❒ 書評：*The Truth Machine: The Blockchain and the Future of Everything*〔眞理機器—區塊鏈與數位時代的新憲法〕by Paul Vigna and Michael J. Casey〔保羅．威格納與麥克．凱西〕（St. Martin's Press, 2018, Hardcover, 320 pp., ISBN 9781250114570）

李宣緯
中央研究院

壹、背景與緣起

No state or corporation can put bricks around the Bitcoin blockchain or whitewash its record. They can't shut down the truth machine, which is exactly why it's a valuable place to record the voices of human experience, whether it's our love poem or our cries for help. This, at its core, is why the blcokchain matters.

— Paul Vigna and Michael J. Casey,
The Truth Machine: The Blockchain and the Future of Everything

故事開始於約旦的敘利亞難民營，多數在這裡的人們因爲戰亂流離失去銀行帳戶與各種證明文件，在傳統的金融和法律體系內，他們失去了身份。然而區塊鏈技術成爲難民回歸正常生活的關鍵，這是首次區塊鏈運用於人道援助，

李宣緯 中央研究院社會學研究所助研究員、國立臺灣大學政治學系兼任助理教授，研究領域爲複雜系統、計算社會學、賽局理論與機器學習。

Hsuan-wei Lee is an assistant research fellow at Institute of Sociology, Academia Sinica. He is also an adjunct assistant professor at Department of Political Science, National Taiwan University. His research focuses on complex systems, computational sociology, game theory, and machine learning.

ISSN 1726-9350 print / 1811-3109 online © *2019 by Taiwan Foundation for Democracy* / Vol. 16 No. 2 / June 2019

世界糧食計劃署用例如虹膜掃瞄等生物辨識，確認難民在聯合國數據庫的數據，重新還原身份以分發糧食或提供協助。難民在營地工作所得到的工資，雇主亦可匯至工作者的帳戶，讓他們在手機上使用電子錢包。區塊鏈減少跨境支付的交易費用、提供可追蹤的各項資產轉移紀錄，亦使得捐給難民的善款做最大程度地使用。有了身份的確認，這些人便和世界經濟重新接軌，可以工作接受薪資、購買物品、證明學歷甚至借貸創業，區塊鏈成爲幫助他們追求安全與福祉的核心技術。

區塊鏈是一種將加密方法與分散式計算結合的資訊技術，利用計算機網絡協作以維護和共享資訊，比集中式的儲存更安全且更不容易被竄改。不只做爲資料庫，自動化的程式也可以在區塊鏈中檢驗條件以執行結果，這十年來區塊鏈技術與在其上的各種加密貨幣，從默默無聞到成爲熱門的投資標的以及企業應用。本書是區塊鏈技術與發展的科普讀物，由兩位經驗豐富的資深金融記者撰寫，他們同時也曾寫過一本比特幣的介紹書。作者以敘事的方式將加密貨幣與區塊鏈技術，用最簡單的語言書寫，並闡述複雜細節背後的內在邏輯。本書提供了區塊鏈技術與產業應用的最新快照，作者也檢視了區塊鏈對政府、科技業和金融業的種種挑戰與風險，以及自由主義與個人主義如何可以透過區塊鏈實踐。

貳、本書核心論述

一、從比特幣、以太幣到第三代區塊鏈的興起

比特幣與區塊鏈可以視爲會計分類帳的革命，但其影響力卻遠不僅只於此。分類帳是對所有權的記錄，定義誰擁有什麼與交換什麼，有了清楚可信任的分類帳後，交易和經濟活動才得以產生。分類帳通常由政府與企業靠法律制度維持，商業行爲遇到紛爭時，也往往是由這些公權力機關裁決或強制執行。這種集中式處理資訊的方式，在速度和效率方面具有許多優勢，但這也意味著

人們必須信任中介機構，讓渡權力交給這些集中式機構協調管理，同時不斷努力限制這些機構過度膨脹它們的權力。

區塊鏈在分類帳紀錄中增加時間的屬性，資訊由一串區塊組成，每個區塊都是一個已加密的數據紀錄，其內容可以是各種文字、圖片或其他訊息，通常人們將資產轉移的紀錄放在區塊中，加密使得這些資訊難以被竄改。在區塊鏈網路系統內的計算機，可以透過解一組需要大量隨機測試的數學問題，驗證一個區塊所需數值，並廣播該區塊資訊至系統內的所有計算機，永久記錄於區塊鏈上，這組幫助成功驗證區塊的計算機，也得到例如比特幣等區塊鏈代幣的財務獎賞。從 2009 年初起，比特幣區塊鏈內每十分鐘就產生這樣的區塊，區塊間彼此連接，按照正確的線性時間排列。區塊鏈的時間相依特性使得這些資訊不能被刪除，如果一個區塊被更改，系統內所有計算機上的區塊鏈需要同時被更改，這有助於保障數據的正確。更重要的是，在開放的區塊鏈環境中，任何計算機可以自行加入區塊鏈，通常不需要被系統預先許可，促進計算世界中眞正的民主與去中心化。

在區塊鏈上的訊息傳輸使用公私鑰加密，公鑰是一個隨機的長數字串，是區塊鏈上的一個地址。私鑰像是公鑰的密碼，擁有者可以任意處置其中資金或進行交易。公鑰與私鑰相聯，任何人都可以用接收者的公鑰地址加密資訊，但加密的消息只能用接收者的私鑰解密。通過這種方式，只需要保密私鑰，公鑰可以在不影響安全性的情況下公開分發。如果想在比特幣區塊鏈上獲得資金，可以使用一個類似電子錢包的軟體創建一個公鑰，讓匯款者把比特幣發送到那個地址，再用自己的私鑰解鎖得到比特幣。

第一代的區塊鏈雖然可以記錄點對點的價值交換，卻不支援應用程式所需的條件判斷與迴圈等高階運算，或者稱爲不具有圖靈完備性，無法執行複雜的應用程式。但在短短數年內，第二代的以太幣區塊鏈便可構建應用程式，本質上它是分佈式的虛擬計算機，可以使用系統內所有計算機執行程式。以太幣區塊鏈關鍵技術創新之一就是開發智能合約，智能合約是存儲在區塊鏈內的計算

機代碼，區塊鏈編碼形成協議與自動判斷條件執行的合約，消除了合同成員之間對可信第三方的需求。智能合約既由計算機代碼定義，又由程式自動執行，允許合約成員自治，決策無需依賴傳統權力集中的權威決定，更有自由、快速、無法被竄改等優勢。

然而按照字面意義自動執行的程式存在非常大的爭議，這些自動執行的合同服從於具有明確指令的規則，但這其中有許多設計者無法預見的情況產生。例如 2016 年以太幣區塊鏈便發生去中心化的組織被沒有違反程式字面意義下的駭客攻擊損失慘重，造成社群分裂擁護不同版本的以太幣。比特幣也曾因社群成員對區塊容量大小等版本議題引起熱烈辯論與形成不同分支。區塊鏈治理更增加了市場機制的考量，依舊要協調成員利益和取得平衡，就算是去中心化的組織，系統內的規則制定和政治角力仍然是重中之重。

第三代的區塊鏈在區塊鏈基礎設施未臻完善下百家爭鳴。目前區塊鏈雖已跨國界與去中心化，但成本太高且系統無法處理大量即時交易，用比特幣買一杯咖啡的錢所需支付的手續費遠超過咖啡價值本身。另外比特幣內的許多區塊鏈在驗證區塊時需要耗費大量運算資源與電力，不環保且不具效率。因此例如使用共識決的權益證明區塊鏈、半官方的私有區塊鏈、分層實現的快速區塊鏈、各種類似區塊鏈技術的分散計算機系統等，許多革新的解決方式應運而生。如果區塊鏈的核心價值是全球分佈式的雲計算，那最後勝出具有速度和經濟效率的版本或許會跟目前區塊鏈的樣貌非常不同。

二、區塊鏈經濟與下一波工業革命

供應鏈是區塊鏈應用的主要領域之一，通過創建數據庫和記錄物品流動以改善協作，不同利害關係人可以在同個平台上自動化檢驗標的、協作、進行身份驗證，解決了協作上最困難的信任問題並減少詐欺的可能性。通過區塊鏈技術記錄諸如從食物、藥品、電子商品到汽車、飛機等物件所有從產地、原物料、生產加工到零售的各種運輸及轉賣數據，人們可以更全面地了解整個商業供應

鏈。區塊鏈的帳目與其相應的被寫入時間，使得人們可以準確記錄各方在資產生命週期內完成了什麼，讓所有利益相關者都能取得並信任這些數據，包括最終用戶在內的每個人都可以知道，誰在何時在哪個地理位置上擁有哪個資產，許多耗時且成本高昂的查核可以自動化，個體間的信任度上升，整個供應鏈因此變得更加透明與具有效率。

透過自動化信任和建立市場，區塊鏈技術將提供全球經濟前所未有的可能性，搭配普及的通訊與物聯網，世界各地的人和組織，包括被傳統金融體系排除於外的群體、可自動判斷執行交易的程式，無論認識與否，將直接連接到相同的平台建立協議。在不依賴集權的平台或其他中介機構下，進行交易和價值交換。在一個支付可以像點對點一樣簡單地發送電子郵件的世界中，信任和交易是自動處理的，轉移資金就像更新區塊鏈中的兩條紀錄一樣簡單。區塊鏈同時納入全球經濟的會計系統，更多交易標的被納入區塊鏈網絡中，在分佈式對等的計算機間進行交換，從而大幅擴大市場的可能性和範圍。

標記化是將資產轉換爲記錄在區塊鏈上的標記單元的過程，在區塊鏈經濟中，無論是有實體的自然資源資本，或是沒有實體的社會資本，任何具有經濟價值的資源都可以被標記化轉變成代幣，這些代幣可以是信用代幣、食品代幣、運輸代幣、社交代幣、能源代幣、投票代幣等，代幣經濟也讓不同價值體系間的資源更快速被轉換，活絡各種前所未見的價值交換。價值交換也不需要事先得到許可，這些點對點的活動沒有國境限制，以極度分散的方式協調更多的人類活動。

另外通過預售代幣的群眾募資引導社群發展的首次代幣銷售，也成爲代幣經濟下區塊鏈企業募資的重要工具。在首次代幣銷售中，一定數量的加密貨幣以代幣的型式分配給投資者，換取法定貨幣或其他加密貨幣。當區塊鏈企業的項目眞正啓動時，這些代幣將成爲該區塊鏈使用的貨幣，而投資者可以以早期較便宜成本取得。但由於代幣的功能和種類繁雜，某些區塊鏈代幣功能類似證券且涉及群眾募資，其中更充滿詐騙風險，首次代幣銷售在各國一直有法規適

用性的管轄權和監理議題。

隨著平台經濟的興起，區塊鏈正在改變我們在整個組織和社會中生產、消費、募資、協作的方式。代幣經濟學改變工業時代企業的結構，因爲它具有以全新方式整合利益相關者的潛力。區塊鏈網絡和代幣經濟是分佈式的，它們沒有集中的組織，因此我們不能用傳統的自上而下的方法發展經濟，而是必須與市場動態相結合。又因爲沒有集中協調，組織內成員依靠市場來預測未來，例如期貨市場價格反映商品資訊，並決定如何分配資源與應對變化。另外，隨著物聯網的普遍和資訊技術的進步，數以億兆計的設備互聯通訊，參與價值交換的主體也可以是自動執行的程式，結合數據科學與系統工程等知識，設備與設備間以動態協調分配資源滿足最終用戶的需求。

三、從政治與社會的角度看區塊鏈

區塊鏈的驗證技術對於公民而言，對個人身份資訊上有更好的掌握，在政治上的直接結果便是促進選民的政治參與。傳統投票遭遇的許多困難，可以用區塊鏈的科技改善：分散化儲存資料使系統結果不容易被網路攻擊竄改、選民利用生物識別工具的身份驗證更多元準確、電子投票縮短等待時間、投票的隱私性得到保證，以及透明和可檢驗的規則減少被操弄的可能，選民對投票機制的信任提升、參與程度提高，提升民主化程度。區塊鏈使資訊更容易被追蹤掌握，同時讓政府的其他部分受益，不僅僅是選舉，一旦將其納入其他政府機構和職能部門，政府與公眾之間的互動將更加直接和安全。

由於區塊鏈的帳目可以公開透明並被驗證，所有交易和資金流動將更容易被追溯與難以竄改，增加被審核的能力，減少貪污的可能。如同區塊鏈企業可以要求確認客戶身份，選民也可以反過來要求各政黨，更清楚揭露其海內外資產及往來資金流向、選舉和非選舉期間各項經費所得與支出，以及背後所支持的財團資訊，無法被竄改的公共紀錄使政治中的暗盤交易更行困難，選民和民意代表有更多監督政府和政黨的能力。

通過去中心化的網絡，代幣經濟可以用來推動社會組織的管理和發展。在區塊鏈經濟中，不需依賴集權組織來定義社會內部的價值。因爲記錄價值的這些數據庫的維護，已經轉移到市場經濟的資訊網絡，任何人或團體可以自行定義他們訴求的理念，爲了相同願景而努力。除了組織本身願景等傳統號召公民行動的力量外，自動化驗證大幅加強網絡協作的能力，在區塊鏈上獲取加密貨幣也能夠給予組織正向回饋。雖然點對點或局部群體的合作長久以來一直存在，但區塊鏈的技術將解除組織許多例如地區性與信任的約束，群體以分散和自願的方式結合與共同行動，強化這種以理念結合的社會群體的行爲與治理能力。若個體對群體信仰的價值做出正向貢獻，例如照顧流浪動物、關懷社區獨居老人、清理公共區域等，經由認定後可以得到代幣的經濟報酬，任何個人或團體將有更大的動機，讓自己的作爲與組織理念趨於一致，這是一個重新賦予個體和組織權力的過程。這種行動不需要預先得到國家或地方政府的許可，在法律的框架內，只要社會組織對於作爲與認證有清楚定義，從行動到激勵機制一切可以自動被裁決、記錄與執行。不必依賴國家的武力或權威，挑戰政府的權力疆界，區塊鏈的信息與技術配合更開放自由的市場機制，將實現個人與社會組織更完整的自主性。

另外，傳統的社交網絡透過上癮機制獲得個人資訊投放廣告的商業模型也將受到挑戰。人們將因爲共同信念在去中心化的社交網絡交流，區塊鏈可以提供更安全的溝通環境及隱私通訊，沒有企業在平台上擷取個人資訊，參與者共同決定獎勵機制與遊戲規則。個人有自己在平台上的聲譽，正向貢獻的創作內容甚至轉發宣傳將獲得獎勵，利用信用評分機制，聲譽或貢獻高的個體將有更多影響力，社群網絡的規則也會不斷藉由個體的決策演化以適應環境變遷與未來挑戰。

參、綜合評論

本書寫於加密貨幣市場急速膨脹的 2017、2018 年間，各產業區塊鏈的最新應用不斷出現，究竟這些市場挑戰者是破壞性創新還是曇花一現，甚至是一場詐騙炒作，其中存在太多需要被時間檢驗的因素。本書精彩描繪加密貨幣在十年間的演變、區塊鏈的潛力以及許多區塊鏈企業的成功案例，或至少是理念訴求。從知名加密貨幣從何而來、它們想解決哪些問題、有哪些技術規格上的紛爭，或遭遇哪些市場和法令挑戰等，這本書提供很清晰的論述。或許因爲篇幅限制、讀者選擇取向或區塊鏈發展本身仍然有高度不確定性等因素，本書沒有著重討論許多區塊鏈具體的技術細節、詳細探討區塊鏈企業會如何失敗的各種潛在風險，以及各國政府如何監管這種沒有疆界的技術創新，是其可惜之處。然而若想了解加密貨幣與區塊鏈的整體脈絡與可能未來，這本書是非常好的入門書籍。除了從技術、商業層面檢視其發展外，作者將區塊鏈的擴張視爲公民爲了挑戰國家與大企業階層化的控制，做出對身份的保護、自由意志的展現與個人主義的延伸，作者切入區塊鏈的視角多元與充滿理想性，是本書的另一特色。最後，或許區塊鏈技術仍在快速變遷與逐漸導入市場，目前尚未有從政治學、社會學等角度出發的區塊鏈專業學術書籍，多數暢銷書仍從商業或技術出發，著重觀察、猜測或技術講解，鮮少區塊鏈應用於政治或社會學的理論得以建立。除了資訊技術外，區塊鏈的研究需要整合不同領域，例如在全球最大的計算機網絡中個體與系統如何互動反饋、加密貨幣價格與集團的運算能力如何影響彼此競爭或合作關係、如何設計考量不同公平性的投票區塊鏈、區塊鏈規則如何隨市場變化調整、個體和企業又該如何以最佳策略因應，可以預見區塊鏈與社會科學領域的結合將應用複雜系統與賽局理論等學科知識，期待未來有更多區塊鏈相關社會科學理論得以被建構與辯證。