文章於 2018 年 3 月 19 日刊登於星島日報

區塊鏈簡介

「區塊鏈」（Blockchain）和大家所熟知的「比特幣」（Bitcoin）有密切關係。比特幣被認為是區塊鏈的一個起源，其底層技術是採用區塊鏈。通俗來講，區塊鏈是一種「記帳的技術」，若把區塊鏈看作一本公開的帳本，那麼區塊就是這帳本的每一頁。每個區塊都記錄了若干筆交易，這些交易的細節，網絡裏任何人都可查閱；每個區塊被標記上時間戳，並附帶上一個區塊的特徵值（hash 值），區塊之間通過 hash 值的運算鏈接在一起。二〇〇八年，基於區塊鏈技術的比特幣誕生，翌年一月，比特幣的第一個區塊——創世區塊（Genesis Block）在一台位於芬蘭的小型服務器上創立。之後，關於比特幣的所有交易都被詳細記錄在一個個區塊中。比特幣借助區塊鏈技術，成為迄今最成功的一種數字貨幣。

促成比特幣誕生

區塊鏈技術是一項顛覆性的創新技術，它依靠複雜的密碼學原理，解決互聯網時代最重要的安全信任問題，使雙方可在毋須第三方介入的前提下完成交易。比如，A 想用一百萬人民幣向 B 兌換一百零八萬港幣。A 和 B 互相不認識，更談不上互相信任，他們不願意把錢先轉帳給對方。為完成交易，他們一起找中間人 C，把貨幣分別交給 C，但 C 卻捲款逃跑了。對於這個案例，利用區塊鏈技術能容易地解決信任問題並達成交易。方法就是寫一個「智能合約」，它不被任何人控制，只能被合約的代碼控制。合約的代碼把一百零八萬港幣轉給 A，把一百萬人民幣轉給 B。如果 A 和 B 雙方同意這個代碼，他們把各自的貨幣轉到智能合約帳戶。然後，這個代碼就放到一個區塊鏈上運行。代碼一旦執行，A 和 B 就完成交易，不用擔心有人賴帳。

區塊鏈有幾項特徵，其一是「去中心化」，它毋須依靠任何管理機構或中心機制。每個區塊鏈上的信息分別存儲在不同的雲端，運算和存儲都是分布式。另一特徵是「不可篡改性」，每筆交易記錄一旦被驗證完畢，就永久地寫入該區塊。每個區塊都會計算一個特徵值，並把該特徵值放進下一個區塊，確保資料

不會被篡改。區塊鏈還具有「開放性」、「獨立性」、「安全性」和「匿名性」等特徵。

區塊鏈技術可應用於智能合約、證券交易、電子商務和物聯網等領域。麻省理工學院（MIT）已利用區塊鏈技術，通過智能手機向逾百名畢業生頒發其電子文憑。目前英國已把區塊鏈列為國家戰略，中國也把區塊鏈列入「十三五」國家信息化規劃。對區塊鏈未來的發展，我們拭目以待！

註：小題為本報所加

恒生管理學院電子計算系助理教授　劉海博士