行政院所屬各機關因公出國人員出國報告書

(出國類別：其他)

區塊鏈技術應用於發行數位貨幣之近況

服務機關：中央銀行

姓名/職稱：吳桂華/一等專員

出國地點：英國倫敦

出國期間：105.11.12~19

報告日期：106.2.15

目 錄

壹、前言

一、考察過程

本次參加金融研訓院舉辦之「英國數位金融及 FinTech 考察團」，期間自 2016 年 11 月 12 日至 19 日，國內參與考察之機構來自銀行、壽險公司、台灣集保公司、IBM 等單位，合計團員 20 名。

本次倫敦主要考察對象及內容包括：

- 金融科技孵化器 Level 39

  歐洲最大的創新金融科技孵化器位在 Canary Wharf 辦公室第 39 樓，Level 39 分租辦公場所給 FinTech 新創業者，累計已有百餘家新創業者進駐，利用其提供之經營資源，如諮詢與討論等，發展新創金融科技。

  Level 39 進駐成員包含 105 家 FinTech 公司、22 家智慧城市(Smart City)公司、21 家資訊安全公司、18 家大數據公司、5 家零售公司及 39 家其他類公司。

- 數位銀行 Fidor Bank

  2008 年金融危機爆發，Fidor 順勢於 2009 年於德國成立無實體銀行以降低成本，並鎖定高數位化程度用戶、中小企業與開發商等對象，提供金融業務。Fidor 於 2015 在英國成立 Fidor UK 數位銀行。本場次演講由 IBM 倫敦辦公室負責 Fidor 計畫之專案經理簡報 Fidor 相關策略及業務。

- 瑞士聯合商業銀行(UBS)

  瑞銀成立區塊鏈研究中心位在金融科技孵化器 Level 39，本次考察 UBS 近期發布的 Utility Settlement Coin(USC)計畫，係以區塊鏈技術發行央行數位貨幣。

- 參加金融時報舉辦 2016 年度銀行高峰會

  研討會邀集不同專家討論英國脫歐、川普當選效應，以及 FinTech 相關議題、會後由金融時報專欄作家 Martin Wolf 結語並提出銀行業

未來面臨的挑戰。

- 邀請「數位銀行」作者 Chris Skinner 於彰銀倫敦分行簡報，分享 FinTech 未來發展。
- 跨境匯款公司 Transferwise(TFW)

TFW 提供網路平台供客戶登入進行跨境轉帳，因該公司的創新交易模式簡單，交易成本低且到匯時間快，成立至今業務迅速成長。簡報者稱，TFW 每月處理跨境支付之交易量達 150 億美元，相較於經由傳統銀行匯款模式所花的費用，TFW 每天約可為客戶節省 150 萬美元[1]。

TFW 在各國的往來銀行[2]開立存款帳戶，透過 API 與銀行介接[3]，俾利自動發送訊息給各國往來銀行進行境內款項支付。

TFW 運作流程如次(詳附錄 1)，假設英國客戶 B 欲匯款予美國友人 A，首先 B 登入至 TFW 網站並將英鎊轉帳至 TFW 的英鎊帳戶；TFW 收到 B 匯款指令及款項後，可自動發送訊息請美國往來銀行將 TFW 帳戶內的美元撥付至 A 所屬之銀行帳戶。

實際上，TFW 並未經由傳統的通匯行(Correspondent Bank)管道進行跨境匯款，只是經由 TFW 平台傳遞支付訊息至 TFW 在各國的往來銀行，再藉由各國便捷的國內支付系統進行境內即時款項支付。當 TFW 的銀行帳戶餘額接近不足以支應客戶的付款指令時，TFW 才藉由傳統通匯銀行模式，以美元(或英鎊)跨國匯款，再換匯成該國貨幣，以補足 TFW 帳戶內資金，此部分則屬於真正的跨境匯款。

此外，為配合反洗錢措施，TFW 已建置一套系統專門處理 KYC 與進行即時交易監控(Real-Time Transaction Monitoring, RTTM)，TFW 認為建置 RTTM 比基本的 KYC 更能有效防制洗錢，因為 KYC 僅過濾已確認的黑名單，然因黑名單會隨著時間及環境改變而變化，唯有

[1] 相較於傳統的匯款模式，假設 TFW 為客戶節省匯款成本為匯款金額的 3%。
[2] TFW 通常在各國只有 1 家往來銀行，如交易量大才可能在另一家往來銀行再開立帳戶
[3] TFW 講者表示，銀行若未與 TWF 直接以 API 介接，則 TFW 可將付款檔案批次傳送予付款銀行，傳送頻率視每日交易量多寡可介於 1~20 次，甚或高達 20 次。

做好即時性交易監控，瞭解交易者與其交易行為與模式之關聯性，動態調整洗錢風險交易預警與評估參數，才能有效防範洗錢行為。

二、研究目的

藉由前述行程參訪，除瞭解英國政府部門在推動金融科技方面之政策外，考察金融科技新創公司亦獲得相當多之收獲，將可作為本行未來推動相關政策及業務之參考。

例如參訪 UBS 聽取該銀行有關區塊鏈的相關計畫，其中 Utility Settlement Coin 計畫係以分散式記帳技術(Distributed Ledger Technology, DLT)發行央行數位貨幣；另外，TFW 案例說明許多金融科技新創公司有新的想法，拜新技術之賜可以快速解決客戶痛點而快速掘起。因此，本行有必要適度瞭解新興金融科技之發展，俾作為未來接受案件申請與修訂相關業務法規時之參考。

本報告後續章節安排如次，第貳章介紹英國推動金融科技情形、第參章進行區塊鏈與分散式記帳技術簡介、第四章說明國外發行央行數位貨幣之研究近況，最後提出本報告心得與建議。

貳、英國推動金融科技情形

一、英國金融科技發展優勢

英國民間發起的前三大金融科技加速器(Accelerator)分別為 Level 39、FinTech Startupbootcamp 及 Barclays Accelerator，本次參訪對象包括 Level 39 及 Barclays Accelerator。以 Level 39 為例，係成立於 2013 年 3 月，為歐洲最大的金融科技孵化器(Incubator)，Level 39 為金融科技創業者提供創新辦公環境、諮詢及創意想法討論等服務，目前有 105 家金融科技新創業者進駐。

依 Level 39 簡報資料，英國金融科技可概分為 4 大業務態樣，包括：支付、軟體、金融數據分析及平台。根據 2015 年統計，支付市場為其中最大市場，總值 10 億英鎊；軟體市場總值 4.2 億英鎊，位居第二；其次為金融數據分析市場總值 3.8 億英鎊；平台市場總值 2 億英鎊。

表 1　2015 年各國金融科技生態環境排名評比

區域	人才取得	資本籌措	政策友善度	市場需求	總分*
英國	2	3	1	3	9
美國加州	1	1	6	2	10
美國紐約	3	2	7	1	13
新加坡	4	7	2	6	19
德國	6	4	5	5	20
澳洲	5	5	3	7	20
香港	7	6	4	4	21

*1 為排名最高、7 為排名最低，總分愈低，排名愈高

資料來源：Level 39 簡報資料

上表為安永(EY)顧問公司 2015 年國際金融科技發展評估排名結果，英國在人才取得(Talent)、資本籌措(Capital)、市場需求(Demand)等因素排

名僅次於美國；在政策友善度(Policy)方面，則居首位。整體而言，英國的金融科技生態環境整體排名為全球第一。此外，倫敦為國際金融中心，聚集了 251 家外國銀行及 588 家海外企業設點，全世界 40%的頂尖企業以及全球前 10 大跨國銀行中有 4 家均將總部設於倫敦，亦為倫敦發展為金融科技中心的主要利基。

二、英國金融業務監理局(FCA)

為推動金融科技發展俾提供消費者更好的金融服務，英國金融業務監理局(Financial Conduct Authority, FCA)於 2014 年 10 月發起創新方案(Project Innovate)，由內部專家組成創新中心(Innovation Hub)，就業者提出之新產品或新商業模式提供法令遵循意見，使 FCA 得配合新科技而進行相關法令之改變。

FCA 於 2015 年 11 月發布「監理沙盒[4](Regulatory Sandbox)」報告，作為推動創新方案的一部分，內容包括業者申請監理沙盒之標準、核准測試方式、安全防護措施、業者申請流程與 FCA 辦理方式等。

監理沙盒第一批接受業者申請的期間自 2016 年 5 月 9 日至 7 月 8 日，第二批接受申請期間則自 2016 年 11 月 21 日起至 2017 年 1 月 19 日止。第一批申請進入監理沙盒的業者有 69 家，FCA 經評估後於 2016 年 11 月間公布 24 家符合進入資格，其中 18 家業者即將在監理沙盒中進行測試。

觀察此 18 家業者測試的業務項目(詳附錄 2)，有 9 家係採用區塊鏈或分散式記帳技術，測試業務範圍(公司名稱)包括：以手機介面進行資金移轉(Billon)、跨境零售支付(BitX、Epiphyte)、協助英國勞工退休金部以手機介面轉帳予第三方受益人(Govcoin Limited)、有價證券私募發行及管理(Nivaura)、未上市公司之股權紀錄及移轉管理(Otonomos)、零售支付

[4] 監理沙盒係指建立一個安全的環境，在消費者權益獲得保障的前提下，讓科技新創業者得以在真實環境中測試其新創產品、服務、商業模式及產品散布模式等，而不受既有法規過多的約束。

(SETL)、以網路介面提供身分識別(Tradle)、資金移轉與捐贈予慈善機構(Tramonex)。

前述跨境支付 BitX 與 Epiphyte 公司提出之業務項目，均係藉由比特幣的轉換進行支付[5]。例如 BitX 公司已成功推出 BitX app 提供使用者手機預付卡功能，使用者可將比特幣轉換成當地貨幣並儲值至手機預付卡內，進行近端實體店面消費。

此外，Epiphyte 公司亦研發手機虛擬金融卡功能，虛擬金融卡有卡號及安全碼(Card Verification Value, CVV)，可用在跨境網路交易。例如位在美國的消費者在大陸網站跨境購物時，可以其持有的比特幣按市場匯率轉換為人民幣，並儲值至手機內的虛擬金融卡進行跨境網路交易。使用者可申請特定金額的虛擬金融卡供單次跨境網購支付使用，金額用盡後虛擬卡片即失效，因此不會有被重複使用或盜用問題。

三、英國央行(BoE)

(一) 成立金融科技加速器

英國央行(Bank of England, BoE)成立金融科技加速器(Accelerator)，邀集不同的新創公司合作，共同研究區塊鏈與分散式記帳技術(Distributed Ledger Technology, DLT)[6]可應用在 BoE 之業務領域。2016 年 6 月間 BoE 發布新聞稿表示，已與 PWC 顧問管理公司在 DLT 方面，以虛擬資產進行交易移轉之概念驗證(Proof of Concept, PoC)。

PoC 過程係建立多個可擴充的分散式記帳電腦節點，採用乙太幣協定(Ethereum Protocol)、工作證明(Proof of Work)交易驗證機制，以及智能合約進行測試，以瞭解如何創設虛擬資產(如央行數位貨幣)、

[5] 參考 http://coinjournal.net/epiphyte-offer-transaction-clearing-settlement-blockchain-uk-fis/ 與 https://www.bitx.co/blog/virtual-credit-cards/

[6]「區塊鏈」與「分散式記帳」略有差異，例如比特幣將許多交易納入區塊並加以串連形成區塊鏈，並進行分散式記帳，因此，比特幣是區塊鏈也是 DLT；但 R3 的 Corda 平台已配合金融交易特性，演變為並未以區塊鏈方式進行 DLT。惟為方便解釋，本文仍比照市場慣用語意，將二者視為相同並交互混用。

如何制定參與單位之權限、以及虛擬資產所有權之移轉等。前項 PoC 計畫幫助 BoE 更進一步瞭解 DLT 技術，以及避免電腦系統單點失靈(Single Point of Failure)等問題。

惟 BoE 表示許多新科技仍處發芽階段，系統仍存在相關問題，尚無法達到取代現有運作系統的門檻。總裁 Mark Carney 於 2016 年 6 月間亦表示，DLT 應用在央行發行數位貨幣部分，仍須一段時間(some way off)[7]，因此歡迎各新創公司與 BoE 金融科技加速器合作，並持續探索 DLT 在以下層面尚待努力之領域：

- 交易規模(Scalability)：系統處理容量是否能負荷大規模交易。
- 安全性(Security)：分散式帳本資料如何避免網路攻擊而受損。
- 隱私(Privacy)：如何保護分散式帳本中，交易人的交易隱私。
- 互容性(Interoperability)：現行 BoE 作業系統未來如何與 DLT 相容，例如分散式記帳技術一旦被大量採用時，既有的金融基礎設施須能與 DLT 系統介接。
- 永續性(Sustainability)：相較於傳統中心化系統，同樣交易量下 DLT 較耗費電腦資源且需要更多的資料儲存容量，如何降低負荷仍待克服。

(二) 研究央行發行數位貨幣之議題

為瞭解 DLT 可能被應用在央行發行數位貨幣之潛在可能與其侷限，BoE 透過不同管道進行研究，例如委託倫敦學院大學進行數位貨幣 RSCoin 之交易驗證機制，以及 BoE 同仁發布之同仁研究報告等，內容詳下節介紹。

(三) 未來 RTGS[8]系統與 DLT 系統之互容性

BoE 於 2016 年 9 月間發表諮詢報告[9]，擬更新 RTGS 系統，並徵詢外界意見。現有系統上線已 20 年，BoE 基於以下 5 點考量，擬更新現有系統：

[7] BoE (2016), speech by Mark Carney, "Enabling the Fintech transformation: Revolution, Restoration, or Reformation?", 16 June.

[8] 即時總額清算(Real Time Gross Settlement)。

[9] BoE, "A new RTGS service for the United Kingdom: safeguarding stability, enabling innovation", Sep. 2016

1、 新系統需因應持續演化的金融體系運作架構，例如手機行動支付等。因此，未來的 RTGS 系統會將非銀行的支付服務提供者亦納為直接參加者。當然連接 RTGS 的使用者，均須符合 BoE 對系統運作的強度，以及防止網路攻擊之相關措施。

2、 支付系統使用者想要更簡化、更具彈性的支付通道，例如交易過程須帶入更多的相關訊息，因此新系統將採用符合國際標準的 ISO 20022 訊息格式。

3、 新系統需能與民間創新的支付介面互容與介接，例如分散式記帳技術一旦被大量採用時，新系統須能與該技術互容，訊息格式應能支持該技術並相互溝通。

4、 網路攻擊種類及態樣愈趨多元,須強化新系統的快速復原能力，使系統能持續運作。

5、 新系統之運作需能配合法規及貨幣政策工具面之持續演進。

綜上，BoE 未來新的 RTGS 系統除採用符合國際標準的 ISO20022 訊息格式，在發送付款指令時能帶入更多訊息外，系統亦前瞻性地考量未來能與區塊鏈技術相容，維持系統的可擴充性與相容性。

參、區塊鏈與分散式記帳技術簡介

一、區塊鏈與分散式記帳技術

區塊鏈(Blockchain)係利用數位簽章及加密技術將點對點(Peer-to-Peer, P2P)交易資料記錄至區塊，經過市場參與者驗證區塊有效性後，再將前後區塊以密碼學雜湊(Hash)連結，形成無法更動、可被查閱的分散式帳本(Distributed Ledger)，此種將資料庫分散式存儲在不同電腦節點的技術又稱為分散式記帳技術(DLT)。

傳統上若只有一份帳本，並由中心單位管理、查閱及維護，屬於中心化控管帳本，例如目前金融體系中各家銀行有自己獨立的帳本；若一份帳本分別由不同單位共同管理、查閱及維護，則屬分散式帳本。

比特幣之運作係由 DLT 網路上不同電腦節點，將交易資料收集、驗證並納入區塊保存，且即時更新分散式帳本。如要建立新的區塊則需取得電腦節點多數決之共識或認可，一旦區塊資料被記錄在各個不同電腦節點維護的分散式帳本，將不易被篡改，從而大幅提升資料安全性。

DLT 依能否參與驗證交易並維護帳本資料完整性之權限分類，可概分為非許可制(permissionless)或稱開放式，以及許可制(permissioned)或稱私有式。若由預選信任的特定電腦節點進行交易驗證，則屬許可制 DLT，若任何電腦節點均可驗證交易及更新維護帳本，則屬非許可制 DLT。

2009 年問市的比特幣，其區塊鏈技術即屬於非許可制 DLT，優點包括：可進行點對點(P2P)直接轉帳、可避免電腦單點失靈而造成系統性的風險、交易歷史資料可追蹤及交易成本低等；但缺點則包括使用者匿名致監管不易、支付交易後的確認時間過長(平均約 10 分鐘)，以及價格波動度高等問題。

比特幣在實務應用上，仍面臨許多限制與瓶頸，因此，近期金融市場在 DLT 之創新應用則多朝向許可制方向研究，並演變出不同態樣的 DLT 平台，主要包括：

(一) Ethereum：2015 年 7 月推出的非許可制 DLT 平台，有原生數位貨幣(Ether)，使用者可彈性編寫程式以利不同場景的自動化智能合約執行，交易驗證者可獲得系統自動發給的 Ether 數位貨幣。

(二) Hyperledger：由 IBM 推出的許可制 DLT 平台，可支持公開與非公開交易的驗證機制。

(三) Corda：由 R3 聯盟提出之許可制 DLT 平台，特別的是 Corda 平台為配合金融交易兩造雙方的資料隱私，並未將多筆交易資料包至區塊內，因而不屬於區塊鏈，且只有該筆交易攸關者(交易雙方及主管機關)才有權共享及查閱該筆交易資料。

(四) Ripple：由 Ripple 公司提出並應用在跨境支付領域之許可制 DLT

平台，創立之初即發行 1,000 億單位數位貨幣 XRP。

以共識決機制為例，比特幣及 Ethereum 屬開放式平台，任何電腦節點均可參與交易驗證(俗稱挖礦)，以獲得系統自動提供之數位貨幣報酬。因此，驗證者係相互競爭進行工作證明；至於許可制平台，因係預選信任的電腦節點進行交易驗證，因此，多採用容錯[10]共識機制。以下表列 DLT 平台主要異同：

表 2 許可制與非許可制 DLT

非許可制/開放式 DLT	許可制/私有式 DLT
Bitcoin、Ethereum	Ripple、Hyperledger、Corda

資料來源：ASTRI, "Whitepaper on Distributed Ledger Technology"

表 3 DLT 資料處理結構

區塊鏈	非區塊鏈
Bitcoin、Ethereum、Hyperledger	Ripple、Corda

資料來源：ASTRI, "Whitepaper on Distributed Ledger Technology"

表 4 共識決機制

工作證明 (Proof-based)	容錯共識 (Fault-Tolerant Consensus)
Bitcoin：採用 Sha 256 工作證明 Ethereum:採用 Ethash 工作證明	Hyperledger：支持不同共識機制，包括拜占庭容錯共識 Ripple：拜占庭容錯共識等 Corda：支持不同的共識機制

資料來源：ASTRI, "Whitepaper on Distributed Ledger Technology"

DLT 的應用已從早期像比特幣一樣著重在支付(含跨境)領域的價值交換(Transfer of Value)，已快速擴展至其他應用領域，包括資產有關的產權登記、交易、轉讓；證券與其他金融商品合約的交易執行與交易後

[10] 以拜占庭容錯共識(Byzantine Fault-Tolerant Consensus)機制為例，係指驗證的電腦節點達成多數決投票門檻(例如 3/4)時，即認定交易為真

之結清算；供應鏈(Supply Chain)物流管理；信用狀貿易融資(Trade Finance)；汽車保險(Auto Insurance)及事故自動化處理；再延伸至社會治理領域，如數位身分認證(Digital Identity)、公證、醫療紀錄、電子投票等領域。

依 R3 執行長 Tim Grant 來台簡報資料顯示，DLT 案例從概念驗證測試到正式商轉應用須歷經以下 5 個階段(5P)。因此，可依所公布之測試階段名稱，據以判斷該研究個案所處之階段。

- 概念驗證(Proof of Concept)測試：以少數電腦節點進行模擬交易及測試。
- 原型(Prototype)測試：以模擬資料交易，並與實際作業系統連接測試。
- 領航(Pilot)計畫實作：以實際資料進行交易，並與實際作業系統連接測試。
- 主管機關許可(Permission)：主管機關介入協助與討論，以避免實際應用階段時遇到法規阻礙。
- 實際應用(Production)：進入實際商轉應用階段。

二、國內區塊鏈技術發展概況

(一) 台灣大學區塊鏈中心研發之 Gcoin 系統

國內已有不少單位相繼投入區塊鏈研究，包括工研院、臺灣大學、政治大學、台灣網路認證公司等單位。例如，臺灣大學於 2016 年 3 月間宣布籌設「國立臺灣大學金融科技暨區塊鏈中心」從事區塊鏈的研究並研發 Gcoin，該中心已把 Gcoin 技術底層完全開源、開放，讓有意從事區塊鏈應用的開發者，可以自由發揮創意開發出服務應用。

Gcoin 區塊鏈協議採取「原生儲值單位等同於數位貨幣」的方式，意即 Gcoin 在節點(可以是央行或金融機構等)接受用戶存入現金作為十足擔保，再據以發行數位貨幣在 Gcoin 網路上流通。Gcoin 採取許可制

的區塊鏈架構，每一個電腦節點(Node)都是受法規認許及市場信任的機構。

區塊鏈生態系統可以分成 3 個部分，包括底層技術協議、中層應用程式界面(Application Programming Interface, API)、以及上層服務應用。Gcoin 做的是底層的區塊鏈建設，完成通訊連結與保密、運算的基礎；中層串接應用情境和區塊鏈基礎建設的 API，由該中心其他團隊進行開發；最上層的應用，則仍有待各界共同討論可能之發展領域。

在交易驗證機制方面，Gcoin 將比特幣的工作量證明機制加以改良，採用動態非線性工作量證明機制 (Non-Uniform and Non-Linear Proof of Work)，根據當時的時間點(Timestamp)往回推算 N 個區塊，每一個參與的聯盟成員依照前 N 個區塊中獲選為驗證者的次數，動態調整其在當時挖礦困難度，也就是調整工作量證明的期望大小。此種調整每個聯盟成員獲選為驗證者的困難度機制，可避免獨佔驗證的可能性，以解決比特幣機制中可能發生的 51% 攻擊(51% Attack)問題。

(二) 台灣網路認證公司研發之區塊鏈系統架構

台網公司近期亦積極研發出區塊鏈系統，可配合金融交易屬性採用實名制認證機制、對交易資料屏蔽以保護金融交易隱私，以及不採用工作量證明之共識決機制以避免浪費電腦運算力等特色。台網公司區塊鏈系統可包括以下幾個子系統：

(1) 身分認證系統(Authorization & ID)：負責身分查核、角色分派、權限與責任核准，以及身分識別等工作。

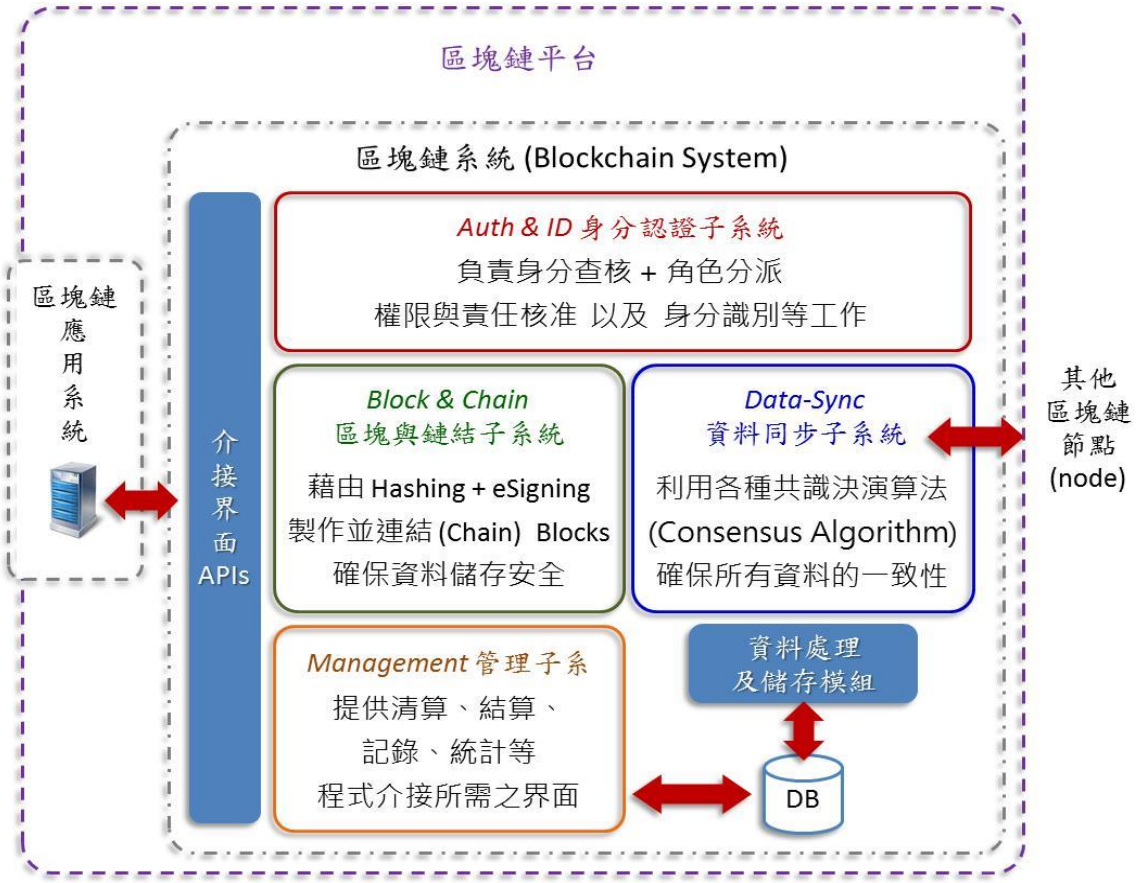
(2) 區塊與鏈結系統(Block & Chain)：負責以密碼學等技術將交易資料製作為區塊，並將所製作之區塊與前一個區塊鏈結起來，以確保資料之安全性及不可更動性。

(3) 資料同步系統(Data-Sync)：因應不同的情境、應用以及生態系，使用不同的共識決演算法(Consensus Algorithm)，將區塊成功的

散佈到其他電腦節點(Node)，並確保所有節點保存之帳本資料的一致性。

(4) 管理系統(Management)：提供整個清算、結算、記錄、統計等管理程式所需之界面，方便其他各項應用程式介接，以產出各項報表並管理各項交易統計數據。

圖 1 區塊鏈系統架構



資料來源：杜宏毅

肆、國外發行數位貨幣之研究近況

目前已有部分國家就分散式記帳技術應用在央行發行數位貨幣之可能性進行研究，包括：英國、加拿大、中國大陸、荷蘭、俄羅斯及日本等。本章分別以央行及非央行為主體所發行之數位貨幣進行說明。

一、以央行為發行主體之數位貨幣研究

2016 年以來已陸續有部分國家探索區塊鏈技術應用在央行發行數貨幣之領域，例如：

- 荷蘭央行 3 月間公布刻正研究央行數位貨幣 DNBCoin[11]。
- 加拿大央行 6 月間進行央行發行數位貨幣(CAD-Coin)之研究，擬運用在金融機構間之結清算交易;11 月間 R3 駐台代表表示，已與加拿大央行合作完成第一階段測試。
- 英國倫敦大學二位學者受 BoE 委託研究，3 月間共同發表央行數位貨幣(RSCoin)運作架構；此外，7 月間 BoE 發布同仁研究報告，揭露央行數位貨幣的運作架構。
- 大陸央行 9 月間在金融期刊發布一系列報導有關發行央行數位貨幣的運作架構，但未揭露細部運作細節，例如交易驗證機制等；11 月間外電報導[12]，大陸央行已對外招募區塊鏈專家。
- 俄羅斯央行 10 月間發布新聞稿，利用乙太幣的底層技術發展央行數位貨幣(Masterchain)，擬應用在銀行之間的交易及結清算，並已與幾家大型銀行進行測試[13]。
- 新加坡 MAS 於 11 月間加入 R3 聯盟，擬與 R3 就央行數位貨幣之發行進行測試與研究[14]。
- 瑞典央行 11 月間發布研究發行央行數位貨幣(ekrona)[15]之資訊，DLT 為被考慮使用的技術之一。
- 日本央行 12 月間發布新聞稿[16]，與歐洲央行(ECB)發起共同研究

---

11 http://www.coindesk.com/dutch-central-bank-preparing-boldest-blockchain-experiment-yet/

12 https://www.cryptocoinsnews.com/china-hiring-blockchain-experts-develop-digital-currency/

13 https://www.cbr.ru/Eng/press/?PrtId=event&id=643&PrintVersion=Y

14 http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/MAS-experimenting-with-Blockchain-Technology.aspx

15 https://www.ft.com/content/0e37795c-ab33-11e6-9cb3-bb8207902122

16 https://www.boj.or.jp/en/announcements/release_2016/rel161207a.htm/

計畫，將探索 DLT 應用在央行數位貨幣及市場基礎設施的可能性，預計 2017 年公布初步研究結果。

Chain.com 執行長 Adam Ludwin 於 2016 年 6 月在 Fed 的一場研討會簡報表示，央行發行區塊鏈基礎的數位貨幣可有二種模式[17]：

- 擔保發行：採「原生儲值單位等同於數位貨幣」概念，以傳統貨幣存放央行帳戶，由央行據以發行 1 比 1 等值央行數位貨幣。
- 無擔保發行：美國貨幣發行無須以外匯存底做貨幣發行之準備，僅基於持有人對美國政府的信任而發行，Ludwin 因此提出第二種數位貨幣發行模式則完全比照現行美國 Fed 發行實體貨幣的作業架構，由 Fed 自源頭即發行數位貨幣，只是由實體貨幣變為數位貨幣。

在選擇何種方式發行數位貨幣較佳時，主要考量在使用者有無信心使用，如以擔保發行方式，使用者瞭解其持有的央行數位貨幣均有銀行提存存款在央行作擔保，能隨時將數位貨幣換回成傳統貨幣，將可增加使用者持有央行數位貨幣的信心。因此，目前採擔保發行模式為主流運作架構，例如：加拿大央行、中國大陸央行、UBS 等。

(一) 加拿大

加拿大央行 2016 年 6 月間發布央行數位貨幣 CAD-Coin 計畫[18]，與 R3 聯盟合作測試，擬將應用在央行與銀行以及銀行間之大額交易結算，10 月間 R3 執行長訪台期間演講表示，加拿大央行委託 R3 完成第一階段測試央行數位貨幣之發行，測試期間曾有 1~2 天連結至央行現有系統，屬於原型測試，未來會再與不同會員機構進行下一階段測試。

雖然加拿大央行及 R3 均未揭露 CAD-Coin 的運作架構，惟從某場研討會與會者拍下之運作架構圖[19]可窺知，加拿大央行係接受銀行

[17] 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

[18] http://www.coindesk.com/bank-canada-demos-blockchain-based-digital-dollar/

[19] http://www.coindesk.com/bank-canada-demos-blockchain-based-digital-dollar/

在央行的存款作為擔保(或稱 100%準備)，再據以發行等值的 CAD-Coin 數位貨幣給銀行，此種運作模式屬於「原生儲值單位等同於數位貨幣」[20]概念。

圖 2 加拿大央行數位貨幣發行架構

資料來源：http://www.coindesk.com/

詳細運作流程如次：

- 擔保(pledge)：銀行將資金存放至央行之集合帳戶(pooled account)作為擔保。
- 產生(Generate)數位貨幣：央行依擔保資金產生數位貨幣 CAD-Coin。
- 央行撥付(Fund)數位貨幣至銀行數位貨幣錢包。
- 數位貨幣移轉(Exchange)：銀行在 CAD-Coin 平台相互移轉數位貨幣。
- 贖回(Redeem)傳統貨幣：銀行以 CAD-Coin 向央行換回傳統貨幣，央行收回 CAD-Coin 並同時將傳統貨幣由集合帳戶撥還給贖回的銀行。
- 註銷(Destroy)央行數位貨幣 CAD-Coin。

[20] Chain.com 執行長 Adam Ludwin 稱此種數位貨幣發行模式為"Title Model"。

(二) 英國

1、 英國央行(BoE)同仁研究報告[21]

2016 年 7 月間 BoE 發布同仁研究報告，揭露央行數位貨幣(Central Bank Digital Currency, CBDC)的運作架構，主要如次：

(1) BoE 以公開市場操作(買斷或 Repo)買進銀行持有之債券作準備（Reserve-backed），並據以發行 CBDC 給銀行[22]。

(2) BoE 發行 CBDC 的金額設定為 GDP 的 30%，該數字係參考主要國家量化寬鬆貨幣政策(Quantitative Easing, QE)規模設定。

(3) 代理機構(Private-sector Agent)如貨幣兌換商等欲將其存款換為 CBDC，須先以存款向銀行買入債券，再由銀行代為以債券與央行承作公開市場操作(Open Market Operations, OMO)，俾使得代理機構可取得 CBDC。此種設計架構，可避免代理機構取得 CBDC 過程中，將資金從銀行抽走，使銀行面臨現金短缺的流動性問題。

2、 BoE 委託倫敦學院大學研究數位貨幣交易驗證機制

2016 年 3 月間倫敦大學二位學者受 BoE 委託，共同發表央行數位貨幣(RSCoin)運作架構[23]報告，內容主要探討數位貨幣的交易驗證機制。

該報告經由 30 個電腦節點模擬交易，每秒可處理約 2,000 筆交易[24]，並認為 RSCoin 的交易驗證機制可有效避免重複支付(Double Spending)等問題。

RSCoin 為英格蘭銀行中心化管理與發行之 DLT 加密貨幣，應用

[21] BoE (2016), Staff working paper No. 605, “The macroeconomics of central bank issued digital currencies”, July

[22] 中國大陸及加拿大央行數位貨幣發行設計架構係以收取銀行之存款作準備，並據以發行 1:1 等值的數位貨幣予銀行。

[23] 本報告內容著重在整體運作架構、交易驗證(含避免重複支付)等議題，而非著重在如何產生數位貨幣，蓋因央行數位貨幣的產生運作方式簡單，多係以特定擔保帳戶(Escrow)內的法償貨幣作擔保，並據以發行等值的央行數位貨幣，即可完成。

[24] 比特幣每秒約僅能處理 7 筆交易，臺大區塊鏈團隊之 Gcoin 每秒約可處理 300 筆交易，RSCoin 每秒可處理 2,000 筆交易，而 Visa 的中心化系統每秒約可處理 2,000~7,000 筆交易。

密碼學使其具有防篡改和防偽造的特性，系統金鑰由央行控制，並由央行選擇聯盟機構(如銀行)參與交易處理、驗證、監控數位貨幣避免被重複支付(Double Spending)等機制，以及共同進行帳簿維護等。

以下介紹 RSCoin 運作架構及特點：

（1）央行中心化管控 RSCoin 發行

採分散式記帳技術，由央行透過金鑰（PKI）技術授權交易驗證單位(Mintettes)驗證數位貨幣移轉交易。Mintette 主要功能在於驗證交易的真實性（交易人數位簽章是否正確），以及確認交易轉出者無重複支付等。

（2）交易驗證過程採二層級單位運作架構

- 第一層為 Mintette 與交易人之運作關係

  Mintette 負責收集 RSCoin 交易及驗證，並且每隔一段時間（Epoch）將交易納入底層區塊（Lower-level Block）並進行維護與更新。

  值得注意的是底層區塊僅係 Mintette 維護之帳本，不對一般大眾公開，亦不屬於真正的區塊鏈。

- 第二層為央行與 Mintette 之運作關係

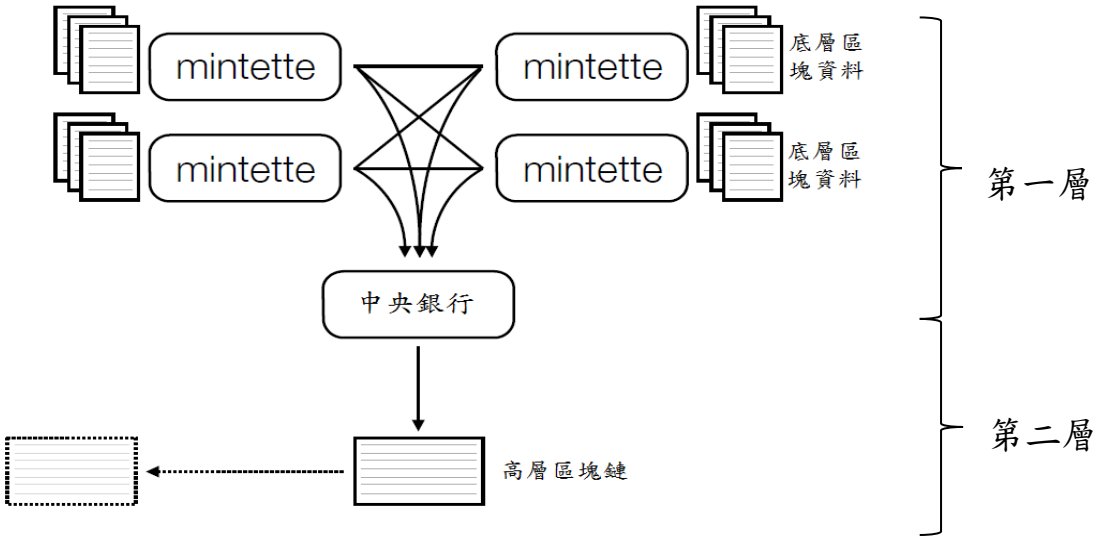
  央行為數位貨幣 RSCoin 的中心管理單位，控制數位貨幣之發行以及管理 Mintette。央行每隔一段時間（Period[25]）會將 Mintettes 傳送上來之底層區塊納入至高層區塊（Higher-level Block）。

  每個底層交易區塊須包含央行授予 Mintette 的公鑰數位簽章方屬有效區塊，央行比對 Mintettes 底層區塊紀錄正確性後才納入高層區塊鏈，並具有不可更動性。

  交易人隨時可檢視央行對外公布的高層區塊鏈資料，且可依 output Mintettes 回覆給交易人的訊息相互核實。

[25] 視處理交易速度、交易量多寡而定，Epoch 可設定為數秒或數分鐘，而 Period 則可設定為數分鐘、數小時甚至日終一次。

圖 3　RSCoin 二層級單位運作架構



資料來源：Centrally Banked Cryptocurrencies, 2016

（3）底(第一)層區塊鏈資料採二階段(Two-Phase Commit, 2PC)驗證

在釐清二階段交易驗證前，有必要說明 Input 及 Output 之概念，基本上一筆轉帳支付交易可分為 Input 及 Output，Input 交易記錄資金轉出者錢包地址及金額，Output 交易記錄資金接收者地址及金額，以及轉出者所剩之金額。

例如甲的錢包地址原有 10 單位 RSCoin，若甲轉出 6 單位 RSCoin 給乙並剩下 4 單位 RSCoin，則此筆轉帳交易之 Input 為甲地址內含 10 單位 RSCoin；Output 則有二個，一個為乙的地址內含6單位RSCoin，另一個為系統自動為甲產生的新地址[26]內含剩下的 4 單位 RSCoin。

若甲嗣後再轉出 1 單位 RSCoin 給丙，則此筆交易的 Input 為甲地址內含 4 單位 RSCoin，而 Output 則有二個，一為丙地址內含 1 單位 RSCoin，另一個 Output 為系統自動再為甲產生一個新地址內含剩下之 3 單位 RSCoin。

此種每次交易後變更錢包地址的設定有利於查驗該筆交易是否有重複支付情形。例如， Mintette 檢查該筆交易 Output 地

[26] 此種轉出後產生新地址的作法與比特幣相同，詳 Narayanan, Bonneau, Felton, Miller, Goldfeder, online course of Princeton University (Feb. 2016),「Bitcoin and Cryptocurrency Technologies」, p.77.

址是否曾在其他交易的 Input 地址名單中出現過，若未出現表示該錢包地址尚未支付過，而無重複支付問題；若曾出現在先前的其他交易 Input 名單中，則表示有重複支付情況，Mintette 將會否決此筆交易。

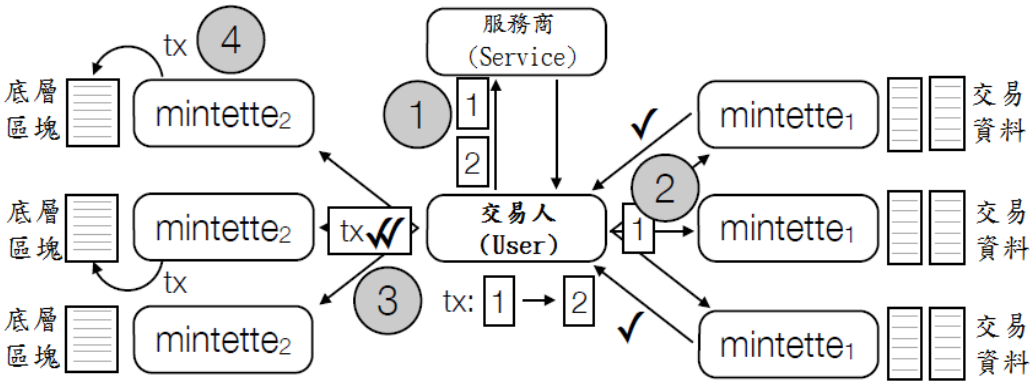
以下說明 RSCoin 二階段交易驗證：

- 第一階段

Mintettes 分為二組，一組擁有並維護更新 Input 交易資料(圖右 $Mintette_1$)，另一組負責 Output 交易資料維護及更新(圖左 $Mintette_2$)。

步驟①：交易人 1 擬轉出資金予交易人 2，先經由中心化系統服務商(Service)得知負責維護 Input 及 Output 交易資料之 Mintettes。

圖 4　RSCoin 二階段交易驗證流程



資料來源：Centrally Banked Cryptocurrencies, 2016

步驟②：交易人將轉帳交易訊息發送予擁有 Input 交易名單的 Mintettes 群組進行 Input 交易驗證，Mintette 接著查驗此筆轉出地址是否曾經出現在以往的 Input 交易名單中，如未出現即表示該轉出地址無重複支付，並回傳交易人「核准(approval)」(圖示為✓)之投票(vote)訊息；但如該筆轉出地址曾出現在 Input 名單中則為

重複支付，將不會被 Mintettes 回傳核准訊息。

交易資料驗證無誤後，Mintettes 會將交易資料納入其負責維護及更新的 Input 交易資料名單。

- 第二階段

步驟③：交易人收集到 Mintette 回傳的多數決核准訊息後，連同此筆交易資訊一併傳送給另一組擁有 Output 交易名單的 Mintettes 進行驗證。

步驟④：第二組擁有 Output 交易名單的 Mintettes 驗證無誤後[27]，即將此筆交易的資金接收者 Output 納入其負責維護的底層區塊，並更新其「尚未支付的 Output 名單(unspent transaction output, utxo) 」，接著回傳訊息予交易人，告知該交易將被傳送至央行的高層區塊鏈。

（4）手續費及交易驗證機制

RSCoin 研究者建議由銀行擔任 Mintette 角色較佳，交易驗證成功可獲取手續費收入；交易驗證可採權益證明(Proof of Stake)的投票共識決機制，並由 Mintette 提存資金至央行的擔保帳戶(Escrow)，Mintette 收集交易進行驗證的金額不得超過其提存之擔保資金。此種設計架構可在 Mintette 未做好交易驗證工作而發生重複支付時，由 Mintette 負擔該筆交易損失，並由央行自 Mintette 帳戶扣除該筆金額。

（5）RSCoin 交易處理效能

前揭研究結果顯示RSCoin每秒約可處理逾2,000筆交易，對區塊鏈的交易處理容量(Scalability)而言，似有明顯提升，RSCoin 研究者表示，未來仍將持續與 BoE 討論數位貨幣如何落實至實際金融環境。

[27] Output Mintettes 驗證之主要項目，包括檢查核准的投票是否達多數決、數位簽章是否正確、此筆移轉交易是否先前未出現過，如一切正確，Mintette 會將此筆交易的 Output 納入其維護的 utxo (unspent transaction output)名單中。

(三) 瑞士聯合銀行

此次參訪瑞士聯合銀行(United Bank of Switzerland, UBS)位在倫敦的區塊鏈研究中心，其研究中的 Utility Settlement Coin (USC)運作架構，係由 UBS 將資金存放在央行帳戶作為準備，並由央行發行等值的數位貨幣(USC)，以作為金融機構間移轉及結清算使用。因此，USC 運作架構與加拿大央行研究中的數位貨幣 CAD-Coin 相似。

UBS 表示該計畫在孵化階段時(Incubation phase, 2015.6~2016.3)，完成運作架構設計，並已與區塊鏈技術提供公司(Clearmatics)完成初步的內部概念驗證(PoC)，利用 5 個電腦節點測試，底層技術修改自 Ethereum，以配合 USC 的許可制分散式記帳。

由於 USC 獲得其他機構及央行的認同，因此進入加速階段(Acceleration phase, 2016.8~2017.1)，由 UBS 與德意志、紐約梅隆、Santander 等銀行，以及 Clearmatics 公司共同成立 USC 聯盟，持續進行測試，並邀請 BoE 參與提供意見。

UBS 表示除與 BoE 接洽外，也與國外央行接觸傳達 USC 的運作概念，甚至認為此概念若能提報至 20 國集團(G20)獲准，則可促使主要國家央行都採行數位貨幣發行架構，屆時進行跨境貨幣移轉支付將可即時完成。

(四) 中國大陸

中國大陸於 2016 年 9 月「中國金融」期刊發表一系列發行央行數位貨幣之文章，發行總體框架為中央銀行與商業銀行的二元體系，中央銀行負責數位貨幣的發行與驗證監測，商業銀行從中央銀行申請到數位貨幣後，直接面向社會，負責提供數位貨幣流通服務與應用生態體系構建服務。

大陸央行數位貨幣體系的核心要素為一種數位貨幣、兩個庫、三個中心。具體而言，該體系包括以下幾項主要構成要素。

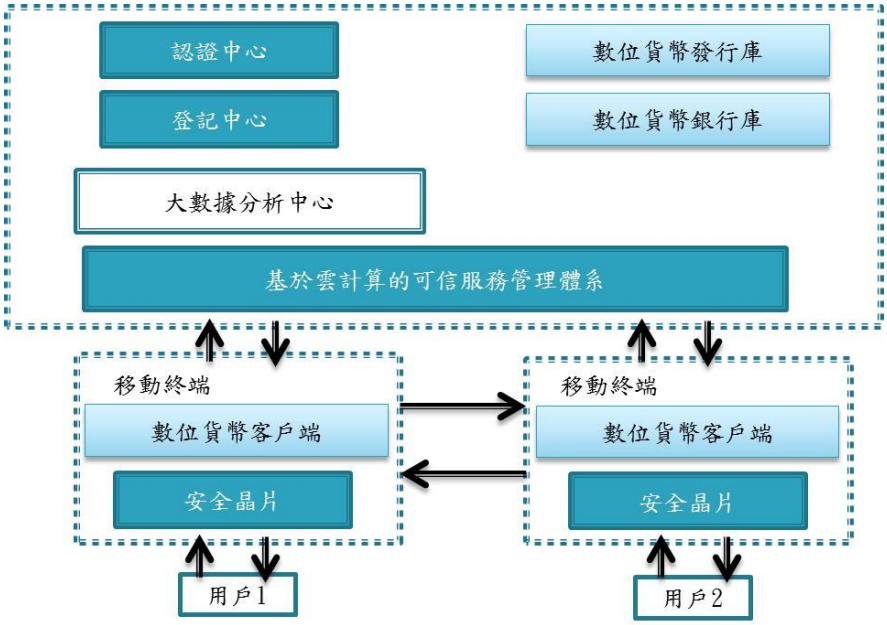
1、 一種央行數位貨幣：

央行數位貨幣私有雲用於支撐央行數位貨幣運行的底層基礎設施，由央行擔保並簽名發行的代表具體金額的加密數字串。

2、 兩個庫

- 數位貨幣發行庫：人民銀行在央行數位貨幣私有雲上存放央行數位貨幣發行的資料庫。
- 數位貨幣商業銀行庫：商業銀行存放央行數位貨幣的資料庫，可以在本地也可以在央行數位貨幣私有雲上。數位貨幣數位錢包：指在流通市場上個人或單位使用者使用央行數位貨幣的用戶端，此錢包可以基於硬體也可以基於軟體。

圖 5 中國大陸央行數位貨幣運作架構圖



資料來源：「中國金融」2016 年第 17 期

3、 三個中心

- 認證中心：央行對央行數位貨幣機構及使用者身分資訊進行集中管理，它是系統安全的基礎元件，也是可控匿名設計的重要環節。
- 登記中心：記錄央行數位貨幣及對應使用者身分，完成權屬登記；記錄流水，完成央行數位貨幣產生、流通、清點核對及註銷過程登記。

- 大數據分析中心：進行反洗錢、支付行為分析、監管調控指標分析等。

4、 數位貨幣的發行與流通

在央行數位貨幣體系中，有央行的數位貨幣發行庫、商業銀行的數位貨幣銀行庫和使用者端(如手機)的數字錢包，三者關係如下：

- 根據數位貨幣發行總量，央行統一生成數位貨幣，存放在央行發行庫中。
- 根據商業銀行數位貨幣的需求申請，將數位貨幣發送到商業銀行存放數位貨幣的資料庫，即數位貨幣從發行庫到銀行庫。
- 使用者向商業銀行申請提取數位貨幣時，數位貨幣從銀行庫到流通環節，進入使用者用戶端的存儲媒介（如手機），即從銀行庫到使用者的數位錢包。

5、 設計要點

- 遵循傳統貨幣的管理思路，發行和回籠基於現行中央銀行與商業銀行的二元體系來完成。
- 數位貨幣本身的設計，運用密碼學理論，增強安全性。
- 貨幣的產生、流通、清點核對及註銷過程登記，參考區塊鏈技術，建立集中及分佈相對均衡的簿記登記中心。
- 運用可信計算技術和安全晶片技術來保證數位貨幣點對點交易的安全性。
- 運用大數據分析技術，進行加值分析，可滿足反洗錢等業務需求。
- 數位貨幣本身的設計應力求簡明高效，數位貨幣之上的商業應用盡可能交給市場來做，同時把技術標準與應用規範做好。
- 構建由央行、商業銀行、協力廠商機構、消費者參與的完整的數位貨幣生態體系，保證數位貨幣的發行、流通、回收之生命週期可控。

二、非以央行為發行主體之案例

依「原生儲值單位等同於數位貨幣」概念，發行主體在接受客戶(個人或公司)存入資金在指定之擔保專戶(Escrow Account)後，即以收受之資金作十足擔保，並據以連結發行等值[28]的數位貨幣(或稱token)予客戶，客戶可逕將數位貨幣進行 P2P 支付，以節省交易成本及時間。

國外應用案例，包括跨境支付公司 Ripple、Tether，以及試驗階段的日本瑞穗銀行與東京三菱銀行等。以下介紹 Tether 公司運作方式，並就有限之資料來源概述前揭日本銀行之測試情形。

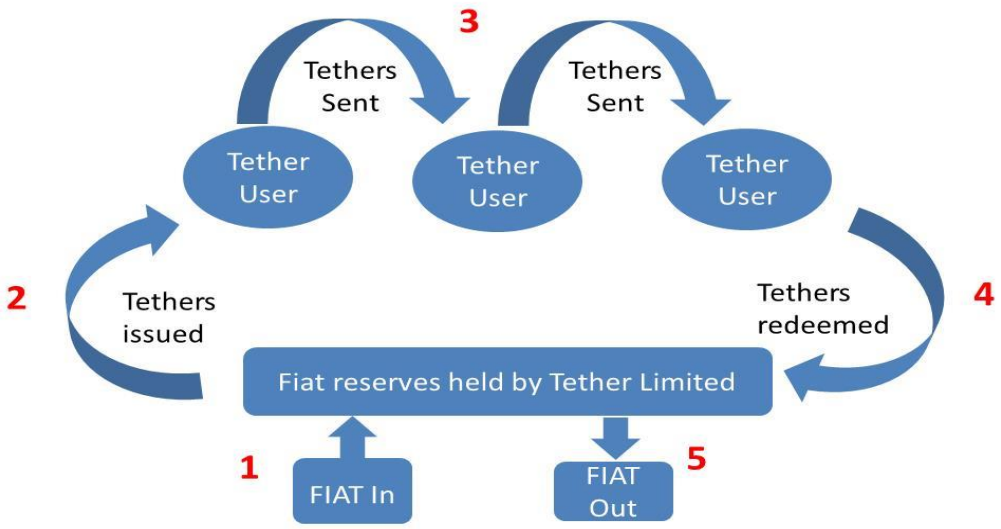
(一) Tether 公司

Tether 為註冊在香港並已商轉之區塊鏈應用公司，Tether 公司收受客戶存入之法償貨幣作準備(reserve)，再據以擔保發行等值的 Tether 數位貨幣，以利其客戶進行後續的 P2P 移轉支付，至於法償貨幣與 Tether 數位貨幣的兌換比率則設定為 1 比 1。Tether 公司 2016 年 3 月間在國內金融研訓院舉辦之講座表示，該公司支持發行美元、歐元、英鎊、日圓、港幣及加拿大幣等數位貨幣。

Tether 公司係採用 3 層式的運作架構，以比特幣區塊鏈作為底層技術；中間層處理 Tether 數位貨幣相關事宜，利用 Omni 內建的比特幣區塊鏈共識決系統，處理 Tether 數位貨幣之發行、交易、流通、錢包儲存等；上層則處理法償貨幣及公司營運事宜，包括收受客戶法償貨幣、進行信託保管，以及稽核 Tether 數位貨幣發行餘額與收受法償貨幣(Proof of Reserves)是否一致等業務。

[28] 為避免發行主體浮濫發行數位貨幣(例如:向客戶收取 100 元作擔保，但卻發行 200 元數位貨幣給客戶)，須有查核制度，確保銀行收取的擔保專戶資金與其發行的數位貨幣金額一致。

圖 6　tether 數位貨幣運作流程



資料來源：Tether 白皮書

以下說明 Tether 數位貨幣(以美元為例)的運作流程：

- 步驟 1：客戶存入法償貨幣(Fiat)至 Tether 公司開立在信託保管銀行的帳戶[29]。
- 步驟 2：Tether 依區塊鏈協定據以產生等值的 tether 數位貨幣，並記(存入)客戶在 Tether 網站開立的帳戶。例如，客戶存入法償貨幣 USD10,000，就會產生對應的 10,000 TetherUSD。
- 步驟 3：客戶以前揭 TetherUSD 在比特幣基礎的平台進行 P2P 支付(含跨境)移轉；一旦 TetherUSD 的流通餘額夠多時，客戶亦可經由與 Tether 公司合作的比特幣交易平台購入 tether 數位貨幣。
- 步驟 4：客戶回存 Tether 數位貨幣至 Tether 公司的錢包地址，並申請兌回法償貨幣。
- 步驟 5：Tether 公司註銷 Tether 數位貨幣，並將法償貨幣移轉至客戶的銀行帳戶。

2013 年 Tether 公司在香港註冊，但為服務美國客戶，Tether 亦向美國財政部所屬的金融犯罪防範網路(Financial Crimes Enforcement

[29] Tether 白皮書揭露其收受的法償貨幣係存放在信託保管銀行，包括二家台灣的境外銀行帳戶，分別為國泰世華(Cathay)銀行及華泰(Hwatai)銀行。

Network of the U.S. Department of the Treasury)註冊為貨幣服務事業(Money Services Business)，該公司宣稱遵循美國及香港有關反洗錢及反恐怖組織活動融資之相關規範。

然而，因 Tether 僅是一般在香港註冊的公司，所收受的法償貨幣係存放在往來的信託保管銀行，客戶與其往來需承擔 Tether 公司及信託保管銀行的信用風險。

(二) 日本瑞穗銀行及東京三菱 UFJ 銀行

日本瑞穗(Mizuho)銀行於 2016 年 12 月間表示，已採用 IBM 的 Hyperledge 技術，完成測試瑞穗銀行數位貨幣(Mizuho digital currency)之發行，數位貨幣與法償貨幣為 1 比 1 兌換關係[30]；另外，東京三菱銀行亦已依類似架構，完成測試其數位貨幣 UFJ coin 之發行，並允許民眾可在 ATM 進行 UFJ coin 與法償貨幣之申領與兌回。

伍、心得與建議

一、心得

英國對 Fintech 的推廣，除 FCA 於 2014 年 10 月發起創新方案(Project Innovate)，由內部專家組成創新中心(Innovation Hub)，就業者提出之新產品或新商業模式提供法令遵循意見，並使 FCA 得配合新科技而進行相關法令之改變外，FCA 亦於 2015 年 11 月發布「監理沙盒報告書」，作為創新方案的一部分，內容包括業者申請監理盒之標準、核准測試之方式、安全防護措施，以及業者申請與 FCA 辦理流程等更具體的作為。FCA 已於 2016 年 11 月間公布進入監理沙盒的新創公司名單，已公布的 18 家業者名單中，有 9 家與分散式記帳技術(DLT)或區塊鏈有關。

在 BoE 方面則是成立金融科技加速器，目的在與新創公司合作，以便深入研究 DLT 可應用在 BoE 的業務領域；此外，BoE 除委託倫敦學院大學二位學者研究 RSCoin 的運作及交易驗證機制外，另亦與 PWC 管理

[30] https://www.cryptocoinsnews.com/japanese-mizuho-tests-digital-currency/

顧問公司在DLT方面,以虛擬資產進行不同所有人交易移轉之概念驗證，以瞭解如何創設虛擬資產(如央行數位貨幣)、如何制定參與單位之權限、以及虛擬資產所有權之移權等。

在國內部分，為因應 FinTech 之興起，本行已採行以下因應措施：

- 2015 年底成立跨局處室「數位金融研究小組」,持續研究 DLT 發展近況與趨勢。
- 2016 年 6 月數位金融研究小組完成「區塊鏈技術與運用及對金融業之影響」內部報告。
- 2016 年 9 月督促財金公司成立「金融區塊鏈研究暨應用發展委員會」,邀集銀行成為會員，並就企金及消金業務分別進行應用案例之測試。
- 2016 年底與票據交換所合作委外研究，就 DLT 應用在跨行轉帳結清算與拆款交易之應用案例進行概念驗證。

未來一旦央行數位貨幣真正推出，任何交易雙方(包括遠端及近端支付)移轉央行數位貨幣，就會如同支付現金一樣，不涉及後續跨行轉帳的結、清算問題，將弱化中間結算機構(如財金公司、票交所、聯合信用卡中心等)之功能；此外，若民眾不再使用信用卡，轉而使用含有央行數位貨幣的手機載具進行支付,那麼將再衝擊到銀行發卡業務及既有的電子支付生態。

由於影響層面廣大，各國央行在考慮數位貨幣之發行時，不僅考量 DLT 是否穩定成熟外，尚須對民眾使用央行數位貨幣之接受度及需求、對國內金融支付生態、金融穩定及貨幣政策的影響進行評估，以便決定是否發行數位貨幣。

二、 建議

DLT 仍處發芽階段，在技術、作業、營運模式及法規面仍存在待解

決的問題，尚無法被廣泛而大量地採用[31]，然因其有不容忽視的潛力可能翻轉金融市場，近來已陸續有部分國家陸續探索 DLT 應用在央行發行數位貨幣之領域，包括：荷蘭、英國、加拿大、中國大陸、俄羅斯、新加坡、瑞典及日本等。

BoE 總裁 Mark Carney 於 2016 年 6 月間表示，欲將 DLT 應用在央行發行數位貨幣上仍須一段時間，因此歡迎各新創公司與 BoE 金融科技加速器合作，持續探索 DLT 尚待努力之領域，例如：系統處理交易規模(Scalability)的問題、分散式帳本資料如何不受到網路攻擊而受損的安全性(Security)問題，以及如何保護分散式帳本資料中交易人的隱私(Privacy)問題等。

考量國際間愈來愈多的央行加入數位貨幣發行的研究領域，爰提出以下建議：

- 持續關注 DLT 在金融領域之研究進展，瞭解國際發展趨勢，俾利本行相關業務之推展。
- 就涉及央行之相關業務(例如：發行數位貨幣)委外研究，期以透過做中學方式瞭解 DLT 的應用潛力與侷限性。尤其是各個 DLT 底層技術(如 Gcoin、IBM Hyperledger 等)運作方式不同，如有不同的委外研究案例，則宜採用不同底層技術進行測試，方能比較彼此優缺點，以利日後選定作為正式商轉案例之底層技術。
- 評估是否加入國際或國內區塊鏈聯盟，以利相互交流有關訊息。

[31] Javier Sebastian Cermeno, BBVA Working Paper (2016), “Blockchain in Financial Services: Regulatory Landscape and Future Challenges for its Commercial Application”, December.

參考資料

一、 中文部分

1. 中央銀行內部研究報告,「區塊鏈技術與運用及對金融業之影響」,2016 年 6 月。
2. 中國法定數位貨幣原型構想,「中國金融」,2016 年第 17 期。
3. 杜宏毅,「如何選擇一個適合應用的區塊鏈平台」,2016 年 10 月 26 日。

二、 英文部分

1. 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
2. ASTRI (2016), "Whitepaper on Distributed Ledger Technology", November, Commissioned by HKMA.
3. BoE (2016), "A new RTGS service for the United Kingdom: safeguarding stability, enabling innovation".
4. BoE (2016), "FinTech Accelerator Proof of Concept-Distributed Ledger Technology".
5. BoE (2016), Speech given by Andrew Hauser, Executive Director, "Building the market infrastructure of tomorrow: CREST, RTGS and the Bank of England, 20 years on".
6. BoE(2016), "Enabling the Fintech transformation: Revolution, Restoration, or Reformation?", 17 June.
7. BoE(2016), "Fintech: Opportunities for all?", 8 September.
8. BoE (2016), "A new RTGS service for the United Kingdom: safeguarding stability, enabling innovation".
9. BoE (2016), "FinTech Accelerator Proof of Concept-Distributed Ledger Technology".

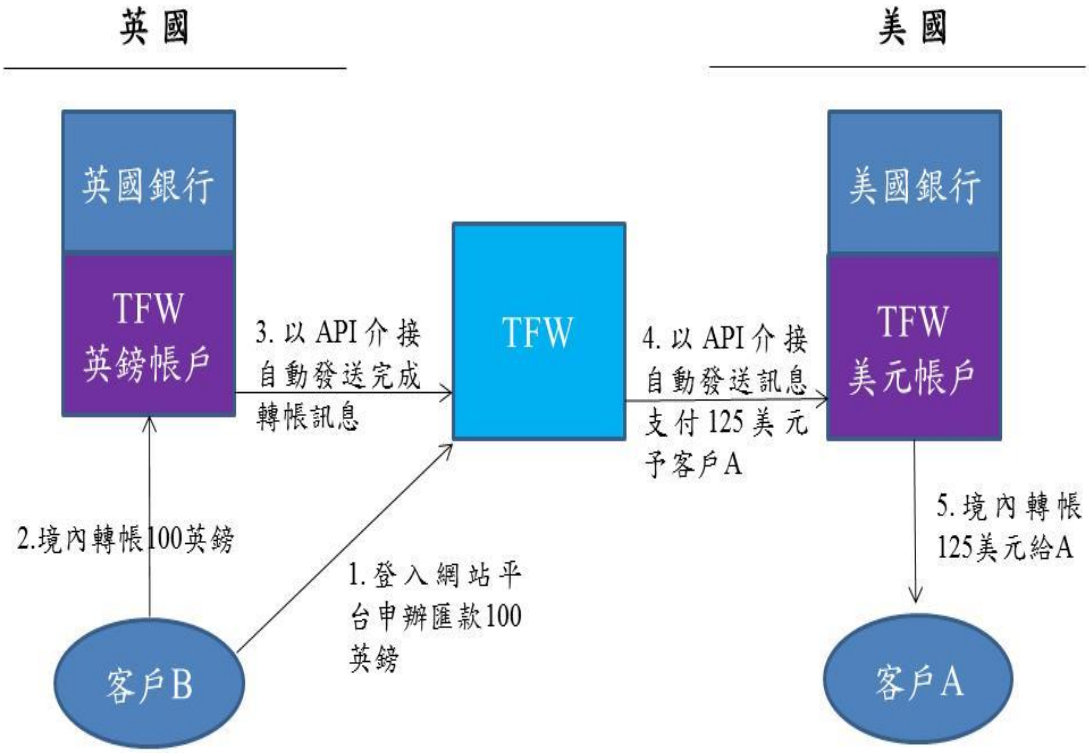
10. BoE (2016), Speech given by Andrew Hauser, Executive Director, “Building the market infrastructure of tomorrow: CREST, RTGS and the Bank of England, 20 years on”.
11. Cryptocoinsnews (2016), BoE RSCoin https://www.cryptocoinsnews.com/englands-central-bank-seeks-bitcoin-clone-in-rscoin/.
12. Cryptocoinsnews (2016), “BoE RSCoin: A Hybrid Digital Currency To Improve Global Trade”.
13. George Danezis & Sarah Meiklejohn (2016), “Centrally Banked Cryptocurrencies”.
14. Deloitte (2015), “State-Sponsored Cryptocurrency”.
15. Gcoin white paper (2016)，https://github.com/OpenNetworking/gcoin-community/wiki/Gcoin-white-paper-Chinese
16. Geroge Danezis & Sarah Meiklejohn (2016), “Centrally Banked Cryptocurrencies”, University College London.
17. Javier Sebastian Cermeno, BBVA Working Paper (2016), “Blockchain in Financial Services: Regulatory Landscape and Future Challenges for its Commercial Application”, December.
18. Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn (2016), “Corda: An Introduction”, August.
19. Ripple (2014), “The Ripple Protocol: A Deep Dive for Finance Professionals”, November.
20. Ripple (2015). “The Ripple Ledger Consensus Process”, February.
21. Ripple (2016), “The Cost-Cutting Case for Banks - The ROI of Using Ripple and XRP for Global Interbank Settlements”, February.
22. Tether White Paper (2016), “Tether: Fiat currencies on the Bitcoin

Blockchain".

23. WEF (2016), "The Future of Financial Infrastructure-An ambitious look at how blockchain can reshape financial services".

附錄 1

英國新創公司 Transferwise 跨境匯款流程



- 假設英國客戶B匯款(付100英鎊)予美國客戶A(收125美元)，B登入至TFW網站並將英鎊轉帳至TFW在英國銀行開立之英鎊帳戶； TFW收到B的匯款指令及款項後，透過API與美國合作銀行的介接，可自動發送訊息請美國合作銀行將TFW帳戶內的美元撥付至A所屬之其他美國境內銀行帳戶。
- 當TFW銀行(美元)帳戶餘額接近不足以支應客戶的付款指令時，TFW才藉由傳統通匯銀行模式，跨國匯款至TFW(美元)帳戶補足帳戶內資金。

附錄 2

英國FCA核准第一批進入監理沙盒之公司

序號	公司	業務內容
1	Billon	An e-money platform based on distributed ledger technology that facilitates the secure transfer and holding of funds using a phone based app.
2	BitX	A cross-border money transfer service powered by digital currencies / blockchain technology.
3	Blink Innovation Limited	An insurance product with an automated claims process, which allows travellers to instantly book a new ticket on their mobile device in the event of a flight cancellation.
4	Bud	An online platform and app which allows users to manage their financial products, with personalised insights, on a single dashboard. Bud's marketplace introduces relevant services which users can interact with through API integrations.
5	Citizens Advice	A semi-automated advice tool which allows debt advisers and clients to compare the key features of available debt solutions.
6	Epiphyte	A payments service provider that aims to provide cross-border payments using blockchain technology.
7	Govcoin Limited	A technology provider that has partnered with the Department for Work and Pensions (DWP) to determine the feasibility of making emergency payments using means other than cash or the Faster Payments Scheme. The payments platform will use blockchain to allow the DWP to credit value to a mobile device to transfer the value directly to a third party.
8	HSBC	An app developed in partnership with Pariti Technologies, a FinTech start-up, to help customers better manage their finances.
9	Issufy	A web-based software platform that streamlines the overall Initial Public Offering (IPO) distribution process for investors, issuing companies and their advisors.
10	Lloyds	An approach that aims to improve the experience for

	Banking Group	branch customers which is aligned with the online and over the phone experience.
11	Nextday Property Limited	An internet-based property company that will provide an interest free loan for a guaranteed amount to customers if they are unable to sell their property within 90 days.
12	Nivaura	A platform that uses automation and blockchain for issuance and lifecycle management of private placement securities.
13	Otonomos	A platform that represents private companies' shares electronically on the blockchain, enabling them to manage shareholdings, conduct bookbuilding online and facilitate transfers.
14	Oval	An app which helps users to build up savings by putting aside small amounts of money. These savings can then be used to pay off existing loans early. Oval will be working with Oakam, a consumer credit firm, and a number of their customers during the test period.
15	SETL	A smart-card enabled retail payment system based on their OpenCSD distributed ledger.
16	Tradle	An app and web-based service that creates personal or commercial identity and verifiable documents on a distributed ledger. In partnership with Aviva they will provide a system for automated customer authentication.
17	Tramonex	An e-money platform based on distributed ledger technology that facilitates the use of "smart contracts" to transfer donations to a charity.
18	Swave	A micro savings app that provides an across-account view; enables a round-up service every time a user spends money and calculates an affordable savings amount based on the user's spending behaviour.

資料來源：FCA