PREFACE

序言

黃序

時下許多熱門潮語，如：元宇宙、加密貨幣、智能合約、NFT、Web3 等前瞻性數位商品應用或經濟生態圈，幾乎多源自於對區塊鏈技術之運用，讓人很想一窺其中奧妙究竟。其實，自學者中本聰(Satoshi Nakamoto)於 2008 年提出 Bitcoin: A Peer-to-Peer Electronic Cash System 論文，便觸發了熱潮，全球如火如荼般地投資加密貨幣，惟支持幣圈背後所蘊藏的區塊鏈技術遂如彗星般地橫空問世，開始為世人所重視與深究。尤其像是「去中心化、匿名性及不可竄改性」等特色更為世人所標榜與尊崇，特別是大大地鼓舞了那些不喜受審查、或厭惡受壟斷基礎網路協議的人們，開始大膽萌生追求強調個資保障、數位自由的烏托邦理想國度之期待，紛紛冀望透過區塊鏈之核心技術應用，實現讓數位世界資產得以彰顯其價值，並透過加密貨幣扮演數位世界的支付要角，創造並真正實現完全去中心化管理的 Web3 經濟，這或許是個理想，但人們卻因此夢想，而對未來有了更美好的期待與努力之憧憬。

本書的兩位作者——李昇暾特聘教授、詹智安諮詢委員，是本人服務於國立成功大學 FinTech 商創研究中心的重要核心顧問，他們憑藉其各自多年累積的學術研究能量及整合產業寶貴的實務經驗，以深入淺出方式介紹這個同時匯集加密演算法、資料結構、點對點網路、共識機制等多項關鍵特色的區塊鏈技術，讓讀者們輕鬆入門了解區塊鏈如何在不同協定共識下，百家爭鳴般地發展出適合各產業應用之多元商業模式或投資商品。尤其，難能可貴的是本書以簡單明瞭之架構設計，從區塊鏈技術的發展沿革、各主流共識協議下的框架開發，甚至是區塊鏈技術應用與理論間可能存在之期待落差，被以詳實易懂方式娓娓地道理釋義，本書無論被作為自修研讀或教科書，相信對莘莘學子於學習區塊鏈應用之路必有所啟

發與助益，同時各領域新手定亦能快速上手熟闇區塊鏈的箇中奧妙，以實現本書科普知識的立著深意期許。

逢此知識科普的新書出版良緣時機，本人再次感激多年以來，亦師亦友的李昇暾特聘教授對於本校 FinTech 商創研究中心之竭力支持與辛勞貢獻，成就本中心研究能量與學企合作持續厚實成長，始得深受我國金融業與實務各界的肯定與信任。本人很榮幸此次獲得兩位作者之邀，為本書撰序，於此聊贅數語，以表至誠推薦之意。最後，本人再次祝福本書作者與有機會拜讀本書的諸位慧眼獨具讀者福慧並進，喜樂幸福常隨、平安健康永伴。

國立成功大學管理學院院長暨
FinTech 商創研究中心主任

李自序

時移重析區塊鏈 境遷新探 NFT
中心去化無何有 來日喜迎 Web3

自本書前版「區塊鏈智能合約與 DApp 實務應用」付梓後至今，回顧短短三年當中，隨著時光推移，緣起緣滅，有的策略技術曾炝到掠不著，讓人們緊追其後，有的卻已經擦落去，消逝在時間的洪流之中，而十餘年前揭櫫「去中心化」並體現「無何有之鄉」願景的區塊鏈仍屹立不搖！在經歷了多次的跌宕起伏，眾所關注的不外乎是濫觴於區塊鏈之比特幣與加密貨幣等息息相關的投資議題，是以「幣圈一天，人間十年」最能彰顯加密貨幣市場的不確定性。

當年拜智能合約之賜興起的 ICO 同質化代幣成為眾人除了 IPO 之外的另一種投資管道，卻因為良莠不齊的專案偏離初衷，最後甚至發生惡意吸金的情事，使得 ICO 不再受到投資人的青睞與信任。而之後出現的證券型代幣 STO 也沒有在市場上掀起太大的波瀾。接著在 2021 年出現的非同質化代幣浪潮，亦即眾所周知的 NFT（non fungible token），將加密貨幣應用推出另一波高潮，創造許多新的商業模式。NFT 雖然承襲了區塊鏈不可竄改的特性，但是不可竄改並不代表可被信任，NFT 遇到如產銷履歷、產品溯源等情況時，仍必須仰賴受信任的中介者。NFT 之於區塊鏈的最後一哩路，時至今日人們依然沒有找出圓滿的解決之道。

技術與話題永遠都不斷在推陳出新，在臉書掀起元宇宙熱度後，更有些人主張可以藉由 NFT 逐漸建構元宇宙與區塊鏈的共生關係，最終實現「人們可以在虛擬世界主張數位資產的所有權」之願景。雖然這樣的應用是否實際符合去中心化的理念仍有諸多爭議，但乘著 NFT 與元宇宙的浪潮，有人重提 2014 年由以太坊共同創辦人 Gavin Wood 定義的 Web3，並將元宇宙與 Web3 劃上等號。於是具有去中心化、對抗威權與審查、強調對於個資有絕對掌控權等核心價值的 Web3 吸引了人們的目光，眾人將實現 Web3 的理想寄託在可體現「無何有之鄉」的區塊鏈技術之上。

區塊鏈對企業的影響，並不如同以往像大數據或人工智慧等破壞式創新技術，可以一個低成本的解決方案，突如其來地轉變傳統的商業模式。反之，它是一種類似改變全球商業與生活型態的網際網路 TCP/IP 資訊基礎技術，須經過數十年的醞釀期來排除技術、治理、組織等障礙，才有機會滲透到產業的各個層面穩健地發展。而結合區塊鏈與 Web3 的去中心化生態圈在本質上是一種維新思潮(亦即為莊子〈逍遙遊〉所言的「無何有之鄉」)，然當前行之有年的各項制度與社會結構則是圍繞在中心化的法則設計，因而去中心化的思維吸引了許多對現實中心化體制不滿與絕望的年輕世代；他們將目光投射到虛擬世界那片未開發之地，欣然擁抱這些帶來希望與機會的相關技術。也正因為如此，在現實與虛擬之間，儼然形成世代之爭；追隨區塊鏈、NFT 與 Web3 等技術更像是反對體制、反抗威權以及世代隔閡的社會運動，而廣被年輕世代接受與歡迎。

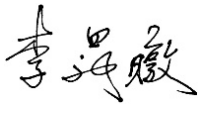
這一波又一波的浪潮，不斷衝擊多年來生活在中心化世界的我們，區塊鏈要能成功，思考模式須徹底地改變，倘若無法從根本心念調整，那麼區塊鏈技術發展到最後徒為枉然。我們曾在哈佛商業評論〈數轉乾坤——企業數位轉型之策略規劃與心法〉策略專文指出：「單純的新技術學習或可另由其他外部資源快速引入，但心法的內化仍需無縫對接，方能發揮整體戰力。」意即企業試圖藉由引進新技術來驅動成員對組織的想像，但應優先執行、卻時常被忽略的是專注於改變組織成員的心態，以及改革組織的文化與流程。其談論的是數位轉型於企業中的應用之道，而核心的精神理念與筆者於協助企業推動數轉時奉為圭臬的心訣：「轉行轉型轉心念，心念不轉空轉型。」有異曲同工之妙。吾人無法單從實驗室的經濟模型得到結果，也無法控制環境所有的變數，唯有分析成性，藉由不斷的觀察與歸納體解局勢，累積知識並進而轉識成智，點滴成涓，才有可能勾勒出最接近真實世界的願景藍圖。

學海無涯，資通訊技術學無止境，可預見未來幾年一定會有更多技術問世。《韓非子．說林上》：「聖人見微以知萌，見端以知末。」鑒古可知今，見微可知著，期勉讀者們能透過本書尋得區塊鏈的發展脈絡，與時俱進，甚至是預見演變的腳蹤，加添自己的技術競爭力。「法不孤起，仗境方生；道不虛行，遇緣則

應。」瞭解各樣資訊技術所生之緣，當進一步了解它與我們生活的相應之道，未來會如何變化，且讓我們都能隨遇而安，帶著平和愉快的心情邁步前進。

單絲不成線、獨木不成林，這本專業書籍的誕生歸功我身邊的一群專才戮力齊心，以及日常萬事運命牽引、涓滴成流的書寫題材。首先感謝本書另一位作者詹智安先生多年來的合作與傾心盡力的付出，書內許多素材皆源自於他過去在金控公司「區塊鏈實驗室」所累積的寶貴實務經驗；接著特別要感謝成大管理學院院長黃宇翔特聘教授為序，筆者有幸經由其主持之教育部深耕計畫「Fintech 商創中心」機會，習得關於區塊鏈與商轉等理論及實務知識。另要感謝成大工設所吳宛蓁同學專業的封面設計，讓本書增添不少光彩，而本系專案助理陸佩君小姐與碁峰資訊公司出版團隊提供了許多編輯協助，對提升本書品質亦是厥功甚偉；最後，感謝內人素娟於逐字校正潤稿與精神上的鼓勵委實貢獻。

資訊技術日新月異，筆者才疏學淺，本書雖經多次校訂增修，疏漏謬誤仍難避免，尚祈讀者先進不吝指正並海涵。



成大工資管系暨資管所 AI 實驗室

中華民國 112 年元月

詹自序

Bitcoin 的成功，讓人們開始關注核心的區塊鏈。雖然區塊鏈號稱是下一個可以改變世界的資訊技術，但其實不論是雜湊演算法、橢圓曲線數位簽章演算法(ECDSA)、Merkle Tree、P2P 網路等，所有區塊鏈使用到的技術幾乎都不是新的發明；即使濫觴於 Ethereum 區塊鏈平台上的智能合約也非全新的概念，它是參考了早在 1994 年就由身兼計算機科學家、法律學家及密碼學家的 Nick Szabo 首次提出的數位合約(digital contract)。因此，區塊鏈可說是一輛組裝巧妙的「拼裝車」罷了！

2017 年 12 月，世界各大加密貨幣首次站上歷史高點後，隨即便因為各國政府對監管強度的要求提高，以及流走著聯準會即將升息的風聲，使得資本紛紛離開高風險市場，致使加密貨幣陷入長期熊市，價格一路崩跌，投資人哀鴻遍野，泡沫化的傳言不脛而走。但加密貨幣往往猶如九命怪貓一樣，皆能起死回生。2021 年 11 月 10 日時 bitcoin 曾創下 1 顆約 68,925 美元的歷史高位。也許誠如美國諾貝爾經濟學獎得主克魯曼（Paul Krugman）的觀點，他認為加密貨幣儼然成為一種信仰，因此無論面對何樣的風風雨雨，加密貨幣未來將無限期存活下去。

到底應不應該投入對區塊鏈的學習與研究？這其實是一個有趣卻又難以簡明回答的問題。尤其區塊鏈的三大核心特色每每被不同的質疑論點聲討：「『去中心化』去得了嗎？」、「POW 不是讓權力更加集中在少數的礦工手上？」、「POS 是不是只要掌控 66%質押權，其他人就難以生成新區塊？」、「比特幣其實只有 1 萬多個節點，這就足以視為去中心化？」、「以太坊只有 8,000 多個節點，也能稱為去中心化？」、「『不可竄改』對於企業的聯盟鏈來說，不是可以透過實體的合約約束來實現嗎？況且 GDPR 的遺忘權讓人們有權利能要求資料控管者刪除其個人資料，但是資料一旦上鏈就會被永久寫到區塊鏈之中，這兩者不是相互牴觸嗎？」、「『不可否認』不代表就可以相信！區塊鏈本身不可竄改所以很安全，但如果寫入區塊鏈的資料一開始就已經是錯的呢？」、「區塊鏈的最後一哩路要如何達成？」

當您問了一個問題之後，似乎就會衍生更多的問題。對於資訊從業人員來說，技術的熱忱與追求是不可以偏廢的。就好比多年前的 .COM 雖然泡沫化了，但時勢造英雄，當今全球前幾名的大型企業幾乎都是網路科技公司！我們只能將自己準備好！如此而已。

另方面，Java 程式語言已是目前大型企業廣泛採用的科技標準，然而綜觀當今書籍市場尚沒有人嘗試將區塊鏈與之結合。筆者有幸曾服務於國內某金控公司的「區塊鏈實驗室」，本書即基於個人對兩大技術之整合的實務心得與經驗來撰寫，希望藉由本書拋磚引玉，吸引更多人投入對區塊鏈的研究；也期許 IT 工程師能多花一些心思在商業模式與企業管理的修為。個人深深感受資訊技術與軟實力是國家產業轉型的軸心，在一個天然資源匱乏的地方，更應該強化新型態商業模式的設計與創新研究動能，拋棄過去數十年的硬體思維，才能夠帶領這塊土地早日走出產業轉型的道路。

本書能夠順利出版，首先要感謝恩師——李昇暾教授多年來持續不斷的鼓勵與指導；同時也要感謝內人洪幸琪小姐，以及我的一對雙胞胎——子嫻與子逸，能夠體諒犧牲陪伴他們的時光，全心投入本書的撰寫。

2023 年 1 月

詹智安于台北市

CHAPTER

07

NFT 與 Web3 實務應用

自比特幣於 2008 年濫觴至今，各界藉由其核心的區塊鏈技術如火如荼推動、創造更多的商業應用，可惜這些專案多屬概念驗證（Proof of Concept, POC）性質，往往缺乏實用價值，也不易商轉。近年來，NFT 的興起被視為區塊鏈應用的明日之星，但是事實真是如此嗎？本章將探討 NFT、元宇宙與 Web3 之間的關係，以及未來可能的發展趨勢，並且帶領各位讀者建置第一個 NFT 智能合約。

本章架構如下：

- 漫談 NFT
- 概說元宇宙
- 縱觀 Web3
- NFT 停看聽
- 我的第一枚 NFT 非同質化代幣
- IPFS 星際檔案系統：NFT 安全守門員
- 搭著 IPFS 直上 Web3 的 NFT 代幣
- 結語

7-1 漫談 NFT

去中心化金融 DeFi

在談論 NFT 之前，先概略介紹何謂「去中心化金融（decentralized finance, DeFi）」。去中心化金融所追求的目標即是消除金融交易的中介者，使之具備所有權分散、交易內容不被否認，且具有透明與抗審查等特性的金融服務與系統。相對於傳統中心化的金融服務（CeFi），以信用卡消費為例，會先由買方的銀行付款給如 VISA 的支付公司，再由支付公司將款項交付給賣方的銀行，最後賣方再到自己的銀行戶頭提領帳款。整個過程除了需耗費時日之外，亦產生交易中介者層層的手續費成本，故 DeFi 被視為下一波金融科技的炸子雞。

然而在 2022 年 6 月 20 日的中央銀行季度報告中，強調投資人應注意 DeFi 的六大風險，包括：資訊不對稱與詐欺風險、市場誠信風險、非法活動風險、營運與技術風險、治理風險、風險外溢到傳統金融市場。DeFi 通常會透過網紅、社群媒體及線上推廣活動等管道宣傳，投資人沒有對等的資訊可以了解相關的風險。實作 DeFi 的區塊鏈與智能合約雖然是公開的，但需要具備一定的技術能力與知識，且 DeFi 能快速、匿名提領資金，可能使得受害者遭遇損失後無從追索。此外，Defi 亦有網路壅塞與手續費攀升問題。因此，投資人在從事相關的投資活動時，仍必須小心謹慎才是。

DeFi 的目標可藉由區塊鏈、加密貨幣以及智能合約等技術加以實現。參考前幾章所介紹的，智能合約是一種運行在區塊鏈的電腦程式，在區塊鏈生態系統中扮演公正且被信任角色。如同現實生活中的契約一樣，可依照事先擬定的規則（程式邏輯）依約自動執行。本書介紹的以太坊（Ethereum）便是最具代表性的區塊鏈技術，可以完整體現智能合約的運作。而 NFT 就是 DeFi 的一種應用，據 CryptoSlam 平台的統計資料顯示，迄今為止，NFT 總銷售額已經超過 360 億美元。這些 NFT 來自 18 個區塊鏈，包括以太坊、Ronin、Solana、Avalanche、Wax、Polygon 和 Flow，其中，以太坊之占比高達 75%以上。

透過以太坊發行的 NFT 數量雖然很多，且支援的錢包也多，但以太坊在交易時往往需要付出高額的 gas，也因為交易速度相對較慢，較適合發行高單價、具有稀缺性的 NFT。其它後起之秀，如：Polygon，便具有交易手續費低、速度快等特性，相對較適合發行一般性、數量較多的 NFT。不過此議題並不在本書探討的範圍內，就留給有興趣的讀者自行研究。

同質化貨幣

在探討 NFT 之前，讓我們先複習幾個和以太坊有關的名詞與技術。「位址」一詞在以太坊中，可以指外部帳戶（externally owned account, EOA）或合約帳戶（contract account）。EOA 是一組公開字串，對映終端用戶的私鑰，可以想像是終端用戶在區塊鏈世界的「銀行帳號」。合約帳戶則是指智能合約的位址，意指智能合約也可以擁有區塊鏈的「銀行帳號」。使得終端用戶與智能合約皆可以擁有以太幣餘額（ether balance），都可以進行以太幣的轉出與轉入，或是觸發與執行其它智能合約。

首次代幣發行（initial coin offering, ICO）是一個廣為人知的智能合約應用，其精神乃源於證券市場的首次公開募股（initial public offering, IPO），兩者的差異為 IPO 是向公眾籌集資金，發行之標的物是證券；ICO 則是向公眾募集加密貨幣，進而發行另一種新代幣（token）。具體而言，ICO 是一種遵循以太坊開發者協議 ERC 20 標準所撰寫的智能合約，在區塊鏈原生的加密貨幣之上，另外創建一種新型態的代幣。

舉例來說，終端用戶將 1 個以太幣轉帳給某個 ERC 20 智能合約，而該合約程式的處理邏輯，會在合約上記錄該用戶兌換了 20 個此 ICO 新代幣。由於合約程式僅記錄終端用戶所持有該代幣的數量，而每一個代幣的價值皆相同，故遵循 ERC 20 所發行的代幣也被稱為同質化代幣（fungible token）。代幣在終端用戶之間的轉入與轉出交易行為，實質上僅是合約程式記錄其所持有代幣數量的增減。（註：可以參考本書第四章完整之介紹。）

ICO 推行之初，眾人將其視為如 IPO 的另一種投資管道而趨之若鶩，但好的構想卻因為良莠不齊的 ICO 專案而偏離初衷，甚至導致惡意吸金的情事發生，使得 ICO 不再受到投資人的青睞與信任。

相對於同質化代幣，當今流行的則是非同質化代幣，即是眾所談論的 NFT（non fungible token）。NFT 是一種遵循 ERC 721 所撰寫的智能合約。在 ERC 721 合約中，可以使每個 NFT 代幣對映到不同的數位資產，且須使用不同金額的加密貨幣購買，造就了每個代幣能夠呈現出獨一無二的價值。ERC 721 於 2017 年 9 月 20 日發表，主要標準的制定與貢獻者是 Dieter Shirley，他是新創公司 Axiom Zen 的遊戲開發技術總監，此公司於同年 11 月 28 日公開推出營運一款知名休閒遊戲——謎戀貓（CryptoKitties），即是基於以太幣交易的遊戲，遊戲中的每隻貓咪為一個 ERC 721 代幣。玩家可以購買虛擬貓咪，也可出售與馴養後代等。

NFT 非同質化貨幣

2021 年，NFT 將加密貨幣應用推向另一波高潮，創造出許多新的商業模式。在國外，佳士得拍賣會在該年 3 月 12 日採用 NFT 拍賣一幅名為「Everydays: The First 5000 Days」的數位照片，最後以近 7,000 萬美元的天價落槌。無獨有偶，在國內也掀起一波 NFT 熱潮，舉凡像是阿妹演唱會、周杰倫旗下潮牌 PHANTACi、霹靂國際布袋戲角色、明華園歌仔戲演出等，甚至國際名廚江振誠也推出可以吃的 NFT。在千變萬化的市場中，人們似乎害怕與任何商機失之交臂，不趕緊發想個 NFT 的應用就落伍了。但究竟 NFT 的真正價值何在？這些食衣住行育樂的商品看似與 NFT 結合，但是在本質、價值上符合 NFT 的真義嗎？

首先，我們須確定 NFT 的商品（如：圖片）是否可如實存放上在區塊鏈上？就技術面來說，若欲將 1 MB 大小的圖片儲存在以太坊的智能合約上，需得透過 215 個 unit256 型態的變數。以 2022 年 4 月的幣價計算，此舉約需花費 304 萬台幣的 gas (手續費)，當然不可行！在經過繁複的資料轉換與運算後，區塊鏈上到底儲存了什麼奇珍異寶？讀者若是透過 Etherscan 等工具追本溯源，將會發現 ERC 721 合約所儲存的 NFT 代幣，其實不過是代幣編號、終端用戶位址（用戶在區塊鏈世界的「銀行帳號」），以及數位商品在網際網路上資源名稱（Uniform Resource

Identifier, URI）之間的對映關係而已。換言之，NFT 行銷上宣傳所稱讓每一項數位收藏品擁有獨一無二的數位身分證，也可以讓擁有者證明其所有權，其實不然，那不過是代幣編號、終端用戶位址與 URI 的結合，充其量只是個資料對照表。

另方面，前述的代幣 URI 顯示的是數位商品真正儲存地，但令人驚訝的是，追蹤該代幣 URI 的超連結往往會發現，人們花了大額鈔票所購買的某些 NFT 商品，只不過是網頁伺服器上的某張圖片，且是毫無保障地被存放在一般的網頁伺服器。倘若該網頁伺服器發生故障或無法存取，那麼所購買的 NFT 商品不就石沉大海了嗎？

再者，智能合約所儲存的前述對映關係雖無法被竄改，然若網頁伺服器管理員直接置換 URI 所對映的數位商品，則原購買的高價數位藝術品不就可輕易被竄改成贗品了？由此可見，NFT 雖承襲了區塊鏈不可竄改的特性，但並不代表 NFT 就可被信任。

NFT 與 IPFS 相輔相成

為解決前述 NFT 相關問題，於是有研究嘗試將 NFT 商品存放到星際檔案系統（InterPlanetary File System, IPFS）。IPFS 是一種分散式檔案儲存、共享與可持久化的網路傳輸協定，可與區塊鏈協同運作。IPFS 參考了 BitTorrent、Git 以及區塊鏈的雜湊樹（merkle tree）等技術實作而成，以解決傳統網頁架構的缺點（如中心集權管理與重覆資料儲存等）。IPFS 根據檔案內容計算雜湊值，並依此做為檔案唯一的識別位址。相同雜湊值的檔案只會被儲存一份，若檔案被複製、修改或重新上傳，便會得到不同於修改前的雜湊值。因此，若能將代幣編號、終端用戶位址，以及 IPFS 識別位址之間的對映關係寫到智能合約上，應可同時驗證數位資產擁有權、確保檔案完整性，亦能儲存大檔案內容，補足區塊鏈不適合儲存檔案的缺點。

前陣子火紅一時的無聊猿 NFT，便是將圖片儲存在 IPFS 的成功案例。雖然圖片上的一個像素（pixel）遭到修改便會得到不同的雜湊值，但以人類肉眼來說，是看不出任何差異的。因此，即使區塊鏈搭配 IPFS，依然無法確認是否買到贗品。

區塊鏈的驗證機制僅是「確認資料有上傳」與「不可否認資料有上傳」，但並不代表上傳的內容是正確且可被信任。如何證明數位資產的真偽？如何驗證數位資產是正版？如何防止數位資產被複製？這些都是 NFT 目前做不到的事。關於 IPFS 將在本章第五節有更詳細的介紹。

NFT 確實帶來很多想像空間，而不是只能做為個人頭像（Profile Picture, PFP）的應用，更勝者可以將藝術品予以資產證券化，讓多人可以共同且合法地擁有 NFT。更進一步，可以讓 NFT 成為「真實資產」在虛擬世界的「產權代表」，例如擁有某 ERC 721 代幣的人，代表其在真實世界擁有某棟房子的產權。或者是 NFT 最重要的功能與特性，可以透過智能合約公平且公正的運作，讓原始的藝術創作者得以合理分潤，而不再受到中間層層剝削。然而，到目前為止，NFT 的實用性還是令人存疑，即便在「賦能 NFT」出現後亦是如此。「賦能 NFT」是指除了收藏功能之外，還可和產品、服務，或是特殊權益進行連結的 NFT，例如：持有 NFT 可以兌換炸雞或是特殊的餐點、享有停車優惠、線下兌換商品、換取遊戲寶物等。可是在前一位 NFT 持有者享用完服務之後，NFT 是否還有價值可以繼續在二級市場上流通？若無搭配長期的會員經營策略，那麼「賦能 NFT」同樣也只是一張漂亮的圖檔而已，充其量只有短暫的行銷效果，淪為炒作一途。

此外在連結實體世界與數位環境的介面上，NFT 遇到與產銷履歷、產品溯源等情況，仍是十分仰賴受信任的中介者。回到問題的根源，萬一在資料寫入時，已發生錯誤或已被竄改呢？NFT 雖然承襲區塊鏈通透與不可被竄改等特性，但同樣地，區塊鏈尚未走完的最後一哩路，NFT 也難以達成。對於如何監理 NFT，目前國際間尚無共識，實作方式也尚在討論、凝聚共識中。我國財政單位認為：「NFT 屬於商品，商品交易該課徵營業稅。」而高等法院之民事判決：「比特幣為權利所依附之客體，其性質應屬『物』，且屬代替物。」刑事法院則多認為：「虛擬貨幣非有形財物，僅屬無形之財產上利益。但是加密貨幣並非合法通貨，同樣從『商品』的角度將之稱為『虛擬通貨』。」因此，以加密貨幣「購買」NFT 的行為，充其量僅是以物易物，陷入無法可管的窘境。

另外，談到 NFT 就不能不討論智慧財產權（Intellectual Property Rights, IPR）。智慧財產權意指：「人類用腦力所創造的智慧產物，具有財產上的價值，並由法律賦予排除他人侵害的權利。」智慧財產權包含著作權、商標、專利和營業祕密，以下是對各項權利簡單的比較說明：

權利	保護對象	申請方式	保護期間	成立要件	是否須公開	法律責任
專利權	可供利用之發明，含物、方法與視覺訴求設計	申請後，經過審查	自申請日期： • 發明：20 年 • 設計：15 年 • 新型：10 年	• 產業利用性 • 新穎性 • 進步性	申請後 18 個月之後，須公開	民事
商標	用於企業服務、產品等任何具有識別性之標識	申請後，經過審查	註冊公告當日起算 10 年，可申請展延，不限次數	識別性	註冊公告	民、刑事
著作權	各種內容創作，如：美術作品、印刷、出版、表演、拍攝或記錄、文學、藝術或音樂等	不需申請，創作完即受保護	• 人格權：永久保護 • 財產權：生存期間及死亡後 50 年	原創性	可公開發表	民、刑事
營業祕密	技術、方法、製程、配方、程序、設計或其它可用於生產、銷售或經營之資訊	不需申請	成立即受保護，沒有法定期限	• 非他人所知 • 具經濟價值 • 合理保護措施	不得公開	民、刑事

NFT 通常聚焦在著作權的討論。著作權簡單的說，就是授權他人製作複製品的權利，賦予創作者與該項作品有關的無形權利。為了有所依據，著作權的產生便不能只是存於腦海之中，必須要確立有形媒介，如：寫下來，錄下來等，以文稿、畫作、數位圖像、影片等實體作品呈現。購買 NFT 猶如購買藝術品，NFT 藝術家仍然保有著作權，買家購買 NFT 後可用於個人用途，並且將之展示，但並沒

有購買該 NFT 的著作權，故沒有散播或販售 NFT 的複製品的權利，也不可以製作該 NFT 的衍生作品。但是如同其它藝術品一樣，買家有權出售 NFT 給其他人。除非有明確的書面協議，作者亦可將將著作權轉讓給買家。

NFT 交易曾在 2021 年蓬勃發展，然而到了 2022 年，全球最大 NFT 平台 OpenSea 宣布將裁員 20%。2022 年 1 月的以太坊區塊鏈 NFT 銷售額，曾達到 50 億美元高峰，但 2022 年 6 月已降到 7 億美元。加密貨幣交易所 Coinbase 也在 2022 年 6 月宣布裁員 1,000 人，占總員工數 18%。因此，若規劃投資 NFT 商品的讀者必須小心謹慎才是上策。

7-2 概說元宇宙

「元宇宙」一詞出自 1992 年的科幻小說《Snow Crash》，描寫人們戴上虛擬實境裝置（VR）在虛擬世界生活。許多影視作品也有類似的詮釋，例如《一級玩家》、《脫稿玩家》等。2021 年 10 月 29 日，社群媒體巨擘臉書宣布更名為 Meta，將虛擬實境納入元宇宙（Metaverse）的願景之中。然部分人士將元宇宙視為行銷炒作，誠如維爾福軟體（Valve Software）創辦人 Gabe Newell 所言：「談論元宇宙的人根本沒玩過大型多人線上角色扮演遊戲（MMORPG）。在線上捏一個虛擬化身（Avatar）是早在十幾年前就做得到的事，並非什麼新發明。」

元宇宙的表現形式大多從遊戲為起點，逐漸整合網際網路、數位娛樂、教育、醫療等。美國遊戲軟體公司 Beamable 的創辦人 Jon Radoff，依市場價值鏈將元宇宙分為七層架構，由下往上概述如下：

- 基礎設施層：5G/6G、新製程半導體等硬體有關部分。
- 人機互動層：物聯網穿戴設備，各式新式人機介紹面。
- 去中心化層：自我主權身分聲張，數位資產和貨幣價值交換。
- 空間計算層：混合現實/虛擬計算，記錄資產在虛擬世界的足跡位置。

- 創作者經濟層：創作者以更多工具進行創作。
- 探索層：如何推拉新體驗給使用者，如：虛擬商店及社群。
- 體驗層：不限 2D、3D，更多元的體驗方式。

其中第三層去中心化層，即為元宇宙和區塊鏈交集之處。服務或系統建置者可以藉由使用區塊鏈與 NFT，對元宇宙的數位資產進行擁有權的確認，也可以在元宇宙的虛擬世界中使用加密貨幣滿足支付的需要。姑且不論元宇宙是否只是噱頭，臉書掀起的這波革命確實帶來另外一個新的議題：「如何在虛擬世界主張數位資產的所有權？」有些人認為可以藉由 NFT 逐漸建構元宇宙與區塊鏈的共生關係，最終實現此一願景。

無聊猿 NFT 的母公司 Yuga Labs，預計出售旗下元宇宙遊戲 Otherside 的 5.5 萬筆虛擬土地，這些土地皆是以 NFT 呈現，預估最多可獲得價值 3 億美元的加密貨幣，可望成為迄今最大規模的 NFT 發行。然而需注意的是，虛擬世界的土地可能不具有稀缺性，不見得符合稀有財的定義。元宇宙雖然可能涉及區塊鏈技術，但是背後完全由企業掌控，可能全然違背去中心化的理念，並且因為其著重於沉浸式體驗，在未來的發展藍圖上，去中心化不必然會成為企業追求的核心價值。此外，當各個企業財團紛紛推出自己的元宇宙，將會形成碎片化的「多重元宇宙」。除非有機會一統由不同企業財團所掌控的「多重元宇宙」，否則元宇宙在現階段不過是個行銷名詞。投資這些新興科技時，應該加以了解其營運方式，避免落入龐式騙局，或是重演 1637 年鬱金香狂熱事件。

本書付梓之際，適逢臉書更名為 Meta 屆滿一週年，Mark Zuckerberg 於 2022 年 11 月初宣布裁員 13%，大約影響約 11,000 多位員工。同時，凍結招聘到 2023 年的第一季度。這也許是因為在新冠肺炎疫情期間，各大科技巨頭評估市場對於資訊科技具有高度需求，紛紛提高投資金額與大舉招聘員工——以 Meta 為例，其雇用人數增加 80%以上，達到約 8.7 萬名員工。但在後疫情時代，人們已走到戶外，資訊市場急轉直下，對於電子商務的需求可能不如之前預期的樂觀。因此，包括 Meta 在內的各大企業，不得不進行大幅度的裁員。

然而 Meta 旗下的虛擬世界 Horizon Worlds 作為元宇宙的入口，已創建約 10,000 個不同的虛擬空間，但卻只有大約 9%的虛擬空間有超過 50 名使用者拜訪過。雖然每月大約有 200,000 名活躍用戶，但多數在使用該平台一個月後就不再返回。甚至 Meta 的內部文件這麼寫道：「這個空蕩的世界令人悲傷。」Meta 在元宇宙的投資金額已超過百億美元，但股價卻在一年中下跌 60%以上。可見這一波響亮的行銷操作市場並不買單，元宇宙是否真的有遠景，就留給歷史去評斷。

7-3 縱觀 Web3

近來乘著 NFT 與元宇宙的浪潮，有人重提 Web 3.0，並將元宇宙與 Web 3.0 劃上等號，但是兩者之間其實並沒有直接關聯。事實上，Web 3.0 濫觴於 1999 年 WWW 的發明者 Tim Berners-Lee 教授提出的語意網（semantic Web）概念，當時是指讓電腦可以模擬人類大腦處理事情，概念類似今日人工智慧（AI）應用。但在不同時期有不同的定義，且包含多層涵義，主要是用來區分網際網路發展過程的方向和特徵。2006 年左右，Web 3.0 可能代表更大量的資料訪問、更高速的網路頻寬與硬體規格。而在 2010 年左右，Web 3.0 似乎又和移動設備、搜索與人工智慧牽涉在一起。現今廣被接受的定義，則是在 2014 年由以太坊共同創辦人 Gavin Wood 所提出的：「其目標為建立一種不受審查、壟斷的基礎網路協議，用以保護使用者的個資。」綜合上述，可以將每一代的「Web」區分如下：

- Web 1.0：人人都是資訊的接收者。由 WWW 開創的新時代，網站架設存在高技術門檻。資訊傳播是單向式，人們只能查詢與閱讀他人分享的資料。
- Web 2.0：人人都是資訊的提供者。隨著社群平台的興起，人們不再需要具備專業的技術背景，便能夠透過平台和他人分享資訊與互動。然而，個資與隱私完全被平台業者掌控，使用者生成內容（User-generated content, UGC）甚至還必須受到平台業者管控。此外，有些企業會蒐集用戶行為販售盈利，但終端使用者並沒分得實質好處，卻還可能因違反平台政策，被凍結與移除帳號，甚至是停權。

- Web 3.0：人人都是資訊的擁有者。藉由去中心化的網路應用，沒有誰可以恣意封鎖與剝奪數位資產。核心的價值包括：去中心化、對抗威權與審查、強調對於個資有絕對掌控權等。這些你我是否覺得似曾相識？是的，這些概念廣納前述所談的種種區塊鏈相關願景，因此區塊鏈普遍被認為是實現 Web3 主要的技術之一。

順便一提，對於這樣一個新興的領域，究竟該稱之為 Web 3.0 還是 Web3？其實都是可以的！若從承襲 Web 1.0、Web 2.0 的命名習慣，那麼就會順理成章的將之稱為 Web 3.0，同時有可能會和歷年的定義衝突。於是加密貨幣圈內崇尚自由與抵禦體制的人士不希望遵循規則，期望打破傳統，因此傾向將之稱為 Web3。本書尊重各種角度與想法，因此本書所提，不論 Web 3.0 或是 Web3 暫指相同的東西。

其實，目前對 Web 3.0 的定義仍然莫衷一是，總括來說，應具有下列元素：

- 使用區塊鏈技術，並讓終端用戶可以完全掌控自己的資料。終端用戶亦可決定資料的分享對象，如：購物紀錄是用戶分享給平台，而不是由平台持有。
- 可基於擁有權的分潤，例如用戶分享創作內容之後，可獲得加密貨幣獎勵。同時，在交易過程不會有角色傾斜的情況，所稱角色如：產品創作人、使用者、投資人等，每個人的地位都是平等的。

在 Web3 區塊鏈世界中，人們皆持有自己的「加密貨幣錢包」，以做為登入各種服務的鑰匙，無需再提交個資給科技巨頭。舉凡聊天內容、分享貼文與影片、販賣資訊、觀看廣告等，所有賺得的加密貨幣皆會自動存入錢包中，透過錢包即可直接進行去中心化的支付與交易。

欲以實作方式體現 Web3 所描繪的遠景，依然面臨眾多的技術考驗。例如：Web3 強調對個資有更多的權力，猶如 GDPR 的遺忘權（Article 17），賦予人們有權要求資料控管者，刪除其個人資料的權利，但是區塊鏈強調追蹤性與不可竄改，資料一旦上鏈，就可能會被永久寫到區塊鏈之中。若嘗試以脫鏈方式儲存個資，問題又會回到原點，面臨被集中儲存或是被竄改的風險。

Web3 另一個顯而易見的問題是，全球如此龐雜的資料要儲存在什麼地方？是否有全球統一的管理方式？前面所提的 IPFS 可能會是個答案，但這項技術發展未臻成熟，尚須經過幾年的驗證。除此之外，根據 2022 年 6 月 ethernodes 觀測網站的資料指出，以太坊節點數目前大約僅 5,712 個，這個數量可代表全球去中心化的分散程度？此程度是否表示整體環境已夠去中心化了？況且，還有許多新興的區塊鏈出現，而這些區塊鏈的節點數明顯達不到去中心化的程度，同時，還只被少數的機構掌握，在這種情況下的 Web3 一點意義也沒有。

要想連接到 Web3 的世界，就必須使用適當的 Web3 瀏覽器。雖然基本上 Web3 瀏覽器和 Web 2.0 瀏覽器沒有太大不同，但 Web3 瀏覽器可以讓使用數據不被企業所用，也可以連接到 DApp。Web 2.0 瀏覽器透過擴充功能，如：安裝本書前幾章示範的 Metamask 錢包，便能悠遊 Web3 的世界。但純粹的 Web3 瀏覽器則不需要額外的安裝。

下方列舉幾個已經內建錢包和支援 Web3 域名的瀏覽器，提供使用者得以更便於體驗 Web3：

- Brave：無需另外下載擴充套件，即可保管加密資產、追蹤投資組合，並與 Web3 DApps 互動。預設封鎖追蹤器、廣告，提升載入速度，亦能保護用戶隱私。觀看 Brave 平台提供的廣告，可獲得 BAT 加密貨幣作為獎勵。
- Opera：以其高效瀏覽、隱私保護、內建的廣告阻擋等功能聞名，亦不需要安裝擴充功能便可以連接與使用 DApp。 2022 年發表的加密貨幣瀏覽器專案（Crypto Browser Project）強調以 Web3 作為發展核心。
- Osiris：使用 Metawallet 作為內建的加密錢包，主要鏈接第二層網路（layer 2），使之能夠更快的進行交易。

未來 Web3 並不會完全取代 Web 2.0，如同當前，最傳統的 Web 1.0 依然存在且運行中。Web3 跟公共鏈的目的皆為打造一台世界電腦，讓所有參與者提供運算環境，成為世界電腦的一環。

特斯拉時任執行長馬斯克（Elon Musk）曾於 2021 年 12 月 21 日於 Twitter（推特）表示：「有人見過 Web3 嗎？我找不到。」他並非完全不相信 Web3，而是認為依目前的技術與環境，談論 Web3 還嫌太早。有人說區塊鏈是一種技術，但筆者認為它更像是一種思維的轉變，也可以說是一種世代的社會運動，反抗威權與政府。綜上所述，DeFi（去中心化金融）、NFT（非同質化代幣）、DAO（去中心化組織）雖解決不同面向的問題，但都可能會是引領下一波 Web3 網路革命的關鍵技術，對技術從業人員來說，還是必須時時關心趨勢變化。

7-4 NFT 停看聽

根據 NFT 數據分析網站 NonFungible.com 資料顯示，在 2021 年 9 月時曾出現日均銷售量 22.5 萬枚 NFT 的盛況。加密數據網站 DappRadar 表示，NFT 在 2022 年第一季的銷售額有 125 億美元之多，但在 2022 年第三季則降到只有 34 億美元。而在 2022 年 10 月——本文撰寫之際，最大 NFT 市場 OpenSea 的銷售額亦連續五個月下滑，足見 NFT 熱潮冷卻的速度之快。這多多少少受到美國聯儲會為了對抗通膨而加息，導致投資人紛紛規避高風險的產品，加密貨幣市場因此遭受重創，比特幣從 2021 年 11 月達到巔峰以來，至今亦下跌約 70%之多。

吾人在投入 NFT 世界時，不妨藉由下列幾個問題來協助自己查驗方向的正確性：

1. NFT 平台是否使用區塊鏈技術？許多 NFT 平台標榜簡化流程，不強調需使用加密貨幣才能購買 NFT 商品，也不提供查詢智能合約位址的功能，如此是否可行？是否有過度行銷之虞？
2. NFT 平台是採公鏈或私有鏈架設而成？前者發行的加密貨幣較具有投資價值，而後者或有喪失去中心化的核心價值之憾。
3. NFT 資產的移轉是否僅能透過特定交易平台？若交由平台全權管控，亦不符合區塊鏈交易透明的核心價值。

4. 所使用的區塊鏈有多少節點？投入前宜透過公開的資訊平台查詢，節點數越少，代表越容易遭受攻擊，無法達成防止竄改交易之目標。
5. NFT 商品存放在什麼地方？如果是在 NFT 交易平台或一般網頁伺服器，仍屬中心化的架構，恐有單點故障（Single Point of Failure, SPOF）的風險，代表一旦主機失效，即可讓整體系統無法運作。
6. 如何驗證「數位資產」為正版？某些 NFT 平台提供自家的證明機制，但由中心化的平台來進行驗證，便難以保證其公正性。長期來看，也許可以透過類似數位憑證認證機構（Certificate Authority）的機制，公開創作者的公鑰與憑證來保障權益。
7. 具有「賦能」功能的 NFT 可以提高獲利效益，須確認 NFT 是否可以享受額外福利以及其交易次數是否設限？若對交易次數加以設限，恐增加日後難以轉賣的投資風險。
8. 購得 NFT 不等於擁有創作者的著作財產權，端視有無創作者著作權之授權。同時，也應確認是否購得「所有權」，否則僅是擁有「數位資產冠名權」，可以向人炫耀「這張圖是我的」，但不一定真正擁有它。

若未能釐清以上各點，大眾面對 NFT 世界的宛若盲人摸象。建立並掌握以上幾個準則，即便面對種類繁多的選擇，也必能在關鍵的時局做出精準的預判。

NFT 與加密貨幣在某種程度上屬於烏托邦式的信仰，不見得有機會實現。然而，其底層的區塊鏈技術，以及衍生出來 Web3 目標，雖仍存在著許多限制，卻有可能改變資訊技術的生態與全貌。企業欲以新創的資訊技術做為市場競爭的決勝錦囊，宜需停看聽，透徹了解 NFT 真義，也應時時關注世界政經的發展趨勢，分析成性便能見微知著、鑑往知來，在投身加密貨幣市場時，能辨明何種盛況只會是曇花一現，哪塊大餌的背後是行銷騙徒暗設的天羅地網，哪條不起眼的窄路是真正可以踏上的康莊大道。

7-8 結語

以太坊與區塊鏈技術未來會如何發展，我們可從相關的社會現象中觀察。當前現實世界的資源多為中高齡者所掌控，不論是土地、房屋等資源稀有值高，被既得利益者所造成的內捲化（Involution），讓整個社會只能重複勞作、發展遲緩，行之有年的各項制度與社會結構皆是圍繞在中心化的思維所設計。去中心化在本質上是一種思維方式，對現實體制的不滿與絕望，反而讓年輕世代的目光投射到虛擬世界，那片未開發之地似乎充滿著機會，相關的技術吸引人們的目光。擁抱區塊鏈、NFT 與 Web3 等技術更像是反對體制、反抗威權以及世代隔閡的社會運動，而廣被年輕世代接受與歡迎。這種情況猶如賽博龐克（Cyberpunk）小說所描繪的世界。賽博龐克是控制論（Cybernetics）與龐克（Punk）的結合詞。這類型的作品大多是以科技已經高度發展的世界為背景，描述著控制與反控制、反差極大的不完美社會。故事中，世界往往被中央集權的政府或大企業完全控制，而不願意服從，卻又有擁有高超技術或是高超能力的主角，則引領人們反抗體制。

多年前網際網路開始普及，其實就是一種虛擬化的開端，而資訊的原生世代比起年長者更能接受生活在網路世界。也正因為如此，在現實與虛擬之間，儼然形成世代之爭。虛擬世界之於殘酷的現實世界顯得相對完美，不會受到物理上的限制。Meta 公司的元宇宙即是基於可以在虛擬世界工作為出發點，這和過去 VR 產品以娛樂為主的觀點是全然不同的，年輕世代更容易接受在虛擬世界工作的趨勢。而在虛擬世界的工作報酬，可能就會以虛擬貨幣支付，並且可以在虛擬世界直接消費購物。NFT 未來的發展不僅只是購買頭像而已，而可能會慢慢發展成為虛擬世界的所有權認證機制，在虛擬世界的消費需要以加密貨幣支付，而所有權的歸屬則是要透過 NFT。在現實物質世界中，銀貨兩訖之後便完成交易，商品可以物理性的交付行為轉給買家，所有買賣交易的核心，其實就是所有權的移轉。但在虛擬世界中，卻很難證明買家對於虛擬商品的所有權。若無法證明虛擬商品的歸屬權，便無法彰顯其價值，那麼就不會有人購買，更遑論在虛擬世界進行交易。

區塊鏈一波又一波的浪潮，不斷的衝擊多年來活在中心化世界的我們。區塊鏈與 Web3 亦是一種思想運動，依靠哲學啟發人們，倘若無法從根源的思維方式徹底調整、改變，那麼區塊鏈技術發展到最後可能只是枉然。在 Web3 真正來臨之前，於是便有人提出折衷的 Web 2.5，即在保有 Web2 良好的使用者體驗，和以使用者為主，更加開放、去中心化的 Web3 之間取得平衡點。這可能才是對區塊鏈未來幾年更好的發展方向。

麥肯錫（McKinsey）在 2022 年 8 月底發布的「麥肯錫 2022 年科技趨勢展望報告」，依照創新度、關注度與投資力進行評分，挑選 14 種值得關注的科技趨勢，其中 Web3 是值得提早因應布局、掌握商機的趨勢。麥肯錫認為 Web3 是網際網路的未來模型，具有將權力下放給用戶的特性，使之能夠更好地控制個人數據變現（Monetization），增強對數位資產的所有權控制。2021 年度，綜合公開與私募市場的投資規模達 1,110 億美元之多，在 14 項科技趨勢中排名第 6。

但如同筆者一再的提醒，雖然 Web3 受到許多關注，但商業模式仍在探討與測試的階段，仍然面臨許多的挑戰。對於資訊從業人員來說，我們僅能持續地跟上腳步，持續培養自己的技術競爭力，隨著未來時局的變化因應行動。企業也應該要跟緊新技術的發展，找到創新的商業模式，擬訂更好的組織發展戰略。

7-9 習題

7.1 請仿照本章範例，創建你/妳的一個 NFT，並部署到 OpenSea 的測試環境。

7.2 本章所介紹的 IPFS 可能可以解決數位資產不一致的風險，除此之外，試想是否有更好的解決方法？

7.3 有人建議直接將 SVG 向量圖像以文字的方式，直接寫到智能合約之中，而不用額外搭配 IPFS，試問，這可能會有甚麼限制？