如何建置一個實用的區塊鏈平台

杜宏毅／臺灣網路認證股份有限公司策略長

一、前言

「臺灣的金融服務應用，如果想要導入區塊鏈機制，要如何建置一個實用的區塊鏈平台？」在過去半年多來，每次演講都會被問到這樣的問題；雖然有些想法，但始終不敢貿然回答這類的問題。一直到最近，手邊三個概念驗證 (Proof of Concept，POC) 的案子已進行到後期，稍有初步的成果，才有機會整理出一些經驗與想法，野人獻曝地在此與大家分享。

接下來，我們將依據過去半年在導入區塊鏈機制於 POC 應用所累積的經驗，嘗試藉由回答以下問題，與大家一同探討，如何才能建置一個實用的區塊鏈平台：

(一) 導入區塊鏈機制是要去中心化嗎？

(二) 金融服務應用有其特性與生態，要如何調整原生型區塊鏈的機制，才能適用於國內的金融服務應用？

(三) 在導入區塊鏈的應用實作上，如何規劃整個區塊鏈平台的系統連結及分布架構？

圖 1　各銀行是以分散式的模式各自提供客戶服務

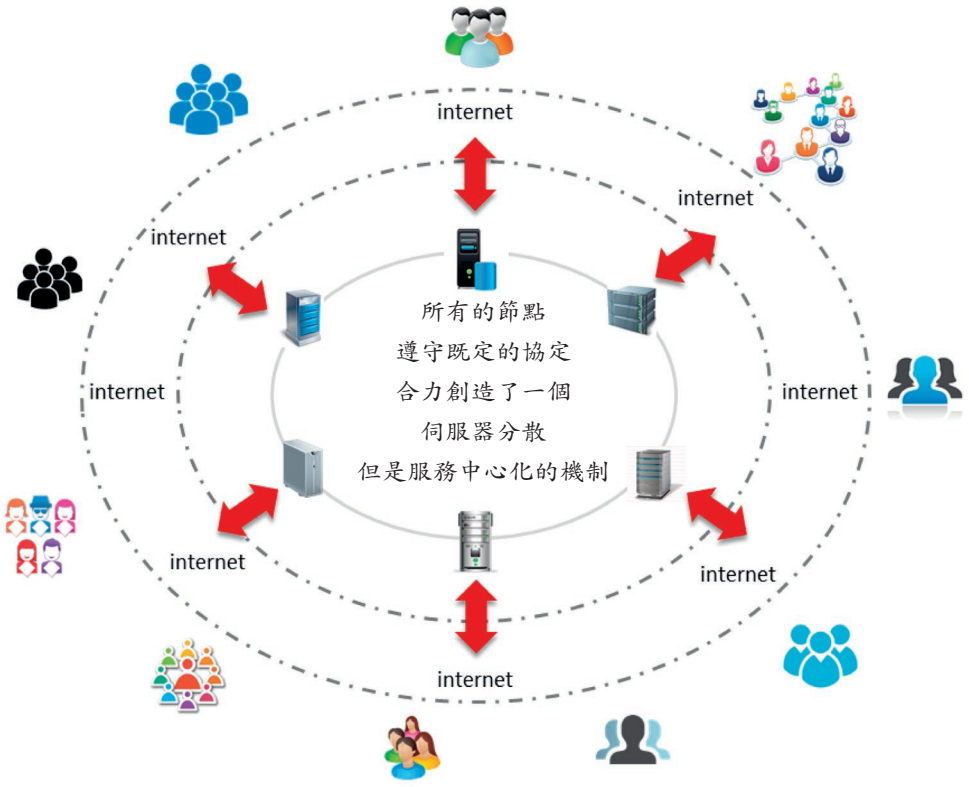

圖 2　Bitcoin 是一間「中央化到極致」的超級銀行

二、中心化 vs. 去中心化

談到區塊鏈，「去中心化」(Decentralization) 總是第一個被聯想到的名詞。大家都以為，區塊鏈的機制是為了去中心化而設計的。其實恰好相反！區塊鏈可說是一個最大的「中心化」(Centralization) 機制！這話怎麼說呢？如果我們回頭探究起源於「比特幣」(Bitcoin) 這類原生型區塊鏈的運作機制，就會明白其中的道理。

平常你我在銀行開設的帳戶，大都是以銀行做歸類，例如，我在兆豐銀行有個帳戶，你在國泰世華銀行有個帳戶，這些帳戶的管理權限，都個別分屬於各個銀行。所以，所有客戶的帳戶，是以「分散式」的模式歸屬於各個銀行的名下，而並不是以一種「中心化」的方式在服務客戶 (如圖 1)。這也就是為什麼帳戶與帳戶之間彼此在進行交易 (如轉帳) 的時候，我們需要一個可以連結所有銀行的「中心」(Center)，提供彼此之間資訊轉遞的功能。

現在回過頭來看看 Bitcoin 的運作機制，到底與一般的銀行帳戶有何區別？大家不妨仔細想想，你我的帳號，在 Bitcoin 的生態系中，是個甚麼樣的概念？不就是「大家都在 Bitcoin 系統中有個帳號」嗎？其實，關鍵就在這個「大家都在 Bitcoin 系統中」！「大家都在」的意思就是「Bitcoin 中央化 (Centralized) 了所有使用者的帳號」(如圖 2) ！

如果以銀行體系做比擬，Bitcoin 本身就是一家最大的銀行，而且是一家「跨國境」的超級銀行。Bitcoin 生態系中「自願」(應該說是被 Bitcoin 的金礦所吸引) 替大家服務的各個「節點」(Node)，其所維護的「帳簿」

(Ledger)，其實就是一個「登載記錄全生態系流水帳的大帳簿」。

基於不同理念所發展出來的系統，當然就會產生不同的運作邏輯。比如說，在現今的銀行體制下，如果要從 A 銀行的某個帳戶，透過 ATM 機制，轉一筆錢到 B 銀行的某個帳戶，整個作業流程至少需要：A 銀行、B 銀行、以及 ATM 作業處理中心三個單位的配合，才能成事；三者分別都要在自己的帳務系統中記錄這筆交易後，整個交易才算完成。但是，Bitcoin 機制根本不是以這樣的概念在運作，整個機制的運作邏輯，基本上就是個「記錄流水帳」的概念。你可以想像一下，如果有一個全世界的人都能夠即時看得到的超大電視牆，牆上永遠都顯示著一本大帳簿，而每一筆 Bitcoin 交易，都會透過系統、即時的記錄並且顯示在這個電視牆上；請問，我們還需要 ATM 轉帳作業中心嗎？其實，如果我們將 Bitcoin 機制視為一間超級銀行，帳號與帳號間的交易，就會簡化成是一種「自行 (ㄏㄤˊ) 交易」。簡而言之，整個作業也不過就是在自家的電腦上，記錄一筆流水帳罷了！

如果我們從「Bitcoin 就是一間超級銀行」的概念出發，去看一些平常報章雜誌的報導、或專家學者的專欄論述，就很容易瞭解他們在說些甚麼、或是說他們到底有沒有弄懂自己在說些甚麼？

比如說：大家常談到，區塊鏈在跨境支付的作業上，可以如何又如何的有效率！
我的回答是：那當然，大家都在同一本帳簿上記帳，那還不容易！還會沒效率！

所以，對一個以「提供中心化服務」的營運單位而言，與其將區塊鏈機制的導入，想像成會導致去中心化的結果，倒不如嘗試著反向思考；想想看，如何藉由區塊鏈技術的導入，創造出一種「進化版的中心化機制」，將所有參與者帶入一個新的合作架構中，藉由「新的科技機制」誘發「人性協同合作的善良面」，共同創建一個共利的生態系。

三、烏托邦 vs. 真實世界

在 Bitcoin 這類原生型區塊鏈生態系中，「參與者」大致上可以分為兩個族群：一種是「終端使用者」(End-user)，例如：持有 Bitcoin 錢包的使用者；另一種是提供服務的「節點」(Node)，負責製作區塊、傳遞區塊、以及維護區塊鏈等工作。原生型區塊鏈生態系在設計上有一個基本假設，就是－「參與者彼此之間的相互信賴度很低」。

任何想站出來服務大眾的人，其實「不需要獲得任何人的允許」，都可以自己準備一台伺服器、下載軟體安裝、經過適當的設定，成為一個「節點」。這些「節點」彼此間並沒有任何的關連性或是信賴關係，只要大家能遵守既定的協定，雖然這些伺服器是「分散在各地」，也可以合力組成一個「中心化」的服務機制。任何一個終端使用者，(在理想上) 都可以透過網路，連結到任何一個節點，獲得 (或是請求) 服務。

這種型態的區塊鏈生態系，其優點就是「各盡所能、各取所需」，大家相信，所有參與者都能藉由區塊鏈的機制，彼此制約，建立一個具公信力的生態系，建立一個「烏托邦」的世界。

但是，大家其實都知道，人有「善」、「惡」兩個面向，為了防範人的「惡」會蓋過「善」(如不遵守公約、擅改或是偽造各項交易紀錄、或是不依照協定維護區塊鏈等)；因

此，區塊鏈機制的發明者與信徒們，就企圖利用各式各樣的科技，設計一些複雜的機制 (如雜湊函數運算、公私鑰的加解密演算法等)，期待能「藉由科技」來「解決法律、政治、管理上所產生的議題」。這些「科技」包含三種核心技術，分別是：

(一) 以「公、私鑰對」(Public & Private Key-pair) 為基礎的「加解密、簽驗章」(Encryption /Decryption、Sign/Validating) 技術。

(二)「雜湊函數」(Hashing Function) 運算。

(三) 以「共識決演算法」(Consensus Algorithm) 為基礎的資料同步機制。

第 (一) 項技術的設計，是為了建立一個「可驗證的匿名制」，以支持「動用帳戶資產時」的「確認機制」，意即以私鑰簽署交易、以公鑰驗證簽署交易的合法性。

採用第 (二) 項技術的用意，則是為了「確保每項交易資料，一旦被包覆進入區塊鏈，都將無法 (或是非常困難) 被更改」。

至於導入第 (三) 項技術的目的，則是希望藉由「共識決演算法」，將系統所產生的區塊，即時布建於每一個參與節點的區塊鏈中，以達資訊即時同步的目的。

因為國內金融服務應用的場景、特性、生態，與當時原生型區塊鏈創立時的假設有所不同，所以，上述三項技術的使用方式，必須進行適當的調整，方能符合需求 (如表 1)，以下分別就「節點的設置標準」、「公私鑰簽驗章機制」及「共識決演算法」，概要說明。

表 1　原生型區塊鏈與金融服務應用型區塊鏈之差異比較表

類型	原生型	金融服務應用型
節點的設置標準	非認許制 (non-permissioned)	認許制 (permissioned)
公私鑰簽驗章機制	與使用者資訊無關聯的匿名制	採用電子憑證式的實名制
共識決演算法	條件式雜湊函數配搭 工作量證明演算法 (POW)	投票民主制演算法 Paxos Algorithm(或是拜占庭式演算法)

(一) 節點的設置標準

「任何想替大家服務的人，不需要獲得任何人的允許，都可以自己準備一台伺服器、下載軟體安裝、經過適當的設定，成為一個節點。」這是一種理想，但是在實際運作上卻很難做到。

因此，「非認許制」(non-permissioned) 的區塊鏈生態系，在金融服務應用的領域中，幾乎是無法被接受的。相對地，任何一項金融服務的應用，在導入區塊鏈機制時，都必須審慎考慮採取「認許制」(permissioned) 的必要性；儘可能事先釐清各個節點所需負擔的責任，訂定意外事故發生時的作業準則，以便將損失降到最低。

(二) 公私鑰簽驗章機制

在原生型區塊鏈生態系中，帳號 (公鑰) 與個人資訊 (如個人姓名或是個人 ID Number) 之間，並沒有建立任何直接關連，

因此，針對每筆「動用資產」的行為，藉由區塊鏈系統，只能追溯到連結於該帳戶的「公私鑰」，而無法追查到公私鑰背後使用者的相關資訊。所以，這種身分識別機制，通稱為「可驗證 (公私鑰) 的匿名制」。

為什麼原生型區塊鏈會採取這樣的機制呢？道理其實很簡單，就是為了「簡單與方便」使用；試想，連提供整個生態系服務的「節點」都是採「自願制」，至於「終端使用者」的「帳號」，還需要有甚麼特殊機制的管理嗎？既然是「烏托邦」，完全的「自治與自制」就應該是建置這類原生型區塊鏈生態系的最高指導原則。

但是，基於「反洗錢」(Anti-money Laundering，AML) 的基本要求，金融機構大都無法接受這種「可驗證」的「匿名制」。然而，「可驗證」的「實名制」，其實就是金融界使用多年的「電子憑證」機制；所以，依 POC 的實作經驗，以區塊鏈平台介接目前所使用的電子憑證機制，提供服務，較為可行。

(三) 共識決演算法

「共識決演算法」的種類繁多，各有其應用的屬性。例如： Hyperledger 平台一開始是使用「拜占庭演算法」，Bitcoin 則是採用「工作量證明」(Proof of Work，POW) 演算法；也有其他生態系是用「驗證其他重要的因子」的演算法，作為資訊同步的機制。當然，每一種演算法都有其被採用的理由與依據，例如：Bitcoin 之所以採用 POW，是因為整個生態系是建立在一個「節點與節點之間毫無信任關係」的假設上；當初的設計者希望藉由 POW 演算法所製造的相互競爭機制，創造出優勝劣敗的生存與獎賞法則 (最終獲勝而得以建立區塊的節點，可得到特定數額的 Bitcoin)，讓所謂「自願擔任節點」的人，願意賣命替大家建立區塊、維護區塊鏈資料的一致性，促使整個生態系的運作得以生生不息。

但是，當應用範疇設定在現今的金融服務領域時，「毫無信任關係」的假設並不存在，所有參與生態系的成員 (或是節點)，應該都是以「認許制」的方式加入這個生態系；也因此，這個生態系中並沒有「必須採用 POW 競爭法則，作為產生區塊以及資料同步」的理由。相對地，我們可以採用一個比較簡單，但是適合於「認許制區塊鏈生態系」的演算法 (文獻上稱之為 Paxos 演算法)，其步驟如下：

步驟一：選出應該製作區塊的節點

節點之間，以每人一票的投票方式，選出製作區塊的節點。獲得超過 1/2 選票支持的節點，就被大家委任為製作區塊的節點。

步驟二：製作區塊

選出節點後，所有的節點，都將手邊的「交易」，傳遞給這個節點。這個節點在收到足夠的交易後，就開始製作區塊。

步驟三：傳遞區塊於各節點

區塊製作完成後，被委任製作區塊的節點，即開始傳遞這個新產生的區塊給所有其他的節點，進行區塊鏈的資訊同步作業。

為什麼不考慮採用 Bitcoin、Ethereum 或是其他區塊鏈平台所使用的 POW 演算法呢？因為 POW 演算法在先天上有其缺陷。

簡單歸納，POW 演算法的做法，就是「挖掘區塊不設限」。事先放任所有節點都可以挖掘區塊、製造區塊，到時候如果發現有兩個區塊同時出現，則藉由「比較兩個區塊被挖

掘時的困難度」，決定區塊的去留；困難度高的留下，困難度低的捨棄。當然，也因此，某些之前被包覆在區塊中的交易，就有可能被釋放出來 (意即原先被認為「確認」的交易，現在有可能被還原成「未被確認」的狀態)；須等待下一回合，看看是否有機會，被其他節點包覆在新產生的區塊中。這樣的做法，將會導致「交易清算的不確定性」(Uncertainty of Settlement Finality) 的現象，亦即「某筆交易的清算，需要多少時間或是收到多少節點的確認，才可以被確定？」這在烏托邦式的 Bitcoin 生態系中，可能可以被接受；但是在事事講求「確定性」的金融服務應用中，應該無法被容忍。

相對地，經由 POC 的經驗累積，讓我們選用了 Paxos 演算法，藉由節點間協議的方式 (投票)、製作區塊、傳遞區塊、達成節點間資料同步的目的；這種做法，不會產生 POW 演算法所造成的「最終清算」(Settlement Finality) 問題，擴展性 (Scalability) 的限制也相對地降低許多。因此，建議往後在選用區塊鏈平台時，採用的「共識決演算法」是否適用於該項應用？會不會產生上述兩項副作用？都必須列為審慎考量的課題。

四、區塊鏈平台架構概述

區塊鏈平台的系統架構為何？使用者如何使用？又該如何與既有的系統介接？依據我們在導入區塊鏈機制的 POC 經驗，整個平台架構的系統連結及分布，大致如圖 3 所示，由「區塊鏈系統」(Blockchain System)、「區塊鏈應用系統」(Blockchain AP System)」以及「應用系統連結閘道」(AP Gateway) 三個主要部分相互支援組成。

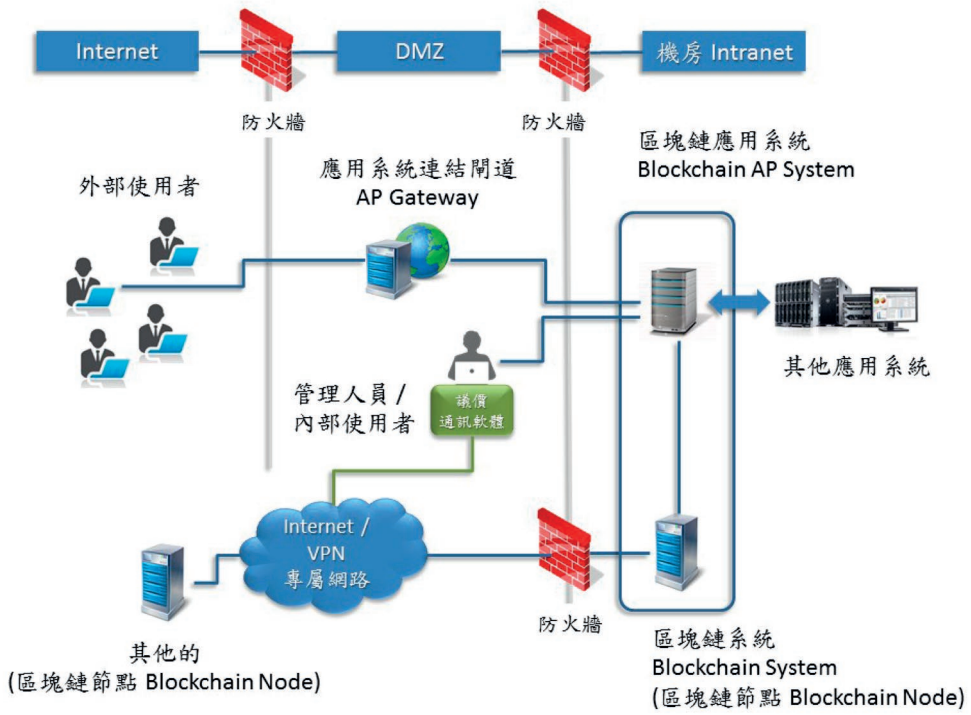

圖 3　區塊鏈平台架構中之系統連結及分布圖

(一) 區塊鏈系統(Blockchain System)

「區塊鏈系統」為區塊鏈機制運作的主系統，負責「區塊 (Block)」的組建、遞送、以及鏈結等工作。該系統採用「共識決演算法」(Consensus Algorithm)，將製作好的區塊，透過 VPN 或是 Internet，遞送到所有參加單位的區塊鏈系統中，以確保資訊即時同步。

這一套「區塊鏈系統」，在區塊鏈平台中，應該是屬於「中性」的系統，無論導入哪一項應用，其功能應該都大同小異，並不會依應用之不同而有所改變；從實用的角度看，只要沒有效能或是安控上的特別需求，不同的應用都可以架構在同一套的「區塊鏈系統」之上。

(二) 區塊鏈應用系統(Blockchain AP System)

「區塊鏈應用系統」(以下稱應用系統) 在區塊鏈平台架構中係負責處理與業務邏輯、作業流程相關的事務。因應不同的應用，在導入區塊鏈機制時，會設計建置不同的應用系統；但是，理論上，一個區塊鏈的「應用生態系」中，所有參加單位 (或稱之為節點、端點) 的應用系統，應該都相同。例如：如果我們將區塊鏈機制導入「未上市股權交易」的應用時，此處所指的應用系統就是「未上市股權交易系統」，所有參加未上市股權交易的單位，除了必須安裝一套「區塊鏈系統」外，都會配置一套與其他節點同樣的應用系統，亦即「未上市股權交易系統」。

同樣地，如果是將區塊鏈機制應用於金融同業拆款作業，那這裡所指的「區塊鏈應用系統」就是「金融同業拆款作業系統」，每個參加同業拆款作業的單位，都應該配備一套同樣的「金融同業拆款作業系統」；至於如何將這套應用系統介接於單位內部的其他系統，則屬於客製化的部分，不包括於此共通的應用系統範圍之內。

(三) 應用系統連結閘道(AP Gateway)

「區塊鏈應用系統」與「區塊鏈系統」的連結，則是透過「區塊鏈系統」所提供的 API，將各項訊息遞送至各節點 (即各參加單位)。例如：將「交易的內容」或「智慧型合約」傳送至「製作區塊的節點」這類的工作，就是透過這個管道遞送出去。

除此之外，內部使用者 (例如該項業務的負責人員) 或是系統管理者，則以「登入系統」的方式，上線使用；如需要開放外部的使用者使用，為了安控作業的考量，建議必須透過「應用系統連結閘道」，才能連結使用「區塊鏈應用系統」；至於「其他應用系統」，則透過「區塊鏈應用系統」所提供的 API，與其連結使用。

五、結語

經過 POC 的經驗累積與驗證，我們發現，原生型區塊鏈所採用的一些技術或機制，必須經過適當的調整，才有可能導入國內金融服務應用的市場；也因此，藉由 POC 所累積的經驗，我們自行開發了一套區塊鏈系統，以方便進行各項的調整。

過去半年多，我們在這套區塊鏈系統上，同時進行了三個不同型態的 POC，其中有與支付相關的應用，也有智能合約的應用，更有大型生態系的應用。接下來，我們將持續與有意願導入區塊鏈應用的單位合作，一起尋求更多的 POC 驗證，藉由經驗的累積，尋找真正適合導入區塊鏈機制的應用，創造更大的市場價值。