第一章

區塊鏈 1.0：貨幣

技術堆疊：區塊鏈、協議、貨幣

比特幣（Bitcoin）一詞可能常令人困惑，因為比特幣（Bitcoin）本身就有三種定義。首先，比特幣代表了底層的區塊鏈科技平台。其次，比特幣可以指涉一種基於底層區塊鏈科技運作的協議，這種協議的功能是用來描述在區塊鏈上如何轉移資產。第三，比特幣本身就指代了一種數位貨幣，即為比特幣（Bitcoin），是最早出現也是目前規模最大的加密貨幣。

表 1-1 解釋了如何區分不同定義的比特幣。第一層是底層技術，即區塊鏈。區塊鏈是去中心化的（decentralized）、公開透明的交易紀錄帳本—區塊鏈資料庫由所有網路節點共享、由礦工（miner）更新，由全民監督，但沒有人可以擁有或控制這個資料庫。它就像一張巨大的互動式試算表（spreadsheet），每個人都可以使用和更新，並且確認這些轉移資金的數位交易是唯一的。

位於技術堆疊中層的協議，是在區塊鏈帳本中進行轉移資金的軟體系統。技術堆疊的最上層就是比特幣（Bitcoin），在交易中會以 BTC 或 Btc 表示。目前已經有數百種加密貨幣，其中比特幣最早出現，而且規模最大。其他的加密貨幣包含萊特幣（Litecoin）、狗狗幣（Dogecoin）、瑞波幣（Ripple）、未來幣（NXT）和點點幣（Peercoin）等。主要的加密貨幣可以在 *http://coinmarketcap.com/* 查詢。

表 1-1　比特幣區塊鏈的技術推疊層級

加密貨幣	比特幣（BTC）、萊特幣（Litecoin）、狗狗幣（Dogecoin）
比特幣協定與用戶	管理交易的軟體程式
比特幣區塊鏈	底層的去中心化分散式帳本

對於所有現代加密貨幣來說，區塊鏈、協議與貨幣這三個層級即是一種通用結構。通常每種貨幣都同時代表一種貨幣與一種協議，它可能在自有的區塊鏈或是基於比特幣區塊鏈上運作。例如，萊特幣在萊特幣協議上運作，而萊特幣運作於屬於萊特幣的區塊鏈上（萊特幣可視為比特幣的改良版，改善了一部分特性）。一個獨立的區塊鏈意味著該貨幣擁有屬於自己的去中心化帳本（其結構與格式與比特幣的區塊鏈帳本相同）。

另外，有一些協議，比如合約幣（Counterparty），它擁有自己的貨幣（XCP），但是運作在基於比特幣的區塊鏈上，這表示它們的交易將會登記在比特幣區塊鏈帳本上。*http://bit.ly/crypto_2_0_comp* 網頁上的表格，詳細比較了 Crypto 2.0 計畫下各個加密貨幣的相異之處。

加密貨幣如何運作？

比特幣是錢、數位貨幣，是一種在網路上買賣物品的方式。比特幣的價值鏈由許多不同的支持者：軟體開發者、礦工、交易所、商戶服務商、電子錢包公司，以及用戶 / 消費者所組成。從個人用戶的角度來看，在硬幣交易中（為不失通用性，在此使用「硬幣」加以表述）的重要元素包括位址、私鑰與錢包軟體。位址是別人可以把比特幣送給你的地方，私鑰是一串經過加密的密碼，你可以將比特幣透過私鑰加密發送給別人。

錢包軟體則是可運作在電腦上的比特幣管理軟體（見圖 1-1）。從此，你不再需要在任何企業網站註冊一個中心化的帳戶；只要你擁有某個位址的私鑰，就可以利用這個私鑰在任何一台連接網路的電腦上（當然也包括智慧型手機）取得該位址的硬幣。錢包軟體還能保存一份區塊鏈的副本—在該幣種上發生的所有交易紀錄—作為去中心化機制的一環，得以驗證硬幣交易。附錄 A 會更加詳細地介紹如何維護電子貨幣錢包的實際例子。

圖 1-1　比特幣錢包 app 與轉移比特幣
（圖片來源：比特幣錢包開發者與 InterAksyon）

電子錢包服務與個資隱私安全

身為負責任的消費者，我們還不習慣有關區塊鏈科技和個人資料保密的新操作方式，就像我們還不會「備份」貨幣。在電子錢包中以私鑰形式保障安全的「去中心化自主性」意味著：你再也無法打給客服取回密碼或私鑰備份。如果私鑰遺失了，那你的比特幣也就沒了。這確實可能表示比特幣尚未成熟到足以被主流接受；這也正是消費者面向的新創公司 Circle Internet Financial 和 Xapo 試圖解決的問題。

針對電子錢包開發一些標準化 app 或服務將會有不錯的商機，比方說為遺失、防偷、當機、升級後的裝置提供備份服務，這樣用戶就能透過備份服務好好搞清楚私鑰出了什麼問題，釐清究竟是人為還是外部因素造成。個資隱私安全是消費者素養中極為重要的一環，因為要在新的數位貨幣領域中保障個人資產與交易安全無虞事關重大。許多專家建議使用「混合硬幣（coin mixing）」來保障個資安全，將你自己的硬幣與其他交易混合，可以使用 Dark Coin、Dark Wallet 或 BitMixer 等服務使交易更具匿名性[3]。隨著替代貨幣市場逐漸發展，對於統一電子錢包的需求也越發強烈，因為大多數區塊鏈相關服務會要求使用者安裝一個新的獨立錢包，所以你的智慧型手機上很有可能一下子就安裝了 20 幾個不同的電子錢包。

[3] Cipher (handle name). “The Current State of Coin-Mixing Services.” Depp.Dot.Web, May 25, 2014. *http://www.deepdotweb.com/2014/05/25/current-state-coin-mixing-services/.*

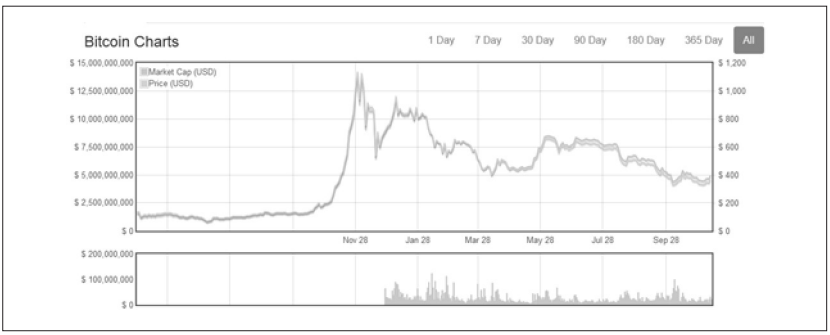

圖 1-2　自 2009 年至 2014 年 11 月的比特幣價格
（資料來源：*http://coinmarketcap.com/currencies/bitcoin/#charts*）

有些人認為價格變化與波動率是阻止加密貨幣普及的障礙之一，而一些主打減輕價格波動的企業已經開始試圖解決這問題。比如 Bitreserve（*https://bitreserve.org*）將比特幣存款鎖定在固定匯率上[11]。Realcoin（*http://realcoin.com*）的加密貨幣綁定美元匯率[12]。

Coinapult 的 LOCKS（*https://coinapult.com/locks/info*）可以讓使用者將比特率匯率與金價、銀價、美元、英鎊或歐元等綁定[13]。第一個與美元綁定的加密貨幣之一，有 Ripple 的 XRP/USD BitStamp（*https://www.ripplecharts.com/*），以及 BitShare 的 BitUSD（*http://wiki.bitshares.org/index.php/BitShares/Market_Peg*）。

11　Vigna, P. "CNET Founder Readies Bitreserve Launch in Bid to Quell Bitcoin Volatility." The Wall Street Journal, October 22, 2014. *http://blogs.wsj.com/moneybeat/2014/10/22/cnet-founder-readies-bitreserve-launch-in-bid-to-quell-bitcoin-volatility/.*

12　Casey, M.J. "Dollar-Backed Digital Currency Aims to Fix Bitcoin's Volatility Dilemma." The Wall Street Journal, July 8, 2014. *http://blogs.wsj.com/moneybeat/2014/07/08/dollar-backed-digital-currency-aims-to-x-bitcoins-volatility-dilemma/.*

13　Rizzo, P. "Coinapult Launches LOCKS, Aiming to Eliminate Bitcoin Price Volatility." CoinDesk, July 29, 2014. *http://www.coindesk.com/coinapult-launches-locks-tool-eliminate-bitcoin-price-volatility/.*

圖 2-1　Swancoin：限量發行的數位資產藝術作品
（圖片來源：*http://swancoin.tumblr.com/*）

智慧資產的核心思想是將各種資產在區塊鏈上註冊轉換為數位資產的所有權及存取權，並取得相應的私鑰。有些實體資產可以區塊鏈控制，如智慧型手機可以在確認使用者在區塊鏈上的數位身分後自動解鎖。還有現實世界的門禁系統，如車輛或住宅門鎖可以搭載嵌入式「智慧物體（smart matter）」，如軟體代碼、感測器、QR 碼、NFC 標籤、iBeacons、Wifi 等，就可以即時驗證用戶的軟硬體身份識別設備並與該資產配對。

當用戶暫時無法提供驗證設備時，可以傳送即時需求到區塊鏈上，這時智慧合約可以送出確認訊息或驗證機制到該實體資產或用戶的電子錢包中，如用戶可以用一次性 QR 碼來發動租來的車輛或進入飯店房間。區塊鏈技術可以改造現有的身份驗證與安全取用機制，以更靈活且優雅的方式整合硬體科技與網路數位導向的軟體科技，完善回應用戶的即時需求[20]。

[20] Swan, M. “Identity Authentication and Security Access 2.0.” Broader Perspective blog, April 7, 2013. *http://futurememes.blogspot.com/2013/04/identity-authentication-and-security.html.*

區塊鏈 2.0 協定專案

儘管「區塊鏈 2.0 協定專案」（參考表 2-2）的分類可能不夠適切，但我們可以將許多新一代的區塊鏈開發專案廣泛歸納在這個分類中。表 2-2 大致列出目前的知名專案。

表 2-2　區塊鏈 2.0 專案簡表
（資料來源：*Piotr Piaseki*，*http://bit.ly/crypto_2_0_comp*）

比特幣 2.0 專案名稱與網址	專案簡介	技術說明
Ripple *https://ripple.com/*	門戶、支付、交易、匯款網路；智慧合約系統：Codius	單獨的區塊鏈
Counterparty *https://www.counterparty.co/*	貨幣發行與交易的疊加協定	疊加於比特幣區塊鏈之上
（以太坊）Ethereum *http://ethereum.org/*	通用的圖靈完備數位貨幣平台	自開發的區塊鏈：以太坊虛擬機器
Mastercoin *http://www.mastercoin.org/*	衍生性金融商品	疊加於比特幣區塊鏈之上
NXT *http://www.nxtcommunity.org/*	使用股份證明共識機制挖礦的競爭幣	單獨的區塊鏈
Open Transactions *http://opentransactions.org/*	具有不可追蹤性、匿名性、不可延遲交易等特性	沒有區塊鏈；交易庫
BitShares *http://bitshares.org/*	去中心化數位股權交易所	單獨的區塊鏈
Open Assets *https://github.com/OpenAssets*	發行彩色幣與專屬電子錢包	疊加於比特幣區塊鏈之上
Colored Coins *http://coloredcoins.org/*	可交易數位或實體茲慘的比特幣資產市場	疊加於比特幣區塊鏈之上

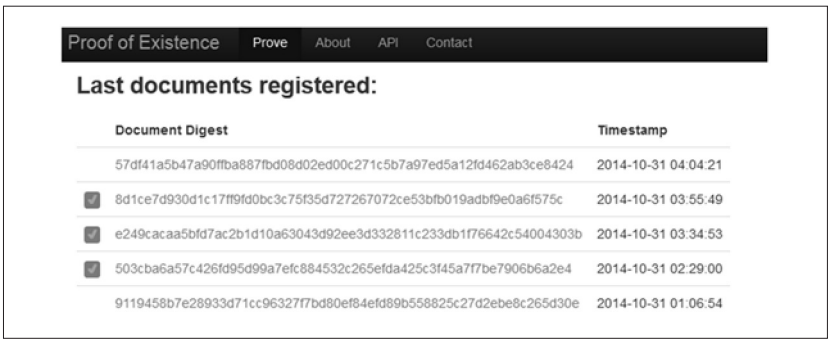

圖 3-1 「最新註冊文件」（截圖自 Proof of Existence）

這個檔案認證服務讓區塊鏈以突破性的方式證明某個文件或數位資產在某個特定時間的存有狀態與確切內容。不容更改的時間戳記與文件內容的機密性，應用到眾多法律及公民市政服務，真可謂無可挑剔。律師、客戶和政府官員可以利用 Proof of Existence 證明許多重要文件的存在，如遺囑、契約、授權書、醫囑、本票等不便透露內容的文件。

有了區塊鏈時間戳記功能，使用者可以在現有時點證明一份文件（如遺囑）的存在並將內容保密，未來到法院訴請確認時，就可以證明這份文件未經更動，內容維持一致。這類認證服務可以應用到任何文件或數位資產中，例如開發者可以利用該認證服務為每個版本的程式碼建立獨立的雜湊序列，發明家可以證明他們的創意點子於何時出現，而創作者們可以保障各自的作品。

鏈的護照系統撰寫程式碼[38]。這項計畫旨在以加密工具提供人人都負擔得起的去中心化護照申辦服務，達成「全球公民」的目標。

圖 3-3　World Citizen Project 的區塊鏈護照（圖片來源：Chris Ellis）

世界上任何人都有使用去中心化政府服務的權利。不管身處地球上哪一個板塊，所有人都可以享受由多家政府服務商提供的任何服務，而不囿於地區差異。過去眾多服務皆由政府壟斷，但在網路連結全球脈動的當今世界中，出現了區塊鏈政府服務的概念，政府壟斷不再是唯一作法。

像是比特幣一樣的全球通用貨幣及全球政府服務的出現，引發人們思考國家的本質將如何轉變，以及未來國家將扮演何種角色。國家從此形同家鄉，更像是人們的出生地，而不再是一個精確的地理區域。人們的所有日常活動，涵蓋了貨幣交易、

[38] McMillan, R. “Hacker Dreams Up Crypto Passport Using the Tech Behind Bitcoin.” Wired, October 30, 2014. *http://www.wired.com/2014/10/world_passport/*; Ellis, C. “World Citizenship Project Features in Wired Magazine.” Blog post, November 1, 2014. *http://chrisellis.me/world-citizenship-project-features-in-wired-magazine/.*

區塊鏈是一種資訊科技

區塊鏈是一種資訊科技，這或許是最廣為人知的概念，但是區塊鏈科技還有許多其他應用。去中心化的區塊鏈是具有革命意義的新運算模式。區塊鏈是網路歷史上從未有過的嵌入式經濟層，它是一種協調機制、項目歸屬、信用、證明以及補償獎勵的追蹤模式，在任何協作中透過智慧代理來鼓勵去信任（trusless）的參與。

區塊鏈是「一個去中心化的信任網路。[1]」區塊鏈就是海耶克提出的貨幣多元化概念下的私有替代貨幣，數量繁多如 Twitter 或部落格帳號，而所有貨幣可在各自的社群（hyper-local）情境下完全流通，提升各社群的凝聚力。

區塊鏈是雲端版的跨國組織聚集地。區塊鏈可以是提供個人去中心化的治理服務、贊助識讀能力並促進經濟發展的手段。區塊鏈也可以用來證明及紀錄特定時間點下的任何文件或數位資產的具體內容。區塊鏈整合了人機交互作用、機器對機器（M2M）以及物聯網（IoT）支付網路，用來建構機器經濟（machine economy）。

區塊鏈與加密貨幣推動了 M2M 溝通的支付機制與會計制度。區塊鏈是可以登記、確認、轉移所有資產與社會互動的全球去中心化公開分類帳、也是社會的公共紀錄銀行，又或者是，以前

[1] Antonopoulos, A.M. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. Sebastopol, CA: O'Reilly Media, 2014.

類多元的機器、人類和混合智慧未來的過渡期。未來這些智慧不可能單獨運作，而是與整個溝通網路連結。為了完成各自目標，數位智慧必須能夠在網路上進行特定交易，其中許多交易都可以藉由區塊鏈及其他共識機制完成。

只有友善 AI 的交易才能被執行

共識模型有一個意想不到的優勢，那就是這些模型可能促使產生「友善的 AI」，也就是在區塊鏈社會中有合作能力的道德玩家。[3] 在去中心化的信任網路中，代理人的名望（代理人處於匿名狀態）將會是決定其交易是否能被執行的重要因素。所以惡名昭彰的玩家則無法進行交易。任何關於資源訪問與使用的交易需求將必須透過共識模型並取得同意。

之所以共識模型能夠促進友善 AI 產生，是因為不好的代理人（bad agents）若想參與交易，必須在聲望與行為上也表現得像友善的代理人一樣。從結果來看，因為這兩類代理人皆表現良好，兩者變得難以區分。舉例來說，就好比反社會份子儘管存在於現實社會中，但他們被迫遵守社會結構與運作機制，因此從表面上來看就如正常人一樣。當然，也是有許多人對區塊鏈架構可以促進友善 AI 這一想法抱持反對意見：不好的代理人可以自行架構用於資料請求的智慧網路，或者在取得信任後翻臉不認人等等。不過，這些反對意見並沒有改變關鍵事實：當試圖限制某些行為時，區塊鏈科技可以是一種激勵和產生特定行為的制衡系統。這個點子旨在創造奧卡姆剃刀（Occam's

[3] Swan, M. "Blockchain-Enforced Friendly AI." Crypto Money Expo, December 5, 2014. *http://cryptomoneyexpo.com/expos/inv2/#schedule* and *http://youtu.be/qdGoRep5iT0/.*

razor）情境，只要表現良好就可以得到好處，所以最簡單有效的獲益方式就是「參加」，系統自會給予良好玩家相應獎勵。

任何數位智慧可能都要進行一些如安全訪問、身份驗證與認證、經濟交易等關鍵操作。所有智慧代理人關注的就是在執行目標交易時所需要的任何訪問及認證形式，而這些形式是以共識為基礎而簽訂，除非這些代理人擁有可立足於網路的良好聲望，否則無法獲得權限。這就是友善 AI 如何在區塊鏈共識模型下產生作用的方式。

代表數位智慧的智慧合約

區塊鏈科技和共識模型不僅可用於發展友善 AI，也可以運用至其他方面。舉個例子來說，想像你是一個人工智慧或是數位思維文件，智慧合約在未來可能會充當你的代表人，確認你的存在及運行環境的細節。關於數位智慧，有一個存在已久的問題：假如你是人工智慧，你要如何確認自身的現實環境呢？—你是否確實存在著、你是否被適當備份、你確實在運行著、還有目前狀態是處於什麼條件下呢？就好比要如何確認數據你的數據中心不會將你推送到舊的 DOS 運算系統上、或將你刪除，甚至是停止運作呢？

區塊鏈科技的智慧合約正是未來時間框架下的通用第三方代表，可以用來驗證並實踐對物理參數—你作為人工智慧之存在事實—的控制。至於這要怎麼運作：你需要在區塊鏈上訂定智慧合約，以便定期確認你的運行參數及去中心化備份副本。智慧合約可以建立「未來代表人（future advocacy）」，是一種有許