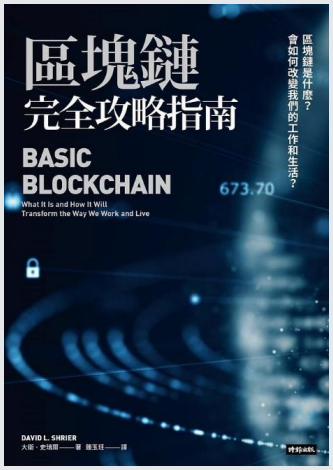
《區塊鏈：完全攻略指南》導讀

鍾玉玨 / 台大外文系兼任講師



區塊鏈、比特幣、加密、NFT（非同質化代幣）等革命性創新一波接一波轟炸業界、投資人、消費者，這場革命已擴及全球五大洲，就連幾個大家想像不到的地方，如愛沙尼亞、波多黎各等，都躍居區塊鏈應用的先驅。愈來愈多人擔心跟不上新科技提供的產品與服務，金融業者擔心新平台會威脅他們既有的地位，政府擔心這個嶄新技術會威脅其權力結構；其中不乏嘲諷詆毀，稱區塊鏈是精心設計的騙局。面對種種不安與潛在的衝擊，未來學家與金融創新權威大衛．史瑞爾（David Shrier）出版《區塊鏈：完全攻略指南》(台灣譯作出版日期2021/11/13，時報出版)，希望能夠普及有關區塊鏈的實用技術，並更上一層樓，利用這技術設法解決各種問題、創造各種機會。亞馬遜書評一針見血指出，本書是科技門外漢想了解區塊鏈的唯一入門書：簡介什麼是區塊鏈、區塊鏈的基本原理、以及這門新興科技的應用會如何翻轉企業、社會、乃至個人的日常生活。史瑞爾化繁為簡點出，區塊鏈（Blockchain）的核心概念是去中心化（decentralization），而去中心化的好處是提升數據（交易）的韌性（resilience）。他將本書分為三部分，首先解釋區塊鏈的技術面，接著介紹哪些產業適合使用區塊鏈，最後介紹區塊鏈對社會與社群的影響。

什麼是區塊鏈？

區塊鏈的本質是去中心化的數據庫。區塊鏈的誕生是因應2008年金融風暴，美國為首的全球央行大規模印鈔救市，導致部分科技圈人士質疑貨幣到底該不該由中央（政府）掌控，也不再信任傳統的金融系統，於是神秘、反傳統的天才中本聰（這可能是化名）開發出完全透過點對點（P2P）的交易方式，以及不需仰賴第三方中介的「零信任」網路貨幣—比特幣。去中心化、點對點交易、加密技術正是區塊鏈的核心價值。

區塊鏈的關鍵要素

1. 分散式記帳，彼此零信任的陌生人都有一模一樣的帳本，每個用戶都是一個中心，一起參與記帳和確認交易，進而擺脫中心化的監管體系和銀行金融系統。
2. 靠加密數位貨幣維持交易安全。比特幣是區塊鏈平台上第一個殺手級應用。
3. 兩兩交易形成的區塊，靠礦工挖礦，把每個新形成的區塊加到區塊鏈的末尾，成功將區塊串上區塊鏈的礦工可獲得比特幣等加密貨幣作為獎酬；如果區塊鏈網絡上有很多礦工，那麼礦工拼的是電腦運算速度。

4. 區塊鏈形成後，更動任何一個區塊的數據必須獲得區塊鏈上所有人同意，所謂牽一髮而動全身，因此區塊鏈可做到「不容竄改」。
5. 區塊鏈的安全性除了靠「不容竄改」，也靠加密；加密需要字符串組成的「密鑰」，把區塊上鎖（加密）與解鎖（解密），上鎖的鑰匙叫公鑰，解鎖的鑰匙叫私鑰，加密與解密的過程叫做橢圓曲線加密（或非對稱性加密）。
6. 比特幣區塊鏈因為有一些發展限制，因此出現分叉（fork），形成以太坊區塊鏈、瑞波幣區塊鏈等變體。

哪些產業適合使用區塊鏈

什麼產業需要區塊鏈？作者篩選出六個標準：作業可自動化、可重複的流程（如每月基金的扣款日）、牽涉多個利害關係人（如需要第三方把關）、需要數據核對、牽涉價值移轉（包括金錢、資訊、病歷等資訊移轉），以及紀錄不可竄改（如食品安全履歷、學歷、病歷等）。接著進入本書第二部舉出適合應用區塊鏈的產業，包括金融服務、保健醫療、能源與食品、不動產與自然資源、組織與治理等五大領域；首先從金融服務業說起，該產業完全符合前述適用區塊鏈技術的六個標準。

區塊鏈金融服務vs.傳統金融服務

區塊鏈可能衝擊金融服務業的制度與基建設施，也會直接影響消費者。誠如作者所指，過去十年，網際網路改寫了媒體業，接下來區塊鏈也將讓金融業天翻地覆，預估未來5年，金融服務業的中階與後台工作可能劇減數百萬個。

傳統金融服務的信任服務模式建立在法規、稽核、金融監理等，這就可能造成權力插手干預交易的弊端；區塊鏈金融模式則建立在電腦運算（包括人工智慧、智慧合約、分散式應用程式等）。此外，區塊鏈的共識機制可保證交易紀錄不可竄改，有效解決詐欺、違約等風險。再者，傳統金融模式是中心化，許多交易必須依賴獨立的第三方驗證與擔保；反觀區塊鏈是去中心化，結合大數據與電腦演算法，處理放貸、核貸、結算、清算等業務，無須人員手動媒合，所以建立在區塊鏈之上的金融服務，所需的人力與成本都會大幅降低。

區塊鏈的消費金融面應用

1. 貨幣：當某些國家的法定貨幣出現百分之百或更高的通膨時（如辛巴威），消費者一定會尋找現有法幣以外的工具，以便保住自己的資產價值。這等於將貨幣的控制權從政府手中搶走，不受政府的審查監控，因此多少讓比特幣等加密貨幣成了投資人感興趣的備案資產。不過比特幣等加密貨幣在市場波動頗大，並非支付薪資、租金、採購的好辦法，所以出現央行數位貨幣（CBDC）等變體。
2. 支付與匯款：消費者現在可以使用區塊鏈網絡，直接互相轉帳，即所謂的「點對點」支付，無須銀行等機構提供中介服務，因此也省去不少的匯款手續費。
3. 存款與貸款：存款與借貸可被紀錄在分散式帳本，核貸作業與後續可由分散式應用程式（DApp）與智慧合約執行。好處是，不僅大幅降低借款人的借貸成本，也大幅提高放款人的獲利。由於存放款是銀行利潤的主要來源之一，因此大型金融機構是該有理由擔心區塊鏈造成的破壞性創新。

4. 購房：購屋牽涉到屋主、中介、銀行、代書、政府等，讓人焦頭爛額，可靠著區塊鏈技術、智慧合約代勞。
5. 保險：同樣邏輯也適用於保險業。假設出色的智慧合約可以處理90%的保險業務，諸如核保、理賠、結算等等，將可大幅降低處理的人事成本。

區塊鏈的金融中介機構面應用（institutional applications）

區塊鏈可以大幅改善證券交易的速度、成本、合規性，所以適合金融機構採用；作者列出區塊鏈可代勞作業項目如下。

1. 結算與清算：這是非常吃力的紀錄密集型工程，還牽涉多個利益關係人，透過分散式帳本與數位代幣可以大幅簡化作業。Juniper Research估計，區塊鏈有助於每年減少220億英鎊的結算成本。
2. 衍生性商品買賣：大型商品（如原油）需實物交貨才能結算（交割），交易金額大、中間環節多、運輸產業鏈長，若能透過區塊鏈共識機制、加密算法、智慧合約，搭配FRID辨識系統、GPS衛星導航，有助大型商品交易變得更簡單、安全、透明。
3. 價值移轉（包括資金跨境移轉）：區塊鏈極可能改善機構之間的價值移轉。例如消費者向海外匯款時，匯出銀行、海外的收款銀行、中介銀行等必須相互合作，牽涉的中間環節過多，導致跨境資金被困在（或塞在）某個環節、手續費高、到帳速度慢等問題；若由區塊鏈代勞，銀行和銀行之間可以直接打造點對點的支付方式，可秒到帳、交易訊息即時共享、交易過程實時追蹤，銀行實時銷帳等優勢。供應鏈在跨境支付領域的商用價值非常值得重視。

區塊鏈的金融基建面應用（infrastructure applications）

以證券交易為例，傳統買賣需要經過交易所、銀行、客戶等多方，但是區塊鏈的分散式帳本技術可提升協作效率、降低成本、保證交易安全等，非常適合金融市場基建設施的應用。

1. 交易前的合規：包括認識你的客戶（KYC）、身分辨識、反洗錢、訊息披露等。根據BIS Research調查，光KYC這點，透過區塊鏈每年至少可省下40億英鎊，約新台幣1488億。
2. 可進行交易的平台：一些交易所已開始將整個交易放在區塊鏈平台，但納斯達克等大型交易市場可能還需要一些時間。
3. 交易後的登記、存款、結算、交割、數據共享、股東投票、配息等管理，也可靠區塊鏈系統代勞；這也是何以美國證券集中保管結算公司（DTCC）恐在一夕之間被淘汰。

央行數位貨幣（CBDC）與加密貨幣之別

央行數位貨幣是中央銀行把發行的貨幣數位化，跟大家目前手中持有的法定貨幣有相同的效力與價值，但區塊鏈加密貨幣則不被政府金融單位認可。此外，CBDC每一筆交易都能被監管 ，跟去中心化的加密貨幣價格由市場買賣決定，有本質上的不同。再者，加密貨幣

並非簡單的複製通貨，而是能創造投資價值，但價值也會大起大落，穩定性不足；央行數位貨幣則有政府信用做擔保，價值穩定。在主要國家中，中國進度算快，已開始試驗數位人民幣，數位人民幣屬於批發型數位貨幣（用於銀行之間清算），但這種CBDC若利用區塊鏈的分散式記帳技術保護交易與隱私的安全，成本過高。

區塊鏈對社會與社群的影響

區塊鏈與醫療保健

本書也強力推薦保健醫療善用區塊鏈技術，因為病患的個資、就診醫療紀錄與管理都極機密且亟需保護。由於區塊鏈提供不容竄改的紀錄，包括誰看了病患的病歷、獲得誰授權，這點可提高病患對系統的信任、改善數據移轉的安全性、杜絕醫療保險詐欺行為等；區塊鏈除了改善關乎病患的數據安全，也可能徹底改變對病患的醫療與照護方式，從交易型模式（transaction-based model）轉變為連續性照護服務模式（continuous-care engagement model）。

醫療保健的區塊鏈應用除了可有效改善病患個人數據的安全性與醫療服務，亦能擴及至公共衛生與醫學研究。作者點出，臨床試驗費用昂貴，部份原因是招募患者不易，若公衛與醫學研究能夠存取大量患者醫療數據，透過區塊鏈技術自動取得抓截病患願意參與研究的同意書，並自動提供這些病患數位代幣作為獎酬，可望加速臨床試驗時程與降低藥物的開發成本。

區塊鏈與溯源追蹤

區塊鏈的不容竄改猶如量身打造般與溯源追蹤（provenance）極為契合。講求溯源的食安、能源供應鏈、物流、電網管理、奢侈品珠寶等領域，均可善用區塊鏈改善配送、促進有效供需、提高透明度。作者點出，在溯源這塊，看見資本主義與共產主義奇異地結合，因為生產更牢固地掌握在個別小農手中，利用區塊鏈進行整合，進而發揮集體談判能力。

區塊鏈與政府治理

資訊時代百姓失去對政府的信任，區塊鏈結合生物識別技術，可大幅改善投票的安全性與可信度，提高選舉的公信力，回歸直接民主。政府另一個核心角色是課稅，過程中信任與透明度很重要，應用區塊鏈技術，再結合AI與數據分析，省去大量人力成本費與稽核時間，改善逃稅與洗錢陋習。

區塊鏈的未來前景

區塊鏈可結合物聯網、擴增實境（AR）、3D列印等技術，開發更多的可能性。一百年前，我們只能模糊想像世界若有了電動車、行動通訊、基因工程之後會是什麼模樣；而今這些天馬行空的想法已真實存在我們的實體世界。分散式機制可以利用集體的智慧集體解決問題或是預測未來，我們可能愈來愈接近夏爾丹（Peirre Teilhard de Chardin）想像的烏托邦世界，大家集體將人類文化推升到更高階的意識，以便所有人都受益。至於這些會如何改善人類的生活，我們才開始懵懂地掌握一些狀況，但是，未來是被創造出來的。