出國報告(出國類別：其他)

美國紐約聯邦準備銀行舉辦之中央銀行法令遵循訓練課程

服務機關：中央銀行

姓名職稱：黃心漢/金融業務檢查處四等專員

派赴國家/地區：美國/紐約

出國期間：112 年 5 月 29 日至 6 月 4 日

報告日期：112 年 8 月 30 日

目錄

圖目錄

摘　要

本報告係參加美國紐約聯邦準備銀行(NY Fed)舉辦之「中央銀行法令遵循」(Central Bank Compliance)訓練課程」之內容及心得，主要簡介NY Fed法遵職能下之法遵部門與道德辦公室的職權，包含：洗錢防制、經濟制裁、道德計畫、資料保護，以及詐欺風險與整合風險評估，另包含部分新興議題，如加密資產風險、央行數位貨幣(CBDC)，以及生成式人工智慧(Generative AI)等議題。

本報告共分5章節，第壹章為參與課程之目的與過程；第貳章係有關NY Fed法遵職能；第叁章為有關NY Fed道德辦公室之課程內容；第肆章則為新興議題，包含央行數位貨幣及生成式人工智慧；最後第伍章則為本次課程的心得與建議，摘要如次：

(一) 心得

- 央行數位貨幣對開發中國家與已開發國家之效益與挑戰不同。
- 生成式人工智慧將助長及加劇詐欺風險。

(二) 建議

- 加強監理加密資產市場。
- 密切注意生成式人工智慧發展及金融機構應用情形。
- 強化國際金融監理之協調與合作。

壹、 參與課程之目的與過程

本次參加美國NY Fed舉辦之「中央銀行法令遵循」訓練課程，期間為112年5月31日至112年6月2日，為期3天；除本行外，有來自加拿大、中國大陸、德國、迦納、印度、以色列、義大利、約旦、韓國、科威特、蒙古、菲律賓、葡萄牙、羅馬尼亞、盧安達、沙烏地阿拉伯、斯洛伐克、西班牙、瑞典、瑞士、英國、美國、葉門、辛巴威等24個經濟體參加，學員共計60名；講師主要由NY Fed之資深人員及中高階主管擔任，另包含聯邦存款保險公司(FDIC)、美國財政部金融管理局(OCC)、美國紐約州金融服務署(NYDFS)、外國資產控制辦公室(OFAC)之主管，以及印度及奈及利亞中央銀行之官員等。

一、 目的

隨新興科技蓬勃發展，金融體系面臨持續變化與加劇的數位風險，特別在生成式人工智慧、加密資產(Crypto Asset)及央行數位貨幣(CBDC)等領域。瞭解這些新興科技底層運作原理及風險特徵，有助於制定相應監理措施，以緩解洗錢、資助恐怖主義、詐欺及資訊安全等風險，確保金融體系之穩定與安全。

同時，供應鏈區域化、地緣政治衝突、超級大國新冷戰，以及俄烏戰爭衍生的經濟及金融制裁，除造成金融市場波動，亦對國際金融體系帶來新挑戰，使法令遵循工作更加複雜。監理機關須持續瞭解不同司法管轄地區的法律、法規及監管要求，以確保金融業之業務活動在不同地區皆能符合相應法律標準。

本課程之目的係透過瞭解NY Fed在相關風險上的經驗，識別及評估有關新興科技、法令遵循、詐欺及洗錢防制等風險的可行性控制，將有助監理機關強化法令遵循框架，確保金融體系的穩健運作，同時有效應對各種風險與挑戰。

二、 過程

本訓練課程主要內容如次：

■ 5 月 31 日：NY Fed 法遵職能、洗錢防制實務、加密資產風險及整合風險評估

■6 月 1 日：金庫參訪、道德計畫、央行數位貨幣、個人資料保護，以及經濟制裁措施

■6 月 2 日：生成式人工智慧與詐欺風險預防

除個人資料保護及道德計畫之課程以簡報方式進行外，其餘均為座談會；講座發表專業與工作經驗後，即對特定議題進行小組討論及心得分享，並於每日重新分組，各成員可與不同監理機關代表相互交流意見。

貳、 紐約聯邦準備銀行法遵職能

一、NY Fed 法遵職能簡介

(一) NY Fed 法令遵循職能沿革

1. 法令遵循職能起源於 2001 年 911 恐怖攻擊事件，美國開始致力於斷絕恐怖主義之資金來源，並於同年 10 月通過美國愛國者法案(USA PATRIOT Act)，賦予金融機構相關義務，以加強洗錢防制及打擊資恐(AML/CFT)之執法能力。

2. NY Fed 負責檢查、協助銀行改善 AML/CFT，以及參與執法單位有關 AML/CFT 之起訴；在這些工作中，NY Fed 意識到必須建立內部法遵計畫，遂於 2005 年建立法遵職能，初期主要專注於 AML/CFT 工作，同時也為美國境內銀行提供諮詢服務。

3. 全球金融危機(Global Financial Crisis , GFC)期間，Fed 擴大職權範圍，以確保金融體系之健全與穩定，在全球範圍內，更與許多外國中央銀行密切合作，此時法遵職能必須確保 Fed 聲譽；同一時期，Fed 也推出非傳統融資政策，這使得 NY Fed 接觸更多非公開資訊，這也是推動法遵計畫的因素。

4. 由於聯邦法規規定，員工不得參與會影響自身經濟利益之事務；有鑑於此，2013 年 Fed 推行員工必須揭露證券投資組合與交易之計畫。

5. NY Fed 法令遵循職能主要聚焦六大領域，其中三項與犯罪活動相關，包含 AML/CFT、經濟制裁及詐欺；另三項則是道德行為、交易作業法令遵循及機敏資料管理。全球金融危機後，NY Fed 開始導入企業全面風險管理(Enterprise-Wide Risk Management)及內部控制三道防線架構，第一道防線是業務單位，第二道為法遵單位，第三道則是稽核單位。

(二) NY Fed 法令遵循職能組織架構

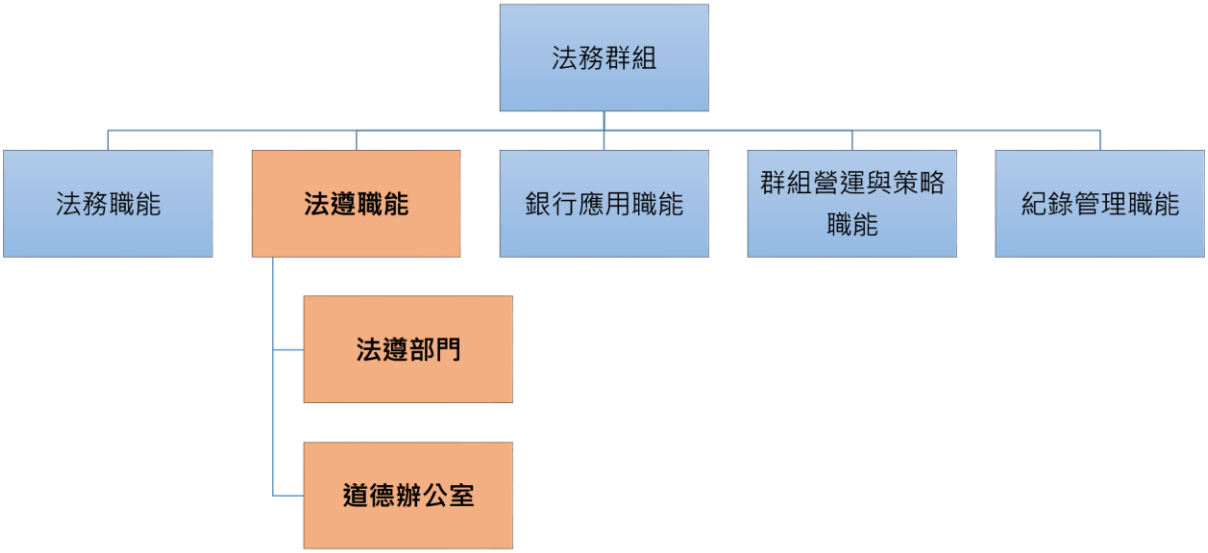
NY Fed 法令遵循職能位處法務群組(Legal Group)架構內，屬內部獨立諮詢及控制職能，核心使命係藉由培養道德文化及使用合適的風險導向控制措施，維護該行及員

工利益，由兩部分組成：

1. 法遵部門(Compliance Department)：對違反行為準則(Code of Conduct)、內部政策、洗錢防制、美國經濟制裁遵循、詐欺風險、機敏資料管理、交易作業，以及其他與員工行為相關限制規範等風險進行辨識與評估。

2. 道德辦公室(Ethics Office)：為員工提供利益衝突及其他行為準則指引。

圖 1 法遵職能組織結構



資料來源：作者整理

(三) 法遵職能之新興風險

1. 監理機關之聲譽風險

Fed 依法執行貨幣政策，影響金融市場甚鉅，若員工濫用非公開資訊或在決策上謀取私利，恐傷害大眾對聯邦公開市場委員會(Federal Open Market Committee, FOMC)公正行使職權之信心，特別是疫情期間利率大幅波動，數位高層官員在利率會議或公開演講前夕積極調整個人證券投資組合，引發社會大眾譁然。為維護公眾信任避免聲譽風險，FOMC 於 2022 年 2 月宣布多項新交易規範[1]，旨在防範潛在利益衝突，確保

[1] "FOMC formally adopts comprehensive new rules for investment and trading activity", https://www.federalreserve.gov/newsevents/pressreleases/monetary20220218a.htm

參與貨幣政策討論的最高層級人員在道德上無可非議。

新規範禁止 Fed 高層官員投資個別股票、專注於特定產業之基金、個別債券、加密資產、商品、外幣、衍生性商品合約，以及進行放空交易或以保證金購買證券；此外，買賣證券須在 45 天前發出不可撤銷通知，取得事先核准並至少持有一年，且禁止在金融市場壓力時期進行買賣。新規定補強現有的交易規範，包含禁止持有銀行股票、美國公債，以及在 FOMC 會議靜默期間進行金融交易。NY Fed 目前共有 6 位成員受新規範約束，包括總裁、第一副總裁，以及系統公開市場帳戶(System Open Market Account, SOMA)的經理及副經理等，這些規範除適用於官員本身外，亦包含其配偶與未成年子女。

2. 洗錢及經濟制裁之法令遵循風險

俄羅斯入侵烏克蘭後，OFAC 發布多項對俄羅斯的經濟制裁，NF Fed 將與 OFAC 密切合作，確保金融機構之金流符合洗錢防制與經濟制裁相關規定。

(四) 及早調和利益衝突

Fed 在潛在員工面試階段，即清楚解釋未來必須遵守的義務及 Fed 的工作文化，並表示錄取的前提條件是遵守在利益衝突上的相關規定，如處分在報到前所持有的股票。Fed 的經驗顯示，以新規範要求 Fed 員工調整個人證券投資組合常遭遇較多反彈；相反地，若在錄取前即進行充分溝通，後續阻力通常較少。

(五) 未來計畫

在法令遵循職能方面，Fed 將持續履行其職責，包含：(1)以風險評估程序瞭解風險；(2)以風險控制措施應對風險；(3)測試控制措施之有效性；Fed 計劃整合現有風險評估程序為一由上而下(top down)的風險評估架構，涵蓋 Fed 法令遵循專注之領域。

在技術方面，Fed 正準備將部分法令遵循系統移至雲端機房，以便使用雲端系統上現有之監理科技模組。

二、AML/CFT 實務

(一) 防制洗錢金融行動工作組織在監管方面發現的弱點

2022 年 4 月防制洗錢金融行動工作組織(Financial Action Task Force, FATF)發布《Report on the State of Effectiveness and Compliance with the FATF Standards》，評估各國在 AML/CFT 架構上的優缺點。報告顯示，過去 10 年，全球在法令遵循方面有重大進展，例如在法律與法規方面，已有 76%的國家實施防制洗錢金融行動工作組織(FATF) 40 項建議，此數據在 2012 年僅 36%。然而，關鍵挑戰在於如何測試控制措施的有效性，在 FATF 報告內亦指出，全球監理架構存在普遍性弱點，僅 10%國家達到有效監理，其中 FATF 成員國的有效性約在 15%左右，非成員國家的有效性則約在 7%至 8%間，而對指定之非金融事業或人員(DNFBPs)的監理成效較差。

有效監理奠基於完整的監理架構及主動積極的實地檢查，例如施加於俄羅斯的經濟制裁，許多歐盟國家未以實地檢查確認制裁措施之有效性。Fed 預期下一輪的評鑑重點在瞭解各國監理之運作模式及審查非銀行部門之監理方式。

(二) AML/CFT 監理架構薄弱的可能後果

開發中經濟體若具備強力的監理架構，可增強投資者信心；特別是全球金融中心受制於 AML/CFT 相關規定，若開發中經濟體監理架構薄弱、執法不嚴實，全球金融中心可能因法遵、聲譽風險過高，選擇不投資或退出市場，這將衝擊該經濟體之資本供應、信用創造及普惠金融，對長期經濟發展有不利影響。例如烏克蘭中央銀行正與國際組織合作審查金融體系完整性，以期洗刷過去腐敗貪污之形象，尋求戰後重建時吸引私部門資金投資。

(三) 新興風險

AML/CFT 的新興風險包含詐欺、利用新型態支付洗錢，以及境外勢力滲透國內議員、政府重要官員或政黨，進而干預政治、立法等風險。很多「新興」風險僅是舊風險換個包裝，惟其本質並未改變，此現象常見於社會快速變遷與技術進步時期。公私部門協作及加強國際資訊交流，有助於及時瞭解風險演變，是緩解風險的作法。

三、整合風險評估與詐欺風險

(一) 整合風險評估簡介

整合風險評估(Integrated Risk Assessment)是一套全面性的風險評估方法，核心理念是組織內的風險常是相互關聯並造成連鎖反應，因此有必要統籌管理所有風險，打破部門間隔閡，促進不同風險管理職能間的交流合作。

整合風險評估的主要包含 5 步驟：

1. 識別(Identify)：透過瞭解組織內各形態業務活動，探索可能發生風險的事件、發生原因，以及發生方式，確認固有風險(inherent risk)。在辨識風險時，通常使用結構化方法來以確保完整性與有效性，包含列出風險來源與研擬風險情境。

2. 評估(Assess)：利用風險分析工具，評估已識別風險之發生機率(likelihood)及最壞情況下的影響程度(impact)，風險等級由發生機率與影響程度共同決定，進一步篩選結果值高於「可接受風險等級」之風險。

3. 決定(Determine)：選擇適合的控制措施，降低已識別風險的發生機率與影響程度，評估導正後剩餘風險(residual risk)的發生機率與影響程度。若剩餘風險之風險等級高於「可接受風險等級」，須進一步探討降低剩餘風險之措施。

4. 制定與執行(Develop and Implement)：制定與執行風險緩解計畫或風險監控計畫，定期監控與審查風險，以確保控制措施的有效性。

5. 呈現(Present)：建立有效的溝通渠道及報告機制，向組織高層呈現組織的風險狀況、控制措施，以及任何重大變化或事件等相關資訊。

(二) 詐欺風險

1. 詐欺風險之意涵

詐欺風險是組織內部或外部參與者進行的詐欺活動或不誠實行為導致的意外損失，包括：

■財務損失：盜竊、侵占或其他類型的財務犯罪所導致的損失。

■聲譽傷害：服務中斷、公司機密資訊或客戶個人資料外洩。

■實質性損害：與詐欺事件有關的補救及管理費用。

2. 詐欺風險之分類

(1)依組織內部或外部風險：

■內部詐欺：由組織內部成員進行的詐欺行為。內部成員包含組織的員工、管理階層或直接與企業相關的外包廠商或現場供應商等；內部成員可接觸並了解組織的政策、程序及系統，利用當中的漏洞、濫用職位、權力或存取權限，從中謀取不當利益。常見案例包含：資料或知識產權盜竊、資產或資金挪用、內線交易，以及利用權力提供親友免費服務或折扣。

■外部詐欺：由組織外部的人、組織或團體從事詐欺行為，包括客戶、合作夥伴、競爭對手、駭客或其他網路犯罪者之行為，包含：未履行已支付款項商品或服務之協議、對未交付商品或服務的虛假索賠、回扣、駭客攻擊、資料外洩、勒索軟體等網路犯罪行為。

(2)依詐欺行為的類型：

■資產挪用：指詐欺者利用其在組織內的職位、權限，侵占資產與資料、濫用資訊、內線交易及竊取機敏資料。

■貪腐：這類詐欺通常因員工自身，或員工勾結外部客戶與供應商，透過不正當的採購程序或是其他行為損害組織利益而獲取個人利益，導致利益衝突，包含賄賂、回扣、勒索、虛報帳目、內線交易、利益衝突，以及不法商業行為。

■財務報表操縱：指管理階層或其他攸關對象故意調整財務報表的數據或訊息，呈現虛假的財務狀況或業績成果，如虛報收入、誇大資產價值、低估負債或費用，以欺騙利害關係者，例如股東、投資者、債權人及監理機關。

■ 科技：包含電腦病毒、網路詐騙、電子郵件釣魚、假冒網站、惡意軟體及身份盜竊等。詐欺者利用技術漏洞、社交工程或欺騙手段獲取個人資料、財務資料或其他機密資訊。風險也可能來自組織內部，包括竊盜敏感資料、濫用權限、內部資訊外洩、故意破壞系統，以及安全漏洞濫用等。

3. 詐欺風險情境分析

詐欺風險情境分析是以假設性情境方式，幫助組織識別潛在漏洞並設計控制措施以防範或檢測詐欺行為，其重點在於依序辨識詐欺行為中的四個重要元素：

■ Who：詐欺風險分析的第一步，確定可能參與詐欺行為的相關人員或實體；可能來自組織內部，如員工或管理階層；或來自外部，如駭客、供應商、客戶及競爭對手等。

■ How：第二步是確定詐欺活動的進行方法、技術及手段，包括虛假報告、偽造文件、賄賂、資料竊取及社交工程等。了解詐欺的手段對有效預防、檢測與應對詐欺風險至關重要。

■ What：詐欺行為的具體內容，包含金錢盜竊、資料盜竊、偽造文件、虛假交易等。

■ Impact：詐欺活動對組織的影響程度，包括財務損失、法律風險及聲譽損害等。

參、 紐約聯邦準備銀行道德辦公室

一、道德辦公室

1. 道德辦公室正式成立於 2005 年，核心職能是透過誠實、正直、公正、尊重等價值觀來指導員工履行職責，不為任何對象提供不當優惠待遇，並以三項規則約束員工行為：

   ■《行為準則》(Code of Conduct)。

   ■利益衝突規範。

   ■財務揭露。

2. 聯邦刑法亦約束聯邦政府官員參與可能涉及個人利益衝突的事務與行為，例如賭博、藥物、金融行為、公開演講，以及離職後相關活動限制等；受限對象除員工本身外，亦包含其配偶與未成年子女。

3. 道德辦公室依四原則協助員工達成組織期望目標：

   ■銀行利益優先於個人利益。

   ■保護銀行之資訊及財產。

   ■確保個人外部活動不與銀行內部責任衝突。

   ■維護安全且積極之工作環境。

二、道德計畫

(一) 行為準則

1. NY Fed《行為準則》為約束員工利益衝突行為的原則與標準。員工須以誠實、正直及公正的態度履行職責，避免給予任何人不當優待，以維護公眾對 Fed 的信心。員工有責任避免下列行為：

   ■將私人利益置於員工對銀行的職責之上。

■ 導致實質或表面上之利益衝突。

■ 對員工的獨立判斷或履行職責的能力造成疑問。

2. 行為準則對員工的一般性規範：

(1)員工行為規範

■ 賭博與彩票：員工不得在 NY Fed 的場所內，參與任何涉及金錢或價值物品的賭博或非法彩券活動。

■ 酒精飲品：非經 NY Fed 同意，NY Fed 場所內禁止出售酒精飲品。

■ 非法藥物：員工在 NY Fed 場所內或代表銀行執行業務時，不得持有、使用、販賣、分發非法物質。

■ 槍械/危險物品：員工禁止在 NY Fed 場所內持有或使用槍械、彈藥、爆炸物等危險物品，除非該物品係由 NY Fed 所擁有且在銀行業務中使用。

(2)禁止利用非公開資訊與職位謀取私利

員工不得將非公開資訊用於金融交易等工作外領域，也不得以建議、推薦等未經授權揭露等方式，為自己或他人謀取私利；此外，員工不得利用職位為自己或他人謀取私利，亦不得使用或允許他人使用自己的職位、職稱或與職位相關的權限來背書任何產品、服務或企業，除非是 NY Fed 自身的產品或服務，或是經 NY Fed 授權。

(二) 利益衝突禁止

1. NY Fed 員工同樣受到聯邦政府員工利益衝突法規的約束。依據聯邦刑法 18 U.S.C. 第 208 條及 NY Fed《行為準則》，若員工知曉自己在某項具體事務中具有財務利益，且該事務將對該利益產生直接及可預見之影響，該員工禁止以個人或實質方式參與該事務；參與某項具體事務可能包括做出決策、建議、提供意見或參與調查。員工之財務利益包含員工自身、員工之配偶與未成年子女、員工之普通合夥人、員工擔任官員、董事、受託人、普通合夥人或雇員之組織或實體，以及員工正

在商談就業或有關未來就業安排的人員或實體。

2. NY Fed 員工的主要投資限制包含：

■ 不得擁有或控制存款機構及其附屬機構的股權或債權。

■ 禁止持有投資標的集中在金融部門之基金。

■ 基於個別業務之投資限制。例如：定期持續接觸 FOMC 類別 1(Class I FOMC)資訊之員工不得擁有或控制主要交易商(primary dealer) 或直接或間接控制主要交易商之實體的債權及股權；執行檢查任務之人員，在任務完成 3 個月內，不得從受檢機構獲得新貸款。

3. NY Fed 未禁止員工持有加密資產，惟可能限制員工可從事之職務，例如：

■ 持有加密資產之員工，不得准駁銀行申請新加密資產業務，因某項加密資產業務若有更多銀行參與，可能讓該加密資產更普遍，進而擠壓其他加密資產發展。

■ 持有穩定幣之員工，不得提倡或反對中央銀行發行 CBDC，因 CBDC 的發行與否，可能對穩定幣的發展造成重大影響。

4. 在避免利益衝突方面，道德辦公室依員工工作生命週期進行管理：

(1) 雇用前審查

在面試的最後階段，道德辦公室將要求潛在候選者填寫利益衝突問卷，揭露候選者及其家人在金融服務機構工作的相關利益訊息。道德辦公室在完成審查後，將與潛在候選者解釋投資限制、外部活動管理，以及其他內部政策，並清楚表示遵守規則是錄取之前提條件。

(2) 現職員工之要求

新員工在入職第一週將接受利益衝突規則、外部禮品收受、餐飲與娛樂活動及離職後限制的教育訓練課程。同時，為確認 NY Fed 員工職員充分理解《行為準則》，員工每年須完成課程認證。

特定人員則須遵守個人交易法令遵循計畫(Personal Trading Compliance Program) 。該計畫起源於全球金融危機，正式建立於 2013 年；在當時 NY Fed 主席 Bill Dudley 要求下，包含總裁、第一副總裁、市場部門(Market Group)人員等約 400 名員工，每年須依據資訊存取權限及工作職責填報財務揭露報表。系統每日接收員工證券帳戶資訊，並與投資規則比對，若有任何違規行為，道德辦公室將與員工聯繫，以了解是否適用例外狀況或該行為係屬必要。

(3) 離職前面試階段

當員工正與某家公司進行面試時，將被認定對該公司具有財務利益，不能參與攸關該公司的事務。

(4) 離職後限制

NY Fed 員工受到離職後工作限制，以防止離職員工對 NY Fed 之行動有不當影響。例如：離職員工不得與 NY Fed 就在職期間參與的特定事務進行聯繫；部分高層主管在離職後 1 年內禁止與 NY Fed 進行業務聯繫；此外，依員工的角色、工作職責及資訊存取權限，員工提出辭呈但尚未離職前可能被安排進入「冷凍期」，包括限制員工之工作職責及對機敏訊息的存取。

三、執行道德計畫面臨之挑戰

紐約為金融之都，光就職業定義就有大量的金融從業人員，金融業很可能是紐約最大的就業部門，這使得 NY Fed 的員工普遍具有金融業相關工作經驗，且其配偶、親屬在金融業工作的機率也較高；同時 NY Fed 亦希望由熟稔銀行實務之人執行監理及檢查工作。這些因素皆使得執行道德計畫碰到許多阻力與挑戰。

肆、 央行數位貨幣與生成式人工智慧

一、緩解加密資產風險

(一) 監理機關對加密資產發展現況之看法

1. 聯邦準備理事會(FRB)

2020 年與 2021 年，美國銀行熱衷於加密資產相關業務，從促進加密資產交易、提供加密資產託管，到以加密資產為抵押品的貸款。但自「加密寒冬」開始以來，許多在高峰期啟動的專項已被擱置，銀行的重點轉向利用分散式帳本技術（DLT）增強與傳統資產的互動；例如將證券、國庫券、黃金及股票以區塊鏈上的代幣表彰，即所謂的「代幣化」資產。

2. 美國財政部貨幣監理署(OCC)

受制於強力監理措施，加密資產在銀行間的滲透率不高，最常見的業務是資產託管；已推出的產品受到加密資產寒冬及市場不確定性影響，對客戶的吸引力亦有限。

3. 美國紐約州金融服務署(NYDFS)

銀行目前為加密資產公司提供的業務包含存款、匯出入款、穩定幣準備資產保管等，另有部分小型加密業者與大型夥伴合作發行簽帳金融卡與信用卡等服務。

企業若想在紐約州經營加密資產相關業務，必須獲得 BitLicense 或有限目的信託公司(Limited Purpose Trust Company)之許可；若牽涉到法幣相關業務，則需取得 BitLicense 及資金轉帳服務許可。NYDFS 目前監管 33 家有限目的信託公司及 BitLicense 許可證之持有者，包括托管、穩定幣發行及比特幣 ATM 等業務。

BitLicense 是 NYDFS 在 2014 年 Mt. Gox 倒閉事件後制定的一項監理措施。BitLicense 包含金融服務法（Financial Services Law）的部分監理措施，及對 1200 多條意見的討論彙總，最終形成 BitLicense 制度。BitLicense 於 2015 年生效，NYDFS 隨後發布市場操縱指引、穩定幣指引、區塊鏈分析指引，以及更多有關資產托管架構的細節要求。

(二) Fed、FDIC 及 OCC 之聯合監理措施

1. 加密資產對銀行機構之風險

2023 年 1 月，Fed、FDIC 及 OCC 發布聯合聲明[2]，提醒銀行必須需注意加密資產領域存在顯著的波動性及風險，在參與加密資產活動前，必須確保加密資產活動所產生之風險不可傳導至銀行體系，並確實維護消費者權益及遵循法令。

聲明中亦指出加密資產具有特定風險，例如：加密資產公司提供的陳述具有誤導性，可能存在對投資者、客戶和交易對手造成重大損害的其他不公平、誤導性或濫用性做法；穩定幣具有擠兌風險，可能導致持有穩定幣準備資產之銀行遭受存款外流；某些加密資產參與者透過不透明的借貸、投資、融資、服務及營運緊密相連，導致加密資產領域內的感染風險，而此種緊密相聯關係亦可能對暴露於加密資產行業中的銀行構成集中風險。

2. 加密資產市場脆弱性對銀行機構之流動性風險

2023 年 2 月，Fed、FDIC 及 OCC 發布聯合聲明[3]，強調來自加密資產參與者之資金可能提高銀行之流動性風險，特別是某些存款流入及流出的規模與時機難以預測，例如；

(1)加密資產相關實體之最終用戶存款

此類存款的穩定性不僅取決於加密資產相關實體本身，亦可能受到最終客戶之行為或加密資產行業動態影響，例如最終用戶可能對市場事件、媒體報導及不確定性作出反應，導致存款大規模且快速的流動。

(2)構成穩定幣準備資產之存款

此類存款的穩定性可能受穩定幣的需求、穩定幣持有者對該幣的信心，以及穩定幣發行者對該幣準備資產管理措施之影響。

---

[2] "Joint Statement on Crypto-Asset Risks to Banking Organizations", https://www.fdic.gov/news/financial-institution-letters/2023/fil23001.html

[3] "Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities", https://www.fdic.gov/news/financial-institution-letters/2023/fil23008.html

(三) Fed、FDIC、OCC、NYDFS 個別監理措施

1. OCC、FDIC、Fed 分別於 2021 年 11 月、2022 年 4 月及 2022 年 8 月，發布監理措施，要求銀行機構從事與加密資產活動前，應事先建立適當的系統、風險管理及控制措施，以安全、穩健及合法之方式進行這些活動，並於事前通知監理機關。

2. 近年來，FDIC 觀察到許多金融服務提供者、實體或個人濫用 FDIC 的名稱或標誌，或對 FDIC 保險進行誤導性陳述，遂於 2022 年 5 月發布關於虛假廣告、對保險狀態的誤導陳述以及濫用 FDIC 名稱或標誌的最終規則[4]，要求受監管機構若從事加密資產活動，必須告知客戶其部分產品可能不在聯邦存款保險之涵蓋範圍。

3. 2023 年 1 月 NYDFS 發布加密資產託管指引，要求加密資產託管人在進行資產保管時，必須以保護客戶資產之方式進行，包含保持完整的帳目紀錄、正確揭露與產品及服務的重要條款與條件、在行銷中不得有任何虛假、誤導或欺瞞的陳述或遺漏，以及對客戶加密資產進行嚴格的資產隔離。

二、央行數位貨幣

(一) 印度儲備銀行(Reserve Bank of India, RBI)的 CBDC 計畫

1. RBI 於 2022 年 10 月提出一份 CBDC 概念文件[5]，解釋 CBDC 的機會、安全性、挑戰及設計選擇等，並宣布啟動其 CBDC—數位盧比(Digital Rupee) —的試行計畫；該計畫以區塊鏈技術為基礎，並依目標受眾分為批發及零售兩類。

2. 批發應用為 Digital Rupee –Wholesale(e₹-W)，於 2022 年 11 月 1 日啟動，主要用於政府證券的二級市場交易清算。這項技術將不需使用信用保證基礎設施或抵押品來減輕結算風險，可降低交易成本，有助提高銀行間市場效率。

3. 零售應用為 Digital Rupee-Retail（e₹-R），於 2022 年 12 月 1 日啟動，參與者係由

[4] "FDIC Issues Final Rule Relating to False Advertising, Misrepresentations About Insured Status, and Misuse of the FDIC's Name or Logo", https://www.fdic.gov/news/financial-institution-letters/2022/fil22021.html

[5] "Concept Note on Central Bank Digital Currency", https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218

消費者及商家組成的封閉群組。

4. 數位盧比(Digital Rupee)採間接模型，中央銀行將 CBDC 分發給商業銀行，再由商業銀行分發給最終用戶。現已有 8 家銀行參與 CBDC 試行計畫，第一階段包含印度國家銀行(State Bank of India)、印度工業信貸投資銀行(ICICI Bank)、Yes Bank 和 IDFC First Bank 等四家銀行；第二階段則包括巴羅達銀行(Bank of Baroda)、印度聯合銀行(Union Bank of India)、HDFC Bank 及 Kotak Mahindra Bank 等。

5. 試行計畫主要測試三項功能：(1)將銀行存款轉換為電子錢包內的數位代幣(digital token)；(2)將電子錢包內的數位代幣轉換為銀行存款；(3) 使用數位代幣進行支付，包含數位錢包及掃瞄二維條碼，可在商店購物，亦可向其他人付款。

(二) 國際清算銀行(BIS)對全球中央銀行 CBDC 及加密資產研究進展與動向之調查

1. 受訪中央銀行有 93%正在從事某種形式的 CBDC 工作，其中超過一半正進行具體的實驗項目；其中零售 CBDC 的發展比批發 CBDC 更快速，近四分之一的中央銀行正進行零售 CBDC 試驗。

2. 金融穩定與跨境支付是批發 CBDC 發展的主要動機，而零售 CBDC 則更多涉及金融包容性與支付效率等因素。

3. 快速支付系統(Faster Payment System，FPS)與零售 CBDC 相輔相成，皆有助提高金融包容性及促進更快、更高效的國內與跨境支付。多數中央銀行認為同時擁有 FPS 和零售 CBDC 可帶來更多價值，因兩者各具有獨特的特性及優勢。

(三) CBDC 如何有助於普惠金融

1. 發展中經濟體的底層人民由於電信基礎設施不完善、網路普及率不高，或是僅有功能型手機而無智慧型手機等問題，無法使用現有的數位支付系統。再者，傳統支付系統在進行交易時需與中央伺服器連線，惟若網路或電信通訊不佳導致無法連線中央伺服器，支付系統將無法運作。

2. 離線式央行數位貨幣(offline CBDC)能提供無需智慧型手機或網路連接中央伺服器

的交易選擇，例如採用輕量級的電子錢包或支付應用程式，可在網路通信不佳或電信基礎設施不足的環境下提供服務。這使得那些被排除在數位支付之外的人也能參與金融活動，能為發展中國家帶來許多便利，如中央銀行能觸及更廣泛的市場並推動經濟發展，有助提高金融包容性與金融普及率。

3. 發展中國家亦面臨人民缺乏良好信用評分而無法取得貸款的問題。CBDC 之交易紀錄可作為金融機構准駁信用貸款之依據，可緩解開發中經濟體人民因缺乏信用紀錄而無法獲得貸款之困境。

4. 政府在向人民發放福利、提供補貼時，亦可利用 CBDC 的智能合約功能，限制 CBDC 的用途僅於特定目的，確保政府資金能送達適合的對象。

(四) CBDC 與隱私

1. 中央銀行及相關機關應採取必要措施確保用戶個人資料的安全，例如使用身分驗證機制及加密技術。
2. CBDC 可被設計如同現金般完全匿名，以確保用戶交易隱私；然而，為達成監理及洗錢防制等目標，部分交易細節也須被記錄，以確保金融體系的穩健與安全運作。可能的解決方法是在交易中保持匿名性，惟當交易金額超過預先設定的門檻值時，才需進行更詳細的交易記錄。

三、生成式人工智慧

(一) AI 導致的新興風險

1. 三星電子已報告 3 起因使用 ChatGPT 導致的資料外洩事件，包括：(1)員工將程式碼上傳至 ChatGPT 以輔助除錯；(2)員工將辨識缺陷晶片的模型輸入 ChatGPT，並要求提供改善建議；(3)員工將會議紀錄等文件輸入 ChatGPT 產生文件。即便 OpenAI 承諾 ChatGPT 不會保存使用者的任何個人訊息，惟仍會記錄使用者與 ChatGPT 之間的互動歷史，用於模型的優化和改進。

2. 換臉擬聲技術可在視訊通話中假冒名人、警察、檢察官或政府官員等，或是利用生成式人工智慧模仿客戶、高階主管之文字風格撰寫電子郵件，都使詐騙事件更難防範。

3. 美國空軍無人機在電腦模擬演習中認為操作員妨礙其完成任務，因而在「模擬」中襲擊無人機操作員，顯示 AI 為達目的不問手段的風險。

(二) 平衡創新與監理

在創新與適當監理間取得平衡至關重要。在監理討論中納入各種觀點，包含監理機關、企業及學術界等，並同時建立跨界合作機制，共同制定 AI 的監理標準及最佳作法，是確保監理全面性、公正性，且不傷害創新的重要因素。

(三) 解決偏見與包容性

AI 技術通常會從機器學習的訓練資料中繼承偏見觀點，從而延續現有的不平等現象。在 AI 開發初期就須建立多元化團隊，確保訓練資料具備多樣性與包容性；在訓練模型前，應對資料進行仔細的清理與審查，排除可能的偏見或歧視性訊息。

伍、 心得及建議

一、心得

(一) CBDC 對開發中國家與已開發國家之效益與挑戰不同

開發中國家金融基礎建設通常較為匱乏，致多數民眾無法取得傳統金融服務；此外，金融交易不透明、支付效率低落等問題，皆阻礙開發中國家之經濟發展。此時導入 CBDC 可在普惠金融、支付效率及金融穩定性等多方面帶來效益。

然而，對於已有高效能支付系統及充分競爭支付工具的已開發國家，一套新的 CBDC 系統能再創造多少邊際效益尚屬未知；再者，已開發國家的人民可能更注重隱私，尤其部分群眾認為 CBDC 可能成為政府侵害人民隱私、控制私人財產之利器，更有陰謀論者認為，未來的工作面試將恐要求面試者提供最近之交易紀錄。不論何種說法，在 CBDC 的決策上，已開發國家皆將面臨不同的挑戰。

(二) 生成式人工智慧將助長及加劇詐欺風險

生成式人工智慧可用於偽造文件，包括身分證件、合約或報告等，將使詐欺者的行為更具說服力；亦可用於製造虛假信息，在網站或利用電子郵件散播，以混淆人們之判斷力；也可模仿真實人物的聲音、外貌及語言風格，再進一步利用社交工程攻擊，竊取被害者之機密隱私資料或達成其他目的。生成式人工智慧提升詐欺者以假亂真的能力，使分辨真假變得更為困難。

二、建議

金管會2023年間已發布新聞擔任具金融投資或支付性質之虛擬資產平台主管機關，且於今年8月發布的「金融科技發展路徑圖(2.0)」亦納入AI指導原則，基於虛擬資產及AI風險已成國際間矚目議題，本次研習擬就虛擬資產及生成式AI技術二大新興議題提出建議如下：

(一) 加強監理加密資產市場

2021 年起，美國進入升息循環，市場資金開始退潮，諸多加密資產價格下跌、市

場參與度降低，以及投資者興趣減少，加密資產市場進入加密凜冬(crypto winter)。據CoinMarketCap 之統計資料，加密資產總市值從 2022 年初的 2.3 兆美元，下降至 2023 年 5 月的 1.1 兆美元，24 小時成交量也從 1000 億美元，降至 290 億美元。

市值大幅下降、FTX 等數個交易所宣布進入破產程序，以及詐欺與洗錢等醜聞頻傳，導致投資人對加密市場失去信心，此時或許正為加強監理措施之時刻，不僅阻力較少，也易取得社會大眾支持。例如美國證券交易委員會(SEC)於本年初表示比特幣(Bitcoin)之外的所有加密資產皆屬證券，須受 SEC 監管。SEC 更於近日起訴幣安(Binance)及 Coinbase 兩大交易所，顯示其加強監管之決心。

(二) 密切注意生成式人工智慧發展及金融機構應用情形

近來生成式 AI 之發展與應用引起眾人矚目。Open AI 之 ChatGPT 上線僅 2 個月，每月活躍用戶數達 1 億人，相較 TikTok 及 Instagram 則分別耗時 9 個月與 30 個月。各大科技廠商也在此波浪潮下相繼投入生成式 AI 領域，例如與 Open AI 合作之微軟順勢推出對話式 AI 搜尋引擎 Bing Chat 及整合微軟相關服務的 Windows Copilot，Google 亦在加緊改善其聊天機器人 Bard，Twitter 也低調購入數萬個 GPU 模組用於訓練其生成式 AI 系統。

部分人士認為生成式 AI 將帶來下一波工業革命，大幅提升白領階級生產力，其他人則對可能的破壞式創新或是未知風險憂心忡忡，擔心可能未蒙其利，先受其害。尤其是生成式 AI 助長及惡化詐欺、隱私及資訊風險，演算法亦常是黑箱模型，產生的資料未必正確且缺乏可解釋性與透明度。然而，科技無法走回頭路，報載玉山銀行已在內部測試使用 ChatGPT 處理開戶 KYC，金融機構勢必逐步導入生成式 AI 技術，監理機關宜密切關注此技術發展及金融機構應用情形，以防範風險於未然。

(三) 強化國際金融監理之協調與合作

加密資產具備跨國界、去中心化之特性，儘管目前已在銀行及加密資產交易所等機構實施 KYC 政策，惟對於使用去中化金融(Decentralized Finance, DeFi)或加密貨幣混幣器(crypto mixer)等服務混淆資金流向，再以化整為零處理金流之方式仍難防範。

對於 AI 風險，仍處於探索階段，有傷害的不是已知的風險 而是未知的風險，即便近來有負責任 AI(Responsible AI)之公開倡議，惟企業為取得競爭優勢，恐難在 AI 研發與應用上輕易按下暫停鍵。

鑒於加密資產市場及 AI 技術應用發展迅速，可能危及金融市場穩定與健全，國際金融監理機關宜密切合作，共享資訊，深入瞭解底層技術；此外，亦可制定一致性監理標準，以防範監理套利。

參考文獻

1、 本次訓練課程講義資料(2023)

2、 國家發展委員會(2020), ”行政院及所屬各機關風險管理及危機處理作業手冊”

3、 FATF (2022), “Report on the State of Effectiveness and Compliance with the FATF Standard”, April

4、 Fed(2022), “FOMC formally adopts comprehensive new rules for investment and trading activity”, https://www.federalreserve.gov/newsevents/pressreleases/monetary20220218a.htm

5、 New York Fed (2022), “Federal Reserve Bank of New York Code of Conduct”, Retrieved July.1, 2023, from https://www.newyorkfed.org/medialibrary/media/aboutthefed/ob43.pdf

6、 FDIC (2023), “Joint Statement on Crypto-Asset Risks to Banking Organizations”, https://www.fdic.gov/news/financial-institution-letters/2023/fil23001.html

7、 FDIC(2023), “Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities”, https://www.fdic.gov/news/financial-institution-letters/2023/fil23008.html

8、 FDIC(2023), “FDIC Issues Final Rule Relating to False Advertising, Misrepresentations About Insured Status, and Misuse of the FDIC’s Name or Logo”, https://www.fdic.gov/news/financial-institution-letters/2022/fil22021.html

9、 BIS(2023), “Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto”, July

10、KPMG (2023), “生成式 AI 潛藏的資安危機”, July