【解牛集】— 刊於〈信報〉，2017 年 8 月 1 日

認識區塊鏈可知比特幣真面目

許佳龍

科大資訊、商業統計及營運管理學系教授

虛擬電子貨幣比特幣（Bitcoin）暴起暴跌之勢令人矚目， 6 月 11 日，比特幣升破 3000 美元後即大幅下滑，最低跌穿 2000 美元。其後，有傳聞投機炒家入市，比特幣需求再度回升，價格反彈。在成交方面，據 Zero Hedge 7 月 25 日的報導，美銀美林發表一份研究報告指出，比特幣、以太幣等大型虛擬貨幣的成交量，最近幾年大幅飆升，如 2012 年，每日成交額約為 4 億美元、如今已飆升至 20 億美元，虛擬貨幣的總體日成交額，已經比黃金還高。

從比特幣急起急跌的走勢看，其投資風險相當高，小投資者若想加入買賣行列，應該對比特幣與建構比特幣的技術基礎——即區塊鏈（Blockchain）有所認識，不宜盲目。筆者試以一般人都容易理解的闡述，來談一下比特幣和區塊鏈技術。由於區塊鏈在商業領域的應用愈來愈廣泛，要普及化應用，也必須讓社會大眾對它有所認識。

比特幣出世之原委

區塊鏈其實是建基於互聯網的技術。2008 年，署名中本聰發表了一份研究報告——《比特幣：端對端電子現金系統》（Bitcoin: A Peer-to-Peer Electronic Cash System）後，隨即在 2009 年作系統的實際運行，第一個比特幣出世。這個「創幣」的新技術，當時還沒有人稱之為區塊鏈（Blockchain）技術，只因技術牽涉一連串的區塊，每一個區塊都會記錄前一個區塊的交易證明及新的交易記錄，形成一條鏈狀結構，最後大家便以區塊鏈名之。

在進一步闡釋前，不妨先說一下比特幣當年橫空出世的原委與目的，是要解決一個在互聯網上數十年來都沒有解決的難題，即如何在互聯網上製造一個真正的現金流。於此，我們回頭看看非互聯網的現實世界，在交易上，我們有電子付款、信用咭、銀行電子轉帳以至現金等交換工具。比較一下，電子轉帳和現金其實有很大不同，不同之處究竟何在？

簡單來說，使用現金進行交易，別人不知道使用者的身份，亦即可以匿名。在互

聯網上，每個人都需要有一個戶口，自從互聯網在上世紀九十年代流行後，一直以來，都無法在互聯網上建立一個「現金概念」的交易工具，即「付錢」後，別人不知道付款者的身份，亦即可以進行匿名交易。

另一方面，在現實世界，大家使用的現金貨幣，都有一個發行貨幣的機構，無論是該國的中央銀行或其他機構，其貨幣都得到用作交易、兌換和儲存的普遍信心和信用。由於互聯網是跨國性的、沒有國界的平台，即使在互聯網上建立起一個「現金概念」的交易工具，但由誰或那個國家來發行這「現金貨幣」？這貨幣可信賴嗎？這些問題一直無法有效解決。

網絡上交易安全可靠

署名中本聰者，以創新的區塊鏈技術，作為建構比特幣的基礎，此舉即成功解決了上述的多個問題。可以說，中本聰以區塊鏈技術創立了比特幣，但區塊鏈技術的特質，又令區塊鏈技術本身，獨立地在商業世界上得到廣濶的應用空間。

區塊鏈其實是一種數碼分類帳，每一個區塊都會記錄前一區塊的所有交易證明，並形成鏈狀結構，且不需要有一個外在的第三方進行發行、也毋須借助任何外在的中心機構監管，就構成一個可共享的數碼分類賬網絡，當中的數字不可篡改、不可偽造，具透明性和可追溯性，因而不僅可有效紀錄比特幣等加密貨幣所進行的交易；也可廣泛用於所有需要中間人作保、認證等市場。

用一般人都可以理解的話來說，區塊鏈技術本身可製造「電子貨幣」，在現實世界，法定貨幣由一張具體紙幣代表及訂明了其價值，但是，在虛擬的網絡世界，區塊鏈所製造的「電子貨幣」，只是一個「電子數字」——這個數碼代表一個可供交易的「錢幣」，這個「錢幣」的交易，都紀綠在一個電子區塊之上。雖然每一個參與交易的人也需要一個戶口，即比特幣的電子錢包，但這個戶口完全與你在現實世界的身份無關。

數字不可更改不可偽造

只要你有一個比特幣電子錢包，你就可以用比特幣進行收取或支付的任何交易；透過區塊鏈技術，所有交易都一一清楚紀錄下來，數字不可更改、不可偽造，具透明性和可追溯性，這些特性，不僅可以讓比特幣在互聯網上具備和發揮充份的「現金概念」，也可以廣泛應用到傳統上需要中間人作保或認証的商業活動上。

由一個比特幣出世一刻，到目前這一刻，應出現過很多的交易轉折。透過區塊鏈技術，每一次的轉手交易都紀錄得一清二楚。與此同時，區塊鏈幣還有一個設計

上的重要特色，就是透過所謂的「哈希算法」（Hash），使已紀錄的交易數碼，百份百不能再篡改。

舉例來說，我昨天給了某帳戶一個比特幣，「哈希算法」可以確保這個比特幣交易是真實的，沒有欺詐做假。因為在區塊鏈中的虛擬電子貨幣交易，都具有透明性、可追溯性和不可篡改的特質。這些特質，正好支持並擔任互聯網上的「現金」角色。

毋須第三方監管

區塊鏈技術還有一個特色，是毋須任何第三方監管，在區塊鏈技術上，由用戶參與其中，中間毋須第三者審核；至於比特幣的發行，也是透過電腦程式一早已編排好，內裡完全沒有政府或監管機構插手其中。換句話說，區塊鏈技術這個特色，也解決了互聯網上「現金系統」難以監管的問題。

可以看到，在現實世界中，錢幣的印製可以由銀行做，但法定貨幣必須有一個監管機構，去確保貨幣體系的運行秩序和安全性。在互聯網上，很難有一個監管機構，因為互聯網不屬於任何一個單一國家。

換言之，區塊鏈技術可以有效解決了這個問題，因為透過區塊鏈技術建構的比特幣，不需要任何個體或組織去發行這貨幣；也不需要有任何第三方進行監管，用戶可以在不信任其他人的前提下，去參與這個虛擬電子貨幣體系。

總結一下區塊鏈技術的特色——

第一，所記錄的數字不可篡改、不可偽造，所有的交易紀錄具透明性和可追溯性；

第二，在上述基礎上所形成的交易安全環境，不需要第三方監管，用戶也可以具信心地進行交易或資產交換。

區塊鏈技術特質廣泛應用

這些特質，便可以在商業世界上大派用場。試想一想，在現實的商業世界，很多交易由開始到完成，過程中間有不少行政程序，根本的原因，在於交易雙方缺乏相互的信任，需要第三方的中間人來作擔保或認証。

以物業交易為例，無論在香港或其他地方，交易中間需要經過一系列法律程序，並交由律師處理。手續之所以如此繁複，是因為需要律師（第三方）去作出認証，

如替買方進行查冊，確保屋契是否完整，內裡有沒有問題；或者由律師去確保買方有足夠的資金付款，賣方的業主身份真實等等。

在電子網絡世界，利用區塊鏈技術的特色，可以把物業過去的所有交易記錄下來，準確無訛，資料亦不可篡改。以查冊為例，把這個物業的屋契資料記錄在區塊鏈之中，包括這物業從建造出來首次交易至今，當中所有持有者進行過多少次交易、物業按揭、多少次轉按等，這樣一來，在物業交易過程中，便可以省卻不少律師的工作，不僅可以節省交易費用，也可以使交易更簡化，更有效率。這是一個區塊鏈技術可以在商業世界很快應用的例子。

「智能合約」節省人力

由於應用區塊鏈技術的活動毋須要監管，也能夠營構出一個安全可信賴的交易環境，使互聯網的用戶能夠有更多的創造空間，去把區塊鏈技術應用到很多商業活動上，這些商業活動，在現實世界中也不容易進行，例如應用區塊鏈技術的「智能合約」。

所謂「智能合約」，簡單來說，兩家公司有一項交易，無論是買賣也好，交換物資也好，透過智能合約，把合約交易條文寫在區塊鏈上，當智能合約紀錄在區塊鏈上之後，當抵達某一特定時點，合約便自動成交，毋須再經過人手去跟進或覆核到底這項交易是否成功，可以看到，透過區塊鏈技術，便可支援這些交易，毋須更多人力不斷地去處理。

筆者接觸業界得到的印象，目前，業界現正積極設計一些應用區塊鏈技術的業務。金管局去年發表一份《分布式分類帳技術白皮書》（Distributed Ledger Technology），讓業界了解不同的創新技術，包括應用區塊鏈技術或分布式分類帳技術在銀行業及支付服務上的應用潛力，可以預見，區塊鏈技術在商業領域的應用愈來愈廣泛。囿於篇幅，對有關區塊鏈與智能合約的應用，筆者另文再續述。

〔區塊鏈技術與應用・二之一〕

〔本文由科大商學院傳訊部筆錄，許佳龍教授口述及整理定稿〕