出國報告(出國類別：其他)

亞洲開發銀行與韓國金融監督院「金融科技與網路安全」研討會出國報告

服務機關：中央銀行
姓名職稱：黃心漢(辦事員)
派赴國家/地區：韓國/首爾
出國期間：107 年 11 月 11 日至 107 年 11 月 16 日
報告日期：108 年 2 月 1 日

目錄

圖目錄

表目錄

壹、 前言

一、研討會目的

本次「金融科技與網路安全」區域研討會係由亞洲開發銀行(Asian Development Bank, ADB)與韓國金融監督院(Financial Supervisory Service, FSS)共同舉辦，研討會主要目的係回顧金融科技(FinTech)發展，使監理人員能瞭解金融科技的最新技術發展，以及這些新科技對監理帶來的挑戰，期能協助各國瞭解並改進監理實務及制度，以提升金融監理功能，並維持金融穩定。

二、研討會過程

本次研討會為期4天，參與學員分別來自11個經濟體，包含柬埔寨、中國大陸、香港、印度、印尼、馬來西亞、尼泊爾、巴布亞紐幾內亞、菲律賓、泰國及我國，共44位央行及金融監理機構代表。課程講師由亞洲開發銀行、日本金融廳、馬來西亞證券委員會、泰國證券交易委員會、韓國金融資安研究所及金融科技公司之資深人員及中高階主管擔任。

本次研討會主題多元，包含金融科技、區塊鏈(blockchain)、加密資產(crypto assets)、普惠金融(financial inclusion)等。研討會進行方式除由講師簡報金融科技基本內容及概念外，亦請各學員分享各自機關資安監理架構及經驗，透過各方意見交流，增進學員對金融科技與資訊安全相關議題之瞭解。

三、報告內容

本報告共分四個章節，除前言外，第貳章為本次研討會著墨較多之區塊鏈。第參章則為研討會其他議題，包含金融科技的影響與對監理架構之衝擊、LenddoEFL介紹、Global Mobility Service介紹、Money Forward介紹、日本開放銀行(Open Banking)、日本金融廳對加密資產的監管。最後第肆章則為本次研討會的心得與建議。

貳、 區塊鏈

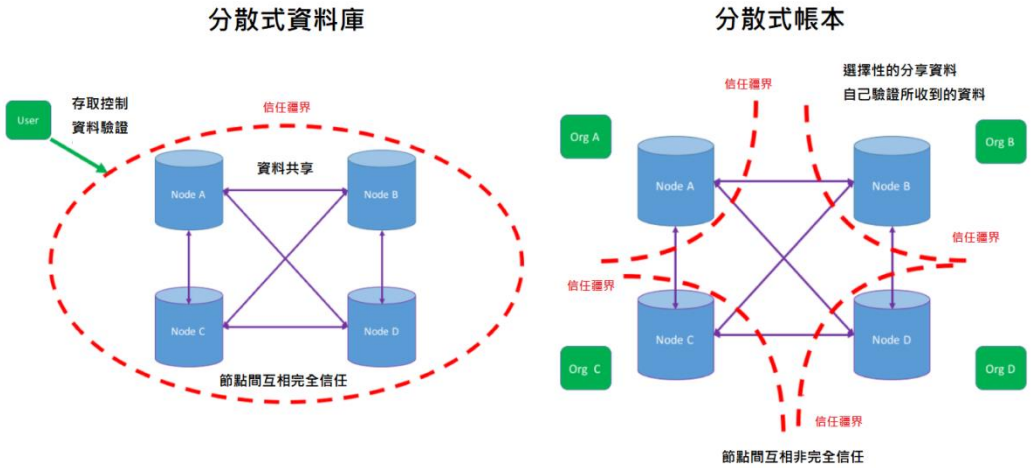
一、中央式資料庫、分散式資料庫、分散式帳本與區塊鏈

中央式資料庫、分散式資料庫(distributed databse)、分散式帳本(distributed ledger technology, DLT)與區塊鏈之區別如下：

(一) 資料庫一般可依物理上的分散狀態區分為中央式資料庫與分散式資料庫。中央式資料庫只有單一節點，分散式資料庫則有多個節點。多個節點代表有較多的系統冗餘度(redundancy)，可增加系統的容錯(fault tolerance)能力，惟須處理系統資料的同步問題，系統的複雜度較高。分散式資料庫受限於CAP定理(CAP theorem)，不可能同時滿足一致性(consistency)、可用性(availability)與分區容錯性(partition tolerance)。

(二) 在分散式資料庫(如圖1)情形下，無論是否由單一組織控制，節點間互相完全信任、共享資料，並驗證由外界傳入的資訊。分散式帳本則屬於一種分散式資料庫，惟節點間不完全互相信任，彼此間選擇性的分享資料，並驗證每筆由其他節點傳入的資料。由於分散式帳本之節點彼此間的非完全互相信任關係，因此需要特別之共識機制以達到系統間之一致性。

圖 1 分散式資料庫與分散式帳本

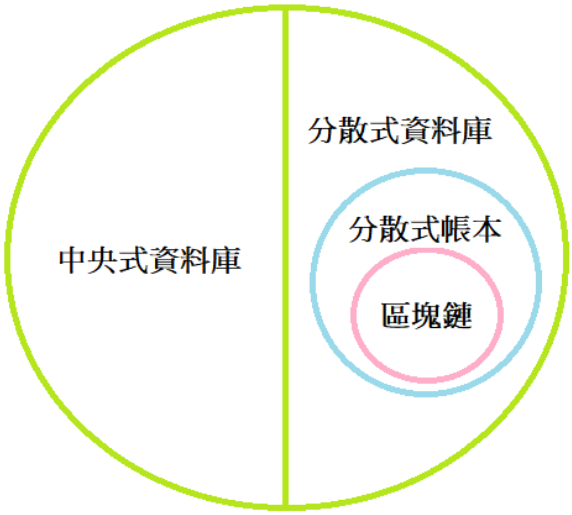


資料來源：Retrieved Dec. 17, 2018, from https://gendal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers/

(三) 區塊鏈是一種採用特殊資料結構的分散式帳本，將資料置於區塊內，並以雜湊值連接區塊。區塊鏈中舊的資料將永遠保存，新的資料則添加於帳本的後面，故區塊鏈是一種只能增加卻不能刪減與修改的分散式帳本，此種結構確保了資料正確與完整性。

(四) 中央式資料庫、分散式資料庫、分散式帳本與區塊鏈之關係可用圖2表示。

圖 2 中央式資料庫、分散式資料庫、分散式帳本與區塊鏈之關係



資料來源：Retrieved Dec. 28, 2018, from https://www.youtube.com/watch?v=J99XKplYRjo

二、區塊鏈與中央式資料庫之比較

(一) 區塊鏈相比於中央式資料庫之優勢

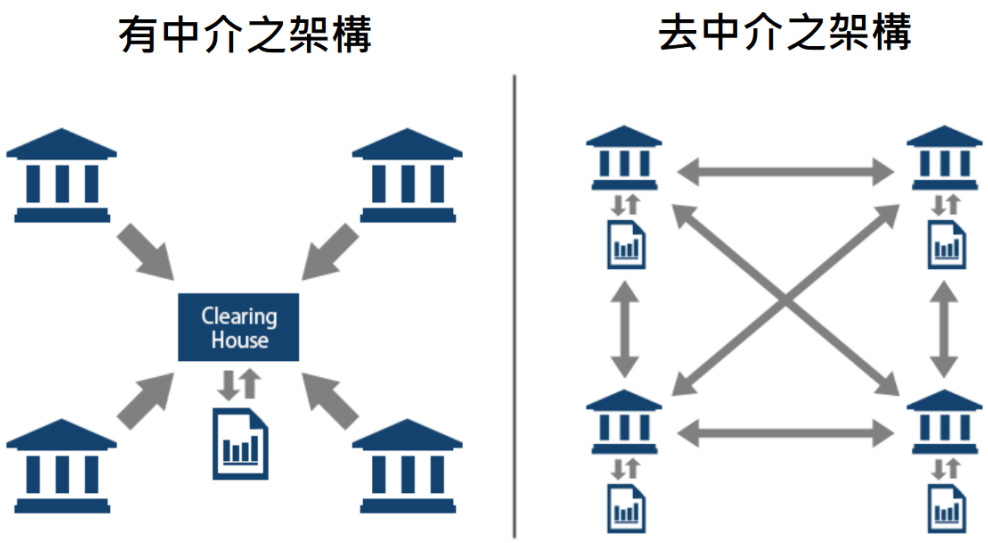
1. 去中介化(disintermediation)：

區塊鏈本質上是一種新型態的分散式資料庫，在無中央管理者的情況下，使多個不完全互相信任之個體可以共享資料庫。每個節點對每一筆新增的資料進行獨立的驗證與處理，每個節點保持平等與獨立，並以共識機制確保節點上資料之一致性。相較起來，中央式資料庫將資料交由單一中心管理者，並由此管理者負責資料的維護與處理。

資料並非是無形的事物，而是存在某個電腦系統中的硬碟與記憶體中，

任何一個具有足夠權限的系統管理者皆可破壞或變更資料。因此當我們把資料委託給某個資料庫時，我們信任的並非是這個資料庫的技術，而是信任管理這個資料庫的組織，而目前確實相當多這樣的組織，如政府、銀行、交易所，甚至包含一些私人公司如優步(Uber)、臉書(Facebook)與亞馬遜(Amazon)。過去這些組織為資料庫之使用者架起了中介的橋樑，傳遞價值，賺取受信任的利潤。然而區塊鏈則以加密演算法、共識機制與分散式資料庫起建立信任機制，取代這些受信任組織，讓使用者可以直接接觸，而達成去中介化(如圖3)。

圖 3 有中介與去中介之架構



資料來源：Retrieved Dec. 18, 2018, from https://www.nikkoam.com.au/adviser/articles/2016/08/fintech-disruptor-or-saviour

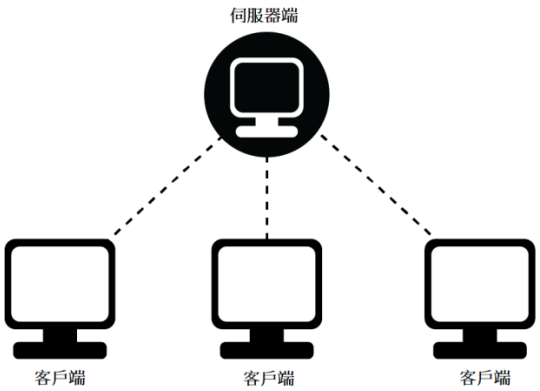
2. 系統穩健性(robustness)[1]

中央式資料庫常使用主從式架構(client-server model) (如圖4)，此種架構主要分為伺服器端(server)與客戶端(client)，資料由伺服器端負責儲存及管理。當客戶端需要使用服務時，則向伺服器端發送請求，並等待伺服器端處理後回復結果。此種架構具有整體系統效能較佳、網路傳輸負荷較低，

[1] 穩健性：系統低抗干擾與處理錯誤，並繼續維持正常運作之能力。

以及存取及管理較易等優點。

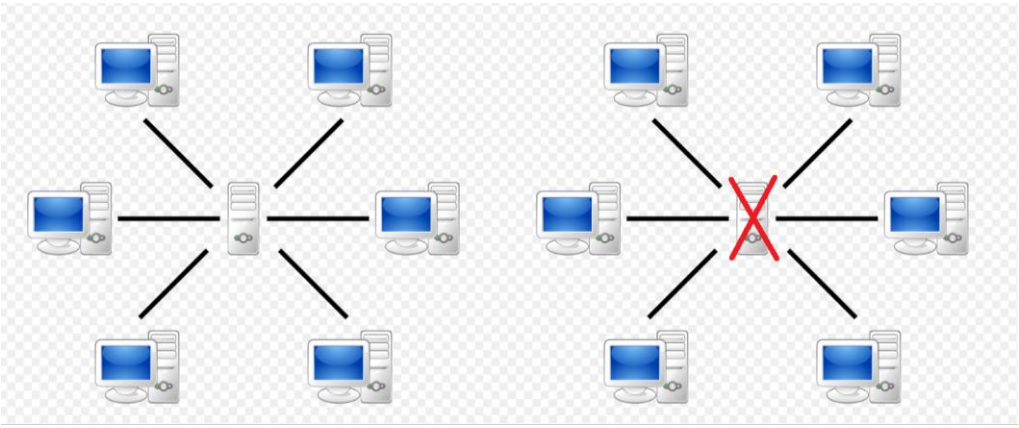
圖 4 主從式架構



資料來源：Retrieved Dec. 19, 2018, from https://www.oreilly.com/library/view/mastering-c-game/9781788629225/4014dd75-bda7-4467-be3c-1f074c6ec25d.xhtml

然而這種仰賴單一個體之結構易有單點失效(single point of failure)之情形，即若某重要元件故障導致伺服器端失效，則將造成整個系統無法運作(如圖5)。此問題雖可透過增加系統內的冗餘度並配合完整災難復原計畫(disaster recovery plan)來緩和，即增加相同功能之元件，在平常運作時將資料備份至備用元件，以及在主要運作元件失效時切換成備用元件，只要備用元件沒有同時失效，系統將仍可繼續運作。惟此法將提高系統的成本與設計複雜度。

圖 5 單點失效



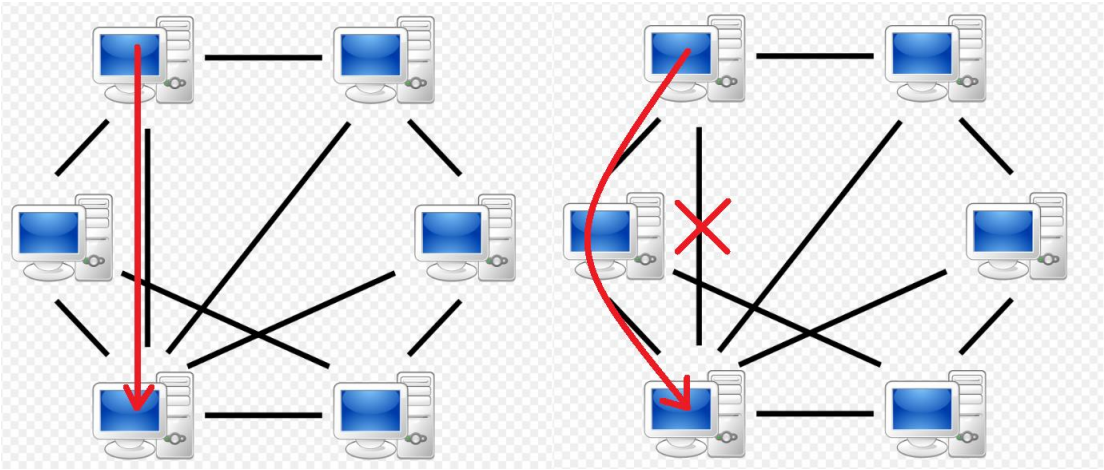
資料來源：Retrieved Dec. 20, 2018, from http://farid-tech.com/networking-information-about-clients-servers-and-peers/

區塊鏈的容錯能力則來自於本質上內建的冗餘度：

(1)區塊鏈具有去中心化(decentralisation)的架構，每一筆資料皆經過每一個節點之驗證與處理並形成共識。對整個區塊鏈系統來說，每個節點皆相同，節點間是平等的，故沒有任何一節點是不可缺少的，任一節點皆可被其他節點取代。

(2)區塊鏈則為對等式架構(point-to-point model)[2]，有成本較低與無須專屬伺服器等優點。當兩節點間的直接通訊失效時，訊息仍可藉由其他節點傳送(如圖6)。外部使用者可將資料傳給任送給任何一個節點，或任意多個節點，區塊鏈之通訊協定將確保收到資料的節點會將資料傳送給其他相連之節點。

圖 6 點對點網路



資料來源：Retrieved Dec. 20, 2018, from http://farid-tech.com/networking-information-about-clients-servers-and-peers/

(3)在區塊鏈網路中，任一節點皆可自由地加入與退出，而不需做任何預告或通知。

(4)區塊鏈亦確保與網路失去連接之節點再重新連接網路後，可獲得中斷期間所產生的資料，並與整個網路共識進行同步。

[2] 對等式架構：網路中各節點直接相連與傳送資料，而不透過一中央節點完成。

(二) 區塊鏈相比於中央式資料庫之劣勢

1. 效能

在相同的比較基礎下，區塊鏈的效能較傳統中心化系統為差，如比特幣目前每秒約只能處理3~4筆交易[3]，而PayPal每秒交易筆數約上百筆VISA甚至達上萬筆。這不單只是因為區塊鏈為新生技術，其架構與程式碼尚未被最佳化，更根本的原因在於其分散式資料庫之本質特性——在新增一筆資料時，區塊鏈不只要作傳統中央資料庫所須作的所有事情，尚須多作額外三件事情：

(1)數位簽章

區塊鏈內藉由點對點網路傳送資料，為了要追溯資料之來源與確保資料完整性與不可否認性，每筆資料皆使用橢圓曲線演算法進行數位簽章，而其餘節點亦須對每筆資料之簽章進行驗證，產生與驗證數位簽章增加整個系統的計算量。相較起來，傳統中央資料庫在安全的傳輸連線建立完成後，並無將每筆資料進行數位簽章之必要。

(2)共識機制

區塊鏈技術本質上是分散式資料庫，故仍須共識機制演算法解決分散儲存時資料一致性的問題，如區塊鏈採用的工作量證明、權益證明(proof of stake, PoS)[4]與實用拜占庭容錯(practical byzantine fault tolerance, PBFT)等方式。在實際運作下，節點間將不可避免來回傳送多次資料，以解決區塊鏈可能的分叉問題並達成共識。相較起來，傳統中央資料庫雖也須處理及放棄一些不符合資料格式與商業規則限制之交易資料，惟這些事情是在單一主機內完成，故可少去很多溝通與資料傳送上的工作量。

---

[3] 依平均交易大小(average transcation size)500bytes 計。https://tradeblock.com/bitcoin/historical/1w-f-tsize_per_avg-01101

[4] 權益證明：一種共識機制演算法，藉由加密資產持有量、持有時間及隨機因子來決定下一個區塊的創造者。可用於解決工作量證明法需消耗大量計算力之問題。

(3)系統內建的冗餘度

由於區塊鏈節點間非完全信任之架構，在鏈上新增的每一筆資料皆須經過區塊鏈網路內的每一節點之檢查與驗證，如交易格式、數位簽章與工作量證明。相同的工作被每個節點重複執行，最終產生一樣的結果而形成共識；但在中心化系統下，這些交易處理與驗證工作就算包含備援系統也只需要做兩次，因此兩者間會有效能間的差距。

2. 資料隱私性

區塊鏈中的每個節點對於資料庫的狀態、資料的內容與資料變動之來源都有完整的讀取權限，也因此每個節點獨立驗證與處理每一筆新增的資料，惟這種對於每個節點完全之透明性，在許多情形下是不可接受的。若該區塊鏈是用於一般資料的存取，由於節點在驗證某筆資料是否有效的時，並不在意資料的內容，故資料在放上區塊鏈之前可以先進行加密，而不影響鏈的運作。但若區塊鏈用於加密資產的交易，節點在驗證交易時須充分了解交易的內容，以確認加密資產的所有權，此時上鏈的資料是完全透明以便於其他節點驗證交易。

傳統資料庫只有單一中心管理者需負責新增資料之驗證與處理，因此也只有該管理者需要完整的了解資料庫的狀態、新資料所造成之變動與資料更新者，其完整讀取權限是限制在本地端(local)，而非所有節點。若須保護資料之隱私性與機密性，可在中心管理資料庫設定規則，以限制其他節點之讀取權限。

整體來說，傳統資料庫是寫入與讀取皆可限制的資料庫，而區塊鏈是只有寫入可以限制的資料庫。雖然目前區塊鏈有發展出技術以提高較高的隱私性，如使用多個地址、交易內容加密及零知識證明[5](zero knowledge proof)

[5] 零知識證明：一方可向另一方證明知道某件事，卻不須向另一方透露額外支資訊。大零幣(Zcash)藉由其零知識證明演算法 zk-SNARKs，可證明”資產的移轉是有效的”，但毋須透露交易方之資訊。

等技術。然而，越想在區塊鏈上隱藏資訊，技術就越複雜，驗證與處理資料所需的計算量也越大。但不論這些技術如何發展，資料隱私性與區塊鏈的根本技術設計在本質有所衝突，故這些技術都不比傳統資料庫的隱私技術來的簡單與直覺。

(三) 比較結論

總結來說，區塊鏈在去中介化與系統穩健性有較大優勢，而傳統中心化資料庫則有更好的效能與資料隱私性，因次考量技術之選擇時，仍須依實際應用情況與需求為主。區塊鏈與中心化資料庫之比較彙總如表1。

表 1 區塊鏈與中央式資料庫

	區塊鏈	中央式資料庫
資料共享	不需資料中心	需資料中心
不可竄改性	資料由多個個體驗證、只能添加資料	資料由單一個體驗證、可複寫
零停機時間	成本低	成本高
交易速度	慢	快
隱私	較差	較佳
自動程序	智能合約	預儲程序

資料來源：Kazumasa Miyazawa (2018) “How blockchain can change financial transactions”

三、區塊鏈的分類

目前區塊鏈可分類為三種類型：

(一) 公有鏈(public blockchain)

又稱為非許可制區塊鏈(permissioneless blockchains)，現有應用包含比特幣與乙太幣等，有下列特性：

1. 任何人皆可下載區塊鏈的客戶端的軟體、加入區塊鏈網路、參與交易驗證，以及將資料寫入資料庫。
2. 任何人皆可成為區塊鏈的用戶，在鏈上完成交易，而不須事先註冊與得到授權。
3. 資料庫公開透明，任何人皆可讀取其內之交易紀錄，惟用戶的真實身份則以假名保護。
4. 資料庫不受單一機構控制，節點依事先設計的規則運作。因沒有任何個體可以控制或竄改資料庫之資料，故被認為最接近「去中心化」。
5. 由於公有鏈參與者數量與身分皆不確定，在共識機制上常使用工作量證明法或權益證明法，並提供經濟激勵機制以鼓勵節點保持誠實。

(二) 聯盟鏈(consortium blockchain)

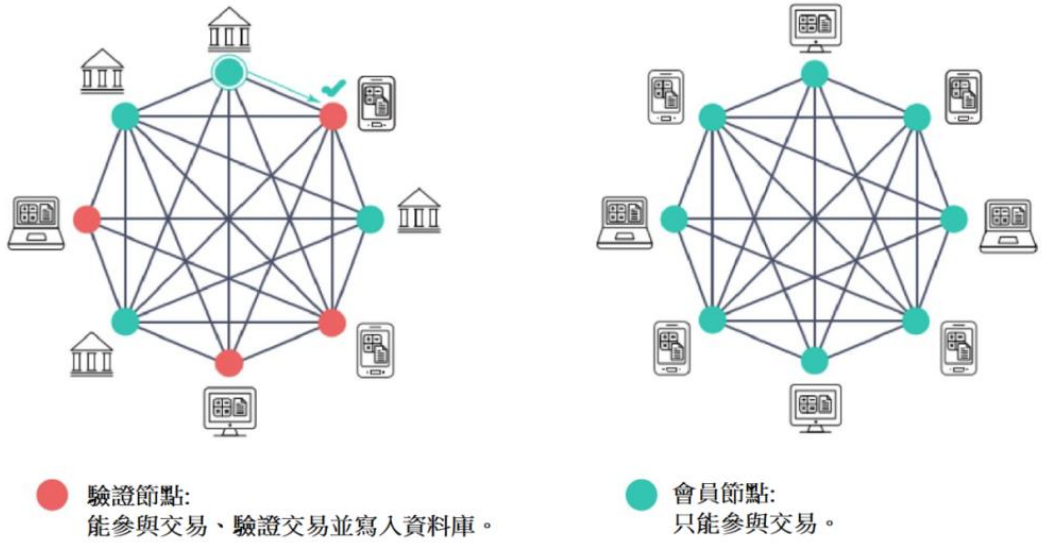
一般來說聯盟鏈較適合於找不到一個可信任第三方作為中介橋梁的應用，如金融機構間的交易與結算、KYC或是產銷履歷之可追溯性。聯盟鏈具有下列特性：

1. 由數個個體組成之聯盟共同管理之區塊鏈，只對經過註冊許可之聯盟成員開放全部或部分功能。
2. 不同節點擁有不同的讀取與寫入權限，有的節點可驗證交易並將資料寫入資料庫，有的節點只能參與交易，亦有僅具讀取權限之審計節點(如圖7)。

3. 運作規則由預先選定的群體決定，被認為是部份「去中心化」。

4. 參與者數量與身分皆已知，在共識機制上常使用權益證明、權利證明與實用實用拜占庭容錯[6]等。由於對聯盟成員來說，降低成本、去中介化與資料安全就是一種激勵，因此通常不需提供額外經濟激勵機制。

圖 7 聯盟鏈



資料來源：Retrieved Dec. 20, 2018, from https://medium.com/7sevencoin/types-of-blockchain-public-private-and-consortium-blockchain-e190604df820

(三) 私有鏈(private blockchain)

與聯盟鏈合稱為許可制區塊鏈(permissioned blockchains)，常用於企業、政府機構的內部數據管理，雖無法解決信任問題，但可改善行政流程並提高組織之可審計性與透明性。私有鏈通常具有下列特性：

1. 寫入權限僅於組織內，讀取權限則有限制的對外開放，資料具有較高的隱私性。

2. 區塊鏈之運作規則由組織自行決定，組織可刪改資料庫內容、審查特定交易，或是對不同交易方有不同回應，因此私有鏈被認為仍是接近「中心化」的系統。

[6] 實用拜占庭容錯：一種較適合聯盟鏈的共識機制，在惡意節點少於三分之一的情況下，可保證系統的正確性。

四、由公有鏈到許可制區塊鏈

(一) 由於公有鏈假設系統中存在最大的不確定性與無信任度，因此許多設計皆是在考慮最壞情況後做出的決定，如使用工作量證明法作為共識機制，以及使用較長的區塊產生時間[7]以避免分叉產生陳腐區塊(stale block)[8]，這些措施雖增加了系統的穩定度，卻對公有鏈效能造成了限制。但對於許多企業與組織來說，無信任度與去中介化的要求沒有那麼高，此時改採用許可制區塊鏈可提供較快的交易速度、較高的隱私性與較低的成本。

(二) 在共識機制上，由於許可制區塊鏈之參與節點彼此知道真實身分且數量已知，故不會有受到女巫攻擊的情況，此時可採用實用拜占庭容錯演算法，不僅達成共識的時間較短、算力消耗較低且具備結算最終性，而無須使用浪費算力且無結算最終性之工作量證明法。公有鏈與聯盟鏈及私有鏈之技術特性之比較彙總如表2。

表 2 公有鏈與聯盟鏈/私有鏈技術特性之比較

	公有鏈	聯盟鏈/私有鏈	
管理單位	無	多個	單一
參與者	自由進出	聯盟成員	組織內部
去中心化程度	完全	部分	無
節點數量	無限制、較多	有限、較少	
交易驗證參與	所有參與節點	被許可之節點	
交易速度	慢	快	

[7] 例如比特幣的區塊時間為平均 10 分鐘，而許多私有鏈則為數秒鐘。
[8] 陳腐區塊：被礦工成功挖出之區塊，但由於有其他區塊先被其他節點接受，而導致該區塊未被接受於最長之鏈中。

資料庫存取	所有參與節點	被許可之節點
結算最終性	無	有
共識機制	工作量證明、權益證明等	投票方式、拜占庭容錯等
身任	假名或匿名	已知
資料隱私性	較低	較高

資料來源：Kazumasa Miyazawa (2018) “How blockchain can change financial transactions”

(三) 在作為貨幣之可能性上，公有鏈並不滿足貨幣最重要之三項功能[9]；聯盟鏈或私有鏈則或可滿足貨幣的功能與去中心化。公有鏈與聯盟鏈及私有鏈貨幣功能之比較彙總如表3。

表 3 公有鏈與聯盟鏈/私有鏈貨幣功能之比較

貨幣的功能	公有鏈(如比特幣)	聯盟鏈/私有鏈
交易媒介	接受性較低 交易成本較高	政府可管理接受性 與交易成本
計價單位	高波動性	政府可控制貨幣供給以降低波動性
價值儲藏	接受性較低 不保證	政府可管理接受性 並提供信任

資料來源：Kazumasa Miyazawa (2018) “How blockchain can change financial transactions”

[9] 交易媒介、計價單位與價值儲存。

五、區塊鏈平臺Hyperledger Iroha簡介

(一) Hyperledger Iroha 為建立 Hyperledger 架構上的其中一個私有區塊鏈專案，由 Soramitsu 發起，目標為 B2C 市場。具有以下特性：

1. 以 C++編程提高系統效率。
2. 對行動應用程式(mobile application)有強大支援，提供 iOS, Android 與 JavaScript 等軟體開發套件。
3. 採用具有拜占庭容錯之 Yet Another Consensus 共識。
4. 具有預先定義好的指令可處理證券、身分、點數、貨幣與供應鏈等交易，其功能類似智能合約。

(二) Hyperledger Iroha 相較於公有鏈在金融交易上，具有以下優勢：

表 4 公有鏈與 Hyperledger Iroha 之比較

貨幣的功能	公有鏈(如比特幣)	Hyperledger Iroha
系統升級管理	少部分大型礦工決定	管理單位決定
交易隱私	無隱私保護 任何人皆可察看交易內容	有隱私保護 監理機關、銀行與個人有不同權限
使用者保護	若私鑰遺失，將無法在存取帳戶內金額	即使私鑰遺失，銀行仍可恢復帳戶存取權
帳戶保護	無法凍結帳戶	必要時，可凍結帳戶

資料來源：Kazumasa Miyazawa (2018) “How blockchain can change financial transactions”

參、 研討會其他議題

一、金融科技的影響與對監理架構之衝擊

(一) 金融科技的定義：

1. 金融穩定委員會(Financial Stability Board, FSB)[10]於2017年指出，金融科技為使用科技促使金融服務創新。歐洲中央銀行(European Central Bank, ECB)則認為金融科技是指使用科技於金融服務中。

2. 金融科技亦可定義為可提升下列功能之科技：

(1)貨幣功能：交易媒介、計價單位與價值儲藏。

(2)銀行功能：支付、借貸與儲蓄。

(3)市場功能：高頻交易。

(4)商業運作：傳導、溝通與管理。

(二) 金融科技帶來的改變：

1. 搜尋引擎、網路頻寬、記憶體空間與中央處理器等術的提升，使得更高頻、更細膩的資料取得、儲存與處理成為可能。指數增長的資料量，配合資料探勘(data mining)與機器學習(machine learning, ML)，未來將先由機器從巨量資料中萃取出資訊，再交由人類判讀與詮釋。

2. 網路分析(network analysis)的進步，使得監理機關可更深入瞭解交易各方的關係。配合上即時資料收集與處理，監理機關將可即時瞭解市場行為變化並做出因應。

3. 資料的格式將從人類較易讀取之格式如pdf、XLS、CSV轉變為機器較易讀取之格式如XML、JSON與鏈結開放資料(Linked Open Data, LOD)等。

---

[10] FSB (2017) “Financial Stability Implications from FinTech – Supervisory and Regulatory Issues that Merit Authorities’ Attention.”

4. 資料儲存方式將隨需求調整、從靜態轉為動態、從關聯式資料(relational database)庫轉變為易於大數據處理的非關聯資料庫如NoSQL[11]。

5. 更高頻資料收集，使得過往每季、每月得資料申報轉變為即時申報。即時資料的取得使得對未來的預測(forecasting)轉變為即時預報(nowcasting)。

(三) FSB(2017)報告指出，FinTech在金融服務的創新，可能藉由下列因素而對金融穩定有正面影響：

1. 去中心化與多樣性(diversification)：金融科技藉由大數據分析、機器人理財(robo advisor)與貸款自動化可降低金融業的進入門檻；分散式帳本在理論上也減少了結算的集中性。去中心化與多樣性在某些情況下可降低金融衝擊，當許多不同機構皆可提供金融服務由時，單一機構倒閉將不致於對市場有太大衝擊。

2. 效率：金融科技採用了機器人理財、監理科技(RegTech)、人工智慧(artificial intelligence, AI)與機器學習改善了作業效率、提高交易速度、降低了成本與資本需求。作業上效率的提升將支持金融機構的商業模式，並對實體經濟與金融系統有正面助益。

3. 透明性：金融科技善於利用資料，並從資料中挖掘資訊。此可提高透明性、減少資訊不對稱，使得風險可以更適當的定價。而金融科技亦可能創造新的金融工具，提供市場參與者新的避險管道。

4. 金融服務的可及性與方便性：金融科技如網路銀行(mobile banking)、機器人理財與保險科技(InsurTech)擴大了家庭與企業取得金融服務之可及性與方便性，此可刺激投資、促進實體經濟發展，並以多樣性之投資降低暴險。

(四) FSB(2017)報告顯示，金融科技亦可能對金融穩定有負面之影響，其管道包含：

[11] NoSQL：為 not only structured query language 之簡寫，為對不同於傳統式關聯式資料庫的資料庫系統統稱。

1. 個體金融風險，可分為：

(1)金融風險：

A. 期限不匹配(maturity mismatch) ：借貸平台使用自有資金借貸或將債權證券化時，可能導致期限不匹配。

B. 流動性不匹配(liquidity mismatch)：目前金融科技公司如電子錢包業者並未實際持有客戶的款項，而是透過銀行帳戶或信用卡進行支付。因此尚未有傳統金融機構具備的流動性轉換(liquidity transformation)功能。惟須密切注意其未來發展。

C. 槓桿：少部分金融科技公司可能在自身借貸平台上以自有資金透過槓桿進行借款。

(2)作業風險：

A. 管理風險：金融科技可能提供類似於傳統金融機構之服務，卻未受到同等級之監管，當這些公司成長茁壯時，可能對金融體系造成衝擊。

B. 資安風險：金融科技大量將資料數位化，並透過網路傳輸，這些行為可能對惡意攻擊者提供更多的系統進入點。

C. 第三方風險：雲端服務可能只有幾家重量級資訊公司提供，機器人理財可能只使用幾家Fintech公司的演算法，可能使風險過度集中。

D. 監理風險：金融科技提供創新的服務，這些服務未被現有的監理架構規範，惟相關法條卻未能即時制定與修正。

E. 金融基礎建設風險：某些創新的支付與結算方式可能演變為重要的金融基礎建設。若經營該業務的公司若遭受營運困難，可能對金融系統造成衝擊。

2. 總體金融風險：

(1)傳染性：若某家Fintech公司遭受重大損失或是駭客入侵，可能會引起消費

者對整體Fintech公司的不信任。另由於AI技術的大量採用，在缺乏人工審核的情形下，自動執行的交易策略可能導致金融市場中的傳染性。

(2)順週期性：在情緒反應上，新的借貸平台通常比傳統金融仲介更加敏感，若有逾期放款的產生，可能導致資金迅速抽離。而機器人理財與社交金融(social trading)[12]通常比傳統資產配置方法有更明顯的羊群效應(herd behavior)，也易造成資產價格的波動。

(3)超額波動：金融科技本質上就是「快」，以較高的效率取代傳統金融服務，故也易放大市場的波動性。如演算法交易可能對某交易特徵或新聞過度反應，而增加資產市場的波動性，導致發生償債或流動性問題，而傷害資產與信用市場。

(4)系統性重要性：DLT、數位通貨(digital currency)與電子錢包，來可能演變為重要的市場基礎建設，其發展有集中化、贏者全拿的趨勢。這些FinTech公司因此有動機採取較為激進的策略以取得較大的市佔率，此行為可能增加道德危險。

(五) 由於金融科技對金融系統之影響取決於市場內部結構，以及風險與創新間的取捨，因此真正的影響須由以下5點觀察：

1. 由於網路效應(network effect)[13]與規模經濟、範疇經濟等因素，金融服務的發展有中心化的趨勢。非金融機構所帶來的去中心化與去中介化，其效果未必如預期般顯著。

2. 在相關風險被適當管理的情形下，妥善運用資料並提高效率有助於金融穩定的提升，惟濫用資料與分析演算法則可能導致作業風險或提高「閃電崩盤」(flash crash)等風險發生的可能性。擁有較高效率的金融科技公司加入，可能導致現有的金融機構面臨獲利減少的壓力，而提高其風險偏好。

[12] 社交金融：在社交平台上，績效好的交易人將交易資訊公開，使得其他交易人可複製他們的交易紀錄。

[13] 網路效應：又稱網路外部性，指每位用戶對某產品之使用價值隨該產品之使用人數上升。

3. 金融科技有助於降低某些作業風險，如改善舊的系統或是作業流程生產線化。惟資安風險、第三方風險，以及其他未知的不確定性，仍可能會產生新的風險。

4. 金融科技有助於提高金融服務的可及性，擴大家庭與企業可取得之金融服務。惟相關風險亦應注意，並維持市場信心，以避免風險累積而致金融系統不穩定。

5. 金融科技導致系統變化的步調加快，將導致信用、流動性等風險的監控變為困難，故主管機關須藉由金融科技調整資料收集與風險監控的方法。

二、信用評分公司LenddoEFL介紹

(一) LenddoEFL 是由 EFL 與 Lenddo 兩家公司於 2017 合併成立。EFL 原是 2006 年哈佛大學的一個專案，於 2010 年轉為營利單位，其商業模式主要利用心理量測與非傳統資料對個人及中小型企業進行風險或信用評分，並將其評分結果提供給金融機構，以做為提供貸款與否之依據。Lenddo 則是 2011 年成立於新加坡的軟體即服務(Software as a Service, SaaS)公司，對缺乏信用紀錄的新興市場個人提供信用評分服務。

(二) 傳統金融通常使用內部資料與官方信用紀錄對貸款者進行信用評分，惟依世界銀行之統計[14]，全球約有 25 億人缺乏官方信用紀錄，4 億個小型企業無法取得金融服務。在缺乏官方信用紀錄下，又因無過去與金融機構貸款之信用紀錄，而無法從金融機構借款，以致「先有雞還是先有蛋」的問題。

(三) LenddoEFL 結合傳統資料與非傳統資料如手機或社群媒體紀錄，配合大數據分析與機器學習，並利用雲端或應用程式介面(application programming interface, API)提供身分辨識與信用評分等服務。

[14] http://datatopics.worldbank.org/financialinclusion/country/mexico

(四) LenddoEFL 使用的資料來源包含：

1. 心理與行為資料：透過網站或手機應用程式對貸款者進行簡單信用評等。
2. 數位足跡資料：電子郵件與社群媒體紀錄等。如電子郵件的資訊可能包含每日郵件數量的標準差、郵件的長度、郵件回應時間與頻繁聯絡之聯絡人數量。
3. 行動電話資料：手機瀏覽器紀錄、行事曆、通話紀錄、聯絡人、簡訊與已安裝之應用程式。
4. 金融資料：如貸款者的申請文件、銀行交易紀錄與電商交易紀錄。
5. 第三方夥伴資料：官方信用紀錄、電信商紀錄與官方其他紀錄等。

(五) LenddoEFL 再以大數據分析、機器學習處理收集到的資料，並藉由 API 連接金融機構或是 LenddoEF 提供的線上儀表板，提供客戶身分驗證、客戶產品需求評估與客戶評分等服務。

(六) 在客戶供客戶身分驗證方面，包含：

1. 身分驗證：使用多種資料來源驗證客戶的姓名、生日、電話號碼、地址、電子郵件與雇主等資料。
2. 身分證件驗證：以自拍與掃描身分證件等方式驗證客戶身分。
3. 文件收集：客戶可上傳工資證明、地址證明或簽名等所需文件。

該產品降低詐欺率、提高貸款申請成功率且只需數秒鐘即可完成驗證。

(七) 在客戶評分方面，包含：

1. 信用評分：判斷借款者的違約率。
2. 收入評分：判斷借款者是否具有高收入。
3. 回款評分：判斷借款者是否具有違約跡象。

該產品成功提高申請到貸款的成功率、降低了貸款者需要支付的利率，以及減少貸款違約率與貸款的評估時間。

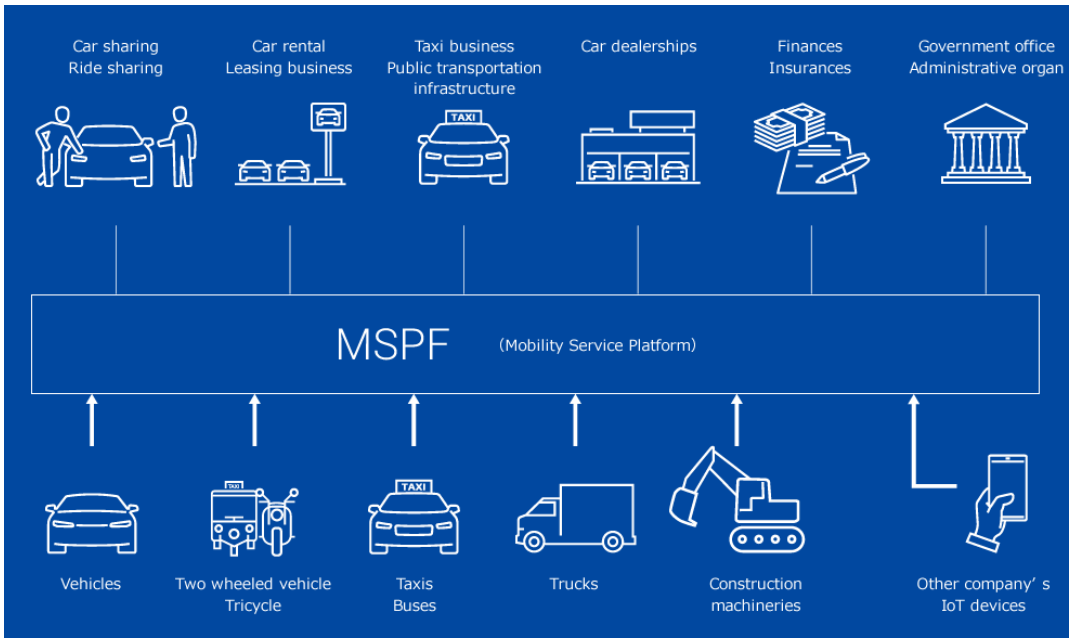
(八) LenddoEFL 的產品在新興市場帶來有效幫助：在菲律賓成功以少於傳統貸款一半的評估時間帶來了 200 萬美金貸款。在印度則於 3 個月內成功完成 6000 筆貸款，每筆貸款平均金額為 250 美元。

三、車貸管理平臺公司Global Mobility Service介紹

(一) Global Mobility Service(GMS)為2013年立於日本東京之金融科技公司，並在菲律賓、柬埔寨與印尼設有分公司。該公司在汽車上安裝一之物聯網(Internet of Things, IoT)元件，稱為行動雲端連接系統(Mobility-Cloud Connecting System, MCCS)。

(二) MCCS上具有多樣之感應器，可收集汽車所產生之大數據並回報給汽車服務雲端平台(Mobility Service Platform, MSPF)。GMS之合作夥伴可透過API存取MSPF上之數據(如圖8)。

圖 8 汽車服務雲端平台



資料來源：Retrieved Jan 1, 2019, from https://www.global-mobility-service.com/en/mspf.html

(三) MCCS另具有遠端引擎啟動控制系統。若汽車失竊，或是若貸款者未能按月繳交貸款，該系統可在安全時停止並鎖定該汽車之引擎(如圖9)。若貸款者恢復繳款後則可遠端解鎖。

圖 9 行動雲端連接系統

資料來源：Marei Oshima (2018) “Global Mobility Service Inc. Company Profiles”

(四) 新興市場由於缺乏可官方之信用紀錄，因此汽車貸款被拒絕率通常較高，如菲律賓、柬埔寨與印尼之被拒絕率分別高達90%、80%與70%。GMS之服務成功將汽車貸款違約率由20%降為0.9%，因而提高了金融機構的貸款意願，使得貸款者獲得貸款的機會上升。

四、理財管理平臺公司Money Forward介紹

(一) Money Forward 為 2012 年成立於日本之金融科技公司，為個人及企業提供簡化會計與理財服務，其服務分為兩個類型：

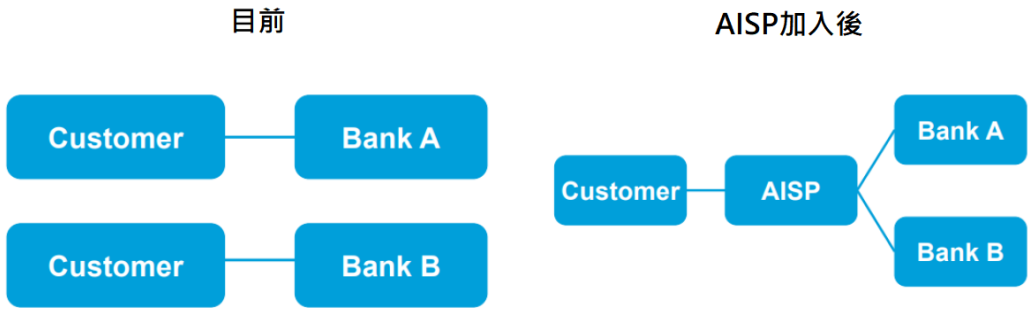
1. 零售(Business to Consume, B2C)：使用手機應用程式 Money Forward ME 整合超過 2650 家金融服務公司，包含銀行、信用卡、證券、外匯、退休金、飛行里程、線上購物、電子錢包與行動支付等不同帳戶，提供自動家庭記帳、消費分類、儲蓄、投資、轉帳等整合式個人金融服務。至 2018 年

10 月有超過 700 萬名使用者，在日本市佔率超過 25%。

2. 躉售(Business to Business, B2B)：以軟體即服務之雲端平台，能從第三方會計軟件匯入交易細節，提供記帳、會計、報稅、支付結算、費用報銷與商業數據分析，並能能自動生成財務報表，使中小企業能在取得會計服務的同時降低成本。

(二) 目前消費者若在不同銀行皆有帳戶，則須使用各銀行提供軟體來存取不同的帳戶。Money Forward 的商業模式則是整合所有帳戶資訊，成為帳戶資訊服務提供者(account information service provider, AISP)[15]，使得消費者可透過單一平台存取所有帳戶資訊，而無須安裝多個軟體，並花時間熟悉使用方式(如圖 10)。

圖 10 Money Forward 的商業模式



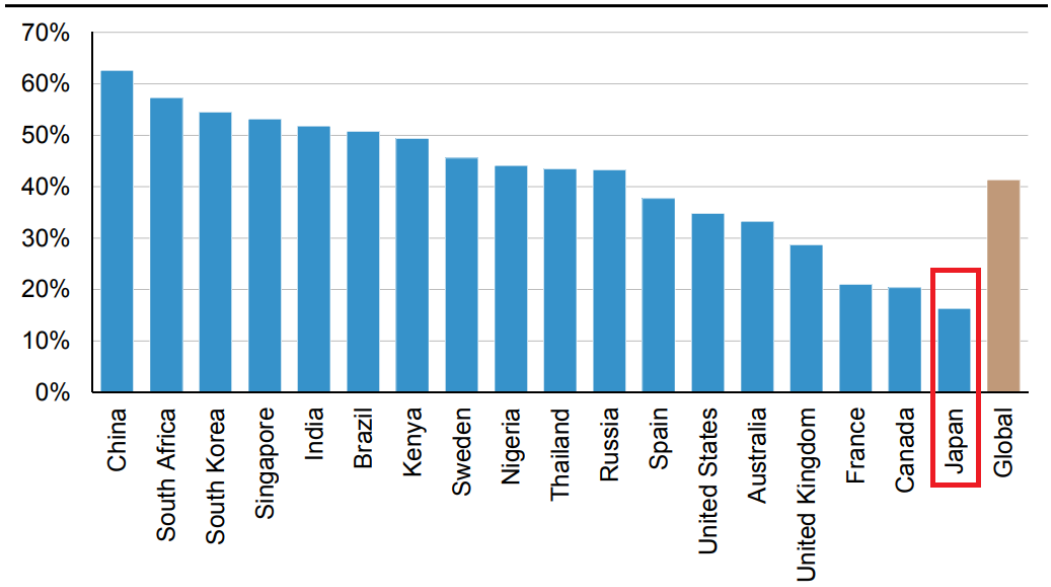
資料來源：Marei Oshima (2018) “Global Mobility Service Inc. Company Profiles”

五、日本開放銀行(Open Banking)

(一) 日本金融宣傳中央委員會(The Central Council for Financial Services Information, CCFSI)之研究亦顯示，超過 80%之消費者依自動提款機與生活圈距離選擇銀行。另由於日本線金線下管道較為方便，而 KPMG(2015)[16]亦指出日本行動滲透率較全球平均為低(如圖 11)。

[15] 歐盟二號支付服務指令下，AISP 為被受權可存取銀行客戶資部分訊之第三方。
[16] KPMG (2015) “Mobile Banking 2015: Global Trends and their Impact on Banks”

圖 11 行動銀行滲透率

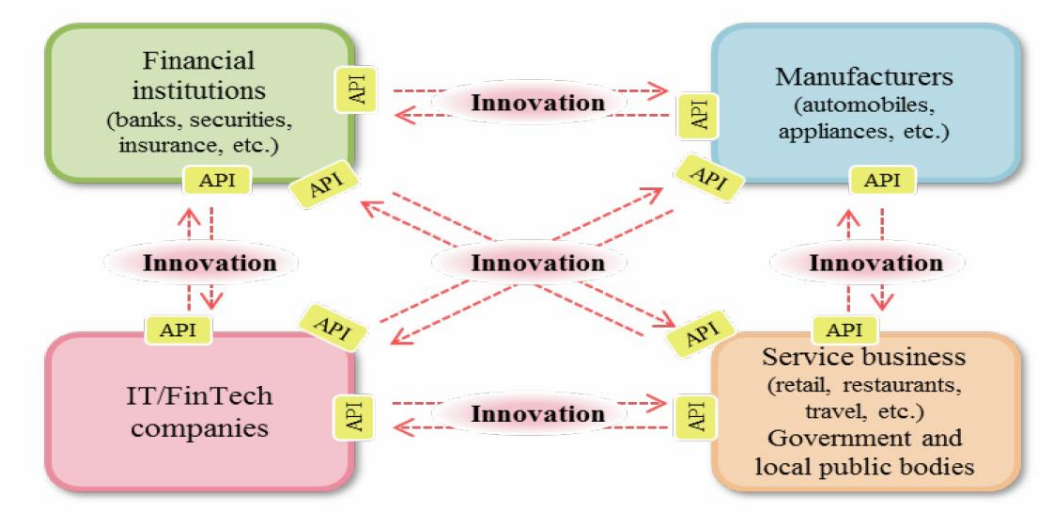


資料來源：KPMG (2015) “Mobile Banking 2015: Global Trends and their Impact on Banks”

(二) 為使支付方式更多元化並降低成本，日本金融廳(Japan Financial Service Association, JFSA)於 2017 年修正銀行法，建立了規範電子支付業者的架構。日本銀行公會(Japanese Bankers Association, JBA)則邀請銀行、資訊科技公司、金融科技公司、學術界專家、律師、消費者聯盟，以及相關主管機關，於 2017 年發表了開放銀行應於程式介面的標準[17]，並規範安全措施與使用者保護等標準，其目標是創造出一個連接金融業、科技業、製造業、零售服務與政府單位之開放 API 生態(如圖 12)。

[17] JBA (2017) “Report of Review Committee on Open APIs: Promoting Open Innovation”

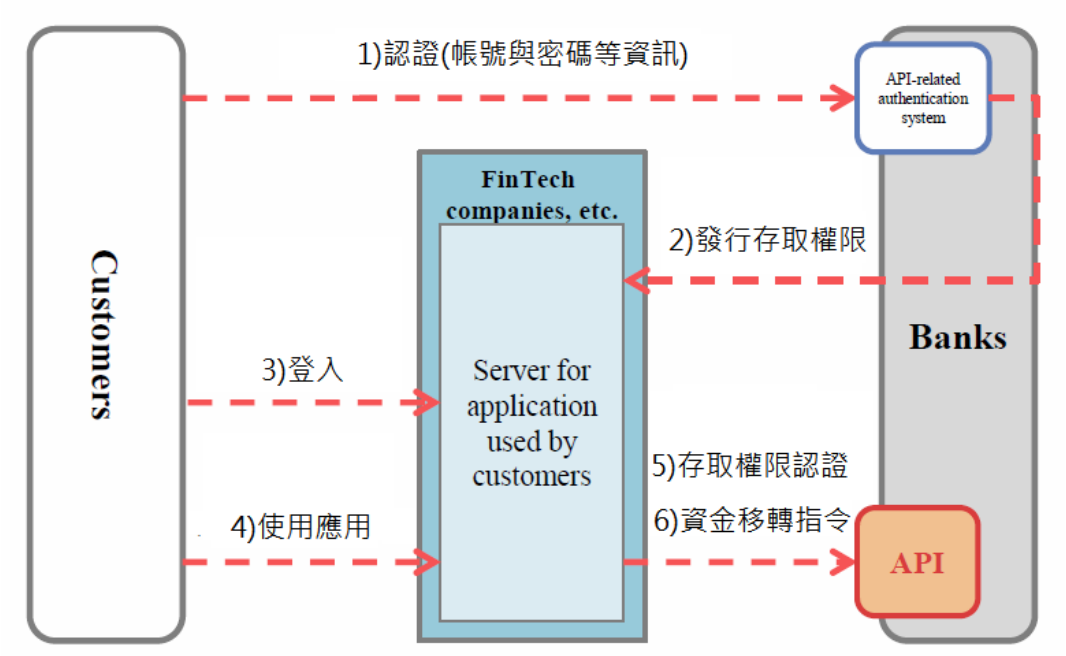
圖 12 開放 API 生態



資料來源：JBA (2017) “Report of Review Committee on Open APIs: Promoting Open Innovation”

(三) 開放 API 使得不同部門可藉由開放的網路安全地共享資料，亦是結合不同資料與服務，促進創新的關鍵技術。開放 API 的簡化架構如圖 13。

圖 13 開放 API 簡化架構



資料來源：JBA (2017) “Report of Review Committee on Open APIs: Promoting Open Innovation”

六、日本金融廳對加密資產的監管

(一) 為滿足七大工業國組織與防止洗錢行動工作組織(Financail Action Task Force, FATF)對洗錢防制與打擊資恐(anti-money laundering/ Combating the Financing of Terrorism, AML/CFT) 之承諾，並避免未來再次發生虛擬通貨交易所破產[18]而致消費者之重大財務損失，日本金融廳於 2017 年建立對加密資產交易所之監理架構，主要內容如下:

1. 建立 AML/CFT 機制，包含：

(1)認識你的客戶(know your customer, KYC)。

(2)KYC資料與交易資料的紀錄與保存。

(3)可疑交易的報告。

(4)內部控制。

2. 依資金結算法(Payment Services Act)規定，交易平台自 2017 年 4 月開始須進行註冊，以進行消費者權益保護，包含：

(1)避免資訊不對稱。

(2)系統安全管理。

(3)消費者資產隔離。

(4)最少資本要求。

(5)外部稽核。

(二) 資金結算法 2 條第 5 款規定虛擬通貨(virtual currency)為具有財產上之價值且具有以下性質者：

1. 可對不特定人作為支付之使用，且得與不特定人之法幣互換。

[18] 如 Mt.Gox 於 2014 年因被駭客盜取比特幣而申請破產。

2. 以電子技術記錄與移轉。

3. 非為法幣或法幣為單位之資產。

(三) 依資金結算法規定，交易平台自 2017 年 4 月開始須進行註冊，惟法令之規範對象並不含加密資產本身，主要是規範虛擬通貨交易服務提供者(virtual currency exchange service provider)，包含經紀商，交易所與保管機構。電子錢包提供者，若無提供經紀或交易等服務，則不屬於受管理之範圍。

(四) 日本金融廳於 2018 年 10 月 24 日核准日本虛擬通貨交易所協會(Japan Virtual Currency Exchange Association, JVCEA)設立，負責對境內虛擬通貨交易所的進行監督。依據資金結算法規定，該協會職責包含下列事項：

1. 制定自律規範，包含系統性風險管理、洗錢防制與打擊資恐、誘導交易與廣告、不公平交易、交易保證金與資產隔離等。首次代幣發行(Initial Coin Offering, ICO) 目前尚在考慮是否列入。

2. 監督協會會員。

3. 對會員採取建議與警告等措施。

4. 處理消費爭議並與其他組織合作。

肆、 心得及建議

一、心得

(一) 區塊鏈解決了無信任第三方下之資料交換問題，但在有信任第三方下則較無用武之地

1. 區塊鏈利用點對點傳輸、密碼雜湊函數、共識機制與公開金鑰加密等技術，經過巧妙的安排與重組，成為一種新型態的分散式資料庫，以較傳統資料庫簡潔之方式解決了共享式資料庫的寫入問題，而此種資料庫型態相當適合輕量級金融交易市場交易資料的紀錄。

2. 在無信任第三方中介下，區塊鏈確保了資料的不可竄改性，達成了各節點下資料庫之同步，但卻有較低的處理效能與較差的資料保密性。在有信任第三方作為中介情形下，若將資料存於第三方的中央資料庫，則可提供更佳的處理效能與資料保密。此時或非利用區塊鏈之適當時機。

(二) 公有鏈在應用上有其適合情況，惟許可制區塊鏈或較適合金融交易

1. 公有鏈之節點身分不確定、數量眾多且數量未知。在不信任的環境下，技術選擇上須考慮最差情況，故共識機制較常採用不具備結算最終性工作量證明，可避免受到女巫攻擊。惟為避免分叉，交易速度較慢，在金融交易亦可能導致雙重支付。

2. 許可制區塊鏈參與節點身分確定、數量較少且數量已知。在有一定信任的基礎下，區塊內之資料可在必要情況下逕行修改，共識機制亦可採用具備結算最終性之實用拜占庭容錯，交易速度較快，或較適合金融交易。

3. 公有鏈則較接近完全去中心化，許可制區塊鏈則或多或少含有中心化的成分。故在技術的選擇上，去中心化與中心化各有適用的情況，沒有優劣之區別。

(三) 金融科技擴大金融服務之可及性，惟資安暴險也同步擴大

1. 金融科技帶來了新的服務，如機器人理財、保險科技、點對點個人借貸(peer-to-peer lending, P2P lending)與新型態支付等。為了提供更好的金融服務，金融科技業者收集更多的個人資料進行大數據分析，利用機器學習技術找出更準確的模型，建立 API 結合第三方服務，提供使用者更及時、更個人化的服務。

2. 惟金融科技大量將資料數位化，以網路傳輸，並透過程式自動執行，可能對惡意攻擊者提供更多的系統攻擊點。另許多公司皆為新創公司，經營者認為其首要目的是創造營收，以致這些科技公司雖與金融業者握有類似的資料，提供類似的金融服務，但在資訊安全上之投資卻遠不及現有金融業者。此外，在監管法規跟不上科技發展的情形下，這些科技公司易形成整個資安保護網的漏洞。

二、建議

(一) 注意金融科技發展與其對金融穩定之潛在影響，並培養相關監理人才

1. 金融科技帶來了便利，惟也導致風險的增加，尤其在超額波動(excess volitility)、資安、管理與監理等風險上。若這些高度資訊化之金融科技發生事故，其傳播速度與影響將更大，可能導致金融市場重大衝擊。

2. 監理機關基於維持金融穩定之目標，可由內部培養瞭解金融科技商業模型與監理之人才，持續關注其發展，以因應未來可能監理趨勢。

(二) 監理機關可依風險導向監理，監控高風險加密資產

1. FSB(2018)指出，加密資產目前尚不致對全球金融造成不穩定。惟其具網路效應，其市場發展速度可能會超越想像，監理機關仍需密切觀察。若加密資產被廣泛運用於支付、清算與證券交易上，則可能成為未來重要金融基礎設施，其發展或對未來金融穩定造成影響。

2. 監理機關可注意加密資產之市值及市值上升速度，以瞭解當加密資產往下崩跌時，可能引發的財富效應；另應注意交易量、槓桿、波動率、與其他資產相關性，以及金融機構可能之暴險，並將必要資訊如價格、成交量與撮合明細等資料建立資料庫，以因應未來可能需求。

(三) 密切注意區塊鏈未來發展，但注意其侷限性

區塊鏈可解決無信任第三方中介下之資料交換問題，或廣義的說，解決共享式資料庫的寫入問題。惟其「無信任」是建立在區塊鏈內，其衍生之加密資產或是智能合約，在與現實世界的資產及服務連結時，仍需建立在「信任」上。若無信譽卓著之個體提供債權保證或作為受信任之的第三方，則易形成詐欺或犯罪的溫床。監理機關宜密切注意其發展，保守地表達對其積極或正面之意見，以免成為不肖業者之廣告。

參考資料

1. 本次研討會主辦單位提供與會人員之講義資料。
2. 洪菁吟 (2018)，「美國紐約聯邦準備銀行舉辦之 Supervision 訓練課程」，中央銀行出國報告，1 月。
3. 李典運 (2018)，「參加 SEACEN 研訓中心舉辦之金融科技研討會出國報告」，中央銀行出國報告，5 月。
4. 蕭裕錦、吳端霖 (2018)，「參加泰國央行「金融科技博覽會」出國報告」，中央銀行出國報告，6 月。
5. Kazumasa Miyazawa (2018) “How blockchain can change financial transactions
6. Marei Oshima (2018) “Global Mobility Service Inc. Company Profiles”
7. FSB (2017) “Financial Stability Implications from FinTech – Supervisory and Regulatory Issues that Merit Authorities’ Attention.”
8. JBA (2017) “Report of Review Committee on Open APIs: Promoting Open Innovation”
9. KPMG (2015) “Mobile Banking 2015: Global Trends and their Impact on Banks”
10. 7sevencoin (2018) , “Types of Blockchain—Public, Private, and Consortium Blockchain,” Retrieved Dec. 20, 2018, from https://medium.com/7sevencoin/types-of-blockchain-public-private-and-consortium-blockchain-e190604df820
11. What is the Difference Between a Blockchain and a Database? . Retrieved Dec.29, 2018, from https://www.coindesk.com/information/what-is-the-difference-blockchain-and-database
12. Vince Tabora (2018) , “ On distributed databases and distribuedledgers,” Retrieved Dec.1, 2018, from https://medium.com/@chainfrog/5-reasons-that-blockchain-is-not-just-a-slow-database-55fe9d913578
13. Judd Bagley (2018) , “What is Blockchain Technology? A Step-by-Step Guide

For Beginners," Retrieved Dec.2, 2018, from https://blockgeeks.com/guides/what-is-blockchain-technology/

14. Dave Bayer, Stuart Haber adn W. Scott Stornetta (1992), "Improving the Efficiency and Reliability of Digital Time-Stamping," Sequences II: Methods in Communication, Security and Computer Science. Springer-Verlag: 329 – 334.
15. Cynthia Dwork, and Moni Naor (1992), "Pricing via Processing or Combatting Junk Mail," Annual International Cryptology Conference CRYPTO 1992: Advances in Cryptology - CRYPTO' 92 pp 139-147.
16. Adam Back (2002), "Hashcash - a denial of service counter-measure," Retrieved Dec.5, 2018, from http://www.hashcash.org/papers/hashcash.pdf
17. Satoshi Nakamoto (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System," Retrieved Dec.10, 2018, from https://bitcoin.org/bitcoin.pdf
18. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder (2016), "Bitcoin and Cryptocurrency Technologies," Retrieved Dec.13, 2018, from https://lopp.net/pdf/princeton_bitcoin_book.pdf
19. Andreas M. Antonopoulos (2014), "Mastering Bitcoin," Retrieved Dec.17, 2018, from https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/
20. GENDAL (2016) , " On distributed databases and distribuedledgers," Retrieved Dec.17, 2018, from https://gendal.me/2016/11/08/on-distributed-databases-and-distributed-ledgers/
21. Blockchains & Distributed Ledger Technologies. Retrieved Dec.21, 2018, from https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/
22. FSB (2018), "Crypto-asset markets：Potential channels for future financial stability implications."