出國報告（出國類別：其他）

State Street「Annual Official Institutions Conference」心得報告

服務機關：中央銀行
姓名職稱：陳珮為 四等專員
出國地點：美國波士頓
出國期間：2019 年 4 月 7 日至 4 月 12 日
報告日期：108 年 7 月 12 日

目錄

壹、前言

職奉派於 108 年 4 月 7 日至 4 月 12 日參加 State Street 於美國波士頓所舉辦之「Annual Official Institutions Conference」。研討會成員來自世界各地的央行與主權基金，主題涵蓋「金融科技（區塊鏈與人工智慧）之應用與影響」，與「環境、社會與治理（ESG）探討及投資」等議題。安排兼具深度與廣度，有助瞭解當今金融科技的影響，以及歐美企業在執行投資時對環境治理原則的重視。

此次課程最大收穫在於激發職探討金融科技趨勢和影響之興趣。當今金融科技中最為市場關注的為兩塊領域，分別為區塊鏈和人工智慧。

區塊鏈之「分散式帳本」和「溢散式傳播」特性，挑戰了傳統中心記帳的思維。而這種完整和分散式紀錄特性，有助提供事後稽核軌跡，有效降低法遵成本。然而非認許式區塊鏈具諸多限制，包括：處理量擴增能力、清算最終性、速度侷限性、耗能耗電和究責問題。為釐清責任歸屬，可考慮「實名制」區塊鏈；如欲改善速度和處理量等其他問題，則可考慮認許式區塊鏈。

而人工智慧領域在導入深度學習後出現突破性發展，其影響力在各領域逐漸擴散。對於機械式和重複式的工作，引進人工智慧系統有助降低時間和金錢成本，但也代表市場對相關從業人員需求下滑，導致就業等社會結構的改變。因此，產業升級和轉型有其必要性。此外，就業市場和社會結構改變，可能會挑戰傳統經濟現象或理論，因此據以決策時需思考既有理論是否有調整的必要性。再者，對於稽核、稅務、會計與交易資料系統可考慮與人工智慧進行結合，有助加快資料整理、關鍵資料擷取。最後，人工智慧擅於處理通則，但較不擅長處理例外，也較缺乏彈性和情感。而感性與彈性則是人類之優勢，佐以人工智慧精華，才是人類與人工智慧共存共榮之道。

貳、區塊鏈之發展與應用

一、 何謂區塊鏈（Blockchain）

區塊鏈係加密型貨幣 (以比特幣為例)背後的底層技術，透過「去中央處理」和「分散式帳本」（Distributed Ledger Technology, DLT）機制為使用者進行點對點支付，從而創造一總帳本，記錄用戶間的交易和資產移轉。茲詳述如下：

1. 何謂「去中央處理機制」:

   即「帳本共享」和「集體維護機制」。整個帳本的運作仍是依照創始者所撰寫的營運系統協定和軟體來運作，但整個交易過程不再需要中介機構協助結清算處理或管理交易紀錄，資料也不是由特定的中央控管機制處理後再分送資訊至各節點（node），而是由眾節點進行集體維護。

2. 何謂「分散式帳本」

   資料的產生來自各節點，並由節點向終端使用者（end user）提供對外帳本服務。為了使記載在各節點上的帳本資料一致，每筆交易由發起方向的節點進行溢散式傳播（propagation casting），最後擴散到全網，使分散的各節點所記載之帳本一致。

3. 為何命名為「區塊鏈」

   所謂「區塊」，係指透過 hash 機制，將交易相關資訊綁定和紀錄在特定格式和欄位[1]裡，而這一個一個資料區塊（block）即構成

[1]包含：「時間戳記」、「Hash 值」 、「前一個 hash 值」、「隨機值（Nonce）」和「困難值（Difficulty）」

總帳簿；所謂「鏈」，則是指將不同區塊透過特殊機制鏈結（chain），以強化資料被竄改的難度。在交易過程中，為驗證交易身份和確保交易安全，另搭配「公開金鑰加密（Public Key Cryptography）」、「條件式雜湊函數計算（Conditional Hashing）」與「工作量驗證（Proof of Work, PoW）」等技術組合。

二、 區塊鏈技術[2]

交易過程中，為確定資產所有權和支配權是權利擁有人，採用「公開金鑰加密技術（PKC-Public Key Cryptography）」；又為確保大帳本系統中所儲存的資料，不會被他人竄改，採用「區塊鏈機制」，配合上「條件式雜湊函數計算（Conditional Hashing）」來增加竄改交易訊息的難度，以及「工作量驗證（Proof of Work, PoW）」來處理分岔問題[3]。以下茲就區塊鏈技術組合之優劣勢與相關建議整理如下表：

等。

[2]參考杜宏毅、宋倬榮（民 107 年）。《區塊鏈之書》。

[3]《區塊鏈之書》曾提到，所謂「分岔」問題係指，區塊傳送到不同節點所需時間不同，因此不同節點所擁有之區塊鏈，其資料不一定是處在完全一致狀態，再加上缺乏中央控管機制，故無從得知其他節點之挖礦進度。若某節點同時接受到來自節點甲和節點乙所製作的區塊，只能先將兩個區塊同時接上手中原本的區塊鏈，形成「分岔」現象。之後再以「共識決(consensus)」方式，決定保留哪一條區塊鏈分支。而比特幣所採用的共識機制為「工作量證明演算法（簡稱工作量證明，PoW）」。而之所以稱為「共識」，係因其中的信任機制是由各節點透過難以篡改的運算證明所達成的共識。

表 1 原生型區塊鏈技術組合之優缺點與相關建議

技術組合	優點	缺點	建議
公開金鑰加密機制	解決對稱式加密技術所產生的中間人攻擊問題	1. 私鑰被盜風險 2. 若公私鑰擁有人之身分採匿名制，容易淪為洗錢管道	1. 妥善保存私鑰 2. 可驗證實名制[4]
條件式雜湊函數計算	1. 交易驗證與提高資料被竄改的難度 2. 由節點來挖礦，可節省中央控管機構之成本	1. 處理量擴增能力 2. 51%攻擊風險 3. 耗費大量時間、運算力和電力	1. 不適合用於即時或高頻交易系統，但可考慮應用在跨境支付或跨國匯兌。另可採用私有鏈方式來擴大區塊包容交易筆數 2. 風險存在，但掌握 51%運算力之成本相對高昂 3. 難以解決
共識決演算法—工作量驗證（PoW）	處理分岔問題	1. 清算最終性問題 2. 耗費大量運算力和電力 3. 速度侷限性	1. 採用其他共識決 2. 難以解決 3. 認許式區塊鏈處理速度，較非認許式區塊鏈之效率高
去中央控管之溢散式傳遞	成本由各節點分攤	1. 速度侷限性 2. 責任歸屬問題	1. 採用私有鏈，藉由調整區塊製作頻率來提高速度 2. 基於究責問題，可考慮認許式區塊鏈
回饋機制	提供挖礦誘因	有發行量遞減問題，難以調節供給量。	不適合用於法幣發行
分散式帳本	1. 每個參與者都能獲得完整備份數據，具不可取消之特性 2. 提供事後稽核軌跡 3. 監管機關資料來源	資料透明的反面為隱私保障問題	透過認許式區塊鏈，讓資訊在不同主體間進行選擇性分享

[4] 杜宏毅博士曾指出，可考慮以區塊鏈平台介接目前所使用的電子憑證機制。

三、 區塊鏈之發展與應用

(一)區塊鏈之發展與應用

現今越來越多企業運用該技術於加密貨幣交易及智能合約，同時展開各種 DLT 概念驗證項目。專家 Melanie Swan 曾將區塊鏈的發展分為三個階段：區塊鏈 1.0、區塊鏈 2.0 和區塊鏈 3.0，茲介紹如下：

表 2 原生型區塊鏈技術組合之優缺點與相關建議

區塊鏈發展階段	時期	應用
區塊鏈 1.0	2008 年~2011 年	數位加密貨幣（以比特幣為代表）
區塊鏈 2.0	2012 年迄今	可程式設計金融之應用，加入了「智能合約」的概念，使得區塊鏈從最初的貨幣體系，拓展到股權、債權與產權的登記及轉讓，證券和金融合約的交易、執行，甚至防偽、虛擬貨幣首次公開發行（ICO, Initial Coin Offering）等金融領域
區塊鏈 3.0	未來	跳脫貨幣與金融領域，擴展到應用在法律、物聯和醫療等領域，進而到整個社會

在 DLT 眾多應用中，與本行業務最相關者，應屬「數位貨幣之發行」。此數位貨幣之發行，非指普羅大眾所發行之虛擬數位貨幣，因其發行多無擔保品(collateral)為基礎，其幣值的漲跌也缺乏實體經濟作支撐，故此探討數位貨幣的發行，係指以 DLT 運

作機制為基礎，由央行發行法幣，大眾透過商業銀行或直接向央行進行兌換。央行發行的數位貨幣優點在於這種數位貨幣是由政府發行，因此較能被使用者信任，穩定的發行量也有助於維持虛擬貨幣匯率穩定，可解決虛擬貨幣價值不穩定與波動大的問題。然而，對於央行發行數位貨幣，需審慎考慮潛在的成本與風險，如平台的管理與整合，以及如何解決隱私權問題。另外，法定數位貨幣對金融體系監管的影響、貨幣政策制定及央行與商業銀行的角色，一直存在諸多疑問。

(二)加密貨幣—臉書幣 Libra 之探討[5]

1. 2019 年 6 月 18 日臉書宣布將於 2020 年正式推出加密貨幣 Libra，並創立機構 Libra Association，邀請信用卡公司、支付和區塊鏈等機構加入。臉書負責 Libra 專案的首席經濟學家 Christian Catalini 曾表示，許多加密貨幣係兩種角色合而為一，包括：

   (1) 投資工具，用來賭注未來價值上漲；

   (2) 交易媒介，在一定規模上允許人們從事有用之事。

   然渠認為上述兩種角色並非完全相容，因作為交易媒介，任何價值波動都會增加該筆交易的不確定性；對於進行全球買賣的商家來說，若不了解該貨幣於另一端或未來一週之價

[5] 參考資料為 Wall Street Journal 專欄作家 Greg Ip 於 6 月 27 日發布文章「臉書幣 Libra 背後之內涵價值」。

值，則此貨幣機制將大打折扣。

2. 臉書提出採行 Libra 之優點，包括：可以將 Libra 換回底層貨幣（underlying currency），且一籃子貨幣的本質相對穩定；再者，Libra 供給完全是靠需求面決定等。

3. 惟 Libra 亦面臨不少質疑聲浪。MIT 總體經濟學家 Roberto Rigobon 質疑，以金本位為例，人們尚可在沒有實體黃金為基礎情況下發行 IOUs；同理，個人和公司亦可在沒有實體資產為基礎下，發行 Libra 計價的 IOUs[6]，一旦有人擠兌 IOUs，危機終將產生。再者，Libra 支付成本可以有效壓低之程度，以及隱私權等相關疑慮仍待考驗。

四、 區塊鏈對金融服務業之影響

(一)區塊鏈對金融服務業之影響

1. 可能弱化了金融中介或信用機構的功能：

在探討區塊鏈對金融服務業影響之前，應先探討為何比特幣創始者中本聰採用區塊鏈機制。可能是因為他資本不足，故無力承擔建立各節點轉帳設備所需費用，而區塊鏈「節點共同維護特性」可有效降低中央控管成本。其次，中介機構未必願意幫一個陌生人擔任結清算角色。再者，各節點相互不識（亦即缺乏信用環境），而區塊鏈之「公開、共識機制、分

[6] 係 IOU 縮寫，相當於借據。

散式帳本、不易竄改」特性，可以讓交易在眾節點之見證和共識下被完整記錄。因此，區塊鏈可降低交易成本，解決信用不足所產生的風險，但同時也可能弱化了金融中介或信用機構的功能。

2. 有助降低法遵成本

區塊鏈之「分散式帳本」和「溢散式傳播」特性，挑戰了傳統中心記帳的思維。而這種完整和分散式紀錄特性，有助提供事後稽核軌跡，有效降低法遵成本。

3. 實名制、認許式（聯盟式）區塊鏈，可能是未來參考方向

(1) 比特幣區塊鏈（非認許式、公開鏈）具諸多限制，包括：處理量擴增能力、清算最終性、速度侷限性、耗能耗電和究責問題。為釐清責任歸屬，可考慮「實名制」區塊鏈；如欲改善速度和處理量等其他問題，則可考慮認許式（聯盟式）區塊鏈。

(2) 認許式（聯盟式）區塊鏈的優點在於參與節點有限，故可加快交易和記帳速度，也可降低單位時間所需處理的交易量。加上許多認許式區塊鏈的本質就是利益共綁，存在一定信任或契約機制，因此無須提供挖擴等經濟誘因，也可降低因防偽或防竄需求，所耗費之大量運算資源和成本。

(3) 然認許式區塊鏈本身就存在一定信用基礎，與比特幣區塊鏈（非認許式、公開鏈）產生的前提—缺乏信用環境—相悖。況且現有機制本身即具有「可追蹤」、「不易竄改」等特性，如此，為何不沿襲現有中心化運作模式而要採用聯盟鏈模式？有人提出觀點如下[7]：

甲、認許式區塊鏈之核心思想在於點對點的網路（peer-to-peer network），除改變了以伺服器為中心的主從式網路架構外，亦可讓資訊在不同主體間進行選擇性分享。

乙、現有的中心化運作模式，參與者對所屬資料、資料存取方式和資訊系統建立，並無直接控制權；然認許式區塊鏈可以拿回主動權，並可透過聯盟鏈來執行智能合約，進行更深入的應用。

4. 智能合約之發展

過去即有「智能合約」的構想，讓資產或價值的移轉，變成可程式化和自動執行。然當時技術尚未成熟，且未出現一個合適平台來自動執行合約，一直到區塊鏈（平台）的出現，才實現了這個想法。另智能合約中的特色在於，參與者無須透過信任彼此來履行義務，因為合約是由代碼編寫、定義和強制執行，除可減少人工干預和人為判斷外，亦可降低監管成本、提高執行效率和減少資源浪費。目前可應用之金融領域包括：保險理賠、租賃服務等，甚至是 P2P 業務模式（如：P2P 借貸或群眾

[7] Frank Lin（2017）。公共鏈 vs. 聯盟鏈 — 談區塊鏈的價值〔電子版〕。哈佛商業評論。取自 http://dweb.cjcu.edu.tw/ShepherdFiles/C0180/File/20180124115022861.pdf

募資等，對金融服務業者構成一定挑戰）。

(二)金融業者對區塊鏈應用之自我需求評估

金融業者在採納區塊鏈技術和執行相關應用時，可從「What」、「Why」、「Who」和「How」著手：

1. What：工欲善其事，必先利其器。在應用區塊鏈前，需先瞭解其技術核心為何。
2. Why：思考為何要採用區塊鏈技術。相較於現行運作架構，它是否能帶來更多效益（如表 3 所示之優劣分析）。
3. Who：參與對象為何？監管機關從中扮演的角色為何？
4. How：如欲執行，可採納何種形式？如：認許式或非認許式區塊鏈等。

參、人工智慧

一、 何謂人工智慧(Artificial Intelligence,AI)

依據東京大學教授松尾豐的定義，人工智慧係指「用人工手法創造出人類般的智慧，而所謂人類智慧係指能夠察覺到事情的電腦。該電腦的特性在於，在資料當中形成特徵量[8]，並將現象予以模式化，而電腦程式就會依據特徵量不同來執行不同動作」。

二、 人工智慧之發展與應用

近期人工智慧出現突破在於「深度學習(Deep Learning)」發展。松尾豐教授認為，深度學習讓電腦可以根據資料，自行取得高層次的特徵量，再據以分類圖片，降低人類參與執行過程。如果把人工智慧想成人腦，可以先從人腦如何運行來理解。人腦是由神經

[8] 機器學習時用於表示資料的變數，也就是資料當中需關注的部分。

元網路所構成，當某一神經元與另一神經元相連的突觸處受到電流刺激時，就會把電刺激傳導給下一個神經元。而深度學習就如同多層神經網路的模型化，各節點（類似人腦突觸處）接受到數值訊號後，經加權加總，再透過函數轉換輸出，進而執行動作。至於有關人工智慧的發展與應用，茲整理如下表：

表 3 人工智慧發展階段與相關應用

時期	發展內容
1956-1974 第一階段 AI 熱潮	✧ 如何使用電腦解決問題
1974-1980 第一次低潮	✧ 計算機內存空間有限、處理速度低落
1980-1987 第二階段 AI 熱潮	✧ 淺層深度學 ✧ 相關應用：垃圾信件分類
1987-1993 第二次低潮	✧ 專家系統維護費用高昂、難以升級
1993-迄今 第三階段 AI 熱潮	✧ 機器學習、深度學習 ✧ 相關應用：自動駕駛、Pepper 機器人、電腦下棋

人工智慧應用在各領域相當廣泛，例如：

1. 法律業：在審閱文件時，想要尋找關鍵資訊，可以透過人工智慧來排除大量不需要的訊息。
2. 新聞業：以 2018 年 11 月瑞士舉行選舉時，Tobi 機器人為媒體巨 頭 Tamedia 用僅 5 分鐘時間，撰寫了 4 萬篇與選舉有關新聞。
3. 金融業：UBS 提供依據人工智慧來提供客戶最佳資產組合或進行波動交易等。

三、 人工智慧之影響

人工智慧的影響在各領域逐漸擴散，對於機械式和重複式的工作，引進人工智慧系統有助降低時間和金錢成本，但也代表市場對相關從業人員需求下滑，導致就業等社會結構的改變。因此，產業升級和轉型有其必要性。再者，就業市場和社會結構改變，可能會挑戰傳統經濟現象或理論，因此在據以作決策時需思考既有理論是否有調整的必要性。另人工智慧擅於處理通則，但較不擅長處理例外，也較缺乏彈性和情感。這是人類具有優勢之處，也是人工智慧目前不足之處。

肆、心得與建議事項

（一）區塊鏈

一、 心得

區塊鏈之「分散式帳本」和「溢散式傳播」特性，挑戰了傳統中心記帳的思維。而這種完整和分散式紀錄特性，有助提供事後稽核軌跡，有效降低法遵成本。然而非認許式區塊鏈具諸多限制，包括：處理量擴增能力、清算最終性、速度侷限性、耗能耗電和究責問題。為釐清責任歸屬，可考慮「實名制」區塊鏈；如欲改善速度和處理量等其他問題，則可考慮認許式區塊鏈。

二、 建議

區塊鏈的發展為金融和監管業者帶來諸多挑戰，執行相關應用前宜思考下列議題：

1. 區塊鏈雖可降低交易成本，解決信用不足所產生的風險，但也可能弱化了金融中介或信用機構的功能。

2. 區塊鏈發展所帶動的新型 P2P 業務模式（如借貸等），可能分食銀行客源。
3. 區塊鏈仍存在網路犯罪之隱憂。由於部分區塊鏈係匿名機制，使得用戶的加密數位貨幣被盜後，將難以獲得保障。
4. 若央行欲發行數位貨幣，需審慎考慮潛在的成本與風險，如平台的管理與整合，以及如何解決隱私權問題。
5. 該技術將對金融業現有法規和監管框架帶來新課題。例如：歐盟一般資料保護規則（General Data Protection Regulation, GDPR）（2018 年 5 月 25 日生效）中規定的「跨境傳輸原則禁止 」與「被遺忘權（Right to be Forgotten） 」與區塊鏈技術相衝突，且不同國家的法規、管理政策皆不盡相同。這些差異在跨國法規的融合及介接上亦會受影響。

另有關單位在採納區塊鏈技術和執行相關應用時，需先瞭解其技術核心為何並思考為何有採用的必要性？相較於現行運作架構，它是否能帶來更多效益？另需思考參與對象與監管機關從中扮演的角色為何？如欲執行，採用認許式或非認許式區塊鏈等？

（二）人工智慧

一、 心得

近期人工智慧出現突破在於「深度學習(Deep Learning)」的發展。深度學習讓電腦可以根據資料，自行取得高層次的特徵量，降低

人類參與執行過程，然而仍較不擅長處理意外，也較缺乏彈性。人工智慧應用在相當廣泛，以金融業為例，UBS 提供依據人工智慧來提供客戶最佳資產組合或進行波動交易等；以新聞業者為例，Tobi 機器人為媒體巨頭 Tamedia 用僅 5 分鐘時間，撰寫 4 萬篇與選舉有關新聞。這類案例也反映未來市場人力需求有下滑可能。

二、 建議

1. 人工智慧的影響在各領域逐漸擴散，對於機械式和重複式的工作，引進人工智慧系統有助降低時間和金錢成本，但也代表市場對相關從業人員需求下滑，導致就業等社會結構的改變。因此，產業升級和轉型有其必要性。再者，就業市場和社會結構改變，可能會挑戰傳統經濟現象或理論，因此在據以作決策時需思考既有理論是否有調整必要。
2. 對於稽核、稅務、會計與交易資料系統可考慮與人工智慧進行結合 有助加快資料整理、關鍵資料擷取。
3. 人工智慧擅於處理通則，但較不擅長處理例外，也較缺乏彈性和情感。而感性與彈性則是人類具有優勢之處，佐以人工智慧精華用之，才是人類與人工智慧共存共榮之道。

伍、參考資料：

1. Greg Ip (2019)“The Worthy Idea Behind Facebook’ s Libra”, Wall Street Journal, June 27.
2. He, Dong et al. (2017), “Fintech and Financial Services：Initial Considerations,” *IMF Staff Discussion Note*, June 19.
3. 杜宏毅、宋倬榮（民 107 年）。《區塊鏈之書》
4. 杜宏毅（民 106 年）。《如何建置一個實用的區塊鏈平台》。財金資訊季刊，90，44-45。取自 https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9006.pdf
5. 龔鳴（民 106 年）。《寫給未來社會的帳本》。
6. 松尾豐（2016）。《了解人工智慧的第一本書》。
7. Frank Lin（2017）。公共鏈 vs. 聯盟鏈 — 談區塊鏈的價值〔電子版〕。哈佛商業評論。取自 http://dweb.cjcu.edu.tw/ShepherdFiles/C0180/File/20180124115022861.pdf