打造農業區塊鏈平臺創新農業動態生態系統

撰文/徐逢桂

比特幣底層的區塊鏈技術在金融業興起「FinTech（Financial technology）」一股浪潮，從各大金融機構到各國央行，無不競相投入、建立標準。區塊鏈技術將網路協定由「TCP/IP」的通訊到「HTTP」多媒體呈現，更進一步帶我們走向更高層次的價值互易網路（Internet of Value），憑藉著區塊鏈去中心化、去信任、集體維護和可靠資料庫的四大優勢，設計出更多的創新價值、服務、營運流程與獲利模式，即將改變所有產業的整個面貌。臺灣的小農經濟一直有著農民低收入、通路不足、生產成本過高、食品安全與食物浪費的問題。整合現有農業資源與大數據，架構農業區塊鏈平臺，擴大契作範圍、精準農業施作、環境友善的耕種，臺灣農業仍有邁向國際競爭的機會。

前言

經濟學理論總假設經濟人為理性最大化者。然而，由於環境、情緒、意願、時間等條件制約，人們往往不能理智地做出符合經濟邏輯的決定；相對的，由程式語言設計出來的演算法卻可行。2015 年 7 月科學雜誌 (SCIENCE) 刊出了 Harvard 大學工程學和應用科學學院院長 David C. Parkes 教授和 Michigan 大學的 Michael Wellman 教授發表的文章，文中提出經濟學的理性模型可以運用到人工智慧上 (AI, Artificial Intelligence)，並討論了人工智慧經濟學的未來。人工智慧關於效率、機率、推理等優化的研究也都是經濟學上的議題，比如說經濟學的「揭示原理 (Revelation Principle)」：在交易博弈中，只有當市場的參與者認為完全暴露他們的需求和供給訊息是符合自己的利益時才能交易。今天的網路廣告完美地實現了這個原理：搜索引擎可以蒐集買賣雙方的供需條件、預算，人工智慧系統根據這些資訊撰寫相應的演算法，媒合出最吻合的廣告投放。傳統經濟系統裡很難看到這樣的機制得以完美實現，而人工智慧系統在這方面可以實現得很好，人工智慧系統可以通過匹配需求和供應，合理分配資源，精準地了解偏好，消除資訊不對等，從而優化整個市場。隨著物聯網 (IoT, Internet of Things) 的興起，把所有物品通過射頻識別 (RFID, Radio Frequency Identification) 等感測設備互相連接，進行智能化識別和管理，人和人、人和物、物和物間的交易運作，就需要一種自主性程式演算來運行。根據美國銀行的估算，機器人和人工智慧的普及，將使許多產業的生產力提升 30%。因此，早在 1994 年 Nick Szabo 提出的「智能合約 (Smart contract)」的理論架構，就被認為可以用來接軌人工智慧經濟。

有別於自然語言起草的合約無強制執行力且需要第三方仲裁，智能合約的條款是用類似於 Java 或 C++ 的程式語言以一連串 If-Then 條件語法表述，然後電腦按照協議條款和一系列定義輸入在合約兩方之間闡述、驗證和自動執行各項條款。智能合約的

程序會定義合約執行需要的「輸入」，比如支付、投票或其他任何可以用代碼表示的行動，轉移實物資產、股權或智慧財產權的管理與控制。一旦交易智能合約得以實行，第三方管理與仲裁則可不必。

然而，電腦程式要怎樣才能讓真實世界的現金、股份、實物等資產在合約雙方之間轉移呢（價值）？再者，由電腦執行這些條款，又怎麼能獲得合約雙方的信任呢（共識）？這兩個關鍵問題一直推遲智能合約的商業運用，直到 2009 年比特幣（Bitcoin）的問市。

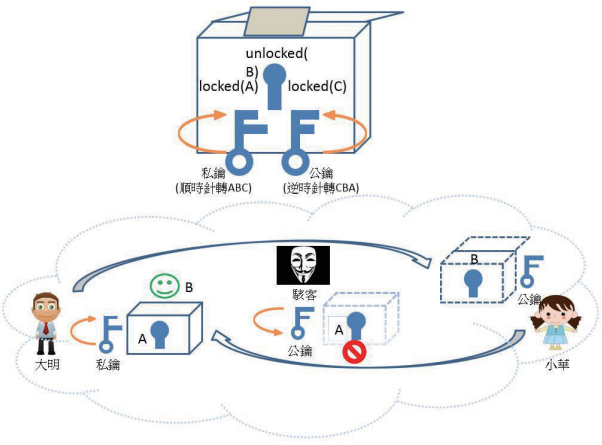
淺談比特幣與區塊鏈

比特幣是一種加密數位貨幣 (digital currency)，乃根據密碼學演算法來做貨幣價值的傳遞與產生，具有去中心化的重要特徵，所謂去中心化即是交易紀錄和清算都不需要一個負責處理的中央機構。比特幣以非對稱加密方法（公私鑰）維持發行系統的安全性；採用 BitTorrent 點對點 (P2P) 的對等網路檔案分享協定和稱為「區塊鏈（帳本）」的資訊科技技術，以分散式協議取得信任共識（拜占庭容忍），達到資產價值交換的目的。

公私鑰加密方法即是公開金鑰加密技術也稱為雙金鑰密碼安全系統，其概念可參考圖一：有一個可以轉動至 3 個位置的鎖，其中 A、C 位置均會把箱鎖上，轉至 B 處的話就能把鎖打開。大明有 2 把鑰匙，一把鑰匙為「私鑰」只能順時針由 A 轉向 C，另一把為「公鑰」只能逆時針由 C 轉向 A。私鑰只由大明持有，接著大明把公鑰及箱子寄給小華，小華收到後把密信放進箱子，再用公鑰逆時針轉至位置 A 鎖上寄還給大明。最後，大明用私鑰順時針就能夠把鎖轉回位置 B 打開箱子。這種方式的高明之處在於雙方不需要事先知道加密方式和交換鑰匙，即使在傳送公鑰期間，有一個駭客偷偷多配了一支公鑰，但在小華上鎖後，駭客仍然無法用公鑰逆時針打開箱子，這樣就能確保信中的訊息只有大明可以讀到了。

至於拜占庭 (Byzantine) 容忍則是一個共識機制建立之容錯計算：拜占庭王國的將軍們領兵與敵人作戰，將軍間只能通過傳令互通訊息，而且必須統一行動才能戰勝敵人。在現實中，有某些傳令或某幾位將軍可能是叛徒，企圖破壞忠誠將軍們的統一行動，所以必須有一個辦法使將軍們的行動能夠達成一致，令叛徒不能使忠誠的將軍做出不一樣的決定。當有 m 個叛徒在搗亂而又無法找出他們的時候，存在一種演算法或稱做彈性協定，通過這種協定，能夠保證忠誠的將軍們達成一致。研究證明了存在 3m+1 以上將軍下的 m 彈性協定，也就是說如果要想容忍 m 個叛徒，必須保證總的將軍數大於 3m。這種容忍容錯計算保障了網路就算是被攻擊或出現偽造簽名、惡意破壞系統、重複發送消息等的任何錯誤，仍然能夠正確無誤地繼續運作存活不受影響。

傳統經濟社會的信用背書系統，參與人需要對第三方機構有足夠信任。然而，隨著參與人數的增加，訛詐的人數越多，系統可信度也隨著降低。此外，兩方金融帳戶的交易記錄是由如銀行等第三方受信任機構所建立，記錄單獨保存於其中央資料庫中，這種方式無法確保記錄的正確完整和資料庫



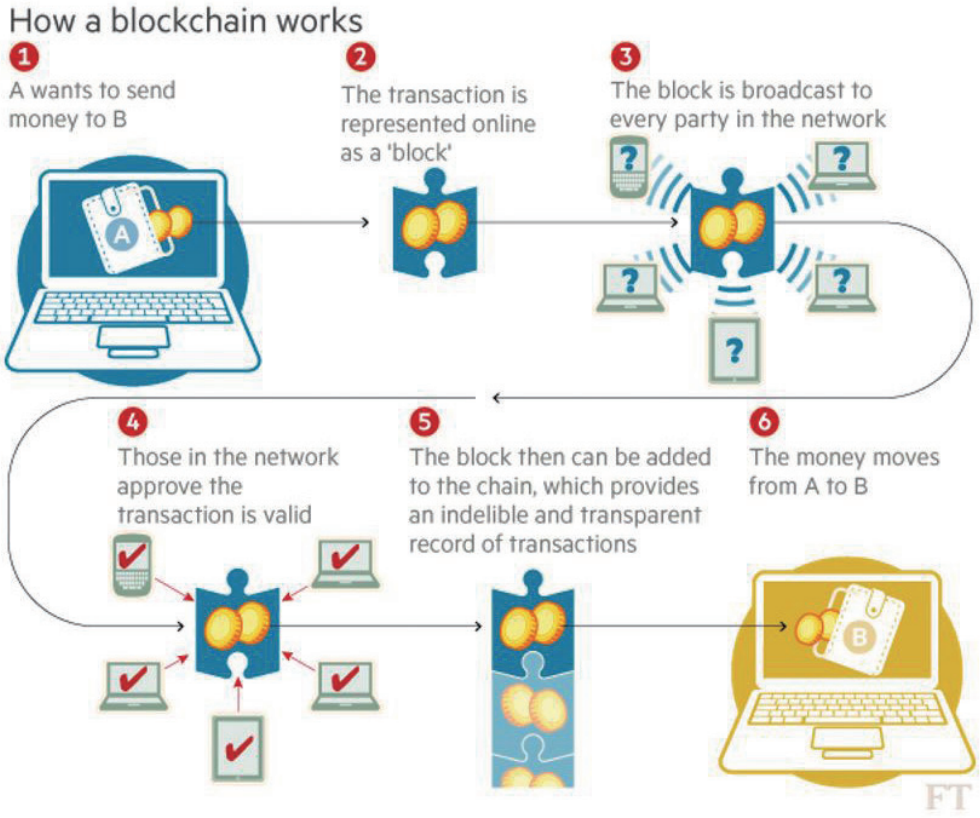
資料來源：本研究整理(2016)。

圖一　圖解公私鑰加密方法

不被攻破篡改，不能保證其安全性。和信用背書系統不同，區塊鏈是一個「分散式共享去中心化的帳本 (Ledger)」，區塊鏈上參與的人不需要對任何人信任，每筆交易記錄同步產生數個複本，由網路中的每個參與記帳的節點共同驗證持有，所有人可以看到全部的交易，最後將每個帳本依照時間戳記首尾相連在一起，形成了一長串排列的數據串，這正是區塊鏈 (Blockchain) 名稱的由來。而且，由於採取拜占庭容忍計算，隨著參與人數與節點的增加，交互複雜的網路上沒有人能完全掌握控制權，系統的安全性反而增加，所以交易記錄無法被篡改、被偽造，永久保存於帳本之中，還可以做到完全的公開。參考圖二：

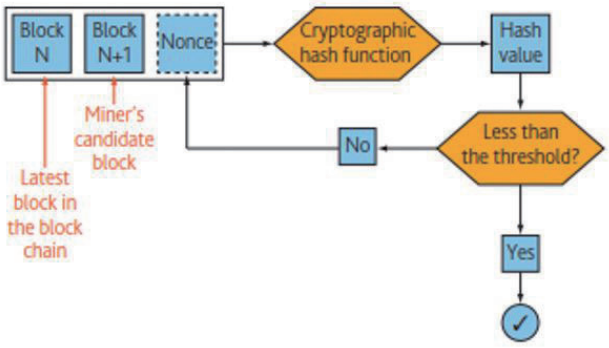
想像一下，村長家有一個佈告欄，所有村民在交易田地的時候都要寫在這個佈告欄上，所有的交易記錄按時間順序保留形成了一個鏈條不可以刪去，這樣在這個鏈條上延伸的交易都是可以相信的。再進一步要求每戶村民家門口都要有一個這樣的佈告欄，每次交易需要跑遍所有佈告欄添加記錄，這樣即使有幾家出現了火災或者記錄被篡改、毀棄，全村仍然可以通過多數原則糾正錯誤，這就是分散式共享去中心化的帳本。

比特幣採用工作量證明演算法 (PoW, Proof of work)，乃是通過對工作的結果進行認證來證明完成了某相應的工作量，就好像通過駕駛考試取得汽車駕照就是學習的證明一樣，不需要時時監測工作、學習的整個過程；工作量證明是一個可以用於網路上應對拒絕服務攻擊和其他服務濫用的經濟對策，因為它要求參與者進行一個數值運算工作，也就意味著參與者需要消耗電腦的運算資源。來執行交易



資料來源：《Banks seek the key to blockchain》by The Financial Times (2015)。

圖二　區塊鏈運作概念圖



資料來源：《Innovations in payment technologies and the emergence of digital currencies》by Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014)。

圖三　比特幣工作量證明流程圖

之驗證（詳如圖三）：任一個節點（被稱為礦工）提供自己電腦的運算資源，採用比特幣平臺提供的一套求解演算法，競賽完成加密雜湊 (Hash) 計算[1]，過程為將尚待驗證的交易打包成為候選區塊，候選區塊表頭 (Block Header) 的雜湊值乃是將前一筆區塊表頭的雜湊值與一 Nonce 隨機調整數作為輸入，通過加密雜湊函數與不斷變換 Nonce 值，重複進行嘗試計算出新的雜湊值，直到找到的隨機調整數使得候選區塊的表頭雜湊值小於一個會根據難度而線性調整的目標值，才會被加到區塊鏈中。首先達成雜湊值小於難度目標值條件的礦工，會將這個雜湊值寫入候選區塊區塊，作為礦工計算工作量的證明，除了可以獲得比特幣獎勵外，並取得區塊鏈上主帳本串連的權利，其他參與節點則繼續去驗證算出的雜湊值是否滿足比特幣平臺要求的運算目標，並接受這個區塊帳本有效，然後以副本形式留存下來，這就是所謂的「挖礦」。由於這個過程中需要耗費自己電腦大量的運算資源，在拜占庭容忍制約下，幾乎沒有任何人可以掌控超過 51% 以上的節點運算結果，從而確保了無需信任的共識建立。在區塊鏈交易驗證方法中，除了工作量證明演算法外，還有股權證明演算法（PoS, Proof of Stake）：採用相同於股權機制，由持股量多寡產生記帳人來創建交易區塊鏈及股權委託證明演算法（DPoS, Delegate Proof of Stake）：間接投票來選出代理人。此兩法皆比 PoW 共識機制消耗較少運算資源，每秒交易量（tps, transaction per second）的表現較好。

區塊鏈上所有用戶都可以建立交易，為了避免「重複消費」，必須有一套嚴謹的規範：例如當發起一筆交易時，預先凍結住全部資金，不讓參與者隨意分配資金，導致資金不足無法交易。比特幣評估交易的依據是：被整體區塊鏈上刪除條目的總資金額必須等於被創建的條目的總資金額。但是這種方法讓比特幣陷入交易確認時間長和難以小額大規模交易的缺陷。另一種方法是以太坊（Ethereum）的智能合約，規定對合約數據的所有修改必須經由程式執行。相較於比特幣的作法，以太坊保留了較大的彈性。

區塊鏈不僅用於金融交易，也可以作為註冊登記和庫存系統，用於所有資產如房屋、汽車等有形資產和選票、創意、名譽、意圖、健康資料等無形資產的記錄、追蹤、監視和交易。區塊鏈就像一個登記了所有資產的試算表，記錄各帳戶持有的各種資產形式的交易。以以太坊為例，憑藉著智能資產 (Smart Property)、智能合約 (Smart Contract) 與去中心化自律組織 (Decentralized Autonomous Organization) 的三項基本元件，在區塊鏈上註冊如氣象資訊、農機具等有形與無形的智能資產，透過互聯網結構建立唯一的識別碼，而由嵌入資產中的智能合約演算法在設定條件下，依照時間驅動（如抵押贖回）、事件驅動（如遺囑執行）、條件驅動（如對賭協議）、銀貨兩訖（如販賣機）等自動觸發所有權協議的執行。

不同的應用情境下，區塊鏈可完全的去中心化，或以有限的去中心化來實現，共識機制的不同讓區塊鏈有了公有鏈和私有鏈的分別。對於公有鏈來說，以比特幣挖礦為例，是由於參與挖礦可以獲得比特幣獎勵，在經濟利益驅動下的節點都願意參

[1]雜湊計算的基礎原理是將不定長度的字元運算變成另一固定長度值的數值。

與挖礦記帳，達到完全去中心化；但對於私有鏈來說，則需要通過另外一套共識機制來確立記帳的參與方式，於此，私有鏈給予特別部門少部份的控制權利，經由區塊鏈系統修改已發佈的文件，並將這些過程記錄下來提供備查。舉一個例子來說：對於一個已修改信用的人，一種方法是設置查閱權限，讓區塊鏈上的普通用戶無權查閱其多年前的信用卡違約記錄；另一種方法是通過監管機構來更改其信用記錄，比如當他還清欠款後，由監管機構將其從黑名單中移除。私有鏈就是以犧牲部分去中心化的特性為代價，來換取對於區塊鏈權限的一些特殊控制，並且可以使用比公有鏈更為高效、靈活、低成本的共識機制。除了公有鏈與私有鏈外，另外還有一種混合鏈，即預先指定一些節點作為可信節點來記帳，其他節點參與交易，外部可以經由指定節點的開放應用程式介面 (API, Application Programming Interface) 進行查詢。目前各金融機構看中的都是混合鏈，使傳統的金融機構可以繼續作為可信節點存在，並且避開公有鏈的「51% 攻擊」。

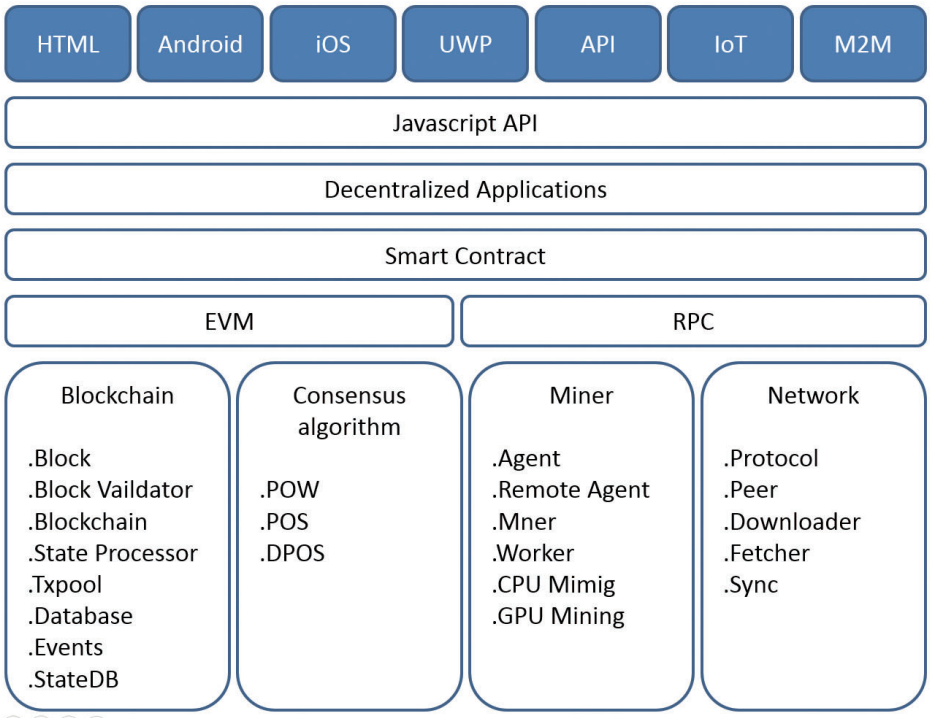
比特幣自 2009 年來經歷無數駭客攻擊和規模不斷擴張，仍以穩定的運行結果證明了區塊鏈的可行性。2015 年 10 月 31 日經濟學人雜誌稱區塊鏈為 Trust Machine，人們能通過網路與陌生人進行資產的交易，以實踐價值互聯的境界。此外，由於智能合約用程式碼而不是自然語言編寫合約條款，也給合約帶來可預測性和清晰度，可以用任何成為信息輸入的重要事實來測試智能合約，這樣交易雙方就可以預先知道合約執行方式及其可能的結果。

解析農業區塊鏈平臺

區塊鏈可以說是革命性的典範轉移，人與人間的互聯網可以同樣使得機器互聯的人工智慧經濟變為可能。農業區塊鏈平臺 (ABP, Agriculture Blockchain Platform) 可結合農業生產、加工製造、銷售、金融與農業政策、科技研究機構、氣候變遷、環境保護等形成全面性策略聯盟(comprehensive alliances)。隨著農業供應鏈環境變化，區塊鏈平臺可即時更新生產進程，是一項「動態生態系統的創新經濟活動」。運用以太坊區塊鏈技術將有形或無形之智能資產通過智能合約完全自動化執行註冊、存儲、確認、交易和移轉。以太坊上的各種應用 DAPP (Decentralized Applications) 中編寫的智能合約程式碼通過以太坊虛擬機器 EVM (Ethereum Virtual Machine) 對區塊進行驗證 (blockvalidator)，帳本由各節點進行共識演算 (Consensus algorithm) 的挖礦 (Miner) 作業和網路層 (Network) 資訊的交換，產生新區塊鏈後，呼叫 RPC 遠端程序[2]，在各節點間實現同步，從而執行各種交易轉帳等具體商業活動的過程。智能合約就像是一個在以太坊系統內的自動代理人，有自己的以太幣地址，當用戶向合約的地址發送一筆交易後，該合約就被啟動，然後根據交易中的相關訊息及自身程式碼的運行，返回一個結果。交易所需數據或交易產生的結果還可以經由 Javascript 程式語言的 API，透過 HTML 網頁、Android APP、iOS APP、Microsoft Windows10 APP、其他平臺 API、IoT 及 M2M (Machine to Machine) 介面等，輸入或輸出有用的數位資訊，詳參圖四。

農業區塊鏈平臺智能資產記錄所有田地資訊、種苗、農藥與肥料使用、農機具的安排等待交換訊息，「商業智慧合約」由時間與條件驅動，從農試所「農糧產銷決策管理資訊整合平臺」匯入銷售預測、天候、水利、土壤等生產條件所產生的生產決策資訊，人工智慧系統運算產生各種情境，經由「生產契作合約」驅動，使用智慧型手機 APP 下達生產命令，指導農民田間作業；「進貨合約」與「派工合約」處理原物料進貨、分級包裝、物流等協力廠商與臨時工的派工；並依據「採購合約」隨時滿足消費者與消費通路的採購；農機具、車輛、倉儲、種苗農肥料等原物料也可貼上 RFID，設備互聯與排工交易，以合乎最大經濟效益的原則大批量施作。所有流程運行的農情資訊由遙測、人工田間調查機構等蒐集完成後，交由物聯網「監控合約」事件驅動運作，隨即

[2]RPC(Remote Procedure Call)遠端程序呼叫是電腦一種通訊協定。該協定允許執行於一台電腦的程式呼叫另一台電腦的程式。

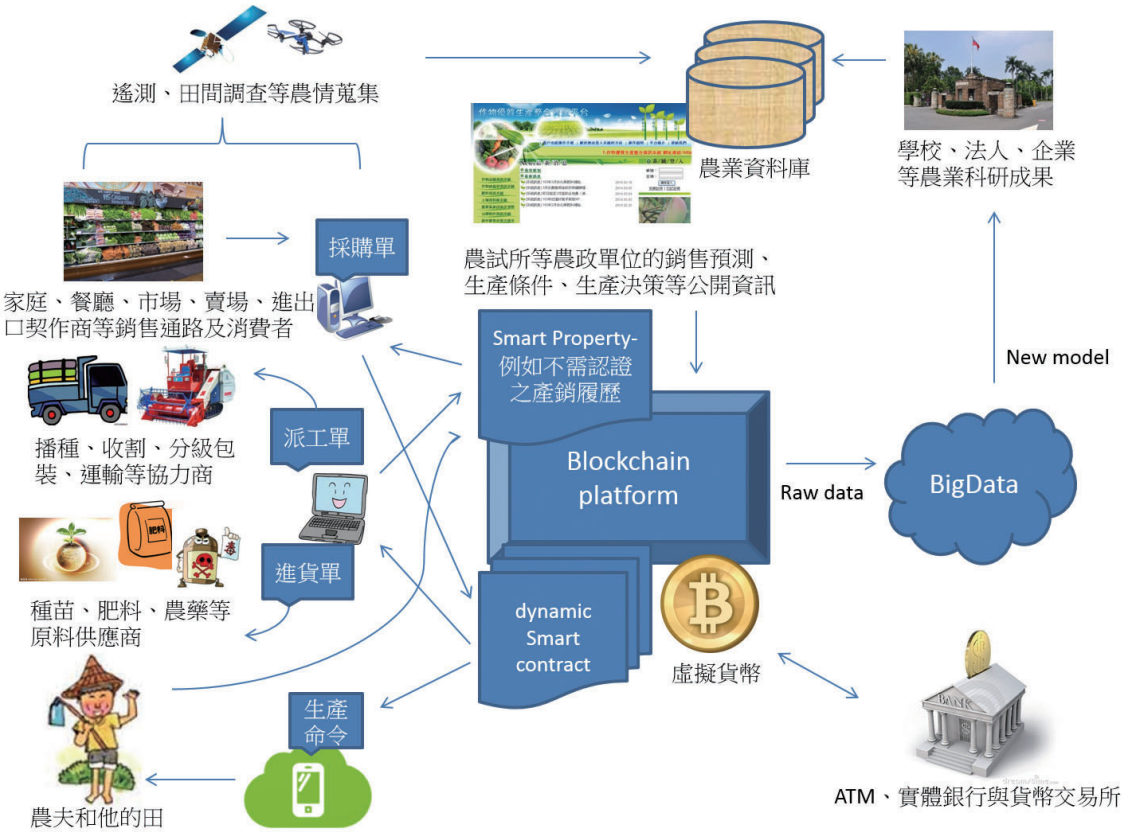


資料來源：本研究整理（2016）。

圖四　以太坊架構

回傳至農試所農業資料庫，以利「農糧產銷決策管理資訊整合平臺」及時處理。農業區塊鏈平臺所收集的大數據資料，經處理後產生新的數據模型，由研究單位做進一步的理論研究，具體研究成果並形成「農業資料庫」與「農糧產銷決策管理資訊整合平臺」的商業智慧。整個生態系統發行加密數位虛擬貨幣「農幣」做為封閉的交易媒介，能有效促進平臺內的價值交換和經濟性操作，並規避貨幣因外部因素影響農產品交易價格波動的風險，最後再交由網路貨幣交易所、虛擬貨幣 ATM 或實體參與銀行執行清算，非常容易兌換到更多的法定貨幣，如圖五所示。

農業區塊鏈平臺亦可導入去中心化政治權力和自主區塊鏈治理，這個概念源自於美國 George Mason 大學的教授 Robert Hanson，他將這個概念取名為 Futarchy：由於民主國家沒有一個成熟的機制即時讓利害關係人與決策者取得正確相關的訊息，而選民也缺少可以不用倚賴政治人物誠信或技術官僚專業的系統來評估與監督政府的決策品質，其後果往往會因為錯誤政策而陷入悲慘的境地。Futarchy 被簡短地描述為「為價值觀投票，用金錢賭上信念」(Vote Values, Bet Beliefs) 的雙重投票機制，並由以太坊專案創建人 Vitalik Buterin 闡述於區塊鏈中。當農政當局決定進行一項農業政策，在農業區塊鏈平臺的治理施作上是一套兩階段過程，第一步通過定期的表決程式展開：個人首先投票表決出具體的目標，例如 GDP 增長 1%；第二步經由預測市場展開：投票表決取得這些成果的建議方案。投票由加密數字貨幣構成，市場預測投票是投資在一個或另一個你想要贏的提案中下賭注，例如，相較於其他合約，如「投資於自動化農業合約」，你可能會下注於「投資於新的生物技術合約」作為實現「GDP 增長 1%」目標的最佳手段。通過這樣的選舉，



資料來源：本研究整理（2016）。

圖五　農業策略聯盟區塊鏈平台運作方式

區塊鏈可以更有效地實現 Futarchy 去中心化政治權力和自主治理的概念。

結語

全球化、科技化與氣候變遷嚴重影響臺灣農業發展，2014 年臺灣農業貿易逆差擴大到了 103.4 億美元，似乎臺灣農業競爭力明顯不足。然而，小農是社會重要的安全閥，根據聯合國糧食與農業組織 (FAO, Food and Agriculture Organization of the United Nations) 統計，在亞洲和撒哈拉以南的非洲，小農提供了高達八成的糧食供應。此外，小農耕作對縮短食物里程，降低二氧化碳排放有著重大貢獻。面對臺灣農業競爭力不足的問題，我們當從銷售通路端來看小農所遭遇的挑戰：2014 年呂雪玉、2013 年陳巧娟、2012 年莊淑媛、2011 年紀力有等人，針對糯米、甜玉米、甘藷、番茄等運銷通路的研究發現 82.5%-95% 的農產品是經由批發販運商或是契作商銷售，但是自產自銷的利潤卻為最高。因此，如何平衡各種通路，讓農戶收入增加，是一項重要的課題。再者，隨著市場建物老舊及農產品批發交易量擴大，各地方現有魚市、果菜市場早已不敷使用，地方政府又囿於預算，無力負擔動則上億臺幣的改建經費，唯有新增其他銷售通路，才能解決這一難題。想像一下，如能在農業區塊鏈平臺上產銷，其透明、快速的交易，除可免除上下游業者大量的交易成本外，亦可主動約束農藥與化肥的使用量，節省生產成本。

2003 年雲林縣古坑鄉打出「臺灣咖啡節」，帶

動臺灣發展地方特色產業的熱潮。隨著各地競相舉辦類似的慶典，邊際效用遞減下，消費者熱情不再，古坑咖啡也就逐漸沒落了。從這個案例來看，凸顯出利用行銷活動來銷售農產品有侷促性。相比之下，農業區塊鏈是一個永久有效的認證平臺，產銷過程的公開透明能清晰記錄食品的產地和加工配料，取代須送驗第三方認證的「產銷履歷制度」，為農產品提供直接品質認證的服務，給消費者帶來足夠的信任。農家也就不需要再花錢辦活動推廣自己的農產品，只要加入農業區塊鏈平臺的完善供應鏈，農產品就能暢銷。

近年來，臺灣糧食自給率大約在 30%上下，2013 年臺灣的糧食自給率大約是 33.28%，同時期農業環境與臺灣相近的日本為 39%，韓國則為 50%。可見臺灣的糧食自給率尚有很大的增長空間。未來，經由農業區塊鏈平臺的導入，食材主要於平臺的封閉經濟體系內在地消費，再加上如「廚餘換糧」、「積點加贈」等農業政策的區塊鏈治理之智能合約協助，可有效提升臺灣自身的糧食自給率。

如今，機器人、物聯網、人工智慧正逐步攻佔人類事務，美國國民收入占比已從勞動力流向資本，跟隨著這一波趨勢，此時不加緊投入農業區塊鏈的運作，更待何時？！ AgBIO

徐逢桂　南京農業大學　博士

參考文獻

1. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014) *Innovations in payment technologies and the emergence of digital currencies*. Bank of England Quarterly Bulletin.
2. David C. Parkes and Michael P. Wellman (2015) *Economic reasoning and artificial intelligence*”, SCIENCE, 349(6245:267-272.
3. Jane Wild, Martin Arnold and Philip Stafford (2015) *Bank seek key to blockchain. The Financial Times*, From www.ft.com.
4. Melanie Swan (2015) *Blockchain-Blueprint for a New Economy*, Tim McGovern, O’ Reilly ,9-11.
5. SUSTAINABILITY PATHWAYSSMALLHOLDERS AND FAMILY FARMERS.From www.fao.org.
6. 呂雪玉 (2014) 台灣番茄產業之產銷分析－以台南市為例。臺灣大學農業經濟學研究所碩士論文，頁28-32。
7. 紀力有 (2011) 臺灣甘藷產業之產銷分析—以雲林縣水林鄉為例。臺灣大學農業經濟學研究所碩士論文，頁24-27。
8. 苑守慈 (2016) 區塊鏈對創新經濟多元產業的影響。中時電子報，From www.chinatimes.com。
9. 陳巧娟 (2013) 臺灣糯米產業產銷分析—以雲林縣為例。臺灣大學農業經濟學研究所碩士論文，頁61-71。
10. 莊淑媛 (2012) 台灣甜玉米產業之產銷分析—以嘉義縣地區為例。臺灣大學農業經濟學研究所碩士論文，頁31-32。
11. 鄭逸寧 (2012) 農委會打造產銷資訊整合平台，農業雲三大構面成形。From www.ithome.com.tw/article/91042。