪及資助恐怖活動之資訊，並分送分析結果」[34]。故各國基本上都設有金融情報中心(Financial Intelligence Unit，下稱「FIU」)，而依據各國金融情報中心所組成的國際組織「艾格蒙聯盟」（Egmont Group）則將金融情報中心定義為：「負責受理（或經同意可提出請求）、分析下列揭露之金融資訊、並送交權責機關之全國性中央單位，包含可疑的犯罪財產或國家法令所定之防制洗錢資訊。」[35]

綜上，各國 FIU 在洗錢防制上扮演非常關鍵的角色，可謂是全國資訊的蒐集者。所以資訊共享的責任也往往落在 FIU 的身上。

美國的金融情報中心（FIU）單位，是美國財政部所屬的金融犯罪執法局（Financial Crimes Enforcement Network，以下簡稱「FinCEN」），FinCEN 透過發

[33] *Id* at 19.

[34] *Id* at 24.

[35] Egmont Group, https://egmontgroup.org（last visited June 27,2022）.

doi:10.6342/NTU202202035

FIU 的洗錢防制情報蒐集、處理和分配等主要工作，在美國的洗錢防制體系扮演樞紐的角色。正如其名，FinCEN 是一個利用制度及技術手段建立起來的政府內反洗錢情報網絡，不僅連接金融機構與執法機構，也組織起各個相關部門的網絡。

運用技術手段建立網絡是 FinCEN 的主要職責任之一，這也是為什麼美國的資訊共享是由 FinCEN 負責運作。其負責並串連銀行的監管體制，包含：

1. 主要負責監理州級會員銀行及銀行控股公司的聯邦儲備銀行（Board of Governors of the Federal Reserve System）。

2. 主要負責監管全國性銀行與在聯邦註冊的外國銀行分支機構的貨幣監理署（Office of the Comptroller of the Currency，OCC）。

3. 主要負責監管州級非會員銀行以及經聯邦保險的儲蓄銀行的聯邦存款保險公司（Federal Deposit Insurance Corporation，FDIC）。

澳洲的 FIU，是澳洲交易分析與報告中心（Australian Transaction Reports Analysis Center，以下稱「AUSTRAC」），是經聯邦議會批准設立的負責國家洗錢防制和資恐防制的監管者。AUSTRAC 的主要工作是對金融業與博弈業等進行監管，承擔洗錢防制、資恐防制以及金融領域犯罪防制的責任，也承擔蒐集、保存、分析金融交易信息與情報。

doi:10.6342/NTU202202035

新加坡的洗錢防制工作架構跟美國與澳洲不太相同。新加坡金融管理局（Monetary Authority of Singapore – 以下簡稱「MAS」）是新加坡的中央銀行和金融服務主管機關，設在財政部之下，為綜合性的主管機關，負責監督銀行、財務企業、保險公司、資本市場服務許可商、金融顧問、貨幣兌換商和匯款代理人[36]；也參與洗錢與資恐防制的立法與制定行政措施，並向金融機構發布和更新洗錢與資恐防制的預防措施與通知。但新加坡的 FIU 是可疑交易報告辦公室（Suspicious Transaction Reporting Office- STRO），負責接收和分析可疑交易報告（STR），STRO 也參與外國金融情報中心交換交易資訊備忘錄（MOU）的談判，以提高金融業和非金融業對洗錢和資恐的認知項目。

我國的 FIU 權責單位是法務部調查局，其於民國 86 年成立洗錢防制中心，後於民國 96 年間立法院通過《法務部調查局組織法》，其中第 2 條第 7 款明定本局掌理「洗錢防制事項」，第 3 條明定設「洗錢防制處」，負責洗錢防制法下之受理與分析金融機構申報之疑似洗錢交易報告等項目。根據法務部調查局 109 年的洗錢防制工作年報，洗錢防制處掌理下列事項：

[36] MAS, https://www.mas.gov.sg/regulation（last visited June 27, 2022）.

doi:10.6342/NTU202202035

1. 洗錢防制相關策略之研究及法規之協商訂定[37]。

2. 金融機構申報疑似洗錢交易資料之受理、分析、處理及運用[38]。

3. 金融機構申報大額通貨交易資料與海關通報攜帶或運送洗錢防制物品資料之受理、分析、處理及運用[39]。

4. 國內其他機關洗錢案件之協查及有關洗錢防制業務之協調、聯繫[40]。

5. 與國外洗錢防制有關機構之資訊交換、跨國洗錢案件合作調查之聯繫、規劃及執行[41]。

6. 洗錢防制工作年報、工作手冊之編修與資料之建檔及管理[42]。

---

[37] 法務部調查局（2020），《洗錢防制 109 年工作年報》，頁 2-3。

[38] 法務部調查局，同前揭註 37。

[39] 法務部調查局，同前揭註 37。

[40] 法務部調查局，同前揭註 37。

[41] 法務部調查局，同前揭註 37。

[42] 法務部調查局，同前揭註 37。

doi:10.6342/NTU202202035

7. 其他有關洗錢防制事項。[43]

全世界 FIU 的類型可分為行政型（Administrative Model）、司法型（Judicial Model）、執法型（Law Enforcement Model）以及混合型四種[44]。具體定義如下。

- 行政型：係指在行政或監理機關下設置的 FIU，作為申報金融機構與執法機關間之緩衝機制。採此模式者例如美國、日本、韓國、加拿大、法國、新加坡等等。

- 司法型：係指在司法機關下建立的 FIU，其有較高獨立性，具有強制處分權及公訴權。採此模式者例如盧森堡、塞普勒斯等等。

- 執法型：係指在執法機關下設置的 FIU，其可以針對分析結果立即進行調查。採此模式者例如澳洲，英國、香港及我國等等。

混合型：係指至少結合行政、司法與執法三個機關中之兩種機關成立一個新的機關設置 FIU，目的在吸取上述各類型優點。採此模式者例如泰國、丹麥、挪威等等。

---

[43] 法務部調查局，同前揭註 37。

[44] 詹德恩（2021），《法令遵循理論與實務-洗錢防制及打擊資恐》，頁 167-169。

doi:10.6342/NTU202202035

美國的資訊共享負責機構是 FinCEN，其為財政部所屬，基本上的定位就是網絡，所以由其負責提供資訊共享需求係屬合理；澳洲 AUSTRAC 本身即兼負金融情報機構的角色，也具有洗錢防制和反資恐防制監管者的雙重角色，另外成立 Fintel Alliance 來負責資訊共享，加強公私部門的合作；至於新加坡的 MAS 雖不是 FIU 的角色，但是新加坡的中央銀行和金融服務管理機構，設在財政部之下，而且也向金融機構發布和更新洗錢與資恐防制的預防措施與通知，所以由 MAS 設置的 COSMIC 平台扮演資訊共享的角色，亦屬合理。

相較而言，我國的洗錢防制處係扮演 FIU 的角色，但與上述國家不同的是，洗錢防制處屬於法務部，而上述國家都是由財政部有關或是兼任金融機構的主管機關之單位辦理資訊共享，所以能有效率地實行資訊共享。而我國因權責單位在法務部，與負責監管金融機構的金融監督管理委員會是平行單位，雖在我國的洗錢防制法架構下，各目的事業主管機關需完全配合法務部洗錢防制相關工作，但法務部畢竟不是直接監管金融機構，所以在溝通上會有些隔閡，而這也有可能造成我國如欲採行中心化的方式由政府主導資訊共享架構，可能會面臨的挑戰。

doi:10.6342/NTU202202035

第二節 資訊共享的方法探討

第一項 中心化與去中心化模式的比較

自從 2008 年比特幣問世之後，去中心化的議題，就不斷地被討論；論者即有指出「去中心化的聲浪高漲，催生了區塊鏈技術的運用。不過在談論『去中心化』之前，我們必須先探討『中心化』，究竟它產生了什麼樣的問題？讓身處中心化社會的人們開始思考？」

目前人類社會大部份的機制，都是以中心化為主，從中央政府到金融機構，都是以中心化的方式運作。中心化的好處很 多，最主要是可以用少數人的力量進行決策與處理事情，進而提高執行效率；在某些層面來看，中心化的確也發生很大的作用。但隨著科技的進度，資訊取得愈來愈方便，也愈來愈快，在長期以中心化運作的制度，也衍生出不少問題。

中心化的缺點可歸納為腐敗(Corruption)、壓制自由(Suppression of Freedom)、單點故障（Single Point of Failure）、地域限制（Geographical Limitations）、不易擴充（Failure To Scale）等幾個缺點[45]，去中心化的擁護者致力打造一個沒有中央

[45] Sadekj（2017）, *Decentralization: Why We Need It? & What Is Wrong With Centralization?*, Steemit, https://steemit.com/steemit/@sadekj/decentralization-why-we-need-it-and-what-is-wrong-with-

doi:10.6342/NTU202202035

控管的環境，而在比特幣問世之後，區塊鏈技術已透過實證證明其可以有效地以去中心化的方式安全地運作，最重要的是其避免了上述中心化所造成的問題。也因為如此，近兩年熱門的去中心化金融（Decentralized Finance，DeFi）即利用區塊鏈的技術，解決了身份認證的困難以及因為中介機構參與而產生的額外成本支出這兩個中心化的問題，同時也在這個基礎上，逐漸發展出有別於傳統金融的金融商品，而開始受到大家的歡迎。

但基於打擊犯罪為目的之資訊共享仍是依附在法規允許的條件下才能進行，基本上脫離不了中央政府的控管，但在施行的架構上，就可以考慮運用有彈性的去中心化區塊鏈的技術，在有管理者的鏈結之下，以分散式帳本的方式資訊共享，在架構上可以避免掉上述單點故障、地域限制、不易擴充等幾個缺點，所以用去中心化區塊鏈的技術方式規劃，是否可以更符合未來的長遠的發展？即值探討。

centralization?fbclid=iwar1-b_ehgm7_po2kpcvfgnkyfhtbbcl05phr9i63wykhdumsk0kfgfzn1mi （last visited Jun 27, 2022）.

doi:10.6342/NTU202202035

第二項 雲端服務

上述提到中心化的其中一個缺點是地域性限制，也就是只能固定在某個地方或只能提供服務給該地區。但除了去中心化以外，最近盛行的雲端服務是否亦能解決中心化的地域性限制問題？

何謂雲端服務？其實雲端不是實體，而是指遍佈在世界各地的伺服器，透過網路連結在一起，而這些伺服器有些是儲存功能，或是資料管理用途，也可以執行應用程式提供或傳遞內容或服務，例如串流影片、郵件或是網站等等，讓使用者可以在需要時隨時取得。使用者不再需要了解『雲端』中基礎設施的細節，不必具有相應的專業知識，也無需直接進行控制。雲端運算描述了一種基於網際網路的新的 IT 服務增加、使用和交付模式，通常涉及通過網際網路來提供動態易擴充而且經常是虛擬化的資源；早期，受限於網路技術及限制，大多數的企業，幾乎都是以大型主機透過集中化的方式，統一運算再對外提供服務，但集中化的方式，就像上述中心化所提到的問題般，不論是在單點故障、地域性限制、不易擴充等面向上，都相對缺乏彈性，所受限制也很大。[46]

[46] Azure, https://azure.microsoft.com/zh-tw/resources/cloud-computing-dictionary/what-is-the-cloud/（last visited Jun 27, 2022）.

doi:10.6342/NTU202202035

自從在 2006 年美商亞馬遜公司（Amazon.com, Inc.）開啟雲端服務之後，雲端解決了企業因資訊系統過於集中而導致彈性不足的問題。企業及終端使用者可以不用在乎其中的 IT 架構如何連線，只要透過類似像 Amazon 的 AWS、Microsoft 提供的 Azure、或是 Google 的 GCP，就可以輕鬆將企業所提供的服務遍及世界各地，不再因 IT 架構的限制而有所限制，相當方便。

雲端服務解決了中心化單點故障、地域限制以及不易擴充等三個問題。如上述，雲端不是單一實體，而是指遍佈在世界各地的伺服器，透過網路連結在一起，以 AWS 為例，如下圖所示，AWS 全球的 IT 機房基礎設施遍及全球 26 個地理區域，而且未來已計劃在澳洲、加拿大、印度、以色列、紐西蘭、西班牙、瑞士及阿拉伯聯合大公國，也就是說使用 AWS 的雲端服務，即可以擁有遍佈在世界各地的伺服器群[47]，但其實雲端服務還是百分之百的中心化架構，蓋雲端服務的控制權僅由提供服務的企業或公部門本身享有，這點中心化的特質不會因為上了雲端而有所改變；但另一方面而言，不論是中心化或去中心化的資訊共享架構，也都可以利

[47] AWS, https://aws.amazon.com/tw/about-aws/global-infrastructure/?p=ngi&loc=0（last visited June 27, 2022）.

doi:10.6342/NTU202202035

用雲端服務所提供的彈性達成資訊共享的目的，而這也是資訊共享是否能普及的重要關鍵技術。

圖 5 AWS 全球基礎設施地圖（資料來源：AWS）

第三節 去中心化模式之探討-以區塊鏈技術為中心

目前大部份國家都是以中心化方式規劃以打擊犯罪為目的的資訊共享，畢竟這是最安全的方式，其運作方式類似可疑交易申報報告，將相關資訊集中報送到一個中心機構，而我國可否以去中心化區塊鏈技術的模式規劃資訊共享架構？

資訊共享最主要的目的是聯合所有的金融機構共享資訊共同打擊犯罪，所以如何讓金融機構可以快速加入也是資訊共享架構設需考慮的重要議題。此時，去中心化的區塊鏈技術設計即可發揮其作用。

doi:10.6342/NTU202202035

如上述，我國的 FIU 是屬於執法型，隸屬在法務部調查局，不會直接監管金融機構，不同於美國及新加坡的設計架構。我國固然可以參考澳洲的方式，設立一個公私結合的獨立部門，在實體辦公室一起合作，加強 FIU 與金融機構間的橫向溝通；以此概念，轉化成線上虛擬辦公室，其效果就相當於大家都在同一個區塊鏈上，透過區塊鏈的技術共享資訊，金融機構的管理者金管會也同時在鏈中，而鏈的管理者即為法務部調查局，以分散式帳本方式共享資訊，雖名為去中心化，但事實上是以有彈性、有管理者的去中心化區塊鏈做為整個資訊共享的核心技術。但區塊鏈去中心的各項安全機制，是否足以大家信任，以下章節繼續分析。

第一項 區塊鏈技術的類型-比較公有鏈與私有鏈

區塊鏈是分散管理資料的結構，相較於現今大部份的資料系統都是以集中管理以利資料運用為前提的中心化建置架構，區塊鏈的運作不需要由中央機構管理資料，而是由全體參加者分散管理之，藉此提高系統的效率。

區塊鏈技術採取的分散式帳本技術其實存在已久，只是近來因科技進步與網路速度加快，以及虛擬資產的普及，證實了區塊鏈技術可以應用在更多的場域，其中最具代表性者就是虛擬資產中的比特幣，2009 年問世的比特幣至今，已凸顯區塊鏈技術的優點：去中心化、不可竄改性、可追蹤性，加密安全性。

doi:10.6342/NTU202202035

區塊鏈技術又可分為公有鏈及私有鏈，此外依其網絡公開的程度不同，又可分成「公有型」、「聯盟型」、「私有型」[48]。其基本特性整理如下：

	公有型	聯盟型	私有型
參與方式（網路）	開放（自由參加）	封閉（許可制）	
代表案例	虛擬資產（ex.比特幣）	設定為金融機構或企業間使用模式	
管理主體	無	多個組織	單一組織
結構前提	防止惡意參加者	不會有惡意參加者為前提	

表 1 區塊鏈的分類（資料來源：大和總研，圖解 Fintech 的知識與技術）

[48] 大和總研（2020），《圖解 Fintech 的知識與技術》，頁 199~202。

doi:10.6342/NTU202202035

所謂公有鏈，係指公有型區塊鏈，是利用公開的網路，任何人都可以自由參加的區塊鏈，例如比特幣或若干虛擬資產基本上即是使用這種方式運作，透過網際網路（Internet）[49]方式連結，讓大眾可以參與比特幣的交易。

至於所謂私有鏈，係指透過限定參加者的封閉網路運作的區塊鏈，只有獲得許可的參加者才可以存取網路；不同於公有型，私有鏈只允許可信任者加入，所以不需要假設有惡意的參加者，可以依照其目的彈性設計，提高處理速度或是隱私性。而私有鏈又可分為聯盟型及私有型，都是屬於許可制方式，如以網路參與方式來分，私有型可以在組織或企業內部，以內部網路（Intranet）[50]方式連結，不開放外

[49] Internet，以 TCP/IP 網路協議串連線全世界的國家或地區，將數千萬臺的主機串流在一起，IP 位址就如同現實世界的電話號碼，每個在 Internet 的主機或成員都擁有自己的 IP，外界可以透過 IP 位址找到這台主機。

[50] Intranet，企業內部或個人家庭中，一樣是以 TCP/IP 網路協議串連家中電腦，不同於 Internet，Intranet 所使用的是內部 IP 地址，就如同企業內部的分機，外界無法透過分機號碼連線，但企業內部可以透過分機，也就是內部 IP 互相連線傳遞訊息。

doi:10.6342/NTU202202035

部網路連線；而聯盟鏈，因是多個組織的結合，所以不可能是內部網路方式連結，需使用虛擬私人網路（Internet VPN）[51]方式連結聯盟內的成員；

目前業界有關區塊鏈實作的軟體中，虛擬資產型例如比特幣等都是使用公有型方式，使用開放式原始碼，例如 Bitcoin core、Litecoin 等，由於其面對廣大的投資者或交易人，並使用公用網路允許任何人都可以自由參加，故可能會發生惡意的參加者，所以程式重點會在如何採取必須共識演算法，例如工作量證明（Proof of Work），以確保鏈上的交易安全性及可靠性。

而混合型類如像以太坊（Ethereum）、NEM 等，雖然也是開放式原始碼，但以太坊更強調的是智慧合約（Smart Contract）的功能，以降低與簽約者之間的信任成本為其主要的優點，所以應用上除可以用於像以太幣的虛擬資產外，有些也應用在聯盟鏈中像 ICO 募資、協議合約，借貸或發行 NFT 等等。

[51] 虛擬私人網路，在 Internet 上，透過防火牆，以加密的方式互相傳遞訊息，就如同私人網路一樣，外界無法得知傳遞的內容。

doi:10.6342/NTU202202035

至於通用智慧合約型，基本上會由機構或組織所開發而成，強調交易彈性及速度，例如 HyperLedger Fabric、R3 開發的 Corda，非常適合應用在聯盟型或私有型，提供特定應用的區塊鏈。

以上歸納如下表所示：

分類	公有型	聯盟型	私有型
虛擬資產型	Bitcoin Core Litecoin		
混合型	Ethereum、NEM		
通用智慧合約型		HyperLedger Fabric、Corda	

表 2 區塊鏈的應用實例（資料來源：大和總研，圖解 Fintech 的知識與技術）

如上述，公有鏈中例如 Bitcoin core 、Litecoin、Ethereum 等都是屬於開放式原始碼，並持續更新中，而聯盟鏈及私有鏈常使用的，包括 HyperLedger Project 開發的「Hyperledger Fabric」，R3 開發的「Corda」，使用智慧合約型實作。

doi:10.6342/NTU202202035

如以金融機構洗錢防制的資訊共享為目的，由於此類資訊共享不僅只是單一組織內的資訊共享，而是涉及多個組織的結合，但又不適合開放予不特定大眾參與，因此本文認為應該是採取特定目的的許可制區塊鏈，特別是使用私有鏈中的聯盟鏈會比較適合。

第二項 私有鏈之優勢

傳統認為區塊鏈-特別是公有鏈的好處：去中心化、不可竄改性、可追蹤性，加密安全性。但這些好處應用於洗錢防制的資訊共享，卻未必完全適用。

以不可竄改性為例，對於使用公有型的比特幣或其它虛擬資產而言，不可竄改性是很重要的機制，因為虛擬資產一方面開放不特定大眾自由參加，一方面又需要維持大眾資料的正確性，所以設計區塊鏈技術的前題必須足以防止惡意的參加者違法破壞區塊鏈技術的正確性。但不可竄改性會衍生出兩個問題，一個是個人資料主體的被遺忘權（right to be forgotten）難以行使，另一個是帳本記載訊息的可更正性[52]。基於洗錢防制目的的資訊共享，其資料來源都是來自於金融機構，現實上不

[52] 呂嘉穎（2020），《初探區塊鏈之不可竄改特性、匿名性所衍生的法律問題》，交大法學評論，頁 51~60 。

doi:10.6342/NTU202202035

可避免會發生資料錯誤或某些原因而需要刪除或更正資料，所以不可竄改性在洗錢防制資訊共享的應用上必需做適度調整，允許適當的資料刪除或是更正。

另一方面，如欲維持上述此彈性的設計，就不可能以完全去中心化的模式架構資訊共享機制，而必須存在一個公正的第三方，負責維護整個區塊鏈帳本的運作，以達到適度的資料刪除或更正。但這並不代表須回歸完全中心化的設計。區塊鏈技術下例如聯盟鏈的設計，固然並非完全的去中心化，但仍保有相對的去中心化特性，即屬適度調整區塊鏈去中心化特性後的安排。

綜上，以洗錢防制為目的的資訊共享，固然亦利用到區塊鏈的特性包括去中心化、不可竄改性、可追蹤性以及加密安全性，但又需要適度調整去中心化與不可竄改性的特質。所以使用私有鏈設計才能符合資訊共享的需求，此外由於此處的資訊共享是屬於金融機構同業間的共享，這些資訊並不屬於任何的公部門及私部門所擁有，如以中心化方式存放，負責的機關就得擔負起保護資訊的絕對責任，而上述的單點故障、地域限制、不易擴充等幾個缺點，還有需要存放龐大資料的資訊設備，以及防範駭客入侵的資安防護等高昂的費用問題就會一一浮現，而去中心化區塊鏈技術係採分散式帳本，可以避免單一資料庫存放龐大資料所衍生的問題，加上私有鏈的彈性的設計，雖說是去中心化，但事實是使用區塊鏈的技術，而本質上仍

doi:10.6342/NTU202202035

是有中心化的管理者，如此才能適用於以洗錢防制為目的之資訊共享，且克服單點故障、地域限制、不易擴充缺點，至於安全性問題是否可以讓人放心且不用花大錢，以下繼續分析。

第四節 區塊鏈技術之安全性探討

上述已說明區塊鏈技術的去中心化特性在資訊共享中所帶來的好處。而去中心化之後，資訊係分散儲存在各個區塊中，此際區塊鏈的安全性就顯得格外的重要，這也是區塊鏈中的資料加密面向強調的重點。雖然資料已被加密，但仍有可能被破解的風險，所以在私有鏈或聯盟鏈的設計上，會再加上使用內部網路或加密網路傳輸的要件，以確保傳輸過程的安全性；以下就此兩個安全性的設計說明。

第一項 資料加密

區塊鏈的結構及加密技術，形成強大的安全機制，以防止區塊鏈的資料被惡意的竄改，具體而言，雖然區塊鏈上的資料係分散儲存在不同的區塊，但每個節點都會寫下記錄，每個區塊儲存的資料用點對點的連接，形成鏈條般的型態，這也是區

doi:10.6342/NTU202202035

塊鏈名稱的由來[53]；區塊鏈技術進一步採用現代密碼學原理保障資料的安全，區塊鏈先將資料數據化加密後再進行傳輸，形成所有人都可以見證、但只有當事人才有權解密與知悉信息內容。上述過程係通過兩種密碼學算法共同完成：一是公開金鑰加密法（Public-key cryptography），也稱非對稱式加密法（Asymmetric cryptography）[54]，二是雜湊演算法（Hash function）[55]。

所謂公開金鑰加密法，是指對數據進行加密和解密時，需要兩個不同的密碼完成；與之相對的，是對稱加密法，加密和解密只需要一個密鑰即可，所以公開金鑰加密又稱非對稱加密算法[56]。在區塊鏈中，將交易中的密碼分為公鑰（public key）和私鑰（private key），區塊鏈系統的參與者因其角色不同而持有不同的密鑰，當

[53] 區塊鏈技術在網路方面是建構在 Peer-To-Peer（P2P）上，節點與節點間互相將資料進行同步，不需要一個地方儲存檔案資料，而是將檔案分散到許多節點，也就是所謂的區塊，每個區塊都各自擁有獨特的識別碼，前後互相連結，組成區塊鏈。

[54] 非對稱式加密，是指加密方式總共有兩把金鑰，一把是公鑰（Public Key），可公開在網路上，用於加密的用途，另一把是私鑰（Private Key），必須自己保存，用於解密使用公鑰加密傳來的訊息。

[55] 雜湊演算法，最主要用於資料或是身份驗證，透過雜湊函數（Hash）將任意長度的字串轉換成固定長度，可在不取得明文的情況，驗證資料的完整性（Date integrity）。

[56] 王毅丞（2018），《實戰區塊鏈技術-加密貨幣與密碼學》，碁峯，頁 4-61~62。

doi:10.6342/NTU202202035

其為交易的見證者時，只能持有公鑰；當其為一項交易的當事人時，其既持有公鑰也持有私鑰。此非對稱加密算法一方面賦予節點上的用戶通過公鑰對所有交易予以驗證的權利與義務，以確保交易的真實性，但另一方面只有交易當事人才能通過私鑰獲取每一個交易的具體內容，從而也確保在分散式的區塊鏈中點對點傳輸的安全性與當事人的隱私[57]。

至於雜湊演算法（Hash function），是指使用雜湊函式把資料壓縮成摘要，並打亂資料組成，進而使資量料變小而便於傳輸，也更大幅提升資料的安全性[58]。區塊鏈使用雜湊值（Hash value）來顯示區塊鏈的狀態，所謂的雜湊函式具有以下特性：

1. 相同的輸入值會輸出相同值，且不同的輸入值會輸出不同值：這是保證輸入值可信任的重要特徵，即使只有一個字母被竄改，也會輸出不同值，故只要確認輸出值，就能偵測被竄改的部份。

[57] 王毅丞，同前揭註 60。

[58] 大和總研（2020），同前揭註 52 ，頁 193~195 。

doi:10.6342/NTU202202035

2. 無法從輸出值（雜湊值）鎖定輸入值：這是為了隱藏輸入而必須具備的特性，可以防止第三者知悉內容。

3. 可以即時將給予的輸入值雜湊化：雜湊函式可以被設計成非常快速，讓整個加密程序不至於拖慢交易速度，有助於建構高效率的系統。

區塊鏈應用上述先進的加密技術，包括公開金鑰加密法再加上雜湊演算法，因此基本上不容易被破解，就算被破解，也能透過雜湊值（Hash value）偵測被竄改的部份，而且這些資料都是分散儲存於在各個區塊，因此可確保區塊鏈的使用安全。

第二項 傳輸加密

如以聯盟鏈規劃資訊共享，則聯盟鏈雖然是屬於許可制而只允許加盟的金融機構使用，但因為涉及廣大的金融機構間的互相連結，還是必需依賴網際網路傳遞訊息，故就算區塊鏈已有公開金鑰加密法及雜湊演算法保障資料安全，但畢竟資訊共享傳遞的都是個人資料，不容許有一點洩露閃失，所以除了區塊鏈技術本身的加密保護之外，在傳輸過程，也需要再增加保護。

doi:10.6342/NTU202202035

目前最安全的網路傳輸，莫過於廣域網路（WAN）點對點專線連接，也就是雙方的區域網路是透過廣域網路中的專屬連線而連結[59]，具體運作如下圖所示：

圖 6　WAN 點對點專線連接（資料來源：粘添壽博士網站）

這種架構是早期網路最普遍的方法，相對安全但費用也相對高，如果是採取中心化的架構，利用此方法連結金融機構的區域網路是可行的，如下圖所示：

[59] 粘添壽，＜廣域網路連結與寬頻網路＞，《翻轉工作室》，http://www.tsnien.idv.tw/Network_WebBook/chap14/14-2%20廣域網路之連接型態.html，（最後瀏覽日：07/13/2022）。

doi:10.6342/NTU202202035

圖 7 中心化網路連線示意圖（資料來源：作者自製）

相對而言，去中心化的聯盟鏈架構，圖示如下：

doi:10.6342/NTU202202035

圖 8 去中心化網路連線示意圖（資料來源：作者自製）

由上圖複雜的連線可知，點對點的專線並不適合去中心化的聯盟鏈。如以本國銀行試算，截至 111 年 3 月底止，我國總共有 39 家本國銀行[60]，加上洗錢防制中心以及金管會，總數為 41 個節點。如以去中心方式設計，各自需要以專線方式串連，專線數量會高達 1600 條，蓋除費用高昂之外，也不容易擴大資訊共享聯盟鏈的規格。

[60] 金融監督管理委員會銀行局網站（2022），《表二-金融機構家數統計》，載於 https://www.banking.gov.tw/ch/home.jsp?id=157&parentpath=0,4&mcustomize=bstatistics_view.jsp&serno=201105120009 ，（最後瀏覽日：07/13/2022）。

doi:10.6342/NTU202202035

但如使用虛擬私人網路（Virtual Private Network，VPN）技術，以現有網際網路連線即可解決這個問題，所謂 VPN 網路是指建立一個安全的連接通道，使網路或計算機之間能安全地進行相互訪問與存取的一種方式；互相連結型的 VPN 即可提供企業網路與企業網路間彼此的資料存取[61]。VPN 之所以安全，是因為在傳輸過程中，加了以下的安全機制：

1. 通道（Tunneling）及加密（Encryption）：所謂通道，係指企業間建立點對點的邏輯虛擬通道，至於加密，則是將欲傳送的資料加以編碼與計算，造成只有發送者及接收者能夠解碼得知內容的其中意義；這兩項保護可以確保未經授權的個人或企業，無法於公眾上讀取到他人的機密文件。一般常見的通道技術協定為 Layer 2 Tunneling Protocol (L2TP)、Layer 2 Forwarding (L2F)、Generic Routing Encapsulation (GRE)以及 IP Security (IPSec)。而加密的技術則依加密

[61] 粘添壽，<VPN 網路規劃與管理>，《翻轉工作室》，http://www.tsnien.idv.tw/Manager_WebBook/chap10/10-1%20 虛擬私有網路簡介.html ，（最後瀏覽日：07/13/2022）。

doi:10.6342/NTU202202035

鑰匙的長度不同，有 DES 及 3DES 等，至於加密鑰匙的管理，則可配合相關的管理伺服器(Certificate Authentication Server，CA Server)來達成[62]。

2. 封包認證（Packet Authentication）：VPN 通道建立後，在傳輸過程中為了確保資料的完整性，以及確認資料沒有被修改過，可以利用封包認證的協定來達成此目的，常見的技術如 AH、ESP、MD-5 及 SHA 等協定。傳送者及接收者於加密通道建立時，便需確認依何種封包認證技術進行資料的傳輸，故當接收者收到資料封包之後，便可利用事先約定好的封包認證方式來檢查封包是否在公眾網路傳輸時被修改過[63]。

3. 防火牆（Firewall）與入侵偵測（Intrusion Detection）: VPN 的網路架構，得先建置防火牆，防火牆除了可以設定以上的安全設定外，也能將可能的駭客入侵或是非授權用戶阻隔於企業網路之外，以保障企業網路的安全[64]。

---

[62] 粘添壽，同前揭註 65。

[63] 粘添壽，同前揭註 65。

[64] 粘添壽，同前揭註 65。

doi:10.6342/NTU202202035

將以上 VPN 網路的三個安全機制套用至以上去中心化的聯盟鏈架構中，各金融機構間即可以使用現有的網際網路線路搭配 VPN 的保護，讓透過區塊鏈傳輸資訊的通道再加上一層保護，進而使未經允許的人無法接觸到機敏的資料。

綜上，區塊鏈獨特的公開金鑰加密技術，以及防止惡意竄改的雜湊演算，再加上傳輸過程的 VPN 加密保護，幾乎可以說是滴水不露的保護；相較中心化架構，負責保存資料的機構，必須投入大筆資金，建置最高防護等級的資訊環境；而去中心化的區塊鏈技術，是把資料以分散式區塊鏈技術存放在各金融機構，金融機構也是公認目前資訊安全防護投入金額相對高的，即便是某一個節點被攻破，區塊鏈的加密防護技術也能確保資料不會被竄改或是最小化的資料外洩，且集合金融機構的力量一起做資料保全的防護，對比由單一公部門機構投入龐大金額，使用去中心化區塊鏈技術，鼓勵金融機構積極參與，降低整體經費的投入，整體來說，會是不錯的選擇。

doi:10.6342/NTU202202035

第五節 區塊鏈資訊共享的國內案例

區塊鏈最主要的特色就是去中心化，許多金融科技公司在區塊鏈的應用，都是以取代銀行角色為出發點設計[65]，但這幾年，銀行也利用區塊鏈的特性，構思很多不錯的應用，既可加快交易速度，也可以節省人力，以下分享幾個金融界應用區塊鏈技術達到資訊共享的案例。

第一項 環球貿易共享區塊鏈

金管會於 2021 年 8 月 31 日核准試辦「環球貿易共享區塊鏈」，由國泰世華銀行及 7 家本國銀行，包括上海銀行、台中銀行、新光銀行、陽信銀行、遠東商銀、元大銀行、永豐銀行，以及國內兩個航運商即陽明海運與長榮海運於在 2021

[65] 區塊鏈用於金融領域之各項應用，比如 Accupass 已開通加密貨幣支付功能，可以直接以加密貨幣支付；投資平台的 eToro 推出加密貨幣錢包，支援用戶存儲比特幣、比特現金、以太幣以及萊特幣 4 種加密貨幣進行投資；跨境支付的 Ripple，推出分散式帳本技術服務的「xRapid」，目的在加速進行國際支付匯款。

doi:10.6342/NTU202202035

年 9 月 23 日共同宣布參與加入在此共享區塊鏈上共享貨運提單資訊，目的在於解決企業重複融資與資料造假問題[66]。

環球貿易共享區塊鏈主要有二大功能：

I. 讓聯盟銀行可在區塊鏈平臺上，查詢企業是否有重複融資。[67]

II. 透過航運介接航運資料，解決資料造假的問題。[68]

區塊鏈技術面臨最大的挑戰，在於資訊安全及系統的穩定，此外各銀行交易的隱私保全在應用區塊鏈技術時也會是一大挑戰。環球貿易共享區塊鏈是台灣首創以區塊鏈技術推動企業間金融資料交換的金融同業平臺，設計上為聯盟鏈方式，被允許的業者才能上鏈，底層架構是以「Hyperledger Fabric」為主，並透過 SHA256 雜湊演算法（Hash function）不可逆的加密方式，讓金融機構可以在安全可控的平

[66] 李靜宜（2021），<8 家銀行 2 大航商共組環球貿易共享區塊鏈，金管會核准試以解決企業重複融資與資料造假問題>，《iThome》，https://www.ithome.com.tw/news/146846 ，（最後瀏覽日：07/07/2022）。

[67] 李靜宜，同前揭註 70。

[68] 李靜宜，同前揭註 70。

doi:10.6342/NTU202202035

臺上，應用區塊鏈技術驗證供應商所以提供的文件，例如發票、訂單，進而可比對航運業者所提供的文件，可以減少人工照會的不便性，也提高作業效率[69]。

根據國泰金控所公布的資料，環球貿易共享區塊鏈的運作如下圖：

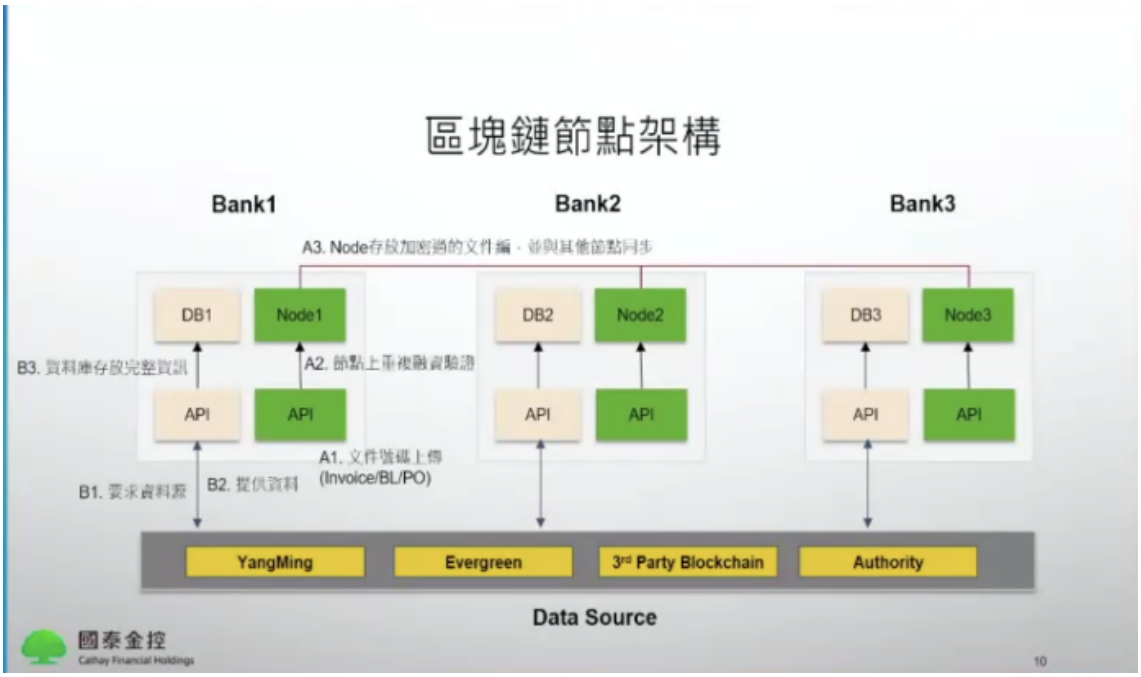

圖 9 環球貿易共享區塊鏈架構（資料來源：國泰金控新聞稿）

目前該聯盟共有 8 家銀行及 2 家海運，但未來可能會有更多其它的區塊鏈聯盟例如全球兩大航運區塊鏈聯盟全球航運商業網路（Global Shipping Business Network，GSBN）以及 TradeLens，其中各節點的銀行或公司即可以透過 API 的方

[69] 莊丙農（2021），<國泰世華「環球貿易共享區塊鏈」金管會核准試辦>，《工商時報》，https://ctee.com.tw/livenews/aj/chinatimes/20210923002319-260410 ，（最後瀏覽日： 07/07/2022）。

doi:10.6342/NTU202202035

式，分享自身資料庫並將資料上鏈，或是透過 API，將鏈上的資料取回使用比對[70]；根據國泰金控數位架構發展部協理陳維銘表示「未來國泰會進一步將不同的區塊鏈聯盟逐一搭配，建立一個金融與非金融業務交錯的生態體系」[71]。

第二項 保險業理賠聯盟鏈

金管會在 2020 年 3 月，核准國內 11 家保險公司，可以透過區塊鏈技術共享資訊，參與的壽險公司有新光人壽、國泰人壽、台灣人壽、 南山人壽、富邦人壽、元大人壽、中國人壽、全球人壽、第一金人壽，產險公司則有國泰產險及富邦產險，由此 11 家保險公司與壽險公會組成的「保險業理賠聯盟鏈」在 2020 年 7 月 1 日正式上線，預計試辦六個月，之後英國保誠人壽、三商美邦人壽、遠雄人壽、安聯人壽、中華郵政、AIA 友邦人壽、法國巴黎人壽及安達人壽等 8 家保險公司也表示有意願加入保險業理賠聯盟鏈[72]

[70] 李靜宜，同前揭註 70。

[71] 李靜宜，同前揭註 70。

[72] 高敬原（2020），<1 家申請、多家理賠！11 家業者組「理賠大聯盟」，保險業＋區塊鏈激出哪些新火花？>，《數位時代》，https://www.bnext.com.tw/article/58303/union-claim-change ，（最後瀏覽日：07/07/2022） 。

doi:10.6342/NTU202202035

保險業理賠聯盟鏈的目的，是希望透過區塊鏈的共享資訊的特色，做到「單一申請、文件共通」的效果，便利保戶也加快保險公司的作業效率。根據國泰人壽表示，聯盟鏈共通的資料，可以分為兩大層面：

I. 個人資料變更：保戶若要變更保單的姓名、身分證字號、地址、電話、電子信箱、電話號碼，只需要在其中一家保險公司申請變更，其他參與試辦的保險公司就會同步更新資料。[73]

II. 理賠申請：保戶需要申請理賠時，只需要向其中一家保險公司提出申請，「理賠聯盟鏈」會將資料同步給其他保險公司受理。但需要注意的是，根據金管會規定，於試辦期間內，申請理賠保單僅限定傷害險和健康險的醫療給付，而排除團險與旅平險。[74]

至於保戶最關心的個人資料安全問題，聯盟鏈背後結合區塊鏈技術的結果，會將保戶同意共享的資料儲存在區塊鏈上，而區塊鏈因為具備分散式儲存驗證的特性，所有的變更紀錄都會在鏈上同步，故未來有任何爭議事件發生時，都有資料可

[73] 高敬原，同前揭註 76 。

[74] 高敬原，同前揭註 76 。

doi:10.6342/NTU202202035

以舉證，足以保障保戶權益[75]；除此之外，保險業理賠聯盟鏈更結合中華電信的結合數位封包加解密與惡意檔案檢測等技術建造平台[76]。

保險業理賠聯盟鏈的運作幾乎符合本文以上分析的聯盟鏈資訊共享運作模式。因為中華電信為網路數據的服務商，可以提供 VPN 傳輸服務予聯盟鏈上的業者，確保個人資料在區塊鏈的傳遞過程中不會被惡意擷取並破解。

另外，如上述，聯盟鏈並非完全去中心化的架構，故需要有公信力的獨立機構負責管理聯盟鏈，此處壽險公會有可能扮演此角色，不需花太多人力及費用，就可以讓整個保險業理賠聯盟鏈安全運作。

第六節 小結

以洗錢防制為目的的資訊共享，必須在法規核准的範圍內才得以施行，中心化方式管理是必然的作法，世界各國，包含本文分析的美國、澳洲以及新加坡，都是

[75] 區塊鏈最要的特點為其不可竄改性，其為分散式帳方式，每本資料都會被分散儲存在不同的區塊，一旦資訊記錄上鏈，就難有人可以善自修改某筆記錄，這功能在比特幣交易已得到實際驗證。

[76] 中華電信資安艦隊先進網路防禦系統服務，於中華電信機房建置高效能、高穩定性以及防禦功能優異的資安服務，協助企業客戶阻絕來自網際網路的功擊，建置 VPN 虛擬通路，保護企業檔案傳輸安全。

doi:10.6342/NTU202202035

採用中心化的方式，由公部門設立平台，提供金融機構間可以互相資訊共享；美國及新加坡都是屬於行政型的 FIU，係指在行政或監理機關下設置的 FIU，作為申報金融機構與執法機關間之緩衝機制，在此架構下，可直接由 FinCEN 及 MAS 做為中心化資訊共享的平台；而澳洲及我國，都是屬於執法型的 FIU，參考澳洲 AUSTRAC 是另外成立公私合作的 Fintel Alliance，以實體辦公室運作，而我國也可以參考其作法，但把實體辦公室轉化成線上虛擬辦公室，使用區塊鏈技術，在公部門主導的聯盟鏈虛擬辦公室上分享其資訊，以分散式帳本方式互相溝通分享資訊，而這些資訊分散存放在各金融機構，透過區塊鏈獨特的加密技術，以及防止惡意竄改的雜湊演算，再加上傳輸過程的 VPN 加密保護，讓整個資訊分享過程如同在實體辦公室一樣的安全，當然，其鏈的管理者還是由公部門主導，提供有彈性的，且符合法令規定的方式共享其資訊。

雖是以打擊犯罪為目的的資訊共享，但在法律層面上是否可行？以下章節分析之。

doi:10.6342/NTU202202035

第四章 資訊共享之法律問題

以防制洗錢為目的之資訊共享，分享的內容有可能涉及金融機構客戶的個人資料或交易資料，故雖然是以打擊犯罪為目的的資訊共享，但仍需探討其法律上的可行性。本章即探討以洗錢防制為目的之資訊分享可能面臨的法律議題。

第一節 我國法規現況

資訊共享在法律層面上，碰到的最大兩個問題即是隱私與資料保護以及金融機構的保密義務規定，於我國現行法律下具體規定於個人資料保護法、銀行法以及金融控股公司法。相關規定在某些層面上，的確限制資訊共享的發生，而行政機關也已適度發布辦法或指引，有條件的放寬資訊共享的範圍及內容，其法規現狀為何，分析如下。

第一項 我國資訊共享之法律問題

第一款 個人資料保護法

資料保護和隱私問題在我國法律規定下主要由個人資料保護法規範之。金融機構基於洗錢防制之目的蒐集與分享客戶個人資料，此際即可能涉及個人資料保護法相關規定。

doi:10.6342/NTU202202035

依個人資料保護法第 20 條第 1 項規定：「非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之」。針對金融機構可否適用上開規定中的第 2 款規定主張個人資料之利用係屬「增進公共利益所必要」？金融機構在符合個人資料保護法第 5 條之規定「尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯」之下，蒐集個人或企業相關一般性資訊（即非醫療、基因、性生活等敏感性資訊），似乎符合大眾理解因開立帳戶所需之資訊，當然金融機構也必須在符合金融交易相關的目的，合理使用客戶的個人資料。如放大以臺灣整體社會福祉來看，金融機構以打擊犯罪為目的的資訊共享，似乎有空間可以主張符合上開第 2 款「增進公共利益」，但如此一來，似乎違反了上述個人資料保護法第 5 條之規定，因為資訊共享並非當事人認為金融機構收集個人資訊的目的之一，由此分析，並不能單純以增進公共利益為由而進行資訊共享。

就上述議題，法務部民國 106 年 1 月 26 日法律字第 10603501350 號函釋曾指出金融機構利用集保公司統一建置資訊系統，而將保有客戶資料與洗錢防制名單進行比對，乃在發揮洗錢防制名單資料庫最大效應，以落實洗錢防制要求，故應可認符合個人資料保護法第 20 條第 1 項但書第 2 款「增進公共利益所必要」。法務部並補充指出，依據洗錢防制法第 7 條第 1 項及第 8 條規定，金融機構對於達

doi:10.6342/NTU202202035

一定金額以上之通貨交易應確認客戶身分，故本質上須透過資訊協助建置，並透過定期更新資訊以達洗錢防制目的；但自建置查詢系統對於規模較小之金融機構造成沉重負擔，所以金融機構委託集保公司統一建置資訊系統，提供服務給予較小型的金融機構。

依據上開函釋，法務部似乎認為基於洗錢防制之目的，可以認為符合個人資料保護法中「增進公共利益所必要」。但上述函釋的見解是否也可以適用於其它基於洗錢防制或打擊犯罪為目的之金融機構間資訊共享？就此筆者認為，集保公司的資訊系統是提供名單查詢服務給予較小型的金融機構使用，有資訊共享的感覺，但於實際運作上，集保公司共享的名單，其實是資恐防制法公告的制裁名單[77]以及名單資料庫廠商提供的名單資料，比如 Dow jones 或是 Refinitiv World-check，而這些名單都是屬於相對公開資訊，並無保密之義務與責任或個人資料保護的顧慮；相較而言，本文討論的資訊共享之資訊，係屬於客戶本身有關的一般個人資訊，故集保公司共享的名單資訊固然可以符合「增進公共利益所必要」，根據個人資料保護法第 19 條第 1 項第 3 款之規定，就可以逕行蒐集並分享，也沒有侵害當事人個人

[77] 例如 UN、OFAC、EU 以及我國等公告的制裁名單。

doi:10.6342/NTU202202035

資料的問題；和本文討論的資訊共享範疇涉及未公開的個人資料而不可直接蒐集或處理之不盡相同。

但如果以個人資料保護法第 20 條第 1 項第 7 款「經當事人同意」作為正當化資訊共享的基礎，是否可行？

同樣係為洗錢防制作業需求，參考永豐銀行個人資料蒐集、處理及利用告知義務內容第八條規定「本行為執行洗錢防制作業並配合全球打擊犯罪、遏止資恐及毀滅性武器擴張之目的，當下列情形發生時，臺端同意本行將其個人資料提供境外金融機構：（一）客戶為受經濟制裁、外國政府或國際洗錢防制組織認定或追查之恐怖分子或團體、資恐防制法指定制裁之個人、法人或團體。（二）本行於定期或不定期審查客戶/受益人/有效控制帳戶之人/關聯人身分作業或認為必要時（包括但不限於：懷疑客戶涉及非法活動、疑似洗錢、資恐活動，或媒體報導涉及違法之特殊案件等)」。可知銀行業者也會彈性使用資法第 20 條第 1 項第 6 款「經當事人同意」之規定，事先取得客戶同意，以符合個資法相關規定。

但是，如果客戶不同意呢？銀行是否可以拒絕開戶交易？根據金融消費者保護法第 10 條第二項規定：「不得僅因金融消費者拒絕授權向經營金融機構間信用資料之服務事業查詢信用資料，作為不同意授信之唯一理由」，所以如果銀行用此

doi:10.6342/NTU202202035

當做拒絕開戶的理由，不容易被社會大眾接受，而且這不符合銀行服務客戶的目的，畢竟銀行是屬於特屬行業。但會不會有其它銀行是可以接受並可交易的？不管以上為何，單以「經當事人同意」之規定事先約定，可能無法完全達到以打擊犯罪為目的的資訊共享。

第二款 銀行法與金融控股公司法

除個人資料保護法之限制外，銀行法第 48 條第 2 項規定「銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密」，其意旨在保障銀行客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。司法院大法官會議釋字第 293 號解釋亦指出「銀行法第四十八條第二項規定『銀行對於顧客之存款、放款或匯款等有關資料，除其他法律或中央主管機關另有規定者外，應保守秘密』，旨在保障銀行之一般客戶財產上之秘密及防止客戶與銀行往來資料之任意公開，以維護人民之隱私權。惟公營銀行之預算、決算依法應受議會之審議，議會因審議上之必要，就公營銀行依規定已屬逾期放款中，除收回無望或已報呆帳部分，仍依現行規定處理外，其餘部分，有相當理由足認其放款顯有不當者，經議會之決議，在銀行不透露個別客戶姓名及議會不

doi:10.6342/NTU202202035

公開有關資料之條件下，要求銀行提供該項資料時，為兼顧議會對公營銀行之監督，仍應予以提供。」

由司法院大法官會議釋字第 293 號及解釋及銀行法第四十八條第二項規定可知，我國法律對於個人隱私之保護相當嚴密，即使是台北市議會以對公營銀行監督為由決議要求銀行透露個別客戶姓名，該理由亦屬正當，但仍被司法院大法官會議釋字第 293 號解釋駁回。

鑑於銀行法 48 條保密義務規定儼然已成為洗錢活動的保護傘，若干利用複雜的政商關係以權謀利、違法超貸屢見不鮮，但政府機關為打擊犯罪而調查資金來源卻因銀行法第四十八條第二項有關銀行保密義務之規定而受到限制，故相關的政策探討也逐漸提出。民國 96 年 10 月，由專題研究作者何思湘在立法院所提之專題研究報告「銀行法有關客戶資料保密義務之立法政策探討」中，即探討客戶隱私與金融監理之間如何正確拿捏得失、權衡輕重之立法政策問題，其分析結果指出「我國銀行之保密義務，已由單純之法律責任，延伸至契約責任，進而負有防制犯

doi:10.6342/NTU202202035

罪之責任。為維護金融市場秩序、加強對銀行監督管理，合理規範並確定銀行之保密義務範圍及尺度，確實有其必要性與急迫性」[78]，並提出兩項建議：

1. 就長期而論，建議參考美國或其他先進國家相關法律，制定我國之「銀行秘密法」或「財務隱私法」[79]。

2. 就短期而言，建議修正銀行法第 48 條第 2 項有關保密義務規定，將揭露客戶秘密之主客觀條件與法定程序納入規範[80]。

其中更建議於銀行法第四十八條條文中另增一項，規定「...有關銀行保密義務之除外規定，其豁免之對象、條件、範圍、法定程序及其他應遵循事項之規則，由主管機關定之。」以符合法律授權明確性原則，並加強國會對主管機關之立法監督。故為了加強監理，聯合打擊犯罪，銀行法第四十八條或許有修法的可能性[81]。

---

[78] 何思湘（2007），<銀行法有關客戶資料保密義務之立法政策探討>，《立法院》，https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6586&pid=83696，（最後瀏覽日：07/13/2022）。

[79] 何思湘，同前揭註 82。

[80] 何思湘，同前揭註 82。

[81] 何思湘，同前揭註 82。

doi:10.6342/NTU202202035

此外，銀行上開保密義務是否必然可以經由客戶同意就予以豁免？論者有持肯定說者，主張客戶同意之後，相關資料已無秘密性可言，故銀行已無保密之義務[82]；而持否定說者則主張目前並無明文規定客戶同意即可豁免此保密義務，況且即使客戶同意，也不代表銀行可以分享給其它人或業者，蓋倘若在分享或傳輸過程發生資料毀損或遺失，銀行仍有未積極保護客戶資料的過失，因此有可能受到主管機關裁罰[83]。

資訊共享議題也存在於金融控股公司的各子公司之間。例如客戶如已在同金融控股公司的銀行開戶，並踐行嚴格的 KYC 程序，倘若其又在同金融控股公司的證券公司開戶時，是否可以延用同金融控股公司的銀行端的資料？就此金融控股公司法第 42 條的保密規定以及第 43 條的共同行銷規定，也是限制金融控股公司資訊共享的障礙之一。

綜上所述，銀行法及金融控股公司法皆以已嚴格限制金控子公司資訊共享的要件，並要求金融機構必須保守秘密。但相較於個人資料保護法，銀行法及金融控股公司法更加強調其金融機構的誠信，畢竟金融機構皆屬特許行業，須由政府核可

[82] 臧正運（2022），<銀行業資料治理的法制挑戰>，《台灣法律 2022 年第 9 期》，頁 70~91。

[83] 臧正運，同前揭註 86。

doi:10.6342/NTU202202035

方可設立，而這代表人民對政府的信賴，才會將自身的財產，放心存放在金融機構；銀行法及金融控股公司法立法目的，都在於保護消費者以及維護金融機構的誠信，以打擊犯罪為目的的資訊共享在未取得民眾同意之前是否可行，仍有討論的必要。

我國主管機關近期也意識到資訊共享對於洗錢及資恐防制的重要性，故在近幾年陸續公布實施相關辦法，以供同一集團內的金融機構共享其資訊，以下繼續分析。

第二項 我國允許資訊共享之辦法說明

金融監督管理委員會（以下稱「金管會」）針對銀行、證券期貨以及其它經金管會指定之金融機構，已發布實施辦法，開放適度的資訊共享。例如「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 8 條第 10 項中提到：「金融控股公司及銀行業應建立集團整體性防制洗錢及打擊資恐計畫，包括在符合國外分公司（或子公司）當地法令下，以防制洗錢及打擊資恐為目的之集團內資訊分享政策及程序。」在此條文中，已經允許金融控股公司在符合當地法令下可以資訊共享，而實務上也的確需要，蓋同一客戶，很有可能在同一個金控或銀行的不同地區海外分行或子行開戶，因可能是使用不同的證件核實開戶，如銀行內部在不同地區間無法

doi:10.6342/NTU202202035

共享開戶資訊，很有可能造成表面上看似不同個體或機構間的金流往來，但事實上是同一個，進而在洗錢防制上可能造成誤判，如果金控或銀行內部可以在符合資料保密法規的之下，訂立資訊共享政策，對於洗錢防制會有很大的幫助。

除此之外，金管會更進一步公布，「銀行業及其他經金融監督管理委員會指定之金融防制洗錢及打擊資恐內部控制與稽核制度實施辦法」，其中第 6 條提到：「銀行業及其他經本會指定之金融機構如有分公司（或子公司）者，應訂定集團層次之防制洗錢與打擊資恐計畫，於集團內之分公司（或子公司）施行。內容包括前項政策、程序及控管機制，並應在符合我國及國外分公司（或子公司）所在地資料保密法令規定下, 確認客戶身分與洗錢及資恐風險管理目的所需之集團內資訊分享政策及程序」。在此條文中，更進一步放寬至金控或銀行之外的金融集團，要求其也都應該因應洗錢及資恐防制需求，制訂集團內的資訊分享政策，除可以減輕 KYC 客戶身份核實的難度，更可以加強全方面的洗錢防制工作。

在證券期貨部份，「證券期貨業及其它經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法」第 4 條第 4 項規定：「證券期貨業及其他經本會指定之金融機構如有分公司（或子公司）者，應訂定集團層次之防制洗錢及打擊資恐計畫，於集團內之分公司（或子公司）施行。內容包括前項

doi:10.6342/NTU202202035

政策、程序及控管機制，並應在符合我國及國外分公司（或子公司）所在地資料保密法令規定之情形下，訂定下列事項：

一、確認客戶身分與洗錢及資恐風險管理目的所需之集團內資訊分享政策及程序。

二、為防制洗錢及打擊資恐目的，必要時，依集團層次法令遵循、稽核及防制洗錢及打擊資恐功能，得要求分公司（或子公司）提供有關客戶、帳戶及交易資訊，並應包括異常交易或活動之資訊及所為之分析；必要時，亦得透過集團管理功能使分公司（或子公司）取得上述資訊。

三、運用被交換資訊及其保密之安全防護，包括防範資料洩露之安全防護。」

證券期貨業的規定其實比上述的金融控股公司及銀行業內部控制及稽核制度實施辦法以及銀行業及其他經金融監督管理委員會指定之金融防制洗錢及打擊資恐內部控制與稽核制度實施辦法更為完整，尤其是其針對交換資訊的安全防護設有明確規範，要求證券期貨業內部間需在做資訊分享更加的注意及小心，值得肯定。

而在「保險公司與辦理簡易人壽保險業務之郵政之郵政機構及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資死內部控制與稽核制度實施辦

doi:10.6342/NTU202202035

法」第 5 條第 4 項規定：「保險公司、辦理簡易人壽保險業務之郵政機構及其他經本會指定機構應訂定集團層次之防制洗錢及打擊資恐計畫，於集團內之分公司（或子公司）施行。其內容除包括前項政策、程序及控管機制外，並應在符合我國及國外分公司（或子公司）所在地資料保密法令規定之情形下確認客戶身分與洗錢及資恐風險管理目的所需之集團內資訊分享政策及程序」。故保險公司的資訊分享政策與上述的銀行及證券期貨公司類似，都必須先擬定集團資訊共享之辦法。

綜上，金融監督管理委員會針對金融控股公司、銀行業、證券期貨業以及保險公司，都已公布資訊共享相關的實施辦法，目的就是希望允許集團內，允許以打擊犯罪為目的的資訊共享。由此以觀，我國現行法下，資訊共享在金融集團內是完全可行且符合 FATF 建議的，但集團外例如金融機構同業間基於打擊犯罪為目的的資訊共享，目前因無法可遵循，再加上上述討論的個人資料保護法、銀行法以及金融控股公司法的約束，故尚無資訊共享的空間。

其它世界各國，是採用什麼方法開放保障金融機構在資料安全的狀況下進行資訊共享，以下章節分析之。

doi:10.6342/NTU202202035

第二節 世界各國在資訊共享之法律問題因應

第一款 FATF 建議

FATF 在 2017 年 11 月公布的私部門資訊共享指引（FATF Guidance on Private Sector Information Sharing）中，已指出資訊共享對於洗錢與資恐防制的好處，故訂定此指引做為世界各國建立資訊共享的參考依據[84]，該指引也提出一般資訊共享可能面臨的法律問題，例如指引中提到法律規定可能會限制基於洗錢或資恐防制目的而提供、存取、共享以及處理資訊，其背後因素可能包括相異的政策目標、客戶資料保密的顧慮，以及記錄留存要求。於部分案例中，受規範的實體對法律制度所允許的共享範圍有不確定性，這種不確定性導致阻礙有效的資訊共享。有鑑於此，各國應克服挑戰，針對不同法規實施有效的資訊共享制度，並針對相關法規提供適當的釐清與指導，藉此消除資訊共享的法規相關歧義[85]。

歸納上述觀察，資訊共享背後最大的挑戰因素有兩個：

---

[84] FATF, *FTAF Guidance-Private Sector Information Sharing*（Nov, 2017）, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf（last visited July 7, 2022）.

[85] *Id*. at 4.

doi:10.6342/NTU202202035

1. 不同的資料保護和隱私 （data protection and privacy，DPP）法律架構和施行狀況：

i. 洗錢與資恐防制法規旨在預防、發現、阻斷、調查以及起訴 洗錢或資恐案件，但其必須兼顧個人資料和隱私權的保護。故 FATF 指出洗錢與資恐防制和資料保護和隱私的公共政策目標並非相互排斥，應可以倡導並達到平衡。[86]

ii. 洗錢與資恐防制和資料保護和隱私此二目標之間存在明顯牴觸，可能是因為各主管機關在法規制定上並未充分協調，導致保護資料和預防及打擊犯罪之間缺乏適當平衡。故 FATF 即使允許共享資訊，資料保護和隱私的法律處罰和風險規避的擔憂，都對私部門的資訊提供、存取、處理、共享資訊的意願產生重大影響。[87]

iii. 如果主管機關能夠進一步清楚說明資料保護和隱私在何種公共利益之前提下，基於洗錢與資恐防制目的可跨境共享個人資料的許可範圍為何，或是說明不同資料保護規範對資料傳輸的限

[86] *Id*. at 6-7.

[87] *Id*.

doi:10.6342/NTU202202035

制，這對據點跨越多個司法管轄區的全球金融機構將更有助益。[88]

iv. 各國應視需要修改或澄清相關法規，以確保適當的平衡。建議負責資料保護和隱私及洗錢與資恐防制的國家主管機關展開更多對話交流，採用相容一致的政策，盡可能協助金融機構符合法規要求。[89]

2. 金融機構的保密規定。金融機構適用的相關保密法規可能會限制資訊共享，例如，根據國家立法，金融機構的保密義務有時不會因具有「正當利益」 或安全顧慮而豁免。[90]

依照上述 FATF 指引，雖然資訊共享對於打擊洗錢及資恐有其重要性及必要性，但 FATF 的專家也理解，各國因法律制度及政府關運作關係，具體推動時會有其推動的困難性，甚至需要修法來解決這個問題。以下即以就美國、新加坡以及澳洲為例，分析其資訊共享時的法律問題解決方式。

[88] *Id*.

[89] *Id*.

[90] *Id*.

doi:10.6342/NTU202202035

第二款 美國、新加坡及澳洲之法律問題因應

美國在愛國者法案 314(b)有關允許資訊共享範圍的指引係採用安全港（safe harbor）方式處理資訊共享的法律問題，具體而言，在 Section 314(b) 安全港條款保護之下，允許兩個以上的金融機構或金融機構協會可以相互共享有關涉嫌可能的恐怖主義或洗錢活動的個人、實體或組織的相關訊息，而金融機構也必須嚴格遵守相關的要求，包括向 FinCEN 發出通知，也必須確認對方的金融機構是否也符合 Section 314(b) 安全港條款的相關規定，以及限制資訊不能隨意對外公開。[91]

如同上述 FATF 指引，資訊共享基本上會與各國的資料保護和隱私以及金融機構的保密規定有所抵觸，所以 FinCEN 以安全港的方式，保證金融機構在 314(b) 的規定下資訊共享的合法性，藉此鼓勵資訊共享，截至 2019 年底的統計，已經有超過 7,000 家的金融機構參與資訊共享。

[91] FinCEN, supra note 7.

doi:10.6342/NTU202202035

新加坡的個人資料保護法的規範主體為非公務機關[92]，所以如果由 MAS 主導的資訊共享平台，並不會有太大的法務問題，而新加坡 MAS 在 2021 年 10 月公布的 Consultation Paper- FI-FI information Sharing Platform for AML/CFT，更進一步提及資訊共享的法律依據。該諮詢文件提及，FSMA 將規定資訊共享平臺 COSMIC 的法律框架，以及金融機構之間因為 AML/CFT 目的風險資訊共享機制，以及針對從金融機構獲得的資訊的使用和保密規定保障措施。另外，針對參與 COSMIC 的金融機構，倘若其係採取合理的謹慎措施且係在 COSMIC 平臺上提供資訊，並且基於善意行事，則 MAS 也規劃提供其免於民事責任的法定保護，藉此鼓勵金融機構參與資訊共享。[93]

澳洲 AUSTRAC，是以成立公私部門協力的 Fintel Alliance 辦理資訊共享，具體而言澳洲 Fintel Alliance 是以成立實體辦公室的方式，結合公部門與各金融機構一起研究洗錢及資恐相關資訊，如有需要其它資訊，會由 Fintel Alliance 成員向其

[92] TPIPAS 制度維運小組（2012），<新加坡個人資料保護法之現況與比較>，《資策會科技法律研究所》，頁 59。

[93] MAS, supra note 22.

doi:10.6342/NTU202202035

金融機構要求提供，在法律上的依據是根據 Section 167 of the AML/CFT Act[94]，而這些資訊只會在 Fintel Alliance 的實體辦公室研究分析，個人資料外洩的機率大幅降低，而銀行保密的問題獲得解決，基本上避免掉個人資料保護法以及銀行保密的問題。

第三節 我國資訊共享之思考與實踐

資訊共享的主要意義，是希望藉由金融機構之間資訊分享，達到聯合打擊犯罪的目的。而為讓金融機構願意分享疑似犯罪的資訊，主管機關必須先解決兩件事，第一個是法律問題，第二個是金融機構參與的意願。

在資訊共享的法律議題上，美國是以 FinCEN 314(b) 的相關規定，金融機構可以在法律安全保障的狀況之下共享其資訊；而新加坡責是由公部門的 MAS 成立 COSMIC 新平台，在 COSMIC 法律框架之下，對於善意行事的金融機構，提供免於民事責任的法定保護；而澳洲則是依據 Section 167 of the AML/CFT Act，由

[94] Australian Government（2006）, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, https://www.legislation.gov.au/Details/C2021C00243 (last visited July 13, 2002).

doi:10.6342/NTU202202035

AUSTRAC 成立獨立的 Fintel Alliance，公部門及金融機構可以在實體辦公室資訊共享。

而在金融機構參與的意願上，美國的金融機構在 FinCEN 的安全港保護之下已經有超過 8000 家參加，且持續增加中，參與的金融機構還算踴躍；而新加坡目前雖只有六家銀行參加 COSMIC 平台，但以目前揭露的文件顯示，未來是強制所有金融機構都要參加；而澳洲的 Fintel Alliance，根據 Fintel Alliance Performace Report 2019-20 的報導，約為 28 家公私部門參與，在泡泡隔離的獨立環境下共享其資訊，免除其法律問題的干擾。

至於我國的現況，除已公布之金融集團內共享資訊之實施辦法之外，金管會在 2021 年 12 月 23 日訂定的「金融機構間資料共享指引」的指引背景中也提到：「金管會將推動金融機構間之資料共享機制，列為金融科技發展路徑圖之重要推動措施，並訂定本指引，明確揭示金融機構間共享之機制，亦減少各機構因重複建置與維護客戶資料所增加之營運成本，及提升效率、發揮加乘效益」。由此可見，金融資訊共享的推展將會是金管會 2022 年的重要工作項目。

目前依法令得共享的資料包括基於共同行銷、洗錢防制及合作推廣目的的資料共享，金管會的金融機構間資料共享指引並將之區分為三類，第一類是金融控股

doi:10.6342/NTU202202035

公司與所屬金融機構子公司間，及金融控股公司所屬之各金融機構子公司間；第二類為非屬金融控股公司之金融機構與所屬金融機構子公司間，及非屬金融控股公司之金融機構與所屬金融機構子公司間；第三類是非屬上述二類之金融機構與金融機構間。不過金融機構間資料共享指引係屬行政指導，其目的在於鼓勵金融機構基於特定目的可以資訊共享，而此指引的規範也再特別強調：「應事先取得客戶同意，落實客戶權益之保障，確保個人資料之保護，確保資料傳輸之安全，訂定妥適之內部管理政策」，換言之，本文上述提到的個人資料保護法、銀行法以及金控法相關規定，仍需嚴格遵守。在上述的討論中，也已知曉「應事先取得客戶同意」在資訊共享窒礙難行的問題。

除此之外，依據目前洗錢防制法第 17 條之規定，公務人員及金融機構人員不具公務員身分不得洩露或交付申報疑似案件，所以法務部在民國 110 年 12 月 28 日公告的「洗錢防制法」修正草案修正第 17 條第 3 項規定，增訂基於防制洗錢目的而為之資訊交流或共享，相關辦法並授權法務部定之，此目的似乎是要解除公部門及私部門因洗錢防制需求，可以有條件的分享資訊。

doi:10.6342/NTU202202035

有鑑於洗錢防制法是特別法，故的確可以以修法的方式，避免個人資料保護法、銀行法以及金融控股公司法的限制，但這方面討論的層面可能會非常大，畢竟這跟社會大眾的權益有關，還有銀行的保密義務也會受到嚴重的挑戰。

而要如何提高金融機構參與的意願，以上的修法當然是重點之一，而資訊共享的方法也是另一個考慮的因素，本文提出的的區塊鏈技術方式的資訊共享，本質上還是屬於中心化，只是採取去中心分散式帳本方式將資訊分散存放在各金融機構，所以在資訊共享的法律議題討論上，與完全中心化的架構基本上是一樣的

本文認為，洗錢防制法第 17 條第 3 法修法至關重要，而參考美國 FinCEN 的安全港方式，或是參考新加坡方式，由主管機關出面背書，讓金融機構間可在主管機關認可的平台或方式辦理的洗錢防制資訊共享，並可以享有豁免於相關法律責任的法定保護，讓金融機構有意願能主動參加資料共享，會是未來資訊共享法制設計的關鍵。

doi:10.6342/NTU202202035

第五章 結論

以打擊犯罪為目的的資訊共享，在洗錢及資恐防制，是相當重要的課題之一，近幾年，各金融機構都已砸下重金在洗錢及資恐防制相關工作，並也都依照規定申報主管機關，如果未來可以在金融機構間辦理相關的資訊共享，聯合打擊犯罪的效果會更好。本文的前段也以 FATF 的建議，以及美國、澳洲以及新加坡為例，說明資訊共享的重要性以及資訊共享後的成果。

上述國家雖然皆是以中心化架構設計資訊共享，但本文嘗試提出不同的想法，先是分析中心化與去中心化的優缺點，並考量我國洗錢防制監管架構的特性後，提出以區塊鏈技術為基礎的去中心化設計，使用具有彈性的聯盟鏈架構，由公部門負責管理，再加上 VPN 的私人通道保護，不論是傳輸過程，或資料保護上，都盡量做到滴水不漏的的加密架構設計，以保障金融機構聯盟鏈間資訊共享的安全性。

在法律議題也是各國資訊共享最需解決的問題。FATF 指出資訊共享需先解決資料保護和隱私以及金融機構的保密規定，在我國，金融機構基於洗錢防制目的分享客戶資訊是否符合個人資料保護法下蒐集、處理及利用個人資訊的要求，恐有疑義，不容易在未取得當事人同意的前提下取得資訊共享的合法基礎；再加上銀行法以及金融控股公司法對於金融機構的保密責任要求，更讓金融機構間資訊共享的

doi:10.6342/NTU202202035

空間有限；未來法務部主導的「洗錢防制法」修正草案也必需針對第 17 條增訂基於防制洗錢目的而為之資訊交流或共享，解除其分享資訊之法律限制，以及避免個人資料保護法、銀行法及金融控股公司法的干擾。本文更進一步建議我國或許可以參考 FinCEN 的安全港方式，或是新加坡方由主管機關擔保金融機構間之資訊共享可以享有豁免於民事責任的法定保護，鼓勵金融機構參與資訊共享，加快金融機構間資訊共享的腳步，並輔以去中心化的聯盟鏈資訊共享方式的架構，讓資訊安全可以更完整，讓範圍更擴大，以最少經費，聯合大家的力量，共同打擊犯罪。

區塊鏈技術，因虛擬貨幣的盛行，而聲名大噪，其去中心化的概念，更讓大家對於未來的數位時代，有無限的想像；雖然在金融科技領域，無法完全做到去中心化的方式，但其區塊鏈分散式帳本之技術運用，特別是在跨領域的資訊共享，能以最少經費，最安全的方式，讓更多的公部門及金融機構可以透過去中心化的技術，在鏈上安全的分享資訊，也期待透過本文的分析，可以推動區塊鏈技術於洗錢防制之運用，提高金融機構開戶效率，加強聯合打擊犯罪。

doi:10.6342/NTU202202035

參考文獻：

一、中文

1. 中文書籍

詹德恩（2021）。《法令遵循理論與實務》。台北：元照。

台灣金融研訓院（2019）。《防制洗錢與打擊資恐-實務與案例》。台灣金融研訓院。

王毅丞（2018）。《實戰區塊鏈技術，加密貨幣與密碼學》。台北：碁峯。

大和總研 Frontier Technology（2020）。《圖解 Fintech 的知識與技術》。台北：碁峯。

Paul Vigna & Michael J.Casey（2019）。《The Truth Machine 真理機器-數位時間的新憲法》。台北：大牌出版。

Camila Russo（2021）。《以太奇襲，一位 19 歲天才，一場數位與金融革命》。台北：早安財經文化。

2. 期刊論文

doi:10.6342/NTU202202035

呂嘉穎（2020）。〈初探區塊鏈之不可竄改特性、匿名性所衍生的法律問題〉，《交大法學評論》，第 6 期，頁 10-19 。

臧正運（2021）。〈探尋資料受信者，在開放銀行下的監理座標〉，《中正財經法學》，第 23 期。

徐珮菱（2019）。〈區塊鏈（Blockchain）與歐盟一般資料保護規則（GPDR）之適用〉，《財金法學研究》，第 2 卷第 4 期。

鄭婷嫻（2018）。〈區塊鏈技術應用於我國公司法理法制之研究〉，《東吳法律學報》，第 30 卷第 3 期。

臧正運（2022）。〈銀行業資料治理的法制挑戰〉，《台灣法律人》，No.9 。

吳盈德（2017）。〈創新金融科技與洗錢防制趨勢〉，《月旦法學雜誌》，No.267 。

TPIPAS 制度維運小組（2012）。<新加坡個人資料保護法之現況與比較>，《資策會科技法律研究所》，頁 59。

3. 學位論文

周靖媛（2020）。《虛擬通貨交易民事法律關係之研究-以虛擬通貨交易平台為中心》，國立臺灣大學法律學院法律學系碩士論文，台北。

doi:10.6342/NTU202202035

魯志遠（2020）。《區塊鏈技術運用於數位證據之研究-以刑事數位證據之蒐集與鑑識為例》，中原大學財經法律學系碩士學位論文，桃園。

邱佳儀（2021）。《我國銀行發展區塊鏈供應鏈金融之研究》，淡江大學國際企業學系，新北。

4. 計劃報告

法務部調查局（2020）。《洗錢防制工作年報》。

FATF 報告（2017）。《私部門資訊共享》。

何思湘（2007）。《銀行法有關客戶資料保密義務之立法政策探討》，立法院專題研究。

5. 決議、解釋、函令或研究意見

金融監督管理委員會（2021）。金融機構防制洗錢辦法。

法務部（2017）。法律字第 10603501350 號，中華民國 106 年 01 月 26 日。

金融監督管理委員會（2019）。華總一經字第 10800037891 號令修正，中華民國 108 年 04 月 17 日。

大法官解釋（1992）。釋字第 293 號，中華民國 81 年 3 月 13 日。

doi:10.6342/NTU202202035

6. 網路資料

法務部網站（2017）。《法務部新聞稿：我國已脫離亞太防制洗錢組織（APG）第二輪評鑑之過渡追蹤程序，繼續爭取第三輪評鑑佳績》，載於 https://www.moj.gov.tw/media/14504/772619593112.pdf?mediaDL=true。

天下雜誌（2016）。《兆豐銀何被罰 57 億？》，載於 https://www.cw.com.tw/article/5077992。

行政院網站（2018）。《我國第 3 輪實地相互評鑑結果》，載於 https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/bdf44d9a-f4f0-43aa-99f2-771f612983acAPG。

鉅享網（2018）。《反洗錢意識高漲 公股銀行法遵成本飆高》，載於 https://news.cnyes.com/news/id/4121196 。

DOW JONES 網站。《Dow Jones Risk & Compliance 是一家提供一流風險數據、集成技術解決方案和盡職調查服務的全球供應商，旨在對監管風險和商譽風險進行管控》，載於 https://visit.dowjones.com/risk/lp/cn/risk-and-compliance/ 。

doi:10.6342/NTU202202035

金管會網站。《今日訂定「金融機構間資料共享指引」》，載於 https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202112230006&dtable=News。

AWS。《Amazon 雲端服務》，載於 https://aws.amazon.com/tw/。

Azure。《Microsoft 雲端服務》，載於 https://azure.microsoft.com/zh-tw/。

Google Cloud。《Google cloud 雲端服務》，載於 https://cloud.google.com。

蔚藍問答。《INTERNET 的起源？》，載於 https://weilan.cool/game/245443.html。

程式人生。《Internet、Intranet 和 Extranet 之間的區別》，載於 https://www.796t.com/p/1421476.html。

翻轉工作室：粘添壽。《廣域網路之連接型態》，載於 http://www.tsnien.idv.tw/Internet_WebBook/chap4/4-2%20 廣域網路之連接型態.html。

翻轉工作室：粘添壽。《VPN 網路規劃與管理》，載於 http://www.tsnien.idv.tw/Manager_WebBook/chap10/10-1%20 虛擬私有網路簡介.html。

doi:10.6342/NTU202202035

Ithome（2021）。《8 家銀行與 2 大航運商共組環球貿易共享區塊鏈，金管會核准試辦以解決企業重複融資與資料造假問題》，載於 https://www.ithome.com.tw/news/146846。

數位時代（2020）。《1 家申請、多家理賠！11 家業者組「理賠大聯盟」，保險業＋區塊鏈激出哪些新火花？》，載於 https://www.bnext.com.tw/article/58303/union-claim-change。

永豐銀行。《永豐銀行履行個資法第八條告知義務》，載於 https://mma.sinopac.com/mma8/term/HouseLoan/永豐銀行履行個資法第八條告知義務.html。

金管會網站。《金融機構間資料共享指引總說明及逐點說明》，載於 https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202112231015490.pdf&filedisplay=金融機構間資料共享指引總說明及逐點說明.pdf。

二、英文

1. 網路資料

doi:10.6342/NTU202202035

REFINITIV 網站。《Access accurate and structured information to help you meet you KYC and Third-party due diligence screening obligations》，載於 https://solutions.refinitiv.com/world-check-kyc-screening/?utm_content=Product%20Name-TW-APAC-G-MAN-Exact&utm_medium=cpc&utm_source=google&utm_campaign=434523_PaidSearchTE&elqCampaignId=13796&utm_term=world%20check&gclid=Cj0KCQiArt6PBhCoARIsAMF5wagHVjlfxMr2wa-0C6AGnkf6gpvhsbITc0DNt5SvPSsVYTZpBngmHB0aAjZIEALw_wcB&gclsrc=aw.ds。

FATF 網站（2017）。《FATF Guidance，Private Sector Information Sharing》，載於 https://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf 。

FinCEN.gov（2020）。《Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another. December 2020》，載於 https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf 。

FinCEN.gov（2020）。《Participation and Reporting》，載於 https://www.fincen.gov/sites/default/files/shared/314bparticipationinfo.pdf。

doi:10.6342/NTU202202035

FinCEN.gov（2016）。《314(b) References in Suspicious Activity Reports (SARs) Suggest Increased Information Sharing Among Financial Institutions》，載於 https://www.fincen.gov/sites/default/files/shared/314bInfographic.pdf 。

AUSTRAC 網站。《AUSTRAC is responsible for preventing, detecting and responding to criminal abuse of the financial system to protect the community from serious and organised crime》，載於 https://www.austrac.gov.au。

AUSTRAC 網站。《Fintel Alliance 2020-21 AUSTRAC ANNUAL REPORT》，載於 https://www.austrac.gov.au/sites/default/files/2021-11/FintelAlliance_PerformanceReport20-21_v5_Web.pdf。

Australian Government 網站。《Anti-Money Laundering and Counter-Terrorism Financing Act 2006》，載於 https://www.legislation.gov.au/Details/C2021C00243。

MAS 網站。《Monetary Authority of Singapore》，載於 https://www.mas.gov.sg。

MAS 網站。《Consultation Paper FI-FI Information sharing Platform for AML/CFT》，載於 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/1-Oct-2021-FI-FI-Information-Sharing-Platform-for-AMLCFT/Consultation-Paper-on-FI-FI-Information-Sharing-for-AMLCFT.pdf。

doi:10.6342/NTU202202035

FSMA 網站。《Financial Services Managers Association》，載於 https://fsma.org.sg。

Federal Reserve 。《Board of Governors of the Federal Reserve System》，載於 https://www.federalreserve.gov。

OCC 網站。《Office of the Comptroller of the Currency》，載於 https://www.occ.treas.gov/about/index-about.html。

FDIC 網站。《Federal deposit Insurance corporation》，載於 https://www.fdic.gov

Steemit 。《Decentralization：Why We Need It？& What Is Wrong With Centralization？》。載於 https://steemit.com/steemit/@sadekj/decentralization-why-we-need-it-and-what-is-wrong-with-centralization?fbclid=iwar1-b_ehgm7_po2kpcvfgnkyfhtbbcl05phr9i63wykhdumsk0kfgfzn1mi。

doi:10.6342/NTU202202035