財團法人台北外匯市場發展基金會

區塊鏈的新金融發展研究

期末報告書

計畫主持人：陳恭

國立政治大學電算中心主任

中華民國 107 年 6 月

摘要

區塊鏈技術源自比特幣，是支撐比特幣運作的帳本（ledger），紀錄比特幣的交易。區塊鏈所提供「可信賴的紀錄」可以讓彼此不完全信任的多方，不必透過中間人或中介機構，直接在網路上進行點對點（Peer to Peer）的交易，並對交易紀錄的維護達成共識。對照目前金融機構與金融市場基礎設施的巨量維運成本中，很大一部分就是花費在透過中心點或中介機構建立交易對象彼此間「可信賴的紀錄」，區塊鏈正是有潛力大幅改變維持這些紀錄的成本、便利性與管理結構。

區塊鏈技術在過去兩年中有了快速發展與實質的成果：從單純地提供可信賴的紀錄，已演進成新一代的應用系統平台；透過智能合約的程式化機制，讓區塊鏈的應用充滿了非常多的想像空間。不僅在公有鏈上，企業內部與企業之間的區塊鏈應用也陸續浮現。尤其是在金融業，不僅有潛力重新塑造整體金融市場的基礎設施，也為新一代的金融業務模式提供了非常多的發展方向。

本報告首先回顧與介紹區塊鏈的發展概況，並提供一個比較全面關照的角度，解析當前區塊鏈平台的關鍵組成要素，以及在應用區塊鏈建構新系統時應考慮的各個面向。接著從三種應用模式：企業內、企業間與新業務模式，分別探討了區塊鏈對支付、銀行融資、保險與證券業可能的衝擊與應用方式，也說明了這四個主題的許多區塊鏈應用方式與概念驗證的案例。

目錄

圖目錄

表目錄

第一章、緒論

第一節、研究背景、動機與目的

區塊鏈（blockchain）源自比特幣（Bitcoin），因此談區塊鏈不免要從比特幣談起。2008 年底，起源於美國的金融危機演變為世界金融危機，形成全球性恐慌。就在這年的 11 月，網路上出現了一份由中本聰（Satoshi Nakamoto）署名的研究報告《Bitcoin: A Peer-to Peer Electronic Cash System》[1]。隔年年初（2009 年 1 月 9 日），中本聰等人發布了依據此報告所發展的比特幣網路軟體，並且上線運轉，開啟了比特幣的實驗。

比特幣是一種基於密碼學的一些方法與其他技術所發明出來的一種虛擬貨幣（virtual currency）[2]，所以在英文裡一般稱比特幣是一種 cryptocurrency（密碼貨幣），這個英文字是從 cryptography（密碼學）與 currency（貨幣）兩個字結合而來的。密碼貨幣的特別之處在於它不依託任何實物（黃金、白銀或是法償貨幣等），也不是由一個獨立的發行機構發行，而是使用密碼學技術來創建，在網路上發行和交易的數位貨幣。反觀，一般所稱的電子貨幣，像是悠遊卡或第三方支付儲值帳戶，都是有發行機構，而且以法償貨幣為計價單位。但比特幣既沒有特定的發行機構（去中心化），也只能存在於網路系統中。加上其價格波動劇烈，並不符合一般對貨幣的認知，所以到目前為止，並未有國家界定其為貨幣，也僅有少數國家，例如日本，認可比特幣為具備支付功能的資產。我們中央銀行與金管會則將其界定為有風險的數位虛擬商品[3]。

比特幣上線初期並未受到大眾的關注，2012 年 11 月以前，比特幣對美元的最高匯率為 33 美元。直到 2013 年 11 月，當比特幣對美元的匯率突破 1000 元，才開始引起世界各國廣大投資人的注意，造成比特幣持續上漲。但 2014 年 2 月比特幣最大交易所 Mt. Gox 因資安事件關閉[4]，凡此種種因素導致比特幣對美元匯率跌到 1000 元以下，直到 2017 年 1 月才回漲到 1000 美元左右。其後比特幣

[1] https://bitcoin.org/bitcoin.pdf

[2] 中央銀行 105/03/24 發布的《我國電子支付機制之發展，兼論央行對數位通貨之看法》報告，將 virtual currency 翻譯成虛擬通貨。

[3] 中央銀行與金管會 102/12 新聞稿：https://www.cbc.gov.tw/ct.asp?xItem=43531&ctNode=302

[4] https://en.wikipedia.org/wiki/Mt._Gox

開始上漲，2017 年 11 月下旬已經幾度漲到 10,000 美元以上。

區塊鏈是支撐比特幣運作的帳本（ledger），紀錄比特幣的交易。在中本聰的報告裡，談了 block 也談了 chain，但並沒有把區塊鏈單獨寫成複合字“blockchain”。檢視 google 的搜尋趨勢紀錄（google trend）來看，大約是從 2013 年初開始，有直接以“blockchain”搜尋的紀錄。所以約略從那時候起，開始有比較多人將它直接寫成一個字，視其為一項新的技術來進行探討，發展至今，區塊鏈的演進已經與比特幣脫鉤，有了自己的途徑，很多學者專家甚至認為，區塊鏈有潛力對目前金融市場基礎設施（Financial market infrastructure, FMI）的結構與運行帶來顛覆式的衝擊，紛紛倡議應投入更多資源研究區塊鏈的技術與應用。從功能來看，區塊鏈就是比特幣底層的帳本技術，為什麼會有這麼大的潛力呢？

簡言之，區塊鏈技術是「可信賴的紀錄」的歷史性發明，它可以讓彼此不完全信任的多方，不必透過中間人或中介機構，直接在網路上進行點對點（Peer to Peer）的交易，並對交易紀錄的維護達成共識。對照目前金融機構與金融市場基礎設施的巨量維運成本中，很大一部分就是花費在透過中心點或中介機構建立交易對象彼此間「可信賴的紀錄」，區塊鏈正是有潛力大幅改變維持這些紀錄的成本、便利性與管理結構。無怪乎 2015 年 10 月 31 日出版的經濟學人雜誌，將區塊鏈稱為「信任製造機器（the trust machine）」[5]，充分突顯了區塊鏈可替不完全信任的各方，建立可信賴的交易紀錄的特性。

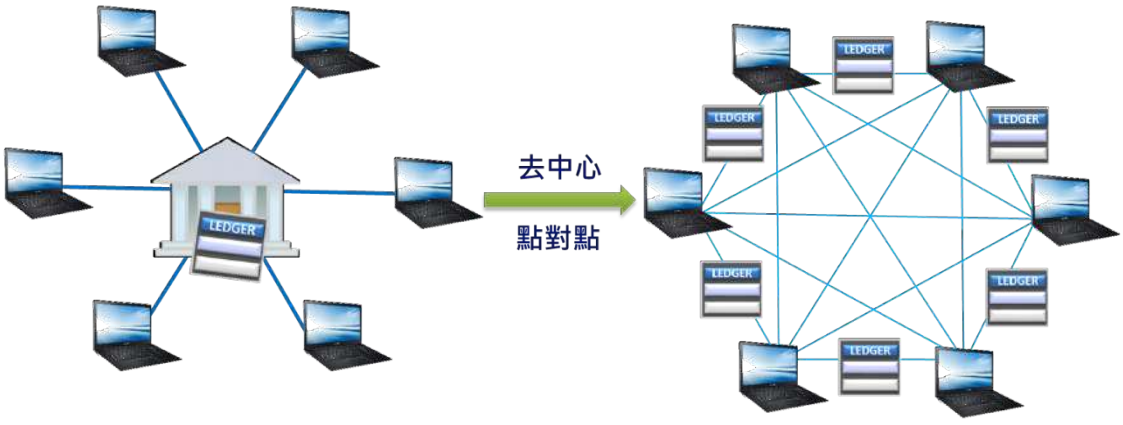

圖 1-1-1 從依賴中心點記帳到各有帳本的點對點交易網路

[5]https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

正因如此，過去三、四年來，區塊鏈的相關技術有了快速地發展，不再限於虛擬貨幣的支付與相關應用，而是朝新一代的網路應用平台邁進。除了底層的帳本或是資料紀錄的功能外，在應用層也藉由區塊鏈可支援執行通用程式的功能，有了更多發展空間。不僅在金融業獲得迴響，其他行業，甚至公部門也都開始注意到區塊鏈的創新潛力，紛紛投入探討區塊鏈的技術與應用。2016 年 6 月世界經濟論壇（World Economic Forum, WEF）發布了研究報告《區塊鏈將如何重塑金融服務業(An ambitious look at how blockchain can reshape financial services)》，以應用主題個案導向的方式，替區塊鏈在金融產業的發展與應用勾勒出一些方向與議題。這也是本研究報告的主要動機：以此報告為基礎，進一步蒐集更多的應用案例與方式，進行歸納與分析，整理區塊鏈在金融領域的各種發展模式，供台北外匯市場基金會與金融同業參考。具體而言，本研究報告的目的如下：

1、回顧區塊鏈的發展概況，解析當前主要區塊鏈平台的功能與特色。

2、歸納區塊鏈在金融業的應用模式，整理導入區塊鏈的考量因素與方向。

3、透過文獻探討與案例分析，探討研究區塊鏈如何能解決金融產業在作業面的一些痛點，以提升作業效率，增加參與者信任。

4、從區塊鏈的特性與優勢出發，參照個案，探討基於區塊鏈的創新金融服務模式的發展。

第二節、研究報告架構

由於區塊鏈是一項滿新而且還在發展中的平台技術，本研究報告第二章將先說明區塊鏈的特性與發展概況，並提供一個比較全面關照的角度，解析當前區塊鏈平台的關鍵組成要素，以及在應用區塊鏈建構新系統時需考慮的各個面向，以作為後續探討區塊鏈應用發展模式的技術背景。

在對區塊鏈的技術與應用面向做了重要且輪廓性的說明之後，本報告將就不同的金融產業，包含支付系統（Payment system）、銀行存貸業務、保險業與證券業四大主題，分別探討區塊鏈所可能帶來的衝擊以及創新應用方式。我們將就區塊鏈如何協助解決各產業現存的問題出發，延伸至區塊鏈可帶來的創新應用，以及可能顛覆產業生態的一些模式加以分析與說明。本報告將聚焦於產業應用與技術支撐，監管與法規的部份牽涉過廣，無法涵蓋於本報告中。

本報告第四章到第七章的結構都是先就產業概況，尤其是一些相關的問題與痛點做一簡要的說明，再就可以如何應用區塊鏈技術來處理這些問題提出一些模型或方案，最後介紹一些國內外之相關個案。首先，第四章著重於支付系統。一切的金融活動都奠基於準確有效率的支付系統，現今的支付系統，歷經電子化、網際網路與行動化等資通訊科技的影響，已經為廣大的消費者與機構提供了非常便利與高效率的支付服務。但在於跨行與跨境的支付服務上，世界各國的金融市場基礎設施（FMI）都還是存在一些作業上或運行模式上可以改善的地方，像是結算與清算（Clearing and Settlement）的時間較長，或是手續費過高等。這也正是許多專家認為區塊鏈可能可以發揮的地方，因此，世界各國已經有許多對區塊鏈如何應用在支付系統的倡議與概念性驗證（Proofs of Concept, PoC），也有新創科技公司試圖以區塊鏈等技術提供另類支付服務的案例，所以本章節將就這些倡議與實驗進行探討與說明。

在於第五章，銀行的傳統核心業務在資金放貸作業，或稱融資，區塊鏈對部分的融資業務也可能造成極大的影響，像是聯貸業務與貿易融資等。這些融資業務往往牽涉多個不同業別，彼此不完全信任的利害關係人，非常適合應用區塊鏈來建構彼此可信賴的交易紀錄，以大幅降低人工作業的成本，並提升整體作業效率。所以本報告第四章將以銀行融資業務為主題，探討一些可以透過區塊鏈予以改善。此外，新興的 P2P 借貸平台，以網路平台撮合無法經由銀行取得融資的個人或中小企業與投資人，如果底層採用區塊鏈技術以及智能合約控管，將可提高借貸平台的透明度與可信賴度，因此本章節也會將其納入說明。

本報告的第六章將探討如何運用區塊鏈於證券業。因公開交易股票的量大，媒合過程相當複雜，又必須在短時間完成，所以一般認為不適合運用區塊鏈技術處理，多數的應用焦點是放在證券交易後的結算與交割（Post-trade clearing and settlement）作業，尤其是店頭交易，此乃因為一方面其交易量相對於公開市場比較少，另一方面其交易模式係對手間直接交易，類似 P2P 交易。這些交易後作業因涉及多方，資訊往往未能及時統整，所以目前多半是以 T+2 或是 T+3 的模式來完成款券交付（Delivery versus Payment, DvP）的手續，有實質改進的空間。若能透過區塊鏈提供多方可信賴的共享交易與資金移轉紀錄，即便不能改成 T+0 模式，也應可以減少人工作業，提升效率。此外，私募股票因交易量小，資訊不夠透明，所以整體作業，從發行、股權登錄、交易到結算與交割都可考慮應用區塊鏈技術。最後，近來盛行的初次代幣發行（Initial Coin Offering, ICO）則是一種

原生於區塊鏈的募資方式，本章節也會加以探討。

接下來在第七章我們將探討區塊鏈對保險業的影響。核保與理賠是保險業務的主要作業，這兩項業務都可以透過區塊鏈提供的可靠的共享資訊加以改善；保險合約中的條款更是適合採用智能合約來提高透明度與自動化落實。除此之外，我們也會探討保險業與其他業種的合作，像是銀行保代業務以及海洋貨運險等等，這些跨業合作若能搭配區塊鏈提供的可信賴紀錄，整體作業的流暢度一定可以提昇。最後，新型態的 P2P 保險應用網路科技與區塊鏈製造的信任，將保險回歸到眾人互保分攤風險的模式，也是我們要探討的主題之一。

第八章總結本研究，我們將回顧區塊鏈的各項特性，並展望未來區塊鏈的發展方向，以能更有效的支援各種金融業務的更新與創新。另一方面，我們也將參考綜合各章節的重點，參考國際文獻，整理出有效地運用區塊鏈的關鍵考量因素與規劃重點，供各方參考。

第二章、區塊鏈技術的發展與現況

本章節先概述說明區塊鏈技術的特色與發展歷程，再就目前幾個主要的區塊鏈平台的特色與運作做一比較性的解析。對技術比較陌生的讀者，可以略過各平台的比較，不會影響後續章節的閱讀。

自從區塊鏈受到大眾矚目後，許多文獻會說明區塊鏈是採用分散式帳本技術 (Distributed Ledger Technology, DLT)，以強調 DLT 的涵蓋範圍比較廣，區塊鏈只是 DLT 的一種實現形式與技術，尤其是 R3 聯盟的倡議。對本研究而言，我們大致視兩者為近似詞，僅在明確需要表達差異時，才區分它們。

第一節、區塊鏈技術的發展概要

至目前為止，區塊鏈的發展可概況分三階段，首先是比特幣的區塊鏈，以及其變型；其次是具備支援應用程式開發的區塊鏈平台，或簡稱具備為智能合約功能的區塊鏈；晚近則是企業區塊鏈的蓬勃發展，以下就這三個發展主軸做一簡要的說明。

(一)比特幣區塊鏈

區塊鏈源自比特幣，功能上它就是比特幣的帳本，記錄在比特幣網路上發生過的每一筆比特幣交易。稱它為區塊鏈是因為它是由一個個區塊與特殊安全鏈結所組成的，每個區塊就像帳簿裡的一頁內容，紀錄交易的明細，區塊之間透過安全鏈結串起來構成整個帳簿，而且安全鏈結是基於密碼學技術建構的，可以保護帳簿，只能新增但無法塗改其過往的交易歷史。記帳的工作由各節點透過創建區塊完成，創建過程是區塊鏈技術的精華所在，它是一個整體節點之間，既競爭又合作的過程，一般稱之為挖礦（mining）。競爭是因為這創建過程像一場解題競賽，需耗費一定的運算資源[6]，勝出者可得到比特幣獎勵。合作則是因為最先挖到礦(完成解題)的節點，必須將新區塊連同它的解題工作證明(Proof of Work, PoW)透過底層的 P2P 網路，廣播給其它節點，就其 PoW 進行驗證確認後，才能被大家納入帳簿內，所以這也稱為分散式共識（consensus）程序。

換言之，比特幣網路的所有節點共同維護、分享一份內容一致的帳本，所以區塊鏈也被稱為分散式共享帳簿。不僅如此，每個區塊的交易內容都採用了安全算法來彙總編碼，即便是竄改單筆交易的內容，都會反映在整個區塊的安全編碼上，各節點可以在驗證中發現而拒絕接受遭塗改的區塊。所以區塊鏈網路中的各個節點，可以信任自己的帳簿跟交易對手的是一致的，不必依賴中間的信賴機構來替雙方對帳(account reconciliation)，從而達到去中介化的特色。

此外，比特幣網路中，交易者不必實名認證，其帳戶是由個人公鑰（public key）經過編碼而成的一段冗長的亂序字母和數字所組成，但每一筆的交易資料在產生之後，都必須以支付者的私鑰（private key）加以數位簽章（digital signature）後，才能進行遞送。所以交易者雖採用匿名制，但透過類似自然人憑證所採用的公私鑰安全管控，交易者無從造假或否認該筆交易，從而確保交易的真實性。加上帳簿內容都是無加密且公開的，故比特幣區塊鏈的特色是所有交易具有透明與可追溯性。

[6] 這過程也是基於安全雜湊演算法的原理，執行時像是玩一個數學猜謎遊戲，需反覆計算，但猜中與否純屬機率問題，也無法事先啟動預作準備。

（二）智能合約(smart contracts)

比特幣區塊鏈的功能以記錄交易資料為主，雖有腳本語言(Bitcoin script)機制，但並不具有完整的程式語言功能，不易用於應用程式開發，主要只能當成一個具特殊功能的分散式資料庫使用。針對此，2015 年中推出的以太坊(Ethereum)區塊鏈，除了提供虛擬通貨以太幣外，其主要特色即為提供了通用的程式語言，支援開發各類應用程式運作於區塊鏈上，讓區塊鏈成為一個通用的去中介應用程式平台。以太坊的白皮書名為「A Next-Generation Smart Contract and Decentralized Application Platform」，強調「智能合約」[7]為其平台特色，其實這裡所謂的智能合約就是在區塊鏈平台上執行的應用程式，所以以太坊的區塊鏈不僅可以儲存資料，還可以使用這些共享資料執行應用程式，進行交易與資產移轉。這是區塊鏈技術發展的一個重要里程碑，因此很多文獻視智能合約為「區塊鏈 2.0」的主要技術與應用。

智能合約是以應用程式的邏輯來實現交易中的條款與條件，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，智能合約的運作都是以「事件驅動」的方式在運作，例如：交易完成七日內，客戶如果提出取消要求，合約就自動失效。這些事件也包含取得外部第三方可信的資料，根據資料值所做的判定結果來觸發智能合約的執行，例如：從氣象局取得降雨量之類的天氣狀況來啟動自動理賠合約等。一般稱這種外部資料源稱為 Oracle（神諭）。

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了合約的指定功能，開始執行程式，執行的結果通常就會引發資產的移轉。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，重點是在於跟區塊鏈技術的結合，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的，像是一般電子商務平台，它們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，而且在它的中心伺服器上執行。但現今的這些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，不僅不能竄改，也會在每個（交易相關的）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

[7] 「智能合約」一詞原是由學者尼克·薩博(Nick Szabo)於 1990 年代初期所提出來的，倡議可以將交易的條款透過電腦化來落實。以太坊沿用此詞，並讓它與區塊鏈技術結合。

易的各方間建立信任，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，像是當供貨量超越過去三個月的平均值後，折扣數可以增加 50%。但廠商之間多半是各自記帳，使用獨立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，這樣雙方可省去原本獨立系統維護費用以及帳本管理費，因而可以省去許多人工或程式對帳的成本。

（三）企業用區塊鏈平台

區塊鏈技術另一個主要的發展趨勢是提供企業應用所需的功能。首先，比特幣或以太坊都是以公開、去中介又無監管的方式運作，一般稱為公有鏈(public)[8]模式。但是對於民間企業，或是政府機構而言，區塊鏈的使用必須要有某種程度的管控與監理；像比特幣區塊鏈這樣公開不設限，又去中介的運作方式，在實行上是有困難的。所以對企業使用而言，區塊鏈平台必須要提供適當的會員管理機制，限制可參與的成員，甚至要求實名制[9]。一般而言，可將區塊鏈的運作模式依開放性參與（Open, Permissionless）或限制性參與（認許制，Permissioned）為主要分類依據，概分公有鏈以及私有或聯盟鏈(Consortium Blockchain)，通常聯盟鏈與私有鏈的差異僅在於參與者是否有跨組織或僅限同一組織內[10]。在私有鏈或聯盟鏈的運作上，通常還會更進一步區分參與節點的權限，例如：可以記帳，可以交易，或只能查詢交易紀錄。

除了會員身分認證與權限管理外，企業應用對區塊鏈平台的需求主要還有兩項：高效能的共識記帳機制與交易資料的隱私保護。首先，比特幣區塊鏈的工作量證明(PoW)共識記帳法，平均 10 分鐘才完成一個區塊，換成每秒平均交易量還不到 10 筆；以太坊在這方面雖有改進，但也不能滿足企業區塊鏈對交易速度的要求。實務上，企業區塊鏈網路的節點規模比公有鏈要小的多，沒有必要採用大規模節點適用的 PoW 共識記帳法，反而是採用像分散式系統中著名的拜占庭

[8]以太坊也可以在一定程度上支援私有鏈(private blockchain)的運作方式，讓建置者可以決定有哪些電腦可以加入運作，成為私有區塊鏈的節點。

[9] 會員管理就是一種中心化的機制，所以私有鏈或聯盟鏈的運作不是完全的去中心化運作。

[10] 檢視文獻，這些分類名詞尚未有大家一致認可的定義。

容錯共識法(PBFT)[11]，就可以大幅提高每秒平均的交易數量。所以各種企業區塊鏈平台都正研發不同的高效能共識法。其次，比特幣與以太坊的帳本內容是完全公開的，企業應用上通常需要對交易資料有所保護，限制僅有與交易相關的成員或監管與稽核單位可以檢視交易的內容。所以新一代的企業區塊鏈平台必須要提供參與成員能保護交易資料隱私性的功能。

目前正在發展中的企業區塊鏈平台，最知名的當屬 Linux Foundation 下的 Hyperledger 計畫的 Hyperledger Fabric 平台，以及 R3 聯盟下的 Corda 平台。這兩個區塊鏈平台都是針對企業組織所設計的，對參與者採認許制，可以私有鏈或聯盟鏈方式運作，而且都不支援任何的原生數位貨幣，也不採用 PoW 的共識法，並提供了限制交易資料分享的隱私保護機制。其中 Corda 平台更放棄區塊鏈的資料結構，強調其特殊的 DLT 的架構更適合企業使用。以太坊社群去年底推出的 Quorum 平台，主要的特色就是修改以太坊平台，提供非 PoW 的共識記帳功能，以及可支援交易隱私的私有交易機制。今年年初成立的企業以太坊聯盟 (Enterprise Ethereum Alliance, EEA) 也是要聯合開放源碼社群的力量，發展適合企業使用的以太坊區塊鏈平台，目前以 Quorum 為參考平台。

第二節、主要區塊鏈平台介紹

本章節就目前幾個主要區塊鏈平台的功能特色作一比較深入的說明。

（一）比特幣區塊鏈

區塊鏈（Blockchain）源自於比特幣（Bitcoin），是比特幣的帳本，負責紀錄所有比特幣的交易紀錄，每個比特幣網路中的節點，都會有一份同樣的帳本，且共同參與維護這個區塊鏈帳本。稱它為區塊鏈的原因在於其構造方式，如圖 2-2-1 所示：它是由一個一個的區塊，透過特殊的安全鏈結將這些區塊串起來構成整個帳本的。每個區塊就像一頁帳本，區塊的流水號（例如：27351）就像帳本的頁碼，反映區塊之間產生的順序。在內容方面，每個區塊都有一個特殊的安全編碼[12]（Block hash，例如：005wp1x93f371a09）與時戳（Timestamp）以及創建這個區塊的 PoW 等詮釋資料(Metadata)，這些是記錄在區塊的表頭(Header)內；

[11] Marko Vukolic, The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, iNetSec 2015. http://www.vukolic.com/iNetSec_2015.pdf

[12] 應用密碼學的安全雜湊演算法（Secure Hash Algorithm, SHA）計算出來的單向、不可逆的數值。

區塊主體（Body）則記錄發生過的比特幣交易內容，每筆交易也有自己的安全編號（例如：500b5uf1z0w2a）。區塊之間的安全鏈結，則是透過每個區塊的安全編碼而實現的：每個區塊會記錄前一個區塊的安全編碼，依此建立區塊間的連結，並可回溯連結到比特幣帳本的第一個創始區塊（Genesis block）。

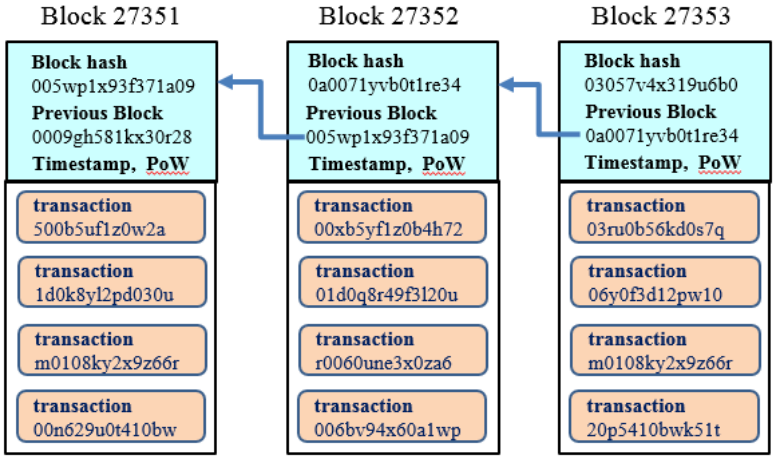

圖 2-2-1 比特幣區塊鏈示意圖

比特幣帳本的這些區塊的創建過程是區塊鏈技術的精華所在，概要說明如下。每當有節點進行支付交易時，比特幣節點軟體就會廣播該交易給網路中的其它節點，讓各節點利用演算法對這些交易進行驗證，並定時創建出新的區塊來記錄這些交易；每個在比特幣網路上的節點都可以參與創建區塊，但只有一個節點可以取得該次區塊的記帳權。這創建過程像一場解題競賽，需耗費一定的運算資源[13]，因為勝出者得到的獎勵是比特幣，因此這過程被類比成挖礦（Mining）。最先挖到礦的節點，必須將新區塊廣播給其它節點進行確認後，才能被大家納入帳本內，這是一個既競爭又合作的程序，稱之為分散式共識程序（Consensus）。如果新的區塊為網路中其他節點所批准接受[14]，這個區塊就會按照順序加附到原有的區塊鏈末端，它的創建者（礦工）也可藉此獲得一筆定額的比特幣與交易費，做為耗費運算資源進行挖礦的酬勞。

由以上的說明，我們得知這個區塊鏈帳本是由所有比特幣網路的節點一起共同維護的，每個節點都共享一份內容一致的帳本，所以這個區塊鏈也被稱為分散式共享帳本。促使大家一起投入電腦資源參與維護帳本（挖礦）的誘因，就是區

[13] 同註 5 雜湊

[14] 每個區塊的工作量證明（PoW），內含一個 nonce 數值，可供其它節點快速驗證區塊的有效性。

塊的創建者可領取比特幣作為獎勵，這也是比特幣的特殊發行方式。不僅如此，每個區塊的交易內容都採用了安全算法來彙總編碼，即便是竄改單筆交易的內容，都會反映在整個區塊的安全編碼上。同時因每個新產生的區塊都記錄了前一個區塊的安全編碼值，因此，改了某一區塊的一筆交易，就得連帶修改該區塊之後在鏈上的所有區塊，隨著區塊鏈的長度增加，困難度也愈高[15]。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，不必依賴中間的信賴機構來替雙方對帳（Account Reconciliation）。

此外，比特幣網路中，交易者不必實名認證，其帳戶是由個人公鑰（Public key）經過編碼而成的一段冗長的亂序字母和數字所組成，如果不借用其他技術手段是無法得知交易者的真實身份。但每一筆的交易資料在產生之後，都必須以支付者的私鑰（Private key）加以數位簽章（Digital signature）後，才能進行遞送。收到交易的端點，必須以該交易支付者的公鑰解密，以確認該交易真偽。所以交易者雖採用匿名制，但透過公私鑰的安全管控，交易者無從造假或否認該筆交易，從而確保交易的真實性。

綜上所述，區塊鏈實為比特幣的帳本資料庫，它是透過比特幣網路上所有的節點集體維護運行的，並具有以下創新特色：

- 毋須中心機構維護帳本：網路中每個節點都會有一份帳本的備份，也都遵循相同的記帳規則來更動帳本，以達到帳本一致性，從而不需要第三方中介機構在交易者中間維護帳本。
- 帳本內容無法竄改：每個區塊的內容透過安全編碼技術，搭配區塊之間的安全鏈結，確保區塊鏈的帳本內容只能新增，不能修改。
- 交易真實性與透明性：交易者雖然可以匿名，但每筆比特幣的交易都需要經過支付者的數位簽章以及公鑰確認，可確保交易的真實性；而且交易內容均寫入區塊鏈，無法否認或竄改，具有透明與可追溯性。

比特幣區塊鏈的另一個特色是它的 UTXO 交易結構，提供追蹤每一筆比特幣交易的簡易方式，以下說明之。

不同於一般支付系統以帳戶餘額為基礎的交易架構，比特幣的創始人中本聰（化名）為比特幣的交易系統設計了獨特的 UTXO 結構，UTXO 是 Unspent

[15] 嚴格說，應該是修改的代價非常高，要擁有超過整個鏈 51%的算力，簡稱為 51%攻擊。

Transaction Outputs 的簡寫，是比特幣交易的基本單位，UTXO 是不可分割且獨一無二，綁定到某個帳戶，這種設計可以讓『雙重花費』(Double spending）的問題很容易被偵測出來。

每筆比特幣的交易都是由數個 Inputs 與 Outputs 組成，代表由來自 Inputs 的比特幣將支付給 Outsputs 端的帳號，所有 Inputs 端的比特幣值總和必須相等或大於 Outputs 端，每個 Input 其實來自於某一個交易的 Output，且必須是 UTXO。

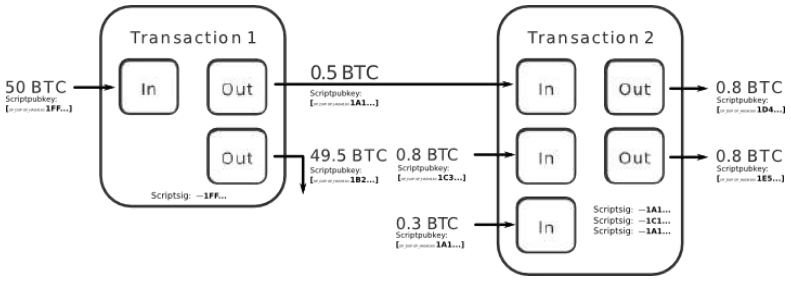

圖 2-2-2 比特幣區塊鏈 UTXO 示意圖

來源：https://medium.com/@lopp/the-challenges-of-optimizing-unspent-output-selection-a3e5d05d13ef

以上圖為例，交易 TX1 有 1 個 Inputs 與 2 個 Outputs，TX2 則有 3 個 Inputs 與兩個 Outputs。交易 TX1 代表 Alice 付 0.5BTC 給 Bob，Inputs 只有一個，幣值為 50BTC，兩個 Outputs 中 0.5BTC 付給 Bob 帳戶，剩餘的 49.5BTC 付給 Alice 自己的帳戶（此為模擬找錢的動作，否則這 49.5BTC 就會被礦工視為交易手續費而取走)。

這兩個 Outputs 原都是 UTXO，但接著 Bob 透過 TX2，將 0.5BTC 協同另兩個 Inputs（也是 UTXO）支付給 Charlie 帳戶 0.8BTC，所以只有 49.5BTC 是 UTXO。TX2 的兩個 Outputs 目前都還是 UTXO，可以當成後續交易的 Inputs 端。也就是說，任何 Ouput 只能當成 UTXO 使用一次，否則即被視為雙重支付而被拒絕。

（二）以太坊

以太坊（Ethereum）是其創始人之一的 Vitalik Buterin 受比特幣（Bitcoin）啟發而提出的區塊鏈平台，以太坊在 2014 年 7 月透過『首次代幣發行』(ICO，Initial Coin Offerings） 集資，並於次年 7 月底開始運行其公有鏈版本。 目前以太坊 （Ethereum Protocol） 有多個程式語言的實作版本，包括用 Go 語言實作的 go-ethereum、用 Rust 程式語言實作的 Parity、用 C++程式語言實做的 cpp-

ethereum、用 Python 程式語言實作的 pyethapp、用 Javascript 程式語言實作的 ethereumjs-lib、以及用 Java 程式語言實做的 EthereumJ 等。

以太坊上也提供了密碼貨幣系統（Cryptocurrency），稱為 『Ether 』，跟比特幣一樣，也是透過類似 PoW（挖礦）的共識過程，進行帳本的維護與以太幣的發行。但以太坊的最主要特色是它的區塊鏈除了能儲存無法竄改的交易資料外，也提供了執行應用程式的平台，並稱這類程式為智能合約（Smart Contract）。

相較於比特幣區塊鏈，這是一大進展，因為比特幣區塊鏈雖然也有腳本語言（Scripting language），但其限制很大（ 缺乏『圖靈完備性』（Turing-completeness)），難以在區塊鏈上實作複雜的交易系統，因此以太坊在其區塊鏈平台上加上智能合約的功能，並提供去中心化的『以太坊虛擬機』 （EVM，Ethereum Virtual Machine）來執行智能合約。以太坊的智能合約可以用多種程式語言開發，包括目前主流的 Solidity（語法類似 Javascript）、Serpent（語法類似 Python）以及 LLL（語法類似 Lisp） 等，都可經編譯後在 EVM 上執行。

因此，以太坊上的交易不限於支付，也包含了執行智能合約的程式功能。使用者透過交易發送來執行區塊鏈上的智能合約，首先交易會經過簽章後發佈到網路上，當網路上的節點（礦工）看到交易後會執行交易驗證，例如檢查簽章、帳戶的餘額及帳戶的 nonce 值等，若驗證成功則將交易放進新區塊中，若新區塊透過 PoW 共識機制被其他節點所接受（Mined），則網路上的所有節點都會執行該交易（Contract Code），並更新相對應的資料（Contract Storage），其結果就是網路上的所有節點都會將相關的資料更新。

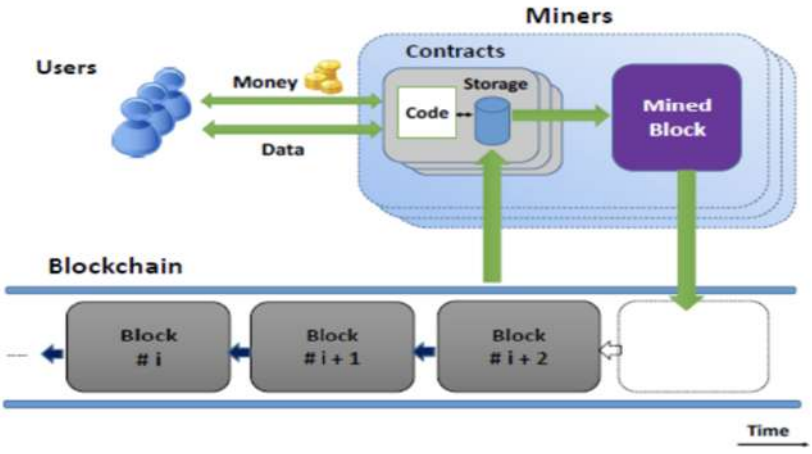

圖 2-2-3 以太坊架構

來源：http://fc16.ifca.ai/bitcoin/papers/DAKMS16.pdf

為避免設計不良的智能合約程式造成無窮迴圈或使用過多的儲存空間，以太坊增加了『Gas』制度，智能合約程式每執行一個步驟，或是儲存資料都會消耗特定數量的 Gas，且必須支付以太幣來購買所耗費的 Gas，作為付給礦工們的交易手續費（每單位的 Gas 的以太幣價格可由使用者設定，以吸引礦工優先執行特定交易）。智能合約執行過程中，一旦 Gas 消耗量超過額度就會被 EVM 停止，撤回執行過的交易。

以太坊公有鏈上使用的共識機制為 PoW，但與比特幣不同的是，在以太坊公有鏈上，區塊產生的速度較快（約為 14~15 秒鐘，比特幣則約為 10 分鐘），由於共識速度較快，增加了區塊被丟棄的機會，也增加了公有鏈被大礦池控制的可能性，因此以太坊使用『GHOST』協議來解決這個問題，使被丟棄的區塊有機會被主鏈收納（稱為 Uncle Blocks）。由於 PoW 共識機制需要大量電腦算力來計算雜湊（Hash）值，相當耗費電力資源，因此以太坊另外提出了以權益量證明（POS，Proof-of-Stake）的共識機制，希望將來能取代現行的 PoW 共識機制。

除了公有鏈外，以太坊也提供了架設私有鏈或聯盟鏈的方式，提供政府或企業組織架設小型且有存取限制的區塊鏈網路。由於這類區塊鏈的運作方式，其參與者之間通常是有一定的信任程度，所以必不需要依靠 PoW 這種耗費資源，又效率較差的共識機制。

有鑑於此，以太坊在 2017 年四月也推出新版本，支援稱為 PoA（Proof of Authority）的高效能共識模組，由區塊鏈參與者決定在某些結點之間，輪流創建區塊供其他節點認證後加入帳本，提供了架構高效能私有鏈或聯盟鏈的方案。

為更進一步提供符合企業或政府組織區塊鏈的應用需求，像是會員認許資料隱私保護等，2017 年三月，微軟、英特爾、思科、萬事達卡國際組織、摩根大通、安泰集團等 30 家科技公司、金融業者、以及研究機構共同創立了以太坊企業聯盟（EEA），希望能將以太坊帶入商業應用的領域。

（三） Quorum

Quorum 是摩根大通（JP Morgan Chase）銀行基於以太坊所開發的『認許制』區塊鏈（私有鏈或聯盟鏈），其目的是提供一個可以應用在企業環境（Enterprise-ready）上的分散式帳本以及智能合約平台。Quorum 的特色是具備比以太坊公有鏈快的交易處理速度（每秒可處理數十到數百個交易），以及提供以訊息加解密

為基礎的交易隱密性（Transaction Privacy）功能。Quorum 為開放源碼的區塊鏈，除了主要的摩根大通（JP Morgan Chase）以外，其他公司或組織如 Ethlib、Zerocoin Electronic Coin Company、Porosity、AMIS 帳聯網、以及微軟等亦與摩根大通有合作關係。

Quorum 的核心架構包含由 go-ethereum 修改而來的區塊鏈（稱為『Quorum Node』），以及提供交易隱密功能的 Constellation 兩個部分。組成 Constellation 的兩個元件分別為 Transaction Manager 以及 Enclave，其中 Transaction Manager 負責儲存、控管與交換加密資料，而 Enclave 則提供封閉（Isolated）的軟體環境以進行資料加解密及存放私鑰。

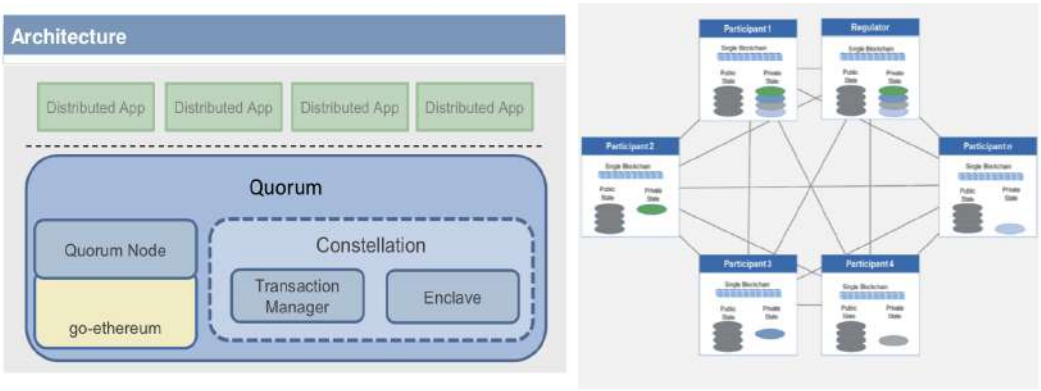

圖 2-2-4 Quorum 架構

來源：https://github.com/jpmorganchase/quorum/wiki/Quorum-Overview

由於 Quorum 是基於以太坊所開發的，因此具備了大部分以太坊的功能及特性，但與以太坊不同的是，Quorum 並沒有採用以 PoW 的共識機制，而是提供了 QuorumChain 及 Raft 兩個共識機制。此外，雖然 Quorum 繼承了以太幣以及以太坊的『Gas』制，但在 Quorum 上面執行交易是不需要手續費的（沒有 Gas price）。另外，Quorum 的區塊鏈結構雖然跟以太坊大致相同，但由於 Quorum 提供交易隱密功能，交易資料並不是公開的，而是被授權的節點才能看到，因此 Quorum 除了以太坊原有的公開的交易資料結構外，又另外增加私有的交易資料結構，以達到將隱密性（Private）資料分開存放的目的。

目前 Quorum 提供兩種共識機制，分別為 QuorumChain 以及 Raft。QuorumChain 是基於時間的投票（Voting）共識機制，其特色是利用智能合約來管理參與共識的權限、以及執行（Send transaction）智能合約來進行投票等。Raft 共識機制是 Quorum 由 ETCD 的 Raft 演算法實作沿用過來的，其特色是票選主

控節點（Leader），以及利用同步日誌的方式，使其他節點（Follower）的資料與主控節點（Leader）保持一致。除了 QuorumChain 與 Raft 共識機制之外，Quorum 也將採用台灣帳聯網公司（AMIS）的 Istanbul BFT 演算法，以提供在 Quorum 上使用拜占庭容錯機制的選項。

在智能合約的開發上，Quorum 與以太坊並沒有太大差異，雖然 Quorum 有隱私交易（private transaction）的功能，但啟用隱私交易功能並不需要修改智能合約，而是在部署智能合約時，以及在後續執行隱私交易時以設定參數的方式，指定私有交易資料的可視範圍。

在以下摩根大通的 Quorum 的產品套件藍圖裡，除了開放源碼的 Quorum Node 以及 Constellation 外，還有 Quorum 的企業應用套件（Quorum Enterprise Toolkit）以及開發工具 Cakeshop。Quorum Enterprise Toolkit 的功能包含 Quorum API、節點管理（Node Manager）、使用者認證（Certificate Authority）、以及系統監控 （Monitoring Capabilities）等。

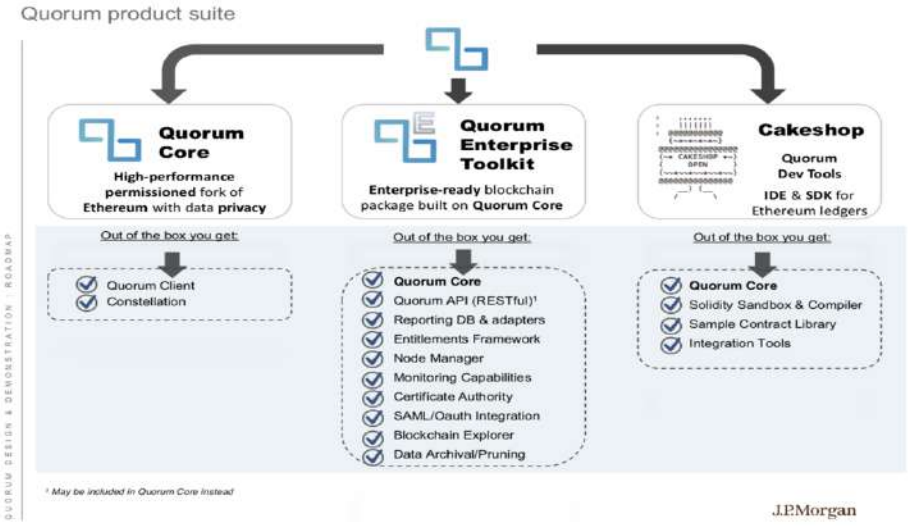

圖 2-2-5 Quorum 產品藍圖

來源: JP Morgan Chase 文件

（四） Hyperledger Fabric V1.0

Hyperledger 目前是 Linux 基金會下的一個企業區塊鏈開源協作專案，參與的企業包括 IBM、思科、英格蘭銀行（Bank of England）和摩根大通（JPMorgan

Chase）等 。Fabric 是 Hyperledger 專案下的一個最知名的個案，而 IBM 則是 Fabric 程式碼的最大貢獻者。 以下就 Hyperledger Fabric V1.0 的功能與技術架構，以及特有的交易流程做一說明。

1.功能架構

圖 2-2-6 展示了 Fabric V1.0 的各個功能模組，以下就幾個重要的模組說明。

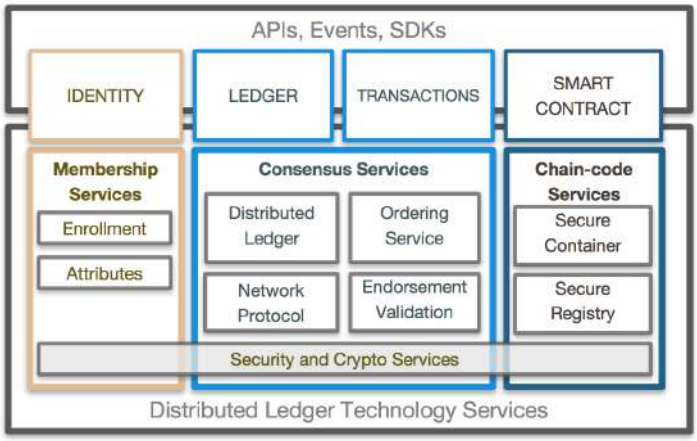

圖 2-2-6 Hyperledger Fabric V1.0 功能模組

來源：https://goo.gl/V8jPfH

Membership Services 負責管理會員身分、身分隱私、內容保密和交易審計功能，以保證區塊鏈平台交易的安全性。Consensus Services 負責節點間的共識協議、分散式帳本的管理、帳本狀態的儲存、以及節點間的點對點協議 。Hyperledger Fabric V1 支援隨插即用的共識協議，如 SOLO、Kafka、SBFT 等。Chain-Code Services 提供安全及輕量的容器（Container）運行環境，以在節點上執行智能合約（Chain-Code），容器環境是經過簽章驗證的安全鏡像，Hyperledger Fabric V1.0 的智能合約可用 golang、Java 或 Node.js 開發 。

2.技術架構

Hyperledger Fabric V1.0 的技術架構分為以下四個部分組成（參見圖 2-2-7）。

（1）Membership：支援隨插即用式的 Membership Service Provider 架構，系統預設為 Fabric 內建的 Fabric-CA，負責管理應用程式、用戶及節點的身分。Fabric-CA 提供用戶身分驗證，負責憑證的生成、發行、展期及註銷等功能。以及提供系統、通道（Channel）和智能合約（Chain-Code）三個層級的權限控管，

使 Hyperledger Fabric 可以在具隱私性與機密性的情境下使用。

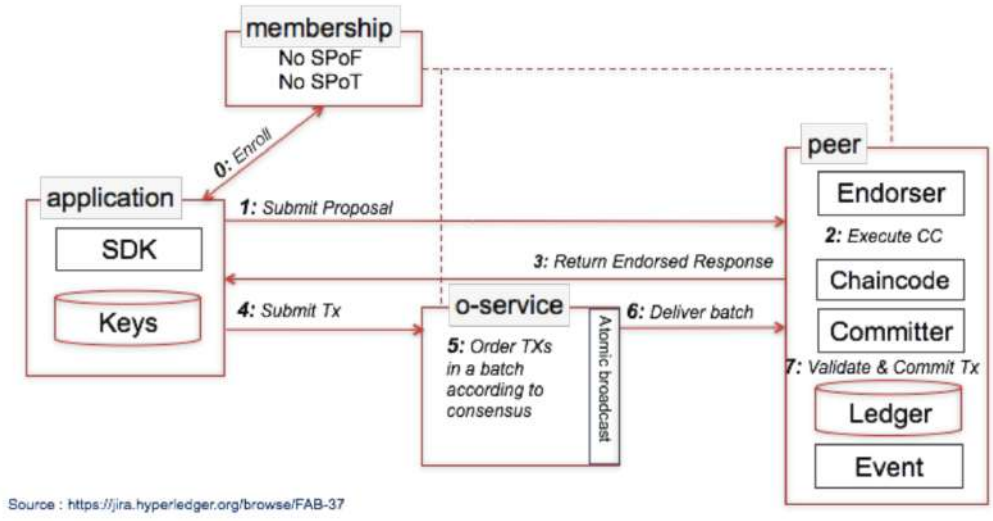

圖 2-2-7 Fabric V1.0 系統架構圖

（2）Peer：參與節點之間組成點對點網路（Peer to peer gossip network），負責維護帳本（ledger）狀態以及智能合約的部署與執行。Peer 分為背書節點（Endorser）和提交節點（Committer）。背書節點負責智能合約的模擬執行，並驗證某個交易是否合法，是否願意為其背書及簽署。提交節點負責對排序後的交易進行檢查，選擇合法的交易執行及維護帳本狀態（World state）。Peer 在不同的應用場景中的角色可以不同。

（3）Ordering Service：是由一組 Orderer 節點運行的共識服務，稱為 Ordering service。負責對所有交易進行排序，把有效的交易加入新生成的區塊，並廣播至相關的提交節點以執行有效性驗證及維護帳本，使得所有節點的帳本狀態保持一致性。Ordering Service 支援隨插即用式的共識模組，例如：SOLO 、Kafka、SBF。

（4） Client application （SDK）：Fabric SDK 為應用程式開發人員提供基本的 API，而這些 API 包含部署及執行智能合約（Chain-Code）、交易訊息處理等功能，應用程式可以監聽 Peer 的事件通知，當交易成功或失敗，或是當區塊被加到子帳本時，Fabric 都可以發送事件通知客戶端的應用程式。Fabric SDK 支援多種程式語言以提供開發人員編寫智能合約，包含 Node.js、Python、Java、以及 golang。

3.交易流程

Hyperledger Fabric V1 的交易流程如圖 2-2-8 所示，分別說明如下：

（1）客戶端應用程式透過 SDK 發送交易：SDK 依據交易的背書策略（endorsement policy）創建交易提案（Proposal）後發送到一個或多個 Endorsing Peer。交易提案中會包含本次交易要呼叫的智能合約（Chain-Code）名稱、方法、參數、及簽章等。

（2）Endorsing Peer 收到交易提案後，透過智能合約（Chain-Code）執行模擬交易，在執行模擬交易期間產生的狀態修改（Read Write Sets），並不會寫入到 Peer 節點的子帳本中。

（3）參與背書的 Endorsing Peer 將原始的交易提案與執行模擬交易的結果（ Read Write Sets）打包在一起簽名後傳回給客戶端的應用程式。

（4）客戶端應用程式發送交易（包含模擬交易的結果）給 Ordering service。

（5）Ordering service 對接收到的交易進行所有交易的排序，將交易整批打包生成新的區塊，並透過訊息通道（channel）廣播發佈給 Committing Peer。

（6）Committing Peer 收到區塊後，會對區塊中的每筆交易進行驗證（endorsement policy、Read Write Sets 的版本狀態等），完成驗證後會將區塊寫入到子帳本，並修改子帳本狀態資料庫。

（7） Committer Peer 通知客戶端應用程序交易處理結果。

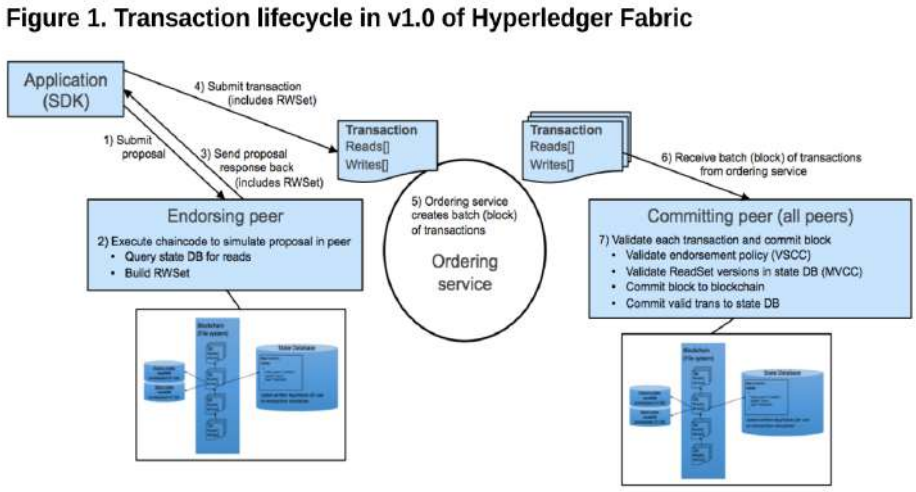

圖 2-2-8 Hyperledger Fabric V1.0 交易流程圖

來源：https://goo.gl/7xExi8

Hyperledger Fabric V1.0 另一項主要的新功能就是提供資料隱私保護的通道（Channel）服務。通道是 Ordering Service 提供的一種通訊機制，基於發佈-訂閱關係，可將 Peer 和 Orderer 節點連接在一起，形成具有保密性的網路，網路上的其他節點並沒有權限來查看通道上的交易。為加強對敏感性資料的保護，可以將有競爭關係的不同公司或節點隔離開來。例如共識服務（Consensus Service）與（Peer1、Peer N）、（Peer1、Peer2、Peer3）、（Peer2、Peer3）組成三個相互獨立的通道，節點可加入不同通道以維護各個通道對應的子帳本狀態，並提高執行性能及交易吞吐量。

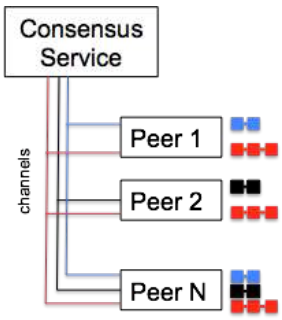

圖 2-2-9 通道（channel）及子帳本（sub-ledger）的結構

來源：https://goo.gl/Erykrc

（五） R3 Corda

R3 聯盟於 2015 年 9 月 15 號成立，其目的為發展金融業的區塊鏈平台與相關應用， 一開始 R3 有 9 家創始機構，發展至今，全球已有超過 70 家金融機構加入，台灣的中信金控公司也是其會員之一。R3 的技術人員在研究過一些主要的區塊鏈平台後，提出了以 DLT 取代區塊鏈的方案，並於 2016 年 11 月 30 日推出自主研發的 Corda 平台，並於 2017 年 10 月釋出 1.0 正式版。

Corda 平台的設計上，僅部分採用一般區塊鏈平台的原則，像是去中間人的交易模式與交易資料的不可竄改性等，但從根本上放棄了區塊加鏈結的帳本資料結構，而特別強調交易內容的保密性，每筆交易資料的內容只會分享給和這筆資料相關的節點，或是有必要知道的節點（如政府或公證人節點），而非像一般區塊鏈那樣廣播給所有節點。也就是說，所有交易的紀錄雖然也是分散儲存於 Corda 網路上的節點中，但大家的帳本內容未必都一樣，帳本有分散但非全員共享，所以其強調是分散式帳本技術，而非區塊鏈。

Corda 採用了類似比特幣 UTXO 的方式來組織它的帳本資料結構，首先，交易的 Inputs 與 Outputs 不是簡單的貨幣，而是狀態（States），每個交易執行智能合約內的程式碼，將給與輸入的狀態轉變為新的輸出狀態來反映業務邏輯的需求，且由智能合約負責檢驗所有的狀態是否符合交易的條款與條件。至於雙重花費這種不實交易則由一個特殊的角色：公證人（Notary），來負責確保。一個 Corda 網路中可包含多個公證人節點，每筆交易的輸出狀態要指定驗證的公證人節點，公證人節點可以檢視過往完整的交易紀錄，故得以提供他們的驗證服務，來確保各筆交易的唯一性，從而避免雙重支付。若有多個公證人節點，它們之間需要透過共識過程來取得一致的決定。下圖簡要勾勒了 Corda 一般交易的流程。

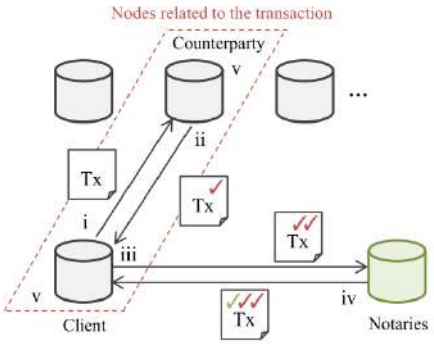

圖 2-2-10 Corda 交易流程圖

來源： JPX_working_paper_Vol20.pdf

主要步驟說明如下：

1.客戶端發送交易給交易對手所擁有的節點。

2.交易對手確認該交易，並於回覆中加入其數位簽章。

3.客戶端也簽署交易，並要求公證節點驗證交易的唯一性。

4.公證節點就其所驗證過的交易與新提交的交易予以比對，如果交易唯一性保持，即簽署此一新交易。

5.交易相關的每個節點執行交易，並將交易結果提交（Commits）給各自的帳本（Ledger）。

綜合以上的說明，我們將各區塊鏈平台的主要差異處摘要如表 2-2-1。

表 2-2-1 主要區塊鏈平台比較表

	Bitcoin	Ethereum	Quorum (EEA)	Hyperledger Fabric V1.0	R3 Corda (DLT)
平台屬性	支付交易	通用性	通用性	通用性	金融業為主
虛擬通貨	比特幣	以太幣	以太幣(名存實亡)	無	無
網路參與限制	公開鏈	公開鏈 私有/聯盟鏈	私有/聯盟鏈	私有/聯盟鏈	私有/聯盟鏈
交易者	半匿名或由鏈外 AP 控管	半匿名或由鏈外 AP 控管	由節點或由鏈外 AP 控管;未來規劃導入 CA 管控	登記制(CA)	登記制(CA)
交易內容	公開	公開	公開或限制	公開或限制分享(Channel)	選擇性分享
共識機制	Mining 工作量證明 (PoW)	(1)Mining PoW (2)PoA (3)將增加 PoS	(1)QuorumChain(Voting) (2)RAFT (3)PBFT	V1.0: Endorsement, Ordering Service (SOLO/Kafka/ SBFT)	交易方相互驗證與 Notary Service (RAFT)
智能合約	簡易功能	有支援	有支援	有支援	有支援

第三章、區塊鏈（分散式帳本）的應用模式與導入規劃

本章節探討企業如何應用區塊鏈以及如何規劃與評估區塊鏈的導入。首先，我們說明三種應用的模式：企業內部流程改善、跨企業組織間的合作以及去中介的新型態營運模式。不論何種應用模式，導入前除了業務流程或營運模式必須有所調整或改造外，整體應用系統的架構也必須有所規劃，才能讓參與各方了解彼此的角色，以利進行各種導入的評估與規劃。所以本章節第二部分將從一個比較抽象的角度來分析區塊鏈應用在建置與部署上的架構性安排，以及各參與方的角色。最後並說明導入區塊鏈應用前，企業組織應該要考量的幾個關鍵面向。文中將混合使用區塊鏈或是分散式帳本技術（DLT），不特別區分其差別。

第一節、區塊鏈的應用模式

對於如何應用區塊鏈技術，我們可以回到區塊鏈的基本功能來發想：讓彼此不完全信任的多方，以某種共識方式，不必透過中介機構或中間人，直接建立、維護與分享可信賴的紀錄。此外，搭配智能合約的功能，這個維護紀錄的過程可以透過程式與外部事件（資料）自動完成。所以我們可以從「多方可直接共享與維護可信賴的紀錄」出發，來建構基於區塊鏈的應用系統。

茲舉一例說明，金融業是高度管制行業，其從業人員都需要取得許多專業的證照，以作為公司內部的考核與升職，或是轉職時的專業憑證。但就人事審查的程序而言，一個主要的課題是：這些從業人員所持有的證照如何判定其真偽？通常為求可靠，都要跟發證機構進行查證。固然，發證機構可以採用電子證書以及網路科技來降低人力查證成本與加速查證流程，但這也仰賴我們對發證機構的信任，相信查證過程不會有人為疏失或舞弊行為（例如：塗改紀錄），而可以順利取得「可信賴的紀錄」。區塊鏈內的資料具有不可竄改的特性，是可信賴的紀錄，如果透過區塊鏈與智能合約來實現證照的查驗，應該更可以讓整個發證與查證的過程，既有效率又可信賴。具體的流程步驟如下(參考圖 3-1-1)：

1.當專業人員通過某項證照考試或要求後，向發照機構的資訊系統申請證書，發照機構進行審查。

2.在確認該人員符合資格後，系統將該人員的相關證照資料（例如：證書的內容經安全雜湊(Hash)函數計算得出的數值），記錄於區塊鏈上。

3.同時取得此筆紀錄在區塊鏈上的交易序號，然後透過資訊系統製作一份電子證書給該人員。

4.電子證書上紀錄著該人員的相關資料，以及那個獨一無二的區塊鏈交易序號。

5.當該人員提出升職或應徵新工作時，可將此電子證書上傳給相關機構的人事部門進行查證。

6.該機構的人事部們就可據其證書的交易序號，到區塊鏈上藉由內容比對來確認此證書的真偽。

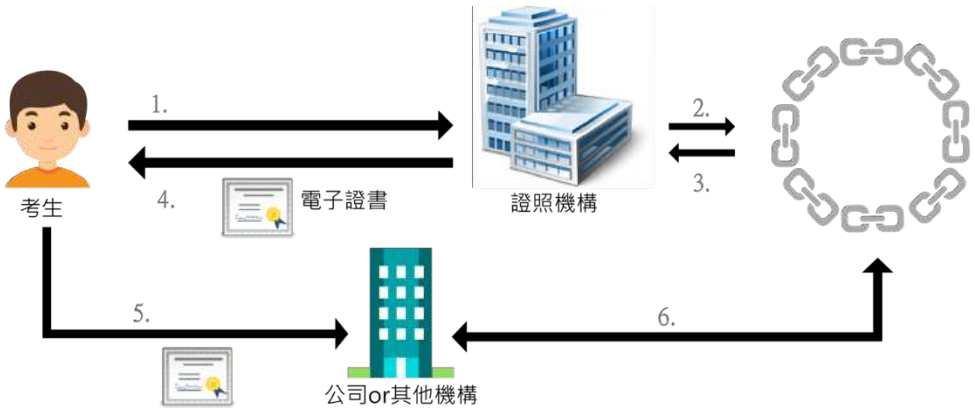

圖 3-1-1 電子證書認證區塊鏈

不僅如此，因為發專業證照的機構不止一家，與其讓各家單獨發放，我們可以擴大範圍，建立一個由多個證照機構組成的聯盟區塊鏈，讓有意願的機構都參與，透過這個聯盟鏈來發行電子證書；在不同證照機構間的證照，也有可能有依賴關係，使得一家機構可能需要跟另一家查證，產生共享可信賴紀錄的需求。其次，改從專業人員的角度，以發行他們的終生證照紀錄證明，而不是僅以單一的證照文件來建構此系統。也就是說，在這個聯盟鏈中，每位專業人員有一張完整的，不分機構或主題的專業證書履歷，記載當事人所取得的各種專業證照。以上的擴充，是從單一機構延伸到多家機構，跨組織之間的共享可信賴紀錄的一個實例。

參考以上的說明與範例，並延伸到區塊鏈去中介的創新金融服務的想法，我們認為發展區塊鏈的應用系統可有三類模式：

(1) 企業或組織內部的流程改善，以提升作業效率並增加參與各方的信任感。此模式尤適合原作業中仍有紙本與人工部分，又需要相當的透明度以及可信賴的紀錄與外界溝通互動。以電子證書為例，發證機構可以透過智能合約將證書紀錄到區塊鏈內，一方面留下可信賴的紀錄，提高證書當事人與使用方的信賴感；另一方面可透過智能合約進行自動查核，提升查證效率。組織龐大的金控公司，或是常需要使用外部資料與客戶互動的保險業，在作業面上的一些流程公司的核保作業與理賠作業也可以採取此模式來運用區塊鏈與智能合約，後面的章節將詳細說明。

（2）跨組織之間的相互作業，透過區塊鏈提供可信賴的共享紀錄，讓組織之間的資訊暢通，並搭配智能合約自動化業務邏輯，達到無縫隙整合跨組織間的作業。通常組織之間缺乏適當的共享資訊平台，以致各種資訊以孤島（Silo）方式散佈組織之間，不僅會重覆也常不一致，需要許多人工協調與對帳工作，效率不彰。若能以區塊鏈提供單一版本的共享可信賴紀錄，將可大幅提升這類的跨組織作業效率。上述的電子證書聯盟鏈就是一個範例，金融業可以運用這種模式的作業非常多，例如銀行之間的聯貸案，或是貿易融資等等。後續的章節將會進一步探討這種應用模式，並佐以個案分析來說明。

（3）應用資通訊科技，搭配區塊鏈優勢，發展新型態的金融服務。網路科技發達，一個網路平台可以很有效率的匯集大量用戶並媒合他們之間的需求與供給，例如：P2P 借貸以及網路互保等新金融業務模式。此類創新通常都需要信任陌生人，但又要同時確保對方的資訊是正確、信賴的。若採用區塊鏈作為底層技術平台，再搭配智能合約事先設定好的業務邏輯來進行交易，即可藉由資訊的共享，創造更多的價值。

本報告後續章節將就各個金融業務主題，探討區塊鏈的應用如何能對相關業務有所助益，或促成創新金融業務，過程中會採用以上三種模式來分析各種實務上的案例。

第二節、分散式帳本的應用架構安排

在第二章，我們回顧了區塊鏈技術的發展概況，也介紹了四個主要區塊鏈平台的功能與特色。但同時我們也說明了目前幾個不同的平台間還是有許多差異存在，不僅在功能上，在應用上也有不同的考量角度。因此，有必要從一個比較高，比較抽象的層級來看待區塊鏈技術，以不綁定平台的角度來做業務應用的發想與規劃。這就是本章節的目的，我們將參考巴塞爾銀清算銀行（BIS）2017 年 2 月出版的一份關於分散式帳本技術的研究報告[16]，說明如何在適當的抽象層級，理解各種區塊鏈平台的技術面設計元素（Technical design elements）與機構面設計元素（Institutional design elements）的特性與要點，以作為後續進行導入規劃與評估的參照依據。因為有不使用區塊鏈資料結構的平台（如 R3 Corda），也因為要拉高抽象層級，本章節將依循該份研究報告，改用分散式帳本技術（DLT），而

[16] Distributed ledger technology in payment, clearing and settlement: an analytical framework. BIS, Feb. 2017.

不是以區塊鏈一詞來進行說明。

基本上，這份 BIS 報告將一個基於 DLT 應用系統的規劃分為兩大構面：技術面設計元素與機構面設計元素，兩大構面的元素選定與搭配後，就構成了一個區塊鏈應用系統的建置安排（Arrangement），或可以理解為系統的配置組態（Configuration），這樣的安排可作為規劃的基底（Baseline），方便後續的進一步評估。以下分別就兩大構面的元素說明。

（一）DLT 技術面設計元素

DLT 的主要目的在於提供「可信賴的紀錄」，所以在規劃 DLT 應用系統時，一個核心的議題就是要在 DLT 上儲存什麼樣的資料（紀錄），以及如何維護與使用這些資料，以及參與各方的的角色與權限。這些面向的規範就是主要的 DLT 技術設計元素。

1.DLT 的紀錄內容

DLT 應用的帳本（Ledger）裡要記錄什麼樣的資料？透過記錄哪些資料可以解決企業內部或跨組織之間的業務痛點？這些資料的範圍、內容與結構是在規劃 DLT 應用系統時的重要基礎，規劃與評估時也必須結合底層 DLT 平台對這方面的支援。

典型以支付為主的 DLT 平台，如比特幣，支援原生的虛擬貨幣，所以它的帳本一定會記錄跟支付與帳戶餘額相關的資訊，這可視為（鏈內）原生的數位資產紀錄。除此之外，DLT 的帳本也可用來記錄其他與應用主題相關的資訊，例如電子證書內容的安全雜湊值，也可以是鏈外的資產資料，例如個人的資產與不動產所有權。不同的平台功能不一，比特幣 DLT 的資料儲存空間與功能都相當有限[17]，但以太坊 DLT 則可支援多種應用系統所需的資料型態，相當彈性。

不支援原生的虛擬貨幣的 DLT 平台，例如 Hyperledger Fabric 與 R3 Corda，則都是透過類似資料庫的機制來儲存各種資料，包含這些資料交易（異動）紀錄，它們的功能與結構存在相當大的差別，但都可支援一般的應用主題，不過由於目前 DLT 的資料儲存功能都還很侷限，不適合儲存大量資料，也缺乏類似關聯式

[17] 比特幣區塊鏈在支付紀錄外，每筆交易紀錄只能額外儲存 40bytes。

資料的結構化查詢語言（SQL）功能，所以在規劃 DLT 帳本內所要儲存的資料時，務必要將這些因素考量進去，必要時可將完整的資料內容記錄在外部的關聯式資料庫，僅將關鍵的資料內容或其雜湊值儲存於 DLT 的帳本內。

除了靜態的資料外，如本報告第二章所述，目前許多 DLT 平台也都支援智能合約，可以將資料處理所需的業務邏輯，透過智能合約一併納入 DLT 應用的鏈內部分來規劃。哪些資料符合應用系統的需求可以記錄到帳本內？哪些事件發生後，智能合約可以依據事先設計的邏輯來處理或產生新的資料紀錄，以及與鏈外的其他系統溝通。例如：處理借貸融資的智能合約就要能定期計算利息[18]或通知外部系統某借貸帳戶逾期未繳息。也就是說，既要規劃所要紀錄的資料外，也要對處理資料的業務邏輯加以識別並納入規劃，視為後續發展智能合約的標的。

2. DLT 內紀錄的更新與共識

DLT 的一個重要特色是紀錄（帳本內容）的更新是透過一個集體共識的過程來完成的，例如，比特幣 DLT 的共識採用的是工作量證明（PoW）的方式，由全體節點一起執行，執行完畢後所有節點會同步更新各自的帳本，使得大家的帳本都有一致的內容。圖 3-2-1 以支付交易為例（A 付 X 給 B），展示這樣由全體共識並共享帳本的 DLT 流程示意圖，說明如下。

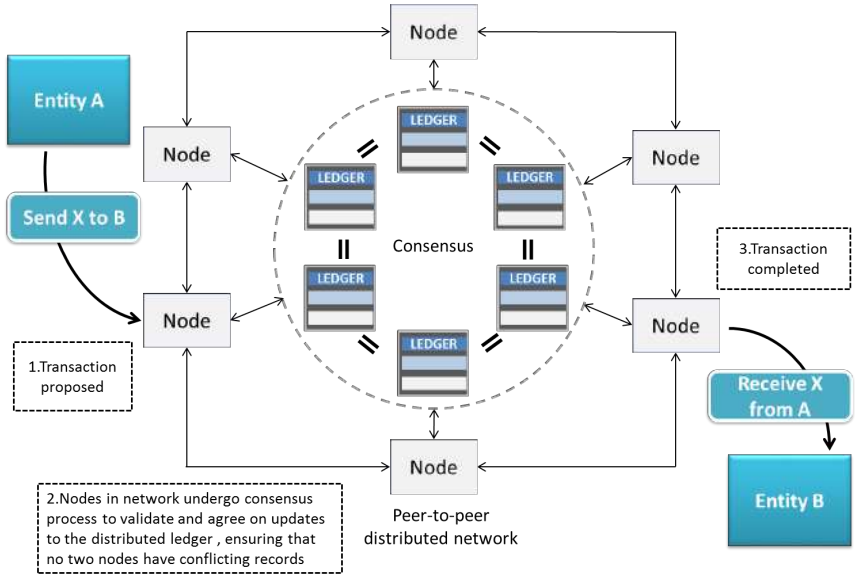

圖 3-2-1 全體節點共識更新帳本的流程

來源：BIS 2017，本研究繪製

[18] 定時功能通常可視為外部 Oracle 提供的服務，按時觸發指定的智能合約以執行其業務邏輯。

第一步：開始時，由 A 提出交易要求，送一筆錢 X 給 B。透過一個 DLT 節點的協助，將此筆交易用 A 的私鑰簽章後，上傳到 DLT 網路。

第二步：這筆交易會廣播傳給 DLT 網路所有的節點，其他節點會藉由 A 所提供的簽章資訊來做交易認證，確認 A 的資料是否正確，包含確認 A 是否有足夠的款項做交易。當交易驗證完成後，就會透過一個共識過程（例如 PoW），讓所有節點確認，再將此筆交易新增到 DLT 的帳本內。

第三步:當所有節點都將自己的帳本跟新到最新狀態後,此筆交易才算完整,而未來的交易也會經由此筆交易的區塊繼續延伸，包含 A、B 雙方的資產狀態與交易紀錄，都會被永遠記錄在 DLT 的帳本上。

比特幣使用的 PoW 共識方式有耗資源、費時與交割最終性（Settlement finality）[19]的問題，所以如第二章第二節中提到的，比特幣之後的 DLT 平台，陸續發展了許多具不同特色的共識機制，例如：PoS、PoA、RAFT 與 PBFT 等。甚至有些 DLT 平台本身就會提供一種以上的共識機制，例如 Quorum 目前提供了三種不同的共識機制，所以在規劃導入 DLT 時，必須對這些不同的共識機制有所了解，並依應用需求進行評估，選取適用的機制。以下就幾個面向說明這些共識機制的特性與使用時機：

- 節點數量：如果參與共識的節點數量不多，只有幾十個甚至更少，不建議採用 PoW 之類的共識機制，應考慮其他的機制。否則，可選擇 PoS 替代 PoW。
- 節點的信賴度：如果參與共識的節點彼此都可以信賴，不會欺騙造假，那可以採用 RAFT 之類的共識機制，不僅效能較好，且可以在低於半數節點有故障的情況下進行共識。否則，要處理不信賴節點就要採用比較複雜的拜占庭容錯共識(如 PBFT)，因為這類共識機制不僅可以處理節點故障的問題，還能在少數造假節點參與的情況下，進行大多數節點之間的共識，但需要比較長的時間完成共識。
- 帳本更新效能：一般而言，要在為數眾多的節點之間取得共識後更新帳本，在效能與吞吐量上一定有所限制。像比特幣 DLT，平均一秒鐘只能處理 10 個以內的交易。如果參與共識的節點數量很少，彼此之間又有

[19] 意指先前交割過的交易，有可能因帳本被整個改寫或分叉（fork）而取消。

很高的信賴度，所運行的環境很可靠也有安全的防護，那可考慮使用比較單純又高效能且會節點輪流決定的共識機制，像是 PoA 之類的。

3. DLT 節點的技術角色與權限

DLT 的共識機制決定各節點如何更新帳本內容，節點數量多寡會影響共識機制的選取與交易吞吐量，所以一個基本的問題是：是否所有的節點都需要參與更新帳本內容的共識過程？以比特幣而言，它的 DLT 是以公開無監理方式運行的（公有鏈），所有的節點都可以參與共識；但如果是多間銀行之間的跨行聯盟鏈，以非公開的方式運行，那就不見得每家銀行都需要參與共識，可以採階層式，制定規則推派代表來進行帳本內容更新的共識。下圖 3-2-2 是取自日本 Mizuho 金融集團聯合其他機構於去年進行的一項跨行支付 DLT 概念驗證[20]，其中只有四家銀行是所謂核心節點（Core nodes），負責執行共識的工作，其餘節點成為一般應用節點（Application nodes），可以發動交易，但不能參與帳本內容更新的共識。

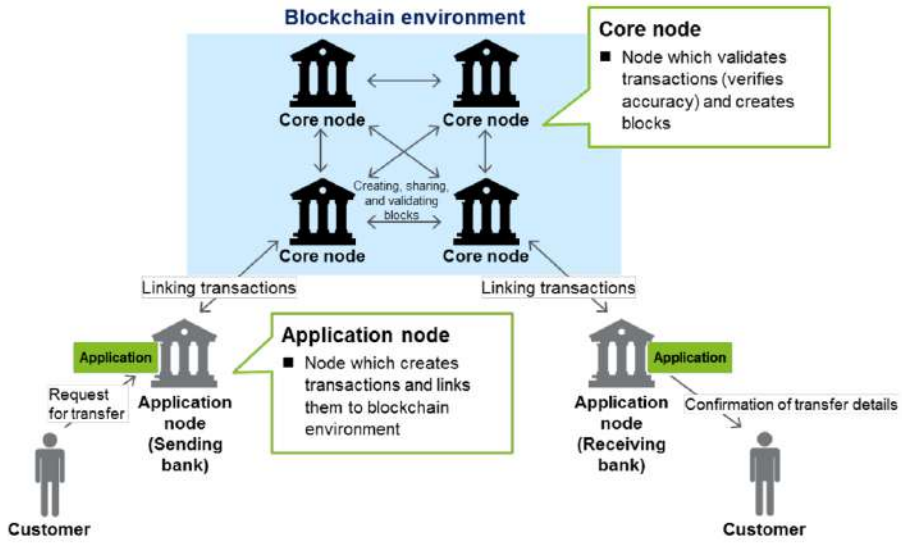

圖 3-2-2 階層式區塊鏈網路案例

來源：Mizuho et al., Blockchain study group

更廣泛來看，在非公開的 DLT 環境中，讓參與的節點扮演不同的技術角色，

[20] Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation, Blockchain Study Group, Mizuho Financial Group, et al., Japan, Nov. 30, 2016

區別彼此的權限，實有必要。以下是 BIS 2017 DLT 報告中列出的一些常用的技術角色與說明（圖 3-2-3：僅由部分節點間進行共識以更新帳本）。

- 系統管理員（System administrator）:

負責整體 DLT 系統的運行與相關服務的安排，包含公證（Notary）、協調爭議、設立節點間應依循之各種標準、法遵與監管報表等，通常擁有最高權限。

- 資產發行者（Asset issuer）:

可在 DLT 網路中發行新的資產，屬於一種特殊的權限。

- 提議者（Proposer）:

可以提出交易或是資料異動要求的節點。

- 認證者（Validator）:

有權參與交易內容驗證，與帳本更新共識過程的節點。如上圖中的核心節點。

- 稽核員(Auditor):

只有查看帳本內容的權限，但無權對帳本做任何異動

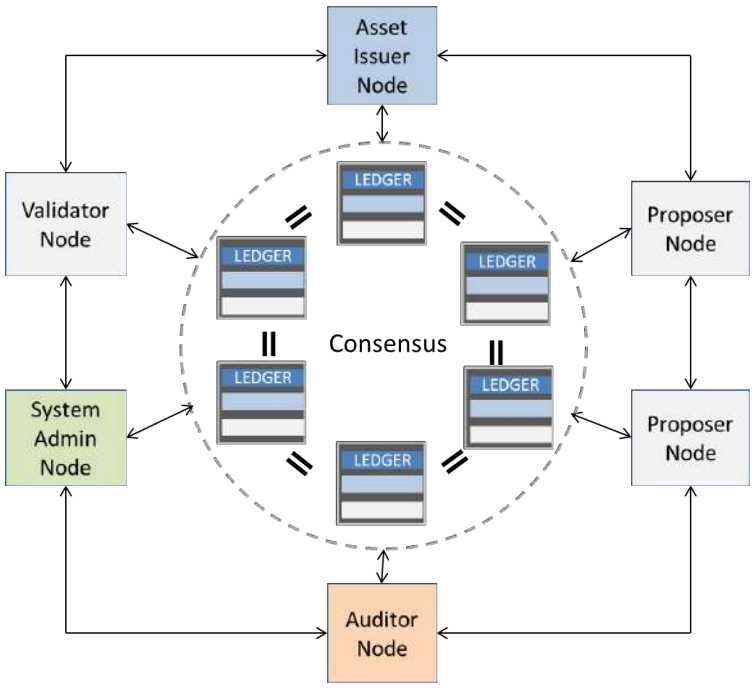

圖 3-2-3 DLT 系統中不同的技術角色

來源：BIS 2017，本研究繪製

4. DLT 紀錄的分享範圍與保護：

除了以上各種技術角色的權限劃分外，也有就帳本內容的分享與保護加以限制的權限需要，不允許每個節點都能檢視所有的帳本紀錄。例如：R3 Corda 就積極主張，所有的 DLT 交易都只應該開放給參與交易的各方以及監管單位檢視，實作上，Corda 的帳本分享範圍不是像比特幣或以太坊那樣廣泛，而是限縮於交易參與方與監管單位的節點，所以在 Corda 平台，每個 DLT 節點的帳本內容是不一樣的，除了監管節點，各自都只能存放自己有參與的交易紀錄。Hyperledger Fabric 平台自 V1.0 版以後，推出 Channel 機制，節點間若有限制交易紀錄分享的需求，就可以定義不同的 Channels，來限制交易紀錄的分享對象，只有隸屬同一 Channel 的節點，方可取得彼此的交易紀錄，甚至連智能合約（Chain-code）的部署，也是以 Channel 為標的。所以一旦確定了 Channel 的架構後，若有跨 Channel 的需求，就無法處理[21]。

以上為使用限制交易紀錄分享對象（Selected data sharing）的方式來保護交易內容的作法，Quorum 平台則是採用加密私有交易內容來達到限制紀錄分享的目的。加密過的交易內容只有參與交易的各方(可包含監管節點)才能解密檢視。所以在 Quorum 底層資料分享看似保持以太坊的廣播方式傳送給所有節點，但私有交易會經過一道額外的加密程序特殊處理，以保護交易內容不外洩。這樣的作法應該跟 Quorum 是基於以太坊的架構有關，雖然是一個具高模組性的擴充架構，卻也因此可能發生部分參與交易驗證的節點，會無法看到區塊裡的某些交易內容，而無法完整驗證該區塊的正確性，從而有可能發生重覆支出的交易沒被檢驗出來，這部分未來可能需要搭配零知識證明 (Zero knowledge proof)技術來克服。

（二）機構面設計元素（Institutional Design Elements）

在規劃 DLT 應用系統的整體組態安排時，除了技術面的設計元素外，我們也要從機構面，就 DLT 的運作與監理兩大設計元素加以考量與評估。這裡牽涉到參與 DLT 運行的各組織之間的權利與義務，如何管理 DLT 的維運，如何變更組態安排的程序等等。

[21] Page 15 and 16 in JPX Working paper 20, The trend in exploring the use of DLT in capital market. Sept. 14, 2017.

1.組態安排的運作（Operation of the arrangement）

一個 DLT 系統的有效運作的前提是組態安排的管理，這牽涉很廣，如前一章節陳述的各種技術面設計元素，像是該採用哪個 DLT 平台，使用哪種共識演算法，參與者的技術角色設定，這都需有專責的管理機構。這就是組態安排在機構面的一個重要設計元素：由單一或是多個參與機構來負責管理組態安排。如果只由一個單一機構負責 DLT 的組態安排管理，極端的情況可能是，這個機構負責建置與維運所有的節點，甚至由它來負責帳本內容的更新，雖然會很有效率，但這已近乎是傳統 FMI 的中心化系統建置方式。通常這些應由多個機構來負責，包含帳本的儲存與更新，以及組態安排與系統維運的管理等。這些機構事先應制定一套詳細的規範，明定參與方的權利與義務以利共同運作這個 DLT 系統。至於日常維運的執行細節，可以交付單一機構，或是第三方來執行。

2.DLT 的取用管理（access to the arrangement）

一個 DLT 系統的取用可以是完全開放與公開，毫無限制的（Unrestricted），任何個人或組織都可以隨時加入或退出這個 DLT 系統，各節點之間並不一定能辨識對方身份，也都沒有技術角色的差別，共同參與帳本的維護。比特幣公有鏈就是一個這樣的範例，所有的組態安排都是透明公開的，要變更也是在線上進行討論的才加以實施的。2016 年間在以太坊上廣受矚目的分散式自治組織（Decentralized Autonomous Organization, DAO）更是一種特別型態的開放組態安排，它們的運作與管理是採用智能合約來實現的，採用的是鏈上的管理規則。相反的，如果取用是有限制的（Restricted），那這個 DLT 的系統就可有一套規則來審核參與者以及規範參與機構的角色等等，而且這些規則，可以與鏈下的法律實務結合，對違規的參與機構行使訴訟。

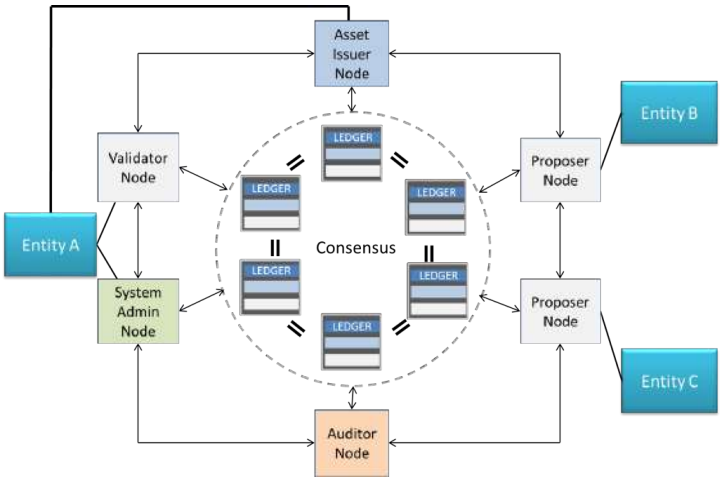

圖 3-2-4 DLT 系統安排中設定參與組織不同的技術角色

來源：BIS 2017，本研究繪製

企業或政府組織建立的 DLT 系統應該都是會有取用限制的。建立這種有限制的 DLT 時，組態安排的規劃就會包含對參與機構設定適當的技術角色的部分。以圖 3-2-4 為例，每個節點都可擔任其中一種以上的角色，每個角色也可能由多個節點來擔任。例如，圖 3.2.4 就是一種組態安排的範例，其中的 Entity A 就同時擔任系統管理員與驗證者的角色，Entities B、C 則是擔任提議者的角色，可以發起交易或是增加新的區塊，但是區塊的驗證與要透過 Entity A 來執行。

根據不同的技術面與機構面設計元素的選取，我們可以獲得四大類的 DLT 的系統組態安排，如圖 3-2-5 所示，最左邊的是僅由單一機構負責組態安排的運作，並且對取用有限制的 DLT，但仍可以區分技術角色，帳本的驗證與共識也可以由單一或多方決定，有的文獻將這種組態安排稱為私有鏈。如果是由單一機構決定，那就是目前的 FMI 的運作模式。最右邊的則是目前公有鏈的運作組態，既沒有取用限制，所有的多方參與者也沒有技術角色的區分，帳本與共識。居中的兩種組態安排是有取用限制的，但不一定會有技術角色的區分，帳本的驗證與共識也可以由單一或多方決定，這兩種組態安排常被稱為聯盟鏈。

Description of arrangement	One entity maintains and updates the ledger (for example, a typical FMI)	Only approved entities can use the service; entities can be assigned distinct restricted roles	Only approved entities can use the service; entities can play any role	Any entity can use the service and play any role
Operation of the arrangement	Single entity	Multiple entities		
Access to the arrangement	Restricted			Unrestricted
Technical roles of nodes	Differentiated		Not differentiated	
Validation and consensus	Within a single entity	Within a single entity or across multiple entities	Across multiple entities	

圖 3-2-5 DLT 系統安排的幾種組態內容。

第三節、導入分散式帳本技術的考量[22]

顯而易見的，DLT 作為一種平台技術，它的導入會對企業組織所牽涉到的部門會產生相當大的改變與影響，所以在導入前，即便是概念性驗證的 PoC 也應有詳細的評估與規劃。本研究參考 BIS 2017 年的 DLT 報告，以及世界各國的一些 PoC 案例，整理出一些考量面向，供金融機構參考。我們聚焦在範圍界定、目標設定與評測，投入成本的評與安全與風險等幾個面向，並且參著上述的組態安排中的各項設計因素，藉此讓 DLT 導入的相關單位得以開始熟悉那些設計元素與相關議題。

（一）界定可掌握的主題範圍

任何的專案都要審慎界定範圍，以確保專案順利執行，DLT 這類新科技的專案更是如此。首先可以從企業的現況思考起，有哪些作業是有改善空間的？這些改善空間是否可以連結的 DLT 的特色與優勢？思考過程，一樣可以套用本章第一節的三種型態來考量：企業內部，跨企業組織與新型態業務。以 DLT 的兩大優勢（提供可信賴的紀錄與智能合約的自動化作業功能）來發想。例如：我們內

[22] 現階段因為 DLT 的技術還在發展中，所謂導入主要仍以實驗性 PoC 為主，而非實際上線。

部的作業流程中，是否仍有紙本與人工作業可藉由 DLT 的導入可以改善的？我們與上下游業務夥伴之間的作業流程是否也有類似的問題，可以透過 DLT 的導入來解決？最後，可以進一步透過去中介或是 P2P 模式發展新型態業務嗎？

有了可改善或創新的業務主題後，範圍的界定就是下一個重要的評估項目。首先，我們可以從價值鏈中識別出受影響的單位與流程，選出一定範圍的參與單位以及作業項目與流程，並訂定適當的實驗目標。例如：導入 DLT 於跨行支付系統時，我們要以小額支付還是大額支付為對象？目前 DLT 的交易處理速度能應付小額支付的吞吐量嗎？目前世界各國還都是以大額支付為主。其次，要聚焦於結算作業，還是連清算作業一並納入實驗導入 DLT 的範圍？這裡要考慮的因素有哪些？實驗目標為何？是否可分階段進行導入實驗會比較可行？

DLT 在跨企業組織之間的作業可以有很大的發揮空間，但如果牽涉到的組織種類與數量愈多，要建構的生態權就愈複雜，這時候非技術性的因素就會更多更難以克服，往往會無法說服大家一起實驗 DLT 的導入。因應這種困難，可以有兩種作法。一是選取可行的導入實驗目標，以凝聚參與者的共識，一起投入實驗。例如：日本 JPX 過去一年多的期間所進行的兩個 PoC，都是以 OTC 證券交易的結算與交割為實驗主題，廣邀相關金融機構參與，包含了發行企業、銀行、集保機構（CSD）與集中交易對手（CCP）等，其中也有中介機構。他們的目標並非要取代這些中介機構，而是著眼於如何透過 DLT 的可信賴紀錄的共享，以及智能合約自動化功能，來提升參與機構間的作業效率，以及節省人力成本。採用務實的目標來凝聚參與者，是比較可行的方法。

另一種作法是減少導入實驗參與的對象範圍。例如：貿易融資（Trade finance）是銀行基於客戶的交易，提供客戶資金或促進貿易行為的一種授信服務。但其作業過程中要處理各類單據，以確認客戶交易的真實性，這些單據都來自於不同的單位，例如海運公司、保險公司、貨運商及買賣方，銀行需要仰賴大量的人工來檢查這些紙本單據的正確性，不過人工的檢查時間較久，也無法完全杜絕人工出錯，或客戶假冒單據的可能性，所以非常適合導入 DLT，實驗無紙化的流暢作業。但這裡會牽涉到非常多的參與者，要進行流程改造將會是一件非常複雜的工作。進一步分析，可以發現這裡面的作業可依參與對象，概分為融資面、海關申報面與物流運送面。所以若從銀行的角度來看，DLT 的導入實驗可先鎖定融資面的作業，將參與對象限縮到銀行與貿易雙方的客戶，從而減少範圍，降低導入的複雜度。待融資面順利實驗完成後，再分階段處理其他兩個作業面的需求。

此外，也可以分階段來界定主題對象與範圍。以巴西中央銀行為例，他們的 DLT 實驗專案在 2016 年 9 月啟動時，先執行第一階段的計畫，目的是挑選應用專案及測試演算法，以及進行 PoC 測試。最初的提案包括身份認證管理、區域性貨幣支付系統(SML)、互惠支付及信貸協議(CCR)、交易結算替代系統(SALT)等，而最後決定選擇 SALT 來進行第二階段的主題。SALT 主要是用來當作 RTGS 系統的備援，當 RTGS 系統無法運作時，SALT 可以取代其主要的核心功能。

（二）目標的設定與評測

有了主題與明確的範圍之外，清楚的目標是專案的另一成功要素。由於目前導入 DLT 多半是實驗性質，所以通常目標的設定首重功能性，評估原來既有作業的各種功能是否可以在更換為 DLT 平台後，仍然能順利執行。這必須詳列要評估的功能，在實驗或導入過程中一一加以評估。

除了功能外，還有許多非功能性目標要考量，例如，跨行轉帳或是證券交易相關業務，對於執行效能都有一定的要求。在設定目標時，就必須將共識機制列為重點評估項目，把交易的吞吐量納入為評測目標。常見的資訊系統非功能需求眾多，可視需要列入評估目標之內。例如：系統可用性（Availability）、延展性（Scalability）、安全性與維護性等等。此外，由於 DLT 平台會分享帳本資料，所以在資訊安全外，也可以將隱私保護納入目標，設定一些保護的對象與內容範圍予以評測。

以下為日本 Mizuho 金融集團等公司所組成的團隊，所採用的 DLT 技術面導入評測面向[23]：

[23] Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation, Blockchain Study Group, Japan, Nov. 30, 2016.

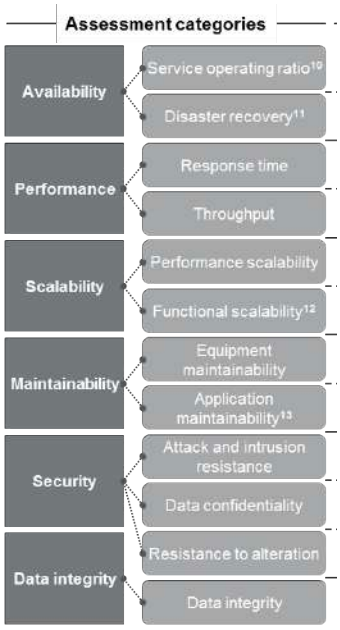

圖 3-3-1　DLT 技術評估面向，非功能性範疇。

來源：Mizuho 金融集團報告 [22]

再進一步，可考量是否有可能透過 DLT 的使用，達到提升作業效率的目標。作業效率的提升通常從加快整體流程的處理速度著手，可藉由價值鏈的拆解來分析作業流程，哪一部分的運作效率低、成本較高、重複性高，這些因素都是可以藉由 DLT 的可信紀錄與智能合約自動化來取代的潛在部分。但作業本身的複雜度也必須加以考量，先從簡單又明確的流程步驟來進行 DLT 導入的實驗，不僅效果會比較容易彰顯，成功的機率也比較高。

處理紙本單據的人工作業是常見的效率提升對象，如果這些紙本單據可以順利數位化並轉成以可信賴的紀錄儲存於 DLT 的帳本內，將可大幅減少人工作業錯誤以及人力成本。尤其是必須透過值得信賴的第三方提供的共享可信賴的紀錄，例如：保險核保與理賠作業所需的的單據，以及貿易融資中的信用狀等，都是這樣的範例。導入規劃的同時，就要選定目標，設定評測與衡量指標，才能有效評估導入的效益。

（三）投入成本的評估

在考量效率的同時，也要考量是否符合成本，畢竟人力與一些作業成本可能因導入 DLT 而節省掉，但 DLT 本生所衍生的成本必須加以考量。雖然根據一些

國外 PoC 的經驗[24]，部分 DLT 的導入成本很難有效計算，但預作必要的考量與規劃仍然是不可或缺的。例如：可以從企業的既有流程來評估，首先，先找出 DLT 能取代的部分，就這部分的開發成本、營運成本與維護成本來當成評估的參考點，再加上為了 DLT 而投入的硬體、軟體、新舊流程轉換成本(例如人員訓練、區塊鏈導入顧問等)，進行評估。

日本證交集團 JPX 與 Mizuho 金融集團的 DLT 驗證報告[22,23]，都包含了 DLT 的建置成本與營運成本的評估，並與現有的系統比較。他們所採用的成本因子類似，不過 Mizuho 金融集團的因子比較詳細一點，如圖 3-3-2 所示。成本因子分為兩大類：建置成本與營運暨維護成本，建置成本又細分為應用開發、中間層、作業系統〈與硬體四小類。根據兩個機構的評估，DLT 的各項建置成本有可能比現有業務系統的低，所以營運暨維護的成本也可能降低。但對應用開發成本能否降低，兩者的結論都認為整體的開發成本可能無實質差異。雖然有這些國外案例的參考，個別機構仍應就個案內容、自身的狀況與本地的成本結構進行評估，才能比較完整的掌握導入 DLT 的成本效益。

導入 DLT 的業務若是新的項目，在成本的評估上要比較的對象，就不是現行業務系統，而是採用不同的平台與技術，可能是 DLT 也可能不是。

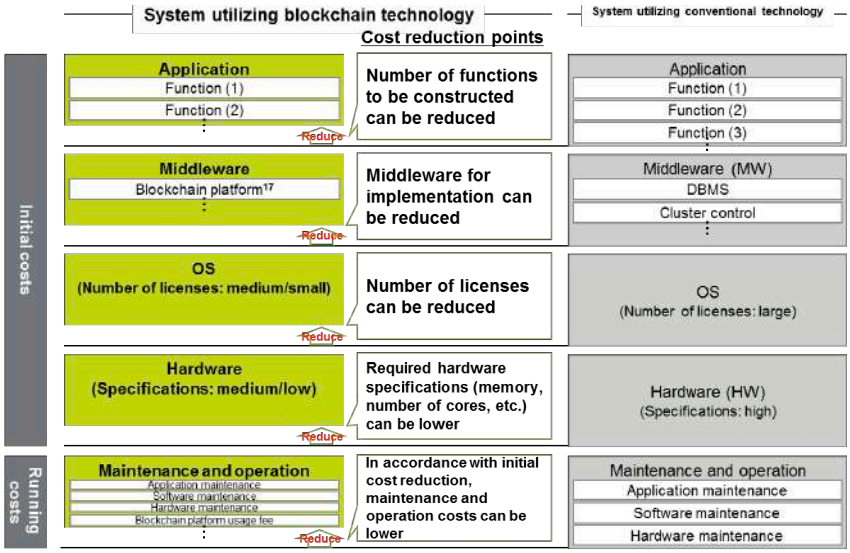

圖 3-3-2 導入 DLT 個案的成本分析比較。

來源：Mizuho 金融集團報告。

[24] A. Santo, et al., Applicability of Distributed Ledger Technology to Capital Market Infrastructure, JPX Working paper No. 1`5, Aug. 2016.

（四）安全與風險

DLT 平台本身雖然都有相當的安全性，但它畢竟還是一項新興且在發展中的技術，需要評估可能會有很多尚未考量到的風險，例如營運風險、法律風險以及如何管理的問題。

在營運風險方面，DLT 應用系統相較於一般應用系統多了一些要考慮的面向，例如：公私鑰或數位憑證的管理、資料隱私需求以及智能合約。DLT 的交易都需要數位簽章的保護與確認，在規劃開發 DLT 應用時，對於如何管理與保護公私鑰，必須及早準備，要將私鑰遺失或毀損時的情況納入考量，建立管理與應變機制。概念驗證性系統或許可以免除發展這些機制，但可以將這些機制列入評估，作為將來發展實際系統時的參考。如前所述，不同的 DLT 平台有不同的資料隱私機制，各有特色與限制，如果因其他因素選選擇了特定的 DLT 平台進行實作或驗證，無法有適切的隱私保護機制，那就要發展替代方案，以補強隱私保護部分。

DLT 應用系統的一大特色就是如何利用智能合約來調整現行的作業流程，進行自動化作業。但當所有流程都自動化後，就需要考量如何在執行過程中避免錯誤或惡意的執行程序，導致交易失敗或是其他風險產生。如何有效測試或驗證智能合約的執行是一關鍵，尤其是當例外發生時，智能合約或是搭配的系統是否仍然能有效運作，也是必要的檢核項目。

此外，一般系統面的營運風險可以從以下幾個面相切入探討：系統的相容性與穩定性、大量資料量下的處理能力，例如支付系統，可能就要考量同時處理大量的交易資料與維持穩定度的問題，還有在顧客付款時與不同商家、支付商的系統相容性、安全性的問題。DLT 應用系統通常無法獨立運作，必須跟現有系統介接，很多營運上的風險就來自於介接部分，例如：介接系統遭到分散式阻斷攻擊（DDoS），或是因不明原因無法運作時，DLT 系統該如何因應，是否有制定災難回復程序等。

法律風險部分，從外部的角度，最重要的一點就是符合法規，一個很基本但不見得容易的議題是在於相關法規的釐清，從眾多法規中識別出，當使用 DLT 技術後，哪些法規是真正有影響、有衝擊甚至抵觸的，然後才容易找出解決方案。例如：如果以 DLT 智能合約的數位簽署交易取代書面的約定與簽署，是否具有

法律效用？此外，對於參與 DLT 運作的各個參與方，彼此之間的權利與義務如何界定？是否有法律約束力？當有爭端時，協調解決機為何等等，這些都是需要留意的法律議題與風險。其次，當所要發展的 DLT 應用系統是跨國的，例如跨國匯款，這時候法律層面的考量將會更複雜。

4.DLT 的運作方式

管理面主要是指 DLT 平台中的參與者管理。如果 DLT 應用系統的使用者是來自不同組織，是以聯盟鏈的形式運作，那首先就要從跨組織的角度來思考如何進行有效的管理。基礎的工作包含制定聯盟的組織章程，界定聯盟成員的資格、角色與權利義務等。這些工作會連帶影響到各成員技術角色的指定。其次，聯盟的成員必須對如何進行 DLT 平台的建置與維運事宜的決策達成共識，並制定解決爭端的規則，以避免決策風險與無法問責。因為 DLT 應用系統的開發過程中，很可能有一些智財權的議題會出現，及早針對這類議題進行成員間的討論並形成共識，將有助於聯盟的運作。

除了這些一般的管理外，DLT 的技術管理也非常重要，這包含非常多的開發與維運面的議題，不容輕忽。以下列舉一些應注意的議題供讀者參考。如果 DLT 平台不是委由單一機構統一管理，當系統軟體因資安問題或錯誤必須更新時，如何要求 DLT 的各個節點進行一致且同步的版本更新？少數節點若未能配合進行軟硬體更新，有可能危害到整個 DLT 平台的正常運作。DLT 資料的備份是否有落實執行？雖然 DLT 的帳本於節點間自動複製，看似不必有備份之需求，但實務上這存在極大的風險。首先，支援選擇性資料分享的 DLT 平台就會有一份交易資料只有少許交易相關節點有儲存的特性，一旦某個節點的資料出了問題，未必能順利從少數其他節點取得資料進行還原。其次，DLT 應用系統若採用階層式節點架構，對於不參與帳本分享的應用節點而言，如果它們上一層的核心節點如果出了問題，帳本資料遺失，那旗下的應用節點在還原資料時難度更高。

不同的產業都有不同的管理重點，例如金融相關的行業，考量的就是 Know-Your-Customer(KYC)、反洗錢(Anti-Money Laundering)、反恐怖主義金援(Counter-Terrorist)，而此部分可以從區塊鏈的節點權限切入，不同的形態的區塊鏈有不同的權限劃分方式，若安全性需求較高，則可以設立較多限制，例如金融體系可能就要有加入區塊鏈網路的限制、節點的使用帳本的權限限制，而同時所有資料都會由相關監管單位來審核，進而達成全面性的管理且符合現下業務流程的運作模式。

第四章、區塊鏈在支付系統之應用

第一節 支付系統介紹

（一）支付系統概要

支付（payment）為金融活動的基礎，負責處理有關貨幣價值轉移的系統，不論是紙鈔、信用卡、手機支付，均須經過支付指令的傳遞、交換、處理與清算的過程，整個交易才算完整，其構成要素包含系統參與者、網路協定、法規、市場慣例等。本報告的主題為區塊鏈之應用，在支付上著重於結算與清算的處理，故將聚焦於「跨行支付」與「跨境支付」。

根據中央銀行編印的中華民國支付及清算系統報告，支付的活動分為大額支付、零售支付兩類：

- 大額支付(Wholesale or Large-Value Payment)

一般而言大額支付大多處理金融市場活動相關之支付，如證券市場、外匯市場交易之支付活動。雖然稱之為大額支付，但通常並未對透過該類系統處理之各筆支付金額設定限額。此類交易金額多較為龐大，通常具有清算的急迫性，若未能立即處理，可能會導致系統性風險，進而影響整體金融市場的穩定。

- 零售支付(Retail or Small-Value Payment)

零售支付以個人或企業部門零售交易之價款收付為主，此部分的交易雖沒有大額支付的清算急迫性，但因為交易種類繁多且交易筆數較多，若支付的系統出問題，可能會影響到資金收付效率與消費者的權益。

另外，支付系統的重要作業為結算（clearing）與清算（settlement），這兩部分跟區塊鏈的應用高度相關。清算作業依支付時點與方式不同可概分為定時淨額清算系統(DNS)、即時總額清算系統(RTGS)，以及混合清算。

- 定時淨額清算系統(Deferred Net Settlement, DNS)

定時淨額清算系統是 1980 年代最常採用的清算機制，係將支付指令儲存在跨行支付結算系統[25]，當支付指令被系統接受後，並未即時辦理清算，而是累積

[25]在台灣是由財金資訊公司、票交所、聯卡中心承辦相關業務。

彙集在中央處理器，待營業日中指定時點或營業日終，以整批作業方式結計參加單位間雙邊或多邊淨應收或淨應付差額後，辦理清算。雖可降低參加單位間整體的清算金額，以節省流動性的需求。然而，最終清算效力只在營業日中指定時點或營業日終發生，若是有參與單位無法履行支付義務，則所有已處理的支付指令被退回重新結算，可能導致其他參加單位面臨清算風險。

- 即時總額清算系統(Real-time Gross Settlement, RTGS)

即時總額清算系統自 1990 年代後期開始為許多國家採用，與定時淨額清算系統不同的是，RTGS 接受所有支付交易採連續即時不延遲、以總額為基礎之逐筆交易進行處理與清算。若參加單位的清算帳戶有足夠餘額或可用的融通額度，則每筆支付指令於進入系統後即執行清算，清算完成的交易即不可撤銷，亦即具有最終清算效力，可有效降低參加單位的清算風險，但也使得參加單位的流動性需求增加，故央行通常會提供一些流動性配套措施，以協助系統的正常運作。

若參加單位的清算帳戶沒有足額流動性時，由系統將支付指令退回發送單位，待清算帳戶有足夠餘額時，再由發送單位重新放行，或者由系統將支付指令暫存於中央處理器，待清算帳戶餘額足夠時再予以執行。

- 混合清算

近年來大額支付系統都改採用混合清算機制。當支付指令進入系統後即累積彙集於中央處理器，在營業日中持續不斷或頻繁地將參加單位發送的支付指令相互抵銷，只要參加單位清算帳戶餘額足夠支付抵銷後的淨應付差額，隨即執行清算，清算完成的交易即不可撤銷。未能清算的支付指令則暫存於排序等候機制，等待下一回合的抵銷與清算。

藉由淨額抵銷，混合清算機制對流動性的需求較 RTGS 機制為低，而且每一回合淨額抵銷後，隨即進行淨應收、淨應付差額的最終清算，亦較 DNS 機制更能降低清算風險，兼顧 RTGS 安全性高與 DNS 節省流動性需求的優點。

（二）台灣支付系統介紹

台灣目前跨行支付結算系統由兩大部分組成：央行同資系統與財金跨行支付結算系統，我國央行與財金公司均提供跨行支付活動，央行同資系統負責大額支付，財金公司則提供零售支付服務為主。整體運作流程大致如圖 4-1-1 所示。財

金跨行支付結算系統辦理金融機構間之跨行支付服務。為協助財金公司跨行清算作業之順利進行，中央銀行同意各金融機構在央行開立「跨行業務結算擔保專戶」之基金，作為逐筆結計跨行支付之擔保，提供金融機構即時性之跨行支付結算服務。各金融機構於營業日開始或日中，自其準備金帳戶撥轉資金至「跨行業務結算擔保專戶」，供當日跨行支付所需。俟營業日終，除留存部份餘額供 24 小時營運的 ATM 使用外，剩餘金額均從各金融機構的「跨行業務結算擔保專戶」回撥資金，俾央行辦理日終清算。不僅方便金融機構集中管理流動性，亦大幅提高清算交割之安全性。

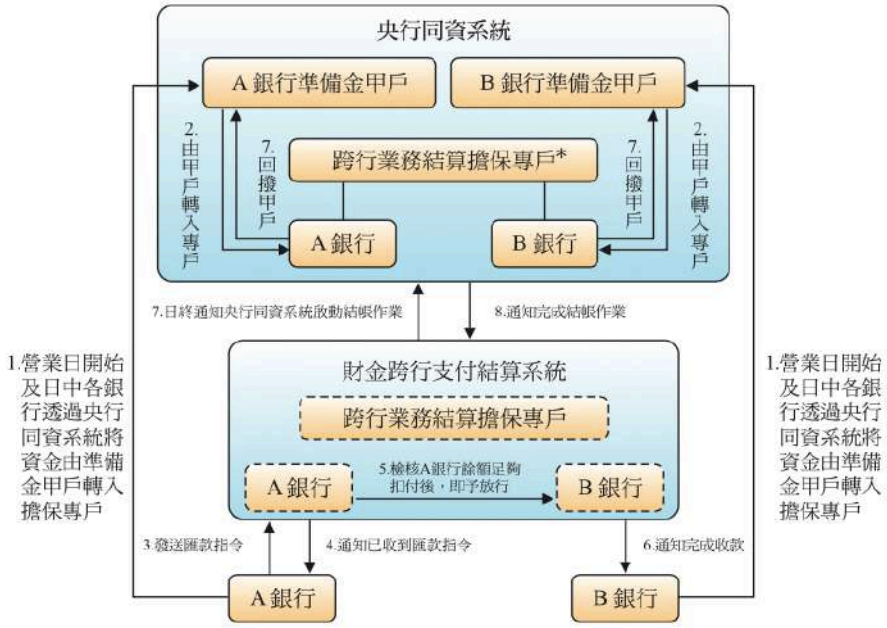

圖 4-1-1 財金跨行支付結算系統之清算流程

來源：中央銀行，中華民國支付及清算系統（民 98）

民國 91 年 9 月央行同資系統全面採行 RTGS 機制，金融機構間之支付交易採逐筆即時清算，每筆支付交易指令於轉出行帳戶內有足夠餘額或可融通額度時，隨即辦理清算，清算完成之交易即不可撤銷，有效阻隔不足額扣付之支付交易進入系統，避免導致系統性風險。

第二節 應用區塊鏈技術於支付系統

區塊鏈藉由多節點參與達到分散式且去中心化、參與節點之間共享帳本及交易無法篡改值得信任的優勢，使得支付過程直接由一方發起，並支付給另一方，不需要透過中心化的第三方機構。區塊鏈的分散式帳本將支付指令儲存為可信賴

的紀錄，作為結算與清算的依據，進而改變結算與清算的經濟活動。具體而言，如果每個參與支付體系的機構都擁有同一份帳本或共享彼此交易的紀錄，原本各金融機構需經由財金跨行支付結算系統提供即時性之跨行支付結算服務的流程可用區塊鏈來做改善。例如：透過區塊鏈上各個參與機構建立共享帳本，直接做交易的結算，再交由央行同資系統做清算。參與機構與央行共享帳本的資料中包含交易金額、交易雙方帳戶、金流流向等。未來區塊鏈技術成熟後，有可能因此增加結算與清算的運作效率外[26]，也同時提昇央行在金融市場經濟活動的監管力度。

如上述提到，支付的方式有分為大額支付、零售支付，故於應用方面，則有不同的考量因素，適用區塊鏈的程度也不同。以大額支付而言，因為金額大，交易數量小，所以使用區塊鏈的分散式帳本需要著重考量客戶隱私、交易安全；但在零售支付部分，雖然金額小，但交易數量多，且交易頻率高，因此區塊鏈就會面臨到難以支援高頻交易的困難。由於本研究只聚焦於單純的跨行結算與清算，而不論是大額支付或是零售的小額支付，其背後的邏輯都是相同的，只需在運作上要針對區塊鏈交易吞吐量與資料隱私方面做不同的規劃。以下提出兩種區塊鏈可應用於跨行支付的結算與清算作業的模式[27]，一是僅執行結算，二是同時運用於結算與清算，分別說明如下。

（一）模式一：運用區塊鏈與智能合約做支付結算

這種模式下區塊鏈與智能合約主要是執行財金跨行支付結算系統的部分功能，清算部分還是由央行同資系統執行。大致的做法是以參與的金融機構、央行同資系統與監管單位構成一支付區塊鏈系統，替區塊鏈的參與機構開發並部署帳戶管理的智能合約。系統可利用智能合約接收交易指令，進行交易結算與帳戶餘額紀錄，並載明與其他參與機構之匯出及匯入款項，以利後續進行清算。一般參與機構的智能合約除接收與紀錄每筆支付指令，也會判斷參與機構帳戶的擔保帳戶餘額是否足夠扣付，或是檢查符合當日額度控管的條件，以執行原本財金跨行結算系統的一些功能。

使用智能合約執行結算作業，透過程式處理邏輯的調整，可以彈性支援 DNS

[26]目前國際間已有多項實驗，應用區塊鏈技術於跨行支付，但多著重於功能與架構，就效率與隱私保護而言，目前的區塊鏈技術不夠成熟，尚未能實際應用。

[27]除此之外，第三節國外案例也將介紹一個實驗，只將區塊鏈用於支付指令的共享，而不改變原有的結算與清算作業。

或 RTGS 兩種不同的清算方式，以下做細節的說明。

1.流程概要

每筆交易指令會經由區塊鏈平台派送到相關機構[28]的智能合約做結算，再由中央銀行的同資系統進行交易的清算，圖 4-2-1 為流程概要。

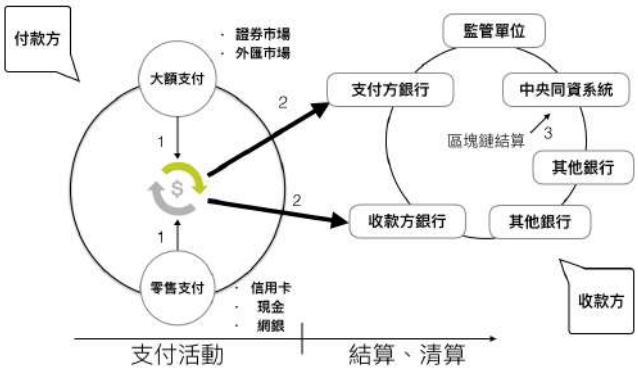

圖 4-2-1 智能合約結算、中央銀行同資系統清算圖

步驟 1：

付款方進行支付動作，付款方可能會經由不同的媒介來進行交易，例如行動支付 NFC、網路銀行、第三方支付、現金等，雖然是不同的支付工具，在支付的指令都會統一傳送到區塊鏈上的智能合約。

步驟 2：

交易指令由智能合約接收，利用區塊鏈的分散式帳本紀錄支付金額、支付對象、支付目的，同時在區塊鏈上執行支付的結算，檢查參與機構帳戶的擔保帳戶餘額，並紀錄支付給收款方的金額。

步驟 3：

由中央銀行同資系統依據區塊鏈智能合約內的結算或淨額交易指令，做實際的清算，以完成支付活動，處理細節會依 RTGS 或 DNS 會有所不同。

以下以表 4-2-1 來解說 RTGS 或 DNS 模式下，支付區塊鏈智能合約的運作方式。表中有五間銀行，分別為 A、B、C、D、E，個別的初始帳戶餘額分別為 140 元、30 元、25 元、40 元、30 元，T1~T10 代表 10 筆不同的支付交易，如 T1，就是由 A 銀行轉 30 元給 B 銀行。這 10 筆支付交易可以透過 RTGS 或是 DNS

[28]視所採用區塊鏈平台的不同，支付指令可能全員共享，或是只在交易雙方、央行與監管單位之間共享。

方式進行結算與清算，說明如下。

表 4-2-1 智能合約交易紀錄與結算表

	A	B	C	D	E	結餘
當天 初始值	140	30	25	40	30	265
T1	-30	30				
T2		20		-20		
T3			30		-30	
T4	20		-20			
T5				50	-50	
T6	-100		100			
T7	80			-80		
T8				20	-20	
T9	50	-50				
T10			-100		100	
結算餘額	160	30	35	10	30	265

情境 1：RTGS

若此用 RTGS 清算，可做每一筆支付交易就進行即時清算。以表 4-2-1 為例，如 T1，由 A 銀行轉 30 元給 B 銀行，若是系統設定是每筆即時清算，則會馬上完成此筆交易的餘額檢查與運算，接著交由央行同資系統進行清算。

情境 2：DNS

假設採用 DNS 清算，於營業日指定時點做一次淨額清算，例如中午 12 點整，以上表 4-2-1 為例。若該日中午結算點剛好在 T9，以Ａ、Ｂ、Ｃ三家銀行的結算流程為例，他們之間有四筆往來交易：上表中的 T1、T4、T6、T9：

T1 中 A 銀行需要支付 30 元給 B 銀行
T4 中 C 銀行需要支付 20 元給 A 銀行
T6 中 A 銀行需要支付 100 元給 C 銀行
T9 中 B 銀行需要支付 50 元給 A 銀行

表 4-2-2　ABC 三家銀行定時清算表

	A	B	C	D	E	結餘
當天初始值	140	30	25	40	30	265
T1	-30	30				
T4	20		-20			
T6	-100		100			
T9	50	-50				
結算餘額	80	10	105	40	30	265

四筆交易的結算運作流程如圖 4-2-2：

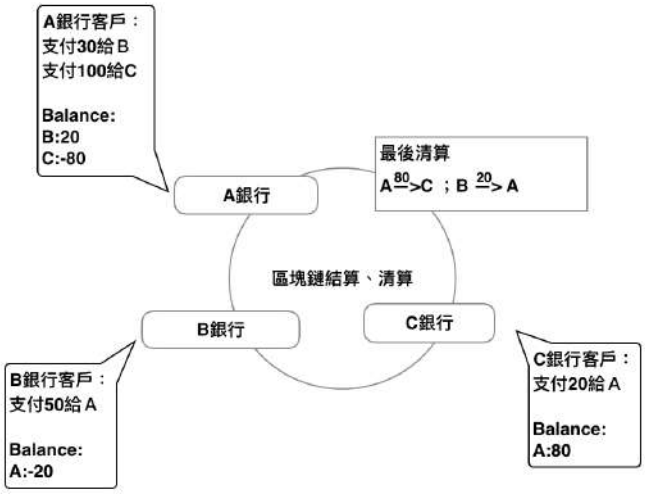

圖 4-2-2 結算智能合約運作情境示意圖

在定時清算前，會先經由系統表結算後，再顯示各銀行最終須執行的支付金額。例如 A 銀行的清算金額即為要從 B 銀行收取 20 元，要支付 C 銀行 80 元，接著，在清算前系統會先檢查三家銀行的帳戶餘額是否足夠，如表 4-2-2，A 銀行清算前的餘額尚有 140 元，B 銀行尚有 30 元，C 銀行尚有 25 元，此時所有銀行的帳戶餘額都足以進行清算，最後清算完，A 銀行帳戶會有 80 元[29]，B 銀行帳戶會有 10 元，C 銀行帳戶會有 105 元。

以上的為概念上的說明，但在實際運作的部分，設計智能合約時還需要考慮到以下幾點問題：

- 由哪筆交易開始做結算

上述的例子都是以 A 的角度開始做結算的判斷，但在實際運作上，可能是要由交易額最大，或是輪流來做。例如，可採用佇列（Queue）儲存支付指令，採用先進先結（First in First out，FIFO）的模式。也可加入優先順序，提供更彈性的選擇。

- 隱私問題

上述總表是以不考慮隱私的問題下，將所有交易都記錄在區塊鏈上，藉由智能合約可自動執行，但實際應用上，應該還是要考慮如何限定分享資料的對象，只在交易對手與監管單位之間分享。

[29] 140-80+20（付給 C80 元且向 B 收取 20 元）

- 大額支付交易

在於實際運作上，還需要考量有急迫性的大額支付交易，故設計區塊鏈的系統時，要同時考慮支付的優先順序需求，增加系統運作的彈性。

（二）模型二：央行發行用於清算的數位代幣

1.發行法定數位代幣方式（Central Bank Digital Token）

發行央行數位代幣方式大致可分為兩類[30]，第一類為擔保發行，就如同新加坡的 Ubin 計畫，是利用法定貨幣與數位代幣採用 1 比 1 的方式發行，另一種是無擔保模式。但因為央行的功能為確保數位代幣的價值，故擔保發行還是主流，例如上述新加坡的 Ubin 計畫與加拿大 CAD-Coin 的計畫。擔保發行的目的未必是要將法定貨幣數位化，進行大量的發行與使用，而是要使用數位化的代幣來加速結算與清算的流程。新加坡MAS 也將與加拿大合作，在未來以央行代幣進行跨境支付的實驗計畫。

2.流程概要

因為是由央行自行發行的數位代幣，故可當成法定貨幣在結算與清算上使用，主要的結算與清算作業將可完全在區塊鏈上運行。例如新加坡的 Ubin 計畫，其中第一階段就是將新加坡幣數位化（SGD on the Ledger, $DR），讓支付交易可以順利經由智能合約作統一的結算與清算，而中央銀行只要當擔保方，其流程架構可參考圖 4-2-3，其中圖例說明如下：

MEPS+: 新加坡央行的跨行結算系統

Participant A's CA: A銀行的實際帳戶，

Participant A's BCA: A銀行的數位代幣帳戶，

Participant A's RTGS：A 銀行的即時清算帳戶，

Participant A's Wallet：A 銀行的交易錢包。

[30] Adam Ludwin (2016), Co-Founder and CEO of Chain, " Why Central Banks Will Issue Digital Currency", https://medium.com/chain-inc/why-central-banks-will-issue-digital-currency-5fd9c1d3d8a2#.sab4sjxy5

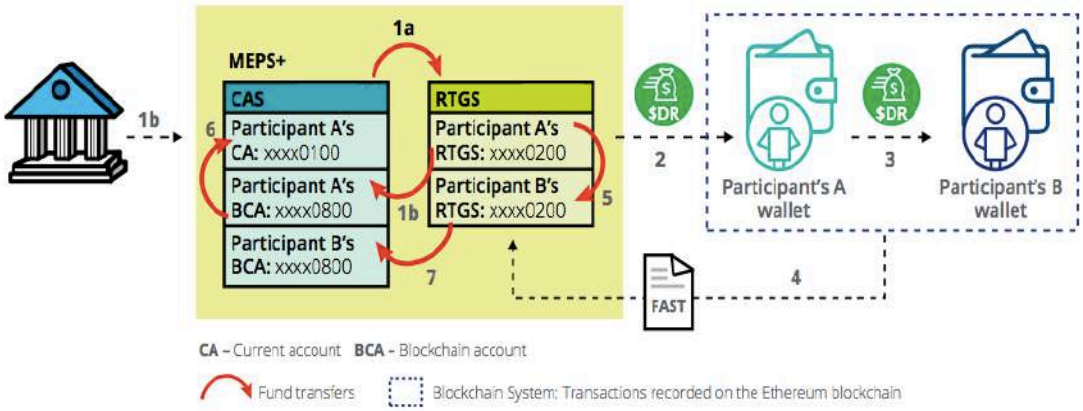

圖 4-2-3 新加坡央行數位代幣使用概念圖

來源: Project Ubin: SGD on Distributed Ledger

圖 4-2-3 可分為兩大部分，第一部分為法幣轉為數位代幣（黃底部分），每日各金融單位藉由法幣與數位代幣 1 比 1 的兌換方式，將法幣換成數位代幣，存入他們在央行的 CA 帳戶（類似銀行準備金帳戶）。當央行收到法定貨幣後，會自動將等額的數位代幣新增到參與銀行的帳戶(Participant's wallet)，接著市場上的交易就會完全數位化，可立即做每一筆支付的結算。每日營業結束時，央行只要讀取各金融銀行錢包的數位代幣餘額，直接做清算，將結算與清算完全自動化。

第二部分為虛線部分，此部分勾勒參與的銀行如何利用錢包做支付交易，因為是數位代幣的交易，可以立即透過區塊鏈智能合約進行結算與清算。由於採用的是 RTGS 模式，所以支付後，銀行的 RTGS 帳戶與其他帳戶將同步。

3.運作步驟：

步驟 1：

（1）央行會先藉由 RTGS 系統來核對目前區塊鏈上的各家銀行帳戶餘額，而每家銀行也會有一個清算帳戶，例如 Participant A's RTGS 就是用來清算目前 A 銀行的法幣。

（2）央行確定法幣數量後，會將同等金額的數位代幣登入銀行的戶頭，如上圖中的 Participant A's BCA 就是 A 銀行的數位代幣帳戶，會同步顯示在 A 銀行的交易錢包 Participant A's Wallet。

步驟 2：

A 銀行的錢包會顯示可用的結算餘額，而當 A 與 B 銀行進行交易時，會將

交易分為一般小額支付，大額支付。

步驟 3：

小額支付部分，會由系統設定好的結算時間做結算，而在全部交易都是以數位貨幣支付的情況下，因為數位代幣會在每一筆交易立即做結算，央行只要在每日固定時間做一次清算即可。

步驟 4：

若有大額交易，可以進行即時清算的要求，系統會將此筆交易直接送至 Participant A's RTGS 進行處理。

步驟 5~7:

大額交易經由處理後，也會立即同步到 A 銀行的 BCA，而清算後也會更動 B 銀行的 BCA，做同步即時銷帳。

因為是由央行所發行的數位代幣，故可視為是法定貨幣，央行可藉由本身的信用做擔保，讓金融機構可以使用代幣做不同的交易，而經由代幣化的運作，除了可以讓金融市場更加穩定、更加有效率之外，也可以讓央行更容易監管每一筆交易。

第三節 個案探討

（一）跨行支付案例

本章節介紹三個國外的實驗案例，包含日本銀行集團、加拿大 Jasper 計畫、新加坡金融管理的 Ubin 計畫，主要都是藉由區塊鏈的智能合約、分散式帳本來改善結算與清算的效率。

1.日本銀行集團

此計畫是由日本瑞穗金融集團(Mizuho Financial Group)、三井住友銀行(Sumitomo Mitsui Banking Corporation)、三菱日聯金融集團(Mitsubishi UFJ Financial Group)、德勤顧問公司(Deloitte Tohmatsu Group)共同進行的區塊鏈實驗，圖 4-3-1 為此次實驗的架構圖，Zengin System 則是日本民營的結算系統(又稱全

銀系統) ，Bank Of Japan-NET (BOJ-NET) 是全日本銀行的清算金融系統，流程為全銀系統結算參加單位之淨應收應付差額後，再透過 BOJ-NET 辦理清算，其方式也是有淨應付差額參加單位先將款項轉進東京銀行協會在日本銀行開立的帳戶，等所有淨應付差額完成移轉後，再從東京銀行協會帳戶將款項轉入有淨應收差額參加單位的帳戶。

但此計畫只運用區塊鏈執行支付的功能，紀錄跨行轉帳的交易紀錄，實際上的結算與清算依然是由原有系統執行。如圖 4-3-1 所示，匯款銀行與收款銀行之間可透過區塊鏈網路進行直接點對點的轉帳交易，然後將結算與清算的作業指令發送給 Zengin 與 BOJ-NET 系統進行。

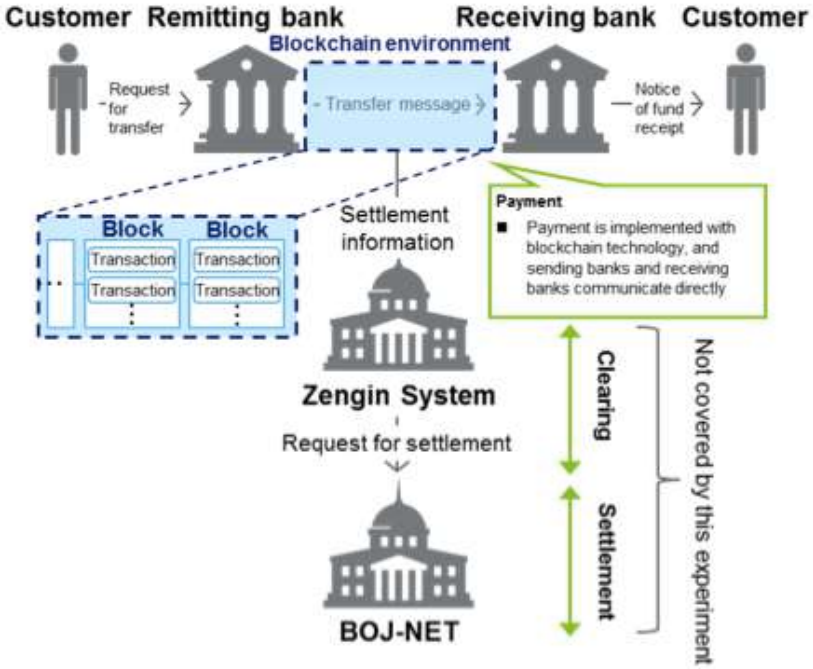

圖 4-3-1 日本銀行團區塊鏈實驗圖

來源：Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation （2016）

根據他們的實驗結果，區塊鏈在於處理結算與清算都是正常的，最後日本以下列幾個面向來檢視實驗成果。

（1）從功能角度來看：

在支付部分，基本上都能經由區塊鏈網路來達成，但在結算方面目前還無法處理太過於複雜的狀況，之後將與結算（Zengin 系統）和清算（BOJ-NET）的運

作方法進行對比，以進行更為精確的評估。

（2）從技術角度來看：

只證明了區塊鏈部分適用性，例如交易吞吐量達每秒 1,500 次，實際運行的水平準是符合業界標準的。但在其他方面，有些問題需要進一步的評估才能達到業界的水準，例如安全、穩定性、防禦攻擊能力等。

（3）從成本較度來看：

需要從應用開發費用、軟體、硬體、維護及運作四個面向去考量

- 開發費用—跟傳統的系統相比，區塊鏈系統本身就已經將應用面所需的智能合約、分散式帳本、共識演算法包含在內，不需再進行過多的低層開發，但考慮到新技術的本身的導入成本較高，故總成本可能不會與傳統的系統相差太多，因為在區塊鏈實際應用的過程中還是會需要做許多前端應用的調整。
- 軟體—服務提供商的定價不同，軟體是否會降低成本目前還無法評估。
- 硬體—與單一系統集中處理的傳統技術相比，多個系統執行分散式處理的區塊鏈技術可能可以降低硬體規格。
- 維護與運作—區塊鏈服務平台之維護及運作費用，可能因服務提供商而異。

實驗目前只限定在支付系統，其他如證券系統、外匯系統的部分可能是會是下一個實驗階段的重點。

2.加拿大 Jasper 實驗計畫

Jasper 計畫為 2016 年由加拿大國營支付機構 Payments Canada 與加拿大央行，以及 R3 聯盟共同推出的實驗計畫，目的在探討分散式帳本於銀行間支付系統的應用，計畫分為兩階段：第一階段，使用 Ethereum 平台測試支付清算的可行性，測試是否能達到金融市場基礎設施準則(PFMIs)的標準；第二階段，使用 Corda 平台並加入流動性節省機制(Liquidity Saving Mechanism, LSM)，進一步評估 DLT 的平台的可擴展性(Scability)及應用上的彈性(Flexibility)。

Ethereum 是 Jasper 實驗第一階段所使用的 DLT 平台，而其用來測試跨行大額支付清算功能(Wholesale interbank settlement)的原型框架則是以 Solidity 所開發的智能合約所構成的。在第一階段的實驗裡，銀行以加拿大央行(BoC)所發行的數位存託憑證(DDR，Digital Depository Receipt)來進行跨行間的支付，並透過抵押(Pledge)及贖回(Redemption)加拿大幣(CAD)的方式與加拿大央行進行數位存託憑證(DDR)的交換。支付(Transfer)、抵押(Pledge)及贖回(Redemption)等三種交易均透過交易代理人智能合約(Transaction agent smart contract)來自動進行，而加拿大央行除了負責維護與部署該智能合約外，也利用交易代理人智能合約來建立銀行的數位存託憑證錢包(Wallet)。

第一階段實驗的主要創新是在 DLT 平台上實現了『單元交換(Atomic Exchange)』的機制，即所有的支付交易必須為即時且完整(Atomic)的，不能有任何交易只完成部分金額的移轉。在這個階段，Jasper 實驗證明了在 DLT 平台上實作 RTGS 支付功能的可行性，但由於 DLT 平台所使用的 POW 共識機制有執行效率的問題，且每筆交易達成共識的時間難以掌握，除了有交易處理能力不足的隱憂之外，也無法達到 PFMIs(Principles for Financial Market Infrastructures)對於交易確定性(Finality)的要求。

另外，由於 Ethereum 平台所提供的交易透明性，對於監控參與銀行的狀態有一定程度的方便性，而且由於 Ethereum 平台上的節點共享同一份帳本，平台本身即具有資料備份的原生功能(Backup natively)，比起其他平台來說，較不會有資料遺失的問題。不過相對的，由於資料透明及共享的特性，在保護銀行的隱私資料上將會有很大的挑戰，因為到目前為止，在 Ethereum 平台上並沒有交易隱密性(Privacy)的機制被發展出來。

Jasper 實驗的第二階段是在 Corda 平台上進行的，其目的是透過實作 Corda 版的大額支付系統，來進一步評估 DLT 平台的可擴展性(Scability)以及在應用上的彈性(Flexibility)。這個階段最主要的創新是加入了流動性節約機制(LSM)，以在既有的 RTGS 清算機制外，新增不同的支付選項。而在資料吞吐量(Throughput)的驗證方面，在第二階段則進行了大量交易資料的模擬測試，藉以驗證 DLT 平台能否處理現行大額轉帳系統(Large Value Transfer System, LVTS) 的日常交易量。

在第二階段裡，節點的角色可分為參與節點、Notary 節點、以及監理

(Supervisory)節點三種：參與節點即一般的銀行，Notary 節點與 Supervisory 節點的角色則由加拿大央行擔任。Supervisory 節點有權限查詢所有交易資料，具有稽核的權限；Nortary 節點則有驗證交易唯一性(Uniqueness)的功能，可確保沒有雙花(Double spend)的問題發生；一般的參與節點除了具發送交易的權限外，也負責與節點本身有關聯的交易合法性(Validity)驗證，而交易的唯一性與合法性驗證則構成了 Corda 平台共識機制的基礎。

Japser 實驗的第二階段也採用數位存託憑證(DDR)來作為支付的工具，但與第一階段不同的是，DDR 與加拿大幣(CAD)在第二階段的兌換率是 1:1，除此之外，DDR 在 Corda 平台上並具備有 UTXO 的特性，被花費的 DDR 稱為『DDR Object』，其中紀錄了傳送方、接收方、發行方、以及日期等資訊，而當交易結束，『DDR Object』就會被寫進相關節點的帳本中。

在 Corda 平台上，只有 Notary 節點與 Supervisory 節點有所有的交易資料，而參與節點則只存放與本身相關的交易資料，Corda 藉著這種資料隱藏機制達到了資料隱私性的要求，但相對的，由於帳本資料不共享，因此在 Corda 平台上，每個節點都需要維持相當高的可用性(Availability)來維持整個 DLT 平台的運作，除此之外，也需要有完善的資料備份機制來避免資料遺失的風險，而這種情形也代表 Corda 平台潛藏有導致運行可靠度(Operational reliability)失效的風險存在。

雖然 Jasper 計畫的第一階段與第二階段的實驗結果符合 PFMIs(Principles for Financial Market Infrastructures)所規範的部分原則，例如符合 PFMIs 對於抵押風險(Collateral risk)、流動性風險(Liduidity risk)、信用風險(Credit risk)、以及交易確定性(Settlement finality)的規範，但實驗的結果發現在 DLT 平台上仍有作業風險(Operational risk)的存在，除此之外，PFMIs 對於存取及參與節點的要求(Access and Participation Requirements)具有明確的規範，例如參與節點必須維持 98%的可用度，但是在 Jasper 計畫中並沒有正式的制定這一方面的規範。

3.新加坡金融管理局（MAS）：Project Ubin[31]

此計畫主要目的在於評估利用分散式帳本產生新加坡數位代幣的影響及其

[31] Ubin 第二階段的計畫成果也在 2017 年 11 月份公布，內容包含 Corda、Hyperledger、Quorum 三個不同的運作架構、流程，同時描述不同平台上的設計差異。

對新加坡金融生態系統的潛在利益。分為兩階段實驗：階段一開始於 2016 年年底，在近期的研究報告中完成了概念驗證 (PoC)，其中包含追蹤參與者餘額的分散式帳本、即時運作，其中在 Ubin 專案利用分散式帳本所產生的數位代幣的方式又稱 SGD-on-ledger，以下將介紹 Ubin 架構圖以及 SGD-on-ledger。

（1）Ubin 計畫架構圖

圖 4-3-2 為 Ubin 計畫的架構圖，利用 DLT 連結 RTGS、MAS、與一般銀行，架構圖分為兩部分，第一部分是藍色虛線，代表的是在 DLT 上的交易流程，分別為 MAS 藉由 DLT 連結銀行 A、銀行 B，以及交易銀行 A 與前端網站的連結；第二部分是 DLT 與 RTGS 的連結，此部分是新加坡的數位代幣在支付交易結算完後，要進行清算時，就由 RTGS 系統進行清算。

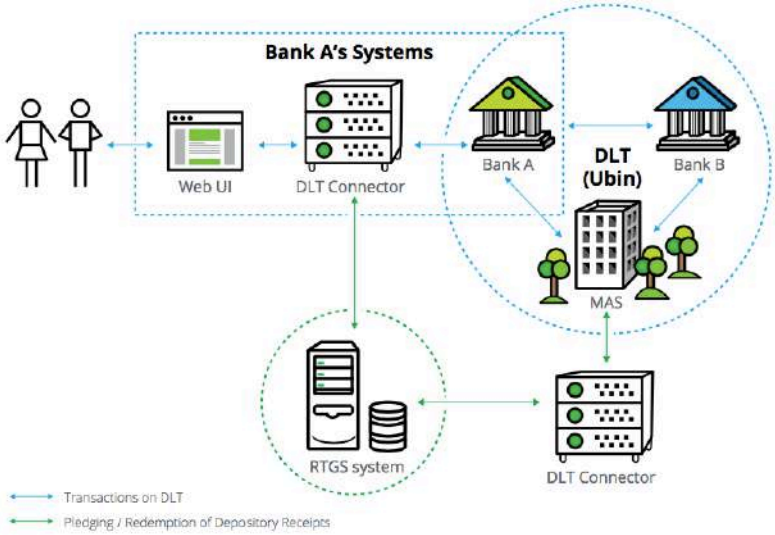

圖 4-3-2 Ubin 計畫架構圖

（2）SGD-on-ledge

SGD-on-ledge 主要是設計來支持 Ubin 計畫中所需要的金流系統，其中有三個特點來符合 Ubin 計畫的需求，第一，其與一般的銀行存款中的新加坡幣不同，此代幣只用於內部區塊鏈網路，第二，此代幣會由現存的法定新加坡幣做擔保，確保內部網路使用上的安全，第三，此代幣可以藉由不同的調整來搭配不同的應用情境，例如若是要用於債券交易，就可以加強銀行與銀行間的交易安全審核，而若是用於結算或是清算，也可調整其交易的速度，經由上述三個特點，可以確保 Ubin 專案運行中的彈性、效率以及安全性。

（二）跨國支付實驗案例

跨國支付在交易雙方中間需要經過許多單位，通常匯款方會被收取層層的手續費，不僅費用昂貴，效率也非常低落，故常被視為 DLT 可以改善的支付作業。以下將以日本、歐洲兩國央行間的 Stella 計畫為例來說明，如何透過區塊鏈進行跨國支付的實驗。

Stella 計畫是由日本央行（BOJ）和歐洲中央銀行（ECB）共同合作的實驗，旨在利用 DLT 改善金融基礎設施建設，並於今年(2017 年)9 月發布了“Stella”專案的報告，其中包含兩國結算系統的現況、分散式帳簿技術（DLT）的測試方式。其研究主要聚焦在流動性節省機制(LSM)的優化，現階段的結果有以下三點，第一，確認利用 DLT 可以達到目前 RTGS 系統所需的結算速度要求；第二，DLT 可增加系統的穩定度；第三，節點數量增加會降低系統的運作效率。

此次兩國央行共同進行了兩種不同的實驗，第一種是單純使用智能合約做結算，但不包含 LSM 的處理，例如待處理金額的處理程序、雙邊清算程序。另一種是較複雜的智能合約，會先做 LSM 的處理再清算。經由兩種智能合約的比較，發現以 DLT 的運作效率而言，LSM 的運算並不會對整理運作的效率有太大的影響，但因為 Stella 計畫所使用的 DLT（Hyperledger Fabric V0.6）使用的是 PBFT 共識演算法，此種演算法的特性是當參與的節點數越多，共識的效率則越低，故此份報告對於影響運作效率方面，節點數量為最主要因素。

Stella 的研究如上述，主要聚焦在流動性機制(LSM)的優化，而現階段的結果有以下三點，第一，確認分散式帳本可以達到目前 RTGS 系統所需的結算速度要求以及讓 LSM 正常運作的基本需求，第二，系統的運作效率會受到網路參與節點的多寡以及參與節點間的距離所影響，第三，DLT 可提升 RTGS 系統的容錯以及穩定性。

第一點—結算速度：

目前日本與歐洲的 RTGS 系統平均流量約為 10~70 RPS ，經測試結果，DLT 的運作可以達到此標準，另外，此實驗為了測試在網路性能與流量附載間的關係，也將交易流量調高至 250 RPS 做測試。

第二點—運作效率：

經由兩種智能合約的比較，發現系統並不會因為 LSM 的運算而降低整體運作的效能，但在於節點數量的增加則會明顯影響 DLT 系統的運作。另外，在於節與節點間的距離，如圖 4-3-3，主要分為大阪到德國以及大阪到東京兩種距離做測試，若是節點互相接近，如大阪到東京，則在於交易延遲的影響就會較小，但若是節點距離過於分散，如大阪到德國，則可能就會因帳本同步的延遲造成節點間的資訊有時間差。

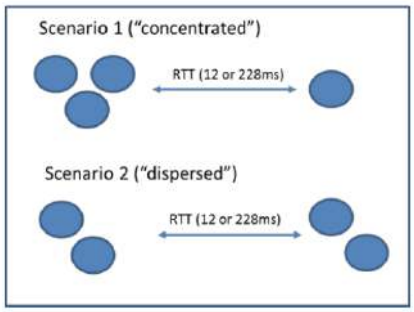

圖 4-3-3 Stella 節點距離測試

第三點—容錯及穩定性：

此實驗針對兩個問題點做容錯性的測試，第一是驗證節點故障，第二是不正確的資料數據格式，在於節點部分，只要系統上的共識演算法持續運作，則單一節點的故障並不會影響整體系統的運作，另外在於不正確的資料格式，實驗經測試，系統能自行檢測出不正確的格式，讓其不影響整體系統。

報告最後指出，在設計分散式帳簿時，需考量到運作效率與系統穩定度。效率方面，關鍵因素包含交易數量（與批量大小相關聯）、創建新區塊所需的時間，這些因素可根據不同的應用，調整節點數量與節點運作方式。在系統穩定性方面，此份報告強調 DLT 可能潛在的問題，例如當核心節點（權限最高的節點）故障時，所有交易都可能被拒絕，而此問題需要獨立處理，無法在交易進行中同步除錯。

(三)新興支付技術與平台

未來創新運用之支付將聚焦在跨國的結算與清算自動化，不同於跨國支付的 Stella 計畫還是需要各國央行介入，以下的 Ripple 案例是用區塊鏈的分散式帳本，

以去中心化的方式達成高效率的跨國匯款。

1.Ripple

目前銀行之間的跨國匯兌要經過許多不同的金融機構，在過程中除了會牽涉多種不同法幣間轉換的匯差損失外，由於中間經過許多金融機構轉手，因此手續費對於銀行也是一筆負擔。

Ripple 就是為了解決銀行間跨國匯兌中的高成本與低效率而成立的跨國支付平台，其區塊鏈網路又稱為 Ripple Network。

Ripple 的交易架構如圖 4-3-4，首先匯款方[32]會經由已加入 Ripple 網路的金融機構將法幣轉換成 XRP 代幣[33]，接著 Ripple Network 會藉由內部的換匯系統將 XRP 代幣轉成收款方的幣別，最後再將換匯後的金額轉到收款方國家中已加入 Ripple 的金融機構，而整個過程的關鍵就是利用 XRP 作為法幣間的轉換媒介完成雙方交易；但在跨國交易流程中，Ripple 為了降低成本提高效率，同時又要兼顧安全性，因此除了使用區塊鏈作為平台底層之外，還建立許多優化跨國交易的技術，例如針對交易網路中的金融機構連結的系統 Ripple Connect，以及針對交易過程中的外匯轉換所推出的 Ripple Stream，還有針對用戶在交易最後，能順利將虛擬貨幣與法幣順利轉換的連結所推出的 Gateway 。

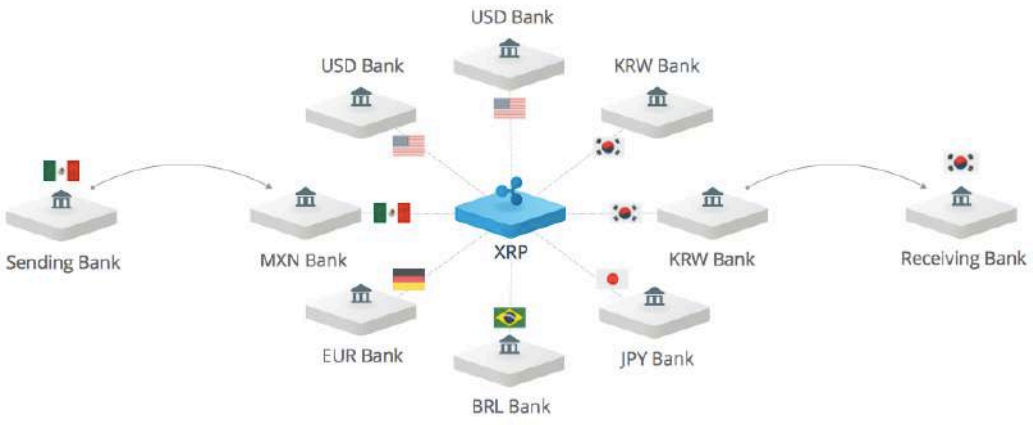

圖 4-3-4 Ripple 架構圖

來源：https://zhuanlan.zhihu.com/p/24477689

在運作流程中，首先會利用 Ripple Network 的區塊鏈網路來連結用戶與金融

[32]匯款方可能是個體用戶、數位代幣交易所或是未加入 Ripple 網路的銀行

[33] XRP 為 Ripple 自行發行的數位貨幣

機構，所有交易都會在 Ripple Network 上進行，如圖 4-3-5，當匯款方發起匯款交易時，就會由匯款方當地的銀行藉由 Ripple Connect 連結對方的銀行，在此過程中的跨國匯率會由 Stream 自動處理，最後在收款方要接收匯款時，就會由 Gateway 來確保 Ripple 網路上的數位代幣可以安全地轉換為法定貨幣或是收款方 Ripple 電子錢包中的 XRP 幣，以下將更詳細的說明各部分的運作方式。

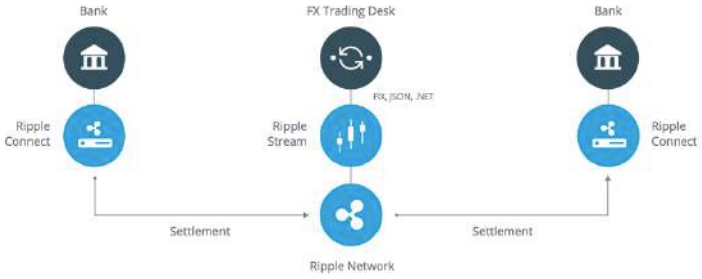

圖 4-3-5 Ripple Network

來源：Ripple.com

（1）Ripple Network 區塊鏈網路：跨國交易平台

Ripple Network 區塊鏈網路是以私有鏈的模式運行，此部分主要功能是建立匯款單位與收款單位之間的連結，Ripple 的使用者進入 Ripple 平台前必須要先通過審核，建立信任基礎，例如收款人與付款人進行交易時，可透過共同信任的朋友或是單位[34]來擔保進行交易，此時雙方就可建立一條信任鏈，未來也可以利用這條信任鏈在 Ripple 網路上完成交易；除了建立信任外，Ripple 平台也發行自己的代幣 XRP 作為不同法幣間的轉換媒介。

（2）Ripple Connect：金融機構間的橋樑

Ripple Connect 是 Ripple 網路匯款流程中重要的單位，除了提供金融單位間安全的訊息管道外，也連結了雙方的金流記帳邏輯，其中記帳邏輯的部分是利用其核心演算法 Interledger，此演算法可以接受不同記帳邏輯之間的轉換[35]，解決不同金融機構或是使用者之間各自不同的記帳邏輯，加速金流的效率，如圖 4-3-6，Ripple 藉由 Interledger 作為中介將雙方的記帳邏輯做連結，直接在平台上做跨國匯款的清算，假設圖中左邊的銀行(下稱 A)要支付右邊的銀行(下稱 B)100 歐

[34] Ripple 上的匯款與收款方可能是一般銀行或是交易所，故共同信任的部分也可能是金融單位

[35]除了金融機構間的記帳邏輯，未來 Ripple 也可能利用 Interledger 連結不同區塊鏈的帳本，進行全球數位代幣與法幣交易的整合

元，首先 A 會將 100 歐元匯入 Ripple 帳戶中，而 ILP 作為中介方，藉由整合記帳邏輯來確認雙方帳戶的狀態，例如確認 A 公司是否已將 100 歐元匯入，確認後會進行匯款，且將完成匯款後的 A、B 公司的 Ripple 帳戶餘額在 Ripple Connect 上做更新，供未來的交易使用。

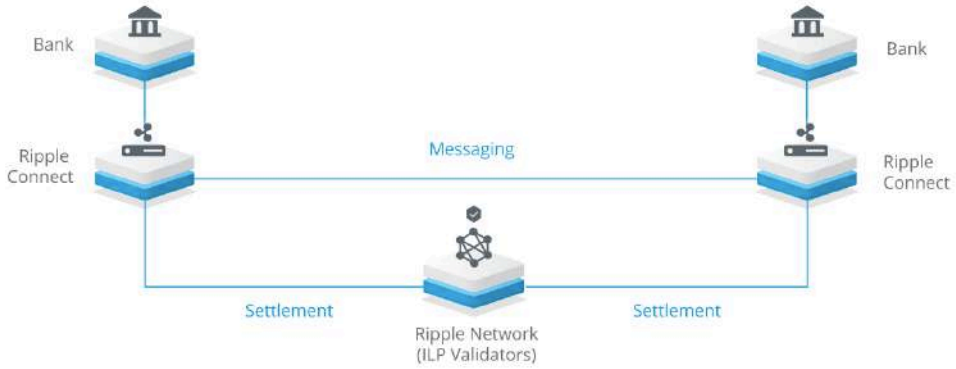

圖 4-3-6 Ripple Connect 運作圖

來源：ripple.com

（3）Ripple Stream：匯率系統

因為各國匯率的浮動，在交易進行中間，匯率的選擇也是跨國匯款的關鍵，如上圖 4-3-6，Stream 就如同小型的匯率市場，藉由每筆匯款的轉換，自動算出最划算的匯兌來讓每筆匯差損失降到最低；此外，Stream 最終目的是連結現存的銀行換匯系統，最終讓一般銀行也能利用 Stream 進行匯率的轉換。

（4）Gateway :讓法幣與 XRP 幣能安全轉換的守門員

Gateway 的部分，如圖 4-3-7，主要功能是確保 XRP 與法幣間轉換的安全，圖的左邊為 Ripple 網路及 Ripple 錢包，經由數位代幣 XRP 的交易都會在這部分做運行，右邊是法定貨幣，在中間的是 Gateway，Gateway 目前是由跨國銀行、當地銀行甚至是新興數位貨幣加密交易所擔任。

在最後收款方收到匯款時，有兩種形式來接收匯款，第一種是直接換成法幣存入銀行戶頭內；第二種是將款項以 XRP 的模式儲存於區塊鏈 Ripple 電子錢包內，在這兩種模式裡，最後都會牽涉到數位貨幣轉換成法定貨幣的流程，而 Gateway 就可以用守門員的角色來確保用戶在數位貨幣與法定貨幣間的轉換安全；但 Gateway 的功能用於虛擬與實體貨幣間的轉移只是第一步，未來，Ripple 會嘗試將所有有價值的資產藉由 Gateway 的擔保來轉換成數位資產。

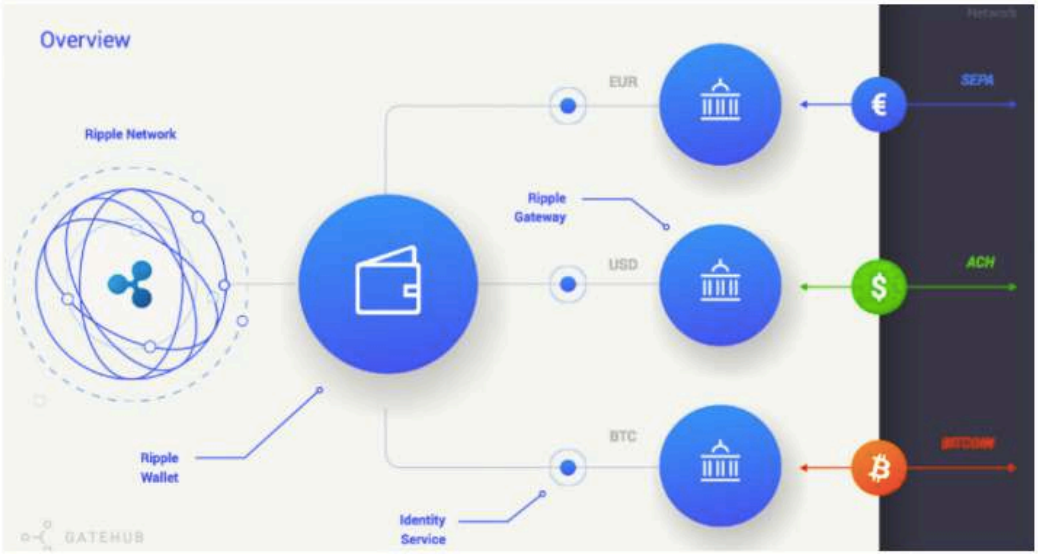

圖 4-3-7 Gateway 架構圖

來源：DASH gateway on Ripple Proposal Review, https://www.dashforcenews.com/dash-gateway-ripple-proposal-review/

第五章、區塊鏈在銀行融資業務之運用

第一節 銀行融資之現況分析

（一）基本介紹

銀行的融資業務包含個人與企業貸款、貿易融資與聯貸等。貿易融資的部分，是源自於買、賣雙方需要銀行做中介擔保雙方交易，如開設信用狀。銀行為了降低信用狀的風險，目前放款對象大多是成熟的進出口商。

另外，在供應鏈的中心廠也開始藉由本身資金雄厚的優勢切入融資的市場，此舉將會侵蝕了銀行的融資業務，如鴻海的富金通就與新創點融網合作，跨足原本專屬於銀行的融資業務，而中心廠切入供應鏈融資的行為又可稱為供應鏈金融。

在個人借貸，近期興起的 P2P 借貸平台也可能影響銀行的貸款業務，P2P 借貸平台不只是針對對一般民眾，未來小型企業也可能以個體戶的身份直接在 P2P 借貸平台上取得需要的資金，且不用經過銀行如此繁雜的認證，快速的借貸效率對於中小企業是非常大的誘因。P2P 平台的底層技術也是區塊鏈可以應用的部分，可提供讓個體戶互相信賴的基礎，來增加 P2P 平台借貸的優勢。

最後，銀行的聯貸業務主要是利用銀行團的方式承接大型企業的貸款需求，如台積電這種資本額龐大的企業，其貸款額度可能就要由多家銀行共同承接。

（二）貿易融資、聯貸的問題點

銀行在貿易融資部分，除了要面對外部的新進者威脅外，銀行本身對於供應鏈廠商的放款也存在許多的問題，例如對於供應鏈中小企業的資訊掌握度不足與放款所需的紙本文件繁雜。

1.貿易融資

貿易融資是銀行基於跨國貿易的單據進行融資，其中單據及商品如表 5-1-1 整理，本研究為了方便討論，將融資方式將以信用狀與 Open Account 兩類做探討，而參與貿易融資的單位，包含進口方銀行、出口方銀行、進口方、出口方、檢驗機構、保險商、物流與海關等。

表 5-1-1 貿易融資相關單據及商品表

重要單據	貿易融資商品
1.買賣契約 2.訂購單 3.銷貨發票 4.包裝單-給貨運公司時的清單 5.貨運提單 6.保險單	1.訂單融資/外銷融資 2.進/出口 Open Account 融資 3.信用狀 L/C 4.Factoring 5.Forfaiting

2.信用狀與 Open Account

信用狀融資與 Open Account 融資的主要差別在於開立證明時是否有銀行介入，信用狀是買、賣雙方藉由銀行作為中介商，擔保雙方的交易的書面文件，廠商可利用信用狀進行融資，而 Open Account 則是進口、出口雙方自行協調的應付帳款紀錄，出口或進口方再藉由 Open Account 向銀行進行融資，相較於信用狀融資，銀行在於 Open Account 就只能被動接收融資需求，無法掌握貿易雙方的實際交易。

- 信用狀

進、出口企業利用信用狀作為交易信任憑據，也就是銀行作為交易護中介方，而出口方可以利用信用狀來進行出貨前的貸款，先取得出貨所需的資金，待收到進口方的付款後再繳還貸款，而其中牽連到的不只是銀行與買、賣雙方，同時還有貨運、保險公司與監管單位，圖 5-1-1 為完整的貿易融資的信用狀開狀流程圖。

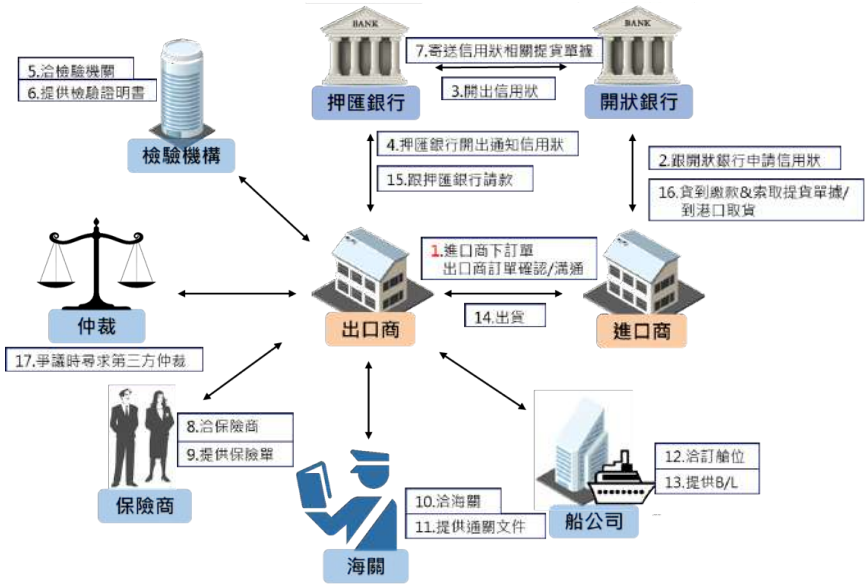

圖 5-1-1 進出口信用狀流程

來源：張瑞辰,2017, 應用區塊鏈加快國際貿易信用狀處理流程

步驟 1： 交易雙方簽訂交易合約。	步驟 2： 進口商向當地開狀銀行申請信用狀。
步驟 3： 開狀銀行向對方銀行(又稱押匯銀行)開立信用狀。	步驟 4： 押匯銀行向出口商通知信用狀生效。此時出口商可以選擇上信用狀來進行融資。
步驟 5~6： 出貨前先由檢驗機關驗貨	步驟 7~8： 在出貨前也會與保險商先進行保險
步驟 9~10： 出口商聯路海關準備出貨。	步驟 11： 與航運公司洽談物流相關的流程，
步驟 12： 同時航運公司會提交出貨證明(提貨單)	步驟 13： 出口商出貨。
步驟 14： 出口商將出貨證明提供給押匯銀行，押匯銀行先行墊款，同時結清融資、利息金額。[36]	步驟 15： 進口商核對提貨單後付款給開狀銀行，開狀銀行依約定時間將款項付給押匯銀行。

[36] 押匯有不同形式，此部分為銀行先押款，收款風險由銀行承擔，若出口商沒有使用信用狀融資，則押匯銀行就不會進行融資的利息結清動作

上述的流程中，進口方簽訂貿易(步驟 1)到出口方出貨(步驟 13)，就隔了 8 個步驟，包含信用狀開立、雙方銀行溝通與出口商的資金調度，同時還要考慮到監管單位與保險單位的介入。特別是新的貿易商或是小型的供應商要申請信用狀時，銀行評估其信用風險的難度相當高，這同時也導致銀行的客戶都侷限在大型客戶。

- Open Account

第二種融資方式為 Open Account，是由中心廠對於上游供應商所提供的應付帳款證明，而上游供應商就可以依此證明向銀行申請融資。但在於 Open Account 的融資過程，雙方銀行不會有接觸，故有可能發生進口商已經將款項付給出口方，但出口方卻沒有及時與當地銀行清算融資款項，這對於銀行的風險高，也是銀行不敢輕易的放貸的原因之一，圖 5-1-3 為目前的 Open Account 流程圖。

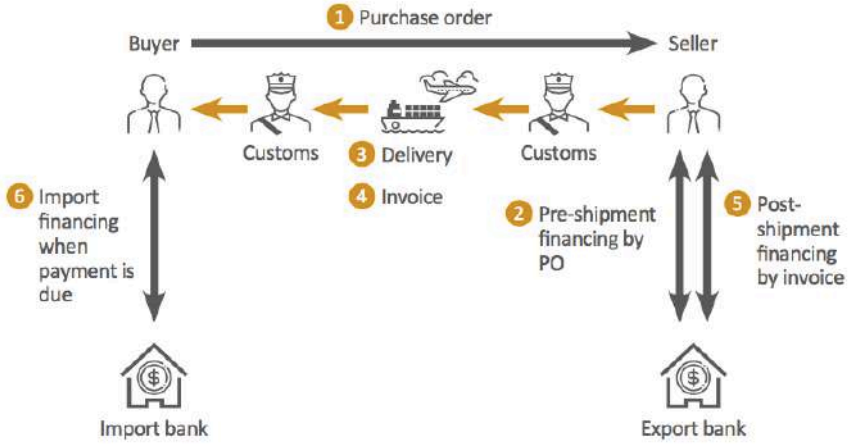

圖 5-1-2 Open Account 交易流程

來源：香港金融管理局,Whitepaper on Distribute Ledger Technology

從圖 5-1-2，在 Open Account 的模式下，進、出口銀行間沒有交集，與銀行的貿易融資是個別進行，所以銀行的對於 Open Account 的信任感就會較低。例如圖 5-1-2 中的步驟 2，在出口方要利用訂貨單(PO)進行航運融資時，出口方銀行就要判斷是否要給予融資，此時銀行難以確認此筆訂貨單的真實性，也不知道買方是否早已預付款項，故對於銀行來說，徵信的成本非常的高。

但 Open Account 的好處是如果銀行接受且信任 Open Account 裡所記載的資訊，包含訂貨單、訂貨時間、交貨時間、訂單金額、付款時間等，銀行就可以利

用 Open Account 中不同的資料來拓展不同的業務，例如訂單融資、貨運融資、買方預付款融資等，故相較信用狀，Open Account 的優勢較為彈性。

3.聯貸

銀行聯貸主要是由一家銀行作為發起單位，召集多家銀行共同認購企業貸款。其中流程包含發起人召集銀行團、審核企業資料、認購比例協調。其中招集銀行團的過程中就會有許多文件的交換，且同時還要考慮保密性；不同銀行間的資訊系統也不同，各種資訊系統導致聯貸的資訊整合非常繁雜，特別是在徵信的部分。該由誰來做也非常重要，且最後當資金有問題時，也得耗大量的溝通成本才能將責任歸屬清楚。如近期的慶富案，就是聯貸事後權責歸屬困難及資料溯源困難的例子。

在 WEF 2016 年的區塊鏈報告中，整理出聯貸的參與者主要包含主導銀行(Lead Arranger)、銀行團(Syndicate)、聯貸需求企業(Requesting Enity)與監管單位(Regulator)，如圖 5-1-4。

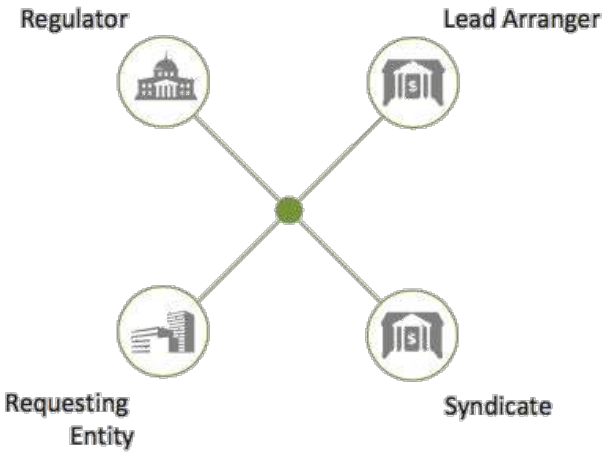

圖 5-1-3 聯貸參與單位

來源：世界經濟論壇(World Economic Forum),2016, The future of financial infrastructure :An ambitious look at how blockchain can reshape financial services

聯貸的運作方式如圖 5-1-5，分為幾個部分。第一部分，貸款提供方及需求方(Syndication)的媒合，此部分會由主導銀行進行籌組銀行團合作夥伴，共同對貸款需求方的貸款金額做分配。第二部分，進行查核(Diligence)，此部分會由主導銀行以及銀行團的聯貸合作夥伴一起對聯貸對象進行徵信、評估貸款風險。第三部分，進行承貸(Underwriting)，承貸是在第二部分的貸款風險評估後，聯貸銀行團會協調各自的承貸金額。第四部分，進行簽約及後續服務(Closing and

servicing)，主要會由主導銀行負責就第三份所擬定的承貸金額、時間、撥款條件等。

圖 5-1-4 一般聯貸流程圖

來源：世界經濟論壇(World Economic Forum), The future of financial infrastructure :An ambitious look at how blockchain can reshape financial services

但聯貸目前存在一些問題，首先對於銀行團，就會面臨到承貸的分配與事後的權責歸屬；除此之外，在風險評估方面，要由各家銀行分別調查，或是由主導銀行進行調查，都需要經過協調，其中的時間成本非常高，而對於貸款申請企業，除了流程繁雜外，為了符合法規，使用資金的限制也非常多，但若是要增加金流的效率，讓貸款申請企業能快速拿到資金，監管單位又需要考量貸款企業是否有將資金應用在正當用途。總結來說，主導銀行、銀行團、貸款申請企業與監管單位四方的資訊流通不便，導致整體運作效率不佳，風險掌控困難。

4.銀行在貿易融資與聯貸的痛點整理

貿易融資的過程中銀行透過審核戶的各類單據，確認客戶交易的真實性，客戶單據包含訂單、提單、發票與保險單的等，這些單據都來自於不同的單位，例如海運公司、保險公司、貨運商及買賣方，銀行需要仰賴大量的人工來檢查這些紙本單據的正確性，不過人工的檢查時間較久，也無法完全杜絕人工出錯，或客戶假冒單據的可能性，同時紙本單據傳遞需要花費 3~5 天，因此總結來說，目前貿易融資有三大痛點，第一，人工審核容易出錯，第二，假造單據，第三較長的文件傳遞過程。而在聯貸部分，也如上文中提到的，資訊流通效率低、風險難以掌握，導致整體流程繁雜，表 5-1-2 為統整表。

表 5-1-2 貿易融資、聯貸痛點整理

	痛點
貿易融資	● 流程繁雜 ● 單據多，查核效率低 ● 資訊傳遞不透明
聯貸	● 流程繁雜 ● 安全性要求高 ● 權責歸屬困難

5.個人貸款—P2P 借貸

全球第一個 P2P 借貸平台為英國的 Zopa，成立於 2005， Zopa 的全名為「Zone of Possible Agreement」，但 P2P 借貸平台缺乏監管、且相互陌生的民眾間也難以信任，平台的營運也潛藏非常多的問題。中國時報 2017 年 8 月對於 P2P 借貸泡沫化[37]報導中指出，以中國為例，前後共有 5000 多家 P2P 平台投入這項業務，但截至今年 7 月，維持正常營運的 P2P 平台只剩下 2100 家 。應用區塊鏈於 P2P 借貸，除了可以解決相互陌生民眾間的信任問題外，也可以加強對於 P2P 借貸平台的監管。

6.供應鏈金融

供應鏈金融的運作模式其實與貿易融資中的 Open Account 融資非常類似，但不同點在於放款者是供應鏈的中心廠，中心廠會利用本身對於供應鏈上游的原物料商的了解來進行放款，相較於銀行，中心廠可以更精準地掌握風險，進行放款。

[37]中國時報(2017 年 8 月)，王孟倫 ,http://news.ltn.com.tw/news/business/paper/1128867

第二節 應用區塊鏈技術於銀行融資業務

利用區塊鏈的分散式帳本、智能合約能有效的解決銀行融資業務的問題，麥肯錫(2016)的區塊鏈白皮書[38]中提到，區塊鏈技術應用在貿易融資業務上不僅帶來非常可觀的成本節約，更能夠將交易流程大幅簡化和自動化，從而提升了交易效率，減少資金閒置成本，降低交易與結算風險，優化客戶體驗 。

（一）貿易融資

貿易融資部分,以銀行角度來說,問題點就是難以取得供應鏈的進出口資訊,所以只能用廠房、資本額來對企業進行徵信，如此不僅讓銀行難以真正了解廠商的運作情形，也讓中、小型的企業難以通過徵信，以至無法進行融資。

延伸來看,資訊難以取得的原因是供應鏈運作方式為了達到高效率與隱私,大多都會以垂直的方式運行,故外部的單位難以切入獲取資料。但區塊鏈的出現,可以利用分散式帳本讓供應鏈「平臺化」，同時又可以確保平行運作過程中，有過去垂直管理下的效率及隱私。就如同過去 A 廠商與 B 廠商進行交易時，C 銀行只能在旁觀看，等 A、B 廠商交易完後再提交相關文件給 C 銀行，銀行完全是處於被動的角色，但若是有了區塊鏈的分散式帳本，C 銀行可以在 A、B 廠商在交易的同時就同步接收資訊，而此資訊不可更改，只能新增，此時 C 銀行就可處在主動的角色，進行融資的協助。

整體而言，對於銀行，雖然可以快速掌握供應鏈上的資訊，但從中心廠的角度，可能會不想將資訊外流給銀行，因為中心廠通常會利用應收帳款期限短、應付帳款期限長的方式來產生閒置資金，而此筆資金就可以用來放款，藉此蠶食銀行的業務範圍，故實際運用區塊鏈還需要考慮許多問題，以下將區塊鏈應用架構模型、須納入分散式帳本的資料考量、權限管理方式與運作模型四部分，依序考量區塊鏈如何應用在貿易融資。

1.需要納入分散式帳本的資料

貿易融資的應用，首先要先了解要分享哪些「關鍵」的貿易資料，例如採購訂單(PO)、商業發票(Commercial Invoices)與提貨單(Bills of Lading)。

[38] 麥肯錫 2016 年 5 月針對中國銀行業所發佈的白皮書,區塊鏈-銀行業遊戲規則的顛覆者

2.區塊鏈應用架構

應用架構如圖 5-2-1，其中參與單位包含進出口商、船公司、海關、保險商、仲裁與檢驗機構，當所有單位都擁有同一份帳本的情況下，就要考量資料的隱私、儲存方式、運用方式，例如鏈上只做資金交易、合約認證，其他隱私性較高的合約細節，如資金目的與客戶資料等，會先存在鏈外的資料庫，經由加密後傳至區塊鏈的帳本上做紀錄，不同的節點也會有不同的權限進行資料的讀取，主要可以區分為核心節點、交易節點與一般節點，接下來將會介紹各節點的權限管理方式與運做功能。

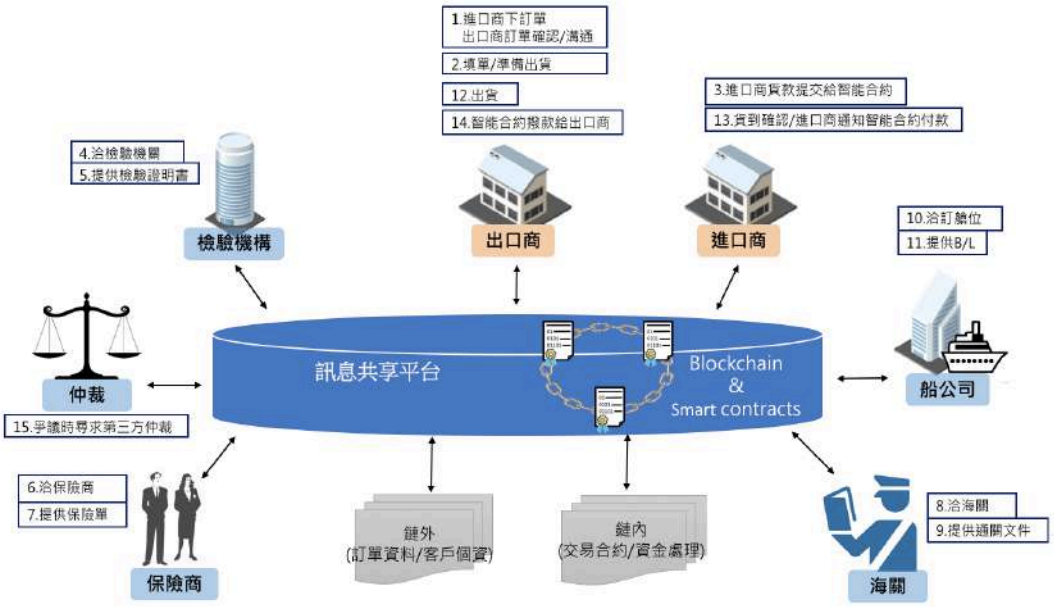

圖 5-2-1 區塊鏈於貿易融資應用模型圖

來源：本研究整理

3.節點權限管理方式

區塊鏈的導入，需要先界定出不同參與者的權限，讓銀行與中心廠協調關於資料隱私、法規等管理方面的議題，表 5-2-1 就是針對區塊鏈的應用權限做分類。

表 5-2-1 區塊鏈於貿易融資之節點權限分類

類型	單位	敘述
核心節點	政府貿易單位 銀行	可決定、審核進入私有鏈網路的單位以及做私有鏈核心系統的更新
運作節點	進、出口商 船公司	可進行交易、交易驗證的節點，也可以進行智能合約的設計
一般節點	檢驗機構 保險商 海關 仲裁	可查看私有鏈鏈帳本的節點，也可以不同角色對資料進行控管。

4.運作方式

如上述，不同節點會有不同的權限，分為核心節點、交易節點、一般節點，如下依序解釋。

- 核心節點部分

可先政府相關的貿易單位協助,連結其他國家一同制訂跨國相關的貿易單據標準、規章協定，再由銀行協助金流部分的規章協定，例如跨國匯款、各國金融法規等相關需要考量的因素。

- 交易節點部分

交易節點主是由進、出口方進行交易用，交易步驟如下：

步驟 1：進口者向當地銀行申請信用狀且放到區塊鏈上，讓銀行審核。

步驟 2：進口銀行接收通知且審核信用狀,同時有權拒絕或接受此合約。若是通過審核，信用狀會自動傳到出口銀行進行審核。

步驟 3：出口銀行有權依照出口方所提供的訂單資料評估是否要接受或是拒絕此信用狀，出口者可以看到此信用狀的申請狀況。

步驟 4：出口者完成出貨後，建立票據及出口資料，此筆資料若生效，會同步存到區塊鏈的帳本上。

步驟 5：出口銀行會審核出口商建立的出貨資料。

步驟 6：進口銀行會審查其資料，進口商會與帳本上的信用狀進行比對，當確認無誤，進口商就會支付交易金額。

步驟 7：如果進口商發現出口商給出的票據或是出口單據有誤，則進口商可以直接拒絕此筆交易。

- 一般節點部分

會依不同的權限索取不同的資料，例如監管單位則能看到屬於自己監管範圍的所有資料，包含金流、物流，或是保險單位可能就要要藉由進、出口商的權限開放，讓保險公司能取得投保相關資訊。

整體而言，區塊鏈應用到貿易融資的方式可經由對於金融單位與進出口貿易商的協調，藉由共享資訊，來降低銀行的風險，同時改善進出口商的融資效率。

（二）聯貸

如上所述聯貸有風險難以評估、事後問題的權責歸屬複雜等通點。WEF 2016 年的報告指出，使用區塊鏈在於聯貸業務的關鍵為建立風險評估架構，以供聯貸參與單位作評估、查核以及承保文件的標準化、在區塊鏈分散式帳本中的金流紀錄，圖 5-2-2 為 WEF 所提出的聯貸區塊鏈應用架構。

圖 5-2-2 WEF 區塊鏈在於聯貸業務應用架構

來源：世界經濟論壇(World Economic Forum),2016, The future of financial infrastructure :An ambitious look at how blockchain can reshape financial services

在於聯貸的區塊鏈應用，以三個部分做說明，首先在於組織銀行集團(Syndication)部分，可分為資料儲存與自動化兩個動作。在於資料儲存，如圖 5-2-2 的步驟 3，會藉由智能合約紀錄申請貸款企業的相關貸款記錄、還款記錄，

也會記錄參與聯貸銀行的風險容忍程度，讓主導銀行及參與聯貸的銀行團合作夥伴能快速掌握企業的信用風險狀況，而自動化的部分，主要是自動化承保，此部分可以讓主導銀行團藉由智能合約的自動風險評估來媒合適合的銀行作為合作夥伴，加快聯貸承保的效率，除此之外，也可以讓監管單位在交易的過程中同步監管，增加整體聯貸市場的安全性。

第二，在於查核(Diligence)及承保(Underwriting)的部分，可藉由智能合約中所儲存的聯貸計畫、企業財力證明來進行自動查核，讓銀行團判斷企業的聯貸是否安全，或是進行風險的評估，不用如一般傳統的聯貸，還要先協調由哪家銀行做風險評估，或是主導銀行在做完風險評估後要如何讓其他銀行團成員信任主導銀行所提供的資料，因為所有聯貸相關的交易都同步在分散式帳本上，可供所有銀行、監管單位查看。

第三，在於簽約及後續服務(Closing and Servicing)，原本過去主導銀行需要將聯貸資金以基金會的模式運作，流程繁雜，但使用智能合約，可以直接在智能合約上設定好資金的運用規則，不用特別以基金會的模式管理資金，增加貸款企業的資金靈活程度。

整體而言，聯貸在於區塊鏈的應用主要在於自動化風險評估、承保、資金管理，雖然效率可以有大幅的提升，同時運作的成本下降，但世界經濟論壇同份報告中指出，需要考量到如何協調各金融單位間、監管單位、申請聯貸企業間的文件、規章、法規。

（三）P2P 借貸

區塊鏈除了可以作為底層技術，讓一般民眾在 P2P 借貸平台上的交易更加安全外，在於未來，中、小企業的融資也可以效法 P2P 借貸平台，在平台上公開融資需求，由投資人自行選擇投資標的，其中需要先建立投資人、融資方的資訊，以及協調平台的管理方式。

區塊鏈在於 P2P 借貸平台的應用模式與上述貿易融資與聯貸的應用方式非常雷同，擷取貿易融資的應用，區塊鏈進出口貿易平台，相對 P2P 借貸就是建立投資人、融資需求方的資料共享平台，擷取聯貸所利用的智能合約自動媒合聯貸銀行合作成員，相對 P2P 借貸就是公開媒合投資人與融資企業，在於第三章的個案將會介紹 KPMG 與政治大學區塊鏈實驗室所提出的中、小企業平臺應用方式。

（四）供應鏈金融

在於供應鏈金融的應用，主要是讓中心廠更精準的掌控上游的供應商，圖 5-2-3，中心廠的上游有三個層級的供應商，此時中心廠就可以利用區塊鏈的分散式帳本來讓不同層級的供應廠商進行資料共享，再利用智能合約來記錄交易憑證，包含登記方、收/付款方、付款日期與區塊鏈存證號，這些記錄在區塊鏈上的資訊，就可以讓不同層級的供應商利用平台提出融資的需求。

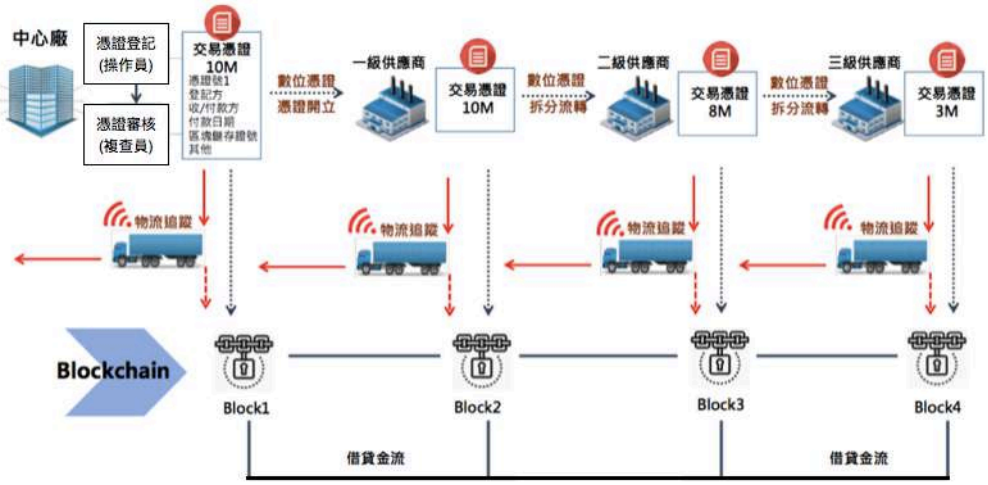

圖 5-2-3 區塊鏈於供應鏈金融應用架構圖

來源：華南金融科技比賽

在於供應鏈金融，雖然供應鏈生態的資訊是掌握在中心廠，但因為各國法規不同以及限制，中心廠可能無法直接利用這些資訊進行放款，但中心廠可以利用本身的資訊優勢，與外部的借貸公司合作，進行供應鏈的放款，在第三節的個案探討，將會介紹鴻海的富金通以及新創 P2P 借貸平台點融網共同利用區塊鏈所建立的供應鏈融資平台，Chained Finance。

第三節 個案探討

（一）新加坡區塊鏈相關計畫

新加坡的區塊鏈相關計畫，Mr. Ravi Menon，新加坡金融管理局(MAS)總裁表示[39]，區塊鏈分散式帳本的“Killer app”將會是在跨境交易的應用，而藉此新加坡當局將會以兩個面向作發展[40]，第一，貿易融資平台 Tradesafe，此平台是由星

[39] In a keynote address on October 9, 2017, at Global Blockchain Business Conference

[40] http://opengovasia.com/articles/8129-singapore-exploring-use-of-blockchain-to-link-national-trade-platform-to-trade-platforms-in-other-countries

展銀行與渣打銀行於新加坡的區塊鏈研究計畫，聚焦於利用區塊鏈紀錄貿易的發票與發票抵押狀況，期望未來能將供應鏈的所有資訊紀錄區塊鏈中，第二，建立National Trade Platform[41]（NTP），此部分是由新加坡海關(Singapore customs)所提出的方案，因為銀行在於貿易融資的部分，常常遇到跨國交易的資訊不對稱的問題，而導致融資業務虧損，故 NTP 主要目的在於跨國的貿易資訊交流，經由兩個發展方向，讓全球的銀行掌握貿易相關的資訊，概念如圖 5-3-1。

在此應用中，銀行與貿易商會利用新加坡的 NTP 平台，共享交易的文件，如發票(Invoice)的相關融資紀錄，銀行也可以藉由每筆融資紀錄來避免重複融資的風險，但在共享資料的過程中，還要考慮到銀行與貿易相關的文件，可能有隱私性，所以 NTP 平台在會先將隱私的文件 Hash 後，存到區塊鏈上，避免隱私的資訊外露。

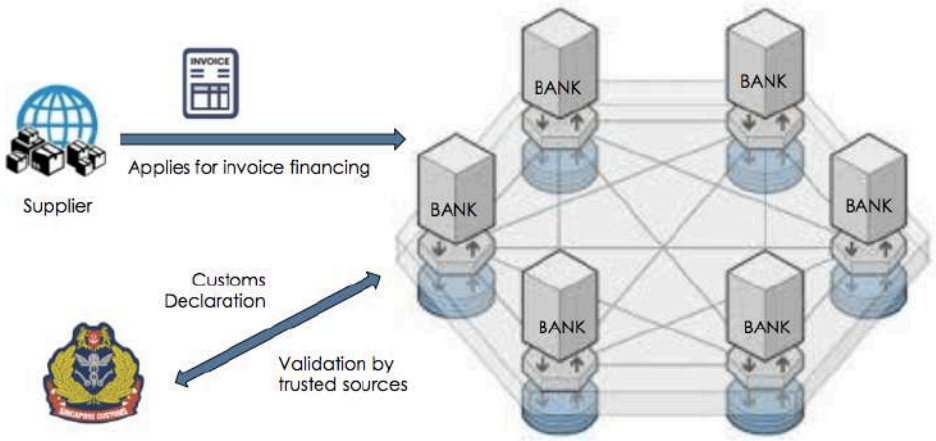

圖 5-3-1 新加坡應用區塊鏈分散式帳本於貿易融資

來源: Singapore Customs

（二）點融網&富金通金融服務商—Chained Finance

最後將探討在於創新應用的部分，首先介紹供應鏈金融的部分，中國新創企業，點融網與供應鏈中心廠，富金通合作，利用區塊鏈技術推出的 Chained finance 區塊鏈金融平台，在前述提到，銀行再於貿易融資最主要的困難就是取得供應鏈上多層供應商的資料，時間成本高，但供應鏈上的中心廠對於上下游廠商營運狀況非常熟悉，故相較於銀行的徵信部門，中心廠更有足夠的資訊來切入融資市場，對上下游的小型廠商進行放貸的信用評估。

[41]https://www.customs.gov.sg/about-us/national-single-window/national-trade-platform

點融網為 2013 年 3 月上線的 P2P 借貸平台，其中共同創辦人之一的蘇海德先生為全球最大的 P2P 借貸平台，Lending Club 共同創辦人，故點融網在創立之初，就擁 Lending Club 的核心技術，富金通本身是富士康旗下的金融服務商，擁有融資租賃、小額放貸、商業保險和私募基金管理等多項牌照，提供富士通集團上游的供應商與下游經銷商，雙方將共同推出區塊鏈的融資平台，命名為「Chained Finance」，目前將鎖定電子製造、汽車業與服務業等。

Chained Finance 主要提供的服務就是將多層級的供應商都引導至同一個平台，讓過去無法提供足夠的信用擔保資訊的中、小型企業也能享有融資的服務。

（三）KPMG+政治大學—中、小企業融資平台

此平台是利用 P2P 借貸平台加上眾籌平台的概念，讓有貸款需求的企業可以在平台上作媒合，而有閒置資金的投資人也可以利用平台找到適當的投資標的，但在於中、小型企業的融資不如一般個人的借貸，故 P2P 借貸的平台需要有更嚴謹的設計，其中包含平台會員的驗證及授權與平台活動的稽核，且為了監管及效率的平衡，所有交易都會經由智能合約自動化。

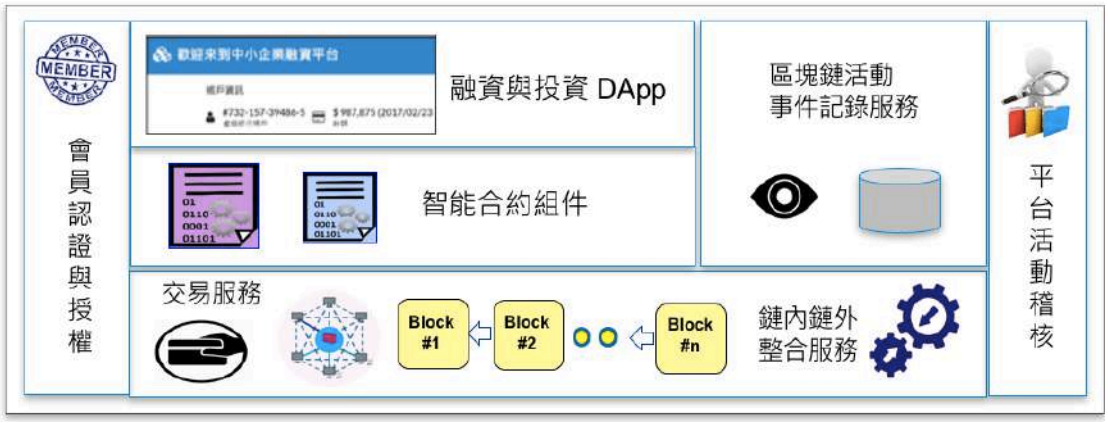

圖 5-3-2 中、小企業融資平台架構圖

來源：KPMG 金融機構區塊鏈發展成果說明

圖 5-3-2 中可以更清楚的看出平台的設計架構，包含會員、活動與鏈內鏈外的服務整合，還要記錄區塊鏈上的所有活動，再利用智能合約運作，運作內容包含融資案申請、實體資產與數位資產同步、投資案管理、債權管理與稽核等六種。

在於運作方面，此平台也設立了相關的監管方式，在圖 5-3-3 中，可以看到融資方與投資方還是需要在特約銀行進行開戶，透過金融體系的第一層防護，而接著再由實體資產轉為數位資產，放置到融資平台上，而此融資平台也會由外部

信評機與監理機構做第二層的防護，而最後在交易時，就會由區塊鏈本身的不可篡改，形成第三層防護，但在如此多層防護的情況下，此平台還是能增加借貸市場的流動性，平台利用眾籌的概念，當貸款需求方將需求放置平台上時，讓單筆資金需求拆分成多份小額的認購額。

區塊鏈平台會利用智能合約進行將融資的分成三層進行融資案的管理，首先第一層，每一個融資案都會有專屬智能合約，第二層，融資合約放置到平台上，第三層，智能合約會將融資合約拆成小額的債權，可讓投資人可以挑選不同的貸款需求進行投資，而投資人的資金會先圈存在第三層的智能合約圈存帳戶，當融資額達到標準時才會將圈存的資金匯到融資申請方的戶頭，此運作的優勢在於可以讓投資人清楚掌握融資源頭，以及確保融資額達標後有確實送到融資方，且在於融資方的還款與投資方的利息也都會經由智能合約做自動扣款還本息。

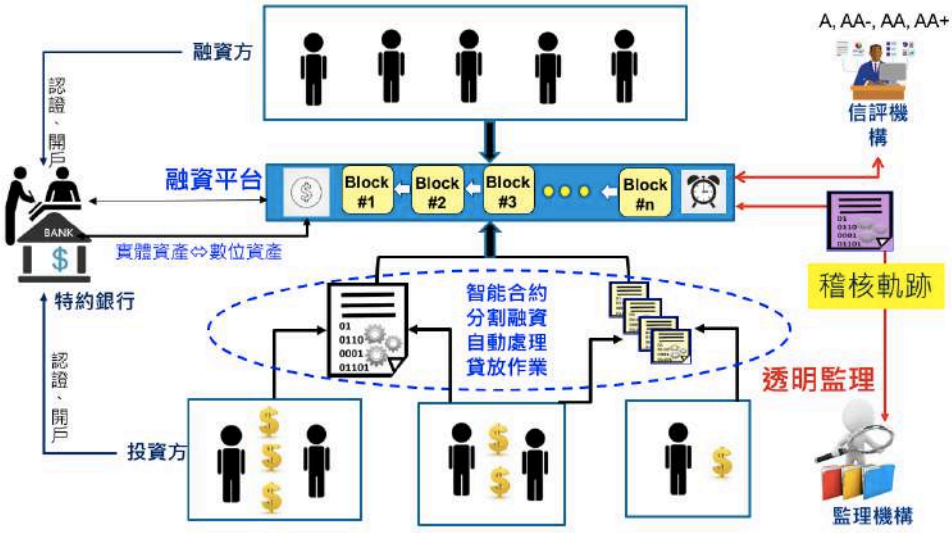

圖 5-3-3 中、小企業融資平台運作流程圖

來源：KPMG 金融機構區塊鏈發展成果說明

而此份成果說明也指出了使用區塊鏈平台的三大效益。第一，訊息透明，方便監管單位監管；第二，利用智能合約自動化作業，增加借貸效率；第三，創造據潛力之新金融商品，例如平台上利用智能合約分割融資金額，就可以增加次級市場的流動性。

第六章 區塊鏈在證券業之運用

證券是財產權的有價證券，本研究將以股票、私募等金融商品運作形態做探討，在第一節會由當前運作模式與問題切入，第二節再說明如何運用區塊鏈技術來改善當前問題和服務的提升。

第一節 證券業之現況分析

證券業整體的流程主要有投資人開戶、委託掛單/下單、撮合與結算交割，首先投資人在購買台股前需先至證券公司辦理開戶，開戶完成後再透過證券公司根據當前市場價格購買或是依照期望的價格委託掛單等待。下單訊息會從證券公司傳送到證券交易所，依照證券交易所下單價格與時間進行撮合。倘若撮合成交，最後將會進行結算交割的作業，本研究將會聚焦在最後的結算交割部分的系統做區塊鏈的應用探討。

臺灣在上市股票交割方面採行的是 T+2 日款券交割制度(Delivery versus Payment ,DVP) 。因此股票買進之後的次二個營業日(T+2 日)上午 10 時前，必須具有足夠的餘額於帳戶中，以支付買進股票。證券商會自動從買方的帳戶扣款，股票也會在同一天存進買方的的集保帳戶中。詳細的作業流程與參與機構如圖 6-1-1，而其中的參與單位與交易過程中的中介機構將依序介紹。

（一）參與單位

1.證券集中市場

在證券集中市場裡，投資人若要進行證券交易，需先至證券公司辦理開戶，之後再透過證券公司進行下單。投資人除可自行訂定價格外買賣外，也可依據市場價格進行買賣委託。接著投資人的買賣資訊會統一傳送到台灣證券交易所，依據掛單的時間與價格進行撮合。

2.結算機構

撮合完成後，證交所會依據當日交易結果以多邊餘額的方式進行結算與交割。在交割制度方面，現行所採的是款券 T+2 日交割制度 (DVP)。在交割期限內，投資人就其應繳交之證券及金額向證券商交割，證券商依其全部投資人經沖抵計

算後之應繳證券及金額向證交所交割，之後證交所會將交割訊息傳至集保所與央行同資系統。

3.交割機構

當集保所與央行同資系統收到交割訊息後，在證券部分，證交所在集保中心的劃撥交割帳戶會與證券公司在集保中心的帳戶進行交割；而款項部分，其清算銀行會經由央行同資系統，與證交所的清算專戶完成款項交割。

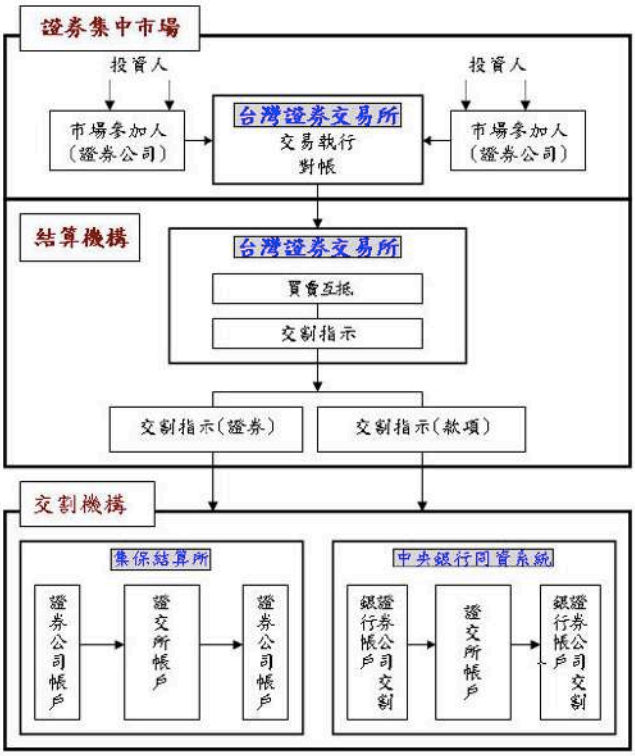

圖 6-1-1 台灣證券市場運作架構

資料來源：台灣證券交易所

（二）交易過程所經過的中間機構

1.證券公司

主要從事有價證券買賣之融資、融券，或融資與融券買賣之代理。依證券業務不同，可分為證券承銷商（Underwriter）：承銷商是指經主關機關特許以包銷或代銷發行之有價證券的證券商；證券自營商（Dealer）：指經主管機關核准，特許自行買賣有價證券之證券商；證券經紀商（Broker）：指經主管機關核准，特許經營有價證券買賣之行為、居間、代理，一般投資人大多透過證券經紀商來進行證券的買賣。

2.證券交易所

證券交易所是買賣股票、公司債、公債等有價證券的市場。集合有價證券的買賣者，經過證券經紀人的居間完成交易。

3.集中保管結算所

主要從事證券的集中、保管與結算等業務，另外還負責有價證券的無實體發行登錄、集中保管、帳簿劃撥和短期票券的結算業務等。

第二節 應用區塊鏈技術於證券業

目前的台灣證券交易市場以集合競價為主，盤中每數秒撮合一次。現階段也正研擬推行逐筆交易，而逐筆交易開放後所產生的高頻交易可能會被當前區塊鏈技術的吞吐量瓶頸及儲存容量所限制。此外，導入後資料儲存的成本也比傳統資料庫高。雖然如此，區塊鏈的導入對於證券業來說，能改善以下幾點問題:

- 縮短結算交割的時間:

台股的結算日期為交易後兩天 (T+2)， 因此投資者交易完成後，資金無法立即取得，限制了投資者的資金運用。透過智能合約的方式，自動化結算與交割的流程，將能縮短交易處理的時間。

- 減低錯誤發生的機率:

在當前交易的處理流程中，證券公司會先將它們的交易訊息發送給證交所，經過證交所的交易撮合後，再將訊息匹配到各個證券公司。此方式會將風險集中於證券公司與證交所，當處理過程發生系統故障或者人為操作失誤，可能就會導致系統無法恢復的後果。此外在證券和資金的保管上，也可能因保管漏洞或錯誤而發生損失的風險。因此可利用區塊鏈多節點的特性，以及智能合約的自動驗證和交易處理方式，以降低可能發生的錯誤。

- 降低交易風險:

當買賣雙方撮合完成後，會給予雙方 T+2 日的結算時間。若結算參與人不能足額履行交割義務，則會造成交易失敗。此部分可藉由智能合約的條件驗證，減少交易失敗的機率。

- 提高交易管理效率:

現金和證券的轉移會在證交所與各個證券公司之間進行，轉移之後資產保留在證交所與各個證券公司的帳戶裡。對大眾投資人而言，交易主要透過中介公司

執行，此種間接模式對投資人而言會造成結算與交割的具體時間不明確，以及帳戶保管缺乏靈活性和保管成本的增加。因此可利用區塊鏈去中心化的特性，直接完成交易與訊息同步紀錄，以提高交易即時性與減少中介的限制和成本。

- 防範不法行為的發生:

各國銀行在洗錢防制與 KYC 上投入相當多的成本，像是目前許多銀行在開戶時，需要客戶提供雙證件確認其身份並瞭解開戶動機與目的等事項，評估開戶合理性，並且經銀行檢核確認，且於完成開戶審核作業，例如：KYC(認識客戶)後，始可受理開戶。因此利用區塊鏈技術除了可以確認帳戶擁有者的身分外，利用區塊鏈的資料公開透明以及不可修改的特性，也能減低不法行為的發生。

由上述說明可知，雖然當前區塊鏈技術存在著處理速度慢與資料儲存成本較高等問題，但就現今存款低利率的時代，可利用導入區塊鏈技術來提高資金流動率以及降低中間處理作業的成本，進而優化整體金融市場的環境。

根據歐洲央行報告指出，區塊鏈的導入並不會完全的去中間化，中間機構還是有存在的必要。從公司申請證券的發行開始，則須有可信任的第三方機構去審核發行公司的條件與背景，發行期間也必須確保發行數量，以降低發行風險。發行的所有資訊也必須做權限上的管理，DLT 具有相當高的安全性，因此需要可信賴的第三方機構做資訊保密與驗證的工作。另外上市公司在證券發行的期間，若不幸發生破產的情形，則必須交由第三方單位來執行抵押與清償的動作，以保障投資人的權利。

（一）區塊鏈導入目前證券業方式

區塊鏈的導入會有不同層面的影響，甚至完全改變現階段的運作架構。由於證券交易牽涉的機構眾多，其複雜的交易作業除了增加處理成本外，也相對提高人為錯誤的作業風險。據歐洲央行的報告估計，若將現行的處理作業以區塊鏈技術取代，將可能減少約 12 億美元的作業成本。然而，導入區塊鏈最大的挑戰，仍在於如何降低新技術對現行體系的衝擊以及法規上的限制。由於金融業是高度管制的產業，為維持交易的穩定與風險的降低，可以用漸進式的方式來進行導入，就以下三種方式來進行說明。

方式一：將部分機構導入於區塊鏈，進行共享資訊，以提高作業效率

當證交所接受證券公司的訊息後進行撮合，可將訊息放入區塊鏈的分散式帳本中，以保障交易雙方。之後證交所根據撮合後的結果來決定交割訊息，並同時記錄於區塊鏈的帳本中。接著，集保所與央行同資系統透過帳本上的訊息確認交割指示後，會自動執行款券的轉移。此方式在維持現有作業機構下，將部分重要機構導入區塊鏈架構中，以簡化目前層級複雜的清算及結算交易流程，並透過智能合約（Smart Contracts）自動化作業，減少人為錯誤，降低證券交易的作業風險和提高資訊管理上的效率，讓整個款券轉移流程更加的安全可靠。另外，利用區塊鏈也可以降低證交所的稽核成本，證交所為確保交易款券流動上的正確性，一般會對證券公司不定期針對交易帳本、款券項目等作查核。因此透過彼此共同擁有的可信賴帳本，可減少稽核所花費的成本。在方式一的架構之下，參與區塊鏈網路的機構均需要事先認證，參與機構的權限也會受到限制，僅被賦予與機構本身角色有關的權限，例如系統管理、交易提交、交易驗證、清算結算、稽核等，這種形態的區塊鏈即為典型的私有鏈，而其做法是盡量保留現行的交易體系及作業模式，以降低對現行機構所造成的衝擊，並與其他組織及參與者進行資訊系統整合的目的。

1.區塊鏈網路架構：

圖 6-2-1 區塊鏈導入證券業方式一

2.各節點功能與權限說明：

- 證交所

此節點主要將證券撮合後的結果寫入到區塊鏈的帳本中，可查看當前市場所有的交易資訊與狀態。而各證券公司也可透過證交所查看本身公司於共享帳本上的相關交易資料。

- 集保所

當交易透過證交所撮合結算，接著會進入待交割狀態。集保所透過查看分散式帳本(DLT)上的交易狀態資訊，得知待交割的交易項目並進行交割的處理作業。此節點主要將交割的處理結果寫入，因此可查看當前所有證券公司持有證券與轉移的資訊。各證券公司也可透過集保所查詢當前所持有證券之紀錄資訊。

- 央行同資系統

此節點可查看當前所有證券公司款項轉移的資訊，主要負責款項轉移的處裡並將處理後的結果寫入於區塊鏈上。另外，各證券公司也可透過央行同資系統查詢當前所屬帳戶之款項資訊。

上述的優點除了節省成本和對現有架構所造成的衝擊較低之外，與 DLT 鏈外的資訊系統的連結及整合也較為容易，因此對初期的導入可行性最高。不過相對的，由於交易仍需要中介機構的介入，與現行架構差異不大，因此對導入 DLT 所帶來的期望效益可能有限。

方式二：移除部分中介機構，使證券公司之間可以直接撮合交易

在集中市場裡，一般投資人還是必須透過證券公司進行下單，但交易撮合後的結算與交割工作則是完全透過智能合約去執行。當身為買賣雙方的證券公司達成交易協定後，證交所會負責管理雙方款券交付的處理作業。當雙方款券確認皆已滿足交付條件後，智能合約會立即自動執行交割的動作。在此架構中，證交所的身分偏向平台管理者的角色，主要確認雙方款券是否能到位。而在證券發行人部分，不同以往發行實體證券後放置集保所，在於方式二，會透過區塊鏈發行數位化證券，因此能直接在區塊鏈上進行證券持有人間的買賣轉移，不需透過集保所執行實體管理票券的作業，提升了搓合流程上的效率。

1.作業流程圖：

圖 6-2-2 證券公司撮合交易流程圖

2.分散式帳本架構：

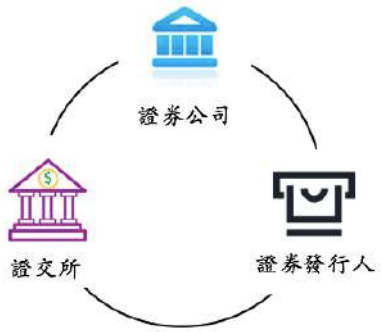

圖 6-2-3 區塊鏈導入證券業方式二

3.區塊鏈各節點功能與權限說明：

- 證券公司

此節點主要將自身所送出的交易需求寫入到區塊鏈中，也可根據登入的帳戶權限，查看當前市場自身的交易資訊與狀態。

- 證交所

此節點主要將交易結果寫入到區塊鏈中。當證交所根據買賣雙方的款券資訊確認交易雙方款券皆足額後，系統會自動執行結算與交割的動作。因此除可查看當前所有證券公司交易與轉移的資訊外，也可查看交易雙方的持有款券數量。

- 證券發行人

此節點主要將自身所發行的數位證券資訊做區塊鏈的寫入，包含所發行數量與價格的資訊。因此可查看當前自身所發行的證券數量、價格與持有人等資訊。

方式二的特點是具備去中心化的清算交割機制，證券商可直接在 DLT 上進行證券買賣，交易的過程也會變得更透明且更有效率。由於 DLT 共享資料的優

點，此架構下所有的參與者共用同一份帳本資料，不會有傳統資料庫系統進行『two phase commit』時所需付出的系統成本（overhead）。不過相對的，分散式即時總額結算（RTGS）在實作上較為複雜，其執行效率比起傳統 RTGS 來說也較為低落。在安全性的考量上，由於券商可直接在 DLT 上進行清算作業，且客戶的帳戶及交易資料均存在於 DLT 上，因此如何保護客戶隱私以及資安防護，將會是導入此型態前所需要考慮的重點。

方式三：直接以點對點方式交易

在此結構下，投資人交易不需透過證券公司下單，而是直接經過電腦撮合與交易的另一方進行買賣。而目前的後續交易流程，也會被智能合約所取代，直接由智能合約做自動結算。因此參與者只會有投資人、證券發行公司與監理單位，能減少交易的作業流程。對於重視市場環境應變的中小企業與新創公司而言，在於資金的籌措將會更有效率促進企業成長速度以及活路整體市場。但因為是投資人雙方直接交易，缺乏中間交易機構的風險控管，所以 KYC 會是此模式架構的重要關鍵。因此監理機關的參與是必要的，主要工作就是對於投資人做身分與風險的管理。目前國外有許多國家開始用區塊鏈技術來做身分的認證，此認證可應用於金融交易上，也可應用於納稅與投票等公共事務的參與。

1.作業流程圖：

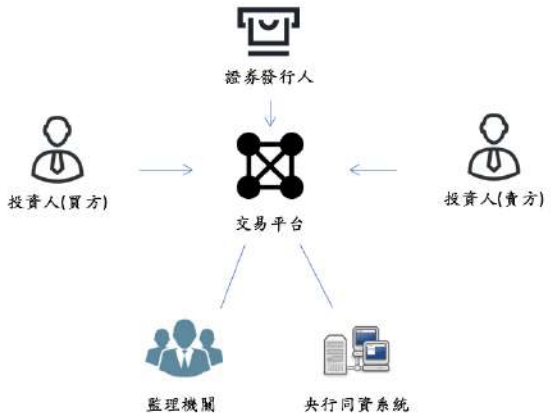

圖 6-2-4 證券業點對點作業流程圖

2.分散式帳本架構：

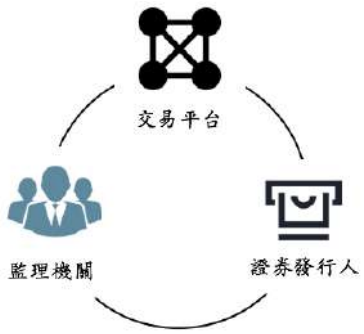

圖 6-2-5 區塊鏈導入證券業方式三

3.區塊鏈各節點功能與權限說明：

- 交易平台

此節點主要負責將投資人所送出的交易需求寫入到區塊鏈中，因此投資人可根據登入的帳戶權限，查看當前市場自身的交易資訊與狀態。而平台系統會根據區塊鏈上的資訊進行撮合並將結果寫入到區塊鏈中。

- 監理機關

此單位主要管理與監督證券的交易，以及風險上的控管。因此監理機關除了能查看所有的交易資訊外，也能蒐集到投資人的相關基本資料 (KYC)，以減少交易問題和防範不法事務的發生。

- 證券發行人

此節點主要將自身所發行的數位證券資訊寫入區塊鏈的帳本，包含發行數量與價格的資訊。因此可查看當前自身所發行的證券數量、價格與持有人等資訊。

在於方式三，民眾能直接經過申請進入 DLT，但因為少了中介機構的管理，所以對於 AML（防洗錢與防資助恐怖主義）的作業上將會有很大的挑戰。另外，由於交易是投資人直接點對點進行，沒有任何中間機構的介入，所以當發生交易糾紛或是遭到詐騙而有金錢上的損失時，民眾可能會有求助無門的風險。再者，由於 DLT 的資訊透明化特性，對於投資人交易的隱私性也將會是一大課題。目前開發當中的相關技術，例如零知識證明（Zero Knowledge Proof），將會是未來導入此架構的重點項目之一，但是此技術也會對系統作業效率有所影響，在隱私

與效率間如何平衡或抉擇，將是區塊鏈技術未來須解決的關鍵課題之一。

（二）區塊鏈導入私募

私募是一種不以公開方式募集資金的證券融資方式，大部分對小規模的特定投資人發行。依據我國證券交易法第 43 條 6 之規定：向「特定人招募有價證券之行為」。其中特定人可區分為三類，第一類為銀行業、票券業、信託業、保險業、證券業或其他經主管機關核准之法人或機構、第二類為符合主管機關所定條件之自然人、法人或基金、第三類為公司或其關係企業之董事、監察人及經理人。

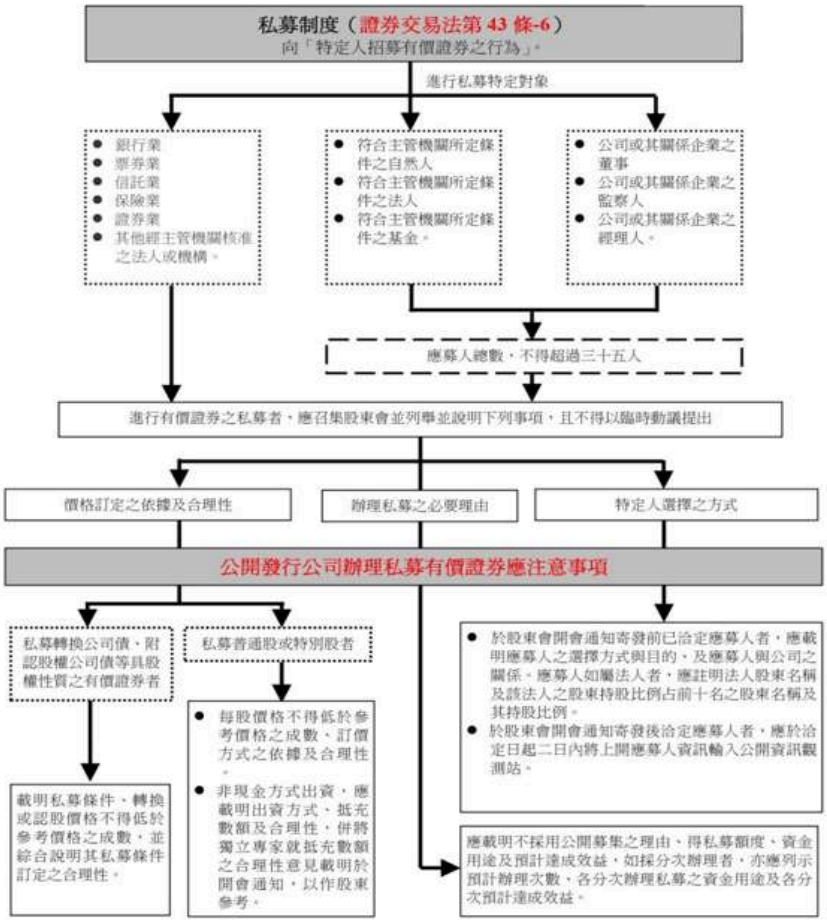

圖 6-2-6 證券業私募制度

資料來源：證券暨期貨月刊

區塊鏈導入私募方式

以私募的方式進行融資可保障尚未公開發行之公司的內部管理獨立性同時滿足其資金上的需求。現行私募交易的結算需幾天的時間，且私募過程有許多需要人工的程序來與第三方之間的作業做銜接。在現有制度和流程上與上市股票交易類似，都有在結算上所需花費的時間成本與行政作業上的風險。因此透過區塊鏈技術，能以自動化的方式減少結算的時間以及去除人為與第三方作業過程中的風險。

1.流程架構：

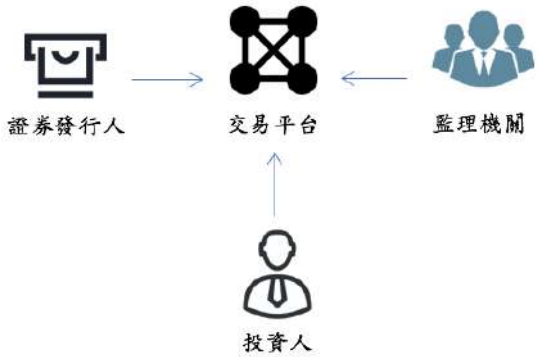

圖 6-2-7 私募流程

2.分散式帳本架構：

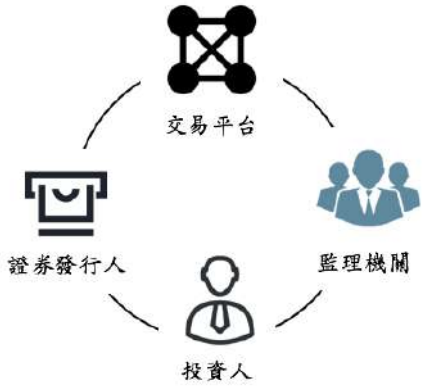

圖 6-2-8 區塊鏈於私募應用架構圖

3.區塊鏈各節點功能與權限說明：

- 交易平台

此節點主要為接收證券發行人所送出的交易需求寫入到區塊鏈中，如募資目標與特定投資人資訊等。之後系統根據所要交易的特定投資人進行訊息的發送，已進行認購與交割的動作。而後續持有人的相關權利會根據智能合約自動完成。

- 監理機關

此單位主要管理與監督證券的交易，以及風險上的控管，因此監理機關除了能查看所有的交易資訊之外，也能蒐集到投資人的相關基本資料(KYC)，並且可對證券發行人進行背景的審核以減少交易問題和防範不法事務的發生。

- 證券發行人

此節點主要將自身發行的數位證券資訊寫入區塊鏈的帳本，包含所發行數量、價格與特定投資人等資訊。因此可查看當前自身所發行的證券數量、價格與持有人等資訊。

- 投資人

此節點主要將自身所收購的數位證券資訊寫入區塊鏈，包含所持有數量與價格等資訊。因此可根據帳戶權限查看當前本身所持有的證券數量、價格與等資訊。

第三節 初次代幣發行(ICO)

ICO 的全名是 Initial Coin Offering，應該是仿照 IPO（證券公開發行）造出來的詞彙，反映它也是一種資金募集的方式，但差別在於 ICO 的發行標的物是一種 coin 或 token（以下統稱為代幣）而不是證券，以及所接受的資金不是法幣，而是某種具市場價值的虛擬貨幣（主要是比特幣或以太幣）。此外，募資的目的通常是從事區塊鏈相關的產品或服務開發。從它的源頭來看，ICO 更像是群眾募資（Crowdfunding）。第一個 ICO 的案例是發生於 2013 年中，由 J.R. Willett 為他所提出的第二代比特幣開發計畫發行代幣 MasterCoin（2015 年改名為 Omni），向大眾募資，大約一個月的時間募集了 5 千個比特幣，依當時市價，約當 50 萬美元。但一直到 2016 年以前，並沒有很多的 ICO 案例，也沒受到太多人注目。

自 2016 年中開始，ICO 的案例與金額開始迅速增加，到 2016 年底，54 個主要的 ICO 案子就募集到超過 1 億美元，其中 ICONOMI 一案就募集了 1 千萬美元。2017 年起，ICO 更是勢不可擋，截至 7 月底，92 個 ICO 案例共募集了超過 12.5 億美元。根據高盛等機構的統計（請參考圖 6-3-1），今年六月與七月，ICO 募得的金額已經遠遠超過全球互聯網創投基金所投入的天使與首輪種子基金。不僅如此，今年 5 月 31 日 ICO 的 BAT，於短短 30 秒內成功募得 3 千 5 百萬美元；八月間 Filecoin 的 ICO 則在 60 分鐘內募集到約 2.5 億美元，成為史上金額最高的案例。根據 Coindesk 的 ICO Tracker 的統計，到今年 11 月 16 日止，累積的 ICO 募資總金額已經超過 36.3 億美元。

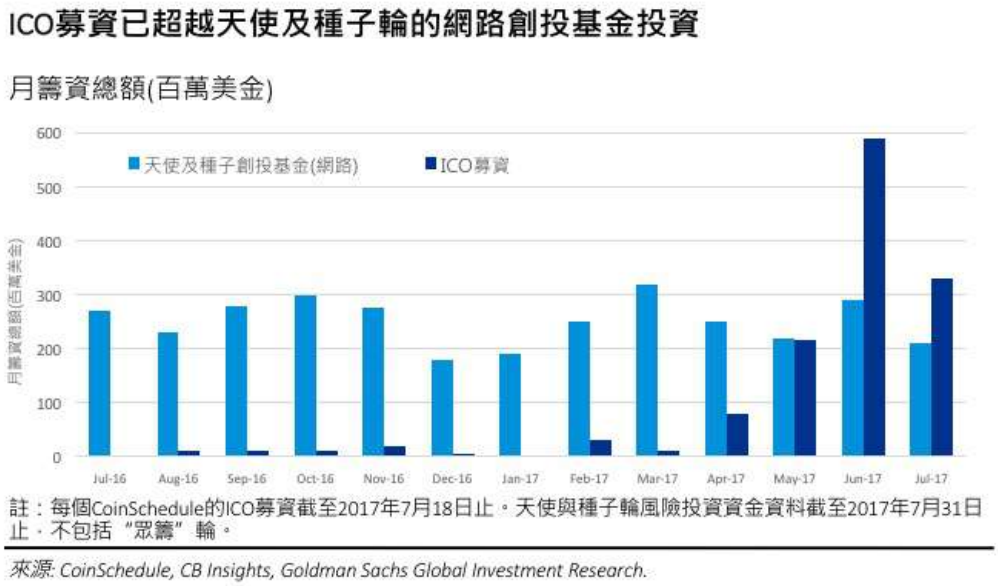

圖 6-3-1 ICO 募資成長圖

我們可以從創業者、投資者與技術平台三方來分析這兩年來 ICO 案例大幅成長的原因。首先，對創業者來說，ICO 可直接訴諸投資人，免除中間機構的審核；在創業初期，透過產品白皮書的資訊，便就快速取得投資者資金，此讓 ICO 比起其它籌資管道有明顯的優勢。對投資者而言，目前的 ICO 均以虛擬貨幣發行代幣，由於比特幣與以太幣對美元的兌率近期持續上漲[42]，帶動了投資者對虛擬貨幣的無限想像，短期市場上流通性高，暫無漲跌幅的限制，也自然獲得眾多投資蜂擁地投入 ICO 的市場。最後，目前大多數 ICO 的主要技術平台均是以太

[42] 此為 2017 年度狀況，但近期(2018 年) 比特幣與以太幣對美元的兌換率不升反跌，且價格波動劇烈

坊區塊鏈，其提供的 ERC-20 程式協定發行[43]，大幅降低發行代幣的技術門檻，並且讓擁有這些代幣的用戶，得以在很多虛擬貨幣交易所進行交易，形成高度流通性。

其實以太坊本身就是一個早期的 ICO 成功案例。2014 年中，以太坊的創辦人為了籌措開發所需資金，發起了群眾募資的活動，號召支持者，以比特幣按一定比例（從 1:2000 到 1:1337）換取以太坊即將發行的以太幣。結果在 42 天內順利募集了 3 萬多個比特幣，當時價值約當 1,700 多萬美元。這種以現在具有市場價值的虛擬貨幣交易即將發行的代幣的募資作法，在當時算是一項創舉，也為日後的 ICO 建立了典範。目前比特幣對以太幣的兌率大約在 1:30 以內，所以當初參與的投資者，如果現在仍持有那些換來的以太幣，投資報酬率是非常高的。

但 ICO 也不是沒有問題的，2017 年 12 月 11 日美國證券交易委員會(SEC)下令要求位於加州的 Munchee 公司終止發行他們用來募資的代幣（Coin）MUN，並須將已募集的 1,500 萬美元退還給投資人。SEC 為什麼會介入干預呢？多數的 ICO 都是類似以報償為基礎（Rewards based）的群眾募資，為了要開發區塊鏈相關的產品進行籌資，它們發行的代幣主要是用來作為使用該產品特定的功能的權利。例如，上述的 Filecoin 的提案是要發展一個基於區塊鏈的硬碟共享服務，以其發行代幣作為供需兩方的交易基礎。另一個案例 BAT 則是要發展一個基於區塊鏈的數位廣告平台，目的在改變現有的廣告投放模式，新模式下投放廣告需要 BAT 代幣，用戶看到好的廣告可捐贈 BAT 代幣來支持內容商，讓優質內容商能獲得更多收入。但是有少部分的 ICO 所發行的代幣從具實質性使用功能，轉向代表相關資產的未來收益權，甚至是有價證券，因此觸動了的證券交易法之管理問題。

這類 ICO 中最有名的案例就是 2016 年五月舉行 ICO 的 The DAO（虛擬自治組織）[44]，它是一個基於以太坊上智能合約而運行的創投基金的變形，在短短 24 小時內募得價值約 1 億 2 千萬美元的以太幣，不過稍後因為程式安全漏洞而停止運作。SEC 經過長期的研究，於 2017 年 7 月 25 日發布了對 The DAO 的調查報告，表明這個 ICO 專案根據美國法律已經構成了證券的發行，如果它仍然存在，發行方 The DAO 需要依法辦理證券發行的登記，支援交易 The DAO 代幣

[43] Ethereum ERC20 Token Standard: https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[44] https://en.wikipedia.org/wiki/The_DAO_(organization)

的虛擬貨幣交易所也必須依法登記為證券交易所，否則就違法。

SEC 依據所謂的 Howey Test[45]來判定 The DAO 的 ICO 是一種證券的發行，這個 Howey Test 採用了四個項目來判定金融商品是否是證券：有金錢的投資與獲利的預期，投資形成共同的事業以及利潤來自他人經營管理的投入。根據 The DAO 的白皮書，它的運作模式的確符合以上要項：ICO 參與者投入具有金錢價值的以太幣，它是參與者們之間的共同事業，參與者預期透過投資獲利，但主要經營管理者是一固定團隊，而非所有的參與者。因此，SEC 認定 The DAO 涉及證券的發行。這次加州的 Munchee 公司的 ICO 案也是一樣，SEC 依照 Howey Test 將其判定為證券的發行，所以必須即刻停止與終止。

儘管如此，這兩個案例只是說明，SEC 的監管主要還是聚焦在證券領域，而不是全面性的封殺 ICO。從另一個角度來看，ICO 的發起者最好先自我檢視是否能通過 Howey Test，否則難免要依證券相關法規處理。就像群眾募資的發展，也有走向以股權為基礎的模式，而必須納入證券交易法管理。除 SEC 以外，新加坡金融管理局 (MAS) 也抱持對 ICO 採逐案評估的原則，並明確指出：“有些 ICO 可能會受到《證券和期貨條例》第 289 章的約束，有些可能不會”。

目前對 ICO 採全面封殺的主要國家是中國大陸，主要原因在於今年以來，各式各樣的 ICO 過於氾濫，已經達到萬物皆可 ICO 的地步，許多不可思議的 ICO 也在短時間募得高額資金，例如：2017 年 7 月 PressOne 的 ICO 上線，連白皮書都沒有，就宣稱要募資 2 億美元，最後雖然沒成功，但也募到約 1.25 億美元。瑞士則是目前對 ICO 相對友善的國家，全球前六大 ICO 活動，其中四個在瑞士發行。(分別是 Tezos，募集 2.38 億美元；Bancor，募集 1.56 億美元，DAO 募集 1.42 億美元，Status 募集 9500 萬美元。) 但瑞士金管局 (FINMA) 也於 2017 年 9 月發布關於 ICO 的指導方針 (FINMA Guidance 04/2017)，對 ICO 加以規範。

在極短的時間內，ICO 變成一個炙手可熱的議題，這顯現市場上渴望創新商業模式的契機，但如何讓這樣的商業模式變成一個健全的生態圈，迄需主管機關給予適當的引領與鼓勵。若在合理的框架管理下運用，ICO 不失為數位商業模式的典範，但如何滿足監理單位對於客戶身分識別 (KYC)、洗錢資恐防制(AML)、消費者權益保護的關注，應該所有的 ICO 發行業者思考的議題。

[45] http://consumer.findlaw.com/securities-law/what-is-the-howey-test.html

ICO 監管議題

ICO 在發行以及應用的過程中，最主要的爭議有三點，分別為投資人保護、洗錢以及現有法規的衝突，投資人保護的爭議主要是因目前 ICO 品質難以評估，且無特定的法規來進行監管，讓投資人受騙後面臨沒有求償管道的困境，洗錢的部分主要是因 ICO 所發行的代幣通常可在數位貨幣交易所進行兌換成法幣的行為，且過程因區塊鏈的特性，容易匿名，讓交易平台淪為洗錢的溫床，最後是在於現有法規的衝突，ICO 目前尚無法律可監管，故目前各國政府紛紛針對 ICO 所產生的問題進行法律制定的研究。以瑞士為例，瑞士政府將 ICO 所發行的代幣目的分為三類做監管，支付代幣(Payment token)、功能代幣(Utility token)、資產代幣(Asset token)，除了各國政府對於 ICO 所發行的代幣做監管外，社群媒體臉書(Facebook)在今年 1 月也宣布禁止任何廠商投放 ICO 相關的廣告，由此可看出 ICO 監管議題的重要性，本文將以瑞士的分類作為探討的主幹。

1.支付代幣(Payment token)：

是指用途僅限於支付用，類似於傳統貨幣，故在實際應用時大多會需要符合洗錢相關的防治法規，在瑞士，主要是將 ICO 的支付代幣的監管方式歸類於洗錢防制法下，另外在新加坡，新創企業若是發行的 ICO 代幣是單純支付的功能，則要符合 MAS 所發布的洗錢法治及打擊資恐的要求。

2.功能代幣(Utility token)：

是指當 ICO 本身是主打提供某項產品或服務時，就會被歸類在功能代幣，雖然目前各國均無明確地表明要如何監管，但各國政府都會向投資人宣導要注意相關的投資風險。

3.資產代幣(Asset token)：

是指當代幣本身會讓持有人獲取股息或是有權參與發行組織的決策時，此代幣就會被視為有價證券，須受證交法的規範，在瑞士則是分為兩類，除了上述的證券類型適用於證交法外，若是 ICO 的代幣有返還本金的概念，則要以銀行法進行監管。

另外以本文所提的美國 SEC，其依據 Howey Test 的四個項目來做 ICO 是否為證券來做監管，特別的是美國 SEC 還自行發行 HoweyCoin 的 ICO 代幣[46]，此代幣的白皮書表明可用於旅遊相關的旅社、交通等相關花費，但此 ICO 項目期實是一項詐欺測試，只要投資者點入官網就會連結到 SEC 的官方網站[47]，藉此提醒投資人需要注 ICO 的投資風險。而新加坡 MAS 則是明確指出假如 ICO 所發行的代幣滿足新加坡「證券期貨法」以及「金融顧問法」下對於「證券」的定義就應以該法監管。

除了上述政府對於 ICO 的監管，ICO 業者也須負起相關的責任，如新加坡的 ICO 業者就需要提供 ICO 平台讓投資人公平參與投資，且若是涉及證交法監管，則需要取得相關的執照，若是 ICO 是針對數位貨幣投資的業務，則需要取得財務顧問相關的執照，最後，若是平台只單純提供數位貨幣的交易媒合，則需要在架設網站以及營運前取得 MAS 的許可，且在 2018 年 5 月新加坡當局已禁止未經過審核的 ICO 代幣於交易所販售，同時警告新加坡當地八家數位貨幣交易所嚴格把關 ICO 代幣的合法性。

在於交易所的監管，除了新加坡當局外，日本金融廳(Financial Services Agency,FSA)也在 5 月向大型交易所 Coincheck 明確指示，禁止提供匿名/匿蹤功能的虛擬貨幣交易，此類虛擬貨幣因其難以追蹤的特性，容易被當成洗錢的媒介，甚至被用來資助恐怖主義(AML)，如 Monero、Zcash 與 Dash，故日本的 Coincheck 正式將這三種數位貨幣下架，另外日本金融廳對於數位貨幣的監管也間接影響到鄰近的韓國，韓國大型交易所 Korbit 也在近期宣布不再提供 Monero、Zcash 與 Dash 的交易服務。由新加坡、韓國與日本對於交易平台的施壓可看出除了 ICO 發行業者外，數位貨幣的通路也是監管的重點之一。

在於監管最嚴謹的中國，雖然目前全面禁止 ICO 的任何活動，但中國當局在於區塊鏈的領域還是有意進行相關的研究，只是態度較為謹慎，故在監管方式尚未明確訂定前將不會隨意開放區塊鏈相關的應用。表 6-3-1 為瑞士、新加坡、美國與中國四個國家針對支付代幣、功能代幣、資產代幣的監管方式或法規的整

[46] https://www.howeycoins.com/index.html

[47] https://www.investor.gov/howeycoins

理。

表 6-3-1 各國對於三類 ICO 代幣的監管方式

	瑞士	新加坡	美國	中國
支付代幣	ICO 發行機構等同於洗錢防制法下提供服務的金融機構。	MAS 所發布的洗錢法治要求。	支付服務機構相關法規監管 向 FinCEN 註冊。	禁止
功能代幣	提醒投資人要注意實質上是否構成資產代幣。	未作出監管說明。	提醒投資大眾需注意相關風險	禁止
資產代幣	證交法 銀行法	證券期貨法	證券交易法	禁止

回到台灣本身，台灣目前已有的銀行法、證交法可對於上述第一、三類進行監管，另外在於洗錢的議題，若是 ICO 所發行的代幣能與法幣互通，則需要遵循政府所制定的 KYC 要求，並進行交易的可疑偵測與回報，而第二類的功能型代幣，因為各國均無明確的法規，故台灣可利用監理沙盒來做實驗，直從各種申請監理沙盒的新創企業來評估適合的監管方式。

整體來說，除了政府外，在於 ICO 的發行單位與投資者也都要建立基本的道德標準，如新加坡對於 ICO 業者的基本責任，或是美國 SEC 利用假 ICO 專案來對投資者的宣導都是為了避免在監管尚未明確前能減少詐欺或是違法的行為，為保重投資大眾的權益，除了 ICO 業者本身要建立起良性的生態圈外，主管機關也可就 ICO 已蓬勃發展的事實，釐清法規的適用性，進行適當的調整或設立專法，以提出具的的因應政策。

第四節 個案探討

區塊鏈在於證券業的應用，會分為一般應用以及創新應用，一般應用主要是在於交易安全、結算效率與降低整體證券風險；而在創新應用上，則會介紹 DAO 這個經由智能合約自動化交易、平台監管的案例，最後，會詳細介紹日本交易所

集團在於區塊鏈的應用方式及流程。

（一） TØ

TØ 是線上 Overstock 零售公司旗下以區塊鏈技術開發的證券交易公司。在 SEC 的核准下，該公司於 2016 年首次在此平台上成功募得了近 200 萬美金的資金，且實現了即時結算。此開發公司成立於 2014 年，成立初衷是希望利用區塊鏈技術去取代特定的證券交易，打擊一些裸賣空（naked short-selling）的不當行為和因透過第三方所造成的損失。旗下 DLR (Digital Locate Receipt) 平台能透過區塊鏈去中心化的特性，減少了中間單位的處理時間以及風險。此外將交易資料紀錄於區塊鏈上，能使資訊更具透明度，對於交易的監管和不法行為的防治更加有利。由於資訊紀錄於區塊鏈中，能使交易紀錄不被竄改，也因此讓平台更具信任度。2017 年 TØ 宣布將進行 ICO 的發行，其發行的代幣 tZERO 預計募資超過 5 億美元，換取的代幣也能在平台上使用。

（二） Linq

Linq 是 Nadaq 與區塊鏈公司 Chain 所合作開發的私募交易平台。透過區塊鏈去中心化的特性簡化了交易流程，且交易雙方透過線上交易能有效減少許多人工的作業，使得透過 Linq 私募股票能縮減結算時間。開發商 Chain 指出：現有區塊鏈技術的應用能將結算時間縮短到十分鐘，降低結算風險，也有效降低資金成本和系統性風險。此外，區塊鏈技術提供了不可任意修改的數位化平台，這對發行者因繁重的審核流程所面臨的行政風險和負擔也將大幅降低，亦對交易雙方帶來一定的信任度。Linq 提供了便利性的管理介面，在 Linq 上發行人能管理自身所發行的股票，包含當前公司價值以及發行的價格，透過清楚的資訊能更容易了解當前變化與方向，提供企業決策上的參考。

（三）The DAO

以太坊的智能合約機制具有強大的程式化能力，提供了發展業務流程自動化的良好基礎，遂有了以智能合約開發基於區塊鏈的去中心化自治組織（Decentralized Autonomous Organization）的倡議。2016 年初，一群以太坊的開發人員，由這樣的想發出發，在網路上號召支持者，以 ICO 群眾募資的方式，成立了一家類似創投基金的虛擬公司，就稱為 The DAO。

這家虛擬公司的運作方式與一般公司階層式的管理不同，它的所有決策都是

透過公司代幣的持有者（類似股東）共同投票所決定，並利用智能合約自動進行投資相關業務的處裡，未來的獲利或是虧損的風險就會依照投資持有的比例而有所不同。此外，代幣持有者也有權對投資項目進行提案，當提案表決得到一定比例的其他股東的支持後，項目便開始進行。

透過智能合約打造的以太坊平台以建立公司運作流程有幾項優點，首先是投資過程更具公開與透明。所有的交易相關資訊都能在平台上得知，因此對投資人更具有保障。其次是由於平台上的作業完全透過程式設計執行，少了許多人工處理的作業，相對來說營運成本也能大幅的下降，人為因素所造成的交易風險也降低。因此吸引了許多人加入投資，The DAO 在 2016 年的五月籌得高達 1.5 億美元的金額，刷新當時群眾募資的最高紀錄。

但同年六月卻發生駭客盜領的事件，此事件不但造成以太幣的下跌，也使虛擬貨幣的安全性遭到質疑。駭客利用智能合約程式設計上的漏洞，從平台上盜領了價值約五千萬美元的以太幣。雖然先前已有專家指出 The DAO 有程式設計上的漏洞，不過還是發生了盜領的事件。所幸後續由於其智能合約有類似閉鎖期的設計，駭客需等待一段時間才能將代幣自由搬移，讓 The DAO 的開發人員得以透過修補救回了遭盜領的代幣。2017 年 7 月美國證期局（SEC）對此事件發表了一篇調查報告，報告中認為 The DAO 的募資方式已符合了證券發行的行為，應該要依法辦理登記管理，以防範投資人權益受損。但對於新興技術的發展而言，公部門如何在監管及創新間取得平衡，是值得深入探討的議題。

（四）日本交易所集團

日本交易所集團（JPX，Japan Exchange Group）分別於 2016 年 8 月與 2017 年 9 月發表了 DLT 的概念驗證（PoC）報告，分享了他們以店頭市場（OTC）證券交易作業為標的，測試運用 DLT 是否可以實現並簡化現行作業流程的實驗結果，以及相關的評估項目。

選擇店頭交易，顯然是考量一般公開市場的交易量大，速度要求又高，不適合以 DLT 來處理。事實上，即便是店頭市場，交易媒合的部分也通常不是 DLT 的強項，所以 JPX 的實驗重點也是除了交易媒合以外的各種作業，尤其是結算與交割作業。不過證券發行、所有權登記與移轉，以及配息與股票分割等股務作

業（Corporate actions）也包含在 JPX 的實驗項目內。

此外，JPX 認為 DLT 的實務應用尚屬初期階段，是否能完全去除中介機構持保留態度，所以他們的 DLT 系統架構在設計上，是盡量在不改變現有單位機構與交易流程的前提下導入 DLT，以減低轉變所帶來的風險。圖 6-4-1 展示了 JPX 的實驗性質的 DLT 系統架構，包含個參與者，實驗的作業項目，以及 DLT 的建置組態安排方式（Arrangement）。

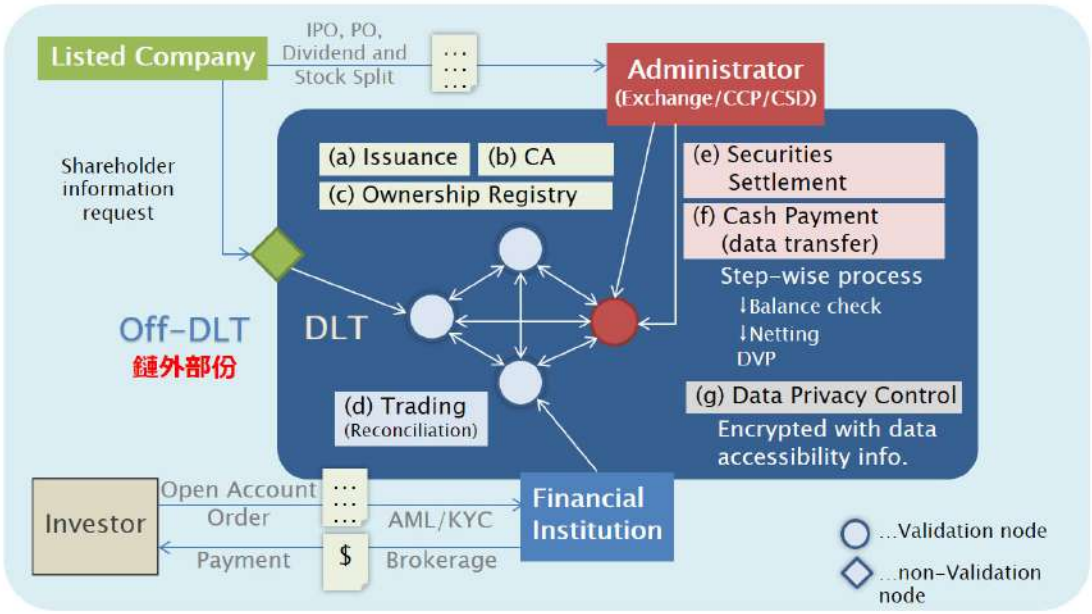

圖 6-4-1：JPX 的 DLT 概念驗證系統架構

參與的角色包含投資人、上市公司、金融機構，以及各個金融市場設施機構（FMI）：證交所（Exchange）、中央交易對手(CCP)與證券集中保管者（CSD）。在 DLT 的組態上，金融機構與 FMI 為驗證節點（Validator）與平台管理者（Admin），投資人與上市公司為非驗證節點。在證券交易部分，主要作業項目，除了交易媒合都包含在內，但部分作業，像是開戶（含 KYC，AML）等是在 DLT 外（off-DLT）進行的。交易資料隱私保護部分，起初是以加密方式搭配權限管理處理，後期改用 DLT 的機制實現[48]。

以下我們透過範例來解說 JPX 實驗中，其系統如何透過 DLT 的資訊分享功

[48] 初期使用 Hyperledger Fabric 0.6，資料必須加密以保護隱私。後期改用 Hyperledger Fabric V1.0 的通道機制，就不必對資料加密。

能來實現主要的結算與交割作業。範例中有三家公司（A, B, C）的股票在場內或場外進行交易，當證券公司將買賣訊息送出後，系統會根據撮合結果得知買賣的證券公司之交易對手方，或是買賣雙方場外協議價格與數量後將交易資料送出。此時會將撮合後的資料結果存入 DLT 中，等待交易對手方的確認。當交易對手方也確認交易條件後，便將交易結果更新至 DLT 中，之後等待證交所執行結算作業。以下兩張列表分別從 A 公司與 B 公司的角度列出相關交易，以利說明 DLT 的運作狀況。

表 6-4-1 為 A 公司當前的交易項目列表，表上顯示 A 公司對 B 公司有一筆 T1 以完成交割，T3 與 T4 兩筆交易訊息送出待交易對手方確認，T5 與 T6 兩筆待交割。

表 6-4-1 證券業交易項目列表（A 公司）

交易序號	股票編號	證券公司(借方)	證券公司(貸方)	成交價格	張數	金額	交易日期	交易狀態
T1	2219	B 公司	A 公司	35	2	70	10/1	交割完成
T3	1110	B 公司	A 公司	10	3	30	10/2	訊息送出
T4	1110	B 公司	A 公司	20	1	20	10/2	訊息送出
T5	3310	A 公司	C 公司	80	1	80	10/2	待交割
T6	1110	A 公司	B 公司	5	2	10	10/2	待交割

表 6-4-2 為 B 公司的交易項目列表，表上根據 DLT 資料顯示與 A 公司的兩筆待確認交易。當 B 公司確認了此兩筆交易後，DLT 上的交易狀態便會立即更新為待交割程序，並等待證交所做後續的確認執行。

表 6-4-2 證券業交易項目列表（B 公司）

交易序號	股票編號	證券公司(借方)	證券公司(貸方)	成交價格	張數	金額	交易日期	交易狀態
T1	2219	B 公司	A 公司	35	2	70	10/1	交割完成
T3	1110	B 公司	A 公司	10	3	30	10/2	待確認
T4	1110	B 公司	A 公司	20	1	20	10/2	待確認
T6	1110	A 公司	B 公司	5	2	10	10/2	待交割

- 結算與交割

證交所依據 DLT 上的權限能檢視當前所有的交易資訊與狀態。當證交所收到買賣雙方即將進入結算的訊息後，會根據款券等相關資訊確認交易條件。確認後會送出交割的指示進行款券的轉移 (DvP)，並將結果存入 DLT 中。

表 6-4-3 為證交所交易表，顯示交易的證券代碼、交易雙方以及買賣交易等相關資訊。根據買賣雙方撮合的結果，此表顯示有四筆交易待交割的交易，分別為 T3、T4、T5 與 T6，而 T1 與 T2 兩筆已完成交割。

表 6-4-3 證交所交易表

交易序號	項目紀錄	股票編號	證券公司(借方)	證券公司(貸方)	成交價格	張數	金額	交易日期	交易狀態
T1	券項	2219	B 公司	證交所	35	2		10/1	交割完成
T1	款項	2219	證交所	A 公司			70	10/1	交割完成
T2	券項	4423	D 公司	證交所	25	2		10/1	交割完成
T2	款項	4423	證交所	C 公司			50	10/1	交割完成
T3	券項	1110	B 公司	A 公司	10	3		10/2	待交割
T3	款項	1110	A 公司	B 公司			30	10/2	待交割
T4	券項	1110	B 公司	A 公司	20	1		10/2	待交割
T4	款項	1110	A 公司	B 公司			20	10/2	待交割
T5	券項	3310	A 公司	C 公司	80	1		10/2	待交割
T5	款項	3310	C 公司	A 公司			80	10/2	待交割
T6	券項	1110	A 公司	B 公司	5	2		10/2	待交割
T6	款項	1110	B 公司	A 公司			10	10/2	待交割

JPX 的 DLT 系統可支援逐筆結算並立即交割，也可採用淨額結算後交割。以表 6-4-4 為例，在每日進行節算時，可先根據雙方的款券金額及數量做沖銷互抵。如 10 月 2 號 A 公司與 B 公司依據結算結果，A 公司因 T3 與 T4 兩筆款項交易總和再扣除 T6 的款項交易金額，所以 A 公司總計需支付 B 公司 40 元 ，而 B 公司也依據券項結算結果，總共需交付 2 張 1110 的股票給 A 公司，表 6-4-4 為證交所在確認雙方交易條件滿足後，所完成的交割指令，並於交易狀態顯

示為交割完成，資料已寫入 DLT 中。

表 6-4-4 雙方交易條件滿足後的交割指令及狀態

交易序號	項目紀錄	股票編號	證券公司(借方)	證券公司(貸方)	成交價格	張數	金額	交易日期	交易狀態
T1	券項	2219	B 公司	證交所	35	2		10/1	交割完成
T1	款項	2219	證交所	A 公司			70	10/1	交割完成
T2	券項	4423	D 公司	證交所	25	2		10/1	交割完成
T2	款項	4423	證交所	C 公司			50	10/1	交割完成
T3	券項	1110	B 公司	證交所	10	3		10/2	交割完成
T3	款項	1110	證交所	A 公司			30	10/2	交割完成
T4	券項	1110	B 公司	證交所	20	1		10/2	交割完成
T4	款項	1110	證交所	A 公司			20	10/2	交割完成
T5	券項	3310	A 公司	證交所	80	1		10/2	交割完成
T5	款項	3310	證交所	C 公司			80	10/2	交割完成
T6	券項	1110	A 公司	證交所	5	2		10/2	交割完成
T6	款項	1110	證交所	B 公司			10	10/2	交割完成

第七章、區塊鏈在保險業之運用

第一節 保險業之現況分析

（一）保險業介紹

保險起源於農漁業的時代，為一群人互相幫助的概念，讓有著相同風險的人，共同集資分散風險；而隨著商業、甚至是全球貿易時代的來臨，保險需求越來越多元，藉由共同集資來分散風險的方式已經無法負荷多種的需求。

第一種集中承保的保險商品出現在十五世紀初期歐洲，稱為水險(Marine insurance)，當時負責承保的保險商會聚集在倫敦的勞依茲(Lloyd's)咖啡店，需要保險的船主或是貿易商會到此聚集地尋求保險商進行投保，其中承保(Underwriting)一詞就是由此發展出來的，久而久之，保險需求漸漸由專業化的保險公司來承辦， 保險公司也隨著全球化的交易，公司規模越來越龐大，但也因為發展過於龐大，故運作方面較制式化。

保險業隨著網路技術的發展，互聯網的出現，讓保險業出現新的運作模式，可稱之為網路互保，網路互保將人與人集資分散分險的概念搬到互聯網上，讓互聯網上的使用者組成互助會，此類的互保模式剛起步，其發展模式值得觀察。

以下會以傳統保險公司以及網路互保的運作流程圖來分析痛點，接著第二節中，會探討如何利用區塊鏈來解決這些問題。

（二）傳統保險

傳統保險的參與單位包含投保人、保險業務員、保險公司、理賠單位與第三方理賠證明單位，另外較大型的保險商品還會有再保險公司的加入，圖 7-1-1 為簡化的保險運作介紹：

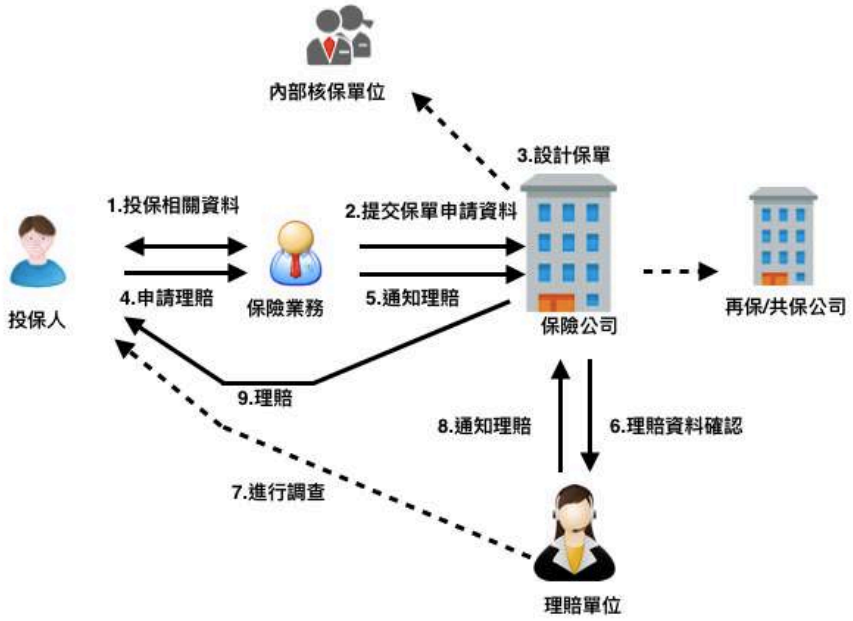

圖 7-1-1 保險業務運作流程[49]

來源：本研究整理

1.投保人與保險公司：

大部分的保險商品，首先都要由保險業務員提供保險資訊的介紹與解說才會進行承保，保險公司也要等保險業務員將客戶資料收集完後由內部的核保單位進行保險合約的制定。因為有保險業務員作為中介單位，保險公司難以確認是否取得客戶完整的資訊，讓保險公司與客戶間存在不對稱的資訊。

2.核保：

核保是保險流程中的核心，保險公司會由內部的核保單位進行保單的資訊的審核與評估，其中特別需要考量保險公司本身的營運能力、合約中約定的理賠金額是否合理或是投保人的風險是否是在可控制的範圍內，因為核保考量因素多，保險公司為了更精準的控制風險，大多選擇安全的大型保險或是一般民眾的產險、壽險，故對於小型的保險，保險公司會相對不願意進行核保。

3.理賠資料確認以及最終支付理賠

當客戶提交相關的理賠文件時，保險公司可能會需要向外部第三方申請相關的證明文件，如死亡證明、物品損壞證明或是農業風災損壞證明等，第三方證明的文件對於保險公司來說，透明度低也不易取得，取得資料後也需要一段時間來

[49]投保人部分，實際上會包含「要保人」與「投保人」，為方便討論，將其視為一體

做審核。在資料審核後，還要依照當初核保單位所制定的合約來評估理賠責任，且其中常會有法律糾紛與責任歸屬問題。

經由上述流程的描述，在於傳統保險業中，可大致整理成以下幾個痛點：

- 保險公司都是被動式的接收資料，特別是在投保人的核保資料，保險公司需要等待客戶提交相關的文件，而對於投保人，也需要等待保險公司的核保，雙方一來一往就會花費許多時間。
- 核保需要耗費許多時間，不同的保險商品有不同的評估方式，除此之外，也造成理賠付款的時間非常的久，可能讓投保人無法即時取得理賠金額，例如醫療與車禍相關的保險，理賠若有延誤，就會造成客戶體驗不好，導致滿意度低。
- 資訊不對稱問題，除了保險公司與保戶間的資訊不對稱，還有大型保單所需要的再保險公司，再保險公司需要處理跨國資料的傳遞或是讓保險商品符合不同國家的法規等繁雜的問題，過程除了耗時外，對於承接再保險商品的保險公司也難以掌握保單完整的資訊，常會因為資訊不對等而衍生出許多爭議。

（三）網路互保平台

近年互聯網風氣盛行，讓人們可以藉由網路互相連結，而互聯網的風氣也帶起網路互保平台的熱潮，網路互保是一種 P2P 保險，利用平台連結眾人，共同分攤風險，如中國的抗癌公社，藉由大眾集資來分散發生癌症時所需的醫療費用；另外，此類保險的運作模式與保險的起源非常類似，只是過去因為沒有網際網路，所以人們無法有效率的進行保險，最終才會發展出中心化的保險公司來做承保，但近幾年的互聯網技術突飛猛進，讓眾人集資分散風險的保險模式又重新活路起來。圖 7-1-2 為網路互保平台的運作圖，一般而言，會由平台直接讓參與者直接互保，另外也有的互保平台會委託外部的保險公司做風險定價，增加平台的專業性，圖 7-1-2 紅框虛線就是由保險公司進行風險定價的部分。

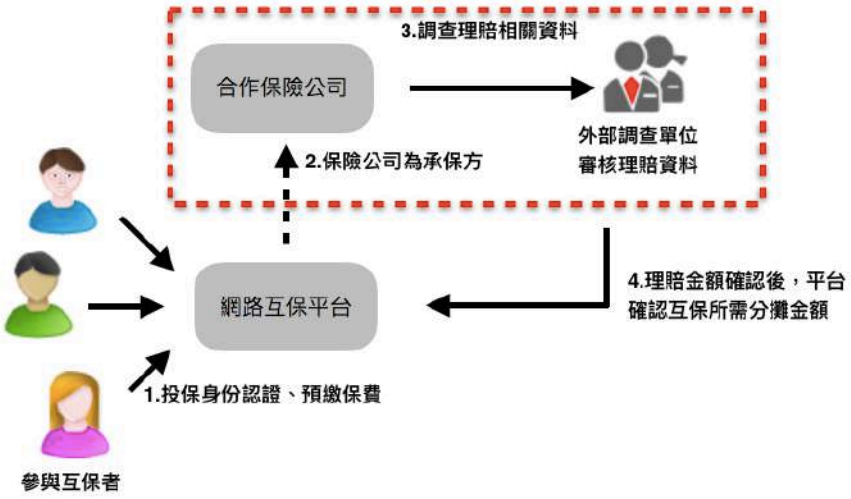

圖 7-1-2 一般的網路互保流程圖

來源：本研究

1.加入平台的方式：

保戶加入互保平台的方式可經由上傳身分證或是手機號碼等簡單的認證，即可加入成為平台會員，同時網路互保平台可能會先預收一筆小額的保費。

2.核保及理賠：

在於此部分，若平台是有與外部保險單位合作，通常就會由保險單位來處理；但若是平台自己做承保的話，就由互保平台的參與者互相做核保，理賠部分也是由理賠申請者自行上傳相關資料，例如中國的防癌公社是由投保人自行上傳相關病例，防癌公社的互保參與者共同監督確認是否達理賠標準。

與傳統保險業相比，網路互保效率較高，但網路互保平台也有以下幾個問題需要注意：

- 平台上的參與者難以互相信任，文件真實性難以驗證，例如中國防癌公社中，投保人所提供的核保資料是否有可信度、最後理賠時是否有足夠的資金或是文件證明如何審核，都是難以建立信任基礎的問題。
- 平台運作的監管，例如文件的標準化，從投保人的資料與風險定價所需的相關證明文件，就算訂出標準，也很難進行一對一的監管，或是進行資料真實性的驗證，另外還有互保平台本身提供的互助會規章、保費分攤方式方式，也很難讓監管單位作監管。

第二節 應用區塊鏈技術於保險業

（一）區塊鏈應用

在於保險業的應用，首先，保險公司之間可利用區塊鏈的分散式帳本進行連結，加強本身的保險業務承辦效率，例如法國保險集團安甚(AXA)所提出的航班延誤險，就是利用區塊鏈網路連結外部資料庫的加速承保及理賠的案例，除此之外，也可進行跨組織的連結，例如保險業與銀行業的保代業務；另外，利用區塊鏈在於保險業的新型態的應用，大多聚焦於 P2P 互保平台，加強互保平台的信任基礎。以下將分成兩個部分介紹區塊鏈在保險的應用，第一部分是利用區塊鏈進行保險公司與跨組織的連結，再搭配智能合約進行自動理賠，第二部分是未來可能創新應用的運作模式。

第一部分，藉由區塊鏈網路連結保險公司以及跨組織，可利用區塊鏈的共享帳本提高保險公司對於客戶資訊的掌握程度，例如核保歷史紀錄與理賠紀錄，以下將介紹如何建立此區塊鏈網路、如何利用智能合約做自動理賠跨組織的應用模式。

1.區塊鏈網路的建立 — 首先要建立基本的區塊鏈運作方式及帳本共享權限管理，權限分類如表 7-2-1，主要可分為管理區塊鏈分散式帳本、可進行交易與可查看帳本資料的權限。可由大型的第三方機構進行建立區塊鏈的主導方，例如保險公會，同時也要讓監管單位加入，確保區塊鏈網路的安全。

表 7-2-1 區塊鏈在保險業之節點權限

類型	單位	敘述
核心節點	保險公會	可決定與審核進入私有鏈網路的單位以及處理私有鏈核心系統的更新
交易節點	一般保險公司	可進行交易與交易驗證的節點，也可以進行智能合約的設計
一般節點	監管單位	可查看保險鏈帳本的節點，會依不同角色開放不同的資料讀取權限。

2.利用智能合約讓保險中的承保與理賠自動化—此部分在於區塊鏈中，因為要自動理賠，可以考慮先由較簡單的保險商品，例如壽險、航班險這類免核保或是參數式的商品切入，省去上傳核保資料的步驟，只要提交申請單就可投保；另外在於理賠部分，則可以利用智能合約自動設定理賠條件，除此之外，利用智能合約將保單部署到區塊鏈上，也可以讓資料的紀錄、追蹤與分享更快更安全，圖 7-2-2 為區塊鏈在於保險業的應用概念圖，以下將介紹保戶投保及理賠的方式：

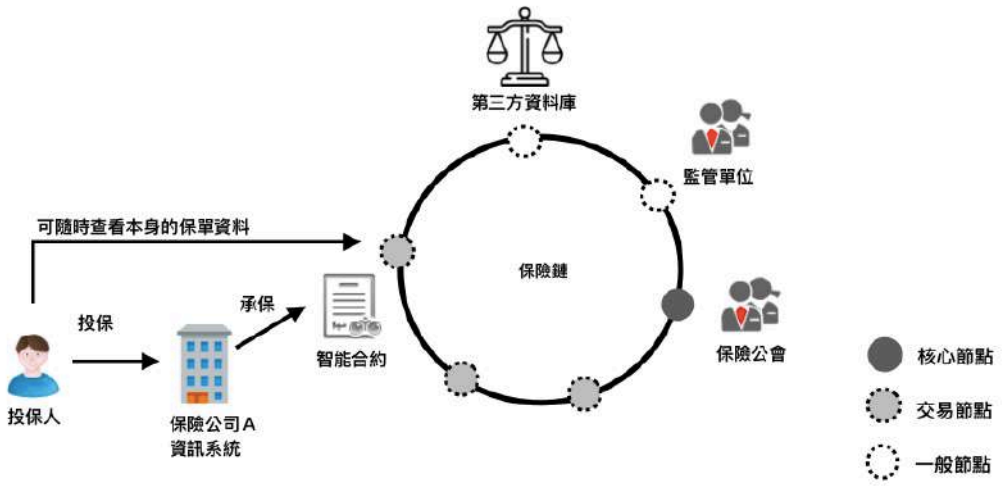

圖 7-2-1 區塊鏈技術下的保險區塊鏈網路

- 保戶投保：

保戶投保時，保險公司利用區塊鏈上的共享資料做承保審核，資料來源可能是過去客戶所做的保單資料，或是醫院的電子體檢資料(第三方資料庫)做身分驗證。當保險公司確認保戶的投保資料後，就會將保險智能合約加至區塊鏈的待驗證區，由其他的一般節點以及核心節點進行智能保單的確認，若無誤，則由上傳保單的保險公司將智能合約加至帳本上。

- 理賠：

理賠部分，會由智能合約連結第三方資料庫進行比對，如連結醫院的被保人生命狀態、車子的里程數與氣象局的氣候監控數據，由智能合約自動判斷是否達到理賠標準。若智能合約收到符合理賠的標準，會自動給予投保人理賠，且將此筆交易在區塊鏈上做更新。

經由加入智能合約，保險公司能有系統性的掌握客戶的資訊，例如保險歷史紀錄、年齡或是職業等，這些記錄在區塊鏈上的資料同時也能藉由設定不同的權限，供監管單位或是其他保險公司查看與監管，例如當客戶承保其他不同的保險

時，保險公司就可以不用再重複確認客戶的個人資料，且同時能確保客戶沒有重複保險或是防止理賠詐欺的發生。

此外，也可利用智能合約來保護較敏感的資訊，例如醫療險，病人資料不用再經由保險公司主動調查，理賠的驗證會透過醫院直接連結保險區塊鏈的帳本做更新，進而保護病人相關的隱私，同時省下理賠調查成本。

未來，一般承保、核保流程都自動化後，保險公司可以專注於開發保單，理賠調查部門可以專注於數據的整合與分析，讓理賠的流程更有效率，也讓投保人與保險公司雙方的資訊更透明。

（二）跨組織連結

區塊鏈除了連結保險公司以及第三方資料庫之外，還可以進行跨組織合作，例如保險業與銀行業的保代業務（Bancassurance，即銀行作為保險商品銷售的仲介機構），此類保險商品的運作模式會讓保戶與保險公司中間隔著銀行，導致保險公司對於客戶的資訊掌握度低，且客戶的資料在於銀行與保險公司間的傳遞效率也不佳，例如保單的核保，客戶資訊是儲存在銀行端，但保險公司需要客戶資料做核保時，資訊需要經過層層的轉交才能完成；再者，資料傳遞的過程中又要考慮客戶個資的隱私，導致核保流程耗時，除此之外，在最後的銀行抽佣以及保險公司收取保費的效率也不佳。

但若是利用區塊鏈，就可以利用分散式帳本解決上述的客戶資料傳遞效率不佳的問題，運作的概念如圖 7-2-3，綠色小方格部分就是利用區塊鏈做資料的共享，讓承保的過程可以讓保險公司同步接收到銀行的客戶資訊，加速相關銀行與保險公司在於顧客保險資料的交換，另外在於保費以及銀行抽佣的部分，也可利用智能合約進行給付。

而目前中國建設銀行與 IBM 合作的區塊鏈銀行保險平臺就是其中一個實際的案例，此服務預計於 2017 年上線[50]。

[50] 因中國建設銀行預計於 2017 年第三季上線，細節資料尚未公佈，在之後的個案章節就不多介紹

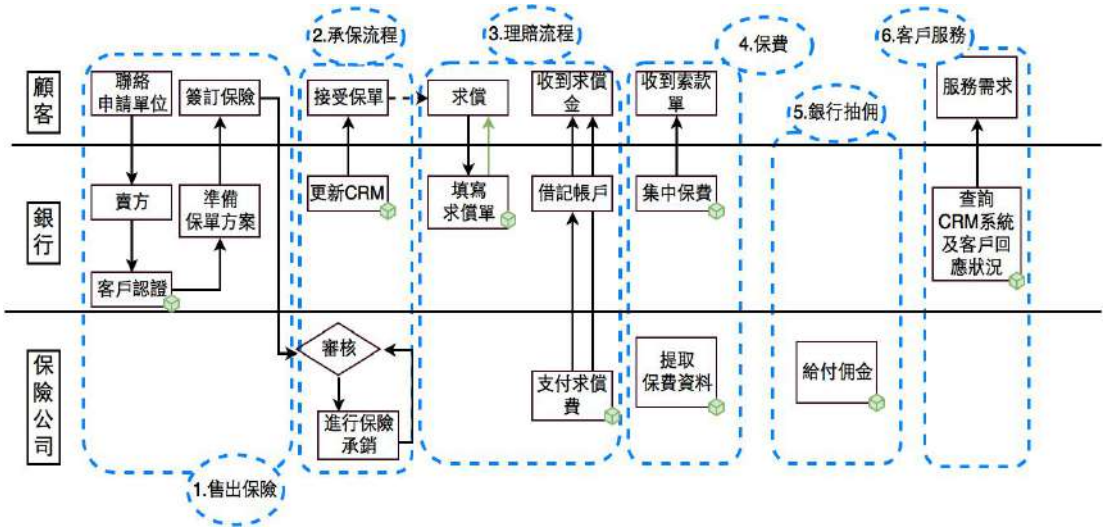

圖 7-2-2 銀行保險架構圖

來源: Deloitte China

（三）創新應用

創新應用，將以 P2P 互保為主軸來做介紹，目標在於解決 P2P 互保平台上雙方難以互信的問題，未來應用的模型可以分為兩種形式做探討，第一種，保險公司為平台上的保險商品做承保的模式，如圖 7-2-3 的 Model 1，保險公司可以藉由區塊鏈的分散式帳本，紀錄平台用戶的資料，專注於設計保單與審核保單，甚至是經由客戶開放的權限提供來做客製化的承保；第二種，直接由平台上的用戶自行互保，如圖 7-2-3 的 Model 2，平台的用戶資料都已經在特定的保險區塊鏈平臺上有可追溯的紀錄或是過去已認證的保單資料，且 IoT 已經可以連結到任何物品，例如手機與單眼相機，甚至是用戶的開車習慣或是身體狀況，平台能先利用區塊鏈來記錄資料，做投保戶的身分認證，讓平台的用戶能互信，除此之外，平台也能利用區塊鏈所記錄的資訊來進行風險評估或是顧問服務，而此應用所需要搭配的技術包含 IoT、Big data 與區塊鏈智能合約身分認證等，都是未來重點發展的科技。在下一章節會以個案的介紹來描述此階段的應用方式。

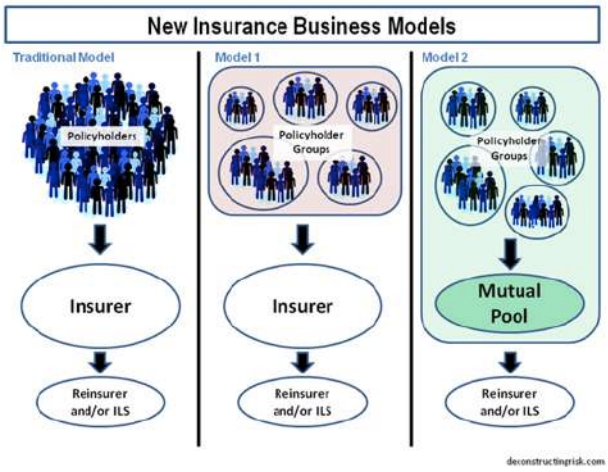

圖 7-2-3 網路保險應用模型

資料來源：deconstuctingrisk.com

第三節 個案探討

區塊鏈在於保險業的個案可以大致分為兩類，第一類是改善承保已及理賠流程，此類將介紹提供航運險與飛機延誤險的法國安盛(AXA)，另外還有針對小型高單價的保險而設立的區塊鏈平台，例如鑽石認證平台 Everledger；第二類是在網路互保的應用，將介紹失業保費理賠的 Dynamis 以及 P2P 保險平臺 MediShares、LenderBot 與 Lemonade。

（一）法國跨國保險集團，安盛(AXA)提出的航班延誤險—Fizzy

在於航班延誤險，過去保險公司要花費大量的人力以及時間來追蹤航班資訊、旅客資訊，且當旅客要申請理賠時，旅客還要自行跟航空公司申請航班延誤證明，非常麻煩，也造成客戶體驗不佳。

而法國的安盛保險集團利用 Ethereum 的智能合約與全球航空資訊庫連結，提供旅客全自動的航班險理賠 Fizzy。目前 Fizzy 應用在巴黎戴高樂與美國之間的航班，理賠條件設定在航班延誤超過 2 個小時，會由智能合約自動判斷是否理賠。此方式與過去理賠最大的不同是，Fizzy 會直接由類似第三方的智能合約做理賠的判斷，讓旅客可以更相信航班延誤險，其中理賠的貨幣目前還是以法定貨幣為準，但未來安盛集團表示，可能會直接利用電子貨幣做支付理賠。

（二）航運保險—安永(EY)、微軟與馬士基集團所推出的航運保險區塊鏈平台

航運保險是貿易融資的一部分，目前的貿易融資，如第五章所述，資訊越來越複雜，且大多文件還是藉由紙本來傳遞，除了紙本的傳遞效率不佳外，也難以確保文件傳遞的安全性，而安永集團全球保險事業負責人 Shaun 表示：

「區塊鏈平台能讓航運保險克服過去因為跨國或是參與單位複雜與紙本所帶來的問題，可藉由區塊鏈平台連結不同的資料庫以及協調各單位的運作，增加整體航運保險流程的效率」

此航運保險平台是安永與區塊鏈新創企業 Guardtime 合作，在微軟的 Azure 平臺上運行，預計於 2018 年開始正式運行，此平台將會利用區塊鏈連結保險客戶、保險經紀人、保險公司與航運公司，分散式帳本將會針對客戶資訊與可以降低風險的資訊做紀錄，且將這些資訊整合進保險的承保過程，以降低詐欺的發生。

此航運保險的區塊鏈平台功能包括[51]：

- 創建並維護多方的資產數據
- 將數據與保險合約連結
- 利用收集的資訊協助保費定價或是加速業務流程
- 連結客戶的資產與交易和支付訊息

（三）鑽石證明平台—Everledger

鑽石的認證大多都是紙本證書，紙本在於保存文件與跨國傳送與驗證較無效率，同時也易於仿造或是損毀；但若是有數位化的紀錄，且確保其不可篡改，就可以讓鑽石的交易市場更健康，降低血鑽石與非法販賣的情況產生。

Everledger 於 2015 年 4 月由 Leanne Kemp 創立，創辦人 Leanne Kemp 利用雷射掃描技術將鑽石資料數位化，為鑽石打造獨一無二的鑽石指紋，其中鑽石指紋又可分為 4Cs，包含 Carat weight、Color grade、Clarity grade、Cut grade，此紀錄會部署到區塊鏈上，買方在買鑽石的同時，就可以在 Everledger 上建立鑽石紀錄，同時此筆紀錄可以用來向保險公司進行投保，而保險公司也會直接利用

[51] 安永 EY, http://www.cicpa.org.cn/Column/hyxxhckzl/xxjhykjhy/201709/W020170914521343287000.pdf

Everledger 的紀錄做鑽石的承保，運作流程如圖 7-3-1，圖中的 Lucy 在買到鑽石的同時，就先向 Everledger 平台做鑽石的紀錄，再利用此紀錄向保險公司做投保：

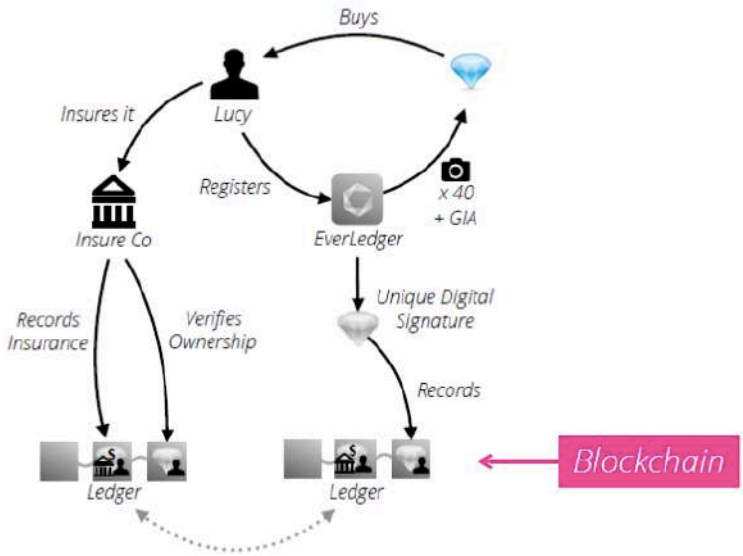

圖 7-3-1 Everledger 鑽石紀錄流程

來源：ThoughWorks Inc.

另外，假設今天有人的珠寶或鑽石遭到偷竊，如圖 7-3-2，小偷 Thomas 準備將偷盜的珠寶販售給 Jane，此時 Jane 可以先向 Everledger 平台確認此珠寶的所有權是否真的屬於 Thomas，同時平台就會發現此鑽石已經遺失的紀錄，同時將保險公司也會收到此筆紀錄，讓 Thomas 將無法順利在市場上兜售鑽石。

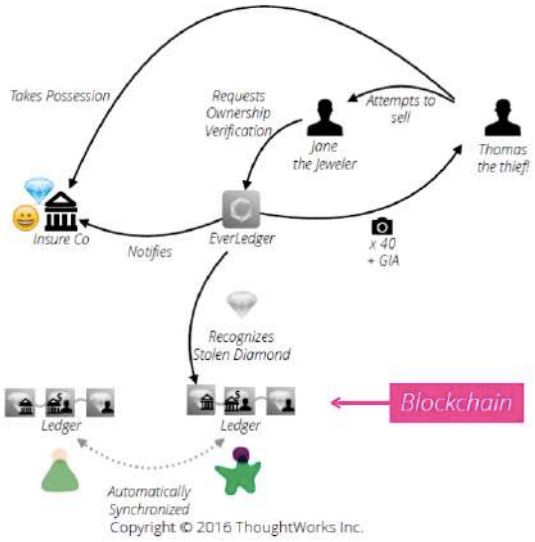

圖 7-3-2 Everledger 防止詐欺流程

來源：ThoughWorks Inc.

（四） Dynamis

Dynamis 是提供失業員工補助金的保險服務，以一般保險業的角度來分析其創新的應用，運作架構如圖 7-3-3，在於承保，Dynamis 利用 LinkedIn 來確認員工就業狀況及就業歷史紀錄，此做法可以大幅降低傳統保險業的承保時間；接著在於理陪部分，藉由智能合約連結 LinkedIn 來收集理賠資料，而理賠的資料會藉由隨機挑選 LinkedIn 上的用戶做審核，且由智能合約對失業員工做自動理賠。

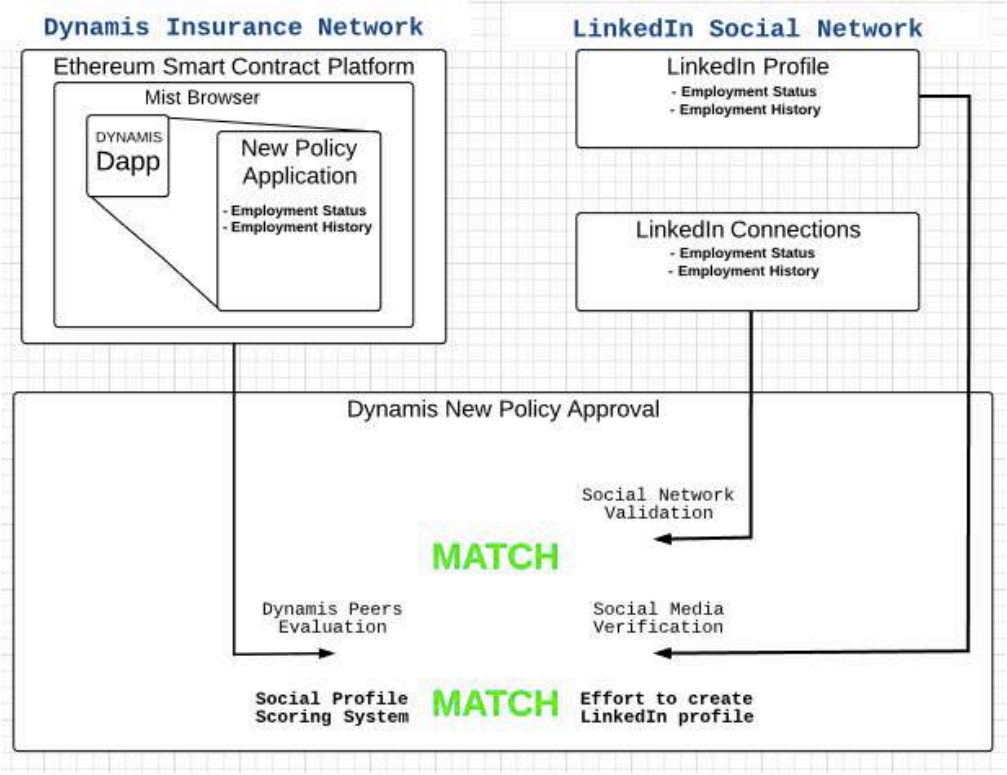

圖 7-3-3 Dynamis 架構圖

來源: Dynamis, http://blog.dynamisapp.com/p2p-insurance-solutions/

除了上述的承保、理賠相對應部分外，Dynamis 還能利用智能合約將員工保險理賠的歷史資料部署到區塊鏈上，確保員工的失業理賠有持續且完整的紀錄，且當員工找到新工作時，也能防止員工重複申請理賠；除此之外，也能利用智能合約中也能設定失業理賠金額與期間，防止平台上的理賠金被無限制的領取，如目前 Dynamis 設定就是最多只能領五個月的失業保險。

Dynamis 的例子中最關鍵的創新就是利用第三方擔保 LinkedIn 來大幅提升區塊鏈的可行性，而其一般的網路互保平台，如中國防癌公社，若是想藉由區塊鏈來增加平台的安全性，除了一般的資料紀錄及追蹤外，還是要想辦法與第三方

的理賠資料單位合作，才能真正確保互保的信任基礎。

（六）MediShares

網路互保其中一個重要的功能就是可以利用網路快速集結承擔相同風險的陌生人， 2017 年 9 月成立的 MediShares 就利用區塊鏈讓分散各地的民眾可以找到承擔相風險的夥伴，例如天災分散各地，沒有特定或是合理保費的保險商品，但經由 MediShare 的區塊鏈保險平台，讓全球各地的人都可以藉由此平台共同對天災互保，再利用全球天氣觀測資訊讓智能合約保單作出相關的保險承保及理賠活動。

MediShares 也提供保戶自行設計保險商品的服務，任何人或是任何單位都可以在此平台上建立智能合約保單，再將保單部署到區塊鏈上。如中國的眾托幫宣稱未來準備利用 MediShare 來創立重症疾病的保險商品，供本身的用戶使用。

（七） LenderBot

LenderBot 是由巴黎新創企業 Stratumn 以及 Deloitte 與支付商 Lemonway，針對小型高單價的商品租賃市場所發佈的區塊鏈微型保險計劃，例如當某人要出租單眼相機、名錶或 3C 商品這類高單價的商品，保險公司可能會因為商品過於小型或是分散，難以進行風險評估及核保而拒絕此筆保險，而 LenderBot 讓租賃雙方自行上傳保險合約的相關資料來解決此問題，簡化過去原本要由保險業務員親自調查或是客戶自行上傳文件證明的承保流程，如圖 7-3-4，由買賣雙方協調好後，直接與保險區塊鏈平台洽談保險，而保單的資料都會經由智能合約部署到區塊鏈上來確保其不可篡改；另外在於保戶的個人隱私，則藉由新創企業 Stratumn 所設計的演算法，將交易雙方的交易過程做加密，讓投保方與租借方可以依照不同的權限得知保單的即時資訊。

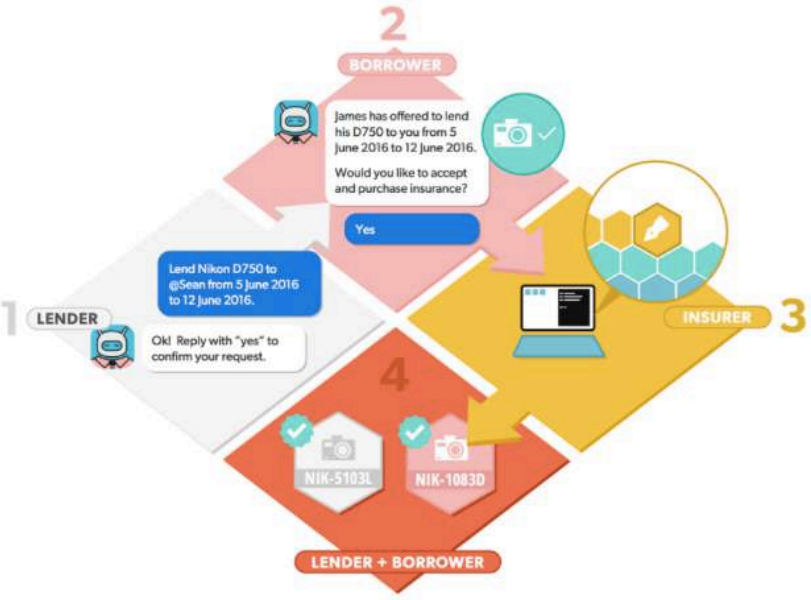

圖 7-3-4 LenderBot 運作架構圖

來源：Stratumn

（八） Lemonade

Lemonade 是全世界第一家註冊為 P2P 互保的保險公司，與其他新創的 P2P 區塊鏈互保平台有些許不同，Lemonade 除了利用區塊鏈來作為保險平台的底層技術外，同時也藉由社會科學及心理學的幫助，首先在社會科學的部分，保戶在投保時 Lemonade 會讓保戶選擇一家慈善機構，當保戶申請理賠後，若是保費有剩餘，就會以投保者的名義對當初指定的慈善機構作捐款，此部分就是利用社會科學，讓投保者除了保險外，還有參與“做善事”的感覺，此外，在心理學的部分，由於 Lemonade 在進入保險市場時，發現保費虛報的比例非常高，經過調查後發現，投保人認為保險公司應該無償理賠損失，而 Lemonade 藉由讓投保人簽訂誠實協議書，且利用投保人與聊天機器人的互動來進行申請理賠，經過觀察，此方式可以有效降低理賠虛報的狀況。

第八章 結論與展望

一、區塊鏈的發展深具潛力，應及早探索與掌握

源自比特幣的區塊鏈技術在過去兩年中有了快速發展與實質的成果:從單純地提供可信賴的紀錄，已演進成新一代的應用系統平台；透過智能合約的程式化機制，讓區塊鏈的應用充滿了非常多的想像空間。不僅在公有鏈上，企業內部與企業之間的區塊鏈應用也陸續浮現。尤其是在金融業，不僅有潛力重新 整體金融市場的基礎設施，也為新一代的金融業務模式提供了非常多的發展方向。

本報告從三種應用模式（企業內、企業間與新業務模式）出發，分別探討了區塊鏈對支付、銀行融資、保險與證券業可能的衝擊與應用方式，也說明了這四個主題的許多應用與概念驗證的案例。這些案例帶給我們以下的啟發：

1.世界先進國家的金融機構都已紛紛投入區塊鏈應用的探索，以及透過概念驗證系統 (PoC) 的規劃與開發，逐步去掌握這項新興科技的特性、強處與弱點，以評估對未來業務發展的衝擊。

2.發想區塊鏈的應用主題，可以從區塊鏈所提供的可信賴的紀錄開始，以對這些紀錄有利害關係的各方的角度去思考，進行概念驗證的規劃與系統開發。

3.對區塊鏈應用的概念驗證可以從很簡單，但有明確目標的主題開始，重點在於啟動對這項新興科技的理解與掌握，而不是上線營運。新加坡海關透過在銀行間透過共享貿易融資中的貸款資料，進而排除廠商重覆融資的概念驗證系統，就是一個好的例證。

4.可結合外部資源，共同進行區塊鏈應用的概念驗證。畢竟這是一項新興的科技，組織內部人員對它的掌握可能不夠，尋找適當的外部技術夥伴，一同進行概念驗證系統的開發是比較務實的作法。國外的案例中，幾乎所有的驗證系統都是以此方式進行的。

5.概念驗證也可以規劃龐大複雜的主題，但宜採分階段方式進行。加拿大央行與新加坡央行對於跨行支付的概念驗證，不管範圍或是技術運用都是相當複雜的，所以他們二者皆採取分階段方式進行，新加坡更是透過制定完整的藍圖，分幾年來完成驗證。

6.要建立多元化的概念驗證系統評估面向。功能性的評估是一定要的，但是其他面向的評估也應該要及早建立。像是軟硬體的成本，對既有業務流程與人員組織的影響等，都應該納入評估項目中。日本幾家銀行聯合進行的跨行支付驗證系統，以及 JPX 的驗證系統，都在事後進行了非常多面向的評估。

7.區塊鏈雖然是一項具顛覆性的底層平台技術，但也必須跟其他技術與非技術面向搭配，才能適切發揮其特色。不能簡單地將其視為萬靈丹，而不切實際的以為只要導入區塊鏈，就可以將所有的問題一次解決。業務流程與人員組織的配合與調整，也必須納入考量，方能獲得創新變革的成功與最佳效益。例如：日本 JPX 的實驗中，就秉持著中間人的角色可以因區塊鏈而重新檢視與調整，但未必能直接取代的方向，進行概念驗證系統的設計。

8.區塊鏈技術所可能促成的新型態金融模式不容小覷，網路效應的爆發點雖然還不明顯，但今年以來的虛擬貨幣（比特幣與以太幣等）的極速漲幅，以及 ICO 的投資熱潮，都在顯示區塊鏈技術的潛力雄厚，有可能在不久的未來，為金融業帶來很大的衝擊，應及早因應。

二、區塊鏈未來朝落地發展的挑戰

區塊鏈的技術仍然持續發展中，不管是交易效能，資訊安全或是隱私保護，以及資料分割作業等方面，都還有許多議題與困難需要處理與克服，才能大規模的落地應用。但也不只有技術面向而已，姑且不論法規面的考量，一項平台型的底層技術要導入任何有規模的組織，乃至於社會大眾的日常金融活動之中，對現行業務流程與人員組織所帶來的影響與衝擊，一定是非常大的。不僅需要審慎的評估，更需要縝密的規劃，以降低導入的風險與失敗的機率。

具體而言，導入區塊鏈並不只是技術難度的問題，還要考量業務流程改變的困難度。SWIFT 機構於 2016 年發布的研究報告中[52]，針對十項與證券業務有關的區塊鏈應用主題進行評估，就這些應用主題導入區塊鏈的技術難度與流程變更難度，繪製了以下的圖表加以說明（圖 8-2-1）。該報告中，透過對許多行業專家

[52] SWIFT 2016: The Impact and Potential of Blockchain on Securities Transaction Lifecycle. https://bravenewcoin.com/assets/Industry-Reports-2016/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle-Mainelli-and-Milne-FINAL.pdf

的訪談與分析，歸納出上圖中各個主題的困難度。同時也指出，很多時後人們多聚焦於技術難度而忽略了流程難度，這對一項新興科技的導入是高風險，是不利的，值得我們留意。

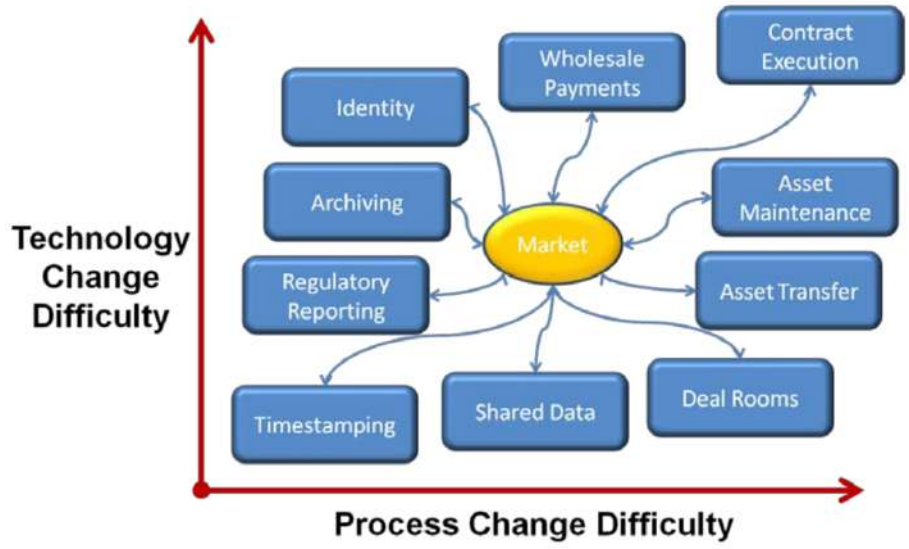

圖 8-2-1 十個區塊鏈應用的技術與流程變更難度圖

來源：SWIFT

此外，由於區塊鏈的特性，在做導入規劃時，我們更要注意相關資料的品質。區塊鏈內的資料不能竄改，從而可提供信賴紀錄給交易中的各方，作為業務流程進行與自動化的依據，但是如果資料品質不佳，進入區塊鏈之前就有問題，甚至遭到塗改，那區塊鏈也無法協助；智能合約更會因為資料品質不好而發生問題，或是得出不正確的結果。因此，在未導入區塊鏈而檢視業務流程的同時，更要關注各個流程點，會進入區塊鏈儲存的相關資料的品質。

最後，區塊鏈應用的大幅落地應用很可能必須仰賴網路效應，也就是說要有許多不同角色的參與者一起推動，藉以吸引更多的參與者，比較容易取得成功。WEF 在 2016 的分散式帳本報告中就曾提出這樣的主張。報告中認為，一個區塊鏈的應用要成功、產生影響力，需要支持者、創新者以及監管單位，在整個過程中之間緊密的合作，但這也會增加過程的複雜度與延遲的可能性。報告並具體說明，成功實現區塊鏈應用必須在三大關鍵項目取得實質的成就。

第一，更換現存基礎設施：區塊鏈是一種底層的基礎設施，如果用它來全面取代目前的許多金融市場基礎設施（FMI）的平台與系統，投資金額會很高，所需的時程也很長。過程中要如何讓區塊鏈新系統搭配原有的系統平行測試，也是

替換成功與否的關鍵。

第二，法規、監管與治理結構的調整：導入區塊鏈應用系統，智能合約所促成的自動化作業對既有的業務流程一定會有所牽動，並連帶有法規遵循與監管治理的改變，所以這方面的調整必須及早規劃與因應。不僅舊的法規也需要適度的修訂，讓新的技術有發展空間，也需要增訂新的監管法規，來處理區塊鏈應用所帶來的新議題。

第三，參與者間利益分配的調合：區塊鏈的應用需要多方參與，但當各方的業務因透過區塊鏈應用而比較緊密的連結在一起時，最容易遇到的問題就是互相注重的利益不同，而導致在應用區塊鏈的方式有衝突，無法順利推動上線。所以如何平衡參與者間的利益需求，避免零和遊戲的競爭也是非常重要的。

在規劃區塊鏈的大型應用的同時，若要周延的處理以上三個面向，勢必會增加系統規劃與建置的時間與成本。但如果一個區塊鏈應用能在以上三個關鍵面向都能面面顧到，就可能成功地建立延展性高、基礎穩固的平台，成為產業中的典範應用，甚至建立標準的作業流程。

參考文獻

DLT 平台

1.（Bitcoin） Bitcoin: A Peer-to-Peer Electronic Cash System, November 2008. https://bitcoin.org/bitcoin.pdf

2.（UTXO）*The Challenges of Optimizing Unspent Output Selection*, Februery 2015.

3.（Ethereum） *A Next-Generation Smart Contract and Decentralized Application Platform*, 2015. https://github.com/ethereum/wiki/wiki/White-Paper

4.（EEA） The Enterprise Ethereum Alliance 網站 https://entethalliance.org

5.（Quorum） J.P. Morgan Quorum 相關網站
https://github.com/jpmorganchase/quorum
https://github.com/jpmorganchase/constellationhttps://github.com/jpmorganchase/quorum/wiki/Quorum-Overview
https://github.com/jpmorganchase/quorum/wiki/Transaction-Processing

6.（Hyperledger ） Hyperledger Fabric V1.0 Deep Dive
https://goo.gl/V8jPfH

7.（Hyperledger）Hyperledger Fabric Design Document : Multichannel Consensus
https://goo.gl/Erykrc

8.（Corda） R3 Corda 相關文件網站
https://github.com/corda/corda

DLT 應用與評估

1.The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services, WORLD ECONOMIC FORUM(2016), Section 5.9 Market Provisioning: Equity Post Trade.
http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

2.Distributed ledger technologies in securities post-trading, European Central Bank, April 2016. https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

3.Applicability of Distributed Ledger Technology to Capital Market Infrastructure, Japan Exchange Group(JPX), August 30 2016.
http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_No15.pdf

4.Proving Ethereum for the Clearing Use Ca, Royal Bank of Scotland, September 2016.
https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjOv9X29JjXAhVSNrwKHe8HBLMQFgglMAA&url=https%3A%2F%2Femerald-platform.gitlab.io%2Fstatic%2FemeraldTechnicalPaper.pdf&usg=AOvVaw2RHX9V6gaVgo9SeQp3cDfx

5.Report on Practical Experiment of Blockchain Technology in Japanese Domestic

Interbank Payment Operation, Mizuho Financial Group, Inc. & Sumitomo Mitsui Banking Corporation & Mitsubishi UFJ Financial Group, Inc. & Deloitte Tohmatsu Group, November 30, 2016. https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/about-deloitte/news-releases/jp-nr-nr20161130-report-en.pdf

6.Distributed ledger technology in payment, clearing and settlement, Bank for International Settlements, February 2017. https://www.bis.org/cpmi/publ/d157.pdf

7.Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet? Bank of Canada, June 2017.https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf

8.Distributed ledger technical research in Central Bank of Brazil, Banco Central do Brazil, August 31, 2017. https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf

9.The Trend of Exploring the Use of Distributed Ledger Technology in the Capital Market, Japan Exchange Group, September 14, 2017. http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_Vol20.pdf

10.Payment systems: liquidity saving mechanisms in a distributed ledger environment, European Central Bank and the Bank of Japan, September 2017. https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf

11. The future is here- Project Ubin: SGD on Distributed Ledger, Deloitte Touche Tohmatsu , 2017. http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Press%20Releases/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf

12.Global blockchain benchmarking study, University of Cambridge, September 2017.https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf

13.FinTech Accelerator Proof of Concept, Bank of England, September 2017.

http://www.bankofengland.co.uk/Documents/fintech/fintechpocdlt.pdf

14.The economics of distributed ledger technology for securities settlement, Bank of England, Evangelos Benos, Rodney Garratt and Pedro Gurrola-Perez, Staff Working Paper No 670, August 2017. http://www.bankofengland.co.uk/research/Documents/workingpapers/2017/swp670.pdf

其他

1.中央銀行網站，中華民國支付及清算系統（民國 98 年）。

http://www.cbc.gov.tw/public/Attachment/972016463871.pdf

2.中央登錄公債系統相關文件，中央銀行國庫局提供。