台灣金融研訓院
Taiwan Academy of Banking and Finance

105 年度自提研究計畫

區塊鏈及數位貨幣在金融業的影響與應用

補助單位：中華民國銀行商業同業公會全國聯合會

計畫主持人 ： 盧陽正

顧　　問 ： 廖世偉、李漢超

共同主持人 ： 林士傑、張凱君

協同主持人 ： 謝順峰、鍾銘泰

研 究 員 ： 李宛蓁、黃杭潯

中華民國 105 年 12 月

財團法人台灣金融研訓院自提研究計畫

區塊鏈及數位貨幣在金融業的影響與應用

補助單位：中華民國銀行商業同業公會全國聯合會

本報告內容純係研究團隊之觀點，

不應引申為補助單位中華民國銀行商業同業公會全國聯合會之意見。

計畫主持人 ： 盧陽正

顧　　問 ： 廖世偉、李漢超

共同主持人 ： 林士傑、張凱君

協同主持人 ： 謝順峰、鍾銘泰

研 究 員 ： 李宛蓁、黃杭淳

中華民國 105 年 12 月

摘要

區塊鏈是跨領域技術的整合，涵蓋資訊安全、密碼學、經濟模型及算法算力，其中最重要的創新在於共識演算法的突破，使其被稱為「信任機器」(Trust Machine)。區塊鏈的特色，包括「去中心化」、「匿名性」、「不可竄改性」、「可追蹤性」以及「加密安全性」。基於上述特性，區塊鏈能夠解決的問題包括：第一、在各方互不相識的情況下建立信任機制；第二、改善中心化導致的成本過高；第三、使資訊真實透明可追溯，同時保護客戶的隱私；第四、依時間順序紀錄資料。我國金融業因應區塊鏈技術興起可考慮下列商業模式：第一、聯合其他同業組建/加入區塊鏈聯盟；第二、結合金融科技公司，發展核心業務的區塊鏈應用；第三、銀行內部自行推動局部領域的應用，實施試驗計畫；第四、銀行成立創客基地，聚焦在金融科技創新與區塊鏈的發展。導入區塊鏈應用技術不必拘泥於任何一種策略，甚至可同時進行。第五、發展區塊鏈技術應用於電子支付及行動支付，實現數位經濟的發展。

目錄

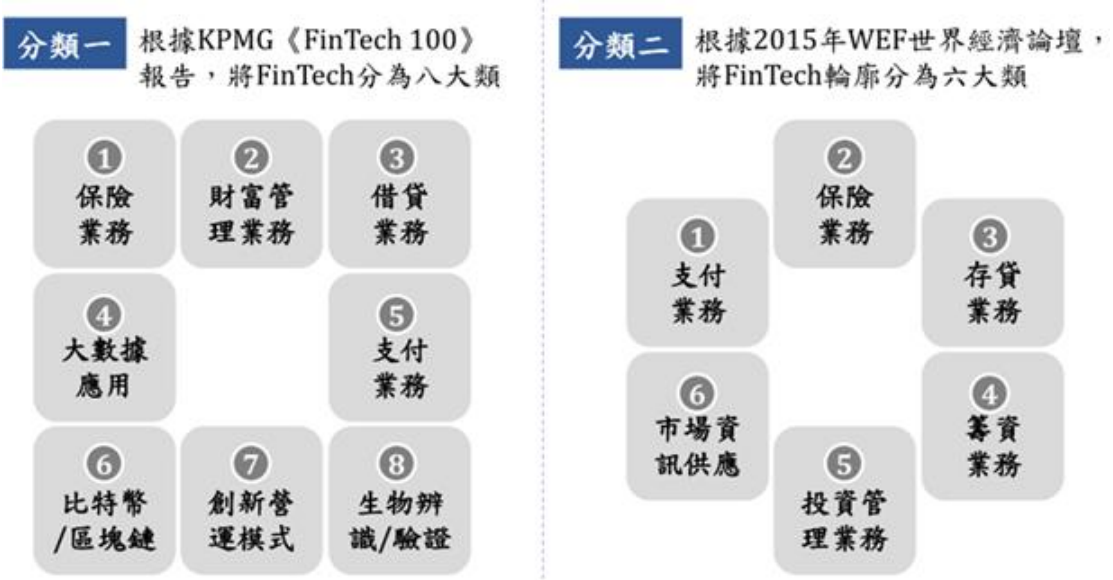
圖目錄

表目錄

第一章 緒論

第一節 研究背景

近來科技金融(FinTech)以燎原之勢急速發展，且發展面向甚廣，一般對於科技金融囊括的面向與分類可參見下圖。



根據 KPMG《FinTech100》報告的分類，科技金融包括我國金融業者熟悉的借貸業務、支付業務，此兩者的創新近年都已獲得長足的進步。另外，比特幣/區塊鏈亦列名其中。事實上，新興的區塊鏈(Blockchain)技術，受重視的程度日益增加，已吸引全球政府機關與金融業巨擘相繼投入研究。目前區塊鏈技術在西方國家研發可謂如火如荼，光是投資到新創公司的資金就超過 10 億美金，是 1990 年代中期對網際網路新創投資的四倍金額。華爾街日報曾表示，虛擬貨幣是金融領域五百年來最偉大的創新之一。達沃斯世界經濟論壇則認為，直至 2027 年，全球將有十分之一 GDP 透過虛擬貨幣科技儲存。前美國聯準會主席柏南克公開肯定比特幣「具有長期前景」。

IDC 發佈對 2017 年台灣十大資訊科技市場預測。在產品應用愈趨多元，產業發展愈趨競爭的態勢下，創新與轉型已是目前企業發展的重心，連帶

帶動數位經濟的推升，企業正透過新的數位科技進行轉型，新的商業型態正在興起。未來三年我們將會看到數位轉型進入新的規模，數位經濟將擴張成為宏觀經濟的一部分。在未來數位轉型的趨勢下，企業必須建立新的策略發展構面與新的 KPI 來因應轉型的需求，IT 領導力將在其中扮演重要角色。IDC 發佈 2017 年台灣十大資訊科技市場預測如下：

(一)平台經濟崛起，台灣將朝複合式/新型態經營模式發展

從 Google、Amazon、Facebook..到 Uber，Airbnb 等不具備實體資產卻能透過創新服務模式創造產業新經濟模式的平台經濟正逐步崛起，帶動全球經濟能量蓬勃發展。IDC 發現隨著產業競爭越來越激烈，平台業者開始著重在創造新的核心經營價值。現今的平台業者正打破傳統思維，逐步由消費者為中心轉變為重視整體平台經濟的生態系統，並能應用數位科技，以最快的速度搶佔市場規模並制訂平台規範。但以台灣的市場規模及型態，較難複製全球單一平台的經營模式。未來能勝出的將是朝多種平台相互運用並透過不同排列組合的經營模式，此類模式才能最大發揮一加一大於二的效果。預期台灣平台經濟將朝複合式經營與規劃方向前進，2017 年將是台灣平台經濟的新契機。

(二)認知時代來臨，人工智慧應用起飛

隨著科技的日新月異，人工智慧技術逐步從研究領域進入商業領域。過去一年，除有不少新創公司透過人工智慧等認知軟體優化產品服務與突顯差異化競爭能力，也有不少企業導入智慧助理、自然語言辨識、生物辨識與機器學習等人工智慧技術優化客戶服務流程與提升客戶體驗，包括金融、證券、專業服務與娛樂等產業都已發展出相關應用。IDC 預估市場對人工智慧技術的需求將持續看漲，尤其是在結合聊天機器人與自然語言辨識等人工智慧技術的智慧助理服務、強調視覺化呈現的人機介面、內嵌人工智慧技術的智慧應用服務、以及生物辨識等應用將是未來一年發展上的亮點。此外 IDC 預測隨著市場對人工智慧應用的高度關注與需求，將使得

台灣認知軟體市場規模將呈現倍數增長，預計市場規模將從 2015 年的 221 萬美金增長到 2020 年的 686 萬美金，年複合增長率將達 33%。

(三)區塊鏈推動創新 ，重新定義市場

在比特幣以及數位貨幣發展後，區塊鏈技術的發展及價值已經逐漸被市場關注及重視。區塊鏈具有開放、去中心化的特性，任何人都可以在上面創造新的服務和應用，對於未來產業創新將扮演一定角色，加上其導入信任機制，使具有高度安全性，IDC 認為區塊鏈將有機會重新定義未來市場運作模式並建構新一代資訊架構。區塊鏈目前已經從金融領域逐步向其他產業延伸，包含數位交易、智慧合約、產銷履歷、資產管理等。台灣在區塊鏈發展上，已有銀行業在金融科技(Fintech)有相關專案的應用及推動，預計未來在 Fintech 外，包括生產履歷、健康記錄、房仲交易、薪資支付等非密集交易等業務上，都將逐步發酵。

(四)數位市場(Digital Marketplace)帶來全新行銷模式與消費者體驗

擴增實境(Augmented Reality)、虛擬實境(Virtual Reality)、混合實境(Mix Reality)等技術在過去一年的發展下，已具備技術形貌。IDC 認為未來這類技術將更快速地導入企業經營核心，並開始轉變企業產品行銷與廣告經營手法。面向消費者為主的行業將首先開始發酵，越來越多以擴增實境/虛擬實境為主的技術將納入企業數位行銷的策略中，此情況將激發更為積極與生動的數位遊戲化行銷模式，並創造出高黏著度的消費者體驗。IDC 預估在 2017 年，台灣 30%以消費性商品為主的大型企業，將透過擴增實境或虛擬實境等技術推出全新行銷手法。行業也從零售型的消費性產品，涵蓋到觀光旅遊、娛樂、文化藝術、室內裝潢設計、房屋仲介等數位商務與服務。這種多元化的數位型態行銷介面，預期能幫助與增強企業與使用者的溝通，也將為消費者帶來全新的購買體驗，而與之相關對應的 IT 設計與解決方案生態系也會從 2017 年陸續衍生擴張。

(五)數位生態催生新一代資安架構

隨著行動化、雲端、Fintech 以及物聯網的應用，新的數位生態因應而生，資安需求也隨著開始變化。尤其做為控管資訊安全的第一道防線「身分與授權管理」(Identity and Access Management，IAM)更顯重要。由於身分與權限管理已打破原有網路邊界，且防護的範圍已從網路、數據到 APPs；因此企業需要強大的權限控管與身份管理以確保資訊安全。IDC 預測生物辨識的導入以作為身份認證、線上交易以及行動支付的重要把關條件將愈形重要。預期 2017 年台灣將有 20%的線上交易會透過生物辨識進行交易。而隨著數位生態的出現所導致越來越多的資安漏洞及事件，已使得企業將資安升級至戰略性的角色。IDC 調查發現台灣超過 26%(亞太地區：14%)的 CIO 認為資安與企業競爭力高度相關；尤其現今資安攻擊漸趨於集團性，且大部分的病毒已無法由特徵碼阻擋；企業在面對未知的病毒攻擊下，大幅的資安設備投資以及人才的培養已成為企業面臨的挑戰。

IDC 預測企業仰賴資安服務廠商的程度將愈形加重。而為因應企業需求的轉變，IDC 認為系統整合廠商將更積極的提供更多元的資安服務；資安原廠間將有更多併購及合作，電信業者亦會結合原有網路設備資源，擴大資安解決方案能量，使得資安服務市場形成新的競爭態勢。IDC 預期 2017 年台灣資安服務仍保有成長動能，2017 年成長將達 17%。

(六)Cloud 2.0：混合雲成為企業數位轉型發展核心

隨數位化時代來臨，企業的營運流程必須更加彈性、靈活與快速的反應市場變化，而雲端及資料中心應用將成為企業轉型的重要支撐。IDC 預測國際大廠將透過雲端及資料中心應用服務積極進行混和雲的策略佈建，在協助企業能夠擁抱現代化雲端設備的同時，也不會犧牲企業本身的安全與管控能力。而對於大型企業而言，混和雲具有因應突發狀況(bursting)與災難備援(disaster recovery)的優點，對中小企業來說，混和雲提供更具成本之效益，未來企業對混和雲的運用更為積極。IDC 預估 2017 年將有超

過 55%的台灣企業規畫將進行混和雲(Hybrid Cloud)相關佈署。

(七)聚合型資訊架構將成企業數位轉型重要基礎

隨者新技術與新商務模式不斷浮現，企業對資訊架構在速度(Speed)，敏捷(agile)，彈性擴張…等需求愈來越高，以期能符合企業對於發展創新服務的需求。另一方面，台灣公有雲(Public IaaS)市場已達 78.28 萬美元，2016 年上半年更較去年同期增長達 55.8%，顯示資料中心運用虛擬化技術提供企業資訊服務已成普遍趨勢。IDC 預估虛擬化技術後的資訊環境更形複雜，對企業資料中心維運帶來更多挑戰，包括不易維護更新、不易偵測系統錯誤、效能瓶頸，不易規劃資源提升計畫，及系統規格效能縮放不夠即時等。為了滿足企業數位轉型需求，且能協助企業面對虛擬化後的挑戰，IDC 認為未來聚合系統、超聚合系統等將對企業基礎架構系統帶來最大效益，IDC 預估 2017 年超規模級資料中心(hyperscale datacenter)將加速採行聚合資訊技術以提升雲端服務水準(service level)，進而幫助企業邁向數位轉型。

(八)3D 列印技術開始扮演企業數位轉型推手角色

隨著 3D 列印的技術日趨成熟，其應用市場也發活絡，全球各國政府在推動數位轉型之下提出預算投資 3D 列印以不落人後。3D 列印技術之所以為各國所關注，在於其間接促成了敏捷式創新與民主化設計兩大數位轉型核心之綜效。不僅可以為企業縮短開發時程加速新品上市先機，也讓消費者能夠藉由 3D 列印技術參與企業產品開發，讓企業能跨界尋求更接近使用者的產品觀點，減少市場測試風險且增加市場反饋彈性。IDC 預期在教育市場外，台灣 3D 列印應用將因數位轉型需求逐步擴散至消費品市場(commodity) 、製造業及醫療產業。除了因數位轉型需求帶來的改變外，3D 印表機市競爭態勢也正在改變。除了原有的 3D 印表機生產製造廠商外，2D 印表機廠商也開始滲透，虎視眈眈的還有材料與服務供應商。在技術需求大增與供給多元化的刺激下，IDC 預期台灣 3D 列印市場 2017 年將有

三成的成長，全年產值將突破 3,000 萬美元。

(九)數位轉型需求驅動電信業朝 SD-WAN，UCaaS 以及 OTT 發展

為因應長期面臨數據營收成長幅度無法彌補語音營收下滑速度的窘境，以及越來越強烈的數位轉型需求，台灣電信業者在網路建置和服務內容的交付上已經開始規劃或導入新的技術。IDC 認為為加速數位轉型，電信業者將積極發展三項業務：SD-WAN、UCaaS 和 OTT Video。在降低營運成本和增強網路管控品質等因素的考量下，IDC 觀察一般企業內部網路的建置將會從傳統 MPLS 或 Lease Line 的架構轉向 SD-WAN。其次，傳統企業的整合通訊 UC 的佈建型態也開始產生變化。IDC 預期 2017 年有 30%的企業會導入以雲平台做為基礎的 UCaaS，以降低資本支出和達成快速佈建 UC 的要求。另外，OTT 服務模式的出現讓原有提供付費收視服務的供應商如電信公司或有線電視業者開始著手進行改善遞送服務內容的方式，採用雲平台架構達成終端用戶 TV Everywhere 的目標。預測這三種新技術或應用於 2017 年將為電信業者最積極耕耘的新市場。

(十)機器人串聯智慧網路，成為智慧家庭發展要角

過去所看到的機器人應用多以工業為主，但近年來可以看到機器人的應用不再局限於工廠的機械手臂，越來越多的商業用途機器人運用在銀行業和零售業，消費機器人也逐步出現。IDC 觀察到廠商投入以消費市場為客群的家庭服務機器人的腳步越來越積極，此類家用陪伴型機器人除有影音互動、教育娛樂功能外，同時具備意外警示回傳，部分更可進一步做到智慧連網，自動遙控家電，成為家庭控管的中樞。IDC 認為 2017 年家用服務機器人仍會以陪伴娛樂為主要功能，預期在 2020 年智慧家庭建置趨於成熟，家用陪伴機器人的功能性將更多元化且更顯其重要性。

另外 2016 年 8 月份世界經濟論壇（World Economy Forum）的調查報告指出，下一代的金融服務基礎架構，將由區塊鏈提供關鍵技術，報告並

預測 2017 年全球會有 80%的銀行機構初步運行分散式帳本，而全球已經有 14 億美元的資金投入到區塊鏈新創之中，未來比起 1990 年代網際網路的投資熱度，區塊鏈將更為超越。調查報告指出，分散式帳本將會出現各種方式的延伸應用，而且因為結合不同科技，它的效益也越來越多元。WEF 調查報告亦指出，區塊鏈將於 2027 年前大幅成長，屆時全球將有十分之一的 GDP 是來自於區塊鏈技術與協議所進行的商業活動。現今互聯網經由網絡與中心化平台，已造就出各種社會經濟的新型態商業模式，並為社會經濟創造出高效率與新機會（如 Amazon、Uber、Airbnb 等）。而未來區塊鏈此新興的去中心化技術，將取代需要第三方實體或虛擬機構為交易平台以提供信任的商業模式，將互聯網引領至更高層次去中心化的價值互聯網境界。

而資誠(PwC)最新發布 2016 年全球金融科技調查報告(Global FinTech Report 2016)，認為對新進的金融科技業者來說，去中心化、降低成本、顧客忠誠度及差異化是金融業最重要的 Fintech 創新概念，且特別針對區塊鏈技術（Blockchain）進行調查，並認為區塊鏈金融將創造金融業的經營模式創新。PwC 調查報告一共調查了來自 45 個國家的 544 位金融業及金融科技業的高階主管，其中有 3 成為銀行業者，財富管理業者、金融科技業者也各占 2 成，其餘包含保險、轉帳及支付服務等領域業者。23%受訪對象為企業 CEO，21%為 IT、技術及各部門主管，14%財務長、營運長，策略長、創新長各占 7%。金融業者普遍認為，在未來 5 年之內，超過 6 成的消費者將透過行動裝置來取得金融服務，且每個月至少使用一次。而新進的金融科技業者。將補足過去金融業者無法提供、滿足的消費者需求缺口，並從這些領域切入金融服務市場。

根據 PwC 最新調查報告結果顯示，有 75%金融業者認為，金融科技帶來的最大轉變，是所有的金融服務與產品，都將更聚焦在顧客身上。有趣的是，高達 8 成金融科技公司認為自己是以顧客為核心的組織，但是只有 53%的傳統金融機構認為自己以顧客為中心。對於 Fintech 帶來的價值，

金融業者認為 Fintech 可以明顯降低金融服務的成本，同時提高服務的效率及品質，根據調查結果，73%金融業者認為金融科技可降低成本，62%認為可提供差異化服務，58%認為可提升客戶忠誠度，這 3 項是目前金融業者認為金融科技的最主要核心價值與機會點，而去中心化則是金融科技業者的創新思維。除此之外，全球高達 83%金融機構都擔憂業務將被金融科技公司搶走，包括消費者金融服務、轉帳及支付服務，也有多數資產管理及保險業者也都認為受到很大的影響。其中銀行業、支付業認為 5 年之內，將會有近 28%業務將遭到衝擊，保險業、資產與財富管理業則認為將有 22%的業務受衝擊。主要對金融業者帶來的衝擊包括營業利潤(67%)、失去市場占有率（59%）、資訊安全／網路隱私（56%）、以及顧客流失率的增加（53%）。

目前有 67%的金融業者認為應充分利用這個金融科技的生態圈，開始布局金融科技，32%建立合作關係，15%開始培育金融科技，22%購買其服務，也有 9%已經併購金融科技公司。而傳統金融業者若和金融科技業者合作，也將面臨不少的挑戰，首先，傳統金融業者認為 IT 系統安全性為最大的挑戰，金融科技業者則認為管理體系和文化差異是一大挑戰，除此之外，法規的不確定性是兩方都極為在意的因素之一，分別有近 5 成（49%）的金融業者及 43%金融科技業者認為這是一大挑戰，其他問題包括商業模式與營運流程的差異等。

過去企業內部採用 ERP 企業資源管理軟體，來傳遞並共享資料與邏輯，讓企業內部的商業流程最佳化，而區塊鏈技術將是能促成下一階段商業流程最佳化大幅躍升的技術，區塊鏈技術能促使整個產業之間的商業流程更進一步達到最佳化，讓不同的或是彼此相互競爭的企業之間傳遞、共享資料。建構區塊鏈技術整合、加密技術及模型，目的是在不需第三方機構協助驗證與對帳的條件之下，維護一套由多個參與者所組成網絡關係的資料庫，簡單來說，便是一個安全的分散式帳本。儘管區塊鏈技術本身目前看起來極為可信，但依舊存在不少挑戰與障礙待突破，此外，若能真正深入

了解區塊鏈技術並進行商業應用，得跨各領域進行知識互通，而這也將帶來許多未知及潛在的應用可能。

區塊鏈用於後臺營運不僅能降低成本，也能大幅提升交易透明度，對消費者及監管單位來說都是一大好處。其中一個熱門的應用領域便是智慧合約（smart contract），能將契約數位化並自動執行與維護。智慧合約概念源自於 1994 年由尼克・紹博（Nick Szabo）所提出。智慧合約之所以稱為智慧的，係因其比傳統的合約向前邁了一步，亦即能夠實際執行資產所有權於特定條件下轉讓的管理與控制。智慧合約為一套以數位形式定義的承諾（promises），包括合約參與方能在區塊鏈上面執行這些承諾的協議。數位形式意味合約可自動化執行電腦可讀的代碼，因為只要參與方達成協定，智慧合約所建立起的權利與義務即能強制性執行，而不需要值得信賴的第三方仲裁（arbitrator），讓人們能通過互聯網與陌生人進行資產的交易（transaction），以實踐價值互聯網的境界。未來企業各種形式有價值的智慧資產或數位資產透過去中心化的區塊鏈來決定資產的所有權。而資產所有權的管理藉由區塊鏈智慧合約的演算法來自動執行，並在約定條件下自動觸發所有權協議的執行。

全球業界現在都在積極尋找物聯網創新商業模式，國際資訊專業研究顧問機構 Gartner 在 2016 年 8 月及 10 月分別發表二份重量級報告：「2016 年技術成熟度曲線報告(Hype Cycle for Emerging Technologies,2016)」以及「2017 年 10 大策略性科技趨勢預測」，在前一份報告當中，Gartner 將超過 2,000 種科技歸類為三大關鍵科技趨勢，並依照到達成熟生產期所需年份做出技術成熟度曲線排列。而 Gartner 發布 2017 年 10 大策略性科技，當中前三大都是智慧元件運用技術的創新，包括(一)人工智慧與先進機器學習(二)智慧應用程式以及(三)智慧物件。根據二份報告歸納，智慧機器(機器學習及機器人)、區塊鏈(Blockchain)平台以及物聯網平台(IoT Platform)將在未來 2 到 10 年內快速發展成為最受矚目的科技新星，智慧製造已躍昇主流，未來「智慧硬體」及「智慧軟體」結合，透過物聯網感測器服務

平台建構智慧精密機械的物聯網環境商機。例如美國家電大廠惠而浦(Whirlpool)與 IBM 人工智慧系統 Watson(華生)推出智慧家電(Home Automation, HA)的合作模式，未來物聯網擴大到教育、醫療、交通、金融等領域，真正落實在你我的生活環境當中。

有了物聯網和大數據技術的加持，人工智慧這二年突飛猛進，人工智慧應用在金融業以生物辨識(Biometric)及區塊鏈(Blockchain)金融平台發展最被看好。生物辨識不需客戶刻意準備資料就可運用，相當符合銀行用戶體驗及身份驗證效果佳以及數位風險控管的要求；而區塊鏈金融的點對點(Peer-to-Peer)去中介化架構融入大數據智慧融資決策模式，未來貿易融資及供應鏈金融將有全新思維，更有智慧，也更節省人力。

微軟今年 4 月宣布推出 BaaS (Blockchain as a Services)後，10 月底與 AMIS、工研院合作推出亞洲第一個「帳聯網」聯盟區塊鏈(consortium blockchain)，與國內主要金控共同推動台灣區塊鏈金融的大商機。未來中小企業建構產業區塊鏈聯盟也將成為趨勢。聯盟內中小企業進供貨訂單交款與財務、經營及其他質性大數據，透過去中心化的密碼編譯節點認證在區塊鏈中流通，資金需求端提供給銀行或由銀行付費購買該區塊鏈資訊，資訊將更加透明及可靠,降低企業倒債及洗錢風險,中小企業貸款更容易；而未來金融帳聯網延伸到產業物聯網，對於銀行建構中小企業融資徵信以及放款決策具有相當大的作用，工業 4.0 時代智慧金融將無所不在。

未來區塊鏈技術發展的趨勢，由於區塊鏈技術基本上是具備加密特性的數位貨幣或支付系統為其主要應用，目前開發的產品或解決方案多為概念或驗證層次，未來發展自動執行合約條款的智慧契約技術，以及以區塊鏈為基礎的可交易資產，即智慧資產，主要為數位貨幣以外的其他金融領域應用或股、債、產權的登記及轉讓，資產有關的註冊、交易活動與其他金融商品合約的交易與執行等。未來如身分認證、醫療、公證、仲裁、簽證、審計、物流、網路投票等均會應用到區塊鏈技術。而目前國際上區塊

鏈的技術發展走向聯盟體制與開源開放平台有三大主流技術，包含金融機構聯盟 R3 所開發的 Corda、Linux 基金會旗下的開源區塊鏈專案超級帳本(Hyperledger)計畫，以及乙太坊（Ethereum），國內則有帳聯網等相關技術。除金融業除分別投入各聯盟、平台之外，微軟、IBM 等也透過雲端平台建立區塊鏈應用的生態系。

以目前最大的區塊鏈聯盟之一，全球 43 家銀行所組成的 R3 聯盟為例，原本外界推測 R3 將從現有區塊鏈協議與區塊鏈供應商之中，挑出一套最適合金融應用領域，且大家都認可的區塊鏈協議，用來打造這些會員銀行之間的跨行清算系統，沒想到他們在研究過所有現有的區塊鏈協議後，決定自行開發一套有別於現有區塊鏈的系統。R3 推出一套自行開發的新分散式分類帳平台（Distributed ledger），稱為 Corda，並宣稱 Corda 不等同於現在火紅的區塊鏈（Blockchain）。R3 市場研究總監 Tim Swanson 也澄清，他們要做的並不是區塊鏈，而是可更通用於金融產業的分散式分類帳平台。

新分散式分類帳平台 Corda 的特色是沒有採礦機制，也不會共享所有資料，符合金融業業務特性及需求。亦即 Corda 是專為金融機構所設計，基於銀行的需求，因此在方法、設計與情境上都與目前的其他區塊鏈技術不同。之所以強調 Corda 並不是區塊鏈，是因為它本身並不具有一連串的 Hash 區塊（A chain of hash block），也沒有像比特幣區塊鏈一樣地採礦機制和礦工角色，銀行並不希望與其他機構共享所有的交易紀錄，因此 Corda 可讓開發者自行選擇不同的演算法機制，在 Corda 平臺上的所有交易紀錄，即使都已經加密，仍然不會共享給所有的參與者。

根據 R3 市場研究總監 Tim Swanson 分析，現階段只在內部讓會員銀行進行測試，有一套完整協議，目標是要平台化，提供足夠彈性，讓各種具法律效力的合約（Legal agreement）可以在各機構之間安全傳遞。未來會先將其中的部分元件開源，讓其他組織可在 Corda 平臺上採用不同演算

法。相較於 Linux 基金會的 Hyperledger，Hyperledger 是非營利開源專案，有多個程式碼基底（Code base）所組成，包括 Intel、IBM、Ripple、Digital Asset Holdings 及 Blockstream 都提出程式碼貢獻，目前 Hyperledger 還在提議階段（Proposal），尚未形成一個帳本（Ledger），且主要來自科技公司的團隊所提出。而專為金融機構所設計的Corda則已經是實際試驗中的產品，因為 R3 本身也是 Linux 專案的成員，未來 Corda 可能成為 Hyperledger 的其中一項專案。

國際多家跨國機構成立 R3 聯盟，也有中國大陸自主建立的金融區塊鏈合作聯盟，顯示在競爭激烈的環境下，相互合作有助建立主導地位，發揮加乘效果。

話說從頭，網際網路的起點始於 1973 年 TCP/IP 協議，它打破了由中心傳遞資訊的傳統方式，突破訊息在傳遞過程中地域、物理及成本的限制；區塊鏈可視為 TCP/IP 協議的升級版，以共識機制確保資訊的真實性。區塊鏈將推動嶄新的共享經濟，形成與資產鏈結的全球開放信用體系(Trust Machine)。

上述種種現象讓我們體認到，做為科技金融的一環，區塊鏈的發展已勢不可擋，且此一技術的應用從最初的數位貨幣，日漸滲透到金融業的各個層面。我國金融業在放眼世界，朝國際化發展的同時，必須密切注意此一趨勢，並且妥為因應。

2015 年是區塊鏈技術被討論得特別熱烈的一年，形成了區塊鏈 1.0、區塊鏈 2.0 和區塊鏈 3.0 的概念。

區塊鏈 1.0 就是以比特幣為代表的虛擬貨幣，雖然問題重重，包括價格的劇烈波動、數量上限可能導致的通貨緊縮、挖礦對能源的浪費、各國政府監管的限制等等，但其仍然是區塊鏈技術目前為止最成功的應用，並為人們勾勒了一幅理想的遠景—全球貨幣的統一，貨幣的發行不

再依賴於各國的央行。

區塊鏈 2.0 可以被理解為區塊鏈技術在其他金融領域的運用。包括目前華爾街金融業者想要聯合打造的區塊鏈行業標準，提高銀行結算支付的效率，降低跨境支付的成本；交易所積極嘗試用區塊鏈技術實現股權登記、轉讓等功能。

區塊鏈 3.0 將區塊鏈應用的領域擴展到金融行業之外，覆蓋人類社會生活的各個層面，在各類社會活動中實現資訊的自證明，不再依靠某個第三人或第三方機構獲取信任或建立信用，實現資訊的共用，包括在司法、醫療、物流等各個領域，區塊鏈技術可以解決信用問題，提高整個系統的運轉效率。

區塊鏈在現階段的發展，其實已漸漸不再只是一項新的技術，若以交通舉例，最初的區塊鏈可能是一家汽車公司推出的一款高級車內之技術，此款車有特別的引擎系統與路線規劃能力，能幫助駕駛人更快也更有效率的到達目的地。然而現在的區塊鏈發展已不僅於此，除被廣泛應用在其他的車款，甚而如店家等其他定點也陸續加入，當更多的車款與商家加入這項系統和使用其路線規劃技術，路線的規劃就更為準確，也因此，區塊鏈相形而言是一項基礎建設。

基礎建設的概念其實是近來才出現的格局，在 2015 年之前的金融科技主要在於現有技術的優化、以及使用者體驗上的提升，但是並沒有涉及到金融行業的基礎架構；而現在隨著區塊鏈的技術提升，即將進入金融科技 2.0 的時代，全面革新金融業傳統的基礎架構，區塊鏈在不久的將來無疑是金融行業的基礎建設！

值得注意的是，獲得重金投資的不只是在區塊鏈基礎建設而已，也在上層應用，諸如金融業的結算系統，數字憑證如股票的發行，及日常生活中的應用。美國證監會（Securities and Exchange Commission, SEC）

在 2015 年 12 月批准了線上證券發行商 Overstock 用區塊鏈發行股票的計畫，預計可大幅降低發行成本。英國首相的首席科學顧問 Sir Mark Walport 也建議英國政府，在主要公共服務上，例如稅收、福利或簽發護照等採用區塊鏈技術[1]。在中國大陸，區塊鏈相關研究也正積極開展，中國人民銀行行長周小川在 2016 年 2 月接受媒體採訪時，再次提到該行正研究發行「數位貨幣」。

區塊鏈的應用場景大致可分為數位貨幣、記錄保存、智慧合約和證券。具體包括跨境支付、電子商務、投票、公證、智慧財產權保護、證券發行交易、眾籌、契約、擔保等各類社會事務。無論是公證、醫療、房地產還是物聯網領域，只要有過多的中介參與，過高的中介成本或者是低追蹤成本和高資訊安全的需求，都會有區塊鏈技術的用武之地。

金融領域存在大量諸如銀行、證券交易所等中介機構，對區塊鏈技術的巨大需求也形成了目前對區塊鏈投入最多的領域，金融系統的去中心化將大大提高系統的運行效率。目前的貨幣發行由央行控制，以政府為中心，進行集中式貨幣管理控制，比特幣的產生是為人們提供一種去中心化的數位貨幣。比特幣的成功對傳統金融機構產生了巨大影響，各大機構紛紛涉入區塊鏈領域，試圖用區塊鏈技術取代傳統金融底層協定。金融領域與社會發展密切相關，金融業對區塊鏈技術的探索對區塊鏈發展起了明顯推動作用，衍生出側鏈、私有鏈等新概念，加速區塊鏈技術成熟與應用。

由於區塊鏈在金融領域應用前景廣闊，全球各大金融機構都積極參與區塊鏈項目的投資，在區塊鏈技術上加強研究，其中包括納斯達克、高盛、花旗、摩根士丹利、瑞銀等。銀行等金融機構的基礎設施融合底層區塊鏈技術結合，將對現有的支付、交易、結算的方式產生深遠的影響，提升其運作的效率。歸納來看，銀行的投資有幾種途徑，其中之一

[1] 參見「臺大金融科技區塊鏈」網頁 https://fintech.csie.ntu.edu.tw/，本章若干內容摘錄自該網頁。

是商業銀行成立內部的區塊鏈實驗室。比如花旗銀行、瑞士銀行等已相繼成立研發實驗室，重點圍繞支付、數位貨幣和結算模式等方面測試區塊鏈的應用，有的還擴大到其員工內部系統中測試。另外就是投資金融科技初創公司。2015 年以來，許多跨國大型金融集團紛紛以創投形式進入區塊鏈領域，例如高盛即聯手其他投資公司向比特幣公司投資。

區塊鏈技術對我國金融業的有益影響，至少包括：

第一，區塊鏈能提供更簡易的清算系統，讓發生交易即為清算，不需要花費額外的時間做清算的動作,且發生交易的當下即產生新的區塊，而新的區塊就會被寫入公開的分佈式帳本之中。

第二，區塊鏈去中心化的特性，讓所有的收付手續更加簡易，無需中間機構的介入，且所有的交易達成都必須足夠節點承認才算完成，才能夠寫入帳本中。

當然我國金融業應用區塊鏈技術時可能會遭遇不少挑戰，例如：

第一，對一般無相關知識的大眾而言，要理解並認同此一新興技術相對不易，相關的宣導和基本概念必須能夠傳遞給一般消費者，讓大眾對此有基本的理解。

第二，法規的出現和制定總是相對落後於實務發展，新興技術往往對現有法規產生挑戰，相關的約束和現有法條的編修勢必得有所因應，此乃保障大眾和企業，也讓整個體系趨於穩定。

現今海外許多先進國家已投入大量資金於區塊鏈的技術研發中；而眾多海外區塊鏈應用的新創公司例如 G Coin,、Hyperledger、Consensys、Eris blockchain 等等亦紛紛興起。截至 2015 年 10 月創投公司累積投入區塊鏈領域的資金高達九億兩千一百萬美元；並且有 30 家以上的銀行以及金融機構已經開始投資並分析區塊鏈領域的科技，證明區塊鏈成長潛力無窮。

雖說區塊鏈在FinTech領域相對而言是新技術，但近兩年在歐美與亞洲國家已陸續出現在金融實務界之應用，或者正式宣示區塊鏈金融之重要性。本章先將相關發展簡要說明如下，較為詳細的介紹請參見本研究報告第三章。

一、歐美國家

(一)2015年

1.2015年下半年美國銀行向專利商標局(USPTO)申請10項與「區塊鏈」技術相關專利。

2.2015年7月，澳洲幾家主要金融機構，諸如澳盛銀行(ANZ)、澳洲國家銀行(National Australia Bank)與澳洲中央銀行(Reserve Bank of Australia)等12家主要金融機構與比利時的環球銀行金融電信協會(SWIFT)合作，共同開發全新的金融服務基礎建設--澳大利亞新型支付平台(New Payment Platform)，預計在2017年下半年上線。

3.2015年12月，IBM、JP Morgan Chase、倫敦證交所、富國銀行與Linux基金會合作，共同宣布「開放帳本計畫」（Open Ledger Project）。

4.2015年9月成立的紐約金融新創公司R3 CEV召集銀行業者組成區塊鏈技術聯盟R3，共同開發區塊鏈的分散式分類帳技術，到2015年底，已有42家銀行加入。

5.瑞士銀行於倫敦成立「Crypto 2.0」團隊，從事數據區塊鏈技術研究，該行宣稱已經開發出區塊鏈技術在20多種用途上，並開發出「智能債券」(Smart Bond)。

6.那斯達克交易所在2015年12月30日宣布與金融創新機構Chain.com合作，在其區塊鏈技術平台Linq首次成功交易一檔個股。這種創新的交易能夠記錄每筆交易流向，從此金融交易將公開透明、降低成本。更甚者，

買賣方可自行交易，去除中間人(Dealer或Specialist)，人工撮合可能走入歷史。

(二)2016年

1.英國JP Morgan Chase2016年1月決定和新創公司Digital Asset Holdings合作啟動區塊鏈試驗計畫，希望簡化流程並加快速度，同時降低錯誤的機率。

2.澳洲聯邦銀行(Commonwealth Bank of Australia)積極發展區塊鏈技術，並以新創加速器的姿態，在2016年1月成功開發出開放性行動支付平台—Albert。

3.西班牙最大銀行桑坦德銀行(Banco Santander)認為如果全世界的銀行內部若都使用區塊鏈技術，到2020年每年約省下200億美元的成本。

二、亞洲國家

(一)2015年

1.中國人民銀行2014年成立專門的數碼貨幣研究團隊，並於2015年初進一步擴充發展，研究使用區塊鏈技術去紙幣，且宣稱「已取得階段性成果」。

2.2015年10月15日全球首屆區塊鏈高峰會在上海召開，來自中國人民銀行金融研究所、人民銀行徵信中心、上海證券交易所、陸金所、德勤會計事務所等全球對區塊鏈技術應用前景有興趣的專業人士參加。

3.中國銀聯、阿里巴巴等多家公司陸續宣布研究區塊鏈技術在眾籌、P2P、證券交易等傳統金融領域的應用。

4.新加坡金融管理局(Monetary Authority of Singapore，MAS)與星展銀行及渣打銀行聯合開發組建以區塊鏈為基礎的記錄系統，該技術將被用在提高進出口商及銀行在發票融資(應收帳款融資)領域的安全性和便捷性。

(二)2016年

1.南韓中央銀行在報告中指出區塊鏈發展的重要性，因該技術特徵在於可以安全高效率的提供金融服務，且不需中介機構負責處理交易資訊。故該行將持續關注區塊鏈技術的發展，進行深度研究，甚至考慮將自行投入分布式帳簿技術的研發。

2.南南韓民銀行與當地的比特幣創業公司Coinplug進行合作，宣布藉由使用區塊鏈技術就可以避免掉中介服務，能夠降低成本，為客戶帶來好處。

3.日本幾家銀行和科技業者，包括歐力士銀行、靜岡銀行、NTT數據公司和NTT DOCOMO合資企業提出對區塊鏈進行研究的主張。

4.日本證交所2016年2月16日宣布與IBM Japan達成共識，一同為區塊鏈技術進行測試概念性驗證((Proof-of-Concept，PoC)。

5.香港政府在財政預算案中明文提到區塊鏈技術，可說是首個提到區塊鏈技術的政府機關，鼓勵業界和相關機構，探討區塊鏈技術在金融業的應用，發展其減少可疑交易和降低交易成本的潛力。

透過對前述事件的觀察認識，吾人應可管窺全球主要金融機構或主管機關已認知到區塊鏈的重要性或致力於發展區塊鏈解決方案，希望實現跨銀行交易，相信區塊鏈技術將逐漸成為主流。加上全球金流的跨境發展與因此而來的競爭蔚為趨勢，台灣的金融業者在這領域更不能缺席，也更突顯本研究議題之重要性。我們希望本研究能有效幫助國內金融業掌控區塊鏈此一新科技的發展與應用。

第二節 研究目的與方法

一、研究目的

顯而易見，我國金融業已無法自外於科技金融方興未艾的創新浪潮，

務須迎頭趕上。區塊鏈技術被認為是科技金融中的新顯學，本研究之主要目的，即在於針對區塊鏈技術進行初步的介紹，在具備區塊鏈的基礎概念之後，再檢視其他國家應用區塊鏈技術於金融業的實例，並探討我國金融業是否能從這些案例中得到啟發。具體而言，我們預期本研究能完成下述工作：

第一，闡明區塊鏈技術的內涵。

第二，剖析全球主要國家金融業應用區塊鏈技術的現況。

第三，省思區塊鏈技術的應用如何為我國金融業帶來突破。

二、研究方法

本研究主要將採取以下方法進行研究：

(一)文獻分析法

蒐集我國及各相關國家或地區之區塊鏈發展現況報導、文獻、政府及企業公開資訊發布、統計資料。並參酌國內外學者專家之論著、報章雜誌、相關主題之座談會或研討會之資料及專家意見，輔以台灣及各國相關法令與文獻，進行綜合歸納、分析與比較。

(二)訪談提問法

針對本研究下之各章節主題，提出理論與實務上所可能面對之問題，透過專家訪談、實地調查等，綜合主管機關、相關部會及金融界之意見，嘗試尋求妥適之因應對策。必要時，考慮提出修法建議或配套措施，並具體提出金融業未來應用區塊鏈之可能趨勢及發展方向。

第二章 區塊鏈的緣起與技術發展

第一節 區塊鏈的緣起—兼談數位貨幣

金融危機爆發之後不久，大約就在雷曼兄弟倒閉的一個月後，2008 年 10 月 31 日下午 2 時 10 分(紐約時間)，中本聰(化名，真實身分成謎)在一個隱秘的密碼學討論群組上發表了一篇論文《比特幣：一種點對點的電子現金系統》(Bitcion：A Peer-to-Peer Electronic Cash System)，闡述了基於 P2P 和加密等技術的電子現金系統架構理念，此即「比特幣」(Bitcion)系統的基本框架。

中本聰如此寫道[2]：「我一直在研究一種新的電子現金系統，完全是點對點(peer-to-peer)，不須透過受信任的第三方…我們將電子貨幣定義為一連串的數位簽名。每個擁有人把貨幣轉移給下一個人，是將先前的交易和下一個擁有者的公鑰(public key)數位簽署為雜湊值(hash)，並將這些加到貨幣的最尾端。受款人可以透過驗證簽名來驗證所有權鏈。」

中本聰描述的線上交換系統，是利用電腦加密讓雙方進行價值交換，但不會洩漏交易雙方的身分或金融帳號等敏感資料。這個系統的主要用意，是要在傳統的金融體系之外運作，讓人們可以直接寄送數位貨幣給彼此。「點對點」就是免除中間人的商務往來概念，不需要銀行或信用卡公司，不會牽涉到支付服務商，或是其他「受信任」的第三方。

就數位貨幣與實體經濟之關係而言，數位貨幣可分為三類[3]：第一類是封閉之數位貨幣體系，主要應用於網路遊戲(如虛擬道具及裝備之購買)；第二類數位貨幣係單向之資金流動，通常對數位貨幣之購買已有兌換比率，主要應用於虛擬商品與服務之購買；第三類數位貨幣則有著雙向之資金流動，在該情況下之數位貨幣與中央銀行發行之貨幣已無實質區別，可用於

[2] 譯文摘自「虛擬貨幣革命」(2016)，保羅威格納、參克凱西著，林奕伶譯，大牌出版/遠足文化事業有限公司。

[3] 許榮、劉洋、文武健與徐昭(2014)，互聯網金融的潛在風險研究，金融監管研究，第 27 期，頁 40-56。

真實商品與服務之購買，中本聰的比特幣即是第三類數位貨幣之典型代表。

中本聰的比特幣系統最重要的創新，是一個不容破壞的共同總帳，他稱其為「區塊鏈」(Blockchain)，任何人可以用來驗證交易的有效性；事實上，區塊鏈可以簡單的定義成一個系統，它讓一群互聯的電腦安全的共同維護一份帳本。中本聰還設計了一套獨特的獎勵機制，鼓勵網絡裡的電腦擁有人維護更新總帳，以便維持系統誠實可信，同時擊退駭客。

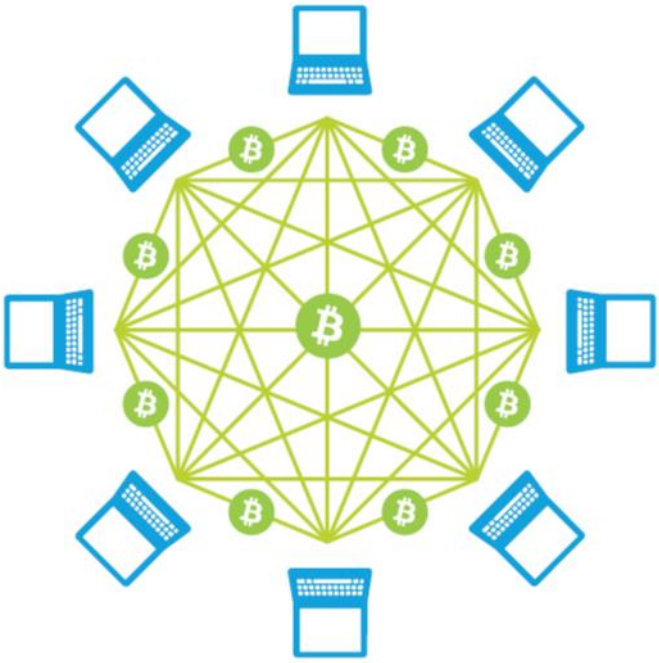
另外為了應付比特幣體系通貨膨脹，或比特幣貶值的疑慮，中本聰制定了一套比特幣的貨幣供給機制。最初四年，通訊協定設定大約每十分鐘固定發出五十枚比特幣。到了 2012 年底時，發行的數量就降為二十五枚，之後每四年減半，直到供應量在 2140 年減少至零為止，屆時總計將發出兩千一百萬枚硬幣。這樣預先設定逐步遞減、釋出數量有限的貨幣供給，能製造稀缺感，為比特幣的價格建立支撐基礎。

2009 年 1 月 3 日，中本聰建立了序號為 0 的第一個比特幣區塊(俗稱創世區塊(Genesis Block))，「挖掘」出第一批的比特幣五十枚，不過當時這些比特幣的價值還是零，因為沒有別人可以轉移，也就是沒有地方可供花用。幾天後，中本聰在密碼學討論群組上再次宣告：「宣布首次釋出比特幣，一個新的電子現金系統，使用點對點網絡以避免重複支用(double-spending)，完全去中心化，沒有伺服器或中央管理機構。」就在 1 月 9 日，出現序號為 1 的區塊，並與序號為 0 的創世區塊相連接，「區塊鏈」於焉誕生。

區塊鏈其實就是支撐比特幣系統運作的底層技術。比特幣的區塊鏈總帳是一長串的區塊，是大約同時間發生的交易群組。只要系統持續運轉，這個鏈便無限制增長。這種依照時間先後排列順序的結構非常重要，因其賦與較早的交易合法性，使用者若企圖重複使用同樣的比特幣餘額，會被視為不合法。藉由將比特幣體系內每個參與者的花費與收入，建立有時間

印記的順序，系統便可追蹤紀錄任何時刻每個人的餘額狀況，以及附屬在每一枚比特幣創造、花用、或收入的識別資訊。

一般來說，區塊鏈是指通過去中心化的方式集體維護一個可靠資料庫的技術方案。該技術方案讓參與系統中的任意多個節點，把一段時間中系統內全部資訊交流的資料，通過密碼學演算法計算並記錄到一個資料塊（block），並且生成該資料塊的「指紋」用於鏈結（chain）下個資料塊和校驗，由系統所有參與節點來共同認定記錄是否為真。



【圖 2-1-1】區塊鏈金融示意圖(資料來源：Deloitte)

在比特幣的應用中，區塊鏈是一個分散式的帳本系統，採用密碼技術來確保交易的正確性，不同的區塊鏈技術採用不同的共識機制。最早使用區塊鏈這個技術的例子即是比特幣的交易系統，比特幣參與者們集體維護一個具時序性的帳本系統(區塊鏈)。其中的每一個區塊網路之參與者都是一個節點，一套完整的帳本因為這些節點而得以保存，帳本中記錄了所有的歷史帳戶訊息，任何一個節點需要發起一個交易行為都需要將交易行為訊息傳遞到區塊網路中的其他每一個節點，如此可以確保此保存於所有節

點上的帳本能精確的更新且驗證這一筆交易行為。

最古老的區塊鏈共識機制是由一種稱為挖礦的過程產生，目的是決定記帳權共識：確認交易並把交易納入區塊鏈之中。挖礦能確保區塊鏈時間順序的正確性，保護網路的中立性。有待確認的交易資料會被打包至某個區塊之中，而為了防止區塊被惡意篡改，區塊必須滿足一項非常嚴格的密碼學規則，隨意篡改的區塊會因為不符規則變得無效，藉由這個機制，沒有一個人能控制區塊鏈中能包含哪些交易，或是任意更動區塊鏈的某一部份。

在一筆交易中，我們只會看到收款對象的位址，一個收款者能夠擁有不只一個位址，也就是說，位址與收款者並無法做到準確的對應。每筆交易的付款與收款對象均可以有一個或多個，由於我們無法得知這些對象實際上是否為同一人，故能達成基本的匿名性。相對於傳統中心化機構的會員申請，要產生一個位址是相對容易很多的，只要符合一定的格式，都會被網路所接受。位址的產生，是私鑰透過一連串的雜湊函數(Hash Function)產生，接下來我們將對私鑰(private key)、公鑰(public key)和位址 (address)的產生方式概略說明[4]，詳細的介紹可參見下一節。

私鑰可以用來管控相對位址的所有資產，從資產的傳送到交換，都需要用私鑰來簽名認證。私鑰基本上可以寫作 256 位元的二進位數，所有符合此一格式的私鑰約有 2 的 256 次方個，寫成十進位的話有足足 78 位數，所以只要隨機程度足夠，是非常不容易跟別人相同的。要產生一個隨機程度足夠的私鑰，最簡單的方法是投擲一枚硬幣，正面取 1，反面取 0，這樣一直投擲 256 次，就會得到一組跟其他人不一樣的私鑰。從私鑰到位址的過程中，私鑰會先透過一個橢圓曲線加密的對應函數得到一個長度為 512 位元的公鑰，橢圓曲線加密的數學式在此不予贅述。

公鑰最主要的功能，為驗證財產的擁有權。每筆交易中需要轉出任一

[4] 摘錄自廖世偉(2016)，區塊鏈不等於比特幣。

財產的時候，須提出公鑰以認證該財產擁有權，並以私鑰對整筆交易簽名認證，用以確定財產擁有者同意此一財產的轉出。當礦工在驗證交易時，會檢查該公鑰是否配對於該財產，也即要能與該資產的位址對應，並同時檢查此一簽名是否屬於該擁有者。雖然私鑰僅能單向轉換成公鑰，一般還是希望公鑰盡可能不要太常出現在公開的區塊鏈上。在轉出財產的時候一定需要公鑰來驗證，所以通常只保護收入端所顯示的公鑰。在收入財產的部分，會再對公鑰做一層的雜湊函數，用以保護公鑰，此一雜湊函數的輸出即為位址。

透過由演算法 SHA-256 與 RIPEMD160 所組成的雜湊函數，一個 512 位元的公鑰將會先由此雜湊函數轉換為 160 位元後，再編碼為位址，因此轉換途徑依序為私鑰、公鑰以及位址，僅由後者是難以回推出前者的。此位址可用於收取別人轉交的財產，而擁有此位址相對應的公鑰與私鑰，便可以再把裡頭的財產轉出。

區塊鏈的核心思想是去中心化。資料的傳輸不再依賴某個中心節點，而是 P2P 的直接傳輸。全網路的每個節點都依據共識開源協定，自由安全的傳輸資料。所有交易記錄是對全網路公開的，每個節點都可備份。

區塊鏈最大的革命性創舉在於信用的建立。在我們日常的社會活動中，信用的建立往往需要依靠第三方機構的證明，這種方式通常會增加交易的成本，降低效率。區塊鏈系統本身能產生信用，這種信用的產生不是來自第三方機構，而是來自程式（演算法），因為區塊鏈記錄資訊的產生是需要全網路節點確認的，一旦生成將永久記錄，無法篡改。除非能擁有全網路總算力的 51%才有可能修改最新生成的一個區塊記錄。

雖然區塊鏈技術最早是由於比特幣的流通為人們所認知，但是區塊鏈的應用卻不僅於此。過去幾年比特幣與其他使用區塊鏈技術的虛擬貨幣 (統稱為 Altcoins) 的發展熱潮逐漸消退，市場也開始發覺區塊鏈的真實價值遠遠不僅止於促成一個無政府虛擬貨幣的流通。北美與歐洲的投資人、

科技新創、金融機構以及政策制定者目前關注的方向已經從比特幣轉移到區塊鏈技術與既有產業生態的連結。

網際網路已經實現了資訊的自由傳遞,但是價值的自由傳遞尚未實現。下一步的可能發展是將資產數位化，在互聯網上登記各類權益資產，實現權益資產的自由流通。與資訊的可複製有所區別，權益資產對應的價值是不可複製的，其傳輸方式顯然與資訊不同，區塊鏈技術有望說明我們實現從資訊網路到價值網路的轉變。

首先，密碼學技術的運用可以低成本的解決資料傳輸的安全性問題，公私密金鑰已經是現代密碼學中一項成熟的技術，能確保傳輸資料本身及發送物件接受的準確性，防止資料被盜取或篡改。另外，使用雜湊值演算法能高效的完成資訊驗證。

其次，P2P 技術大幅降低對單個節點的依賴性，提高了整個網路的可靠性。某些節點的退出不會對整個系統的運作造成影響，不需要建設過於複雜的伺服器組，一般伺服器即可運作，系統維護更加靈活。

最後，權益資產在實現自由流通的同時需要記帳，而區塊鏈本身就具備帳本的功能，通過時間序列化的區塊記錄每一筆發生過的交易，公開透明，可追溯驗證，不可篡改，使資訊查核變得簡便。這些特性進一步擴展了區塊鏈的應用範圍。

第二節 區塊鏈技術初探

比特幣在數位貨幣的譜系中，隸屬於「加密貨幣」 (cryptocurrency)，支撐比特幣的核心技術「區塊鏈」，便構築於密碼學(cryptography)之上。

一、(非對稱)公鑰密碼學簡介

密碼的使用，在凱薩大帝的時代就已有跡可循，當時採用了現在稱為「位移密碼」(shift cipher)的密碼術。舉例來說，假設我想傳送 CAT 這個單字，我就先把二十六個英文字母平移，譬如左移五個位置，對應如下表所示：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

上表中第一列代表原來(平移前)的字母排序，第二列代表平移後的字母排序。現在我依據上表，第一列的 C 對應第二列的 H，第一列的 A 對應第二列的 F，第一列的 T 對應第二列的 Y，因而可將 CAT 轉換為 HFY，然後將 HFY 寄發給我欲傳送的對象。這裡的 CAT 稱為明文(plaintext)，HFY 稱為密文(ciphertext)，「英文字母左移五個位置」是我的「加密鑰匙」。收到密文的人，只要知道我是依據上表將明文加密，便可同樣依據上表解密，只要將密文中的字母從第二列對應到第一列，便可輕易回推出明文。將「英文字母右移五個位置」就是「解密鑰匙」。在位移密碼的例子中，很容易可看出「加密鑰匙」和「解密鑰匙」是對稱的，我們甚至可以說，位移密碼的「加密鑰匙」和「解密鑰匙」本質上是同一把，只不過要朝相反方向「轉動」。

密碼術的出現雖早，然而自凱薩大帝以降的兩千多年，密碼學面臨的困境始終如一：如何安全無虞的發送解密鑰匙給密碼傳送對象？

假設現在有兩位情治工作人員：韓特與慕德。慕德急於傳遞 CAT 這個訊息以告知韓特，有外星人偽裝成貓咪混進了他們的國家。慕德可以先將 CAT 轉換成密文，但要讓韓特看懂密文，就必須讓韓特知道解密鑰匙[5]，可是慕德要如何將解密鑰匙交給韓特，同時不讓外星人或其他國家的人有機會竊取呢？

慕德可以將解密鑰匙放在堅固的小型保險箱裡寄去給韓特，然而這個保險箱的鑰匙必須放在另一個保險箱裡寄去給韓特，那另一個保險箱的鑰匙又必須再找一個保險箱...如此下去沒完沒了。或者，他們兩人可以約在紐約市曼哈頓 125 街的麥當勞見面並交付解密鑰匙，不過要是他們可以這麼做，那也不必使用密碼傳遞訊息了，畢竟當面討論外星人的陰謀應該更為清楚省力。

此處真正要處理的問題，是如何讓素未謀面的兩人，透過密碼安全的傳遞訊息。

在西元 1976 年以前，「解密鑰匙如何安全發送」被公認是密碼學中無解的難題，直到 Whitfield Diffie 與他當時在美國史丹福大學的同事 Martin Hellman 合作，終於跳脫既有的窠臼，對這個問題做出劃時代的貢獻[6]。Diffie 與 Hellman 的關鍵想法，在於找出一個「單向函數」(one-way function)。所謂「單向函數」，在這裡可以想像成一種運算或是一種操作，這種操作具有某種程度的「不可逆性」，例如將黑色顏料與白色顏料混合成灰色顏料很容易，但反過來要從灰色顏料中分離出黑色顏料與白色顏料，卻是非常困難的事[7]。在某種意義上，Diffie 與 Hellman 繞過解密鑰匙的發送過程，建構出一種新的鑰匙交換系統，他們提出公鑰密碼的想法，成為公鑰密碼學(public-key cryptography)的濫觴(事實上他們還一併處理了看似毫不相關

[5] 以位移密碼的例子來說，就是要讓韓特知道英文字母應該向哪個方向平移多少位置。

[6] Diffie, W. and M. Hellman (1976), "New Directions in Cryptography", *IEEE Transactions on Information Theory*, 22, (6), pp. 644-654。兩位作者憑藉其在密碼學領域的貢獻，於 2015 年獲得有「電腦科學界的諾貝爾獎」之稱的「涂林獎」(Turing Award)。涂林(A. Turing)是英國科學家，近代電腦科學的先驅之一。

[7] 較為形式化的說法是這樣的：函數 f 對於給定的數據 a，可以輕易算出 y=f(a)，但根據給定的 b，卻很難倒過來求得 x 使得 b=f(x)，同時也很難找到相異的 a_1 與 a_2 使得 $f(a_1)=f(a_2)$，這樣的函數 f 就是一種單向函數。

的數位簽署(digital signature)問題，我們會於稍後說明) ，不過在當時這是一種完美但不可行的構想。

Diffie and Hellman (1976) 在概念上邁出巨大的一步，但實際應用時居於關鍵地位的單向函數，一時卻未能發現(1976 年的文章中提出三個單向函數候選者，稍後皆證明不堪使用)。當他們在美國西岸繼續埋頭鑽研時，位於美國東岸的應用數學與電腦科學重鎮—麻省理工學院卻率先傳出好消息，任職於此的三位學者 Ronald Rivest，Adi Shamir 與 Leonard Adleman 拔得頭籌[8]，找到了一個合用的單向函數：因數分解。依三人的姓氏縮寫，密碼學中將他們的方法稱為 RSA 演算法。

接下來我們說明 RSA 公鑰密碼演算法的操作步驟。首先我們令數字 01 代表英文字母 A，數字 02 代表英文字母 B…數字 26 代表英文字母 Z。舉例來說，如果我們要傳遞的訊息是 CAT 這個單字，則可數位化為 30120。

現在慕德要傳遞訊息給韓特，步驟如下。(每一步驟後方的括弧內容是對應該步驟的具體範例，為了說明簡便，假設要傳遞的訊息是 T 這個字母，數位化後就是 20。)

準備工作：

一、韓特隨機選取兩個相異(大)質數[9] p 與 q，並將此二數相乘得 $n=pq$。

(取 p=3，q=23，則 n=69)

二、韓特任意選取一個數字 e，但 e 必須與乘積 $(p-1)(q-1)$ 互質[10]，e 稱為「加密次冪」。韓特將 n 與 e 的值(公開)傳送給慕德。($(p-1)(q-1)$=44，e 的選擇不只一種，此處我們取 e=9)

[8] Rivest, R., A. Shamir, and L. Adleman, (1978), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, 21, pp. 120-126。三位作者因為提出此一公鑰密碼演算法，於 2002 年獲得「涂林獎」。

[9] 所謂質數，是指因數只有 1 與本身的整數。2 是最小的正質數，也是唯一的正偶質數。

[10] 兩數互質意味此兩數的最大公因數是 1，例如 15 與 22 互質，但 15 與 12 不互質。此處要求 e 必須與 $(p-1)(q-1)$ 互質，是為了確保在後續步驟 4 中一定能找到「解密鑰匙」d。

慕德加密：

三、慕德依據 n 與 e 的值將數位化信息明文 m 轉化成密文 c，此處 c 是m^e除以 n 的餘數[11]。慕德將密文 c (公開)傳送給韓特。

（英文字母 T 之數位化明文 m=20，$e = 9$，$m^e = 20^9 = 512000000000$，

$n = 69$，$512000000000 \div 69 = 7420289855 \cdots \mathbf{5}$，所以密文$c = 5$。）

韓特解密：

四、韓特根據(僅有他自己知道的)p 和 q 之值，計算出(p-1)(q-1)的值，並據此求算「解密鑰匙」d，這裡的 d 是一個正整數，且會使得 d 與 e 的乘積 de 除以(p-1)(q-1)的餘數為 1[12]，或者說 de 減 1 之後可被(p-1)(q-1)整除，即 $de - 1 = (p-1)(q-1)k$，k 為正整數。

(已知 p=3，q=23，(p-1)(q-1)=44，e=9，尋找正整數 d 使得$9d - 1 = 44k$，可解出一組解 k=1，d=5。)

五、韓特將密文 c 取 d 次冪，也就是計算c^d，接著再計算c^d除以 n 的餘數，便可將明文 m 還原[13]。

(c=5，d=5，$c^d = 5^5 = 3125$；n=69，$3125 \div 69 = 45 \cdots \mathbf{20}$，所以 m=20。)

上述 RSA 公鑰密碼演算法的操作步驟，有幾處尚須略作說明。首先注意到韓特所選取之 n 與 e 的值，是加密與解密的必要資訊，但可透過公開途徑傳遞(例如登在報紙上或貼在網頁上)，因此數對(n,e)稱為韓特的「公鑰」(public-key)；但 p 和 q 的值只有韓特自己知道，因此數對(p,q)稱為韓特的「私鑰」(private-key)。此處必須強調：公鑰和私鑰是成對生成的。

慕德接收了韓特的公鑰之後，便據此將其所要傳遞之訊息由明文 m 轉

[11] 數學式可表示為 $c \equiv m^e (mod\ n)$ 或 $c = \mathrm{mod}(m^e, n)$，其中 a ≡ b (mod n) 讀做「模 n 之下，a 同餘 b」，其涵義為「『a 除以 n 的餘數』與『b 除以 n 的餘數』相同」，或者說「n 可以整除(a-b)」，亦即「n 是(a-b)的因數」。符號 mod(a,b) 代表 a 除以 b 的餘數。

[12] 以數學式表之即為 $de \equiv 1\ (mod\ (p-1)(q-1))$。

[13] 數學式可表示為 $m \equiv c^d (mod\ n)$，或 $m = \mathrm{mod}(c^d, n)$。

換為密文 c，也就是「以公鑰加密」，再透過公開途徑將密文 c 傳遞給韓特。韓特再以其私鑰解密，將密文 c 還原出明文 m。一個關鍵的問題是，步驟四中利用私鑰(p,q)找到的「解密鑰匙」d，是否真能保證在步驟五中將密文 c 還原出正確的明文 m？答案是肯定的。不過若要對此一事實給出嚴謹的證明，需要動用初等數論中的工具，例如費馬小定理，由於牽涉到較多技術上的細節，此處不擬詳述[14]。

另外一個不可忽視的議題，在於 RSA 公鑰密碼演算法的安全性。假設現在神盾局也意圖解譯出明文 m，其所能獲取的資訊包括公鑰 n、e 與密文 c，請問是否足以成事？

破解密文的關鍵，顯然在於能否找出演算法步驟四中的「解密鑰匙」d，而為了找到解密鑰匙，神盾局必須知道 p 與 q，換句話說，必須將 n 做因數分解。範例中 n=69，很容易看出$69 = 3 \times 23$。倘若韓特選取的 p 與 q 非常大，使因數分解 n 所需的時間足夠長，長到超過密碼訊息的時效性，則這樣的密碼傳遞即可視為安全的。

例如 1977 年時，科學美國人雜誌(Scientific American)的數學遊戲專欄在介紹了 RSA 演算法後，向讀者提出一項挑戰：請依據公鑰(n,e)解譯密文 c，其中

n =

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541；

e = 9007；

c =

[14] 密碼學的基礎與數論息息相關，不少密碼學家也同時身兼數論學者。有興趣深入密碼學領域的讀者，可參閱 Koblitz(1994)，Hoffstein, Pipher, and Silverman (2014)，Parr and Pelzl (2010)，其中 Parr and Pelzl (2010)是極佳的密碼學入門書籍，Hoffstein, Pipher, and Silverman (2014)用到的數學較多，Koblitz(1994)則是一本經典之作。

96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154；

以 1977 年時的知識與技術水準，估計因數分解 n 需要 40000000000000000 年的時間才能完成，因此該專欄提供美金 100 元給任何 1982 年 4 月 1 日前破解密文的人，應該頗為安全。由於因數分解技巧與電腦科技的精進超出預期，密碼在 17 年後的 1994 年遭到破解，解密的過程共花了七個月，將這個 129 位數分解為

p =

3490529510847650949147849619903898133417764638493387843990820577；

q =

327691329932667095499619881908344614131776429679929425397982885 33；

最後得到明文訊息

m =

200805001301070903002315180419000118050019172105011309190800151919090618010705；

轉譯成英文(其中 00=空白)就是

the magic words are squeamish ossifrage

在這裡對傳統密碼術與現代密碼術稍事整理以資比較。傳統的密碼術是這樣的：一、加密方選擇某一種加密規則，對資訊加密；二、解密方使用同一種規則，對資訊解密。現代的非對稱密碼術其方法則是：一、解密方生成一對密鑰，即公鑰和私鑰，公鑰可以公開，私鑰則須保密；二、加密方獲取解密方的公鑰，利用公鑰為資訊加密；三、解密方得到加密的資訊後，利用私鑰解密。

接下來我們要介紹，對於在匿名網路上傳遞訊息極為重要的數位簽署。上例中由慕德以公鑰加密，再由韓特以私鑰解密的過程，其實可以逆轉，也就是由韓特先以私鑰加密，再由慕德以公鑰解密。這個 RSA 演算法的逆過程，為數位簽署的問題提供了解答。

數位簽署遭遇的主要困難，在於簽名的「不可複製性」難以解決。讓我們暫時換個場景，現在假設韓特必須確認某一情報的真(T)偽(F)回覆慕德，如果慕德收到的訊息是「T」，他如何確定這個訊息是由韓特所發出，而不是由敵人所偽發的假訊息？倘若他們之間用傳統的紙筆溝通，則韓特可在信紙上簽名。簽名當然有被偽造的可能，而當訊息以數位傳輸時這個問題更大。一個解決方法是這樣的：韓特先以私鑰將訊息明文「T」加密成「簽署文」，然後將明文與簽署文同時發送給慕德，慕德依據公鑰解密簽署文，如果解密的結果與明文一致，則慕德可相信這則訊息是由韓特所發。這裡看不到真正的「簽名」，數位簽署演算法中的「不可複製性」完全彰顯在單向函數的逆方向。

這裡稍微做個歸納。如果韓特要發出一個訊息給慕德，他希望讓慕德確認這條訊息是自己發出的，但又不想讓第三人得知訊息的內容，則韓特的可行作法如下：首先，韓特先用自己的私鑰替訊息做第一層加密；接著，韓特對經過第一層加密的訊息用慕德的公鑰做第二層加密。第一層加密的目的是證明這個訊息確實是韓特發出的，因為只有韓特的私鑰能完成這樣的加密；第二層加密的目的是確保訊息只有慕德讀得到，因為只有慕德的私鑰能為第二層解密。慕德收到密文後，以相反的順序做兩次解密即可：先用自己的私鑰解密收到的資訊，然後用韓特的公鑰再解密一次。有了這樣的技術保障，即使在匿名的網路環境中，也不必再顧慮通訊的安全性。

最後要補充說明的是，RSA 演算法選取的單向函數是(大整數的)因數分解，隨著公鑰密碼學的發展，其他單項函數次第出現。目前以橢圓曲線

密碼術[15](Elliptic Curve Cryptography, ECC)安全性較高，其單向函數由橢圓曲線而來，這是數論中一個歷史悠久的分支。ECC 的主要優勢，是在某些情況下比其他方法(例如 RSA)使用更小的密鑰就能提供相當等級的安全性。依據美國國家標準與技術局的設定，對於最小密鑰長度的要求，RSA 是 1024 位，ECC 只需 160 位。著名的比特幣也是以 ECC 技術加密。

二、公鑰密碼學在區塊鏈的應用

接下來我們以比特幣為例，說明區塊鏈的運作，並可看出公鑰密碼學居中扮演的角色。

首次使用比特幣時須先下載用戶端，可選擇不同種類的錢包軟體，安裝後首次運行時，需要花費一段較長時間進行資料同步，此時會下載比特幣有史以來的所有交易紀錄。資料同步完畢後，「餘額」和「未確認」項顯示的就是最新資料。切換到「接收」功能表，會看到軟體自動生成的一個位址，看起來像一長串亂碼般的字元，這就是「收款帳號」。每個比特幣位址的金額及其變化是公開的，也就是每個用戶端都可以看到，因此如果希望保密或區分不同的付款人，可以為每個人甚至每筆交易單獨生成一個位址並提供給對方。每個人可以為自己創建任意數量的帳戶。

比特幣的位址與一般的銀行帳號有什麼不同呢？事實上，比特幣位址就是以非對稱密碼技術產生的公鑰，而和公鑰對應的私鑰就藏在錢包檔裡。因為公鑰和私鑰必須成對生成，所以比特幣位址無法任意設定。依據公鑰公開、私鑰保密的原理，比特幣位址可以公告周知，但錢包檔則須妥善保管。

比特幣體系不存在現金，所有的價值轉移都需透過帳戶進行，因此比特幣的支付概念類似於銀行轉帳，可是比特幣體系中又不存在任何類似金融機構的角色，如何建立「信任」就成了問題。比特幣體系對此問題的解

[15] 可參閱 Koblitz(1994)或 Washington(2008)，Koblitz 本人即是橢圓曲線密碼術的發明者。

決方法是這樣的：假設韓特要轉帳給慕德一個比特幣，韓特便寫下一則聲明，表示從其位址轉帳一個比特幣到慕德的位址，然後用自己錢包檔裡的私鑰加密，再將加密後的訊息傳播到整個比特幣網路上。網路上的人都有韓特的位址(也就是韓特的公鑰)，因此任何人都可用其位址解密，驗證這條訊息確實是韓特所發出。接下來，透過歷史交易資料(每個人在下載用戶端時已將所有歷史交易資料同步，且之後會隨時間經過更新)可計算出韓特的位址確實擁有至少一個比特幣。於是整個比特幣網路公認此筆轉帳，韓特錢包中減少一個比特幣，慕德錢包中增加一個比特幣。而這筆交易稍後(大約十分鐘之內)也會加入比特幣的交易紀錄塊，成為歷史交易資料的一部分。

前段提到「整個比特幣網路公認此筆轉帳」，這件事的細節則牽涉到比特幣中「挖礦」的概念。比特幣的本質是一個公開的記帳系統，而挖礦的本質就是爭奪記帳權。挖礦的工作內容，就是將過去一段時間內發生、尚未經過網路公認的交易資訊蒐集、檢驗、確認，最後打包加密成為一個無法被竄改的交易紀錄塊，從而成為這個比特幣網路上公認已完成的交易紀錄，永久保存。從事挖礦工作者被暱稱為「礦工」。

當韓特指示錢包將一個比特幣轉帳給慕德時，他就同時向整個網絡廣播這筆待完成交易，並附上許多重要資訊，包括雙方指定的錢包位址、日期與時間印記、以及其他訊息。每個挖礦節點(也就是電腦)的礦工都在蒐集這類資訊，並壓縮成一加密字串，稱為「雜湊」(hash)，以便讓相對龐大的資訊量得以縮小。依使用的雜湊演算法不同，壓縮過程會產生不同的雜湊值。比特幣採用的演算法稱為 SHA-256，會產生總長六十四個取自數字及字母的字元。雜湊演算法可讓礦工將同時發生的交易湊在一起，首先礦工的軟體端接下第一筆交易的雜湊值(匯集包含在內的底層數據)，再結合下一筆尚未雜湊化的原始交易資料，形成新的雜湊，這個雜湊值已包含兩筆交易了，然後第三筆原始交易資料，形成新的雜湊，以此類推，不斷將所有新進的資訊包裹成一個雜湊值，交易就是這樣被包裹到區塊鏈的關

鏈基礎成分—區塊的。

不斷包裹交易資訊的同時，電腦/礦工也在競爭記帳權，企圖搶先「密封」其中一個區塊，亦即將區塊嵌入區塊鏈總帳。競爭獲勝的關鍵在於計算力，必須快速算出新的可能區塊雜湊值，將所有數據抓到包裹一切的新區塊編碼，然後連結到前一區塊的區塊雜湊值。勝出的區塊雜湊值必須符合比特幣核心演算法判定為目前區塊的獲選號碼。獲勝的礦工可以獲得伴隨這些交易而產生的交易費用，外加一筆額外的報酬。交易費用一般都是轉出資金方提供給挖礦者的，因此不是系統新增的貨幣；額外的報酬是新生成的比特幣(這也是爭奪記帳權被稱為「挖礦」的理由)，這就是比特幣系統新增貨幣的方式[16]。

總的來說，區塊鏈中每一筆交易產生時，都需要原本的價值擁有者進行數位簽署認證這筆交易，驗證中的交易資料會被打包至區塊中，並透過雜湊演算法進行記錄。數位簽署讓交易產生了可驗證性，雜湊演算法則提升了交易的偽造難度，也成就了區塊鏈的安全基礎。

[16] 比特幣的數量控制機制與此額外報酬有關。依據比特幣系統的設置，大約每十分鐘可以產生一個交易紀錄塊，最初每生產一個交易紀錄塊可獲得五十個比特幣的額外報酬，但是該報酬每隔四年會減半，最終整個系統中頂多只會有兩千一百萬個比特幣。

第三節 區塊鏈的特色

區塊鏈的特色，包括「去中心化」、「加密安全性」、「不可竄改性」、「可追蹤性」等等，其中「去中心化」堪稱區塊鏈最為核心的特性。

簡述「去中心化」的意思，就是不存在主導一切的個人或機構，而是由集體參與者共享決定權。有別於過往常見的「伺服器架構」，所有資訊都儲存在伺服器上，使用者通過伺服器傳遞交流資訊，區塊鏈採取的是「P2P 架構」，或稱「點對點架構」。在 P2P 架構中，伺服器並非必要，透過網路連接的每部電腦都是獨立個體，稱為「節點」，某個節點發出的資訊可以被其他所有節點接收。

從「去中心化」衍生出的關鍵一點在於，整個系統裡沒有任何一個人擁有唯一決定權，這意味著沒有人可以單獨在這個系統中竄改帳簿或修改規則，因為個別的更動會被整個網路否決。除非能夠同時控制整個系統中超過 51%的節點(這在比特幣體系中稱為 51%攻擊)，否則單個節點上對資料庫的修改是無效的，也無法影響其他節點上的資料內容。因此雖然理論上可以更改資料，但在區塊鏈的環境下，交易一旦驗證確認完成後，數據篡改的難度和代價將會相當龐大，這也導致了區塊鏈的「不可竄改性」，從而提升交易資料的可信任度。

在比特幣的體系中，每個節點都掌握完整的帳本，因此每個節點都可以獨立統計出比特幣有史以來每個帳號的每一筆流動，也能算出每一個帳號當前的餘額是多少。區塊鏈將所有的交易紀錄存放在多個節點，去中心化的資料留存方式讓買賣雙方得以隨時追溯交易歷史，提升資訊透明度，降低偽幣流通的風險，這也就確保了區塊鏈上價值交換的「可追蹤性」。

在一般的商業銀行系統中，我們只知道自己的交易紀錄和帳戶餘額，而在區塊鏈網絡裡，每個人可以知道任何人的交易紀錄。比特幣是分散式系統，新的區塊將寫入分散式帳本，所有節點的帳本將同時更新，所有節

點依然共用完全一致的帳本。每個節點因預先設定的協議而生成，也是由協議約束而參與到執行環節，準確的承載著資料和資訊。在這個系統裡，若有任何事情發生錯誤，是沒有客服人員可以幫忙的。區塊鏈不是建構在信任情感上，其可靠性是透過特殊的數學函數和程式碼達到的，也就是所謂的「加密安全性」。

基於上述的這些特性，區塊鏈能夠解決的問題包括：第一、在大家互不相識的情況下建立信用機制；第二、改善中心化導致的非技術方面成本過高的缺點，包括管理成本、組織架構的佈建等；第三、能使資訊真實透明可追溯，便於核對與審計，可以提高效率，但同時保護客戶的隱私；第四、記錄有時間序列的資料，例如交易確認、版權登記等。

使用區塊鏈技術有幾個相當顯著的好處，例如在集中式的管理環境中，交易的正確性皆由中央控管單位負責，而在分散式帳本的去中心化環境下，區塊鏈讓每個擁有交易紀錄的節點，以多數決的方式取得資料正確性的共識。共識決機制牽涉到每個節點的存放資料，就結果而言降低了中央控管單位因資安事故導致金融詐欺事件的風險。

其他的優點還包括：使用者可完全控制自己的資產，沒有第三方機構組織保管或限制使用。交易成本非常低，讓小額支付(micropayments)得以實現。財產可以在幾分鐘內就完成轉移，交易紀錄可以在短時間內獲得保障。任何人可以在任何時間驗證每個交易紀錄，亦即區塊鏈具有高透明度。應用區塊鏈技術可以打造任何去中心化的應用軟體，它可以安全管理和傳送資料。

對於金融機構來說，區塊鏈至少帶來下列幾項商機。第一、數位貨幣：將可大幅降低銀行間清算、結算和法遵、審計成本，並催生更多創新應用場景。第二、跨境支付與結算：降低跨境支付與結算的交易成本，提供營利空間。第三、供應鏈金融：簡化、自動化流程，降低成本並優化客戶體驗。第四、證券發行與交易：取代人工作業、提升交易結算效率、重置融

資交易流程。

當然也有一些挑戰需要克服，例如交易紀錄都是匿名的，一方面雖然保障了用戶的隱私，另一方面卻使管制機構無法追蹤非法的交易行為。另外區塊鏈上的虛擬貨幣(例如比特幣)非常不穩定，在市場上不容易取得且需求劇烈變化，導致價格很容易受到虛擬貨幣市場的突發事件影響。

以目前的情況而言，區塊鏈技術還處於起步階段，但由於各方相繼投入大量資源研發此一新興技術，我們可以樂觀預期，接下來應該持續會有技術革新促使區塊鏈更為安全穩定。下一章我們先來檢視目前主要國家在區塊鏈技術發展與應用的現況。

第三章 區塊鏈在主要國家金融產業的運用經驗

如前面章節所述，區塊鏈概念原自密碼學，某種程度上代表以 P2P 為基礎的去中心化體系，正如一套中立的電腦系統般，能在安全的前提下自動化進行交易，創造可靠且不容易刪改的數位交易記錄，並提供稽核、監管和所有權轉移，可說是可程式化的金融服務。

雖說區塊鏈在 FinTech 領域相對而言是新技術，近兩年才在歐美與亞洲國家陸續出現在金融實務界之應用，或者正式宣示區塊鏈金融之重要性。然而，區塊鏈的技術或概念在數年前已透過比特幣的話題而逐漸廣為人知。早在 1998 年，Wei Dai 發表文章闡述一種具有匿名與分散式特點的電子現金系統，將其命名為「b-money」；2008 年 10 月中本聰（Satoshi Nakamoto，日本經常譯為中本哲史）在一個密碼學網站 metzdowd.com 的郵件組列表中發表一篇論文，描述如何建立一套去中心化的比特幣電子現金系統；到了 2009 年 1 月 3 日，中本聰開創比特幣 P2P 開源使用者群組之節點和雜湊函數(Hash Function，亦稱雜湊演算法)系統，其對等網路和第一個區塊鏈同時開始執行，同時也發行史上最早的 50 個比特幣。2012 年 10 月，BitPay 發行報告表示，已有超過一千家商家透過其支付系統來接受比特幣的付款。因此，稱呼比特幣是區塊鏈技術在金融支付領域最早的實際應用實不為過。

當然，除了比特幣外，區塊鏈概念近來在金融實務上已有不少應用，不少金融科技公司應運而生，諸如 Chain、Ripple 與 DAH(Digital Asset Holdings)等，並在各自領域有所擅場，且成功吸引許多創投基金、金融機構甚至老牌科技公司投入資金，例如 Andreessen Horowitz、花旗集團與 IBM 等，為簡化說明，茲將這些金融科技公司與其資金來源整理如【表 3-1】所示。

【表 3-1】區塊鏈技術公司與其主要投資資金來源

公司	主要業務	資金來源
Blockstream	區塊鏈與側鏈(Sidechain)開發	Reid Hoffman、Khosla Ventures、Real Ventures 等 40 家金融機構
Chain	區塊鏈底層技術、應用開發與諮詢	Khosla Ventures、RRE Ventures、Thrive Capital
Circle	數位貨幣發行技術支援、電子錢包應用	Breyer Capital、International Data Group (IDG)
DAH(Digital Asset Holdings)	基於區塊鏈的數位化證券發行與交易	Citigroup、CME Group、IBM、JP Morgan
Ripple	跨境支付與結算	Andreessen Horowitz、IDG

資料來源：麥肯錫、CrunchBase，本研究整理

區塊鏈發展技術並非僅是金融科技公司的事情，金融機構亦不可能讓金融科技公司專美於前。是以面對金融科技的潮流以及區塊鏈技術的創新發展，世界主要金融機構業已採取相應措施。然則各家採取的策略不一，根據麥肯錫 2016 年的報告，大致可歸類為以下三類：(一)聯合其他同業組建區塊鏈聯盟，制訂行業標準，例如 R3 CEV 集結超過 40 家跨國金融機構建立行業監管及相應的技術標準；(二)結合金融科技公司，發展核心業務的區塊鏈應用，諸如 Visa 及 Capital One 各自透過戰略投資金融科技公司，掌握區塊鏈技術帶來的業務機會;(三)銀行內部自行推動局部領域的應用，快速實施試驗計畫，例如 UBS、花旗集團、德意志銀行、法國巴黎銀行與英國巴克萊銀行皆自行設立區塊鏈實驗室，研發或透過與金融科技公司的合作，針對不同的應用環境進行測試。

話說回頭，就地域別觀察目前全球的區塊鏈發展狀況，區塊鏈投資主要集中在北美、歐洲，台灣所在的亞洲則排名第三，並且以新加坡、日本

與中國大陸為主。為供國內金融業者與主管機關借鏡參考，本研究特別蒐集相關重要發展案例於本章。

第一節 區塊鏈在歐洲金融業之發展與應用

區塊鏈技術在歐洲金融業的發展可說相當蓬勃，除了商業銀行業者外，保險公司、外匯交易商，甚至中央銀行都投入發展，值得我們參考。

一、瑞士銀行等

瑞士銀行（UBS）在區塊鏈的發展可說是歐洲銀行業的先行者之一，該行於倫敦成立「Crypto 2.0」團隊，從事區塊鏈技術研究，宣稱已經開發出區塊鏈技術在 20 多種用途上，並開發出「智慧債券」(Smart Bond)。此外，該行除了在倫敦自行設立實驗室研究開發區塊鏈技術外，也聯合德意志銀行(Deutsche Bank)、西班牙桑坦德銀行（Banco Santander）與紐約梅隆銀行（BNY Mellon）等其他三家大銀行籌組聯盟開發新數位貨幣，期盼未來將成為業界標準，金融業者可藉由區塊鏈技術進行交易清算與交割，並擬向多國央行推廣此構想，目標在 2018 年初進入商業市場。

本次率先開發的「結算專用幣」（Utility Settlement Coin）的瑞士銀行，聯手三大銀行與同樣位於歐洲的電子經紀商毅聯匯業(ICAP)，共同發展數位貨幣系統，這也是銀行業在區塊鏈技術最具體合作案例之一，主要意義在於大型銀行首次聯手就一種具體的區塊鏈技術進行合作，以充分利用分散化的計算機網絡的威力，提高金融市場運作效率。結算專用幣係基於由 Clearmatics Technologies 研發的一種解決方案，可讓金融機構購買債券、股票等證券，無須等待轉帳程式完成，反之可直接在央行將數位貨幣轉換為現金，節省交易後清算交割的時間與成本。

對此，合作方之一的桑坦德銀行研發與創新部門主管 Julio Faura 表示，「目前銀行與機構之間的交易流程不但困難、耗時且耗費成本，這也是我們都擁有龐大內勤辦公室的原因」。他認為，最新技術可簡化流程與提高

效率。該行曾公開表示如果全世界的銀行內部若都使用區塊鏈技術，到2020 年每年約省下 200 億美元的成本。

UBS 金融科技創新部門主管 Hyder Jaffrey 指出，專案團隊擬於 2017 年尋求監管機關和央行的許可，目標是在 2018 年初在有限度且低風險的前提下導入商業使用。

二、德國安聯集團

德國保險業巨擘安聯（Allianz）宣布成功運用基於區塊鏈的智慧合約處理巨災互換和債券交易[17]，並認為該技術能夠促進金融工具的市場化。該公司之所以導入此一技術，係因為重大災害之後保險公司和投資者之間的理賠申請往往拖延數週甚至數月，而使用智慧合約技術可能將流程縮短到數小時之內。安聯此次的導入是結合投資管理公司 Nephila 合作進行技術測試，顯示用區塊鏈智慧合約可以顯著加速和簡化保險公司與投資者之間的交易處理和資金結算。此外，Nephila 指出該技術測試的其他好處，包括增加掉期的市場化和把智慧合約用於其他保險交易的機會。除此之外，安聯風險轉移（Risk Transfer）部門的首席保險長 Richard Boyd 表示：「區塊鏈技術可以增加巨災互換和巨災債券的可靠性、可控性、速度，因為它減少了中間商確定投資者交易和支付合法性過程中的手動操作、驗證、審核」。安聯此舉的主要目的正是在於透過替換存在於全部流程的手動操作，避免延遲和人為錯誤風險。此一案例的重要意義和啟發在於安聯是近幾個月內宣布探索區塊鏈技術的國際大型保險公司。

三、荷蘭中央銀行與銀行業者的努力

荷蘭中央銀行（De Nederlandsche Bank，DNB）在區塊鏈的潮流中也不缺席，已經加入區塊鏈的布局之中。該行在年報上宣布要發展屬於自己

[17] 巨災互換（Catastrophe Swap，CAT swaps）和債券是一種交易工具，能讓保險公司按照預先約定的觸發條件規避重大災難造成的潛在損失。

版本的數位貨幣--DNBcoin。除發行數位貨幣 DNBcoin 外，荷蘭央行也直接參與區塊鏈的研發，還自行成立工作小組，推動幾起大型區塊鏈實驗。另外，荷蘭央行也於 2016 年 9 月成立區塊鏈園區。

除了荷蘭中央銀行外，民營的荷蘭銀行（ABN Amro）本身除了是 Linux 基金會領導的 Hyperledger 專案聯盟以及 R3 聯盟的成員，也是區塊鏈金融科技公司 DAH 的投資者，該公司已宣布與位於南荷蘭的代爾夫特理工大學合作，將在該大學的區塊鏈實驗室內共同開發應用程式。雙方公開表示，他們的目標是希望能夠創建可靠且適當地處理大量數據和大量用戶的系統，並著眼於在未來六個月內創建工作應用程式。此外，荷蘭銀行員工將參加該大學舉辦的研討會和講習班，以便促進銀行工作人員對區塊鏈技術的認知。

除了前述案例外，德國的德意志銀行及英國的巴克萊銀行也都自行成立區塊鏈實驗室，自行研發或透過金融科技公司的協助，針對不同的業務應用場景進行研發探索。在世界上所有央行之中，英國央行(Bank of England)可說是相當積極進行區塊鏈技術的研究與探索。為了維護英國金融系統穩定，即時支付結算系統是提供英國央行英鎊儲備的平台，為銀行間交易提供安全的最終結算手段，2016 年英國央行正在計劃創造未來新一代即時(Real-time)支付清算系統的新願景，傳統商業銀行面臨新的異業競爭對手，以及隨著新技術興起出現的機會，即時支付清算系統服務必須能夠應對金融體系結構的各種變化，而區塊鏈分布式帳簿對維護銀行金融穩定來說十分具有吸引力但仍不夠成熟，英國央行目前積極研究分布式帳簿平台面臨的隱私、安全、互操作性、可伸縮性和可持續性問題。

英國銀行業龍頭巴克萊銀行是區塊鏈領域創新領導者，也是首家實驗 Corda 平台（R3CEV 區塊鏈聯盟的新分布式帳本平台）的機構，其與以色列新創公司 Wave 合作完成全球第一筆用區塊鏈技術結算的貿易，此次第一筆交易取代的銀行結算方式是信用狀及 SWIFT，通常採用信用狀方式做

此類結算需要 7 到 10 天，但運用區塊鏈技術貿易結算僅用不到 4 小時就完成，效率大幅提升成本也大幅下降。這筆信用狀交易為愛爾蘭農產合作社 Ornua（前身為愛爾蘭乳品局）價值近 10 萬美元的乳酪與奶油出口提供擔保，保證出貨給 Seychelles 貿易公司。巴克萊銀行透過 Wave 設置區塊鏈平台執行，運用 Wave 的技術完成貨運單據、保險等文件的數位加密簽章，創下以區塊鏈技術完成貿易雙方之間實際信用狀交易的全球首例。

2016 年 2 月英國新創事業 Electron 也加入區塊鏈電業應用的行列。英國能源管理機構 Ofgem 提出建立中央集中資料註冊機制的計畫，改善過去英國電錶沒有中央註冊機制，若是用戶要攜電錶轉換電力公司，往往要花上 17~20 天的處理流程時間的問題，並希望 2019 年前能應用區塊鏈機制來建立註冊資料以及進行轉換作業，可節省建置大型集中資料中心來記錄所有的電錶資訊的龐大經費，讓用戶能達到隔日就能轉換完成的目標，用戶攜錶更換電力公司只要幾分鐘時間。這也可應用於瓦斯錶與瓦斯公司。區塊鏈還可整合電錶用來支援需求反應服務，或是用戶與用戶之間的電力交易，Electron 看好高度發展潛力，將免費提供區塊鏈平台給電力公司，當平台建立後，Electron 可發展無數衍生應用商品。Electron 接受英國政府創新獎勵已建立一個模擬資料系統測試其區塊鏈平台建置區塊鏈攜錶轉換系統，目前尚在商業化模式轉換當中，小型電力公司對爭取客戶攜錶轉換有興趣，大型電力公司則著眼於衍生應用。

2016 年德國央行創建一個新的證券交易區塊鏈商品雛形。該商品由德國央行和德國證券交易所共同開發，目前已進行進一步的測試。德國證券交易所是超級帳本 Hyperledger 聯盟的成員，該原型產品能夠完成電子證券和數字貨幣的轉帳、息票付款和證券贖回，德國機電大廠西門子（Siemens）西門子與紐約新創事業 LO3 Energy 合作將區塊鏈技術應用於微電網電力交易市場。

第二節 區塊鏈在美洲金融業之發展與應用

如前所述，美洲是區塊鏈技術在金融應用比較領先的地區，因此有不少案例可以提出參考。本研究在此主要列出區塊鏈技術在北美資本市場的應用，以及投資銀行如何在資產交易與外匯市場應用區塊鏈技術。此外，討論兩個跨國區塊鏈聯盟—R3 以及 Hyperledger 的發展[18]，希望能帶給台灣金融業者參考與啟發價值。

一、區塊鏈在美國 NASDAQ 的應用

區塊鏈技術在金融業的應用中並不僅限於銀行業，其高度安全性也引起交易所產業的重視，是以美國 NASDAQ 在這區塊鏈的潮流中也沒有缺席，在 2015 年 12 月 30 日宣布與金融創新機構 Chain.com 合作，採用區塊鏈技術打造新交易平台 Linq，這是第一個透過區塊鏈平台進行數位化證券產品管理的 Pre-IPO 系統平台，隨後在 Linq 首次成功交易一檔個股。這種創新的交易能夠記錄每筆交易流向，從此金融交易將公開透明、降低成本。其交割結算時間從三天大幅降低至十分鐘，交割風險大幅降低 99%，同時也減少交易所為了維護交割安全而付出的龐大資本支出。更甚者，買賣雙方可自行交易，去除中間人(Dealer 或 Specialist)的作用，行之有年的人工撮合制度可能因此走入歷史。

此種交易還有幾個重要的意義，對於股票交易者而言，區塊鏈可以消除對基於紙筆或者電子表格的記錄依賴的需求，減少交易造成的人為作業疏失，提高交易平台的透明度和可追蹤性；對發行股票的公司而言，Linq 實現了更佳的管理股票數據功能，讓 NASDAQ 在私募股權市場中為創業者和風險投資者提供更好的服務。此外，NASDAQ 亦將採用區塊鏈技術為上市公司提供股東電子投票服務，由於北歐的愛沙尼亞擁有國民電子身分系統因此當地公司將率先採用。

[18] 平心而論，此兩聯盟成員並非僅限於美洲金融機構，然而考量其主要發起者多在美國，故就地域別將其歸類在美洲區域。

二、Overstock 的應用

美國證券交易委員會（Securities and Exchange Commission，SEC）也在 2015 年 12 月通過 Overstock 用區塊鏈發行股票[19]，目前至少已有五家企業透過該區塊鏈平台發行股票。在此之前，Overstock 已經使用區塊鏈來發行私募債券，這種交易概念上類似 NASDAQ 的交易平台 Linq，不需要獲得金融監管部門的批准[20]。SEC 批准 Overstock 利用同樣的方式來發行公開證券，可以透過區塊鏈技術發行股票以免去中間人的成本。

雖說區塊鏈技術潛在市場龐大，但 Overstock 也在向 SEC 申請允許以區塊鏈技術發行證券之文件中，明確指出其選擇將公司訊息儲存在任何人皆可查閱之公開區塊鏈，可能導致個人對其隱私安全的疑慮。即便有此風險，仍認為區塊鏈技術應用於發行證券，將有助完善證券市場交易環境，透過區塊鏈技術，將可紀錄所有交易，從中減少中間人控制市場的空間，並減少賣空之套利行為。

三、高盛集團導入區塊鏈

美國著名投資銀行集團--高盛集團（Goldman Sachs）在 2015 年 11 月替旗下的區塊鏈技術結算系統「SETLCoin」申請專利。SETLcoin 是一種多資產的數位貨幣，適合各種不同資產的交易，包含股票、債券以及現金。前述的交易資產可以轉換成等值的 SETLcoin 資產，並且可以在 P2P 錢包系統上進行交易。該公司申請專利的文件載明，「交易者使用他們各自錢包中的相關資金，透過一個開放的交易，並且使用所描述的技術來交易證券。SETLcoin 的所有權在確認和驗證後，將被即時轉移給新的所有者，這是基於點對點網路系統中的網路帳本，能夠確保可以準確且即時地執行」。顯而易見的是，為了讓這種系統得以運作，交易雙方都須擁有 SETLcoin 錢包和 SETLcoin 軟體來下達交易指令，然而不要求必須是同一種貨幣。

[19] 據 Overstock 提供的公開檔案顯示，SEC 已經批准其 Form S-3 申請，允許 Overstock 透過區塊鏈技術公開發行股票。

[20] Overstock 早在 2014 年 4 月發起一個 tØ .com 平台幫助投資者進行股權交易和結算。

其意義在於如同法定貨幣一樣，如果想要達成交易，交易雙方都要相信所使用的這種貨幣，並承認該貨幣的價值。

除此之外，高盛集團進一步希望使用區塊鏈技術來取代傳統外匯市場交易機制，據美國專利商標局(The United States Patent and Trademark Office，USPTO)於 2016 年 9 月 8 日透露訊息，高盛已經提出相關專利申請文件。高盛在申請專利文件中列舉目前外匯交易方式所面臨的問題，以及加密貨幣存在的問題。高盛表示外匯市場中的金融交易會產生大量結算風險，一般包括兩個部分。就加密貨幣而言，高盛提到了比特幣和瑞波幣（Ripple Credit），並解釋稱二者透過使用不易歸咎於現實中具體一方的任意帳號隱藏了某一方的身份，然而大型的金融機構（如中央銀行）往往因為交易的規模和數量過大，可能會向市場參與者洩露其身份而無法依賴它們。第二個部分在於它們缺少可以協助監管者進行反洗錢的身份檢查。高盛在申請文件上表示：「就其本身而言，需要有能夠像比特幣和瑞波幣一樣迅速處理交易的新系統和方法，且不會犧牲參與方的隱私」。當然，區塊鏈在北美的發展並不僅限於高盛集團，不讓高盛專美於前，美國銀行在 2015 年下半年也向 USPTO 申請 10 項與區塊鍊技術相關專利。

四、R3 聯盟

討論區塊鏈在金融業的實際運用，就不得不提到目前凝聚最多(金融)機構、勢力最為龐大的--R3，該聯盟為一跨國際組織，在紐約和倫敦等地設有據點，團隊營運肇始於 2015 年 9 月的紐約 R3 CEV 公司，主要致力於為銀行業者提供探索區塊鏈技術的管道以及建立區塊鏈概念性產品，會員銀行將共同研發區塊鏈技術，開發全球金融服務業的新商業應用，並建立一致的標準和協定，讓區塊鏈技術更能被廣泛採用，提升整個網路之間的影響力，技術人員來自 IBM、巴克萊銀行、Google 與微軟等公司。其創辦人 David Rutter 曾公開表示，R3 是金融市場加密與交易的創業實踐，將專注於開發一個能將區塊鏈技術應用於金融市場的架構。目前該聯盟的成員

已經自最初的巴克萊銀行、西班牙對外銀行、澳洲聯邦銀行、瑞士瑞信銀行、高盛、美國摩根大通銀行、蘇格蘭皇家銀行、美國道富銀行與瑞士銀行等九家創始銀行，經過幾次的擴充成員，擴大到目前的五十多家金融機構，聯盟成員及加入日期如【表 3-2-1】所示[21]。吾人可以觀察到從 2016 年 6 月開始，加入的金融機構就不是僅限銀行業者了，關於此點，業者曾表示對此一聯盟還會不會繼續擴大的疑慮，R3 表示，其允許銀行加入的「初始視窗」已先關閉，2016 年開始，聯盟將尋求與非銀行金融機構和團體合作，希望區塊鏈聯盟能吸引更多不同產業共同參與。

[21] 有趣的是，俄羅斯最大的銀行 Sberbank 在 2015 年 12 月宣稱要加入 R3，卻沒出現在最新的會員名單中。

【表 3-2-1】 R3CEV 聯盟成員與加入日期

日期	成員
2015/9/15	巴克萊銀行、西班牙對外銀行、澳洲聯邦銀行、瑞士瑞信銀行、高盛、美國摩根大通銀行、蘇格蘭皇家銀行、美國道富銀行、瑞士銀行等九家
2015/9/29	美國銀行、紐約梅隆銀行、花旗銀行、德國商業銀行、德意志銀行、滙豐銀行、三菱日聯金融集團、摩根士丹利銀行、澳洲國民銀行、加拿大皇家銀行、瑞典北歐斯安銀行、法國興業銀行、多倫多道明銀行等十三家
2015/10/28	日本瑞穗銀行、北歐聯合銀行、義大利裕信銀行等三家
2015/11/19	法國巴黎銀行、加拿大帝國商業銀行、荷蘭安智銀行、麥格理銀行、富國銀行等五家
2015/12/17	加拿大滿地可銀行、丹麥丹斯克銀行、義大利聯合聖保羅銀行、法國外貿銀行、日本野村銀行、北方信託、芬蘭 OP 金融集團、桑坦德銀行(西班牙國家銀行)、加拿大豐業銀行、日本三井住友銀行、美國合眾銀行、澳大利亞西太平洋銀行等十二家
2016/4/25	日本 SBI 金融集團、南韓韓亞銀行、巴西伊陶銀行(Bank Itau)等三家
2016/5/24	中國平安集團
2016/6/3	友邦保險(AIA)
2016/6/23	日本豐田金融服務
2016/8/31	美國大都會人壽

資料來源：維基百科、R3CEV 網站，本研究整理

值得一提的是，我國銀行業者--中國信託銀行也在 2016 年 10 月 12 日宣布啟動區塊鏈發展計畫，加入 R3 聯盟，成為台灣首家 R3 聯盟會員。R3 聯盟創始人暨執行長 David Rutter 也表示，中信銀加入 R3 聯盟，是 R3 聯盟拓展亞洲市場的重要里程碑，十分期待雙方共同合作開發真正跨國界的國際區塊鏈應用。

R3 聯盟為金融機構創建可在安全環境下彼此合作的開發平台，目前已協助會員銀行完成多項區塊鏈的實驗專案。具體言之，2016 年 3 月 3 日，R3 宣布其 40 家銀行成員已經測試五種不同的區塊鏈技術，用於發行、交易和贖回固定收益產品。這被認為是區塊鏈技術在金融市場中最大的一次真實試驗。R3 公司嘗試的五種分散式帳本分別由 Chain、Eris Industries、Ethereum(以太坊)、IBM 和 Intel 這五家公司提供，這幾家公司目前都在開發開源專案或為企業研究這類技術。

以跨境匯款業務而言，R3 聯盟已成功測試將過去須透過中間行確認，歷經結算、電文交付與換匯等過程的匯款時間，從以往三至五天的作業時間，縮短至三到五秒，且未來計畫應用區塊鏈技術，針對放款撥貸與保險理賠等項目創造更多金融革新。

此外，貿易融資業務方面，則在 2016 年 8 月由瑞士銀行、美國銀行等 15 家聯盟銀行，透過 R3 聯盟進行開發的區塊鏈技術平台 Corda，以無紙化的作業程序完成 Corda 分散式分類帳技術的應用測試。值得注意的是，Corda 並非傳統的區塊鏈，而是專為金融業設計的分散式分類帳平台。不具有一連串的 Hash 區塊（A Chain of Hash Block），也沒有像比特幣區塊鏈般的採礦機制和礦工角色。由於 R3 發現銀行業者普遍不希望與其他機構共用所有的交易紀錄，因此在 Corda 平台上的所有交易紀錄，即使都已經加密，仍然不會公開給所有的參與者。Corda 主要的特徵如【表 3-2-2】所示。簡而言之，Corda 可在受監管的金融機構之間，管理並維護金融協議（Financial Agreements）。Corda 採用許多區塊鏈技術的優勢與特性，同時也捨棄讓區塊鏈技術無法融進大多數金融領域的設計理念。

【表 3-2-2】Corda 主要特徵

1.不會公開共用不需要的數據：機構們只有在簽有協議的情況下才能合法知道一些數據；
2.工作流程是去中心化的，只在各個公司之間而沒有領導機構；
3.在單個節點上 Corda 實現了一致性；

4.設計具備控制和監督的職能；
5.處理過程由可關聯的節點相互交叉驗證，而不是在廣泛的範圍內納入不相關的驗證者；
6.支援大量機械性的場景交易；
7.使傳統合約和智能合約無縫對接；
8.建立在行業標準上的一個工具；
9.沒有使用本地加密貨幣。

資料來源：本研究整理自網際網路資料

數位貨幣方面，則由加拿大中央銀行運用 R3 聯盟的技術，與加拿大各家銀行共同進行，測試以區塊鏈技術發行、轉換和結算央行資產概念的可行性。

五、Hyperledger

超級帳本（Hyperledger）聯盟成立於 2015 年 12 月，成立宗旨是共同建立並維持一個跨產業且開放的分散式(Distributed)分類帳技術平台，該聯盟係緣起於 IBM 的 Linux Foundation 於 2015 年發起的推進區塊鏈數位元元技術和交易驗證的開源專案，乃 IBM 的 Linux 基金會聯合 30 家初始成員（包括 IBM、Accenture、Intel、J.P. Morgan、R3、DAH、DTCC、FUJITSU、HITACHI、SWIFT、Cisco 等）共同成立。相較於 R3 的成立比較從金融機構的角度出發，Hyperledger 的科技內涵較為濃厚，其成員除了金融機構外，還包含科技公司與其他產業的企業，目標是讓成員合作，共建開放平台，開發來自多個不同行業的各種應用案例。目前主要成員除荷蘭銀行(ABN AMRO)、Accenture、Cisco、The Depository Trust and Clearing Corporation（美國證券集中保管結算公司，簡稱 DTCC）等，也陸續吸引許多像 R3 CEV 及 DAH 的區塊鏈聯盟及金融科技公司加入，目前共有 81 家金融、科技及區塊鏈技術團隊，如【表 3-2-3】所示。其中也包括 13 家中國大陸的公司，包括艾億數融科技公司、Onchain、比鄰共贏（Belink）資訊技術有限公司、BitSE、布比以及三一重工等。

【表 3-2-3】Hyperledger 主要成員

金融機構	ABN AMRO、ANZ、BNY Mellon、CME Group、Deutsche Börse、DTCC、Gem、itBit、J.P. Morgan、London Stock Exchange、SWIFT、Tequa Creek Holdings、Wells Fargo
(金融)科技公司	Blockstream、Bloq、Cisco、DAH、eVue Digital Labs、Fujitsu、IBM、Intel、Montran Labs、NEC、NTT Data、R3、Redhat、Ribbit.me、VMWare
其他領域機構	Accenture、Hitachi、Milligan Partners、Thomson Reuters

資料來源：麥肯錫、Hyperledger 網頁，本研究整理

吾人從表可知 Hyperledger 聯盟的成員中有許多知名科技公司，是以該聯盟主要的技術來自於成員中的科技公司提出的程式碼乃毋庸置疑。進一步說明，IBM 貢獻出數萬行已有的 Open Block Chain 程式碼，Digital Asset Holdings 貢獻企業和開發者相關資源，R3 貢獻新的金融交易架構，Intel 則貢獻和分散式帳本相關的程式碼。此一聯盟出現的意義，在於宣告區塊鏈技術已不再是一個單純的開源技術，而是正式被主流機構和市場認可的可應用技術。同時，Hyperledger 首次提出和實現的完備許可權管理、創新的一致性演算法和可拔插的架構，對於區塊鏈相關技術和產業的發展都將產生深遠的影響。

目前 Hyperledger 主要有兩大子專案：

1.fabric：包括 fabric 和 fabric-api，最早由 IBM 和 DAH 發起，目標是區塊鏈的基礎核心平台，支援 pbft 等新的 consensus 機制，支援許可權管理。

2.sawtooth Lake：包括 arcade、core、dev-tools、validator、mktplace 等，是由 Intel 貢獻和主導的區塊鏈平台，支援全新的共識機制 Proof of Elapsed Time（PoET）。

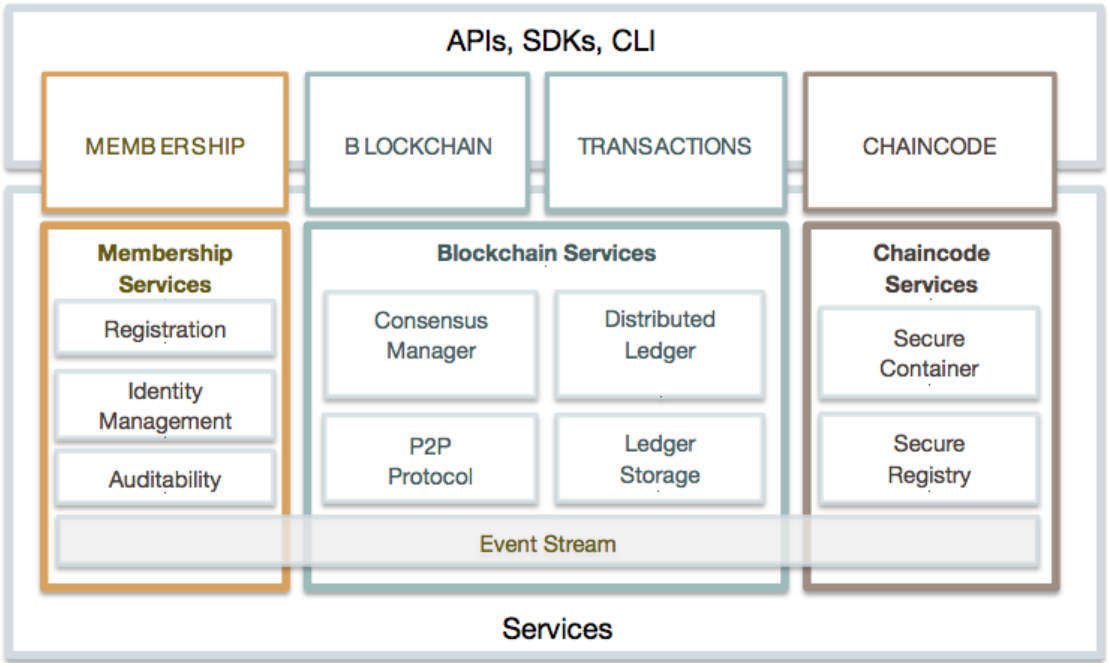
當然，以上專案仍處於初始的孵化（Incubation）階段。另外，專案有幾個成員們共同約定遵守的基本原則：

1.重視模組化設計：包括交易、合同、一致性、身份、儲存等技術場景。

2.程式碼可讀性：保障新功能和模組都可以很容易添加和擴充。

3.演化路線的可擴充性：隨著需求的深入和更多的應用環境，不斷增加和演化新的項目。

整個聯盟專案的模組架構如【圖 3-2-1】所示，包括三大組件：區塊鏈服務、鏈碼服務（Chaincode）以及成員權限管理（Membership）。



資料來源：Hyperledger 網頁

【圖 3-2-1】Hyperledger 模組架構設計

對於吾人而言，Hyperledger 的重要意義在於區塊鏈的金融科技業務不是單純由科技公司主導或者金融業者主導，而是結合各種領域業者的專長共同開發。其次，Hyperledger 下的部分功能已經不再是實驗室裡的概念技術，而是準備推到市場的實務技術。更甚者，此一聯盟成員非常龐大，且包含另一個全球性的 R3 聯盟，這更象徵開放的核心價值。

第三節 區塊鏈在亞洲金融業之發展與應用

談到吾人所在的亞洲地區區塊鏈在金融方面的應用發展，似乎較歐洲與北美洲為慢。以往亞洲的金融機構給人的印象是對比特幣和區塊鏈技術缺乏興趣，更甚者，銀行似乎忙著對這類的數位貨幣發出警告，而非投入相關業務。此乃有跡可尋，2014 年發生在日本東京的 Mt Gox 倒閉事件[22]和中國人民銀行打擊比特幣交易，其後果便是亞洲各金融機構普遍對比特幣產生防範心理。不過，隨著近期全球金融領域對區塊鏈技術的熱情逐漸高漲，如同歐洲和北美的同業一般，亞洲的銀行體系也開始表現出對該項顛覆性技術的關注。

一、中國大陸

在中國大陸，人民銀行副行長易綱在 2013 年 11 月表示，從人民銀行角度，短期內不可能承認比特幣的合法性，同年 12 月 5 日人民銀行等五個部委發布關於防範比特幣風險的通知。令人驚訝的是，人民銀行在最近轉變先前態度，先在 2014 年成立專門的數碼貨幣研究團隊，並於 2015 年初進一步擴充發展，研究使用區塊鏈技術去紙幣，且宣稱「已取得階段性成果」。於 2016 年 1 月 20 日在北京召開「中國人民銀行數碼貨幣研討會」，會議認為，發行數碼貨幣可降低傳統紙幣發行與流通的高昂成本、提升經濟交易活動的便利性和透明度、減少洗錢及逃漏稅等違法犯罪行為，並可提升央行對貨幣供給和貨幣流通的控制力、協助普惠金融的實現。上述各項功能的可及性，是以區塊鏈技術為核心。換言之，人民銀行對於區塊鏈技術應用於貨幣的去紙幣化，已經表現出不同於以往對比特幣的保留態度，轉而予以高度肯定。

除了人民銀行之外，2015 年 10 月 15 日全球首屆區塊鏈高峰會在上海召開，來自中國人民銀行金融研究所、人民銀行徵信中心、上海證券交易

[22] Mt.Gox 最初由 Jed McCaled 在 2010 年 7 月建立，後來在 2011 年 3 月賣給了由 Mark Karpelese 創建的 Tibanne Co.，一度成為全球最大的比特幣交易所。於 2014 年 2 月因被駭客盜取比特幣而下線，暫停網上交易，2014 年 2 月 28 日向東京地方法院申請破產保護。

所、陸金所、德勤會計事務所等全球對區塊鏈技術應用前景有興趣的專業人士參加。中國銀聯、阿里巴巴等多家公司也陸續宣布研究區塊鏈技術在群眾募資、P2P、證券交易等傳統金融領域的應用。

ChinaLedger

中國分散式總帳基礎協議聯盟(ChinaLedger)係由位於上海浦東新區陸家嘴的萬向區塊鏈實驗室（WanXiang Blockchain Labs）於 2016 年 4 月發起成立，當時總共有 11 家中國大陸金融機構、科技公司及研究單位參與，金融機構裡包含區域性商品交易所、產權交易所及金融資產交易所組成，成員如【表 3-3-1】所示，並由中國證監會所屬的中國證券業協會互聯網證券委員會擔任專案顧問，聯盟秘書處設立在萬向區塊鏈實驗室。成立宗旨是希望利用和改進現有的區塊鏈技術，應用在專屬中國大陸的商業環境。如同該聯盟官網敘述，希望透過開發中國大陸的區塊鏈底層技術，使得中國大陸擁有符合自己國情的區塊鏈底層技術，不再使用由歐美國家主導的底層技術。在這方面，ChinaLedger 聯盟將會成為探索底層技術的重要力量，以增加中國大陸官方、人民銀行及各金融機構在全球內的話語權，進一步維護其國家經濟金融主權。

【表 3-3-1】ChinaLedger 聯盟成員

金融機構	中證機構間報價系統股份有限公司、浙江股權交易中心、樂視金融、矩陣金融、中國印鈔造幣總公司、招銀前海金融、瀚德金融創投、上海股權託管交易中心
(金融)科技公司	通聯支付、大連飛創信息技術
其他領域機構	萬向區塊鏈實驗室

資料來源：ChinaLedger 聯盟網頁，本研究整理

ChinaLedger 聯盟的主要工作任務是共同合作研究區塊鏈技術，從場外交易切入，結合中國大陸現有政策法規和中國大陸金融行業特有的業務邏

輯，開發區塊鏈產品使其符合中國大陸的政策法規、國家標準、業務邏輯和使用習慣的區塊鏈技術底層協定。根據該聯盟公開資料，未來該聯盟的底層技術協定將會是開源的，各成員可以在這個基礎協議上搭建具體的應用場景。

技術方面，該聯盟除中國大陸國內金融科技團隊自有技術外，尚延聘海外技術顧問增加研發能量，諸如 UBS 集團資深創新經理 Alex Batlin、多倫多交易所首席數位長 Anthony Di Iorio、比特幣核心開發者 Jeff Garzik 以及乙太坊的創辦人 Vitalik Buterin，後者同時也是萬向區塊鏈實驗室的共同創辦人，相信此一安排可確保技術來源的穩定性。

類似其他金融業區塊鏈聯盟或組織，ChinaLedger 仍須面對交易的保密考量和監理機關的要求，由於從既有公開資料中能夠查閱到的較為徹底的密碼學隱私解決方案包含零知識證明、環簽名和同態加密三種，但相應的技術方案與實際需求尚有差距。有鑑於此，ChinaLedger 在白皮書中特別提出一種基於集中交易對手（Central Counterparty，以下簡稱 CCP）的雙鏈隱私保護方案，協助交易與結算的進行[23]。換言之，可以把所有參與者都能訪問的分散式帳本記為「鏈 A」，把只有 CCP 和監管者能訪問的分散式帳本記為「鏈 B」。在鏈 A 上，交易指令以密文形式出現。交易發起方將對手方資訊和交易內容資訊用自己的私密金鑰簽名，然後打包用 CCP 的公開金鑰加密，發給智能合約。所有參與人均可透過分散式帳本技術平台，在鏈 A 上見證這一筆內容被加密的交易。如果交易是資金和資產在鏈上對流，雙方都需提交這種格式的交易指令。CCP 用自己的私密金鑰解密後，將明文的交易指令發到鏈 B 上，檢驗交易指令中發起者簽名的有效性，並獲得鏈 B 做出的是否透支的判斷。如果透支檢查正常通過，CCP 在鏈 B 上替交易雙方完成交易後餘額的維護。上述手續完成後，CCP 在鏈 B 上生成、在鏈 A 上向發起方發送交易確認消息。在此一雙鏈模型架構下，普通

[23] 主要參考自 ChinaLedger2016 年 10 月公布的《面向中國資本市場應用的分布式總帳白皮書》。

參與者在鏈 A 上看不到交易的細節。如有需要，被法律賦予監管職能的監管者方可透過開設在鏈 B 上的監管者帳戶，看到從鏈 A 發起的所有交易的明細。

二、新加坡星展銀行在區塊鏈的努力

星展銀行與渣打銀行在 2015 年底宣布與金融科技公司 Ripple 合作，將區塊鏈技術應用在供應鏈金融業務，利用智能合約及點對點跨境交易的技術，將流程自動化並提高安全性。如果能通過區塊鏈的技術將供應鏈金融的流程數位化並利用其公開、安全及不可篡改的特性，合作三方認為，將能大幅度減少貿易鏈上的欺詐案件，為銀行節約數百萬美元的風險損失。目前這一合作案正在尋求更多銀行的加入，一起測試該技術的實用性。

除了銀行業者自身的動作外，新加坡的金融主管機關--金融管理局(Monetary Authority of Singapore，MAS)也與星展銀行及渣打銀行在 2015 年開始聯合開發組建以區塊鏈為基礎的記錄系統，該技術將被應用在提高進出口商及銀行在發票融資(應收帳款融資)領域的安全性和便捷性。此一計畫苟能成功，相信對於進出口貿易暢旺且銀行貿易融資業務量龐大的新加坡而言，有相當的貢獻性。

值得一提的是和兩家銀行合作的 Ripple 公司，成立於美國的 Ripple 為一家利用類區塊鏈概念發展跨境結算的金融科技公司，Ripple 正式成立於 2012 年，當時多數公司還只專注在比特幣協議，Ripple 在區塊鏈技術上沒有競爭對手，它建構出一個沒有中央節點的分散式支付網路，希望提供一個能取代現行 SWIFT(環球同業銀行金融電訊協會)網路的跨境轉帳平台，打造全球統一網路金融傳輸協議。Ripple 的跨帳本協議(Inter Ledger Protocol)可說是讓參與協議的各方都能看到同樣內容的一套帳本，透過該公司的網路，銀行客戶可以實現實時的點對點跨國轉帳，不需中心組織管理，且支援各國不同貨幣。

如果 Ripple 協議成為了金融體系的標準協議，在網路中的各方都能任

意轉帳貨幣，支付就會像收發電子郵件一樣便宜且快速，最重要的是將節省相關的跨行異地以及跨國支付手續費。截至目前全球已有 17 個國家的銀行加入合作，共同參與 Ripple 為金融機構打造的解決方案。包括渣打、西太平洋銀行（Westpac）、澳洲國家銀行、瑞穗金融集團、蒙特利爾銀行金融集團和上海華瑞銀行等都在 Ripple 的網路中成功進行過轉帳，包括留學生轉帳並等商業化產品。

銀行有許多交易成本高但低利潤的交易業務，因為轉帳流程複雜但收取的費率沒有大型交易那麼多。Ripple 在這類交易具有利基，因此是目前國際上最成功的區塊鏈技術公司。Ripple 的主要業務是幫助銀行讓跨境支付更便捷，其核心產品則是 Ripple 協議。Ripple 協議的前身是 2004 年開發的 Ripplepay，第一代系統 RipplePay.com 誕生於 2005 年，能透過全球網路為社群用戶提供安全的支付服務。Ripple 協議本質上是一個即時結算系統結合貨幣兌換與匯款網路，藉由分布式開源網路協議、共識總帳(consensus ledger)和原生的貨幣 XRP(瑞波幣)完成。另外，Ripple 的帳本與比特幣不同，需要允許才能加入，即銀行不用擔心匿名方涉入交易之中。而且 重點是 Ripple 的分布式帳本不需要使用自身的 XRP 數位貨幣也能運作。

Ripple 在 2014 年產生第一位銀行用戶：德國網路銀行 Fidor。Ripple 開發出了新的點對點交易流程，銀行不再需要支付代理費。之後又獲得兩家美國銀行對 Ripple 協議的支持，並在當年 12 月與全球包括美國銀行和匯豐銀行等 65 個國家的支付服務公司 Earthport 合作，Ripple 逐漸受到市場重視。Ripple 採用區塊鏈技術為全球大型銀行解決金融交易問題，2016 年 9 月再度獲得 5,500 萬美元融資，包括渣打銀行、埃森哲創投、SCB Digital Ventures、泰國商業銀行和日本知名金融集團思伯益控股(SBI Holdings, Inc)；連同之前投資過 Ripple 的 Google Ventures、A16Z 、IDG 等多家創投也都再度參與了本次投資。目前 Ripple 已完成了 30 個試驗項目，並與全球 前 50 大銀行中的 15 家合作，其中包括瑞銀與渣打，而有 10

家都處於商業化合作階段，截止目前 Ripple 共獲得了 9,300 萬美元融資。

三、日本金融機構在區塊鏈的應用

2015 年 12 月，日本住信 SBI 網路銀行(SBI Sumishin Net Bank)已經宣布他們在開發概念證明，旨在和野村綜合研究所（Nomura Research Institute，NRI）探索區塊鏈銀行的應用，野村綜合研究所是野村控股公司的研究分支。SBI Sumishin 是日本最大的信託銀行，由 Sumitomo Mitsui 信託銀行與 SBI 控股公司合資成立。NRI 成立於 1965 年，是日本老牌的民間智庫單位，負責為包括金融業在內的多個產業提供諮詢服務和 IT 解決方案。

雖然目前關於這個專案的資訊還很少，NRI 表示將會尋求「監測業務方案」為 SBI Sumishin 準備原型的目標。但是，一家區塊鏈公司 Dragonfly Fintech Private 將會參與項目的研發。在幾份聲明中，NRI 高級主管 Minoru Yokote 指出，該專案正是該組織尋求擁抱分佈式金融技術的一個典型案例。Yokote 說：「NRI 致力於研究區塊鏈技術帶來的挑戰，並且建議將這一新技術應用到銀行業」。

日本幾家銀行和科技業者，包括歐力士銀行、靜岡銀行、NTT 數據公司和 NTT DOCOMO 表示將投入資源對區塊鏈進行研究。此外，日本證交所(Japan Exchange Group)在 2016 年 2 月 16 日宣布與 IBM Japan 達成共識，一同為區塊鏈技術進行測試概念性驗證((Proof-of-Concept，PoC)。技術方面，將採用 Linux 基金會 Hyperledger 計畫中的區塊鏈技術。日本交易所規劃將區塊鏈技術先導入在交易及結算上，從 2016 年 3 月起先從低成交量的市場著手測試。當然，此一類型的試驗計畫並非只有日本交易所著手進行，德國的 Deutsche Borse、美國的 CME Group 與 DTCC 亦為該計畫的成員。

當然，歐洲及亞洲地區塊鏈在金融業務的拓展並不僅限於前述案例或事實，其他進展如下所示：

1.南韓：南韓中央銀行在報告中指出區塊鏈發展的重要性，因該技術特徵在於可以安全高效率的提供金融服務，且不需仲介機構負責處理交易資訊。故該行將持續關注區塊鏈技術的發展，進行深度研究，甚至考慮將自行投入分散式帳簿技術的研發。2016 年 12 月南韓金融投資協會(Korea Financial Investment Association) 計劃成立政府和民間聯盟，研究比特幣底層創新技術在南韓社會和產業中的應用，並與南韓 21 家金融投資公司和 5 家區塊鏈技術企業簽署合作備忘錄，成立分布式帳本技術研究區塊鏈聯盟，這是南韓成立首家區塊鏈聯盟，南韓金融投資協會 IT 委員會將與聯盟成員共享其區塊鏈案例和技術研究成果。

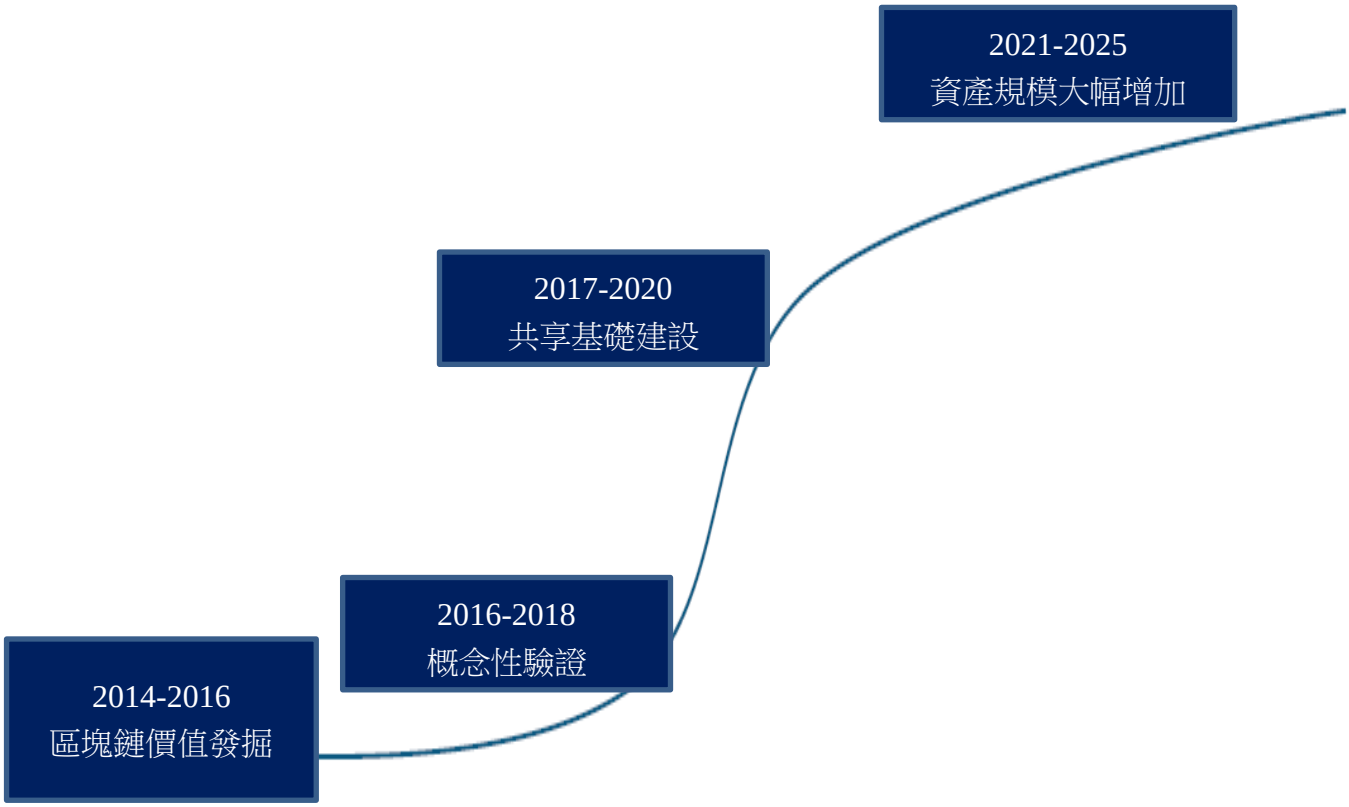
比照日本和俄羅斯的公私合作方案，南韓規劃包括 2017 年完成個人身份驗證的區塊鏈解決方案、2018 及 2019 年完成清算結算自動化、2020 年完成區塊鏈技術的場外交易。南韓金融機構在區塊鏈領域已經有了計劃，南韓最大的銀行控股公司之一韓亞金融集團(HanaFinancialGroup)是南韓第一家加入 R3 區塊鏈聯盟的機構，南韓證券交易運營商南韓交易所(Korea Exchange)亦發起區塊鏈平台，讓新創企業在公開市場上進行股權交易；南韓新韓銀行(Shinhan Bank)將規劃南韓和中國大陸銀行之間比特幣區塊鏈的匯款服務合作。南韓國民銀行與當地的比特幣創業公司 Coinplug 進行合作，宣布藉由使用區塊鏈技術就可以避免掉仲介服務，能夠降低成本，為客戶帶來好處。

2.香港：香港政府在 2016 年財政預算案中明文提到區塊鏈技術，可說是亞洲第一個提到區塊鏈技術的政府機關。香港政府鼓勵業界和相關機構，探討區塊鏈技術在金融業的應用，發展其減少可疑交易和降低交易成本的潛力。2016 年 11 月，中銀香港將區塊鏈技術應用於房貸申請業務，目前已成功完成首宗估價，另有兩間銀行均已同意加入區塊鏈房貸技術。區塊鏈房貸技術透過共享帳簿技術，建立及傳送完整、加密的資料。房貸相關單位獲得確保真確的文件之餘，過往紀錄不能竄改，大幅提升偽造文件難度。中銀香港每年估價逾 2 萬次，銀行藉精簡驗證估價報告流程，節省成

本並加快房貸物件估價及貸款審批程序。中銀香港目前與兩家物業估價公司合作，未來會邀請其他估價公司及銀行同業參加，強化區塊鏈物業估價資料，未來亦會研究把區塊鏈技術應用於貿易融資、電子證件管理及跨境支付等領域。

除了前述案例外，與亞洲鄰近的澳洲在區塊鏈的應用也是不落人後，2015 年 7 月，澳洲幾家主要金融機構，諸如澳盛銀行(ANZ)、澳洲國家銀行(National Australia Bank)與澳洲中央銀行(Reserve Bank of Australia)等 12 家主要金融機構與 SWIFT 合作，共同開發全新的金融服務基礎建設--澳大利亞新型支付平台(New Payment Platform)，預計在 2017 年下半年上線。此外，澳洲聯邦銀行(Commonwealth Bank of Australia)也積極開發區塊鏈技術，並以新創加速器的姿態，在 2016 年 1 月成功開發出開放性行動支付平台—Albert。

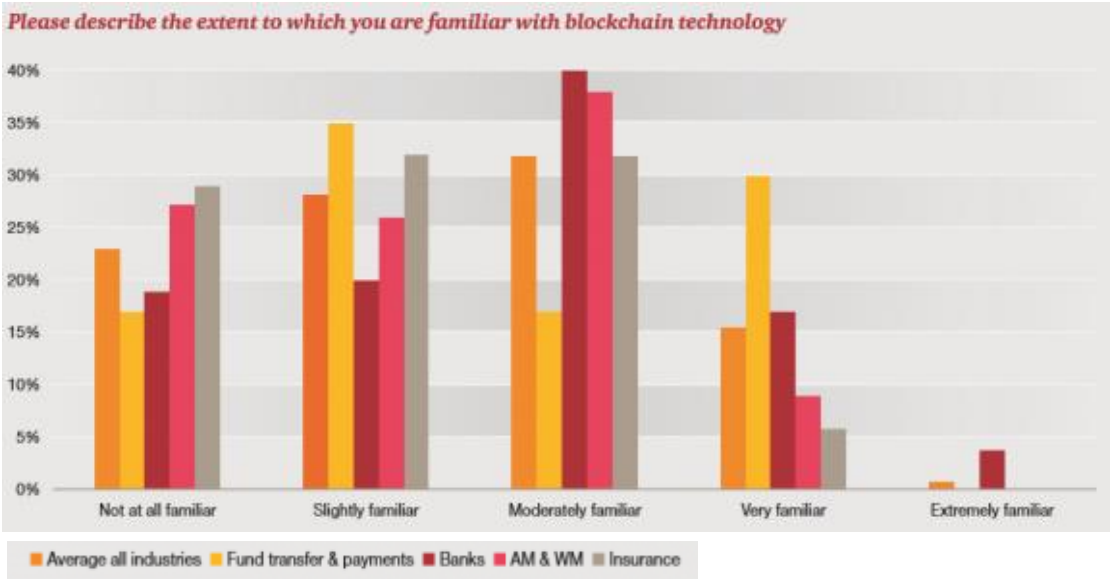
根據 Morgan Stanley 2016 年 4 月最新研究報告，2014-2016 年為區塊鏈價值發掘過程，2016-2018 年為概念性驗證階段，2017-2020 年為共享基礎建設階段，2021-2025 年預估資產規模將大幅增加。區塊鏈技術從概念到實證，2017 年將是關鍵變化很大的一年，2018 年將會開始有商業化應用實務。



資料來源：Morgan Stanley

【圖 3-3-1】區塊鏈之發展趨勢預測

根據資誠(PwC)2016 年全球金融科技調查報告，資誠調查金融業者結果顯示區塊鏈將改寫整個金融產業的規則。在區塊鏈方面，有 56%金融業者對於區塊鏈技術理解重要性，但對於此技術將帶來的影響，有 57%金融業者表示不確定或是不清楚該如何面對，甚至有超過 83%金融業者坦言，對區塊鏈技術還不是很了解。對區塊鏈技術了解程度較高的是支付服務的業者，有 3 成自認對區塊鏈技術及運作方式熟悉。



資料來源：PwC

【圖 3-3-2】2016 年全球金融科技調查報告-區塊鏈

如同企業內部過去採用 ERP 企業資源管理軟體，來傳遞並共享資料與邏輯，讓企業內部的商業流程最佳化，PwC 認為區塊鏈技術將是能促成下一階段企業商業流程最佳化大幅躍升的技術，區塊鏈技術將能促使產業之間的商業流程更進一步達到最佳化，讓不同的或是彼此相互競爭的企業之間傳遞、共享資料。然而儘管區塊鏈技術前景十分看好，但依舊存在不少挑戰與障礙待突破，未來區塊鏈技術進入商業應用潛力十足，將對金融業現有的利潤池(Profit Pools)帶來重大轉變，並重新分配給具有高運用效率的新區塊鏈平臺業者，區塊鏈不僅能降低成本，也能大幅提升交易透明度，對消費者及監理單位來說都有相當大的影響。

全球信用卡大廠 MasterCard 也正在開發區塊鏈以及分散式帳本的相關技術，除釋出 3 項 APIs 可連結到自家內部的區塊鏈，於 2016 年 11 月在美國提出 4 項支付以及交易上的應用區塊鏈專利，包括區塊鏈交易中的授權、處理與安全問題。另一家信用卡大廠 Visa 亦將於 2017 年推出以區塊鏈技術為基礎的「Visa B2B Connect」服務，顯示國際信用卡公司亦非常重

視數位貨幣以及區塊鏈對信用卡產業帶來的影響。企業將傳統支付系統與區塊鏈結合，確保去中心化及帳戶安全。

全球四大會計師事務所安永(Ernst & Young)宣布 2017 年安永瑞士(EY Switzerland)將接受用戶使用比特幣付款，安永瑞士蘇黎世大樓將安裝比特幣 ATM，瑞士法郎兌換成比特幣，員工也會配有安全的電子錢包(EY wallet app)，讓員工熟悉區塊鏈與數位貨幣，用比特幣購買商品與服務，為全球會計界的首例。

原始創始機構高盛(Goldman)及西班牙國際銀行(Santander)宣布退出目前全球最大擁有超過 70 間金融機構的 R3 區塊鏈聯盟，包括摩根士丹利(Morgan Stanley)和澳洲國民銀行也極有可能不參與 R3 1.5 億美元全球史上最高的最新融資案，另外摩根大通(JP Morgan)、麥格理銀行(Macquarie Group)以及美國合眾銀行(US Bancorp) 也計畫退出 R3 陣營，而美國銀行、巴克萊銀行和瑞銀集團等其他 R3 早期成員，則仍是該聯盟的成員，全球區塊鏈陣營預計將進行重整，隨著區塊鏈應用漸成熟，區塊鏈技術及應用市場將會更加競爭激烈。隨著越來越多金融機構退出 R3，非代表區塊鏈將沒落，卻是代表區塊鏈技術日趨成熟，金融機構已開始積極選定投資對象，組織競爭也隨之增加。

過去兩年內許多區塊鏈組織和策略結盟出現，不少組織具有雙重會員身分，因此區塊鏈組織重整會員關係是重大趨勢，期望機構本身的區塊鏈投資可以成為主流市場應用。

第四節 小結

他山之石，可以攻錯。透過對前述區塊鏈案例事件的觀察，吾人應可約略窺知全球主要金融機構或主管機關已認知到區塊鏈的重要性或致力於發展區塊鏈解決方案，希望實現快速或低成本的跨銀行交易且降低作業疏失帶來的成本，相信區塊鏈技術在金融業的應用將逐漸被金融業者重視。加上全球金流的跨境發展與因此而來的競爭蔚為趨勢，台灣的金融業者在這領域更不能缺席。

根據世界經濟論壇（World Economic Forum，簡稱 WEF）在 2016 年 8 月 12 日發表的報告，全球區塊鏈投資總額已達 14 億美元，有近百家企業加入各區塊鏈組織，研發超過 2,500 項金融科技專利，預計在 2017 年將有八成銀行啟動區塊鏈專案，更是佐證了吾人對前述趨勢的看法。該報告同時指出，區塊鏈技術目前處於過度期望的高峰期（Peak of Inflated Expectations），此一階段可說是百家爭鳴，但僅有部分創新應用可能成功，將有更多是失敗的。當科技無法滿足過度期待，大眾回歸理性後，該技術就開始進入泡沫化的谷底階段（Trough of Disillusionment）。區塊鏈技術目前已進入炒作的區間，但還沒有到頂端，預計炒作仍將持續一段時間。就現在這個時間點而言，泡沫尚不會破滅。換言之，本章討論的案例在未來並非皆能成功，區塊鏈的發展仍是現在進行式，目前區塊鏈技術在西方國家已經進行實務端的應用，在中國大陸也正積極開展，但國內則仍未見到官方訂定相關的發展規劃。

綜上，說區塊鏈技術是繼網際網路之後最具顛覆性的革命性技術亦不為過，它將開啟一系列新的商業模式。現在的區塊鏈技術所處的發展階段，類似處於 20 世紀 90 年代中期的網際網路技術，根據麥肯錫 2016 年 2 月針對全球主要金融機構高階主管的訪談調查，有約 46%的受訪者認為最快一年半，最慢三年就可看到區塊鏈技術帶來的實質影響。是以對金融機構而言，區塊鏈的布局，宜早不宜遲。當然，本章的目的在於提出參考案例

供參考，不管成功或失敗，相信都有值得參考或帶來啟發之處，其後續發展仍值得吾人持續關切。建議趁著區塊鏈技術在各個先進國家還處於進行式的階段，金融機構或政府主管機關將之納為重大發展議題，持續關注與有效投入。

第四章 區塊鏈及數位貨幣對我國金融業之影響

第一節 區塊鏈目前在台灣之發展

誠如第三章所述，區塊鏈應用不只在國外起飛，台灣也隨金融科技浪潮，趕上了這一波區塊鏈風潮。金融業者方面，第一金、華南金、玉山金、中信金、國泰金及富邦金是台灣目前積極投入區塊鏈應用的金控公司；台灣大學的 G Coin 則嘗試建構本土第一個最底層的區塊鏈協議;另外亦有非金融業者從事區塊鏈應用平台的發展，例如 MaiCoin(現代財富科技)。詳述如下。

一、區塊鏈在金融業的應用

目前國內富邦、國泰、玉山、中信等四家金控分別透過催生帳聯平台、串接電子病歷、建構支付場景、評估加入國際組織，富邦率先宣布要籌組區塊鏈金融聯盟，後來更支持成立了臺灣第一家商用企業區塊鏈公司。富邦金控成立帳聯網路科技公司（AMIS），邀請國泰、台新、中信加入增資成為 AMIS 股東、或只使用服務，目的在讓各金控子銀行的存款帳戶彼此相連，未來匯款與支付能更快更省成本。中國信託宣布加入 R3，還成立 50 人規模的實驗室，國泰人壽要用區塊鏈來結合電子病歷優化理賠作業。玉山金控則和臺大資工在校園實驗區塊鏈行動支付。財金更要號召臺灣金融機構共建區塊鏈平臺。區塊鏈這把金融變革大火，不只在國際蔓延四方，現在也燒進了臺灣，開始成了臺灣金融圈新一波的競賽場。

第一銀行率先針對供應鏈、洗錢防制、智能合約、電子禮票券履約保證、跨境融資業務與全球資金管理等六大面向積極發展，有效解決資訊流與資金流痛點並滿足監理所需，在區塊鏈領域中，可說是業界首次最寬廣與最深入的系統整合規劃。早在 2016 年初，第一銀行便已成立專案小組，並規劃打造「數位金融區塊鏈應用實驗室」，針對區塊鏈議題，定期討論戰略佈局與業務應用，為加速落實與發展，更攜手台大金融科技暨區塊鏈

中心廖世偉教授與其團隊，定期交流與合作；計畫從上百家客戶中，選出一家中心廠，展開平行導入與測試，透過平行導入策略加以驗證區塊鏈成效與提升客戶滿意度，這項創新計劃執行的結果，也引起業界高度關注。

華南銀行於 2016 年 10 月完成我國首樁區塊鏈技術的金融應用模型，命名為 HNoTe，是模仿比特幣的架構而建構[24]，但 HNoTe 不強調貨幣特性，內容可包含原生貨幣外產生之合約或其他通知事項，並開發 API 部分以執行指令，另建立錢包，與比特幣相同，可隨時產生帳號，主要傳輸應用面的訊息。HNoTe 目前為測試階段，暫時只開放內部員工以手機測試傳遞有價證券的交易訊息，使用者可以透過介面進行收付款、轉帳與交易資訊確認與查詢，同時還具備知識文件共享網站與資訊查詢的建置，可有效簡化銀行傳統交易的流程與風險。為了讓使用更便捷，華銀的區塊鏈還結合行動載具，將 HNoTe 結合行動裝置，用手機掃碼 QRcode 迅速串接交易畫面及結果，真正發揮區塊鏈「高安全、低成本、快速便捷」的應用綜效。

富邦金控在 9 月 20 日宣布要籌組金融區塊鏈聯盟，時任富邦金控的董事長蔡明忠表示，要用區塊鏈技術來串連銀行間的支付交易，簡化匯款與轉帳的流程，減少中央清算的成本。富邦自今年 3 月就宣誓建設「帳聯網平台」，由財富科技（MaiCoin）與工研院提供技術資源，採 Etheruem 的區塊鏈協議打造企業級應用。

中國信託在 10 月 12 日宣布啟動區塊鏈發展計畫，並且成為台灣首家加入金融區塊鏈聯盟 R3 的金融機構。中國信託表示，將要與全球多家大型機構一起鑽研區塊鏈的創新應用。另一方面，國泰金控則是打算將區塊鏈的信任特性應用在壽險領域，推出電子病歷，與長庚醫院合作線上調閱保戶病歷，提升工作效率與用戶體驗。

玉山銀行選擇與台大金融科技暨區塊鏈中心合作，應用該中心團隊所研發出的區塊鏈協議 GCoin，共組區塊鏈發展專案，打算在台大校園試行，

[24]訪談華南銀行 HNoTe 研發團隊，完整記錄請參閱本研究報告附錄。

用區塊鏈促成校園的互連、互通、共享與共治。

另外值得一提的是，中央銀行唯一投資之民營事業財金資訊公司，也主導規劃籌備區塊鏈平台協助國內金融機構應用區塊鏈。財金公司過去主要承接跨行的業務資訊交換、跨行交易、帳務清算服務以及協助國內金融機構與國際組織連結，擔任銀行第三方的角色，一直以來扮演著國內金融機構之間的中介，其背後由中央銀行負責管理。此次財金公司組區塊鏈平台，是為了避免金融機構在區塊鏈上的重複投資，因此主導建構一個區塊鏈平台，並且共同開發共用規則，協助國內大中小型機構創造區塊鏈應用機會。

區塊鏈的興起，將打破傳統金流的架構，財金公司不僅扮演國銀體系金流串接最為重要角色，也直屬央行管轄，顯示區塊鏈的議題不僅受到央行、金管會高度重視，而且可望能夠獲得主管機關的支持開放。財金公司組建區塊鏈平台，主要讓所有銀行不分規模大小，都能將區塊鏈新技術擴大應用到金融服務層面。財金公司成立「金融區塊鏈技術研究與應用委員會」，國內有 46 家銀行、票券公司等各類金融機構加入該組織；此外財金公司在該委員會架構之下成立企業金融、個人金融兩種委員會，除選出區塊鏈「示範」業務之外，各銀行也將被分配投入資源建構該平台。除了銀行之間分工外，另一大議題，就是要選出各會員銀行認為最具迫切性的區塊鏈金融服務，作為試驗區塊鏈的標的。財金公司將請各個銀行建議各自認為應該應用區塊鏈的金融產品或服務來做概念性驗證(Proof of Concept，POC)。並且用選定的技術進行 POC，驗證交易安全性、速度、節點數要多少才適合等等。金融機構屬於高度監管對象，對交易的要求是絕對的安全、穩定，因此會在平台建立後，經過充分的驗證，產品才會上線。

2016 年底，已選定驗證項目，個金方面為公益捐款，企金方面為企業資金管理。驗證項目的選擇方式，主要考量可行性、貢獻度、以及創新程

度[25]。所謂可行性，是要評估這項業務的參與銀行家數多不多，另因目前區塊鏈技術未成熟，且規劃的驗證期間僅半年，不能找太複雜的業務，要短期能驗證、上線的項目，以負面表列方式選擇，排除目前區塊鏈技術做不到的高頻交易,以及由於涉及跨國司法管轄權、各國外匯管制標準不一、洗錢防制、找不到國外機構做驗證等因素，暫時先排除跨境業務；貢獻度方面要評估這項業務對銀行、民眾是否能提高方便性,及創新後業務流程、技術上可解決什麼問題。

對於採取何種區塊鏈底層協議，財金公司目前持開放態度，不排除任何區塊鏈技術，例如 Hyperledger 及以太坊各有優缺點，以太坊的本質是以虛擬貨幣來打造的區塊鏈技術，優點是其本身即為一信任機制，可解決網路信任問題，不需要中介單位，但這也是他的缺點，因為金融機構有監理問題，不太可能完全使用匿名交易，目前以太坊有在研擬要將匿名改為實名，但還需要時間；Hyperledger 的優點是實名制、認許制，剛好符合本國金融支付要求，且很多大型金融機構皆有參與，未來業務延展性較佳。技術在發展階段，無法確定未來主流平台，所以不排除任何區塊鏈技術平台，對金融機構而言，「學習」才是目前的重點。

財金公司指出，發展區塊鏈需要資金，也需要規模經濟支撐，現在已有多家銀行相繼投入區塊鏈的研究，但許多銀行礙於資金與規模經濟問題，不易投入區塊鏈的領域，也難以運用區塊鏈的技術提供更有效率的金融服務。平台的成立將能匯聚資源幫助中小型的銀行在區塊鏈發展上不落人後，財金公司所搭建的平台將可望提供銀行集體發展區塊鏈的機會。

二、底層區塊鏈協議的建構

台大金融科技暨區塊鏈中心是由在台灣積極推動區塊鏈技術研發的台大資工系廖世偉教授[26]領導，在 2015 年年底時，全世界開發出來的區塊鏈

[25] 研究團隊訪談財金資訊公司黃昱程副總經理，完整記錄請參閱本研究報告附錄。
[26] 廖世偉教授原任職於 Google，曾因對 Android 平台的開發貢獻而榮獲 Google 創始人獎。他離開 Google 總部後，回國加入台大資工系，率領學生投入區塊鏈技術研發。

原始碼僅僅只有五個，其中之一就是由台大新創團隊自主研發的台大區塊鏈技術 G Coin，G Coin 也成為台灣第一套自行開發的區塊鏈協議。

區塊鏈的生態體系可分為底層協議、服務供應商以及區塊鏈上層的應用，如比特幣、Ripple 和 G Coin，都是最底層的區塊鏈協議。而由部分 G Coin 團隊成員組成的 DiQi 則是區塊鏈服務供應商，有些服務供應商會自己開發一套區塊鏈，有些則拿現成的區塊鏈協議來修改，再提供 API 或是服務給金融機構。位於區塊鏈生態系最上層的則是區塊鏈應用平台，如比特幣交易所、美國 NASDAQ 所採用的 Linq 交易平台。

G Coin 區塊鏈開源釋出後引發國內各界的高度關注，銀行、科技大廠和新創團隊都積極想要搶進這個領域。本節接下來即以 G Coin 為核心，檢視目前台灣區塊鏈技術的進展[27]。

根據第二章的說明，我們已經知道「區塊鏈技術」由密碼學、數學、演算法及經濟模型所組成，結合點對點的網路關係（P2P），並採用分散式共識演算法，來解決傳統分散式資料庫的同步問題，可說是一套整合跨領域技術的基礎建設。「區塊鏈」本質上是一種「分散式共享帳簿」，由網路系統中的參與者集體維護，屏除中央集權的金融機構層層驗證，卻能確保交易安全與正確。

以金融應用為例，其運作原理由多個節點組成一個網路，當某一個節點要發起一筆交易時，會先將交易廣播給其他節點，此時所有節點都可以經由共識演算法來決定誰可以驗證這筆交易，而這個取得共識的過程（比特幣區塊鏈稱作挖礦），就像是讓所有節點一起來解一道數學題。

各節點解題過程中，驗證中的交易資料會被打包至區塊裡，並透過嚴格的密碼學規則來保護，一旦區塊中的資料遭到竄改，或不符合密碼學規則時，該區塊便會失效，無法完成交易驗證。

[27] 改寫自辜騰玉(2016)，「3 大面向一次搞懂區塊鏈，美國 NASDAQ、跨國銀行都搶著用」；及本研究團隊與廖世偉教授訪談內容。

當其中一個節點先解出題目時，便由該節點將驗證過的交易寫進區塊鏈中，並廣播通知其他節點。而資料一旦被寫進區塊鏈之中，便無法再被竄改。這樣的機制讓所有節點能共同維護一本帳本，並由每次最快解題完成的節點來負責記帳，以確保公平性，一旦有人入侵網路想竄改帳本紀錄，也會立刻被發現。

在區塊鏈出現之前，大部分的網路交易都仰賴金融機構作為可信賴的第三方。在這種基於信用的模式下，所有交易資訊的提供與存儲都被掌握在第三方手上，交易者對於第三方必須完全信任，並且無法參與驗證。

2008 年出現的比特幣區塊鏈技術，是一個去中心化交易平台的概念性驗證，其採用密碼學技術來控制貨幣的生產和轉移，屬於一種加密電子貨幣，比特幣可經由挖礦的過程產生，並讓所有參與者透過驗證交易和記錄來獲得比特幣，使得支付的過程可直接由一方發起，並支付給另一方，中間不需要再通過任何金融機構或第三方機構。

不過，比特幣只是其中一種區塊鏈技術應用，區塊鏈最重要的核心創新在於其算法算力，也就是共識演算法，而不同的區塊鏈技術採用不同的共識機制。事實上，想要直接將比特幣的交易體系移植到金融業，尚存在許多問題，例如確認交易需要耗費十分鐘以上，這樣一天下來無法完成多少交易；工作量證明演算法浪費過多資源，大幅提高成本等等。要將區塊鏈擴充到一般的金融體系，勢須經由底層技術予以調整，使其有別於傳統的比特幣區塊鏈，例如：比特幣區塊鏈可以自由加入，只需在電腦或行動載具上下載軟體即可，這種可以自由加入的區塊鏈稱為「公鏈(public chain)」；相對於公鏈，對於加入資格設限的區塊鏈，則稱為「私鏈(private chain)」。由多家銀行組成的區塊鏈聯盟 R3CEV，就是一種私鏈。

由於比特幣區塊鏈技術開源，大家都可以拿來修改成自己的版本，或是重新開發一套新的區塊鏈，如台大目前開源釋出的 GCoin、Linux 基金會的 Hyperledger 和 Ripple，都是不同於比特幣的新區塊鏈協議，這些區塊

鏈和比特幣區塊鏈已經大不相同，這裡我們便以比特幣區塊鏈和 GCoin 區塊鏈作為主要比較對象，並分別從效率面、安全面、法規面檢視。

效率面可從結算速度來看，理論上比特幣區塊鏈每秒可處理的交易筆數（TPS）為 7 筆，每 10 分鐘可完成一次結算，而 GCoin 區塊鏈則 15 秒就能完成一次結算，大幅改善了比特幣的結算速度瓶頸。區塊鏈的結算速度在第一個區塊產生時就會先設定好，而這個時間取決於驗證題目的難度及網路節點的運算能力，要在兩者之間取平衡，但是，如果將結算時間設定的太短，容易產生分叉情形，也就是各節點沒有取得一致的共識，導致帳本不同步。

此外，參與節點數、交易廣播到各節點的速度也都是影響因素。如比特幣這種非實名制的區塊鏈，因為強調公平性，因此有太多節點同時一起解題，必須花很多時間在決定驗證者的階段。而像 GCoin 這種實名制區塊鏈，儘管結算速度已經遠高於比特幣，但在廣播的機制上仍然會遇到一定的效能瓶頸。因此，若要縮短結算時間，不只要修改最開始的區塊，還得解決分叉的問題，而 DiQi 研發的動態難度調整技術，便是為了要降低產生分叉的機率。

從安全面來看，動態難度調整技術也解決了比特幣的安全隱憂。比特幣區塊鏈設計的一大問題是，如果區塊鏈網路中有人掌握了 51%以上的運算能力，也可說是過半的運算資源，就有可能會破壞區塊鏈網路的安全性，掌握交易驗證權利，就是所謂的 51%攻擊問題。因此，DiQi 調整許多參數，也花很多時間做演算法優化，讓各節點仍具有公平的驗證機會，確保即使有人壟斷大半的區塊鏈網路運算能力，仍無法掌握每次的交易驗證權。

簡單來說，比特幣原本採用的工作量證明做法（Proof of Work），像是發同一道題目給大家解，誰先解出來就有驗證交易的權利，而 DiQi 改用動態難度調整技術後，就是透過演算法分發不同難度的題目，如果節點運算能力較強，一直取得驗證權力，就給較難的題目，這麼做可提升公平性，

讓各節點都有機會算出答案，而不被少數人掌握。

以前的網路沒有透過算法算力來保護，像是傳遞郵件的過程都可能被竄改，但在區塊鏈中，受到密碼學和數學保護，其安全加密機制即使是當今運算速度最快的電腦天河二號，也得花相當於 250 兆年（2 的 48 次方）的時間才能破解，以目前的科技來說，區塊鏈是足夠安全的，並具有可追蹤性與不可竄改的優勢。

再從法規面來看，這也正是比特幣區塊鏈與非比特幣區塊鏈最大的不同之處。由於比特幣是一種虛擬貨幣的應用，因此面臨各國法規的限制，但區塊鏈本身可結合認許制或其他方式來管控節點，決定讓哪些節點參與交易驗證及存取所有的資料，並提供治理架構（Governance Structure）及商業邏輯（Business Logic）兩大關鍵特性。事實上，GCoin 的 G 便具有 Governance Structure 及 Global 這 2 層涵義。

目前區塊鏈可分為非實名制和實名制兩種，前者如比特幣區塊鏈，後者如 GCoin 區塊鏈。GCoin 區塊鏈目前已經可做到認許制 (Permissioned Blockchain)，能配合金融監管所需的反洗錢 (AML) 與身份驗證 (KYC) 規範。

銀行和金融機構想採用的都是實名制的區塊鏈，為了滿足金融領域的應用需求， DiQi 團隊從去年開始，開發新的區塊鏈架構，要讓區塊鏈上的節點具有不同的身分，包括聯盟（Alliance）、發行者（Issuer）及一般使用者（或稱錢包），其中，只有聯盟成員才具有驗證交易的權力，各個發行者可產生資產，而一般使用者則指用戶或錢包。

在結合認許制之後，若善用區塊鏈的不可竄改性與可追蹤性，區塊鏈將是政府建立可管可控的 IT 基礎建設時的一大利器。若想要應用在現實世界中，確保交易紀錄的安全性及可追蹤性，就必須採用實名制才能運作，如臺灣的自然人憑證便採用實名制。而比特幣並非實名制，無法與現實世

界融合，大家都看得到公有金鑰，但不知道這把金鑰對應到哪個人，沒辦法追蹤交易來源對象。

實務上原本存在兩種信任體制：一種是相信政府或大公司的中心化系統;另一種是只相信自己,也就是所謂的分散式系統,基於零信任基礎下，每個人都擁有完整帳本，如比特幣區塊鏈，但這樣衍生多餘性和複雜性，不僅每個節點都可看到完整帳本，在交易傳遞上也因此較為複雜。因此現在出現了第三種選擇,可視為一種截長補短的複合型體制,也就是如 GCoin 這類的新一代區塊鏈，不僅做到去中心化，同時藉由認許制來控管節點的身分與驗證權力。

三、非金融業者發展的區塊鏈應用平台

目前非金融業者在台灣發展的區塊鏈應用平台，大概以 MaiCoin 的知名度最高。MaiCoin 是一站式的數位資產交易平台，提供用戶以新台幣買賣兌換比特幣、以太幣，基本上就是一個虛擬貨幣交易所。依據其網頁上的介紹，MaiCoin 的現有服務包括：即時兌換、電子錢包以及商家服務。每個用戶(沒有年齡限制)皆可免費申請一個 MaiCoin 帳號。

MaiCoin 除了是台灣第一個比特幣買賣交易平台，更積極推動實體商家採用比特幣付款。由於看好目前台灣的支付市場需求，MaiCoin 想藉區塊鏈來解決目前支付系統無法跨領域的問題，以加速區塊鏈應用在台灣落地[28]。MaiCoin 體認到儘管全球銀行積極投入區塊鏈技術，但要在受高度監管的金融產業中導入區塊鏈應用，取代既有金融業務模式或支付系統，並不是件容易的事。台灣支付市場最大問題是，各種錢包之間無法整合，尤其行動支付領域特別明顯，現有金流往往只能單向運行。

過去買賣雙方的交易通常有銀行或第三方作為交易中間人，來解決彼此之間的信任問題，而銀行能做的事包括處理訊息流以及錢的保管，但現

[28] 本小節部分內容摘錄改寫自辜騰玉(2016),「臺灣新創 Maicoin 切進主流金融支付市場，靠區塊鏈處理跨領域資訊流」。

在大家對銀行的印象卻只停留在錢的保管，忽略了處理訊息流帶來的價值。但這種金流與訊息流整合的作法，往往會走向中心化架構。因此 MaiCoin 開發區塊鏈 API，協助國內銀行與商家導入區塊鏈技術應用，但並非要完全取代現有的金流系統，而是靠區塊鏈來處理跨領域的資訊流，再與既有的金流支付系統整合。概念是將資訊流與金流拆解開來，訊息流部分藉由區塊鏈技術來做點對點的資訊交換，產生無數交易後，結算部分由於需透過法定貨幣來完成，因此每天再經由銀行之間做一次結算。至於現金流還是採用傳統金流系統，商家或消費者要進入區塊鏈進行消費，需到相對應的銀行進行儲值後，才能在區塊鏈上交易，與商家進行交易完成，之後商家再與相對應的銀行來做清算。對銀行來說，除了既有金流系統之外，需增設另一個與區塊鏈串連的節點，靠媒介來讓消費者儲值後，便能在這整個區塊鏈帳聯網上進行交易。

MaiCoin 採用 Ethereum(以太坊)區塊鏈協議，打造一套私有區塊鏈，並訂定 API，提供給銀行及商家，替商家增設區塊鏈節點。銀行的節點較特別，只有銀行能做儲值跟兌現。選擇 Ethereum 主要是因為它有比較完整的寫智慧契約功能，可用涂林完備(Turing-Complete)的程式語言來處理較複雜的合約內容，更能處理跨領域的政策需求。

第二節 區塊鏈及數位貨幣為金融業帶來之商機與挑戰

區塊鏈擁有「去中心化」、「加密安全性」、「不可竄改性」、「可追蹤性」、「匿名性」等特色，因此凡是在某一程序中出現太多的中介參與，或是過高的中介成本，或者有低追蹤成本和高資訊安全的需求，都可能潛藏著區塊鏈技術的用武之地。除此之外，區塊鏈可以通過減少勞動密集過程和消除重複工作而節約成本。區塊鏈的數據透明性、安全性和系統的高效性使之可以被應用於很多領域，甚至產生一種全新的商業模式。

目前多家銀行積極投入區塊鏈產品的應用研究，包括數位貨幣、交易訊息（Message）、確認函（Confirmation letter）、通知郵件（Notice）、議價（Price Negociation）、日記帳（Ledger）、智慧合約(Smart Contract)、智慧資產載入(Smart Asset)等等，區塊鏈技術的應用將會愈來愈寬廣。透過區塊鏈金融的串聯，金融消費者將可獲得更好的服務，除了所有的交易時間及成本大幅減少之外，各銀行之間更將因為區塊鏈金融的合作產生新的交易協定。目前金融業對於區塊鏈最有共識的運用項目，包括與跨境匯款相關的跨境貿易融資、帳戶及交易資料查詢、信用卡紅利積點的跨銀行共同兌換、飛機航班延誤險等保險辦理、區塊鏈平台資訊共享等，這些都是金融業對於區塊鏈金融業務最為看好的項目。

接下來我們打算討論幾項區塊鏈為金融業帶來的可能商機與挑戰，必須強調的是，限於篇幅及目前所能獲取的文獻，此處僅針對目前較受關注的幾個面向介紹，然而區塊鏈的應用場景，以及隨之而來的衝擊，將隨著時間經過而愈趨多樣難測，金融業者面對此一充滿爆發力的新金融科技，允宜緊盯其發展趨勢。

一、跨境支付與外匯交易

如果沒有區塊鏈，那麼非面對面的支付、匯兌、或者任何金融價值的傳輸，幾乎總是必須透過受交易各方信任的中介機構，來完成金融價值傳

輸的流程，有時還需要不只一個中介機構。每多一個中介機構，就會多一筆費用。因此銀行間(尤其是涉及跨國的銀行間)的結算，不僅手續繁瑣，而且成本高昂。

區塊鏈分散式的統一帳本和點對點的特徵，能提升效率、節約成本。不少金融科技的創新者，都在試圖跨越現存的金融中介機構，建立全新的「點對點」交易規則。據估計，區塊鏈技術能在國際支付業務中，節省約150 億到 200 億美元的交易成本。

外匯交易的市場風險很大，一般的交易流程如下：交易的一方將資金轉給中間商，如外匯結算服務商；外匯結算服務商會一直持有交易初始方的資金，直到交易對方提供資金。這一流程的問題是，初始方的資金直到結算完成，都會凍結在特定的交易中，而整個過程往往需要耗時一天。區塊鏈的功能是帶來「近實時」的交易，提升外匯交易市場的清算速度。過去的一年多裡，銀行業者一直嘗試利用區塊鏈技術縮短交易到清算的時間，同時讓成本更低，不過多數項目仍處於起步階段，例如瑞銀集團與 Ripple 的合作。但根據高盛申請專利之文件中的表述，這些系統有其缺陷，特別是在受高度監管的金融服務中。高盛指出，這些系統在隱私方面存在問題，如同任何人都能看見比特幣區塊鏈上的任何交易，如果銀行區塊鏈完全透明，那競爭對手就能為某一交易做出反向交易。比特幣與 Ripple 也缺少身份認證機制，無法幫監管者查處反洗錢活動。高盛希望綜合區塊鏈的優點（主要是速度與效率），但改善處理隱私的技術，並符合金融監理規範。例如，高盛版本的區塊鏈允許私人交易，僅讓需要知道的人得以看見；也允許監管者獲取數據庫，並符合反洗錢法案的規範。

以區塊鏈來改善跨境支付與外匯交易的程序，可以看成是比特幣區塊鏈概念的直接應用：所謂跨境支付與外匯交易，本質上就只是價值的交換，只不過這時價值的載體不再是比特幣。然而此處有一個問題：在這種處理跨境支付或外匯交易的區塊鏈上，誰來負責原本比特幣區塊鏈上礦工的工

作？因此實務上比較可行的做法，是將處理跨境支付或外匯交易的區塊鏈架構在比特幣區塊鏈上，仍然由比特幣區塊鏈的礦工來驗證交易的合法性。

二、供應鏈金融

先看一個近期發生的相關案例，地點在中國大陸，但因受官方刻意壓制，整個事件的來龍去脈並不十分清楚，僅能經由外國媒體的報導拼湊出一些輪廓。

總部設立於中國大陸青島的德誠礦業有限公司，主要經營鋁土礦、氧化鋁以及一些銅精礦的進口業務。2014 年，德誠與四家不同的倉儲公司分別出具倉單，利用銀行間訊息不對稱的漏洞，去不同銀行重複質押，造成實際的銀行貸款缺口可能超過 10 億美元。此種詐騙模式的操作是由做為第三方的倉儲公司夥同往來企業，針對同一批貨物，開具多張倉單，然後由企業找上不同銀行，必要時勾串銀行授信人員，向銀行質押騙取多筆貸款。以一批價值十億元的氧化鋁為例，通過在不同銀行的重複抵押融資，企業就可以輕鬆獲得二、三十億元甚至更多的貸款。據熟悉內情的消息人士表示，基本上每筆銅精礦或氧化鋁背後，都存在三、四次不同銀行的重複抵押，甚至有些極端的情況，同一批貨物在不同的公司、從不同的銀行重複抵押，實際獲取的貸款金額可放大十幾倍。

渣打銀行在上述案例發生後，即停止在青島港區周邊企業的金屬融資業務。這種金屬融資業務與我們習稱的貿易融資業務並不完全相同，但面臨的風險頗為類似：銀行要如何確定，貿易商沒有重覆使用貨物發票？

在傳統的貿易融資業務中，金融業者承擔的主要風險之一，即是銀行並不清楚客戶是否以同一張發票向不同銀行請款。若能以區塊鏈技術建立一套分佈式帳本系統，加入該系統的會員銀行每當收到顧客發票時，即將發票號碼輸入分佈式帳本，則基於區塊鏈的「可追溯性」，且每家會員銀

行均有完整的帳本，因此可輕易偵測出是否有發票重覆使用的狀況。區塊鏈的「不可竄改性」，則保證發票資料的真實無訛。至於信任機制的建立，可以由參與區塊鏈聯盟的銀行各自提供一個電腦節點確認紀錄；或者基於會員銀行間的彼此信任，乾脆省略挖礦機制。

如果不使用區塊鏈技術，而銀行要對每一張收受的發票向所有同業查核是否重複，可以想見必將耗費大量的成本與時間，實務上並不可行。如果是建立一個類似「發票中心」的資料庫統一管理，則無法保證資料不會被竄改，且一但遭受駭客攻擊，有資料損失或洩漏之虞，在資訊安全的強度上遠不如以區塊鏈技術建立的分佈式帳本。因此區塊鏈在貿易融資的業務上，確有其獨具的優點。

渣打銀行與星展銀行合作建構，貿易融資專用的分佈式帳本，目前已接近完成階段，正在尋求有意結盟的同業，預期不久的未來即將進行商業化運作。

三、反洗錢

在國際金融體系中，「洗錢」一直是個惱人的問題。世界銀行估計每年全球的洗錢總額高達美金 2 兆~3.5 兆，大約相當於全球 GDP 的 3%到 5%。即使各國的金融監理機關訂立各種反洗錢規範並督導銀行確實執行，但據信被揭露的洗錢金額遠低於真實的洗錢金額，恐怕還不到 1%，而多家銀行已為此被課以鉅額罰款。若計入這些罰金，粗估全球金融業每年防制洗錢的成本大約美金 180 億元。區塊鏈技術的成熟，可能可以藉由分散式帳本共享金融交易訊息，來簡化洗錢防制流程以提高效率。

防制洗錢的現行做法，主要針對兩點，一是監視可疑的資金流動，二是對新開帳戶進行查核。每當有新顧客上門要求開戶，銀行就有責任針對新顧客實地查核，確認其身分及該帳戶的受益所有權(beneficial ownership)，並與洗錢黑名單交叉比對。鑒於個人與機構帳戶所有權結構的複雜性，

KYC 的程序中充斥著人工作業。而針對資金流動的監控，銀行通常會使用外部軟體商提供的資料分析軟體，再以人工作業審視每日的可疑資金移動，約占總支付交易的 2%~5%，不過誤報率(false-positive rate)相當高，可能超過 99%。

由於缺乏銀行間共享資料的做法，造成各家銀行重複對同一顧客實地查核，浪費不少資源。而前述針對可疑資金流動監控之誤報率過高的問題，除了資料分析軟體本身不夠好，也很可能與缺乏足夠的資料判斷有關，以致虛耗許多人力。

區塊鏈技術有潛力改善反洗錢過程。首先，利用區塊鏈紀錄編纂帳戶詳細資訊，包括每一筆交易的細節，並儲存所有交易的歷史資料，基於區塊鏈的可追蹤性，這麼做可以提高交易監控的透明度和效率，從而降低偵測可疑資金流動的誤報率，節省人力成本。對銀行來說，由於每一顧客的所有交易資料都可被追蹤，應可更符合反洗錢規範，法遵成本得以降低。另外，藉由銀行間在區塊鏈上共享顧客資訊，當可有效降低 KYC 的成本。

四、大數據與區塊鏈的結合

在數據資源開發利用的過程中，大數據服務商都希望獲得更多的數據，讓政府和其他握有巨量資料的機構把數據開放出來，這樣才能去做數據的挖掘和分析。但是政府層面開放數據會擔心侵犯個人的隱私；民營企業則擔心洩漏商業的秘密；許多機構亦把數據資源當成是奇貨可居的重要資產，都不會輕易開放出來。因此，數據的開放、共享、交易、流通，沒有大家所期望的那麼簡單。從技術的角度來保障數據資源的開放和流通，而不僅僅是國家另立專法，或者政府制定制度、政策，需要其他解決方案，則數據需要一個可靠的載體。

區塊鏈正是一個可信任的載體，通過程序系統與演算法建立起一整套的信任機制；區塊鏈也是一種資料庫，它能夠記錄所有發生在各節點間的

價值轉移。也就是說，區塊鏈不僅幫助網際網路建立了價值的轉移，也建立一種可信的網際網路資料庫基礎。隨著區塊鏈得到各方越來越廣泛的運用，成為下一代 IT 基礎設施的時候，當越來越多的節點被連到了網際網路上形成物聯網，這些物聯網的節點通過某種契約關係形成智能化的合約或者智能化的資產，未來區塊鏈便可能成為萬物互聯的帳本。從這個帳本獲得的數據，不但數量龐大，且藉由區塊鏈的匿名性與加密安全性解決了洩漏個資或商業機密的問題，區塊鏈的可追溯性與不可竄改性則保證了資料的完整與真實，因此是產生大數據的理想來源之一。部分本國銀行已致力於大數據的開發與應用一段時間，區塊鏈的興起或將有推波助瀾之效。

五、其他

與當今銀行系統一樣，證券業也面臨交易手續複雜問題。傳統的證券交易，需要經過中央結算機構、銀行、證券公司和交易所這四大機構的協調工作，才能完成股票的交易，效率低、成本高。在高盛最新報告中估計，股票交易量中約有 10%需要一定程度的人工處理，而如果引入區塊鏈技術，這就完全沒有必要。區塊鏈的第一個證券業應用是美國證券交易所 NASDAQ 的實驗，NASDAQ 去年底推出了一個證券區塊鏈帳本 NASDAQ Linq，可以用來將私有股權的交易記錄數位化，追蹤交易的時間可以大幅縮短到幾秒鐘之內就可以完成，最顯著的好處就是減少了清算交易的成本。

區塊鏈也可以助群眾募資一臂之力。群眾募資的主要風險，除了投資計畫本身可能失敗之外，募來的資金是否妥善應用亦是關鍵。導入區塊鏈之後，募資的金流及提撥的金額都記錄在區塊鏈上，讓每筆交易皆可稽查及可追蹤，使金流更透明，且無法竄改。如此一來，應也有助於提高群眾募資的成功率。

另一個區塊鏈的熱門應用領域是智慧合約（smart contract），能將契約數位化並自動執行與維護。智慧合約概念源自於 1994 年，由尼克・紹博

（Nick Szabo）所提出。智慧合約之所以稱為智慧，係因其比傳統的合約向前邁進一步，亦即能夠實際執行資產所有權於特定條件下轉讓的管理與控制。智慧合約為一套以數位形式定義的承諾（promises），包括合約參與方能在區塊鏈上面執行這些承諾的協議。數位形式意味合約可自動化執行電腦可讀的代碼，因為只要參與方達成協定，智慧合約所建立起的權利與義務即能強制性執行，而不需要值得信賴的第三方仲裁（arbitrator），讓人們能通過互聯網與陌生人進行資產的交易 （transaction），以實踐價值互聯網的境界。未來企業各種形式有價值的智慧資產或數位資產透過去中心化的區塊鏈來決定資產的所有權，而資產所有權的管理藉由區塊鏈智慧合約的演算法來自動執行，並且可以在約定條件下自動觸發所有權協議的執行。

六、小結

可以預見，區塊鏈應用技術將會愈來愈寬廣。透過區塊鏈金融的串聯，金融消費者將可獲得更好的服務，除了所有的交易時間及成本大幅減少之外，各銀行之間更將因為區塊鏈金融的合作產生新的交易協定。目前區塊鏈在金融業的主要發展方向可參見表 4-2-1。

【表 4-2-1】 區塊鏈金融目前發展方向

運用項目	方式	效益
跨境支付與外匯交易	跨境電子商務透過區塊鏈協議完成交易	交易雙方大幅降低成本時間
貿易融資	銀行組建聯盟共用分佈式帳本	會員銀行可即時查詢發票資訊以降低風險
人壽保險	推動登載於區塊鏈上	減少核保及理賠時間

	之電子病歷	提升客戶體驗
信用卡紅利積點兌換	各銀行可以互通信用卡紅利積點業務	擴大銀行間業務及共同行銷

跨境支付及外匯交易，應是最能看見區塊鏈成效的兩大業務，以往銀行在作跨境匯款時，都要透過押匯等手續來完成，通常得花上超過一天的時間，但引進區塊鏈技術之後，將可大幅縮短時間。區塊鏈能加速銀行後台清算，達到交易即清算的境界，連稽核手續都可節省。也就是說，區塊鏈使金流在市場更快更透明。另外，區塊鏈不但能幫銀行節省成本，還能化身金融創新的基石，除了打造行動支付、P2P 借貸平台，也能用於群眾募資、有價資產發行，乃至製造業用來改善供應鏈的效率。

從上述各類區塊鏈的應用不難看出，區塊鏈技術為銀行帶來的成效，多始於降低成本或降低風險，達到為銀行「節流」的目的；接著藉由提升客戶體驗，達成「開源」的效果。因此區塊鏈的應用，應可確實提升銀行的競爭力與獲利能力。區塊鏈對現在的金融機構來說，有點像是 1995 年網際網路剛出現的時候，若沒有進行產業升級便會失去競爭優勢，當大家都開始電子化，採用人工紙本作業的銀行就會被淘汰。同樣的，如果未來當大家開始進入區塊鏈時代，還在採用傳統資料庫的銀行，恐怕會因高營運成本而難以生存。

根據區塊鏈專家的評估，區塊鏈在台灣要進入商業應用的階段，大約還需要三年的時間，因為必須面對法規限制，以及整個完整的體系置換，體系內系統更新的每一個環節都必須審慎思量，反洗錢的系統也要照顧完善。他更表示，三年的時程是較樂觀的說法，前提是法規都配合的狀況。目前在區塊鏈金融政策法規方面，所提出之區塊鏈技術各項應用服務中，有相當大的比例需要針對現有的法規法條進行調整，我國監理沙盒(Regulatory Sandbox)機制目前進入修法階段，2016 年 12 月 19 日已通過立

法院財委會初審，凝聚七大共識，包括監理沙盒的精神融入金融八法中，修改的金融八法分別為銀行法、保險法、證券交易法、期貨交易法、電子支付機構管理條例、電子票證發行管理條例、證券投資信託及顧問法以及信託業法。

第三節 我國金融業如何因應區塊鏈技術之興起

經過第三章的敘述說明，吾人得以知曉台灣在區塊鏈金融應用或比特幣發展過程中並非先行者。然而從 2016 年開始，局勢有了轉變，金管會在 2016 年 5 月發布「金融科技發展策略白皮書」，也將區塊鏈與行動金融、雲端服務、大數據、生物辨識並列為五大基礎建設，顯見政府已體認到，金融業結合區塊鏈技術已是刻不容緩。我國金融業應如何因應？根據前述的麥肯錫 2016 年報告，金融機構可採取三種行動策略：(一)聯合其他同業組建/加入區塊鏈聯盟，諸如財金公司於 2016 年 11 月宣布籌備區塊鏈平台，已將國內 45 家大大小小的金融機構納入「金融區塊鏈技術研究與應用委員會」；(二)結合金融科技公司，發展核心業務的區塊鏈應用，諸如玉山銀行與台大資工系副教授廖世偉及其團隊所研發出的區塊鏈協議 GCoin 合作，共組區塊鏈發展專案；(三)銀行內部自行推動局部領域的應用，實施試驗計畫，例如中國信託商銀在 2016 年 10 月宣布設立行內跨事業群的區塊鏈實驗室。(四)銀行成立創客基地，聚焦在金融科技創新與區塊鏈的發展。例如第一銀行正規劃與學界共同成立創客基地，為有創意有實力的創業者提供更實質的創業場地與完整財務諮詢。接下來我們對此四種策略略作說明，並列舉台灣金融業者已採取之行動。

一、組建區塊鏈聯盟

關於金融創新或金融科技的推廣應用，以往是民間的動作比政府快，台灣金融科技公司曾多次呼籲政府對區塊鏈等新金融科技設置沙盒，並和其他區塊鏈技術公司合組區塊鏈聯盟。中央銀行轉投資的財金資訊公司在 2016 年 10 月 17 日發函給國內各銀行，表示將成立「金融區塊鏈技術研究與應用委員會」，為國內銀行業者搭建「區塊鏈平台」，由於係由有官方背景的財金公司主導，加以目前加入該聯盟並不需要特別繳交費用[29]，故已吸引 45 家金融機構加入。

[29] 相對地，中國信託商銀加入 R3 聯盟每年須花費 25 萬美元。

財金公司前身為金融資訊服務中心(金資中心)，過去在國內一直扮演金融機構之間的橋樑，也是金融科技創新的重要推手，主要承接跨行的業務資訊交換、跨行交易、帳務清算服務以及協助國內金融機構與國際組織連結，擔任銀行第三方的重要角色，其背後由中央銀行負責管理。是以本次由財金公司出面籌組區塊鏈平台，亦可說是金融主管機關協助國內銀行業者發展區塊鏈應用。

財金公司副總經理兼發言人黃昱程表示，為避免各家金融機構在區塊鏈上的重複投資，是以規劃由該公司出面創造一個區塊鏈平台串連國內金融機構，並且共同開發共用規則，協助國內金融機構創造應用機會。尤其考量國內金融機構規模大小不一，透過財金公司將業者結合在一起進行開發，可讓中小型金融機構也運用區塊鏈技術[30]。

黃昱程表示「目前全國 45 家銀行都已經加入委員會」，2016 年 11 月底會召開委員諮詢會來選定底層技術，2016 年年底以前將從國際上的主流技術，包含 R3 聯盟所開發的 Corda、IBM Linux 基金會旗下的 Hyperledger 以及以太坊三者之中選出主要平台，同時也不排除國內如帳聯網等相關技術，期望在一年內完成台灣金融區塊鏈。

11 月底的諮詢會另一個重點在於委員會要選定導入哪些金融產品進行概念性驗證。財金公司近期請各銀行建立他們認為應該進行 POC 的項目，可能的業務是供應鏈融資、跨境支付或貿易融資等，預計將在企業金融與個人金融方面各選出兩項產品，並且用選定的技術進行 POC，驗證交易安全性與速度，也驗證節點數要多少才適合等。黃昱程也表示，由於金融機構屬於高度監管行業，「外界對跨行交易的要求是希望接近 100%的安全、穩定，因此一定會在做完充分的驗證之後，才開始考慮試營運」。等明(2017)年底平台建立後，產品上線或試營運的項目才會明朗。

話說回頭，由於只有一年左右的準備時間，黃昱程坦言這是一大挑戰，

[30] 本段以下財金資訊公司部分主要引用改寫自沈庭安(2016)。

「內部導入技術需要流程，外部也有流程要走」。除了時間緊迫之外，還有技術的門檻，由於區塊鏈技術仍然很新，真正將技術導入到國內 45 家銀行機構內部，還是需要一定的門檻與時間。

面對外界區塊鏈的快速發展，黃昱程也分享他的觀察心得，「很多國內或國際上的發展，看起來都講得很多，但做得很少」。他觀察區塊鏈應用的實際內涵，其實成果並不豐碩，他也理解應用的難處。而區塊鏈的精神在這些應用的過程中不斷修正，導致一些核心精神的消失，甚至衍生出缺點來。因此，區塊鏈技術其實並不像外界所想的那麼完美。

除了前述的財金公司區塊鏈大聯盟外，富邦金控也宣布將籌組「金融區塊鏈聯盟」，成立帳聯網路科技公司(AMIS)，由 Maicoin 創辦人劉世偉擔任執行長，實際帶領 AMIS 研發團隊的工程副總林祐德，則是台灣區塊鏈早期研究者之一的政大資科系教授陳恭的學生。由於以太坊技術已有龐大社群，是以選擇以太坊作為基礎來發展自主區塊鏈平台，更邀請以太坊創始人 Vitalik Buterin 擔任顧問，目的在於讓各銀行的存款帳戶彼此相連，節省未來匯款與轉帳支付的集中清算成本，同時提高匯款支付速度。已邀國泰、台新、中國信託等金融同業加入，可以增資入股成為 AMIS 股東，亦可只使用該平台之服務。

二、結合金融科技業者

玉山銀行在國內金融科技的發展，向來是處於領先的腳步。本次區塊鏈的浪潮也不選擇缺席，該行在 2016 年 5 月宣布與台大資工系副教授廖世偉及其團隊所研發出的區塊鏈協議 G-coin 合作，共組區塊鏈發展專案團隊，研究試驗方向包含支付、帳聯網、智能合約與供應鏈金融等，第一步將先在台大校園的封閉小環境試行小額支付等應用。玉山除了 IT 團隊成員加入外，業務團隊成員也會加入此一專案團隊。

值得一提的是，與玉山銀行合作的「台大金融科技暨區塊鏈中心」，成

立於 2016 年 3 月，是台灣第一個金融科技暨區塊鏈中心。該中心成立召開記者會時，行政院科技政委鐘嘉德親自出席記者會，業者包括新光創投董事長洪國超、歐付寶董事長林一泓也都出席表達合作意願。當時想找該中心合作的，不只第三方支付業者，國泰金控與玉山金控也都對區塊鏈技術表達高度興趣。甚至阿里巴巴集團主席馬雲，也親自前來台灣找廖世偉教授洽談。廖世偉教授同意無償授權 G-coin 技術，積極與業界合作，推動商業上的應用。

玉山銀行與台大金融科技暨區塊鏈中心的合作，以台大學生與校園商家做為區塊鏈應用的實驗場域其來有自。因國內目前一般非信用卡方式的手機支付，店家通常要 T＋2 日才能收到款項，透過區塊鏈技術，商家可像現金交易般快速收到款項，預計明(2017)年第一季可望發表應用成果。同時，玉山以台大校園做為區塊鏈前期應用的封閉環境，導入監理沙盒的實驗概念，未來也會把實驗結果回報給金管會，讓主管機關設計區塊鏈監理規範與制度參考。

此外，另一個值得關注的重點是相關的金融科技人才培育。為因應數位金融發展潮流，玉山銀持續推動培育數位金融人才的計畫，和各大學擴大合作培育人才且擇優延攬至玉山銀工作。尤其為爭取更多優秀人才加入區塊鏈的研究發展及應用，以及因應其他金融科技發展，今(2016)年擴大和台大的培育課程合作，期望藉此培育更多數位金融人才。

三、內部推動區塊鏈實驗與應用

中國信託銀行在台灣金融界而言，算是發展區塊鏈應用的先行者，除了前述的加入 R3 聯盟之外，也在 2016 年 10 月宣布成立「中國信託區塊鏈實驗室」，跟中華電信、台灣大學與政治大學的研究團隊一起投入區塊鏈技術研發，R3 聯盟全球協作實驗室負責人 Tim Grant 也親自來台表示支持。該銀行區塊鏈實驗室負責人李約表示，中國信託區塊鏈實驗室成員約 50 人，背景包含來自銀行、證券與保險等事業單位，分別專注在業務規劃、

資訊技術以及法令遵循上。中國信託所屬的跨國區塊鏈聯盟 R3 的成員也會加入實驗室，參與專案討論以及擔任顧問角色。希望將區塊鏈技術運用在跨境匯款、貿易融資、信用卡點數交換等方面。

中國信託在區塊鏈的未來發展規劃上，可以歸納出三個面向：其一為「跨境鏈」，與全球的金融機構進行跨國貿易、技術開發以及聯繫；其二為「境內鏈」，大致上是表現在點數交換或者轉帳支付上；其三則為「行內鏈」，行內各事業單位或者其他跨國組織目前也都利用區塊鏈來提升內部效率，包括資金調度的自由度以及洗錢防制等，如【表 4-3-1】所示。

【表 4-3-1】中國信託商銀規劃的區塊鏈分層應用

層級	應用
跨境鏈	跨境匯款、外匯交易、貿易融資、國際聯貸、境外信託
境內鏈	信貸、支付轉帳、財富管理、紅利點數、證券、保險、信託
行內鏈	行內資金調度、洗錢防制、認識客戶(KYC)

資料來源：中國信託，本研究整理

中國信託案例的啟發在於一家銀行可以同時採取多元的方式進行區塊鏈發展應用，不用針對前述三種發展策略三選一。中國信託區塊鏈實驗室負責人李約經理表示，該行的區塊鏈實驗室已經籌組一年，原本預期行內鏈將是最快達成的應用領域，但加入 R3 後，相信跨境鏈層級跨境支付的進度將大幅提前，有可能比行內鏈、境內鏈先行。而原本外界預測區塊鏈的全面商轉時程也將從 2020 年提早到 2019 年甚至 2018 年底。另外一件值得留意的事，有其他金融同業及金融科技業者質疑中國信託不加入本土

的區塊鏈聯盟，卻每年花費 25 萬美元在國外的區塊鏈聯盟，中國信託總經理陳佳文表示，該行並不排除加入國內的聯盟，然區塊鏈不能只侷限在國內，「因為區塊鏈不能自己玩，確實加入國內聯盟，匯款給富邦、國泰等金融機構會變得很簡單，但是加入國外聯盟的話，對技術提昇，與金融的國際化，是必要的一步」。

當然，區塊鏈除了方便金融業本身的交易進行或節省成本外，也可運用在相關的跨領域使用上。國泰金控旗下的國泰人壽正規劃把區塊鏈應用在電子病歷上，讓理賠作業與保險商品開發更有效率。由於國泰人壽關係企業國泰醫院目前僅與長庚醫院合作線上調閱病歷，國泰人壽若想調閱保戶在其他醫院的資料，仍須靠人工處理，有的醫院即便看到客戶同意書，也可能基於個人資料保密等因素，不便提供客戶資料。國泰人壽正是希望基於區塊鏈的信任機制，突破現有問題。

四、成立創客基地

擅長企業金融的第一銀行，近年來提供企業客戶供應鏈融資、銷售鏈融資、價值鏈融資等創新服務，協助大中小型供應商與銷售通路最直接的資金挹注。最近，第一銀行將再融合區塊鏈底層技術，多鏈接軌，不僅規劃區塊鏈與支付結合，更計畫整合企業上下游金融應用、跨境融資與全球資金調度管理等業務。第一銀行指出，區塊鏈的特色應是「動合無形，贍足萬物」，將以不著痕跡的方式提供在各項客戶服務之中。金融與科技融合只是過程，隱藏效益也並非都顯而易見，然其背後能解決金融問題與提供附加價值才是真實而有意義的。

目前第一銀行已規劃與學界共同成立創客基地，聚焦在金融科技創新與區塊鏈的發展，將為有創意有實力的創業者提供更實質的創業場地與完整財務諮詢，希望藉由產官學合作激盪火花，打造出創新的金融業務模式，協助育成優秀的新創團隊，並鼓勵新創人才加入第一銀行的實驗室，藉由雙方的交流，激盪出各式創新服務，共創雙贏。

類似創客基地的做法，在國外多有實例可循，只是未必與銀行合作。以新加坡為例，創投公司 Life.SREDA 旗下之新創公司即以金融科技為發展主力，其中當然包括開發區塊鏈應用的新創事業，例如 Otonomos 致力提供線上財務、技術及法律服務予企業，採取區塊鏈技術，協助企業運用分帳式資料處理愈來愈多資料記錄，並防止被竊取與篡改，企業透過 digital share wallet 的申請使用，迅速達成 P2P 的股權移轉，以吸引共同創辦者、私人投資或大眾資金，並運用區塊鏈技術自動更新企業的資本結構表，協助企業管理公司。而加密技術則有助建立公司安全的資訊系統、股份轉讓、董事會投標決議等，提供企業一全新的數位秘書服務系統。再如 Quoine Exchange，是新加坡一家提供比特幣交易和其他加密貨幣相關服務的新創公司，以亞太地區為標的，其商業模式係採取 B2B2C（business-to-business-to-commerce），為比特幣交易提供後端引擎。目前主要市場在日本，為日本最大的比特幣交易中心，並且在世界領域也是名列前茅，從成立之初的日元計價交易開始，現已拓展至美元、歐元、新加坡幣和港幣等十種貨幣。

新加坡政府以國家的高度，替新創產業提供場域，作為新創產業之育成中心，成立類似美國矽谷之 LaunchPad 新創企業聚落生態體系（ecosystem），目前該聚落位於「BLK 71」、「BLK 73」和「BLK 79」等三座大樓(前述創投公司 Life.SREDA 以及其旗下之新創公司即設立於此)，可租用面積約 30 萬平方英尺，鄰近新加坡國大學(NUS)、科技園區、生技園區及媒體園區，且比鄰新加坡標新局（SPRING，負責中小企業）及新加坡科研局（A*STAR，新加坡國家級研發機構），為新創企業發展提供了完整的生態體系。政府單位中以新加坡標新局負責提供財務諮詢，其亦與民間共同設立「SPRING SEEDS 種子基金」，協助新創企業發展。新加坡政府為促進該國金融科技的創新，於新加坡金融管理局(MAS，即新加坡中央銀行)設置一筆新幣 2 億 2,500 萬元(約合新台幣 56 億元)，為期五年的專款，用來補助新創業者成立實驗室的人力費用。執行程序上先由業者支付

研發人員薪水，再向政府申請專款補助，換言之，實際由政府(部分)負擔科技創新研發人員的薪資成本。該項政策之優點在於，直接將資金投入創新的關鍵要素—人力資源上。此外，新加坡政府在挹注資金直接投資的對象，並未限定該國企業，採取開放態度。這些做法，實堪我國政府借鏡。

五、小結

區塊鏈應用領域雖廣泛，但是台灣資源有限，且台灣金融環境長久以來存在過度競爭的境況，能否透過合作帶來事半功倍之效，端視經營者的策略考量。在推進區塊鏈技術應用方面，應審酌己身產業優勢與應用需求切入，金融業應密切注意國際機構其動向。

綜合前述因應策略，並檢視幾項國內金融業區塊鏈技術發展經驗，可以歸納出幾點發現心得：1.國內金融業在區塊鏈的實驗發展已經展開，現階段可說是各自努力發展，國際間三大技術平台 R3 Corda、Hyperledger與以太坊皆有其擁護者;2.導入區塊鏈應用技術不必拘泥於任何一種策略，甚至可同時進行；3.人才是金融科技發展的重要根據，國內金融業者對於培養人才以及與學校或國際現有技術團隊的接軌也應多所著墨。

此處必須強調，人才是金融科技發展的重要根據，因此科技問題同時也是人才問題，金融業對於區塊鏈的人才培育尤需特別重視。這是因為區塊鏈與其他大部分金融科技(例如行動支付)不同，區塊鏈本身只是一項技術，而該項技術並非僅針對單一特定金融業務，欲判斷區塊鏈究竟適合應用於何種金融場域，則必須同時對金融業與區塊鏈均具備相當程度的瞭解。即舉前述區塊鏈應用於貿易融資為例，非金融業出身的區塊鏈專家不太可能看出貿易融資業務潛藏著區塊鏈技術的用武之地；同樣的，銀行業者即便早已通曉貿易融資的風險所在，但如果對區塊鏈一無所知，自然也想不到植基於區塊鏈技術的解決方案。

區塊鏈技術的這項特性，一方面造成金融科技新創事業某種程度的進

入障礙，另一方面，這也恰恰顯示出金融業者培育相關人才的重要性。由於銀行的業務琳瑯滿目、包羅甚廣，而區塊鏈技術僅此一端，所以幾乎可以確定，區塊鏈這項金融科技在金融業的應用，不至於被科技業者壟斷，金融業將佔有一定的主導地位。事實上，最先看出區塊鏈可用於改善某項業務並具體執行的銀行業者，等於開闢出一片新藍海，巨大獲益可期；而隨著日後其他業者紛紛跟進，也將有助於整體金融業的提升。因此目前的當務之急，是必須增加金融從業人員對區塊鏈的認識。

對於金融業者如何培育區塊鏈相關人才，在知識經濟的時代中，有機會接觸新觀念的人員，當然是多多益善，但在考量控制教育訓練成本的前提下，我們建議可採取兩階段的作法：第一階段屬於策略面，第二階段劃歸執行面。

首先，針對行內中高級主管介紹區塊鏈，介紹的內容不必過於強調技術面(將基本概念解釋清楚即可)，最主要的目標是要讓這些兼具資歷與視野的金融專才，得以確實掌握區塊鏈的特性。一旦讓中高級主管確實掌握區塊鏈的特性，則搭配其豐厚的金融專業素養，就有可能看出應用區塊鏈在銀行業務(不論是改善傳統業務或創造新業務)的嶄新切入點，至少可以對區塊鏈技術的應用與發展，形成正確的方向感，在面對其他同業率先導入區塊鏈時，有能力思索自家銀行的因應之道。

倘若確定要將區塊鏈應用於某特定金融業務，則可針對該項業務相關人員介紹區塊鏈，及如何應用區塊鏈於該項業務的作法。可以想見，在推行這類革新時難免會遇到阻力，最常見的情形，是原本負責該項業務者不認為有改變的必要。所以此處所謂向其介紹區塊鏈，其實兼具溝通的功能，為能化解歧見，並有助於日後工作推動順利，介紹的內容可視情況加強技術面的深度，某些技術性的細節也須具體說明。

第五章 結論與建議

第一節 研究結論

區塊鏈是支撐比特幣系統運作的底層技術。比特幣的區塊鏈總帳是一長串的區塊,每一區塊是大約同時間發生的交易群組。只要系統持續運轉，這個鏈便無限制增長。一般來說，區塊鏈是指通過去中心化的方式集體維護一個可靠資料庫的技術方案。該技術方案讓參與系統中的任意多個節點，把一段時間中系統內全部資訊交流的資料，通過密碼學演算法計算並記錄到一個資料塊（block），並且生成該資料塊的「指紋」用於鏈結（chain）下個資料塊和校驗，由系統所有參與節點來共同認定記錄是否為真。區塊鏈在本質上是一種「分散式共享帳簿」，即每個參與節點都保管並隨時更新一份相同的總帳。

區塊鏈是跨領域技術的整合，涵蓋資訊安全、密碼學、經濟模型及算法算力，其中最重要的創新在於共識演算法的突破，使其被稱為「信任機器」(Trust Machine)。如果信任是主要的區塊鏈使用動力，銀行間已互相信任，為何我們還需要一個信任網路？答案是當檢視目前信任系統的經營成本時，會發現這些成本已變得過度龐大[31]。部分是因為法規造成，部分是因為各金融機構專用系統之間的複雜整合所需。

區塊鏈如何引入公鑰密碼學與數位簽署的技術，以構築其信任機制，亦為本研究報告的論述重點之一,詳細內容可參閱第二章。區塊鏈的特色，包括「去中心化」、「匿名性」、「不可竄改性」、「可追蹤性」以及「加密安全性」等等，其中「去中心化」堪稱區塊鏈最為核心的特性。基於上述的這些特性，區塊鏈能夠解決的問題包括：第一、在大家互不相識的情況下建立信用機制；第二、改善中心化導致的非技術方面成本過高的缺點，包括管理成本、組織架構的佈建等；第三、能使資訊真實透明可追溯，便於核對與審計，可以提高效率，但同時保護客戶的隱私；第四、記錄有時間

[31] 引述自 Mougayar(2016)。

序列的資料，例如交易確認、版權登記等。

區塊鏈的生態系可分為底層協議建構團隊、服務供應商以及區塊鏈上層的應用。如比特幣、Ripple 和 GCoin，都是最底層的區塊鏈協議。而區塊鏈服務供應商有些會自己開發一套區塊鏈，有些拿現成的區塊鏈協議來修改，再提供 API 或是服務給金融機構。最上層則是區塊鏈應用平台如比特幣交易所、或是美國 NASDAQ 所採用的 Linq 交易平台。

目前全球的發展狀況，區塊鏈投資主要集中在北美、歐洲，其次才是亞洲，且以中國為主。北美約有十幾家區塊鏈服務提供商，並且獲得當地金融機構與政府單位的重視，而台灣目前真正握有實際技術的區塊鏈服務商不多，大部分只是比特幣交易商。

過去一年多來，區塊鏈在我國雖逐漸受到高度重視，但截至目前均停留於概念性驗證(Proof of Concept)的階段，也就是許多產業對區塊鏈有興趣，正在試探它可能的應用方式。在進程上，區塊鏈 1.0 是加密數位貨幣體系，區塊鏈 2.0 是強調智能合約的金融科技，區塊鏈 3.0 則是物聯網。目前已經驗證的成果是金融清算以及加密貨幣的部分，區塊鏈 2.0 智能合約的商業應用還未被驗證，因此台灣目前的進展，應該是正由區塊鏈 1.0 往區塊鏈 2.0 的方向移動。

目前我國區塊鏈在技術發展上，已不同於比特幣區塊鏈每十分鐘確認一次交易，台大 G-coin 及國內部分銀行業者已可做到每十五秒清算一次，雖然仍不足以應付高頻交易，但已較比特幣區塊鏈速度快四十倍。此外，目前比特幣區塊鏈只要系統中超過一半以上的電腦達成共識，即可修正交易紀錄，台大 G-coin 竄改資料的難度遠過於此，必須達到 99.99%的參與者達成共識方能修改。由此可見，G-coin 的區塊鏈架構，更能配合國家監管需求，可兼顧交易效率與用戶資料安全。

區塊鏈或分佈式帳本交易處理系統，將為金融市場帶來巨大衝擊，最

直接的運用就是清算業務，可降低交易的複雜性，並有效監控諸如股票、債券等有價證券資產的交易過程。區塊鏈能加速銀行後台清算，達到交易即清算的境界，連稽核手續都可節省。區塊鏈不但能幫銀行節省成本，還能化身金融創新的基石。除了打造行動支付、P2P 借貸平台，區塊鏈也能用於群眾募資、跨境匯兌、貿易融資、有價資產發行，乃至製造業用來改善供應鏈的效率。

區塊鏈對現在的金融機構形成機會與挑戰，銀行若沒有進行產業升級，極可能失去競爭優勢。當各家銀行紛紛導入區塊鏈，此時還在採用傳統資料庫的銀行，恐怕會因相對較高的營運成本而難以生存。面對此種變局，對銀行來說有兩種選擇，一種是自己採用一套區塊鏈來提供服務，如美國 NASDAQ 所採用的區塊鏈平台 Linq；另一種則是和別人一起共用同一套區塊鏈，如全球 42 家銀行組成的區塊鏈聯盟 R3，便是想要找出一套大家都認定的區塊鏈，作為這些銀行之間的交易清算平台。

R3 聯盟提出了金融區塊鏈的概念，並完成了概念驗證，以清算貿易和 KYC 業務會是 R3 優先推出區塊鏈產品的項目。R3 運用區塊鏈的概念，但不是直接使用區塊鏈技術，而是改用分散式帳本技術來發展出適合金融系統每秒上千、上萬筆交易需求的專用平臺，解決擴充性問題以及提供權限讓各國政府機關也可以參與實施監理。目前 R3 也和其他區塊鏈技術建立互聯，可以支援各大主流區塊鏈技術。

當前的發展態勢已等同於進入區塊鏈的戰國時代，亦即各種區塊鏈協議逐漸成形，但行業標準尚未確立。由於區塊鏈有技術上的進入門檻，金融機構從理解區塊鏈，到接受區塊鏈，再進而發展出一套成熟的區塊鏈技術，真正應用於業務上以創造新價值，恐怕還需要長達數年的時間。目前的重點還是要著眼於實驗區塊鏈技術，展示區塊鏈的能力，並從中學習未來走向。

要使區塊鏈的商業應用廣為大眾接受，最重要的關鍵之一，便是使用

區塊鏈處理的交易，必須被認可具有法律約束力，並在法遵需求可接受的範圍內。而這牽涉到重新檢視記錄保存或法遵規則，或者至少得確保新法令不會讓各機構無法使用區塊鏈來執行這些交易。

總而言之，透過區塊鏈的確能夠解決一些問題，但也有很多問題是區塊鏈不能解決的。區塊鏈技術本身終究只是一項技術，重要的是金融業者想解決什麼樣的問題，而金融機構或是其他產業，採用這些技術來解決問題又能創造什麼樣的價值。發現銀行業潛在的需求，並找出真正需要靠區塊鏈技術或分散式分類帳所解決的問題，對國內銀行業來說才是最重要的課題，也是最大的挑戰。

第二節 建議彙整

如同前面章節所述，不論是區塊鏈或者其他科技金融的發展，相信都將帶來席捲全球銀行業的新浪潮，尤其區塊鏈的發展更是注重專業人才的投入，金融業者與主管機關都必須更快速地訂出發展計畫，以因應傳統金融產業科技轉型對台灣的衝擊。職是之故，本研究提出幾項重點建議[32]：

一、區塊鏈雖源於數位貨幣，推動金融科技應側重於區塊鏈技術

區塊鏈雖然與虛擬貨幣關係密切，但是與貨幣相關的議題，往往牽涉到國家的總體經濟及總體貨幣政策，因此對台灣的金融業來說，目前不需要投入過多關注在虛擬貨幣本身的發展。若以推動金融科技發展為主軸，則應該著重在區塊鏈技術本身。比特幣等各式虛擬加密貨幣，只是區塊鏈技術應用的一環，完全不能等同於區塊鏈技術。區塊鏈技術應用在銀行業務的空間很大，包括研究透過區塊鏈技術進行貿易融資、供應鏈融資、B2B跨境支付與交易後台結算業務等。

二、建立銀行業通用的標準創造區塊鏈技術最大效益

由於銀行業區塊鏈技術要發揮最大效益，建立一個大多數銀行業通用的標準至重要，如果必須大規模調整現有基礎設施，而區塊鏈技術能否真正成為銀行和企業交易的底層技術標準仍待投入研究，對銀行業來說更加需要審慎評估，且領導性銀行帶頭投入之後其他銀行是否跟進也是關鍵，然而 Fintech 公司已經積極投入當中，包括未來產業包括金融業透過區塊鏈技術將基礎設施轉移到雲端的趨勢，未來銀行業與 Fintech 的競合發展值得關注，包括 IBM 和微軟與國際性銀行的合作專案包括貿易融資、外匯結算、智慧合約等在未來二年將有實際成果，目前國內銀行業尚在整合階段，借助財金公司等機構的起頭中介角色十分重要。

[32]參考「從新興關鍵趨勢看金融業創新經營策略」(2015)、「台灣銀行業者發展亞洲區域銀行之研析」(2015)及「銀行業關鍵性人力資源供需之研究」(2016)等台灣金融研訓院研究報告。

三、金融業應積極培育區塊鏈相關人才

人才是金融科技發展的重要根據，因此科技問題同時也是人才問題。區塊鏈本身只是一項技術，而該項技術並非僅針對單一特定金融業務，欲判斷區塊鏈究竟適合應用於何種金融場域，則必須同時對金融業與區塊鏈均具備相當程度的瞭解。在考量控制教育訓練成本的前提下，我們建議銀行可採取兩階段人才培育的作法：第一階段屬於策略面，針對行內中高級主管介紹區塊鏈，介紹的內容不必過於強調技術性細節(將基本概念解釋清楚即可)，最主要的目標是要讓這些兼具資歷與視野的金融專才，得以確實掌握區塊鏈的特性；第二階段屬於執行面，在確定要將區塊鏈試行於某特定金融業務後，則可針對該項業務相關人員介紹區塊鏈，及如何應用區塊鏈於該項業務的作法，為能化解歧見，並有助於日後工作推動順利，介紹的內容可視情況加強技術面的深度，某些技術性的細節也須具體說明。

目前幾乎所有區塊鏈協議都是開源的，因此要取得區塊鏈協議的原始碼不是問題，重點是要找到好的區塊鏈服務供應商，協助導入現有的系統。而銀行、保險公司等金融機構必須對區塊鏈有一定的了解，才能知道該如何選擇，並應用於適合的商業情境。國內金融業者對於培養人才以及與學校或國際現有技術團隊的接軌也應多所著墨。由於台灣的金融科技發展較之部分歐美國家，仍有進步空間。是以建議金融業者除自行培養內部人才外，亦可考慮透過稅制優惠設法吸引國際間區塊鏈或相關金融科技專業人才，除了藉由引進國際專業人才帶來技術提升與相關管理制度外，也可做為國內金融業者發展金融科技的種子，透過與本地人才的交流，激發更多的創意與靈感。

四、透過區塊鏈技術推動銀行業、製造業及物聯網產業之可應用性

物聯網產業是我國五大策略新創產業的重點，物聯網業者可以透過區塊鏈技術監管智慧裝置與外部智慧網路裝置的互動狀況，確保智慧裝置的正常營運與智慧系統自動更新軟體與智慧派員維修程序，以及包括透過區

塊鏈技術控管食品安全履歷的建立等。銀行業方面，目前受限於「共識機制(Consensus)」,每筆交易都得獲得區塊鏈上的每一個成員同意才能生效。未來 Hyperledger 可以將共識機制改良為適用銀行業的機制，只要涉及交易者同意即可，不需要每位成員同意只需交易雙方同意即可生效，可讓一些小額 P2P 交易的執行效率更快。亦即未來因 Hyperledger 採開源專案的特性，銀行業及其他金融業、製造業、物聯網產業可以透過區塊鏈貢獻原始碼來創造出配合屬於該產業業特有特性的底層協定。

五、提高區塊鏈金融從業人員專業訓練與產學合作

與非金融業者競爭，區塊鏈在金融端的應用仍屬前瞻性的科技，需要學有專精的科技專才。為了吸引金融科技專業人才，薪資福利是重要的條件。例如台灣金融業從業人員的薪資水準相較於國際型金融機構或其他亞洲區域金融機構仍屬偏低。區塊鏈人才是金融資訊整合性專業的人才，也是目前各國金融機構競相追逐的對象，人數相對稀缺，建議台灣銀行業者適當參考國際薪資水準，逐漸提高金融科技相關從業人員待遇。尤其針對特殊專長或關鍵業務職位，則考慮儘快與國際水準接軌，避免因薪資福利而在人才競爭上無法與其他國外金融同業競爭[33]。

台灣要發展區塊鏈等金融科技，必須有更多金融科技的創新研發基地，建議金融業者可以與大專院校合作，透過大學院校研究中心延攬跨院、跨校、跨產業的優秀研究人才，仿效國外金融業者建立產學合作平台及創新實驗室，提供更多國際金融科技知識交流與創新研發成果分享，協助金融科技的研發創新工作，舉辦金融科技創新提案競賽，協助優秀創新方案盡快落實於產業實務運作中[34]。

六、金融業應追蹤區塊鏈的發展趨勢，並給予長期穩定的合理投資

並非所有銀行都必須在現階段投入大量人力財力發展區塊鏈，畢竟發

[33] 參考閻台生、彭勝本與謝順峰等(2016)。

[34] 本段內容引用改寫自王儷玲「解讀金融市場/發展金融科技」,經濟日報,2016 年 11 月 14 日。

展區塊鏈需要資金，也需要規模經濟支撐。但是我們建議，銀行對於區塊鏈技術的發展與應用，至少應有「長期穩定的合理投資」，如此才不至於在未來金融業配合區塊鏈轉型時受到太大衝擊。

區塊鏈應用領域極為廣泛，但考量台灣資源有限，且台灣金融環境長久以來存在過度競爭的景況，能否透過合作帶來事半功倍之效，端視經營者的策略考量。在推進區塊鏈技術應用方面，則應審酌己身產業優勢與應用需求切入，同時金融業者應密切注意國際金融機構及金融科技公司在區塊鏈技術與應用方面之動向。

七、面對區塊鏈技術興起，我國金融業有數種具體因應模式

第一、聯合其他同業組建/加入區塊鏈聯盟，例如財金公司於 2016 年 11 月宣布籌備區塊鏈平台，已將國內 45 家大大小小的金融機構納入「金融區塊鏈技術研究與應用委員會」；第二、結合金融科技公司，發展核心業務的區塊鏈應用，例如玉山銀行與台大金融科技暨區塊鏈中心所研發出的區塊鏈協議 GCoin 合作，共組區塊鏈發展專案；第三、銀行內部自行推動局部領域的應用，實施試驗計畫，例如中國信託商銀在 2016 年 10 月宣布設立行內跨事業群的區塊鏈實驗室。第四、成立創客基地，聚焦在金融科技創新與區塊鏈的發展，例如第一銀行正規劃與學界共同成立創客基地，為有創意有實力的創業者提供更實質的創業場地與完整財務諮詢。建議導入區塊鏈應用技術不必拘泥於任何一種策略，甚至可同時進行。

八、政府提出吸引與培育區塊鏈或金融科技相關人才建議

政府對於區塊鏈或其他金融科技之發展與未來趨勢也有相當認知，是以在民國 105 年 5 月公布《金融科技發展策略白皮書》，內容包含 4 大面向、8 大主軸以及 11 項施政策略，也納入區塊鏈發展相關議題，足見此一議題已然成為政府機關關切議題，經由具有央行背景的財金資訊公司出面號召成立本土區塊鏈聯盟更是一個明顯例證。當然，本計畫相信在區塊鏈

的發展上,仍有值得持續留意加強者,是以本研究在此對於整體金融產業、教育環境與政府提出吸引與培育區塊鏈或金融科技相關人才建議如下：

(一) 持續檢討與放寬引進優秀金融科技人才規範

隨著網際網路的發達與資訊的傳播便利，未來人才的流動將更全球化，更強調對外部環境的對應，隨著更多新世代投入職場，如何吸引外籍優秀區塊鏈或金融科技人才將是我國主管機關與銀行業者需要不斷調整因應之政策。考量提升人才戰力，他國已相繼提出新政策措施來吸引其他地區優秀人才，如法國針對有技術專長或特殊專長的人才設立「人才護照」;日本政府則推出「專業人才積分政策」,藉此吸引海外專業人才，期望可滿足國內的人才缺口，台灣若要再區塊鏈發展上有所斬獲，在人才吸引方面更不能掉以輕心。

(二) 強化金融業者、學校與培訓機構之交流合作

區塊鏈等科技金融人才的培育，並非單靠銀行業者或學校一方即可成功，是以本研究建議需要透過三方合作，整合金融業者、學校與金融培訓機構資源。尤其考量目前大專院校培養人財金融專業訓練不足，常被業者評論有學用落差，本研究建議部分大學可成立「金融科技學院」,在其中規劃設立金融區塊鏈學系或學程。規劃定位至少院級以上的學程，甚至是跨院的金融科技聯合課程。學校可以向國際取經，設計結合財務、資訊、營運與管理等各種科學的學程，並依校方資源調整資師資與課程，建立種子師資培育。

(三) 政府出面成立金融科技研究發展中心

建議政府出面整合既有學術機構、金融機構，金融資訊廠商，以及新創科技金融公司聯合成立金融科技研究發展中心或類似機構。金融機構可以提供金融領域的實地運作了解，提供專業技術性業師，挹注師資陣容。金融資訊廠商則負責能力提供財金、法規等方面的龐大數據庫(如倫敦帝國

學院與數據廠商合作金融監管科技)。政府方面則可設計提供稅賦優惠，或是專案的獎勵，給予協助發展區塊鏈技術的金融機構或金融數據廠商，協助減輕在成本以及授權上的負擔。

(四) 擴大國際交流，與國際 Fintech 課程接軌

考量目前國際上金融科技發展情況，歐美先進國家甚至中國大陸金融科技發展仍有值得台灣仿效之處，建議邀請各國金融或科技重要領袖，來台進行經驗分享。尤其是在國際金融機構工作的區塊鏈學者，以及全球成功金融科技新創專家。然而此工作耗費甚大，不易由台灣的單一學校可以做到，建議除可以由前述國家級金融科技研究中心協助邀請外，其他的國家級學術機構，如中央研究院，亦可以其在世界學術界的高度、國家級資源，引進國際級業師，進行深度的培育及布局。

(五) 政府可在推動區塊鏈應用上更為積極開放

政府可參考新加坡的作法，替科技金融新創產業提供場域，作為新創產業之育成中心，成立類似美國矽谷之新創企業聚落生態系；亦可同時與民間共同設立「種子基金」，協助科技金融新創企業發展；或設置一筆專款，用來補助科技金融新創業者成立實驗室的人力費用，直接將資金投入研發創新的關鍵要素—人力資源上。此外，挹注資金直接投資的對象，也未必要限定本國企業，可採取開放態度，以收廣納國際人才之效。

(六) 強化金融科技監理作為後盾

區塊鏈等前端金融科技的發展固然是幫助銀行提高獲利或載與科技金融業者競爭中扳回一成的動力來源，然亦須在後面設定保護傘，謹慎控制相關風險。如同玉山在台大校園實施的區塊鏈實驗場域般，建議政府在鼓勵發展區塊鏈等金融科技的同時，也不要忽略引進各國金融科技監理(Regulatory Tech)之發展經驗與技術，強化金融科技之監理效能，透過大數據分析與量化分析為資訊安全與風險管理做有效的把關，並儘快研擬配套以強化金融科技之法律遵循、資訊安全、風險管理與消費者保護。

參考文獻

1. Cruz, K. (2014), "The Truth Behind Truthcoin." *Bitcoin Magazine*, September 25.
2. Clenfield, J. and P. Alpeyev. (2014), "The Other Bitcoin Power Struggle." *Bloomberg Businessweek*, April 24.
3. ChinaLedger(2016)，《面向中國資本市場應用的分布式總帳白皮書》，2016 年 10 月。
4. Diffie, W. and M. Hellman (1976), "New Directions in Cryptography", *IEEE Transactions on Information Theory*, 22, (6), pp. 644-654.
5. Higgins, S. (2014), "Sidechains White Paper Imagines New Future for Digital Currency Development." *Coindesk*, October 23.
6. Hoffstein, J., J. Pipher, and J. H. Silverman (2014), *An Introduction to Mathematical Cryptography.* Undergraduate Texts in Mathematics, Springer Verlag, New York.
7. Hofman, A. (2014), "Bitcoin Crowdfunding Platform Swarm Announces First Decentralized Demo Day." *Bitcoin Magazine*, September 30.
8. Koblitz, N. (1994), *A Course in Number Theory and Cryptography.* Volume 114 of Graduate Texts in Mathematics, Springer Verlag, New York.
9. Mougayar, W. (2016), *The Business Blockchain.* John Wiley & Sons, Inc. (徐瑞珠譯，區塊鏈的商業應用)
10. Parr, C. and J. Pelzl (2010), *Understanding Cryptography.* Springer Verlag, New York.
11. Rivest, R., A. Shamir, and L. Adleman, (1978), "A Method for Obtaining

Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, 21, pp. 120-126.

12. Swan, M. (2015), *Blockchain: Blueprint for a New Economy.* O'Reilly Media, Inc., Sebastopol, USA.

13. Tapscott, D. and A. Tapscott (2016), *Blockchain Revolution.* Penguin Random House LLC, New York.

14. Vigna, P. and M.J. Casey. (2014), "BitBeat: Could Bitcoin Help Fight the Ebola Crisis?" *The Wall Street Journal*, October 8.

15. Washington, L. C. (2008), *Elliptic Curves.* Volume 50 of Discrete Mathematics and Its Applications, Chapman & Hall/CRC.

16. 王儷玲(2016)，「解讀金融市場/發展金融科技」，經濟日報，2016 年 11 月 14 日。

17. 李鈞（2014），比特幣：過去、現在與未來，台北市，遠流出版事業股份有限公司。

18. 沈庭安（2016），【打造臺灣最大銀行區塊鏈平臺】央行終於出手，財金公司串連國內 45 家銀行組區塊鏈平臺，iThome 新聞，2016 年 11 月 13 日。

19. 保羅威格納、麥克凱西(2016)，「虛擬貨幣革命」，林奕伶譯，大牌出版/遠足文化事業有限公司。

20. 許榮、劉洋、文武健與徐昭(2014)，互聯網金融的潛在風險研究，金融監管研究，第 27 期，頁 40-56。

21. 閻台生、彭勝本與謝順峰等(2016)，「105 年度銀行業關鍵性人力資源供需之研究」，台灣金融研訓院，2016 年 12 月。

22. 鄭貞茂、董瑞斌與謝順峰等(2015)，「台灣銀行業者發展亞洲區域銀行之研析」，台灣金融研訓院，2015 年 11 月。

23. 劉世偉、胡一天、管中閔與廖世偉(2015)，打造「帳聯網」將成台灣金融科技新武器，台灣銀行家雜誌，頁 66-69，11 月號。

24. 麥肯錫(2016)，《區塊鏈—銀行業遊戲規則的顛覆者》，麥肯錫中國銀行業白皮書，2016 年。

附錄一 訪談紀錄

華南銀行訪談紀要

「區塊鏈及數位貨幣在金融業的影響與應用」

一、時　間：2017 年 01 月 11 日(星期三)上午 10：00-12：00

二、地　點：華南銀行資訊科技處(台北市中正區泉州街 15 號 4 樓)

三、受訪者：杜文宗處長、林大園科長

四、出席者：林士傑副所長、張凱君研究員、李宛蓁分析師

五、會議記錄

1. **杜處長：**華南金控目前有加入財金公司及 KPMG 兩個區塊鏈相關組織，並將區塊鏈分為兩塊進行，一為業務端，由數位金融部負責，一為技術端，由資訊科技處資訊規劃開發部負責，目前已上線的 HNoTe 即由本部門所開發。

2. **以區塊鏈發展現況，是否有建議的商業應用模式？**

杜處長：

區塊鏈技術目前面臨的問題在於瞭解技術後該如何實際應用，如貴院研究報告內所說，區塊鏈是一種技術，應用上非一蹴可及，雖有部分人士樂觀認為科技發展快速，一兩年內即可能蓬勃發展，但我認為目前區塊鏈實際應用上尚有缺口，僅處於討論階段，須花較多時間研究如何應用區塊鏈技術，但開發不能停滯，因考量內部資金調度問題，華南金控僅先將技術帶入紅利積點。

華南銀行各部門會在每年年初討論該年度的發展方向，現在還不確定今年要以紅利積點為方向或從金控落實應用區塊鏈技術，確立方

向後較能與同業分享經驗，目前技術與應用尚未串聯，業務方不瞭解區塊鏈技術，對效率、保密等方面存疑，溝通上有隔閡，應設法解決這項疑慮。雖國際上已有許多區塊鏈應用實例，但台灣對這項技術有信心的人不多，還需要時間溝通。

3. 華南銀行開發的 HNoTe 目前已可執行，是否可介紹一下其主要功能？

林科長：

先由 HNoTe 的建置說明，HNoTe 是模仿比特幣的架構而建構，比特幣是一虛擬貨幣，建置時有討論是否執行 Hcoin，但因貨幣議題較為敏感，故調整後改為 HNoTe。

HNoTe 不強調貨幣特性，內容可包含原生貨幣外產生之合約或其他通知事項，並開發 API 部分以執行指令，另建立錢包，與比特幣相同，可隨時產生帳號，主要傳輸應用面的訊息，但目前為測試階段。錢包有實做 Mac 機器及 windows 機器兩部分，HNoTe 建置了 HNoTe.info 及 HNoTe.org 兩個網站，.org 部分主要闡述 HNoTe 理念，.info 部分會將程式做分享，會如此規劃主要是為了在集團內測試，是否只要在.org 下載錢包，即可加入鏈內。

華銀目前有加入財金及 KPMG 兩個研討會，財金主要在測試區塊鏈於企業金融方面的應用，目前較偏向轉帳部分，想將區塊鏈套入 EDI 交易上，目前業務組及技術組皆有加入。轉帳有幾種方式，如通匯、ATM、EDI 等，EDI 為較早期的轉帳方式，希望套入區塊鏈技術後，EDI 可不用透過財金公司而是以 P2P 的方式轉帳。KPMG 的部分，主要在討論中小企業融資，實驗由客戶端發出融資需求，透過區塊鏈連結起來。

區塊鏈技術需要以區域聯盟的方式集體運作才有機會發展，最有機會的就是以類似財金公司這樣的角色來主導，因區塊鏈技術的應用，僅單獨一家銀行難以運作，故華銀在區塊鏈技術應用方面，並未有進一步的研究，僅參與研討會瞭解實作情形，KPMG 主要使用以太坊技術，財金則傾向使用 IBM 的 Hyperledger 來實作，目前還在評估，下一步將使用較主流的技術運作，才有機會與外部串聯。

R3 聯盟方面，目前台灣僅中國信託有加入，雖有來行說明組織架構，但因費用昂貴，業管單位還在評估中。

4. HNoTe 與比特幣之間的關係為何？

林科長：HNoTe 是模仿比特幣架構，使用 C 語言另外寫一套程式。

5. 如果是模仿比特幣的架構，是由誰擔任礦工角色以建立信任機制？

林科長：目前為實驗階段，使用 4-5 台機器代表礦工節點來擔任礦工角色，下一步實作，如果有需要也可使用虛擬化 VM(虛擬機器)製造多節點。

6. HNoTe 可用來調度集團內資金，所以是類似帳本的概念嗎？

林科長：是，我們要解決在 HNoTe 內原本有的幣別計價單位，內部資金要如何做幣別兌換，且符合主管機關的規範，這是一項挑戰。

7. 所以需要另外的計價單位，不能使用新台幣嗎？

林科長：也是可以的。

8. 在資金調度方面，HNoTe 改善了哪些問題？

杜處長：資金調度較有效率。剛剛提了兩個部分，一個是實際資金的問題，會顧慮央行規範，要視主管機關想法而定，較為複雜。另一部分是紅利積點，其本身即有一換算方式，可以不用考慮幣別兌換問題，

且點數可兌換百貨用品，但目前僅行內測試，希望未來無論客戶或其他同業都願意加入。

9. HNoTe 目前行內測試情形如何？

杜處長：因大家對區塊鏈還很陌生，溝通上有困難，僅團隊內的人員在使用。

10. 區塊鏈用在貨幣流通上會受主管機關限制，但在資訊流通上可能有發展的空間，比如紅利積點，對消費者而言，若可整合各家銀行信用卡的紅利，使用上會更加方便，區塊鏈是否可作為整合的工具？

林科長：若要整合，會產生主導權的問題，因各家銀行紅利計價方式不同，若要統合各家銀行的紅利，該由誰主導是一個問題。

11. 所以目前台灣需要一個領頭的單位，而非中心單位，就如科長所說，財金公司適合扮演這個角色，目前也已集結眾多業者，那適用的情境為何？

林科長：目前是針對案件討論的狀況，如紅利積點。

12. 目前 KPMG 主要在嘗試中小企業融資方面的應用，是否類似資訊交換？

林科長：是的，類似徵信的概念，無論客戶在哪家銀行貸款，只要在這個區塊鏈上，即可分享資訊。

13. 但銀行也許不見得會希望其他同業知道自己有哪些客戶？

林科長:所以這也是一個難題,目前只是將技術跟業務套在一起討論，部分細節有待商榷，比如在去中心化的架構下，開戶、轉帳等皆可自己處理，中間若發生錯誤，客戶該找誰？融資撥款時，是否有手續費的問題？何時撥款？很多細節沒有考慮到，未來還有一段路要走。

杜處長：提出一點個人經驗分享。十多年前，某商店提出辦卡買商品可積點，點數可換購商品，後來發展到於多家特約商店消費皆可累積點數，且每間特約店皆可抵用，對消費者來說十分便利，類似紅利積點的區塊鏈應用概念，但後來店家認為於店內消費的點數，會使別家店生意變好，即取消此方案。會發生這種情形，表示開辦當時沒有經過審慎考慮。紅利積點兌換商品的本意是培養客戶忠誠度，這種紅利積點共用的作法似乎不是合理的商業模式。

14. HNoTe 已可上線，國內是否有其它銀行已應用區塊鏈實作？

林科長:目前富邦在行內實作使用真實貨幣轉帳,但不清楚進度如何。

15. 銀行是否可能與異業合作，讓業務進一步擴大？例如使用區塊鏈技術改善食品安全問題，未來行動支付可查詢食品中各原料來源及中間商資訊等等？

林科長：改善食安問題應由政府著手進行，加入區塊鏈技術也許可改善食品標示造假問題。

杜處長：這是一個好方向，通常談到區塊鏈應用，很容易朝著數位貨幣的方向思考，如果可以脫離這個思維，也許是個機會。

16. 剛剛提到的中小企業融資，分享的其實是銀行內部非常機密的資訊，銀行是否會有疑慮？

林科長：所以未來要實際應用可能會改變一些作法，需要分享的資訊才分享，但目前還是實驗階段，沒有這麼快可以實踐，以目前 HNoTe 實行狀況，區塊鏈較不適合套用在銀行即時交易部分，Hyperledger 及以太坊皆在測試將其變形，期待未來可適用於商業用途。

17. 證券業是否會受到較大影響？

杜處長：本金控對於區塊鏈在證券部分的應用，是交由證券子公司研究，在交易撮合的層面是有些擔心，如果交易不須經過交易所，未來也不需要證券業了。大家對於技術可以解決的問題還需要溝通。

18. 為適於金融業應用，區塊鏈技術需要改進，華銀的區塊鏈是否可配合調整？

林科長：IBM 的 Hyperledger 可做為參考，實作上正在觀看風向，若有明確方向，會直接導入新技術。

19. Hyperledger 是否為開源程式碼？

林科長：Hyperledger 與比特幣相同，皆是開源程式碼，可以直接引用，只是目前人力主要放在比特幣區塊鏈，若要使用 Hyperledger 還是需要投入部分人力研究，或是未來有成立聯盟，會直接參與聯盟，用同樣技術實作會發展較快。

20. 華銀原則上是自主開發區塊鏈技術，必要時再將開源技術帶入，為何選擇採用 Hyperledger？

林科長：以太坊與 Gcoin 等都是以比特幣為基礎做調整，Hyperledger 較接近金融業應用。

21. 財金公司與 KPMG 運作模式為何？

林科長：開業務會議訂定方向，再做技術開發，兩個研討會皆委託外部廠商，財金公司委託 IBM，KPMG 委託政大開發，並訂定研發期限。KPMG 另與金融研訓院合作，將業務與技術人員分開，不定時召開小組會議。

22. 財金公司目前的主軸是放在 EDI 嗎？希望達成什麼目標？

林科長：是的，他們希望開類似錢包的軟體，透過區塊鏈技術使交易

流程透明化，將 EDI 改為 P2P 模式。

23. 中小企業融資的議題也十分重要，如果供應鏈自成區塊鏈，可提升效率嗎？

林科長：產品供應鏈有層層關卡，若導入區塊鏈技術，確實能提升效率，但涉及的單位較多，不容易建構。

財金資訊股份有限公司訪談紀要

「區塊鏈及數位貨幣在金融業的影響與應用」

一、時　間：2017 年 01 月 17 日(星期二)上午 10：00-12：00

二、地　點：財金資訊股份有限公司(台北市內湖區康寧路三段 81 號 6 樓)

三、受訪者：黃昱程副總經理

四、出席者：林士傑副所長、謝順峰研究員、張凱君研究員、李宛蓁分析師

五、會議記錄

1. **是不是可以請副總經理談一談財金資訊公司目前在組建國內金融區塊鏈平台的規劃或進度?**

金融區塊鏈研究發展委員會，目前參加銀行共 46 家，目的是要統一區塊鏈系統、建立區塊鏈技術平台，其中區分為個人金融及企業金融兩組，各安排 10 家銀行擔任諮詢委員，每組再細分為業務小組及技術小組。

業務小組在 2016 年底，已選定驗證項目，個金方面為公益捐款，企金方面為企業資金管理。所謂驗證，是在擬真環境下運作，非實際營運,會有幾個驗證節點,但目前尚未討論到節點放置處這類的細節。

驗證項目的選擇方式，主要考量可行性、貢獻度、以及創新程度。所謂可行性，是要評估這項業務的參與銀行家數多不多，另因目前區塊鏈技術未成熟，且規劃的驗證期間僅半年，不能找太複雜的業務，要短期能驗證、上線的項目，以負面表列方式選擇，排除目前區塊鏈技術做不到的高頻交易，以及由於涉及跨國司法管轄權、各國外匯管制標準不一、洗錢防制、找不到國外機構做驗證等因素，暫時先排除跨境業務；貢獻度方面要評估這項業務對銀行、民眾是否能提高方便

性，及創新後業務流程、技術上可解決什麼問題。

銀行方面選擇驗證項目亦有三項考量，第一，無論技術、業務皆是由下而上，各銀行提出一至三項驗證項目，經投票表決排序；第二，業務項目要可解決大部分的問題，例如公益捐款，可利用區塊鏈不可篡改、可追溯的特性，解決捐款流向的問題；第三，應從業務、交易流程，找出可藉由區塊鏈技術提高效率、減少人力的業務，例如外科手術須向醫院申請診斷證明再去保險公司申請理賠，可利用區塊鏈技術提高效率，目前國泰僅於集團內試驗，未來若可跨機構，效益會較明顯。

對於採取何種區塊鏈底層協議，財金公司目前持開放態度，不排除任何區塊鏈技術，例如 Hyperledger 及以太坊各有優缺點，以太坊的本質是以虛擬貨幣來打造的區塊鏈技術，優點是其本身即為一信任機制，可解決網路信任問題，不需要中介單位，但這也是他的缺點，因為金融機構有監理問題，不可能使用匿名交易，目前以太坊有在研擬要將匿名改為實名，但還需要時間；Hyperledger 的優點是實名制、認許制，剛好符合本國金融支付要求，且很多大型金融機構有參與，未來業務延展性較佳。技術在發展階段，無法確定未來主流平台，所以不排除任何區塊鏈技術平台，對金融機構而言，「學習」才是目前的重點。

銀行方面分三種策略，第一種是加入國際已成熟聯盟，如 R3、Linux 等，但加入成本高且短期效益有限，目前國內僅中國信託加入 R3 聯盟；第二種是國內自行組織聯盟，可找異業合作組織，或加入像財金公司目前組織的聯盟；第三種是直接投資新創業者。目前國內以加入

財金公司所組聯盟的銀行居多，因資源共享、資訊互通的概念，一來成本低二來避免重複投資浪費。

區塊鏈技術發展預估最快還要二到三年才會成熟，目前 POC 進行得不太順利，針對區塊鏈的缺點改進，也許兩三年後可實際應用在很多地方，長期來講一定有可運用之處，銀行應保持關注其發展並實作 POC 的態度。

面對因應國際發展趨勢的建議，因區塊鏈技術前景不明確，但可能有潛在用途，因此目前較適合簡單、小規模的驗證，如果規模太大，未來如果在技術或業務的發展與現在的預期不同，變更或轉向會很困難。發展區塊鏈應用的過程，會有一定的風險。

2. 區塊鏈欲發揮效能，需要多一些銀行參與，但是銀行彼此間不見得願意分享客戶的資訊，如何解決這個問題？

這是區塊鏈發展自我矛盾的現象，希望達到交易透明化，但銀行不願分享客戶資料，所以要調整為「有限度的資料分享」。

台灣及中國大陸目前積極實作的紅利積點，雖然紅利積點確實需整合，但反向思考紅利積點與區塊鏈的關係，其實不使用區塊鏈技術也可實行，紅利積點的目的在於維持客戶忠誠度，若使用區塊鏈技術打造紅利積點平台，所有客戶皆可在平台內兌換任何一家銀行的點數，市占率較高的銀行會不願意參與，雖然區塊鏈技術套用在很多業務上都有效用，且可讓消費者更便利，但不符商業模式。

以目前的區塊鏈技術，已可做到條件變更，在實名制、認許制的情況下，希望做到僅利害關係人及監管單位能互通資訊，達到有限度的資料分享。認許制是指必須經過同意才能加入某一區塊鏈聯盟，例

如比特幣區塊鏈不須經過同意，大家皆可加入，即非認許制。

3. 目前區塊鏈技術可以做到有限度的資料分享嗎？

以以太坊來講還需修正，Hyperledger 大致可做到，但目前版本為 0.6，1.0 後會更完整。不過目前還沒實際運用，如果無法完全達到標準，就需要自行修正程式，要嘗試後才知道，且 POC 與實際上線也有落差。

4. 剛剛提到企金的 POC 為企業資金管理，目前計畫如何運作？

企業同意使用區塊鏈技術，處理將資金由 A 銀行轉到 B 銀行的交易，如此企業及銀行皆可看到所有交易情形。初期試驗階段，不可能所有企業及銀行都加入。

5. 企業資金管理使用區塊鏈技術對銀行的好處為何？

銀行想瞭解企業交易情形需透過財經公司查詢，未來可直接透過區塊鏈平台查詢提高效率，若順利流程也可簡化。

6. 用於企業資金管理的區塊鏈平台也會吸引企業加入嗎？

是的，對銀行及企業來說，要查詢交易情形會變得較容易，但就如剛提到的有限度的資料分享，銀行僅可查詢自家客戶的資訊，不能看到別家銀行客戶的資訊。

7. 非銀行業者在區塊鏈的應用上似乎也很積極，對金融業會有什麼影響？

本質上銀行較穩健保守，監管體制較嚴謹；新創業者較敢冒風險，屬中低度監管。目前非金融的新創業者確實較積極，第三方支付也是由非金融業者突破出來的，如果沒有新創業者冒險突破，消費者也無法享受這項服務，但銀行的立場相對尷尬，自己開發市場不夠大，與

新創業者合作，利益又要平分。

8. 大企業供應鏈複雜，若大企業與新創公司合作，自組區塊鏈，對銀行是否會造成很大的衝擊？

有諮詢過部分銀行，大企業與銀行已合作很長一段時間，並有一套運作機制，銀行認為供應鏈融資在台灣已經發展得十分完善，除非區塊鏈可大幅簡化流程，降低成本，否則大企業加入區塊鏈的可能性不高，且中心企業並不想透露太多資訊給衛星企業。

供應鏈、聯貸、信保這些融資方式，看似跨很多機構，可透過區塊鏈技術提高效率。假設跟主辦行申請聯貸，相關資料要提供給參貸行，多家銀行看到相同資料，效率可提高；申請間接信保，原需經過銀行評估後送信保，若透過區塊鏈，可同時申請信保及銀行貸款，提升效率。但實務上，聯貸案需統一條件，統一申請才有可能縮短流程；信保還是希望經過銀行同意後再作業，除非信保認為銀行一定會同意，才有可能提高效率。

區塊鏈技術需要所有流程電子化才能解決問題及達到跨機構的效益，跨機構十分複雜，需所有相關機構皆加入區塊鏈運作，例如申請房貸，要申請謄本並於地政事務所辦理設定才能向銀行貸款，如果過程全使用區塊鏈運作，當然可降低成本提高效率，但涉及單位包含地政事務所、代書、律師等，不只有銀行，所有機構皆加入的區塊鏈效益最高，但跨機構跨平台也意味著推動不易，而且還可能會產生個資的問題。

銀行需要思考為何使用區塊鏈技術，使用後可解決什麼問題？這是個關鍵，而不是為了區塊鏈而區塊鏈。例如國內目前有電子簽章法

可處理，但反過來想，使用電子簽章法處理即可為何要使用區塊鏈？也許最後需評斷何者成本較低、使用效率較高。像目前台灣網路認證公司，可將書面文件設定 QR code，掃描即可看到完整文件，不需要區塊鏈也能處理，但區塊鏈是另一種方式。另外像跨境匯款，需經過台灣及國外主管機關同意，且目前各國對洗錢防制越來越嚴格，要如何透過區塊鏈處理。

9. 區塊鏈在實名制的情況下，以其不可篡改、可追朔的特性，對洗錢防治是否有幫助？

如果改成實名制，確實可以加強金融監理，但目前虛擬貨幣區塊鏈並非實名制，本質上類似商品交易，對央行而言非屬貨幣，因貨幣需廣泛作為交易媒介，數位貨幣僅少數人使用，且貨幣需有記帳及價值儲藏的作用，數位貨幣價格波動幅度大，現階段並不適合做為貨幣。

10. 區塊鏈如何解決跨境支付問題？

舉例來說，在德國將歐元轉換成 RIPPLE 貨幣，轉到美國後再將 RIPPLE 貨幣轉為美金，必須有一個貨幣轉換的機制，要視轉換價格是否透明、有公信力。

11. 現行的跨境支付機制有何缺點？

目前對跨境支付的批評是手續費較高、時間較長，透過區塊鏈可降低成本並所短時間，但發展多年並沒有顯著改善，因為涉及單位過多，一定需要收取手續費，成本部分需精算過才會知道，除非匯率相當優惠，且數位貨幣不會錯帳或產生消費糾紛，不然還是需要中介單位。

12. 除了支付以外，區塊鏈還有哪些發展機會？

國內支付有許多未被滿足的地方，才會發展新的支付工具。中國大陸因金融不發達，才會發展第三方支付，但台灣的支付工具系統已相當完整，金融普及率相當高，這種環境下要發展新的支付工具很困難。

13. 未來若數位交易越來越普及，是否有發展的可能？

網路支付有三個問題，第一，需要有規模經濟才能發展，各家網路業者皆有使用者，大家都希望保留自身客戶，很難整合；第二，消費者支付習慣的問題，長期發展不容易改變；第三，網路支付策略，我稱作花園圍牆，為了達成規模經濟，會在支付系統內自成生態系並築起高牆，培養客戶忠誠度。所以我很認同往非支付方向發展，像生產履歷，若能使用區塊鏈技術可解決很多食安問題。金融服務方面，交易鏈複雜、跨機構的金融商品較能凸顯區塊鏈的效益，如利率交換或 CDO 等衍生性金融商品，區塊鏈可使其透明化，降低資訊不對稱風險。

14. 目前區塊鏈發展，有哪些法規是需要調整或放寬的嗎？

財金公司是按照銀行法 47-3 條運作，目前沒有法規問題。

在區塊鏈的發展階段，法規並沒有適用不適用的問題，長期來看我認為無論什麼單位要發展區塊鏈，做相同業務要有相同的監管標準才公平；短期及中期需要在某項法規下創造創新空間，又要兼顧監管公平不讓目前業務受影響，這部分可比照電子票證條例，儲值與存款皆是將價值儲存，為鼓勵一卡通、悠遊卡發展，避免阻礙創新又要兼顧監管公平，所以設定提存存款準備金限額，可以用某種風險管理機制，在一定額度下用其他方式處理，如此規模小又可控管風險。

但我認為不見得需要設立專法，專法有好處也有缺點，有時設了專法以後大家反而綁手綁腳。

15. 區塊鏈對銀行授信的影響？政府提出五大創新產業，資產型態可能非實體，區塊鏈是否可解決智慧資產、數位資產的問題？

部分新創事業評估原則會和原來不同，但會不會因區塊鏈而改變則有待觀察，聯徵及銀行本身評估系統各自獨立，有些銀行有其獨特授信體系，並不希望與其他機構連結。

16. 您對數位貨幣有什麼看法？

數位貨幣的發行者不一定是央行，例如以太坊及比特幣，只是普及程度不高，未來數位貨幣持續發展，普及率提高後，銀行較會受到影響。

數位貨幣發行者非央行，法償性較弱、可兌償性較差風險較大，若要發展數位貨幣，對發行者需有一定的信任或足夠的擔保，如銀行或央行，目前數位貨幣沒有發行者，如果要發展起來，一定要解決風險問題，另外若以法定貨幣為清算平台，要解決流動性問題及資訊不對稱問題。

17. 是否可能達成實體、數位雙元貨幣？

若數位貨幣僅作為暫時的價值儲藏，則有可能達成，但若要將資產轉為數位貨幣，一定要有值得信任的發行者。但目前已經有人將比特幣視為投資工具，因比特幣供給有限，由需求決定價格。

18. 您對 FinTech 業者發展區塊鏈有什麼看法？

非銀行業者要投入 IT 及人力成本，也需要靠手續費賺取收入。像中國大陸的阿里巴巴、微信，與銀行實聯可轉帳，一開始標榜無手

續費，但後來還是有收取，因為銀行向他們收取手續費，有成本就必須收取。

IT 產業建置成本不低,雖然會聽到大家說現在的新創業者規模小、技術進步，初期建置成本不會太高，但要做大時，IT 處理速度及容量勢必要大，不僅建置成本，還有備援成本、維護成本，且法遵成本也越來越高，跨境國家越多成本會越高，要有專則及法遵主管甚至洗錢防制的主管，這些都是成本，但一開始都沒有考慮這些問題，且因洗錢防制，每筆交易都續透過類似聯徵的機構，交易速度也會受影響

台灣銀行業在國際上的競爭力尚有待提升，有財金公司、信保、聯徵等跨機構的資訊交易平台成為台灣特有的優勢，但新創業者現在卻在思考如何替換掉這些平台，他們不了解建置成本有多高、且民眾還是較信任這些平台。

19. 財金公司所組的金融區塊鏈研究發展委員會是否定期開會？

諮詢小組每月開會一次，大會三個月開一次會，大會主要是報告諮詢小組發展進程。

20. 目前正在推動的是業者認為應優先進行的項目嗎？

對，但因技術在發展，雖然有選出一些項目，還是會視技術發展及業務需要做調整。現在是邊學習邊調整，技術要從消化吸收到實際應用，且區塊鏈所用的程式語言與現在所用的有些微不同，還需要一段時間。

附錄二 其他文獻

一、英國央行數位貨幣研究報告

二、我國中央銀行數位通貨研究報告

(2016.3.24 央行理監事會報告)

三、美國國會比特幣和區塊鏈技術專案研究報告