

分散式帳本與區塊鏈的應用現況與挑戰

◎羅鈺珊／中華經濟研究院第二（國際經濟）研究所 助研究員

區塊鏈改變目前政府、組織與產業樣貌，許多國家政府與企業已經積極投入，為了掌握區塊鏈發展與應用趨勢，有必要儘快針對臺灣如何利用區塊鏈概念或技術，開創新的產業發展契機，進行前瞻性的研究，並檢視可能面對的問題與挑戰，以協助政府與產業在相關領域的發展。

關鍵詞：分散式帳本、區塊鏈、產業應用

Keywords: distributed ledger, blockchain, industrial applications

帳本是記錄一連串的資產轉換與交易過程資訊，並由可信賴的第三方中間人維護與查證內容真實性；為了確保交易過程與帳本內容的準確度，往往需要耗費不少查證、確認交易內容與審計的時間與成本。隨著資訊與網路科技的快速發展，資訊記錄由紙本轉向數位化，使得資訊的流通變得快速有效率。目前大多數的數位資訊與交易依賴集中式的資訊架構，如政府、金融機構、網路平台、大型私有資料庫的維護管理；然而集中化管理的問題在網路時代也陸續浮現，例如

中心機構容易成為被有心人士攻擊的目標。此外，數位科技允許多人同時在不同地點分享或擷取資訊內容，但也因為集中式數位資料容易被更新、修改或刪除，造成許多管理上的困難。

此外，在各類數位科技大量應用於金融服務之後，網路科技帶動的數位創新已經成為新議題，數位金融生態系的各利益關係人亦開始意識到集中化架構的信任問題。為了尋求一個更可信賴的機制來管理數據資料，降低交易與監管成本，分散式帳本科技（Distributed

Ledger Technology) 的應用近年成為各國政府與企業積極探索的領域，並被視為可能對未來組織、商業行為與市場帶來新的紀元。

分散式帳本與區塊鏈概念

分散式帳本是將數位紀錄依照時間先後發生的順序記載在數據庫（帳本），並在通過參與者同意的規則或是獲得一定數量的贊成票之後，被記錄並加密保存在帳本上。我們可以把分散式帳本想像成一個公司或供應鏈的協作工作表單，每個參與者將其工作紀錄上傳並儲存於雲端的表單上，並被檢視是否符合規則或被認可；在一定的時間後，所有被認可的紀錄依照記載時間被蓋上時間戳章與加密簽名，並存放在一個新鎖定的工作表單上，這個表單無法被更改，且所有參與者均可隨時瀏覽紀錄。帳本可以是不需許可、任何人都可以加入的公有帳本，也可以是屬於少數擁有者、需要許可的私有帳本，或是由產業或聯盟許可的共享帳本。

區塊鏈技術也是一種分散式帳本的概念，採用加密演算法將前後帳本資訊鏈結起來，如比特幣中工作量證明（Proof-of-Work）的哈希（Hash）值，串接前後的帳本與工作表單；在帳本與工作表單經驗證後，所有參與者都能得到一個副本，故鏈結的區塊鏈除了更難變更，也能回溯並確保整條帳本的正確性。因此在應用層面上，若採用區塊鏈技術，從生產、供應至交易過程，每位參與者都擁有一份資訊，所有加入的資

訊都必須通過共識，每一個變更的步驟與變更者都將被永久紀錄且保存在每個參與者的節點，具有可追溯、不可逆、不可竄改的特性；其點對點傳輸與去中心化的特性，也降低中心機構被攻擊與複雜行政程序的成本。

應用趨勢

基於分散式帳本能有效降低認證、網絡交易與協作等成本、並能透過公私金鑰來控制資料讀取與修改權限，兼顧透明度與隱私安全性，且具可信賴的優點，因此在金融保險服務、醫療健康、慈善公益、共享經濟、供應鏈、物聯網與智慧製造、所有權與版權、政府與公共服務等，均有極大的應用效益（見表1）。

雖然分散式帳本與區塊鏈的應用目前還在初步發展階段，但基於可操作性與未來效益，許多企業與政府紛紛投入，目前銀行與保險機構基於維持其信賴地位、降低交易審查成本、提升安全與效率，為投入研究與應用最積極者；而政府單位預估將會是這個科技應用的最大使用者與推動者之一，目前英國、中國大陸與澳洲及部分美國地方政府均已發表其區塊鏈政策報告。

根據IBM與Economist Intelligence Unit針對16個國家200個政府機構所做的調查，在2018年底之前，有90%的政府機構計劃在民眾服務、金融交易管理、資產管理、合約管理與法規遵從方面投資區塊鏈的運用，以降低跨部會合作成本、提升效率與透明度。



表1 分散式帳本的應用領域

金融保險	支付、交易結算、貿易與供應鏈金融、虛擬貨幣、眾籌、信貸、保險、投資
醫療健康	數位病歷、處方簽、健康與運動管理、醫療研究、醫療保險給付
政府與公益	投票、身份認證、工商管理、地籍與資產管理、福利支付、稅務、慈善公益、遺產管理、法律刑事紀錄
版權與所有權	專利、著作權、版權、追溯認證、傳播溯源、槍枝限制品買賣追蹤
學術與人資管理	學歷與訓練證明、產學合作、人資履歷、勞工訓練補貼
共享經濟	租車、租房、跨企業品牌數位集點或紅利共享
物聯網	物品與裝置溯源、追蹤、認證、安全控制、裝置與裝置溝通管理、供應鏈管理、智慧家庭/工廠/辦公室管理

資料來源：作者整理。

許多國家已經開始小規模地進行公共部門的區塊鏈測試使用，如愛沙尼亞結合無鑰簽名基礎架構（keyless signature infrastructure）與區塊鏈技術，監控公部門數據的變動，除了已啟動區塊鏈投票與醫療健康檔案管理計畫，也預定將這套基礎設施建立在全國的公私部門當中。英國也已經開放其雲端設施給區塊鏈新創，希望促進區塊鏈在公共服務的創新與應用，其工作與養老無恤金部門（Department of Work and Pensions）也開始運用區塊鏈測試社會福利支付；喬治亞共和國則利用區塊鏈保護土地所有權並驗證房地產轉讓。

以商業應用而言，杜拜成立全球區塊鏈委員會（Global Blockchain Council）將開始針對健康資料、鑽石買賣、商業登記、數位遺囑、貿易與物流等進行研究測試；美國德拉瓦州（Delaware）因應免稅天堂地位，也開始利用區塊鏈技術來儲存合約與企業資訊；

中國大陸除了發起「一帶一路一鏈」政策，希望透過區塊鏈技術快速帶領中小企業打通一帶一路的貿易，以及透過綠色能源鏈發展綠色能源與綠色金融之外，貴州也將啟動全球第一個區塊鏈小鎮；澳洲政府也提及將運用區塊鏈確保如奶粉與牛肉等澳洲產品在銷往其他國家的過程中不被仿冒或置換。

分散式帳本與區塊鏈的應用案例

區塊鏈的廣泛使用奠定在其結合其他科技，如智能合約與IoT感應器等的運用上。為了使讀者容易了解區塊鏈的運用方式，以下列舉案例說明。

1. 整合政府公共服務

目前民眾或企業組織有大量的數據資料儲存在不同的政府部門，如身份證與戶籍資料、工商登記資料、社會安全資料、稅務資料、犯罪資訊、出入境資訊等，許多時候

這些資料是儲存在個別的政府單位，因此常需要花費時間跨部門調閱資料，有時也會造成資訊不對稱的情況，發生包括逃漏稅、冒領年金與福利金、溢領或沒有領到失業救濟金、企業無法查證員工犯罪紀錄等問題。

若政府能設立一個中央資料庫統合企業與個人的資訊，透過公私金鑰與智能合約決定誰可以在某段期間內讀取或變更資料，不僅可以了解個人與企業與各部門過往的互動紀錄，也可以在智能合約條件生效，譬如在醫院死亡證明簽發或長期病患多久時間沒有就醫紀錄時，政府福利系統自動停止年金發放或派員前往訪視。

2. 食品安全鏈

食品安全的問題層出不窮，包括假冒來源與培養方式、添加不被允許的物質、運送過程瑕疵等，而一般消費者與監管單位很難在不爆發食安危機或未經舉發的情況下發現這些問題。

以牛奶供應鏈為例，可以導入物聯網與智能合約，奶品製造商可與牧農訂定飼養過程與條件，當牛奶送到製造商時若符合條件則智能合約自動生效付清款項；批發商與製造商之間、以及與零售商之間都可以訂定包括製造、運送與存放條件的智能合約，包括添加要素、整個過程的溫度與濕度控制等，並在感測器監控下送至批發商與零售商，在條件達成時自動付款或沒有達成時退回、支付賠償或更改合約條件。

在整個從生產、運送至交易過程，所有的數據與智能合約條件都會傳送至區塊鏈中保存，讓食安單位與消費者可以隨時查看，確保整個供應鏈符合要求，也讓消費者可以清楚知道產品製作過程，安心消費或選擇產品。

3. 投票行為

每當選舉時，常常可以看到開票後對正確性的質疑，包括是否有代替投票、選票或票箱被動手腳、以及在投票期限之前因為突發事件或發現不實資料反悔已經投入票箱的選擇等。

美國維吉尼亞州的新創企業 Follow My Vote 即開發區塊鏈投票系統，並在美國總統大選期間完成測試。概念與流程為，想要參與區塊鏈投票者需申請一個用戶證書（類似電子錢包概念）和一個投票機會，並透過身分證、生物辨識或網路相機確認選民身份，並使選民可以將他的一票加密投入候選人錢包中，並在任何投票開票過程中驗證自己的選票是不是有被竄改。如果規則許可，也可以在投票期限之前更改自己的選票。

現在人民對政黨與政府信任度不高，也因為數位科技趨勢下，發聲管道多元，不需要透過政黨發聲，在公民對議題的覺醒之下，未來有可能有越來越多的事件票透過區塊鏈技術來進行，包括由民間發起對政府政策的支持或反對票，而不只是選舉或政黨票。



4. 資料所有權、智慧財產、貴重或管制物品溯源

對於貴重物品與智慧財產權，源頭極其重要。在鑽石溯源的追蹤上，有鑒於每年約有1億英鎊的珠寶詐騙損失，Everledger與大型全球鑽石認證商合作，為每顆鑽石建立數位身分證，並記錄其產地與特徵之後，將所有資訊與交易紀錄記入區塊鏈，並與執法單位與保險公司合作，監督鑽石來源與流向。受管制的槍枝彈藥也可以透過相同方式清查去向。

在智慧財產權方面，許多藝術創作者因為網路流通快速，無法獲得應有的創作報酬，且往往需要繳給平台大量權利金。目前已經出現許多音樂區塊鏈新創，包括Ujo Music、Dot Blockchain Music、Mycelia、Spotify 也收購 Mediachain 並將利用區塊鏈解決音樂來源與使用權利的問題等。

其基本概念是在創作後將作品上傳取得作品位址，利用區塊鏈時間特性可以不用向每個國家申請智慧財產權，並在使用者下載時依智能合約將利潤分配給創作者與其他參與製作或表演的人。同樣的，文章創作與其他智慧財產權也可以依此模式，而獲得的數位貨幣可以使用在合作商家的支出或是交易成現金。

此外，現在網路上的資料與數據所有權屬於誰，可以怎麼運用的爭議尚未解決。而區塊鏈的應用可以讓所有權回歸至個人，由個人

決定該怎麼運用，並追蹤被使用情況。以健康醫療為例，個人可以依照條件將自己的健康生理資料去除身份之後匿名放在資料庫中供研究者、教學者、保險公司、私人醫師或個人使用；智能合約中也可以包括使用資料的收費條件。除了個人詳細知道自己的健康與醫療紀錄，也可了解自己的資料被如何運用。

在高齡社會來臨，需要延長自身身體健康條件，避免造成社會與個人太大的資源負擔，且在物聯網將朝向成果收費的情況下（依據成效與使用方式收費），也可透過開立運動處方簽，由智慧穿戴裝置了解病人執行情況，提供獎賞或懲罰。同樣的資料也可分享給保險公司，設立更準確的客製化保險條件，避免蓄意欺騙或單純因為年齡限制無法投保。

發展機會與挑戰

由上述分散式帳本與區塊鏈應用概況可發現政府部門將會是區塊鏈的最大使用者與受益者之一，雖然業界對分散式帳本與區塊鏈的應用多抱持著正面的看法，但因其還在發展初期，應用與發展上有許多未知且待解決的風險。

首先是新創技術的發展與應用成功率低，且常常遇到未知的挑戰，譬如比特幣的挖礦方式反而造成器材、設備、水電能源的競爭，不僅造成另一種中心化與進入障礙，也造成資源上的浪費；但目前也有許多企業企圖利用其他科技方式解決。

目前分散帳本的技術尚未標準化，也

難以達到規模化。在公有區塊鏈中，去中心化的特性可能造成有問題發生時雖然可以知道是在哪個環節發生錯誤，但卻可能求償無門。在應用上，目前多還是既有企業與政府主導分散式帳本系統，比較傾向以聯盟或私有鏈方式建構，若少數人掌握誰可以加入，且如金融應用需要匿名機制，可能無法解決原本的中心集權與透明化的問題。

此外，對一個正在快速發展的技術，失敗或遇到挫折是常態，但人們與政府往往會因為這樣的挫折失去信心，約束其發展。目前投入分散式帳本與區塊鏈技術應用的族群多是二、三十歲的年輕人，在顛覆式創新快速發展之下，要使既有政策制定與管制者了解並願意接受需要極大的溝通成本。以目前的共享單車、汽車、住宿為例，多數國家還在思考如何管理這類新創時，已經有不少新創想以區塊鏈的去中心化來取代Uber這類的共享平台。

由於未來無法確切掌握，政府應該結合新創，在其公共部門服務領域盡快開展小規模試驗，從做中學，了解可能面對的問題並尋求解決的方法。此外，區塊鏈的隱私特性，將會引發黑色區塊鏈發展；亦即如走私、藥品與槍枝販賣、賭博，以及如近期綁架電腦駭客要求比特幣付款等非法行為，均有誘因透過區塊鏈發展。這不僅是臺灣，也是未來國際間政府需要共同合作防範的問題。

臺灣的下個產業契機

在產業方面，臺灣雖然有許多銀行聯盟積極投入，但多基於金融科技（Fintech）架構。香港VeriFi企業主席黃平達來臺演講時曾提醒，臺灣的強項在科技而非金融，而區塊鏈與智能合約的應用是設計給機器對機器的溝通，與人工智慧、物聯網、雲端運算具有密不可分的關係。目前仍是以ICT硬體研發製造為主的臺灣，若能把握發展可信任機器/產品的機會，掌握Know Your Machine優勢，並思考在區塊鏈下的創新商業服務，應該大有可為。

此外，臺灣已經錯失網路平台的機會，但區塊鏈將可能讓臺灣企業不再得依附Google、Amazon、Facebook、Apple、阿里巴巴等平台；且透過虛擬產品/服務/貨幣或資料等交易，實體貨品服務的全球貿易重要性將大幅下降，此亦可減緩臺灣目前遭受的國際邊緣化困境。

