【解牛集】— 刊於〈信報〉，2018 年 3 月 27 日

區塊鏈發展機遇與局限性

黃昊
香港科大商學院會計學系副教授

近日，在招聘網站，招聘區塊鏈相關人才，付出職位年薪逾百萬年元的公司，為數不少。從事區塊鏈技術的上市公司，股價也飆升，彷彿一搭上區塊鏈技術發展的列車，就前途無量，為區塊鏈的發展前景，抹上一層神奇也充滿無限憧憬的面紗，公眾亦為之目眩。本文擬另闢蹊徑，分析區塊鏈技術，包括智能合約的局限性，其橫空面世，未必像有些人所說那麼具顛覆性和巨大的「革命性」。

區塊鏈本身，是一種「分散式帳本技術」 (distributed ledger) ，帳本不需要儲存在中央的資料庫，每一區塊都記錄前一區塊的證明號，形成鏈狀結構。在網絡上，每個參與者（節點）都擁有一個完整的交易賬本副本，並透過「哈希算法」（Hash），使已紀錄下來的交易數碼，難以篡改，不可偽造，具透明性和可追溯性，因而被視為為可取代需要中間人擔保和認証等商業交易，亦即交易雙方並不需要「信任」，透過區塊鏈平台也可進行交易。

智能合約應用受制約

看深一層，區塊鏈這個「去中心化」系統所作的交易或活動，其實目前的中心化系統也可以完成任務。譬如，當前大家正興致勃勃談論的以太坊（Ethereum）區塊鏈與智能合約（Smart Contract），其應用也有相當制約。

智能合約只是一種電腦編程，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平台，就像一個「可信任的隱形人」，擔起很多現時需要簽署合約時，需要第三方保証才能進行的商業交易活動。

用一個簡單例子來說明智能合約的本質。譬如一個售賣機，合約的條款很簡單，當消費者投入若干貨幣，這個機器便會自動彈出一罐飲料。引伸來看，把智能合約嵌入一個公有區塊鏈（public blockchain）內，好處是，合約條款可以自動執行，但弊處其實也有不少。

譬如，透過電腦編程式所預先編好的條件或條款，必須考慮到所有情況，把一切可能的事件後果清楚說明與界定。不過，據經濟學合約理論，由於人的理性有限，

對於未來發生什麼事難以完全預期。因此，普通合約的條文也無法涵蓋所有未來發生的事故，此為「不完全的合約」。

不完全合約弊端難克刻

既然合約不完全，簽署後，往往因變故而需要重新進行談判，但智能合約似乎難以妥善處置，因為智能合約是以電腦語言說明觸發 A 條件時，自動執行 R 結果；觸發 B 條件時，自動執行 S 結果，觸發 C 條件時，自動執行 Q 結果……，智能合約要涵蓋所有觸發條件和可能結果，編程員或智能合約的發起人，能夠不受人類有限理性的制約嗎？恐怕不能吧。

既然合約不完全，事發後，因變故而需採取有效處理的權力，該由誰來掌控？在現實世界，答案很簡單，權力歸該項資產的所有者，這種「剩餘的控制權」，即「剩餘權力」（residual powers）的有效配置，於 2016 年摘取諾貝爾經濟學獎桂冠的經濟學家哈特 (Oliver Hart)便強調，在擬訂契約條文時舉足輕重。

據此來看，如果在智能合約簽署後，出現不可預見的變故，重新談判的「剩餘權力」如何配置？又如何在區塊鏈平台上進行？

無法完全排除交易信任

另一方面，智能合約裡面，如果有一些結果判斷，需要從區塊鏈平台外取得資料或信息才能完成，譬如，某家跨國保險公司目前透過智能合約售賣航班延誤保險（flight delay insurance），合約條款規定，如果航班延誤了 2 小時，購買了該航班的乘客將獲得賠償，而賠償限制在從巴黎到美國的航線上實行。過去，乘客購買了航班延誤保險，航班延誤了，乘客需要提出賠償申請，可能還需要提供証明，如今賠償一定自動並且即時作出，對乘客當然是一個好消息。

但再想深一層，提供賠償服務，這家保險公司其實可以透過一個企業內部的中心系統來進行，毋預採用一個去中心化的區塊鏈平台來進行，為什麼要多此一舉呢？

當中，起碼有兩項信息和操作，是在這個智能合約區塊鏈平台以外發生的，即亦是需要從區塊鏈平台以外的資料庫攫取，第一，要取得該航班的起飛時間，這項須從外部資料庫（Oracle）取得的信息，合約雙方必須信任其為正確。第二，當這份智能合約在區塊鏈上，觸發了賠償條件而執行賠償，但賠償本身，也不是在區塊鏈平台上直接進行，而是區塊區平台把賠償的資料，傳給保險公司，再由保險公司把賠償金轉到乘客的帳戶裡。如果公司不作賠償，乘客也無法領取到賠償金。

因此，智能合約所標榜的毋須交易信任，觸發預定條件而自動執行所指結果的技術特色，到結果的最後執行，依然需要有信任成份。就像買了智能合約的航班延誤保險，蘊含了對保險公司（第三方）會作出賠償的信任。因此，智能合約毋須雙方信任，便可達成交易的「特色優點」，便須要從應用無限的憧憬中，打上折扣。

事實上，保險公司完全可以經由內部的中心系統，拿取相關資料，自行作出賠償服務，並不需要把智能合約投到區塊鏈平台上進行。

合約的簽定，立約雙方必須明白合約的條款內容，這是立約行為的基礎。筆者認為，智能合約並不能完全取代傳統的文書合約。舉例來說，銀行給你一份業務合約，你簽約前，可以細閱合約的條款，明白其內容和所指。假如以一份智能合約的形式立約，便要把內容轉換為電腦編程語言。如何確保在轉換過程中，機器語言百份百表達了合約的內容，而無一絲一毫扭曲、錯誤嗎？智能合約簽約的時候，要麼需要能讀懂機器語言，要麼需要相信機器語言完全表達了合約內容。無疑，這會增加交易成本，並需要一定的信任，有違智能合約不需要信任的宗旨。從交易與利益的角度看，成本高，也必然制約智能合約的應用普及化。

DAO 被盜事件啟示

傳統的立約行為，交易雙方可能需要找專業律師來進行內容解讀，而智能合約可能除了需要律師，還需要專業的編程人員，對條款是否精確反映立法條文的原意進行核校，立約成本可能反而更高。

在把合約內容轉換為電腦程式語言的過程中，如果過程中編寫出錯，或因無法涵蓋所有條件和結果，發生了一些逸出合約原意以外的事故，由於智能合約已嵌入到區塊鏈上，交易不能改動，結果也不能篡改，其後果也構成弊端。

記得 2016 年以太坊發生的 DAO 被盜事件。DAO 是去中心化自治組織，2016 年 4 月，「THE DAO」項目進行眾籌，不到一個月，累計籌集了超過價值 1.5 億美元的以太幣，所有籌得的以太幣都存在於同一位址平台。由於 DAO 使用了以太坊的智能合約，其運行規則在合約創建時已被固化，黑客透過智能合約電腦語言程式中的漏洞，成功「盜取」了 360 萬枚以太幣。

盜幣事件馬上引起起了激烈辯論，究竟是合約內容重要，還是程式碼（coding）重要？從上文的討論中看到，任何智能合約嵌入到區塊鏈上，在現實商業世界中的應用，都不能完全排除在交易中的信任成份。換言之，信任始終扣著交易在現

實上的最終實踐，故而智能合約的應用範疇，絕非無遠弗屆，其應用範疇有不少局限性。

實事求是看待區塊鏈技術

譬如，土地的權益人，把一份出售土地的智能合約嵌入區塊鏈平台上，關鍵之處，並不在於合約本身，而在於確認這塊土地的產權所有者，正是在區塊鏈平台上擬出售土地的人，亦即需要在區塊鏈以外進行信息互動，跟區塊鏈以外的人、事或物打交道，結果也要對第三方作出信任，否則交易無法最終完成。即使在區塊鏈上完成買賣交易，除非政府承認這區塊鏈所做的交易，否則，在現實世界中的土地業權轉換登記，如何取得合法的地位？一旦土地業權出現糾紛，法律的最終裁決由誰來裁定？如何終止透過智能合約進行帶有欺騙性的非法交易？由於區塊鏈是一種「分散式帳本技術」，並且有無數分散的節點（node）在操作，如何終止區塊鏈平台上的交易？連串的問題，智能合約要進一步發展是無法迴避的。

區塊鏈技術具有創新性、有用，像九十年代的互聯網，大家覺得具發展前景和空間。事實上，最近幾年，除了「首次公開代幣發售」（ICO ・Initial Coin Offering）以外，在其他範圍，似乎並未看到有具體的創新性應用。無可否認，區塊鏈技術當下仍處於摸索性發展初階，如果我們實事求是，認識區塊鏈應用技術的局限性，從其有局限性的分析基礎上，老老實實地探索其應用，而非對它作出過度虛幻的憧憬，反而對區塊鏈的健康發展更有幫助。

〔本文由科大商學院傳訊部筆錄，黃昊教授口述及整理定稿〕