本書簡介

歡迎來到《第一次挖礦就上手》。我們將在這裡協助你進入加密貨幣挖礦的美妙世界。當然你可能覺得自己並不需要我們的協助，只要去 Google 或其他搜尋引擎用關鍵字搜尋一下，就可以發現很多有用的教學資訊，照著直接開挖即可！

哈！各位請試試看吧。其實這就像是直接從消防水管裡喝水一樣，你會瞬間淹沒在大量令人困惑的部落格文章、相互矛盾的加密貨幣新聞、難以理解的維基百科內容，以及充滿誤導的 YouTube 影片中……

這就是本書問世的目的。我們的職責是把挖礦的相關知識，分解成可以理解、易於消化的、一般人就可以閱讀並了解的小知識片段。

關於本書

這本書可以為你解釋、簡化並揭開加密貨幣挖礦世界的神秘面紗，因為你必須先了解自己需要知道什麼和做什麼，才能決定是否以及如何開始加密貨幣的挖礦事業。

我們將在本書中為你詳細解釋：

- 加密貨幣挖礦的工作原理以及用途（當初加密貨幣的發明，不可能只是用來賺錢吧？）
- 不同演算法及運作方式，包括工作量證明、權益證明、委託權益證明等，以及到底何謂「雜湊」（hashing[註 1]）的全部內容
- 不同類型的礦場：礦池挖礦、個人挖礦、雲挖礦等

註 1　hash 譯為「雜湊」（亦有譯為散列），例如「雜湊函數」（hash-function），但一般談論挖礦硬體算力值時，也常使用音譯的「哈希」值，兩者所指相同，特此說明。

- 不同類型的硬體：CPU 挖礦、GPU 挖礦（顯卡挖礦）、FGPA 挖礦和 ASIC 挖礦
- 如何選擇合適的加密貨幣進行挖礦
- 如何尋找與使用礦池挖礦服務
- 如何設置挖礦硬體和軟體
- 如何計算潛在收益（或損失！），考慮挖礦網路的雜湊率（全網算力）、礦機雜湊率（礦機算力）、貨幣匯率、電價等
- 哪裡還有更多有用資源，可以協助導引你的加密貨幣挖礦之旅
- 以及更多相關內容！

愚蠢假設

我們不想預設任何立場，不過我們必須假設如果你正在閱讀本書，應該就已經對網際網路和加密貨幣有初步了解。我們假設你已經了解如何進行線上工作，也知道如何使用個人電腦設備。我們還假設你應該了解如何買賣加密貨幣（要去交易所之類），也知道必須使用加密錢包，並且知道必須維護加密貨幣的安全性。

加密貨幣挖礦本身就是一個極為複雜的主題，需要用到一整本書的篇幅來加以解釋。因此，你最好先了解這些基礎知識。本書當然會偏重於更高階的主題，亦即加密貨幣的挖礦，因此這些純粹關於加密貨幣的基礎知識，並非本書的主要內容。我們建議各位觀看彼得製作的 8 小時線上影片課程「*Crypto Clear*：*Blockchain & Cryptocurrency Made Simple*」（加密貨幣釋義：讓區塊鏈和加密貨幣變得簡單），各位可以在 CryptoOfCourse.com 網站找到該課程。無論如何，你必須學習如何安全地使用加密貨幣，以保護自己的加密貨幣免受盜竊和遺失的風險。

本書使用的圖示

跟所有《*For Dummies*》系列書籍一樣，本書也會使用幾種「圖示」來突顯某些段落，提醒各位注意特別有用的訊息。以下就是這些圖示含義的簡要說明：

Tip（訣竅）圖示代表為你提供「額外的訊息」，這些訊息可以協助你對正在討論的概念有更多的見解。

Remember（牢記）圖示代表這是值得牢記的訊息。

Technical Stuff（技術內容）圖示代表這是可以跳過的技術內容，但如果你是喜歡背景知識的人，當然也可以深入了解。

Warning（警告）圖示可以協助各位遠離麻煩。它的目的在讓你提高警覺，避開那些對你的網站或業務可能有害的陷阱。

在本書之外

除了你現在正在閱讀的內容外，本書還附帶了可以免費造訪的備忘資源清單，裡面涵蓋了各種有用的資訊，例如常用加密貨幣的背景訊息、貨幣可分割性、最受歡迎的礦池挖礦服務等。若要取得此備忘清單，只需造訪 www.dummies.com 網站，並在搜尋框中輸入「**Cryptocurrency Mining For Dummies Cheat Sheet**」（**加密貨幣投資的小白速查清單**）即可。

關於彼得的「*Crypto Clear*：*Blockchain & Cryptocurrency Made Simple*」（**加密貨幣釋義：讓區塊鏈和加密貨幣變得簡單**）8 小時影片課程，請造訪 www.CryptoOfCourse.com。

如何閱讀本書

跟所有優秀的參考工具一樣，本書的目的也著重於可以在「需要」時閱讀。本書分為幾個單元：加密貨幣背景和基礎；挖礦相關基礎訊息；如何開始加密貨幣挖礦；挖礦經濟學；和「十」的單元（挖礦的十項、十大……相關要點）。我們建議你可以從頭開始閱讀，並按順序通讀整本書。如果你只想知道如何找到提供挖礦服務的礦池，請直接閱讀第 7 章。如果你想了解如何估算開採特定加密貨幣所需的設備成本，請閱讀第 11 章。如果你只想了解不同的挖礦形式，第 4 章正適合你。

加密貨幣確實是相當複雜的主題，加密貨幣的挖礦更是複雜。本書涵蓋的所有主題都是相互關聯的，所以我們強烈建議你在開始挖礦之前，詳細閱讀本書的所有內容；因為在開始挖礦之前，你必須對涉及到的所有相關內容，都有更深刻的了解。畢竟遇到任何損失時，賠掉的都是你自己的錢！

本章內容

- » 探索數位貨幣
- » 使用區塊鏈
- » 雜湊區塊
- » 了解公鑰加密
- » 使用私鑰簽署訊息

Chapter 1
加密貨幣釋義

你可能迫切希望立刻開始進行挖礦作業，但在挖掘加密貨幣之前，我們希望你能確實了解加密貨幣的實際含義。

加密貨幣感覺仍然如此新奇，人們對加密貨幣的興趣，多半是近幾年才開始出現。雖然各種形式的加密貨幣，大致自 1980 年代以來就已陸續出現，但大多數參與其中的人，對於加密貨幣到底是什麼以及到底如何產生的理解並不確實。所以一般的加密貨幣擁有者，甚至可能不知道他們擁有的到底是什麼東西？

因此在本章中，我們將回顧加密貨幣的歷史，以及加密貨幣的不同組成成分之間如何協同運作。一旦徹底了解到底什麼是加密貨幣，便可為加密貨幣的挖礦建立更穩固的基礎。

數位貨幣簡史

加密貨幣算是一種特殊類型的數位貨幣，但仍屬於數位貨幣的一種。

那到底什麼是「數位貨幣」（*digital currency*）呢？數位貨幣是一個範圍相當廣泛的術語，涵蓋了各種不同定義的事物。但在一般意義上，它就是以「數位形式」而非以「有形形式」存在的貨幣（例如硬幣和紙幣即為有形的形式）。而且我們可以透過某種「電子網路」，例如網際網路或私人銀行網路之類，來轉移這些數位貨幣。


TIP

其實連信用卡交易都可以視為數位貨幣的交易。因為當你在商店（不論線上或實體商店）使用信用卡或簽帳金融卡時，資金都是以「數位方式」轉移；這種網路當然不可能把有形的實體美元鈔票或英鎊紙幣打包，再把它們郵寄給店家。

先從網際網路開始

各種加密貨幣的故事，真的都要從網際網路的時代開始說起。雖然數位貨幣在網際網路廣泛使用之前就已經存在，但要讓數位貨幣有實際用途，就需要有一種數位貨幣的「傳輸」方式。如果沒有人使用數位通訊網路（1994 年之前很少人使用）的話，數位貨幣也很難形成實際的用途。

在 1994 年之後，數以百萬計的人開始使用全球數位通訊網路，也就是網際網路時，出現了一個實際的問題：我們該如何在網路上花錢？當然從現在的角度看起來答案很簡單：使用信用卡、簽帳金融卡或 PayPal 帳戶即可。但當我們回溯到 90 年代中期時，情況要複雜得多。

收取信用卡支付的難題

讓我們回到 90 年代中期，某些讀者可能還記得（我知道許多讀者都太年輕了，以致於完全不記得有這回事），人們對於在網路上使用信用卡消費，抱持著相當謹慎的態度。還記得 1997 年時，我開了自己的出版公司，並透過網站銷售書籍，我（也就是彼得，另一位作者泰勒太年輕了，應該不記得 1997 年的事）經常會收到購書者在信件裡，

裝進從網站上列印的書籍封面，然後附上一張支付書籍費用的支票。我明明在網站上放了「信用卡支付」的選項，但大多數人根本不想使用；因為他們不相信網際網路可以保障信用卡資料的安全性。

此外，當時的商家如果想設置信用卡支付功能，不但很麻煩費用也很高。完全不像現在把信用卡選項添加到網站上，真的是非常簡單的操作，所有電子商務軟體幾乎都內建這項功能。而且像 Stripe 和 Square[註 1] 這樣的刷卡服務，完全降低了商家進入的門檻。商家獲得收取信用卡支付的功能，已經不再像過去那麼麻煩與昂貴。

當然，我們剛剛談的還只是商業交易方面，那個人交易呢？例如一個人該如何把欠朋友的飯錢轉給對方，或是父母如何把生活費轉給唸大學的孩子呢？（我是說在 PayPal 或銀行轉帳之外，基於網路的轉帳。）如果我們想生活在更方便的數位世界中，就應該要有某種數位貨幣。


REMEMBER

現金有個相當重要的特點：現金交易本質上是「匿名」的，沒有紙本紀錄或數位交易的電子紀錄。因此很多人認為要有等效形式的匿名或假名的數位貨幣，才能算是傳統現金結算方法的重大改進。

很多人相信一定有更好的方法，亦即我們需要發明一種用於數位世界的數位貨幣。就目前來看，這種觀點似乎很幼稚；然而回顧過去，很明顯地，信用卡公司不會眼睜睜的看著幾兆美元的交易，轉移到網路上。他們絕對想要分一杯羹，不願放棄壟斷的局面，所以今天在美國和歐洲大部分地區，主要的交易方式，依舊是透過各種銀行卡的交易。

來談點大衛．喬姆

在 1990 年代中期，人們開始在網路上進行各種活動。然而出於不同原因，許多人不想或無法使用信用卡（見上一節）。使用支票也很困難（除非你想郵寄），直接傳送現金也是不可能的。（不過，我要為各位年長的技客們說一個笑話：我確實記得曾經有一位朋友告訴我，請

註 1　兩者均為方便的信用卡支付服務，降低了商家提供信用卡支付選項的門檻。

把我欠他的 10 美元用 UUENCODE 編碼，然後透過電子郵件寄給他。再次聲明，這是彼得在說話；我敢打賭，泰勒太年輕了，應該不知道 UUENCODE 是什麼？[註 2]）

不過早在 1983 年，一位名叫大衛・喬姆（David Chaum）的人就寫過一篇論文，題目為「免簽名且無法追蹤的交易」（Blind Signatures for Untraceable Transactions）。喬姆是一位密碼學家（cryptographer，也就是從事密碼學工作的人）暨電腦科學教授。他的論文描述了一種使用密碼學創建數位現金系統的方法，該系統可以實現匿名交易，就像現金一樣（現代密碼學是保護線上通訊的一種科學；我們稍後再談）。事實上，喬姆通常被稱為「數位貨幣之父」或「線上匿名之父」。

結果呢？ DigiCash、E-Gold、Millicent、CyberCash 等

把網際網路、複雜的線上交易、對線上使用信用卡的恐懼、對類似現金的匿名線上交易的渴望，以及大衛・喬姆在 80 年代的論文（見上一節）通通加在一起，最後會得到什麼呢？

首先是大衛・喬姆 1990 年的 DigiCash 數位現金系統。可惜的是，喬姆先生的理念似乎太過領先於時代，DigiCash 到 1998 年就倒閉了。還有 E-Gold（電子黃金），一種據說是由黃金支持的數位現金系統，還有 DEC 的 Millicent（是的，大多數讀者應該都太年輕了，不太可能聽過 DEC。我一邊寫這個數位現金的「歷史」，一邊開始覺得自己有點老了），還有 First Virtual（第一虛擬）、CyberCash（網路現金）、b-money（B 錢）、Hashcash（哈希現金）、eCash（e 錢）、Bit Gold（點金）、Cybercoin（網路代幣） 等。還有擁有 1 億美元的投資資本的 Beenz（賓錢）；由琥碧戈柏代言（真的！）的 Flooz（流金）；被指控洗錢後關閉的 Liberty Reserve（自由儲備金）；和中國的 Q 幣等。

註 2　UUENCODE 是指「Unix-to-Unix encoding」，亦即在 Unix 系統下，將資料藉由 uucp 郵件系統傳送的編碼程式。

除了 Q 幣還在騰訊 QQ 服務上使用外，所有當時出現的這些數位貨幣都已經消失了。值得注意的是，這些早期的數位貨幣中，或多或少都需要受信任的第三方，也就是中心化的管理。

當然這股數位貨幣的潮流並未就此結束。雖然起步很艱難，經歷了許多嘗試錯誤，但很多人仍然認為世界需要類似現金的（換句話說，匿名的）線上交易方式。因此，一個新的時代即將開始：加密貨幣時代。

早期的數位貨幣當然也依賴於密碼學（這是真的），然而它們卻從未被稱為加密貨幣。直到 2008 年加密貨幣與「區塊鏈」相互結合後，大家才開始使用「加密貨幣」這個稱呼，而且直到 2012 年左右，這個專有名詞才真正開始廣泛的出現（區塊鏈是一種特殊形式的資料庫，本章稍後會詳細介紹）。

比特幣白皮書

2008 年，中本聰（Satoshi Nakamoto）在一個名為「密碼龐克郵件列表」的密碼學論壇上，發布了一份題目為「比特幣：點對點電子現金系統」（Bitcoin：A Peer-to-Peer Electronic Cash System）的文件，宣稱「……我一直在研究一種新的電子現金系統，完全是點對點的，不需要受信任的第三方……」。

中本聰表示，以下這些屬性是比特幣的關鍵重點：

- 透過點對點網路防止雙花（雙重支付）。
- 沒有鑄幣方或其他受信任方。
- 參與者可匿名。
- 新代幣[註3]由 Hashcash（哈希現金，前面提到過）式的工作量證明生成。
- 新代幣生成的工作量證明也為網路提供動力，以防止雙花。

註 3　代幣（coin）是加密貨幣（cryptocurrency）的簡化說法。

這份文件讀起來相當枯燥，但值得花幾分鐘朝聖一下，你可以在 https://bitcoin.org/bitcoin.pdf 找到這份文件。比特幣白皮書的開頭寫著：「一種純粹的點對點版本的電子現金，允許線上支付直接從一方發送到另一方，無須透過金融機構……」。中本聰解釋，他的方法解決了「雙花」問題，這也是困擾早期數位貨幣的一個重大問題，也就是本質上容易被複製的數位貨幣，必須能夠確保同一個貨幣不會被重複花用。

中本聰還描述了使用區塊鏈的功能，不過「區塊鏈」一詞在白皮書中並未出現：

> 「我們建議……使用對等網路。網路將交易雜湊到一個連續的，基於雜湊演算法的工作量證明鏈中，來對交易進行時間戳記，形成一個除非重做工作量證明，否則無法更改的紀錄。」

比特幣：第一個區塊鏈應用

早在 2009 年 1 月，中本聰便已啟動比特幣網路，使用了區塊鏈（這個概念自 1990 年代初就已經出現，不過這是第一次被正確使用），並創建了區塊鏈中的第一個區塊，稱為「創世區塊」。

創世區塊包含了 50 個比特幣，以及「*2009 年 1 月 3 日泰晤士報報導，英國財相將對銀行進行第二次援助*」的文字，當作比特幣系統為何如此重要的理由和解釋。中本聰也繼續對協議進行編碼更新，執行一個節點，並可能開採了大約 100 萬個比特幣，這個數字將使他在 2017 年底，成為世界上最富有的人之一（至少在「帳面上」如此）。

2010 年底，中本聰發表他的最後一篇論壇貼文並正式退出這個項目，此時已經有許多其他加密貨幣愛好者，加入網路開始挖礦，並且支援項目程式碼的後續開發。接下來的事大家應該都知道了。

中本聰是誰（或什麼）？

中本聰到底是什麼人（或女性），還是某個組織呢？沒人知道。中本聰似乎不是真名，比較可能是化名。如果有人確實知道中本聰是誰，應該也不會說出來，因為這是加密貨幣界最重大的祕密。

有一位日裔美國人名叫多利安・普倫提斯・中本聰（Dorian Prentice Satoshi Nakamoto）。他除了本名是中本聰之外，也是一位受過專業訓練的物理學家、系統工程師以及金融電腦工程師，也許他就是中本聰，然而他多次否認這件事。

住在離這位中本聰家只有幾個街區遠的哈爾・芬尼（Hal Finney）呢？他在比特幣出現之前就是密碼學家了，他也是最早使用比特幣的人之一，並宣稱自己曾經透過電子郵件與比特幣的創始人進行過交流。有人認為他「借用」了附近鄰居中本聰的名字，作為自己的化名。

還有長期涉足數位貨幣領域的尼克・薩博（Nick Szabo），他甚至在中本聰的比特幣白皮書發表之前，就發表了比特黃金（bit gold）白皮書。克雷格・懷特（Craig White）呢，他一度宣稱自己就是中本聰，但後來被指控詐騙。當然也可能是芬蘭經濟社會學家維利・萊東維爾塔（Vili Lehdonvirta）博士，或是愛爾蘭密碼學研究生麥可・克利爾（Michael Clear）？或者是申請了一項專利的三個人，這項專利裡包含了中本聰比特幣白皮書裡使用的晦澀語句「在計算上無法逆轉」（computationally impractical to reverse）。也有人說是日本數學家望月新一（Shinichi Mochizuki）或杰德・麥卡萊布（Jed McCaleb），也有人懷疑是某個政府機構或其他類型的團隊，甚至還有人認為是伊隆・馬斯克（Elon Musk）。好吧，完全沒人知道中本聰是誰，但各種理論都有。

比特幣的第二大謎團呢？中本聰擁有大約 100 萬個比特幣，在 2017 年 12 月的市價約為 190 到 200 億美元左右。然而一般認為屬於中本聰的這些比特幣財富，完全沒有被轉移或花掉；他為何不動這筆錢？

何謂區塊鏈？

要了解加密貨幣，就要先了解區塊鏈。區塊鏈技術很複雜，不過沒關係，你並不需要了解一切，只要了解基礎知識即可。

區塊鏈屬於「資料庫」的類型，**資料庫**只是把數據結構化的整合在一起。假設你蒐集了一堆姓名、街道地址、電子郵件地址和電話號碼，

並將它們輸入文書軟體內，這樣並不能算是資料庫，充其量只是一堆無結構、亂七八糟的文字。

但如果你把這些資料輸入電子表格中，第一列是名字，第二列是姓氏，然後是電子郵件地址、電話號碼、街道地址、城市名稱、郵遞區號、國家等列，這就變成了結構化的資料，也就可以說是一個資料庫。

大多數人都一直在使用資料庫。如果你使用某種財務管理軟體，例如 QuickBooks、Quicken 或 Mint，你的資料將會儲存在資料庫中。如果你使用聯絡人管理軟體來儲存聯絡人訊息，它也會被儲存在資料庫中。因為在各種軟體背後，資料庫是現代數位生活不可或缺的一部分。

全球區塊鏈 —— 區塊鏈網路

區塊鏈就是一個資料庫；它以結構化的形式儲存訊息。你可以將區塊鏈用於各種不同的目的：例如用於**產權登記**（誰擁有這塊土地，如何擁有的？）、或**供應鏈追蹤**（你的酒或魚來自何處，如何運送到你手上？）。區塊鏈可以儲存各種類型的資料，就加密貨幣的情況而言，區塊鏈儲存的是「交易」的資料，包括誰擁有多少加密貨幣，由誰給他們的，他們又把手上的加密貨幣給了誰（是否花掉了）等資料？

當然，區塊鏈有幾個特性。首先，它們必須以網路形式運作。例如比特幣網路、萊特幣網路、以太坊網路等，就像電子郵件網路或網際網路一樣。

就比特幣而言，它是由遍布整個地球的幾千個節點或伺服器所組成的網路。

每個節點都擁有比特幣區塊鏈的「副本」（目前交易紀錄的複製），彼此透過網路相互聯繫並保持「同步」。他們使用**共識**系統，就目前有效的區塊鏈資料庫的內容達成協議。也就是說，它們都擁有區塊鏈的相同副本。

雜湊：為區塊按上「指紋」

由於在許多不同電腦上都有副本的區塊鏈，結構非常強大，使得駭客入侵或想操縱區塊鏈的做法會變得相當困難。區塊鏈還有另一個同樣強大的功能：**雜湊**（*hashing*，又稱哈希或散列，以下均統一稱為雜湊）。**雜湊值**是一串長數字，等於一種數據指紋。區塊鏈使用雜湊的方式如下：

1. **執行節點的電腦蒐集並驗證將要添加到區塊鏈的比特幣交易（在區塊鏈內的地址之間發送的比特幣交易紀錄）。**
2. **當電腦蒐集到夠多交易時，它會創建一個資料區塊並對資料進行雜湊處理：亦即將交易資料傳給一個特殊的雜湊演算法進行處理，該算法將雜湊值回傳。**

   這是來自比特幣區塊鏈中的一個區塊的真實雜湊範例：

   ```
   00000000000000000000297f87446dc8b8855ae4ee2b35260dc4af61e1f5eec579Th
   ```

   雜湊就像是由數據資料做成的指紋一樣，由於複雜數學運算之故，它不可能與任何其他數據資料重複。如果雜湊數值稍微改變一下，例如把其中一個 0 變成 5，或 A 改為 B 的話，雜湊值便無法與原始數據相符。
3. **雜湊值被添加到交易區塊中。**
4. **區塊被添加到區塊鏈上。**
5. **繼續為下一個區塊蒐集更多交易。**
6. **又一個完整的交易區塊準備好後，將前一個區塊的雜湊值添加到新區塊中。**
7. **整個區塊，包括交易資料和前一個區塊的雜湊值，再次被雜湊。**
8. **重複此項過程，並創建帶有時間戳記的區塊鏈。**

因此，每個區塊都會包含兩個雜湊值：前一個區塊的雜湊值和目前區塊的雜湊值，而後者是把所有比特幣交易和前一個區塊雜湊值的組合，再進行雜湊處理後而創建的。

這就是把所有區塊串連在一起形成區塊鏈的方式（見圖 1-1）。由於每個區塊都包含前一個區塊的雜湊值，也就是擁有前一個區塊的「指紋」。事實上，每個區塊也因此可以確定它在區塊鏈中的位置，因為來自前一個區塊的雜湊值可以標示出當前區塊的所在順序。

圖 1-1：每個區塊的雜湊值都會儲存在下一個資料區塊中，如此便可利用雜湊值，將區塊鏈以順序的方式連結在一起。

「不可竄改」的區塊鏈

你可能聽過區塊鏈是**不可竄改的**，這個說法是指它無法被輕易更改。如果比特幣區塊鏈說你擁有 *x* 個比特幣，你便確實擁有 *x* 個比特幣，這點不會有爭議，因為沒人可以進入區塊鏈加以破壞，或是以某種方式來修改變動區塊紀錄。

各位可以想像一下，如果有人進入一個區塊（假設這個區塊叫做區塊 A）修改了數據，會發生什麼情況呢？例如修改一筆向某人發送 1 個比特幣的資料，改成發送 9 個比特幣。

如此一來，區塊 A 中的雜湊值便無法與其數據內容相符。請記住，雜湊就是辨別數據的指紋，因此如果你更改數據，指紋將不再符合。

好吧，那駭客可以重新雜湊區塊 A 的數據資料，然後保存「修正」後的雜湊。但是等一下，現在下一個區塊（區塊 B）又不能符合了，因為區塊 B 帶有區塊 A 的雜湊。所以現在駭客只好繼續修改儲存在區塊 B 中的區塊 A 雜湊值。

但是修改之後，區塊 B 的雜湊值又與區塊 B 的數據資料無法相符了，因為該雜湊是由區塊 B 的交易數據和區塊 A 的雜湊所創建出來的！

因此，區塊 B 必須重新雜湊，並更新其雜湊值。可是再等一下！這不就表示儲存在區塊 C 中的區塊 B 雜湊值又不一樣了？

看看這樣一路下去要修改到什麼時候？如此修改勢必波及整個區塊鏈。也就是只要修改某個區塊中的一個字符，整個區塊鏈就都被破壞了。為了解決這個問題，駭客必須重新計算區塊鏈的區塊。從被駭的區塊開始，必須被「重新挖礦」。因此，看似簡單的駭入修改資料，變成了無法輕鬆完成的重大計算難題。

所以這種雜湊函數，再加上幾千個其他節點都必須與區塊鏈的相同副本「同步」的這個事實，讓區塊鏈幾乎不可能篡改；因此並不容易被駭客入侵。

由於沒有人可以改變它或摧毀它，因此駭客無法進入這樣的點對點節點網路，修改交易來竊取加密貨幣。政府也無法關閉這種網路（例如中國嘗試在其境內禁止比特幣活動，但區塊鏈仍會繼續存在於其他國家），恐怖組織亦無法加以摧毀，或者是一個國家無法攻擊並摧毀另一個國家境內的區塊鏈等。由於區塊鏈在各地電腦上存有許多副本，只要有夠多人繼續使用這種區塊鏈，它就是不可篡改且堅不可摧的存在。

錢在哪裡呢？

你可能很想知道「加密貨幣到底放在哪裡？那些錢到哪裡去了？」或者，你可能聽說過加密貨幣「錢包」，並認為這就是存放加密貨幣的地方。抱歉，這是錯誤的想法。事實上，加密貨幣錢包裡面並沒有錢，也就是沒有加密貨幣。

加密貨幣區塊鏈通常被描述為「**分類帳**」（*ledgers*）。Google 字典將分類帳描述為「一本帳冊或其他特定類型的財務帳戶集」。帳本已經存在了幾百年，經常用於記錄個人、企業、政府部門等各種交易。你的銀行帳戶或信用卡對帳單，就是一種分類帳，可以用來顯示你的個人交易紀錄，包括你付給別人的錢，以及你從別人那裡獲得的錢。

在區塊鏈中查詢收支

區塊鏈並沒有為每個錢包地址儲存加密貨幣餘額。整個區塊鏈中，也沒有任何地方說明任何特定所有者擁有多少加密貨幣，或任何特定地址與某人相互關聯等。你可以查詢的是以區塊鏈瀏覽器追蹤你的所有交易，亦即加密貨幣的傳入和發送，區塊鏈瀏覽器是根據這些交易，「計算」出你的加密貨幣餘額（也就是你擁有多少錢是靠所有交易的計算而來）。

從加密貨幣的角度來看，區塊鏈就是一種數位分類帳，記錄了你發送給別人的加密貨幣，以及你從別人那裡收到的加密貨幣。

你可以這樣思考：假設你有點強迫症，喜歡記錄自己口袋裡的現金。所以你隨身帶著記事本，用來記錄你每次往口袋裡放錢和每次花錢的時間，然後計算目前的餘額。這本記事本就算是一種交易帳本，對吧？

加密貨幣跟這種現金交易帳本非常類似，只差不能放在你的口袋裡。區塊鏈就是帳本；它會儲存每筆交易的紀錄（包括你購買或被發送的加密貨幣，何時花費或出售加密貨幣，以及你現在擁有的餘額等）。

不過這一切並不是放在一個小袋子裡，也沒有把加密貨幣存放在某個地方。區塊鏈只是儲存在分類帳中的一系列「神秘的」（或虛擬的）交易紀錄，完全沒有實體貨幣被轉移；有的只是說明貨幣已被轉移的更新紀錄。

帳本上說你擁有加密貨幣，代表每個人都可以驗證並接受你擁有這些加密貨幣。請記住，前面說過這本分類帳在加入區塊鏈後便無法篡改，無法被駭客入侵（相關訊息請參閱上一節）。因此，如果分類帳上說你擁有半個比特幣，你便絕對擁有這半個比特幣。而且你還可以把這半個比特幣賣（發送）給其他人，分類帳更新後便可證明對方擁有它！

那錢包呢？錢包是用來存錢的吧？不不不，加密貨幣錢包裡並不儲存加密貨幣，它所儲存的是私鑰、公鑰和錢包地址。私鑰是最重要的，因為它們控制著與你的加密貨幣在區塊鏈中關聯的地址。

加密貨幣中的加密是什麼意思？

加密貨幣中的**加密**是指密碼學的加密，那密碼學到底是什麼？

根據牛津英語詞典，密碼學是「編寫或解決密碼的藝術」。維基百科的解釋更複雜也更數位化：「安全通訊技術的實踐和研究……密碼學是關於建構和分析並防止第三方或公眾閱讀私人訊息的協議」。

密碼學的歷史至少可以追溯到 4000 年前，由於人們偶爾就需要發送各種祕密訊息，這也就是密碼學存在的意義。

現在的密碼學在電腦協助下，遠比古典世界的古代密碼學要複雜得多，應用範圍也更廣。事實上，密碼學已經是網際網路不可或缺的一部分。如果沒有密碼學，網際網路就無法按照我們想要的方式運作。

也就是說，每次你在使用網路瀏覽器時，幾乎都在使用密碼學。例如瀏覽器地址欄中的小鎖圖示，如圖 1-2 所示。

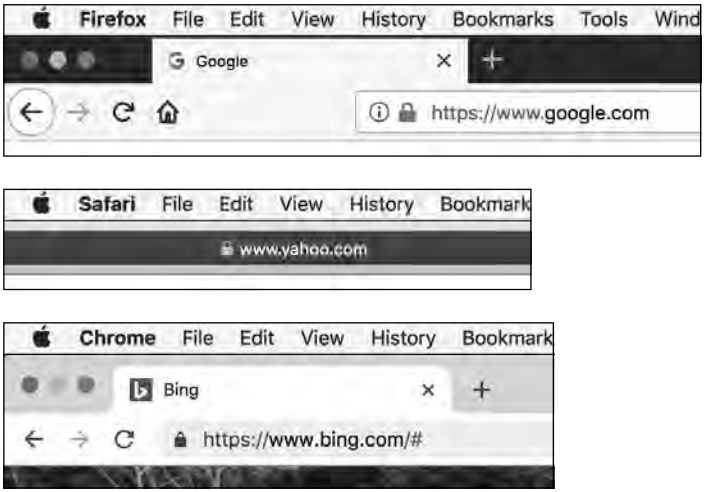

圖 1-2：瀏覽器的鎖定圖示，代表傳回網路伺服器的數據，將會使用加密技術進行加密。

鎖定圖示表示這個頁面是安全的。當你在瀏覽器和網路伺服器之間來回傳送訊息時，該訊息將被**加密**（打亂資料）。因此，當它在兩點之間距離幾百或幾千英里的網際網路傳輸中被截獲時，訊息便無法破解讀取。舉例來說，當你的信用卡號傳輸到電子商務網站時，它會先被你的瀏覽器加密，再傳送到網路伺服器，然後由接收伺服器進行解密。

所以區塊鏈是加密的，對吧？不對！加密貨幣使用了密碼學，但並不是為了打亂區塊鏈中的數據資料，因為區塊鏈是開放的、公共的且可審查的。圖 1-3 展示了為比特幣設計的區塊鏈瀏覽器範例。只要使用區塊鏈瀏覽器，任何人都可以觀看區塊鏈、並查看自創世區塊（比特幣創建的第一個區塊）以來，發生過的每一筆交易。

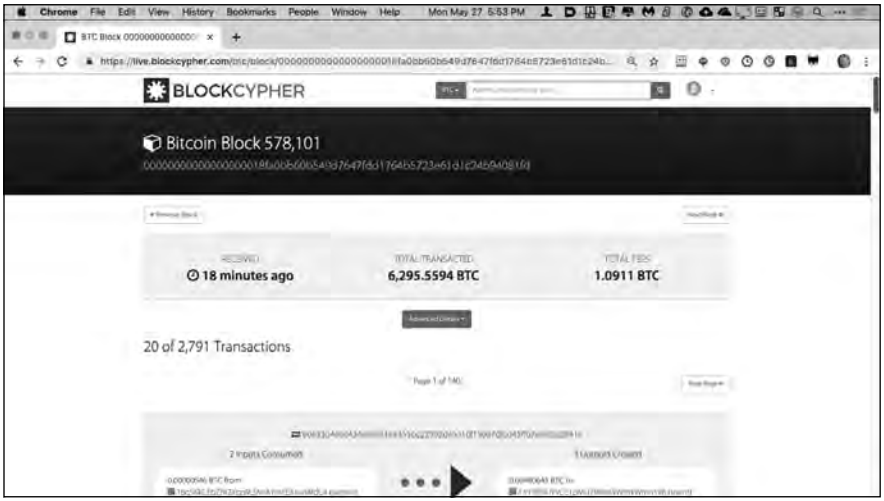

圖 1-3：https://live.blockcypher.com/btc 上的區塊鏈瀏覽器工具範例。

將區塊鏈加密

事實上，我們也可以建構加密的區塊鏈，將區塊鏈中的數據進行加密。雖然比特幣區塊鏈並未加密，而且任何人都可以查看（使用如圖 1-3 中的區塊鏈瀏覽器），但我們也可以創建一個隱藏交易數據的「加密區塊鏈」，例如大零幣（Zcash）便是如此。不過一般加密貨幣區塊鏈並不會加密，任何人都可以讀取其中儲存的交易紀錄。

所以加密貨幣並不是加密區塊鏈中的數據，而是加密你發送到區塊鏈的訊息，這些訊息就是觸發交易和更新區塊鏈分類帳的訊息。

公鑰加密魔法

公鑰加密是使用數位加密魔法所創建出來的一個聰明的小技巧。這類加密都是使用非常複雜的數學來完成的，即使是擁有數學學位的人，可能也難以理解的那種數學理論。這些超難數學理論的名稱，聽起來通常都像是卡邁克爾數（*Carmichael numbers*）或戈帕密碼（*Goppa codes*）這類，也就是那種我無法理解，你應該也不懂的數學（好吧，

應該說大多數讀者都不懂，別吹毛求疵了）。這當然沒關係，就像我們也不是很清楚「重力」的原理，但我們每天都在使用重力。

所以，請忘記這種驚人的數學原理到底如何運作，而應該考量的是它實際上完成了什麼？因此，接著我們要請各位想像有一個保險箱，上面有兩個鑰匙孔和兩把相關的鑰匙。其中一把是公鑰，另一把是私鑰。你把某些東西放進保險箱，然後使用公鑰把保險箱鎖起來。一旦保險箱門關閉鎖上後，公鑰就無法再打開保險箱；亦即不能用來解鎖保險箱拿取物品。接著私鑰就派上用場了，打開這個保險箱的唯一方法便是使用私鑰。

事實上，這個神奇的數學保險箱是「雙向」的。你可以用私鑰鎖住保險箱，但是上鎖後就不能用私鑰打開保險箱了，只有公鑰才能打開用私鑰鎖定的保險箱。

這兩把鑰匙神奇的關聯在一起。它們只能相互搭配使用，而且沒有其他的鑰匙。不僅如此，私鑰 X 僅適用於公鑰 X，反之亦然。你也不能使用公鑰 X 鎖定保險箱，然後使用私鑰 W 或私鑰 K 解鎖保險箱。

好的，同樣的原理，但是現在換成電子訊息來看。我們可以使用公鑰鎖定電子訊息，也就是說，使用公鑰對訊息（例如從你的瀏覽器發送到網路伺服器的電子郵件或訊息）進行干擾或加密。

而在另一端（電子郵件收件人或網路伺服器）收到該鎖定（加密）的訊息後，只有使用私鑰才能將其解鎖閱讀；而且在這個時候，公鑰無法解鎖了（無法打開你的訊息）。因此二者就像是用神奇的魔法關聯在一起（好吧，是數學的關聯在一起），沒有別的解釋了。

加密是一種相當方便的訊息保密工具。亦即我可以給你一把公鑰，讓你寫一條訊息給我，然後你用我的公鑰把訊息加密發送給我。一旦訊息加密後，世界上便沒有任何人可以閱讀這條訊息，除非他們擁有我的私鑰。所以只要我小心的保護我的私鑰，我就是世界上唯一能解讀這條訊息的人。

這些鑰匙的名稱並不是隨便命名的。「私鑰」應該是真正私密的，這個世界上只有你，沒有其他人可以擁有它。而「公鑰」顧名思義是可

以公開的，你可以把它傳送給任何人。例如你想讓人們透過電子郵件將訊息傳送給你的話，你就可以在網站、電子郵件末尾、名片上或其他任何地方，發布你的公鑰，以便讓任何想要發送訊息給你的人，都可以用你的公鑰加密，因為大家都知道你是世界上唯一可以閱讀這條訊息的人（前提是你小心保存了私鑰）。


TIP

電子郵件到底如何加密呢？電子郵件加密已經存在了幾十年，但似乎從未吸引大眾的關注。然而你每天都會自動為大多數電子郵件加密，因為 Outlook、Gmail 和 Yahoo! Mail，以及其他一些郵件系統如 ProtonMail 等，都是預設將郵件加密。

當你在網路上傳送信用卡訊息時，其過程本質上就是網路瀏覽器的作用過程；瀏覽器使用網路伺服器的公鑰對數據進行加密，如此便只有帶有相關私鑰的網路瀏覽器，才能解密和讀取這條信用卡訊息（好吧，這樣說有點把過程簡化了。瀏覽器到伺服器的通訊過程比這個描述要複雜得多，還要涉及到暫時的處理密鑰等；但其基本原理仍然適用）。

發送到區塊鏈的訊息

當你把交易發送到區塊鏈時，你使用了公鑰加密。也就是當你想向其他人發送比特幣時，你會向區塊鏈發送一條加密訊息，上面寫著「把我的 *x.xx* 個比特幣發送到這個地址」。

可是等一下，我剛剛才告訴過你區塊鏈並沒有加密，現在我又告訴你發送到區塊鏈的「訊息」是加密的？如果你本來就打算要讓大家解密這個訊息，那又為何要關心發送到區塊鏈的訊息是否被加密呢？

好吧，還記得我說過這種「鎖定 / 解鎖」的原理是雙向的嗎？你可以用公鑰鎖上，用私鑰開鎖，也可以用私鑰鎖上，用公鑰開鎖。無論哪種方式，資料都是加密的，差別在於誰有能力解讀它。如果你用公鑰加密某項訊息，世界上唯一能解密的人就是擁有對應私鑰的人。但是如果你用私鑰來加密訊息的話，世界上唯一能打開它的人就是……每個人都可以啊！因為任何人都可以獲得公鑰。記住！公鑰本來就是公開的。

那到底用私鑰加密訊息的目的是什麼？很明顯地，我們並不是要保護這條訊息，因為任何人都可以解密此訊息。所以加密的目的是「簽署」訊息（交易），以證明相關公鑰的所有權（屬於擁有私鑰的人）。

用私鑰為訊息簽名

假設我在網站、電子郵件和名片上發布了我的公鑰。有一天你收到一條似乎來自我的訊息，你該如何確定訊息是我發送的呢？我用的方法是使用我的「私鑰」加密此訊息。你只要拿我的公鑰（這是公開的）來解密訊息即可，如果這則訊息真的是我發送的，我的公鑰便可將其解密，讓你可以閱讀訊息。如果不是我發送的，我的公鑰便無法解密此訊息，代表訊息是來自其他人所發送。

因此，使用私鑰加密訊息時，我等於簽署了訊息，證明訊息是我發送的。收件人便可知道該訊息是由擁有可打開此訊息的公鑰「相關聯的私鑰」的人所發送。

區塊鏈地址：你的錢的家

區塊鏈中的所有加密貨幣都與地址相關聯。這是我剛剛使用 blockchain.com 上的區塊鏈瀏覽器，從比特幣區塊鏈中抓取的一個地址範例：

```
1L7hHWfJL1dd7ZhQFgRv8ke1PTKAHoc9Tq
```

區塊鏈上可以有數以兆計的不同地址，所以這個地址基本上是「唯一」的。那這個地址是怎麼來的？地址是來自一個從私鑰生成它的錢包（實際過程要透過很複雜的數學），該錢包裡面包含了一個公鑰和一個私鑰。

REMEMBER

公鑰與私鑰與地址的關聯：公鑰是從私鑰創建的，而地址與公鑰相關聯；事實上，地址是由公鑰創建的。因此，這三者在數學關係上獨一無二，相互關聯。