【解牛集】— 刊於〈信報〉，2017 年 8 月 15 日

以太坊造就智能合約登場

許佳龍

科大資訊、商業統計及營運管理學系講座教授

筆者前文扼要介紹了比特幣和區塊鏈技術的特性，本文續談比特幣與區塊鏈技術，接著便討論以太幣（Ether）、以太坊（Ethereum）區塊鏈與智能合約（Smart Contract），務使一般人都能認識區塊鏈的應用技術關鍵。事實上，要推廣區塊鏈在商業上的普及應用，首先要讓公眾對之有所認識，這無疑是推廣應用的前提。

據筆者接觸到銀行業界對區塊鏈技術應用的潛質評估，很多都持樂觀態度。在一些論壇上，甚至有研究人員相信，區塊鏈他日可以取代互聯網，亦即今天在互聯網上進行的交易活動，完全可以在區塊鏈中進行。不過，筆者要提出一點，區塊鏈如今有那麼大的應用潛質或憧憬空間，最大的原因在於其兩大特性——

第一，區塊鏈可以把所有交易完整地紀錄下來，也能夠確保交易紀錄的數字不可篡改、不可偽造、具透明性和可追溯；

第二，區塊鏈技術所構成的交易安全環境，毋須第三方機構去管理與監管，用戶也可以有信心地進行交易或資產交換。

對缺乏政府監管不放心

不過，是否每一家商業機構的每一項業務都需要上述這些交易特性？答案是「不一定」。因此，當大家興高采烈對區塊鏈技術充滿暇想時，我們也須注意到，區塊鏈歸根究柢只不個是一種技術，這技術有其應用好處，但不一定適合每家商業機構或業務。筆者曾參加過一些論壇和跟業界討論過，有業界人士表示，對於缺乏政府的監管，他們始終有點不放心。譬如，比特幣就是一個例子，由於比特幣沒有一個發行機構，即使政府想監管，也不得要領，這個沒有第三方監管的市場運行秩序，予人有不規範的擔心。

對於比特幣的發行，是透過個體或團體進行「挖礦」而增量，簡單來說，其實是在「礦池」上通過運行複雜程序算法而得出來。可以說，比特幣整體的設計，「挖礦」的目的，就是為了製造區塊。基於交易訊息紀錄在區塊之上，只有新的區塊，

才可增加新的交易，而區塊與區塊便可形成一條能無限制伸延的鏈條。據筆者所知，由 2009 年迄今，比特幣已建立共四十多萬個區塊。

至於比特幣設計的區塊容量為 1「百萬位元組」(1 megabyte • MB)，當達到 1MB，就產生一個區塊出來。由於比特幣愈來愈流行，交易也愈來愈多，漸漸發覺容量 1MB 並不足夠，所以衍生出激烈的討論，究竟是否需要更改當初的設計，把區塊的容量增大。

擴容爭議致比特幣「分裂」

囿於原有區塊 1MB 的容量限制了交易速度， 因而在比特幣礦池之間，有提出不同的解決方案，包括有建議 1MB 容量不變，但可在這個 1MB 容量區塊上，增加一個 3MB 的「隔離見証」區塊（Segregated Witness ，簡稱為 SegWit），亦即不是把區塊容量（block-size）變大，而是把區塊的「載量」（block-weight）增加。就好像香港的電車，過去當交通繁忙時，在電車之後加上一列「拖車」。這增加載量的「隔離見証」區塊，把交易的細節，如交易金額、認證資料等分開來處理，從而提升原有 1MB 區塊可以盛載的交易數量。

但是，亦有不同的解決方案建議，包括要求直接把容量擴大到 8MB，並拒絕執行「隔離見証」（SegWit）。兩個陣營意見不合，提倡直接把容量擴大的陣營在 8 月 1 日起透過硬分支（hard fork）另起爐灶，形成另一個數位加密貨幣 Bitcoin Cash（BCC），令比特幣形成「分裂」之勢。幾日之內，BCC 已成為市值第三大的加密貨幣，後續發展，須拭目以待。

虛擬貨幣價值由供需決定

明白到電子虛擬貨幣的特質、出台、發展和價值所在，才不致作出盲目投資。很清楚，比特幣只是一種虛擬貨幣，沒有實體性價值，嚴格來說，跟一張公司証券無異，價值取決於大家對其未來前景所形成的邊際供求關係。由於交易頻率目前不算高，因此，只要邊際的供應或需求出現變化，都可能導致當日的價格急上急跌。

究竟比特幣有沒有一個真正的價值，委實也很難說。想深一層，即使在現實世界，美元的紙幣，其價值也是由人（中央銀行作為「法定人」）來賦予。比特幣的價值，嚴格來說也如是，事實上，虛擬電子貨幣的價值，由買賣雙方來決定。

討論至此，我們看看另一個經常提及的「以太幣」（Ether）。最近，以太幣的價格也告飆升。很明顯，以太幣受到矚目，主要是背後的以太坊（Ethereum）技術

潛力。

以太幣與智能合約

比較一下比特幣和以太幣的分別很有意思。比特幣純粹是「貨幣交易」，亦即只擔當貨幣的功能，包括交易、計價與儲值等，不涉及其他範圍；然而，以太幣的出世，並不是以「貨幣交易」為目標，而是有一個更高的理想，亦即透過以太幣背後的技術——以太坊（Ethereum），用來支援「智能合約」（Smart Contract）的執行。換言之，雖然比特幣和以太幣同樣使用區塊鏈技術，但以太幣的區塊鏈平台——以太坊，是讓智能合約能在平台上進行交易。

可以說，以太幣設立的目的，較比特幣還要宏大，創辦人布特林（Vitalik Buterin）冀全球的交易透過智能合約的形式，可以在以太坊的區塊鏈上紀錄下來。

所謂智能合約，早於上世紀九十年代，此理念由電腦科學家、法律學者和密碼學專家尼克・薩博（Nick Szabo）提出來，但由於當時缺乏可賦予交易雙方信任的執行平台，令智能合約無法在產業世界得到應用。以太坊的面世，讓智能合約有登場的機會。

看深一層，以太坊允許開發人員能編程「智能合約」。簡單來說，智能合約其實是一種電腦編程，當一個預先編好的條件被觸發時，便能自動執行相應的合約條款。以太坊區塊鏈技術所形成的安全可信的平台，就像一個可以信任的人，擔起很多現時需要簽署合約，靠第三方保証，才能進行的商業交易活動。

以太幣設立目標宏大

如果以太坊成功，意味全球的種種交易，能夠透過智能合約的形式，在以太坊的區塊鏈上紀錄下來，則不僅顛覆目前不少傳統的商業交易模式，如需要律師設計好交易的法律依據和進行監督保証，也可以使以太幣的交易量大幅增加，流通量和交易頻率都會較比特幣為大，用途更廣泛。然而問題是，以太幣目前的交易量相對還是不大。

另一方面，以太幣和比特幣還有一個不同之處，由於以太幣用來支援智能合約，而智能合約牽涉更多程序的編寫，因為每一個參與的人，都要編寫本身的智能合約，故在程序編寫過程中，導入了額外一重的保安顧慮。換言之，合約編程寫得好不好，有沒有漏洞，便大有文章。如果合約寫得不好，有漏洞，就容易為「黑客」所乘，把合約更改，從中盜取以太幣。

雖然區塊鏈本身的安全性完全沒有問題，但問題是，基於以太坊的區塊鏈技術支

援智能合約，在把智能合約的內容訊息「嵌入」區塊鏈的中間，之前的過程就有機會讓「黑客」從中做手腳，從智能合約設計者身上或合約本身的交易中，盜取以太幣。事實上，以太幣被「黑客」盜取也發生過幾宗。

從這個角度看，以太幣的資投風險較比特幣為高，因為上述這個原因，導致信心問題。當投資者信心受損時，以太幣無可避免受到拋售，價格遽跌。

認識區技術是推廣應用前提

可以說，區塊鏈技術和智能合約其實也不是什麼難以理解的東西，一般人覺得，即將來臨的區塊鏈技術應用，好像莫測高深。記得上世紀九十年代，當互聯網最初面世時，很多人既不懂其運作之所以然，也不通曉其應用，但如今連不懂得用電腦的人也可以輕易每日上網，甚至在網上進行交易，可以預期，區塊鏈技術的應用亦將日趨普遍，只要我們理解其技術概念和編程原理，理論上，每個人都可以透過學習編寫出智能合約。當然，筆者不能斷定區塊鏈技術的應用，會否比互聯網更廣泛，但當下一刻，要推廣區塊鏈技術在商業活動上的廣泛應用，必須讓公眾對此技術有所認識。

總括來說，區塊鏈技術以下的特性，包括所記錄的數字不可篡改、不可偽造，一切交易紀錄都具透明性和可追溯性，在此基礎上所形成的交易安全環境，便不需要有第三方監管，用戶都有信心進行交易或資產交換。區塊鏈技術的所有應用，都圍繞著這些特性而展開。當理解箇中技術含義後，你便可以決定是否置身其中，參與應用這些技術的種種商業活動。〔**區塊鏈技術與應用・二之二**〕

〔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〕