智能合約的發展與應用

陳　恭／政治大學資訊科學系教授

一、前言

智能合約 (Smart Contract) 一詞是由學者尼克 · 薩博 (Nick Szabo) 於 1990 年代初期提出，倡議可以將交易的條款透過電腦化來落實；但是，當時並沒有得到太多的回響，接下來自然也沒有獲得太多的發展。

直到這幾年，智能合約才隨著區塊鏈 (Blockchain) 技術的興起，逐漸在金融業中流傳開來。2015 年中推出的區塊鏈平台－以太坊 (Ethereum)，其白皮書名為「新一代智能合約與分散式應用平台」(A Next-Generation Smart Contract and Decentralized Application Platform)，強調智能合約為其平台特色，一舉將智能合約這個名詞推到一個新的層次，讓大家開始注意到智能合約的重要性，甚至視其為「區塊鏈 2.0」的主要技術與應用。簡言之，區塊鏈平台提供多方可信任的網路共享資料庫，智能合約使用這些共享資料，執行應用程式，進行交易與資產移轉。本文依此脈絡，就智能合約的發展與應用作概括性的介紹，並說明其所面臨的議題與挑戰。

二、智能合約的沿革

本章節就智能合約的概念緣由與演進概要說明，並就現今智能合約的運作方式加以解說。

(一) 智能合約的緣起

當年尼克 · 薩博提出智能合約這個概念時，還沒有相對應的平台可以落實他的想法，所以為了具體闡釋智能合約的內涵，他舉了自動販賣機當作例子來說明。我們可以設想一部自動販賣機裡的電腦軟硬體是按著以下的規則來運作：

如果使用者輸入 10 元且按 A 按鈕，機器就輸出巧克力棒；

如果使用者輸入 10 元且按 B 按鈕，機器就輸出乖乖包；

如果使用者輸入 20 元且按 C 按鈕，機器就輸出咖啡；

…。

意思是說，自動販賣機在跟它的使用者進行交易時，所依循的「條款與條件」(terms and conditions) 就是智能合約的體現，而且是透過電腦軟硬體自動化執行，毋須藉由第三者的協助。

但自動販賣機畢竟只是一個個案，尼克 · 薩博設想的應該是一個平台，能讓交易的兩造，透過通用的軟體工具，將彼此的交易條款與條件，表達成自動執行的程式碼，並稱這些程式碼為「智能合約」。這裡的重點是軟體的特性－可程式化 (programmable)，透過智能合約將兩造之間的資產移轉，變成可程式化的，只要透

圖 1　比特幣區塊鏈特性

過電腦程式的邏輯變化，就可以實現各種的交易條款與條件。這種想法深具應用潛力，但那時候技術還不夠成熟，也沒有適當的平台，所以智能合約就僅能停留在概念的層次。

（二）區塊鏈與智能合約

現今我們談論的智能合約跟區塊鏈是息息相關的，簡單說，智能合約就是在區塊鏈平台上執行的應用程式，所以要談智能合約，還是要先從區塊鏈的特色說起。

區塊鏈是源自比特幣 (Bitcoin) 的底層技術，比特幣是近來最受矚目的網路世界虛擬貨幣，它的重大突破，在於可以不透過銀行或其他受信賴的中介機構，就可讓網路上的每一個用戶，直接將其帳戶內的比特幣，匯入另一個用戶的帳戶中。這種作法完全有別於當前的金融支付的運作模式，開啟了一種「點對點」(peer-to-peer)、直接進行資產移轉的可能性。區塊鏈就是這裡的幕後功臣，提供點對點支付比特幣的功能。

區塊鏈這個名詞聽起來很技術性，但功能上它就是比特幣的帳本，記錄在網路上發生過的每一筆比特幣交易，可視為一種功能單純的資料庫；不過，這個資料庫是透過網路運行的，每個在比特幣網路上的節點 (Node) 都有一本帳本，而且大家的帳本內容都一樣。正因為這帳本分布在每個節點，內容又都一樣，所以區塊鏈也可稱為「分散式共享帳本」(distributed shared ledger)。在運作上，每當有一筆比特幣交易時，只要由某一個網路節點，透過一個共識過程[1]，將這筆交易記錄到它的帳本後，就會自動複寫到所有節點的帳本內，確保大家的帳本是一致的。不僅如此，區塊鏈的技術內涵並確保這帳本的內容只能新增，不能修改[2]；所以區塊鏈網路中的各個節點，可以信任自己的帳本跟交易對手的是一致的，而不必依賴中間的信賴機構來替雙方對帳 (account reconciliation)。比特幣區塊鏈特性如圖 1 所示。

1　以比特幣為例，這個共識過程包含了所謂的「工作量證明 (Proof of Work, POW)」，簡稱為挖礦的程序。

2　嚴格說，應該是修改的代價非常高，幾乎不可能。

近 3 年來，區塊鏈技術已經有了許多快速蓬勃的發展，漸漸成為一個新的網路平台技術，我們可以在上面發展各式各樣的區塊鏈應用程式，像比特幣這類的虛擬貨幣，也只是區塊鏈平台上的一種特定應用。也就是說，新一代的區塊鏈 (如：以太坊、Hyperledger 與 R3 Corda) 除了資料庫的功能外，也可執行應用程式；帳本內儲存的不只是資產的交易紀錄，也包含應用程式要處理的資料；這些應用程式的邏輯就是在處理有條件、且比較複雜的資產移轉，為的是實現交易合約的條款與條件，因此這類程式就被稱為「智能合約」。

但這樣的智能合約，其實已經超越了尼克 · 薩博當年所倡議的智能合約，它不僅僅只是紙本合約的電子化或程式化，重點在於與區塊鏈技術的結合，得以在一個受信任的平台上執行。因為傳統合約的電子化，可能還是依照一個強大中心的模式來執行合約邏輯，像是亞馬遜電子商務平台，它所執行的許多程式也像是在實現合約的條款與條件，只是這些程式都只有一份，而且是在亞馬遜的中心伺服器上執行。但現今的智能合約是部署在區塊鏈平台上，會自動複製到網路中的每個節點，且在每個節點上執行。區塊鏈的技術，確保各節點執行相同的程式邏輯，產出一致的帳本異動；進而在交易的兩造間建立信任，有效支援它們直接交易，毋須中間機構來替他們對帳。

例如，供應鏈的上下游廠商，對於供貨量多寡所對應的折扣數，可能都訂有合約，以特定的條款來規範；但多半各自還是會自行記帳，使用各自的應用程式來管理進出貨。如果採用了區塊鏈與智能合約來管理雙方的交易帳務，雙方不僅會有一致的帳本，用來異動帳本內容的應用程式，也可透過智能合約的機制而一致化，這樣就不必雙方都有自己的系統、自己的帳，因而可以省去許多人工或程式對帳的成本。

(三) 智能合約的運作

智能合約是以應用程式的邏輯，來實現交易合約中的條款與條件；因此，不同的區塊鏈平台所提供的智能合約，多少會有些差異。但一般說來，智能合約的運作，多半是以「事件驅動」的方式進行；智能合約程式一旦部署到區塊鏈平台上後，當合約所設定的事件發生時，一些條件就會成立而觸發合約的指定功能，開始執行程式；執行的結果，通常就會引發資產的移轉。以線上購買數位音樂為例，我們可以開發一個交易用的智能合約，裡面明定好每首數位音樂的分潤方式，依作曲者、作詞者、製作者與線上購物平台訂好分潤比例；一旦消費者於線上完成支付手續後，就觸發了轉帳功能，將費用依比例自動分配到相關人士的帳戶內。

上述例子的事件，是交易合約本身主動來觸發智能合約的轉帳功能，屬於區塊鏈內部的事件；但很多智能合約所仰賴的事件或條件是外部的，其資訊是由區塊鏈外部的系統所管理，智能合約必須去跟這些外部系統要求相關資訊。例如，很多農作物可能因為天氣的大幅變化而招致大量的損失，我們可以替這樣的農損，開發一個保險的智能合約，規範在特定的氣候狀況下，農民可以獲得相對應的賠償金。這裡觸發理賠交易的條件，必須仰賴中央氣象局的天氣紀錄，這時智能合約就必須定期去跟氣象局的系統索取氣象資料。我們稱這種具權威性的外部資料源為「神諭」(Oracle)，安全又有效取得外部 Oracle 資料，是很多智能合約運行的一個重要依據。

圖 2　智能合約的應用

三、智能合約的應用

區塊鏈與智能合約的應用範圍相當廣 (如圖 2)，各行各業都有可能。它既可以用來改善既有的業務流程，包含減少人為錯誤、降低成本與提高客戶滿意度；也可以用來支援發展新的業務模式，或開發新的市場。但區塊鏈與智能合約也不是無所不能，以區塊鏈的帳本資料庫而言，它的功能有限，沒有方便的查詢工具，效能也不特別好；它的強項是「自動複寫」與「防竄改」，所以區塊鏈的適用場景，應該是有「資訊共享」需求，又「不完全互信」的多方互動環境下，才得以彰顯它能促成信任、免除中間人的優勢，以下將分別舉例說明。

(一) 優化現行業務流程

首先，我們以保險理賠自動化為例，這是一個既有的業務流程，我們可以運用區塊鏈與智能合約來實現並優化這個流程。作法不外乎將理賠的申請文件經過適當的處理後 [3]，儲存於區塊鏈資料庫內；接著將理賠審查的邏輯實現於智能合約內，收件後自動進行批審。這樣得以提升整個流程與理賠規則的透明度，增加保戶對保險公司的信任感；此外，也可提升流程效率與客戶滿意度。

(二) 發展新型 P2P 業務模式

進一步來探討保險與保險理賠這個主題，我們不難發現中國大陸目前興起的「網路互保」的新型業務模式，也是一個非常適用區塊鏈與智能合約的應用場景。這裡甚至不必然有保險公司的角色，只需由網路互保平台提供適當的智能合約，並將運作規則透明化，再搭配特約銀行的金流服務，就可以讓有意投保、或投資的人來參與運作；參與者彼此之間未必互相信任，但透過區塊鏈與智能合約提供的技術

3　文件內容過大時，可以用雜湊值 (Hash Value) 儲存於區塊鏈，若有隱私顧慮，則需加密處理。

性信任機制，大家皆得以放心地參與，無須藉由保險公司或其他中間人之手。其實這就是一種毋須中間人的同儕商業模式 (Peer-to-Peer，P2P) [4]，不只保險，還有許多類似的範例，像是衍生性金融商品交易、P2P 借貸、群眾募資與 P2P 租用服務等都適用。

（三）物聯網的應用

近來「物聯網」(Internet of Things，IoT) 的技術逐漸成熟中，我們離 Device-to-Device(D2D) 的時代已經不遠，很多 D2D 的應用場景，也是區塊鏈智能合約可以發揮的地方。以電動車與充電器為例，我們可以讓這兩種設備都有自己的區塊鏈帳戶，它們之間的互動，就可以透過智能合約來居中處理，依充電量的多寡來計算費用，並觸發金流，由電動車的帳戶支付給充電器的帳戶，自動完成。在能源管理方面，當個別住戶的太陽能面板要將儲存的電，賣回給電廠時，也可以用 D2D 的智能合約來加以處理。所以，不管是 P2P 或是 D2D，智能合約都有很大的發揮空間。

四、智能合約的議題與挑戰

不管是區塊鏈或智能合約，都還是發展中的新興技術，一定有許多議題與挑戰有待克服，才能真正落地應用；以下我們分別就技術面與法律面，簡要探討智能合約可能面對的議題與挑戰。

（一）技術面

從技術的角度，智能合約其實就是部署於區塊鏈平台上的軟體程式，所以一般軟體工程所關心的議題，智能合約也一樣適用。例如：當需求規格不夠嚴謹時，常造成開發人員誤解需求，而導致程式的執行結果與用戶的預期不符。就智能合約而言，因涉及資產的移轉，甚為敏感，其規格之制定必須更為嚴謹，以確保紙本合約的條款與條件，能如實地實踐於智能合約之中。就如同我們簽約前，會找律師過目合約條款是否恰當，未來，則可能需要具備智能合約專業素養的律師，才能協助擬訂合約規格、以及審查智能合約。短期而言，從定型化契約著手來開發智能合約，應該比較可行；如英國巴克萊銀行曾進行了一項金融衍生性商品的智能合約實驗專案，他們就是以「國際交換交易暨衍生性商品協會」(International Swaps and Derivatives Association，ISDA) 所制定的定型化契約作為基礎。

其次，有了嚴謹明確的規格後，我們如何確保開發出來的智能合約，確實符合規格？亦即，如何以嚴格的程式證明程序來驗證智能合約的正確性？雖然短期還無法有嚴格的「正確性」證明工具，但至少我們可以開發對智能合約進行功能測試的有效工具。然而即便有了功能正確的智能合約，我們尚須關切它們是否有安全上的漏洞？是否會遭到攻擊而導致資產損失？例如去年 (2016) 年中發生的 The DAO 事件，就是一個代表性的案例。在這個案例中，用來控制 The DAO 這家虛擬公司的智能合約程式有瑕疵，導致駭客得以運用正常的程序，將公司的大筆資金移轉到指定的帳戶。所以我們需要發展智能合約的安全檢測工具，以及沙箱環境，以利進行隔離執行，確保其安全性；在以上這些工具都還未成熟時，我們可以透過一般軟體品質提升的方法與工具，以確保智能合約的安全，例如：安全指引、程式化測試與

4 這裡的 P 可以是個人，也可以是公司或組織。

程式碼審查等。

撇開以上的軟體工程面向的議題與挑戰，回歸智能合約的本質，我們若真要以智能合約處理現實世界的需求時，仍然要面對虛實之間的整合問題。簡言之，在受信任的區塊鏈平台實行可程式化的資產移轉，是智能合約的主要特色，但這裡的資產是無形的數位資產，如果要連結到鏈外的實體資產的移轉，智能合約就需要跟鏈外的系統整合，一起連帶運作才能完成；這其實是目前實務上要優先處理的一項重要議題。也就是說，現行區塊鏈智能合約的應用系統，尚無法單單依賴智能合約來運作，仍須搭配既有的系統，統整後才能處理實體資產的移轉。

（二）法律面

技術之外，智能合約在法律方面也有許多的議題與挑戰。以上面提到的 The DAO 事件為例，駭客因發現了該合約程式的漏洞，而得以非預期的方式將大筆資產移轉走，這樣的行為有無違法？若有，要在哪個司法管轄權，依怎樣的法律條款來起訴？抑或是駭客只是比較瞭解這個合約的特色，依約行事，毫無法律責任？這些都是有待釐清的重要議題。此外，當智能合約運行時，若造成他人損失，當事人可以對誰問責？開發智能合約的程式人員是否要負連帶責任？還是只有智能合約的所有人要負責？

雖然智能合約以程式碼實現合約的條款與條件，比起以自然語言撰寫的傳統合約，具備有可預測性和清晰度的當然優勢，但在可預見的未來，智能合約不會完全取代以自然語言制定的法律合約，因為還是有很多類型的合約不能完全用程式碼表述或用電腦執行；即便是可完全自動執行的合約，一旦合約雙方遇到訴訟情況時，也還是需要參考法律條文和定義合約雙方權利的概念，才能依約處理。因此，智能合約的出現，雖然會引發我們重新評估目前的法律合約，但仍然需要透過持續地嘗試、辯論與調整，我們才會界定出那些是適合以程式碼實現的合約類型和條款，而哪些合約還是比較適用自然語言，以及怎樣將兩者結合以達到最好的效果；也只有這樣的社會化過程，才能逐漸取得大家的共識，讓智能合約取得合宜的法律位階，落地實現。

五、結語

經濟學人雜誌將區塊鏈類比成「製造信任的機器」，的確是一個蠻適當的比喻。人與科技之間的信任是一個有趣的課題，隨著科技的進步，人類的生活本日益離不開科技，但我們在享受科技帶來的便利時，卻也會不時煩惱科技對我們生活造成的衝擊、以及對隱私的侵犯；我們在信任科技之餘，也常持戒慎恐懼之心。

回想二十多年前，網際網路興起，電子商務開始發展，很多專家預測電子商務的便利性，將對商業價值鏈帶來很大的改變與重整，會有「去中間人」(disintermediation) 的效應，也會對實體商店造成莫大的影響；但同時，也有許多人對網路購物抱持著非常保留的態度，擔憂個人資料遭到盜取濫用，造成財物損失等等問題。現在看來，電子商務非常的發達，深入我們的生活之中，不過中間人與實體商店依然存在，個人隱私的問題也日益嚴重。這或許可以給我們在面對今日區塊鏈智能合約技術，如此快速發展的情況下，提供重要的參考與借鏡；就如同網際網路一般，這種新興技術也是屬於基礎建設型，不論行業，對我們在資料的管理與資產的交易上，皆可能帶來極大改變！

雖然目前還不成熟，但愈早去探索與理解，愈能讓我們掌握並產生信任，進而善加運用，創造價值。

※ 參考文獻 / 資料來源：

1. https://github.com/ethereum/wiki/wiki/White-Paper。
2. BlockCharge – EV Charging via the Ethereum BlockChain(HQ)： http://ecosocial.me/love/elektromobil/blockcharge-ev-charging-via-the-ethereum-blockchain-hq/。
3. Pete Rizzo(2016)，How Barclays Used R3's Tech to Build a Smart Contracts Prototype, http://www.coindesk.com/barclays-smart-contracts-templates-demo-r3-corda/。
4. Michael del Castillo(2016)，The DAO Attacked: Code Issue Leads to $60 Million Ether Theft, http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/。
5. http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-work。