區塊鏈應用於林業之現況與挑戰

⊙林業試驗所主任秘書室・林俊成 (ljc@tfri.gov.tw)
⊙國立臺灣大學森林環境暨資源學系・邱祈榮
⊙林業試驗所林業經濟組・詹為巽、徐韻茹

什麼是區塊鏈？

隨著比特幣(Bitcoin)的興起，區塊鏈(Blockchain)技術的應用引起全世界的關注，世界經濟論壇(World Economic Forum, WEF)創辦人施瓦布(Klaus Schwab)提到，區塊鏈將繼蒸汽機、電力和電腦發明而帶動第四次工業革命；俄羅斯聯邦儲蓄銀行(Sberbank)副主席夏洛夫(Andrey Sharov)也預言，區塊鏈技術會讓銀行在10年內消失(商周，2016)。所謂區塊鏈是基於分散式帳本技術(Distributed Ledger Technology, DLT)的原則下運作的一種資料結構。DLT用於跨多個電子帳本記錄和共享資料，每個帳本具有完全相同的記錄，並由電腦伺服器組成的分散式網絡所共同維護和控制(Rocamora & Amellina 2018)。DLT有三個關鍵特徵：帳本的分散式特性，共識機制和加密機制(World Bank 2017)。在DLT內，資料由網絡的不同成員以互補的方式共享、驗證和存檔，當網絡成員將資料輸入系統時，由其他成員驗證該條目並分配數位簽章以證明其在網絡中的存在和有效性(Rocamora & Amellina 2018)。同時區塊鏈中的資料在網絡的所有節點之間共享，所有節點中都存在相同的資料使其不易被竄改。因此，區塊鏈技術引入了更高的透明度和效率，使網絡能夠在不可信賴的環境中完成可靠的交易(Figorilli et al. 2018, Pinna & Ibba 2018)。

區塊鏈是由一個個稱為「區塊(blocks)」的小型加密資料集組成的線性序列，其概念如圖1所示，這些區塊中都包含前個區塊的引用和複雜加密的解答，該加密用於驗證交易，作為分散式帳本系統交易記錄，並分散於電腦或資料庫所組成的網絡中(Figorilli et al. 2018, Lin et al. 2017)。一個區塊有兩個部分，標題和內容，標題包括一組特別的區塊引用標識碼，創建區塊的時間以及返回上一個區塊的鏈結；而內容，通常是經過驗證的數位資產和指令，例如所進行的交易，其金額以及這些交易當事人的位址。

區塊鏈中每個區塊都連接到各項交易，系統或節點(node)中的成員只能添加經過其他節點驗證的交易，在將新區塊添加到區塊鏈之前，需要一致的機制來驗證此區塊是否滿足預定的標準和系統規則，此驗證步驟稱為hashing，其功能包括解決指定的數學加密。這個加密的正確答案稱為nonce。一旦節點找到了nonce，其他節點就會對其進行驗證，然後將一個稱為hash的加密標標籤提供給交易。然後，創建由該加密的數字標識組成的資料區塊，在達成共識後才可以將新的區塊添加到區塊鏈中。新的區塊將鏈接到同一鏈中的有同樣資料的先前區塊，當一個區塊被添加到區塊鏈中時亦將通知系統成員取得分散式帳本中區塊的副本。

區塊鏈系統基於以上特徵，可以歸納出8項功能(Rocamora & Amellina 2018)：

1. 作為一種靈活的資料結構，區塊鏈可以管理各種類型的資料並將其轉化為有價值的數字資產。有關單一文件、交易、證書、

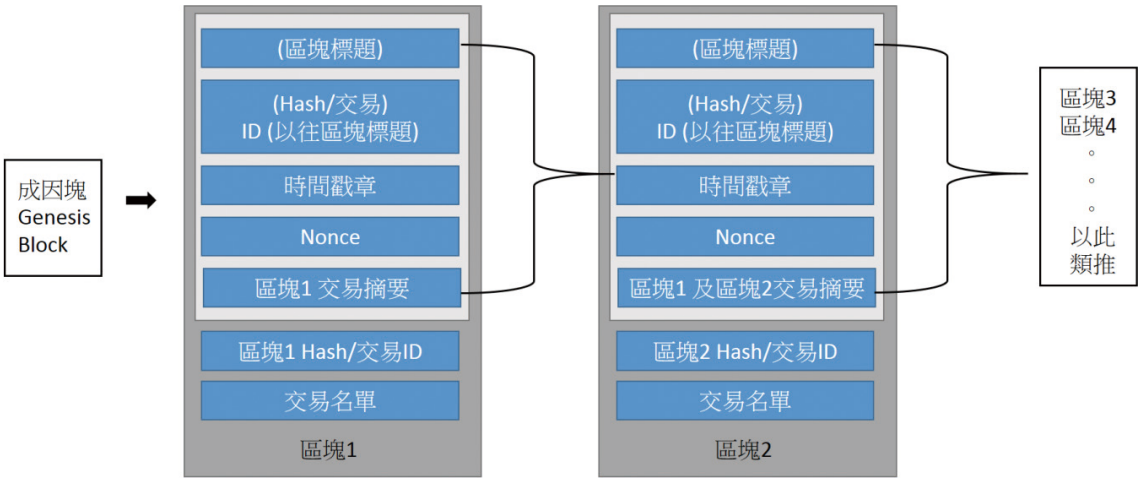

圖 1 區塊鏈之結構(修改自Rocamora & Amellina 2018)。

事件、數量、儲備、身份、產品或其中一組的訊息，涵蓋從能源到消費品的廣泛領域，可以全部共同商定為新資產，一旦以數字方式記錄在區塊鏈中，即可以作為「加密貨幣(cryptocurrency)」進行交易(Rocamora & Amellina 2018)。

2. 利用實時運行自動化和數字化操作的定製程序，區塊鏈已被用於創建「智慧型合約(smart contract)」，這是一種通用產品類型，可促進、驗證和記錄多方之間的交易和協議。智慧合約將減少為所有相關方支付和結算所需的時間，這將大幅度地減少當前執行人工驗證所需的傳統第三方的需求(Rocamora & Amellina 2018)。
3. 區塊鏈系統屬分散式的，使交易運行得更快，點對點交易(peer to peer transactions)讓非正規或小型企業可以獨立運作，因此，越來越多對等企業面對新的貨品、商品和服務(Rocamora & Amellina 2018)。
4. 區塊鏈資料庫保留自創建第一個區塊以來執行的所有資產和指令的完整歷史記錄，並將控制權分配給所有系統成員。此資料問責制(data accountability)可讓交易雙方不會在只單靠一方(如銀行)的信譽下進行交易(EY 2017)，在區塊鏈的參與者和審核員之間建立新的信任類型(Rocamora & Amellina, 2018)。
5. 區塊鏈系統的優勢之一是其透過數字加密協議，用於保護和記錄交易的資料安全性(data security)。這表示區塊中的原始資料、檔案、證書和其他資產對其所有者和各方保持安全。區塊鏈的資料庫的分散式賬本也很難攻擊，因為網絡攻擊必須同時攻擊每個資料副本，才會破除區塊鏈系統的資料安全性(EY 2017, Rocamora & Amellina 2018)。
6. 為了預防詐騙(fraud prevention)，每個區塊標籤和資料引用號碼、創建者、驗證者、共識創建時間以及包含先前交易訊息的其他區塊的鏈接都可以被追蹤和破

譯。它提供了具體、可追溯和永久的資產所有權。由於區塊鏈未經所有相關方的同意不能被修改或操縱，它可以防止腐敗的政府或公司不公平地驅逐或扣押人的資產(Rocamora & Amellina 2018)。

7. 以分散式方式管理帳本可降低雙重記錄的風險，減少因資料庫協調差異導致的錯誤，消除執行事務的等待時間，並減少對中介的需求。還可將每個區塊的副本分發給系統的每個成員來嵌入備份系統。這些功能將提高涉及多方的任何類型業務的營運效率(operational efficiency)。在2018年初，區塊鏈技術開發商和一家獨立研究機構之間的合作宣布了區塊鏈技術在將移動產品交付時間提高34%，生產力提高29%，品質提高11%(Aricent 2018, Rocamora & Amellina 2018)。
8. 區塊鏈系統可以加強物聯網系統(Strengthening IoT networks)，收集並安全的儲存即時資料。透過從物聯網設備收集的加密資料直接儲存到區塊鏈中，物聯網網絡運營商可以節省大量成本和技術工作，為每個設備建立和整合單個物聯網網絡。區塊鏈的加密安全措施和分佈網絡還可以幫助解決物聯網的安全性問題並提高其可靠性(Rocamora & Amellina 2018)。

區塊鏈與木材追蹤

非法伐採一直是為危害全球森林資源的主要原因之一，根據聯合國環境和刑警組織(UN Environment and Interpol)估計，全球的原木貿易量約有10~30%是非法的，意味著非法伐採及其貿易會導致每年至少510~1,520億美元的損失(Nellemann et al. 2016)。且非法木材貿易也導致全球林產品價格下跌，衝擊森林永續經營目標的達成(邱祈榮等人，2009)，不僅造成嚴重的資源消耗，也對當地經濟造成傷害。因此如美國雷斯法案修正案(Lacey Act Amendment)、歐盟木材法案(European Union Timber Regulation, EUTR)及澳大利亞禁止非法伐採法案(Illegal Logging Prohibition Act, ILPA)，透過法令管制木材進口來杜絕非法伐採木材及其製品流入市場，以確保商品具合法性和永續性。皆要求市場上木材及其製品之生產商和進口商，在首次進入該國國內市場時，都必須透過盡職調查體系(Due Diligence System, DDS)或盡責調查(Due Care)來進行風險管理，其目的在於降低及避免非法木材及其製品進入國內市場，進而確保所有進入國內市場的木材及其製品屬合法伐採與貿易的(林俊成、邱祈榮，2017)。但是此過程較為依賴紙本證明，過程冗長、較昂貴且不環保，內容物亦容易被篡改。屬於集中設計的監管鏈，也有複雜手動認證程序(Düdder & Ross 2017)。

如圖2所示，區塊鏈系統有助於追蹤木材的問題，當局監督合法木材並在區塊鏈中證明其合法狀態，區塊鏈條目(交易)可以鏈接到物理證據，例如其數字形式的DNA簡檔作為加密散列，進口公司就可以查詢區塊鏈以獲得複合產品或其組件的認證資訊(Düdder & Ross 2017)。

Paletto and Notaro(2018)的研究結果顯示，約有30%的義大利受訪木材製造商願意為認證木板支付2.40%的平均溢價，而19.0%的人願意為認證木板支付2.68%的溢價(Figorilli et al. 2018, Paletto & Notaro 2018)。

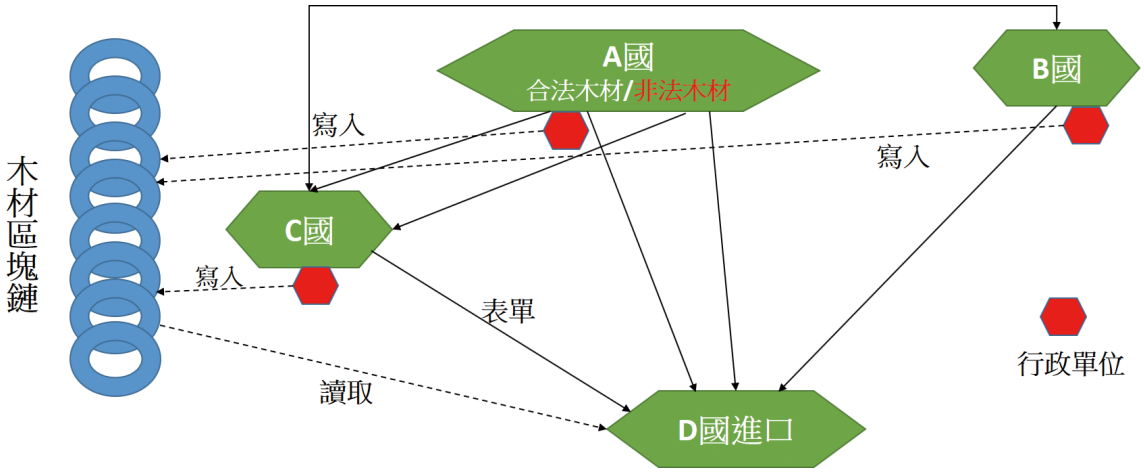

圖2 使用區塊鏈技術的非法木材的盡職調查COC情景(修改自Düdder & Ross 2017)。

Sperandio et al.(2017) 對從森林到工業的無線射頻辨識(Radio Frequency Identification，RFID)和開源技術實施進行了經濟評估，分析簡化操作和更有效利用資源的真正可能性(Figorilli et al. 2018, Sperandio et al. 2017)。這表示如何使用這些技術進行木材可追溯性已經可行，且經濟上可持續，因為大多數擬議方案與追蹤木材的價格上漲低於5%，因此與上述結果相符(Figorilli et al. 2018)。作為一項取決於供應鏈維度，且不斷發展的技術，區塊鏈實施所帶來的成本增加在經濟上也被認為是可持續的(Figorilli et al. 2018)。隨著資通訊技術的快速發展，區塊鏈應用成本將迅速降低(Figorilli et al., 2018；Tian, 2018)。Düdder & Ross(2017)亦認為區塊鏈技術可以預防供應鏈之供貨量的弊案，這是當前供應鏈管理系統的一項重大挑戰。區塊鏈技術亦可讓對環境和社會負責的商品之採購更高效，更值得信賴。使公司行號可以更負責任的從通常被視為高風險市場的區域採購到更廣泛的原物料，同時確保環境和社會可持續性，可能可以將以前被認為是無活力林地的森林區，轉變為油棕樹種植園和其他農業用途(Düdder & Ross 2017)。

區塊鏈系統不但可以提升供應鏈效率、減少廢棄物，亦可以透過提供公司和產品相關的詳細即時訊息，實現可持續生產和消費以及循環經濟的最重要影響之一。消費者得到的產品相關訊息受到零售商及其在整個供應鏈中的影響的限制，無法得知商品的生產和貿易可能對世界許多領域產生巨大的負面可持續性影響，如環境污染和森林伐砍等。可以提供即時和詳細訊息的區塊鏈為此問題提供了解決方案，透過QRcode或RFID晶片追蹤和紀錄區塊鏈上的產品訊息，消費者將不再需要依賴銷售產品的公司提供的已被過濾的訊息，只需透過區塊鏈系統取得產品規格和相關訊息。

區塊鏈還可以大幅提高可持續發展相關認證的完整性和實用性，例如與公平貿易或有機產品相關的認證。可持續性標準和標籤

一直是可持續消費發展的核心工具。由於缺乏產品相關訊息，此類認證一直是產品可持續性最可靠的保證。然而，可持續性標準和標籤系統存在一些缺陷，使得它無法獲得可以滿足道德消費需求的大眾。透過其分佈的性質，區塊鏈為這種情況提供了解決方案。依靠一個集中實體來保證產品的可持續性會產生固有的偏見，因為任何第三方都可能容易受到賄賂、社交工程或有針對性的駭客攻擊(Provenance 2015)。透過分散的資料記錄，區塊鏈使供應鏈參與者、認證者和消費者能夠即時取得不可變資料。雖然供應鏈參與者之間的關係是線性的(生產者由認證機構審核，誰發布認證，構成消費者唯一的信任點)，但透過區塊鏈，各方之間的信任結構變得多向，如圖3所示。

然而，區塊鏈技術目前與木材供應鏈追蹤所遇到的問題包括：

1. 一個可以識別計算、性能、持續性、安全性和隱私需求的數位追蹤技術。
2. 能使用智慧型合約分析工具來支持用戶的生產性應用流程的開發，並保證智能合約的安全性和安全性的區塊鏈。

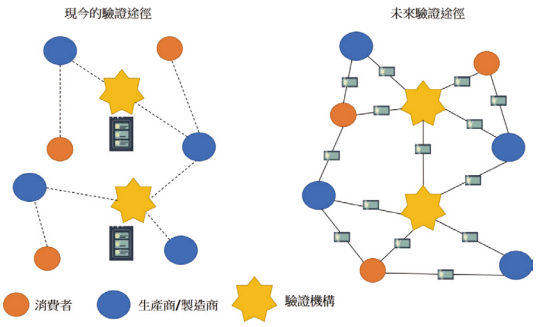

圖3 區塊鏈裡供應鏈參與者之間的線性關係(修改自Provenance 2015)。

3. 具有合約管理結構的系統，當無法恢復交易時，可以在區塊鏈技術上提供安全的執行環境。

區塊鏈與氣候行動、碳管理

除了永續經營外，氣候和碳管理也是與林業經營息息相關的議題。尤其是在1997年的京都協議後，許多國家開始限制每年生產的溫室氣體量，而其中一個方法是建立排放交易計劃(Emission Trading Schemes, ETS)。如果產生的溫室氣體超出預定的上限，參與國家必預付費補償，個人或公司行號可以透過購買碳抵消來限制自己的碳足跡，而用於購買補償所獲得的資金，會流向減少溫室氣體排放的計劃。這種方法的交易侷限於區域性，且缺乏透明度(Düdder & Ross 2017, Thrill 2018)，但區塊鏈系統就可以改變這種現況，透過建立代幣化的碳信用交易平臺，公司行號或個人能透過智慧型合約，購買不同類型的碳信用代幣，而此區塊鏈系統又稱為氣候幣(Climatecoin)。區塊鏈的智慧型合約的特點，可能有助於擴大處理毀林和森林退化的機制，同時佔全球溫室氣體排放的10%(Düdder & Ross 2017, Obergassel 2015)。任何符合CDM(Clean Development Mechanism, CDM)黃金標準的計劃都可以創建自己的代幣，並附上碳信用額度，這些電子代幣將於智慧型合約中發放，並將其與乙太坊區塊鏈(Ethereum blockchain)連接(Thrill 2018)。

以減少森林伐砍和恢復退化森林成果進行付費的REDD+，其機制內的付款方對核實減排量的有效性持謹慎態度(Drazen & Graham 2018)，此外，人們對其交易缺乏透明度和防

止重複計算表示關切(Düdder & Ross 2017)。所以在第23屆締約國大會(COP23)會議中，提議將區塊鏈系統之智慧型合約功能與REDD+結合實施的可能性(Bakkegaard 2017)，將區塊鏈技術與REDD+實施中存在的問題相結合。這個提議讓許多學者覺得值得研究，以求證區塊鏈的智慧型合約可以將REDD+機制的實施，促進到多大程度(Düdder & Ross 2017)。區塊鏈系統可以在不受信任的環境中創建信任，可以跳過中間人，允許點對點交易和追蹤所有權的特性，可以跟REDD+完美的搭配(Robinson 2018a)，將區塊鏈的潛在優勢與REDD+面臨或持續面臨的挑戰相互連結如圖 4所示(Robinson 2018b)。如果每次消費都有相關的碳價，且由REDD+計畫抵消而節省的每噸碳都可以在區塊鏈上註冊，消費者亦可以追蹤他們的交易記錄。理論上，這項技術可以消除與多中心治理相關的複雜性，並允許森林所有者透過與消費者的點對點互動，以獲得更大的保護森林的利益(Robinson 2018a)。智慧型合約也可能有助於碳交易，將計算機代碼代入區塊鏈，以便自動促進、執行和執行協議或履行協議(Verhagen 2017)。

結語—使用區塊鏈的主要挑戰

國際上已經有許多國家、機構已經開始或打算將區塊鏈技術納入林業管理使用，如西班牙已經成立名為ChainWood的工作小組，透過在工業物流中實施區塊鏈技術來提高西班牙木材供應的可追溯性和效率(Yakubowski 2018)。在西伯利亞，也有鋸木廠生產公司透過區塊鏈技術(WoodsCoin)讓投資者提供融資。WoodsCoin可以讓伐木廠接受委托，透過機械化的方法伐砍木材、準備和鋸切原木、形成鋸材部分、加工成品木製品、將產品裝載到運輸系統(Bitcoin Exchange Team 2018)。泰國也有專案小組將透過區塊鏈技術鼓勵民眾植樹，2019年以清萊府退化森林區域為

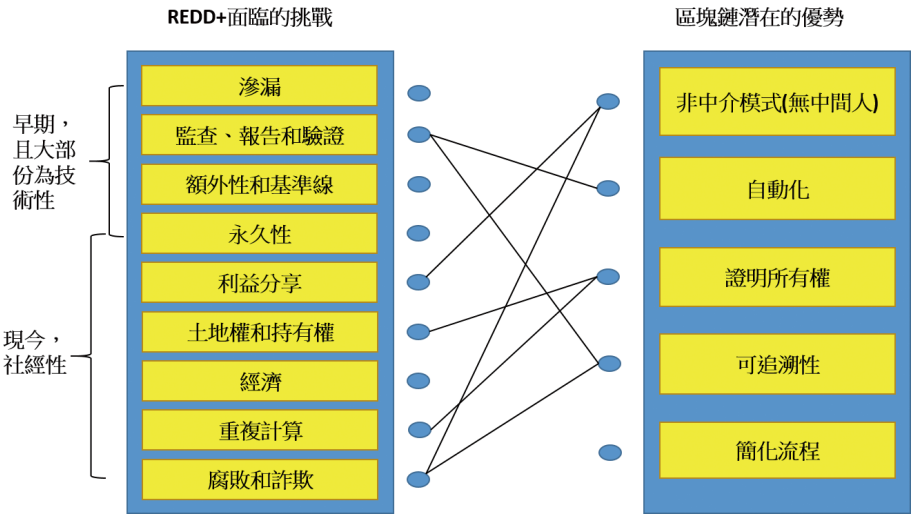

圖4 區塊鏈的潛在優勢與REDD+面臨或持續面臨的挑戰概念圖(修改自Robinson, 2018b)。

目標，種植者可依其所種植的每棵樹成長情形，獲得森林幣(Forest Coins)為回報，預計未來將該區規劃成生態旅遊區，並且將其行動擴展至泰國其他退化森林區(CoinSchedule 2018)。國外亦有企業將區塊鏈技術納入其碳信用貿易策略，IBM跟Veridium Labs合作創造數位代幣，目的為讓碳信用貿易簡單化。同時，知名冰淇淋品牌-班傑利公司(Ben & Jerry’ s)每賣出一支冰淇淋，就會捐一分美元給Poseidon基金會，並且會讓消費者自行選擇要不要加入捐一分美元的行列。然後由Poseidon 基金會匯總捐款以購買補償，並讓消費者看到他們的捐款如何幫助抵消冰淇淋筒的碳成本(Sherry 2018)。

區塊鏈的特性可以很好地適用於許多環境應用，其中包括減少森林伐砍造成的排放(Chapron 2017, Robinson 2018b)。儘管有許多學者觀察到許多潛在的應用，但由於區塊鏈仍屬新技術，仍然面臨著許多挑戰。隨著它逐步進入更成熟的階段，區塊鏈可能會解決其大多數問題，並獲得更多的市場焦點(Rocamora & Amellina 2018)。如上所述，由於該技術有望對大多數經濟造成困擾，因此區塊鏈面臨著許多不同的挑戰如圖5所示，這些挑戰可分為三類，即技術挑戰、監管挑戰和社會挑戰(Rocamora & Amellina 2018)。根據Hileman和Rauchs(2017)的觀點，區塊鏈採用面臨的最大挑戰是缺乏監管框架，其次是保密問題和機構不情願(Hileman & Rauchs 2017, Rocamora & Amellina 2018)，同研究評估的其他挑戰包括技術不成熟、構建業務網絡的困難，與資料保護法的潛在衝突以及性能問題。EY(2018)進行的另一項調查證實了這些調查結果，61%

圖5 區塊鏈面臨的主要挑戰(修改自Rocamora & Amellina 2018)。

的受訪者認為監管複雜性是廣泛採用區塊鏈的最大障礙，其次是與傳統技術的整合(51%)以及對區塊鏈能力缺乏一般性了解(49%) (EY 2018, Rocamora & Amellina 2018)。在REDD+方面，區塊鏈也有無法解決的問題(Robinson 2018b)，例如雖然區塊鏈可以記錄缺非機構(如原住民社區)的土地權利，但它無法首先設定這些土地權利，在區塊鏈技術可以記錄和保護這些權利之前，政府仍然需要承認原住民社區的權利(Robinson 2018b)。區塊鏈對於REDD+的某些技術方面也很有限，例如解決永久性問題，即使區塊鏈擁有所有森林中的每棵樹都的DNA記錄，也無法阻止非法伐木者將其伐砍，並釋放出多年來在保存的碳(Robinson 2018b)。這些控制森林伐砍活動的措施，突顯了使用區塊鏈技術管理氣候變化的想法，且目前這些計畫都處於初期階段，這項技術仍需要時間才能成為主流(Robinson 2018b)。