出國報告(出國類別：開會)

參加 SEACEN 研訓中心
「加密通貨與央行業務政策高峰會」
報告

服務機關：中央銀行

姓名職稱：吳桂華科長

派赴國家/地區：馬來西亞/吉隆坡

出國期間：107.5.2~107.5.5

報告日期：107.7.31

目錄

壹、前言

本次參加 SEACEN 研訓中心於馬來西亞吉隆坡舉行之「加密通貨與央行業務政策高峰會」，為期 1.5 天，自 5 月 3 日下午至 5 月 4 日。5 月 3 日為各國央行代表與講者閉門會議，5 月 4 日則對外開放大眾參加。

會議安排來自國際清算銀行(BIS)、歐洲央行(ECB)、國際貨幣基金會(IMF)、加拿大央行、瑞典央行，以及 SEACEN 研究部門主管等 10 餘位講者進行簡報；在閉門會議部分，共計 13 國(包括馬來西亞、南韓、泰國、印尼、印度、菲律賓等)與會央行代表合計 74 位出席，其中地主國馬來西亞央行(BNM)出席人數 40 餘位。

BIS 指出近年各國央行積極研究央行數位通貨(Central Bank Digital Currency, CBDC)，主因 1、科技創新帶來發行數位通貨新構想；2、新對手想加入支付及金融中介服務，與現有對手競爭；3、部分國家現金使用量下降；4、私部門加密通貨引起廣泛注意。例如，瑞典央行講者表示，近年來現金需求下降，因而促使該行思考是否需發行 CBDC。該國現金使用量下降原因包括：1、民眾使用卡式支付之費率降低；2、民眾使用行動支付(Swish)綁定銀行帳戶，進行支付與轉帳比率提高；3、2017 年瑞典部分鈔券改版，民眾繳回舊鈔過程不便，又降低民眾持有鈔券之動機[1]。

藉由參加本次會議，除與部分講者與央行與會者討論及交流重要訊息外，亦瞭解國際間對於利用區塊鏈或分散式帳本技術(distributed ledger technology, DLT)在央行相關業務之研究情形。例如，發行 CBDC 面臨之問題與挑戰，以及對私部門加密通貨(如比特幣)交易與首次代幣發行(Initial Coin Offering, ICO)之監管進行分享。

本報告除第壹章前言外，第貳章簡介加密通貨與區塊鏈技術，第參章說明 DLT 應用在發行央行數位通貨之研究，第肆章介紹對私部門加密通貨交易之監管，最後提出心得與建議。

[1] 會議期間洽詢瑞典央行講者獲告，該行於 2017 年 6 月底廢止使用 100 及 500 克朗舊鈔，民眾在 2018 年 6 月底期限前可將舊鈔回存銀行或郵寄回央行。回收舊鈔過程中，民眾除須填報表格說明何以舊鈔在法償期間未使用原因外，另須負擔 100 克朗費用。此外，民眾舊鈔回存銀行時，常有銀行拒收。此等原因均會導致民眾持有鈔券動機下降。

貳、加密[2](虛擬)通貨與區塊鏈技術

一、加密通貨簡介

(一) 比特幣開啟加密通貨之路

2009 年虛擬通貨比特幣問世後，其應用之區塊鏈技術受到各界矚目，比特幣交易及驗證過程應用密碼學技術，因此也稱為加密通貨(cryptocurrency)。比特幣之運作係由全球各電腦節點(node)[3]競相收集各筆比特幣交易，包入各自製作之區塊，再以數位簽章及密碼學等技術，對區塊內交易加以驗證[4]，並以各自製作之區塊資訊[5]解答系統設定之密碼學謎題(puzzle)[6]，最先成功解謎者可將其製作之區塊與前一區塊鏈結，形成幾乎無法被竄改之區塊鏈帳本。解謎過程需耗費電腦運算力，因此成功解謎的節點可獲得系統發給之比特幣作為報酬，使比特幣供給量增加。

(二) 以太幣為首次代幣發行先驅

相對於比特幣發行量從零開始，由礦工挖礦所獲報酬而逐步增加，以太幣於 2014 年推出時，係以首次代幣發行(ICO)方式發行 7,200 萬單位以太幣，並收取比特幣。嗣後，再透過給付礦工以太幣作為其驗證交易之報酬，使以太幣供給量逐步增加。

二、去中心化運作須搭配共識演算機制

虛擬通貨之主要特色，除採用加密技術外，其交易處理有別於現行金融交易需透過中心化單位處理交易與記帳，而採用 DLT 之去中心化運作

---

[2] 虛擬通貨係採用區塊鏈技術對交易進行分散式記帳，各報告有不同之稱法，部分稱為加密通貨或數位通貨，因此，本文將虛擬通貨、加密通貨、數位通貨視為相同。至於本文後續提到之電子貨幣，則非採用區塊鏈技術，類似國內悠遊卡之儲值支付工具，而有別於前揭虛擬通貨。

[3] 比特幣電腦節點俗稱礦工，可自由選擇加入或退出挖礦，屬於開放式(或非核准制)的公有鏈；另一種為核准制的私有鏈，參與交易及驗證之節點，須先經聯盟核准才能加入。私有鏈成員彼此認識，因此大多以合作協調的投票方式，達成製作區塊的共識，而非採比特幣彼此競爭的工作證明機制，以提高運作效率。

[4] 交易驗證主要係查驗交易者發送交易之數位簽章是否正確、付款方帳戶餘額是否足夠、以及是否有重複支付(double spending)。

[5] 解謎所需之主要資訊包括前一區塊雜湊值(hash)、自製區塊內所有交易雜湊值(merkle root)、猜測隨機值(nonce)、區塊產生時間(timestamp)等。

[6] 解謎過程稱為工作證明(Proof of Work)，亦稱為挖礦，中本聰曾將挖礦過程比喻為各礦工同時擲 37 枚硬幣，誰先擲出 37 枚均同一面者即勝出，並可獲得系統發給之比特幣作為獎勵。比特幣系統會定期(約 2 週)調整謎題難度，以維持系統平均約每 10 分鐘產生一個新區塊之速度，若參與挖礦者愈多，致解謎時間愈快完成時，系統會增加投擲硬幣數量(例如增至 50 枚)，以提高謎題難度。

機制，由多個節點同時驗證交易並記錄在帳本上。

然因全球間各節點間互不認識，為使各節點所維護之區塊鏈帳本一致，並對於誰製作的區塊才是被認可者有一致之共識，DLT 需要一套共識(consensus)機制。比特幣區塊鏈系統採用之機制稱為工作證明(Proof of Work, PoW)，係由各節點彼此相互競爭去解答前述謎題。

概念上，DLT 與區塊鏈略有不同，依 BIS 定義[7]，DLT 範圍較區塊鏈廣，區塊鏈只是 DLT 其中一種型式，並非所有 DLT 均採用區塊鏈技術。例如，部分 DLT 系統[8]只將交易資料傳送給交易雙方節點進行分散式記帳，再傳送給公證節點驗證，但並未傳送給全部節點，此時，每個節點保有之帳本並不相同，此種 DLT 型態與比特幣區塊鏈各節點均保有相同一套總帳之做法不同。為利說明，本文後續內容不區分二者差異，將交互使用。

值得注意的是，BIS 近期報告指出，私部門虛擬通貨之系統設計存在瑕疵，例如透過全體節點同時對所有交易進行驗證之運作效率低、對電腦與電力之耗能高、系統不具擴展性而無法同時處理大量交易、交易不具最終確定性[9]；此外，虛擬通貨價格波動大、具投機性，尚難以成為廣泛使用之支付工具。

參、央行數位通貨(CBDC)之研究

雖然虛擬通貨有前述缺點，惟支撐其運作之底層區塊鏈技術，被視為有潛力被應用在其他領域。因此，近期部分國家央行持續研究該等技術應用在發行 CBDC 之可能性。

然而，各國在研究 CBDC 時，通常不直接使用前揭具瑕疵之虛擬通貨 DLT 或區塊鏈技術，而係加以改良後，再進行研究測試。以下提出國際間主要機構與央行對於發行 CBDC 之研究、看法及其問題與挑戰。

---

[7] Beck and Garratt (2017)。

[8] 例如，R3 推出之 Corda 平台。

[9] 例如採用工作證明(PoW)機制，可能因二個礦工節點同時產生區塊，而有分叉情況，導致被包在區塊內交易之價值是否完成移轉具有不確定性。此等交易最終性無法確定的情況，不適宜應用在交易完後須具最終性之金融交易領域。

一、BIS 對貨幣之分類

BIS 依據四個不同面向，定義貨幣態樣：

- 依發行者(issuer)：可分為央行與非央行發行之貨幣。
- 依形式(form)：可分為數位貨幣與實體貨幣。
- 依使用者普及性(degree of accessibility)：可分為大眾均可使用與僅限特定使用者。
- 依技術(technologies)：依支付移轉之機制，可分為代幣基礎(tokens)[10] 與帳戶(account)基礎貨幣。

代幣基礎貨幣之特色係對於交易驗證採用去中心化作業，可能採用例如虛擬通貨之區塊鏈交易驗證機制；或是採用非區塊鏈技術之去中心化作業。例如捷運悠遊卡之離線交易，使用者乘坐公車之感應支付，係經由近端感應即在收付雙方載具內晶片直接增減彼此交易金額，而該筆交易並未經由後端之中心化作業即時處理卡片內資金餘額之撥轉。

帳戶基礎貨幣係一般大眾在央行開戶，支付後由央行以中心化作業方式在雙方帳戶內即時進行餘額撥轉，概念係將目前可在央行開戶之對象由銀行擴及至所有大眾，其特色係可採用實名制。

BIS 認為 CBDC 尚無完整定義，概念上，只要是央行採數位化發行、列為央行負債，並具備貨幣三項定義-支付、儲存及記帳單位，即屬之(詳圖 1 灰色區域)。換言之，銀行等金融機構存放在央行準備金帳戶內的存款亦算是廣義的 CBDC，只是近期討論之 CBDC，多聚焦在採用 DLT 或區塊鏈技術。

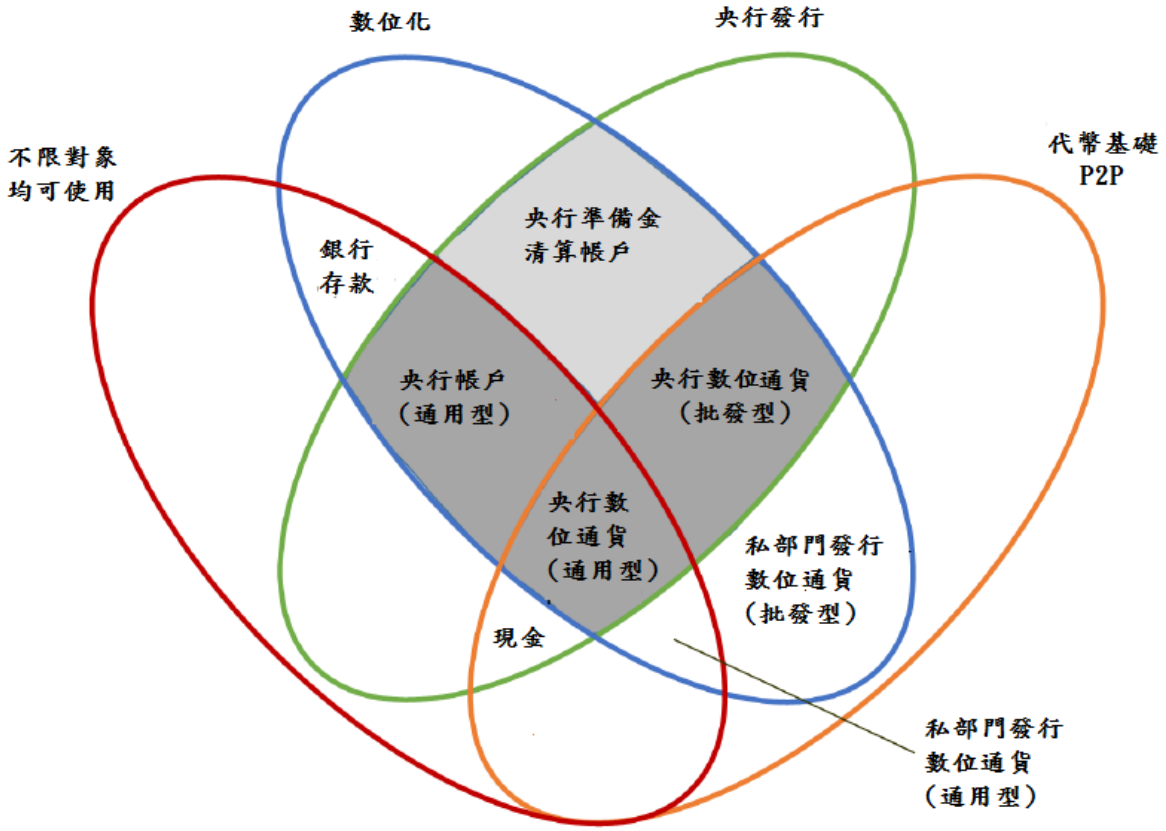
依 CBDC 使用者普及性，可分為二大類：

- 第一類：批發型(wholesale) CBDC，僅供銀行使用在跨行支付及結清算作業。目前部分國家央行已陸續測試研究如何應用 DLT 技術在發行批發型 CBDC，以進行跨行支付及結清算作業。
- 第二類：通用型(general purpose) CBDC，不限使用對象，可供一

[10] 部分報告稱為價值基礎(value base)。

般大眾、商家使用，例如應用在零售支付等領域。因涉及問題廣泛，不僅是技術層面，還包括銀行存款可能流向央行，導致銀行擠兌之金融穩定議題。因此，目前各國多僅停留於發行及運作架構之探討階段，尚無央行提出具體之測試研究結果，但有部分央行[11]已明確表示無推行計畫。

圖 1　BIS 對貨幣之分類



資料來源：BIS (2018a)

二、 CBDC 可具備之特性

央行研議發行 CBDC 時，可思考其是否應具備以下特性：

- 可用性(availability)：CBDC 可全時(24/7)使用，可設計為無到期日或是有限定到期日(例如：從產生、發行、贖回均在一天內完成)。
- 匿名性(anonymity)：代幣基礎 CBDC 可設計為匿名式。

[11] 如丹麥、澳洲、瑞士等國央行。

- 移轉機制(transfer mechanism)：CBDC 之移轉可設計為採用代幣基礎之點對點(P2P)移轉方式；或採用帳戶基礎由中心化單位即時記錄與撥轉雙方款項。
- 附息(interest-bearing)與否：與其他央行負債一樣，不論何種基礎之 CBDC 均可設計為計息(正利率或負利率)或不計息。
- 設定限額(limits or caps)：CBDC 之交易或持有金額可設定限額。

三、 國際間對通用型 CBDC 之研究與看法

(一) BIS 看法

DLT 技術應用在發行 CBDC 除仍存在相關技術問題[12]外，亦涉及許多非技術面問題，包括銀行存款可能流失，衝擊金融穩定、反金融中介及整體支付生態等層面，爰須各界深入思考。因此，目前僅部分國家提出發行架構之構想，尚未對外公布實際相關測試結果。各層面挑戰如次：

1. 發行方式

帳戶基礎 CBDC 允許大眾在央行開戶，除涉及央行是否適合直接面對大眾之定位問題外，央行亦須對開戶人進行實名認證(KYC)與反洗錢(AML)等作業，對央行及金融體系是重大轉變，爭議仍大。

代幣基礎 CBDC 之支付移轉作業，可採用 DLT 技術，或採用類似悠遊卡逕自載具內餘額直接扣付移轉之技術，因支付過程採去中心化作業，可避免單點失靈問題，但因匿名交易，則有違反洗錢防制之疑慮。

2. 金融穩定議題

央行若允許一般民眾可在央行開戶並持有央行 CBDC，將產生以下問題：

(1) 銀行存款可能流失

因 CBDC 相對銀行存款無信用風險，如發生金融危機，將加速民眾將銀行存款轉為 CBDC，導致存款自商業銀行大量流失之「數位擠兌(digital run)」現象，造成金融市場不穩定，此亦為 BIS 關切之重點。

[12] 詳本報告第 4、5 頁有關 CBDC 之說明。

惟部分講者認為，前述擠兌現象不致於太嚴重，因現行存款保險機制已協助銀行降低信用風險避免擠兌；另為避免資金從銀行轉移至中央銀行帳戶可能產生之金融不穩定，央行可採配套措施，例如，設定每位民眾持有 CBDC 之限額等。此外，發行 CBDC 反而會對商業銀行產生自律效果，因為銀行必須持有更多準備、資本以健全其經營，甚或提高利率，才可避免存款流向 CBDC。

(2) 弱化銀行金融中介功能

CBDC 可設計為附息或不附息，附息會與銀行存款競爭，即使在金融穩定時期，亦可能導致銀行存款流向央行；若為不附息，則在金融危機時期，可能會因銀行信用與倒閉風險提高而使得銀行存款流向央行。長期以往，銀行資金流失之壓力可能影響其承作放貸業務之能力，除非銀行轉向依賴批發市場[13]或提高存款利率吸收資金，否則可能會弱化銀行金融中介功能。

3. 法制議題

各國央行對 CBDC 之發行、管理及擴大央行開戶對象範圍之相關法律授權規定均尚不足，未來如有發行需求時，亦須一併配合增修。

4. 交易隱私問題

數位通貨本質上可替代實體鈔券，惟若數位通貨採記名式發行，恐引發民眾對隱私權遭侵犯的疑慮，而排斥使用；若採匿名式發行，則可能違反洗錢與資恐相關法規，權衡何種發行方式甚為重要，各國央行在發行前需清楚瞭解國內民眾實際上對 CBDC 的需求及原因為何。

5. 整體支付生態議題

央行發行 CBDC 目的之一，係可提供民眾便利之支付工具，惟央行需另投入經費建置整體支付生態系統；此外，央行與民間競爭提供零售端支付服務是否有其利基或較具效率，宜多加深思。

6. 實體鈔券與 CBDC 可能並行甚長時間

[13] 例如銀行間拆款市場或發行金融債券等。

許多民眾對數位化貨幣不熟悉而不願使用，即使發行 CBDC，央行仍有義務對有實體鈔券需求之民眾持續提供服務，從而產生實體通貨與 CBDC 並存現象，此種並存情況應會持續很長時間甚或不會消失，央行同時發行與管理兩種貨幣之成本勢必增加。

7. 對執行負利率政策之影響

部分報告認為央行發行 CBDC 後，有利於執行負利率政策。惟實務上 CBDC 與實體貨幣如果並存，即使央行將 CBDC 利率降至零以下，民眾亦會轉為持有實體鈔券，而使得負利率政策效果無法發揮。

(二) 美國聖路易 Fed 看法

2018 年 4 月美國聖路易 Fed 發布報告[14]，將央行加密通貨定義為採用去中心化方式(如 DLT)，進行交易處理與驗證作業，且使用者可匿名交易之運作機制。

由於央行加密通貨之匿名特徵與防制洗錢作業相牴觸，該報告認為，央行不應冒著損及名譽之風險發行央行加密通貨[15]，但可考慮發行央行電子貨幣(central bank electronic money)，允許大眾、企業均得於央行開設帳戶，並用以進行支付。央行電子貨幣之交易處理係採中心化記帳作業、由央行獨占發行，且央行電子貨幣無信用風險，民眾應有需求。

聖路易 Fed 依 3 個面向將貨幣類型區分如次(圖 2)：

第 1 個面向為實體貨幣或虛擬通貨：實體通貨包括現金鈔券、黃金等，虛擬通貨則包括銀行存款、央行 CBDC 與比特幣等。

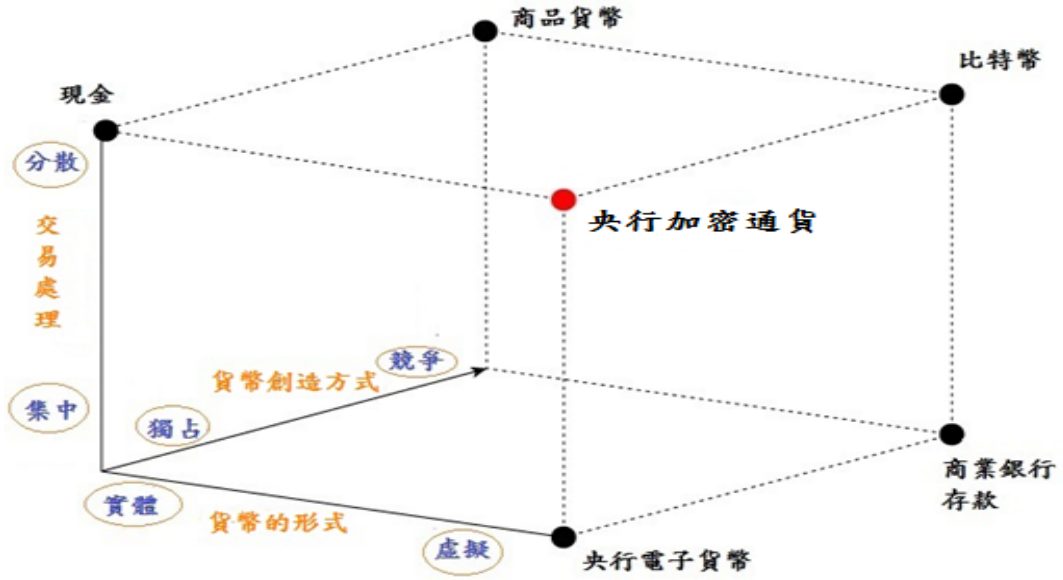
第 2 個面向為交易處理方式，可分為採中心化或去中心化方式處理交易。

第 3 個面向為獨占或競爭方式發行貨幣，例如各銀行在央行之存款，屬於央行獨占發行之貨幣；而各銀行競相吸收客戶之存款，則屬銀行競爭發行之貨幣。

[14] Berentsen (2018)。.

[15] 聖路易 Fed 報告指出，目前許多談到發行央行數位(加密)通貨之報告，經檢視其內容，多係指央行電子貨幣。

圖 2 聖路易 Fed 之貨幣類型



資料來源：Berentsen (2018)

聖路易 Fed 認為可考慮發行央行電子貨幣之主要理由如次：

1. 使用現金的成本比電子支付高，現金交易較易助長犯罪、洗錢及逃稅，亦會限制央行負利率政策的效果。
2. 民眾對央行電子貨幣有需求，主因交易方便，且央行無信用風險。
3. 大眾在央行開戶之執行難度不高

央行如允許大眾可在央行開戶，該帳戶存款餘額僅作為電子支付使用，且不涉及其他授信業務。因此，央行對該等帳戶可採取較寬鬆之監管力度，但基本的 KYC 作業仍為必要。

央行不一定要自己提供發行電子貨幣之基礎設施，可以法令規定要求銀行必須幫其客戶在央行開戶，這樣可使銀行客戶經由其既有之網路銀行介面連接至央行帳戶，以利資金撥轉。

4. 央行電子貨幣可提升金融穩定

央行電子貨幣會對商業銀行產生自律效果(disciplining effect)。銀行為避免客戶資金轉移到央行電子貨幣帳戶，必須持有更多準備與資本，以健全其經營，或提高存款利率。

為避免資金自銀行轉移至中央銀行帳戶可能影響金融穩定，央行可

採配套措施，包括：設定大眾在央行電子貨幣帳戶之限額、央行可快速融通資金給提供擔保品之銀行。

5. 央行可調控電子貨幣帳戶利率水準，作為政策操作工具

對於在央行開戶使用央行電子貨幣之大眾與金融機構，央行可給付低於銀行存款之利息，並以該利率作為政策利率下限。此外，央行可調整該帳戶存款利率，以直接影響在央行開戶之大眾及金融機構；相較於傳統上先由央行執行貨幣政策操作傳遞至金融機構，再間接傳遞至全體家計單位之作法，此種傳遞機制會較快速且有效率。

此外，部分民眾批評 Fed 只對銀行存放之超額準備付息，但卻不准民眾存放央行獲取利息之政治敏感性議題，亦可因此獲得舒解。

(三) 加拿大央行看法

2018 年 5 月加拿大央行發布報告[16]，支持由央行中心化發行及驗證交易的央行電子貨幣。主要內容如次：

1. 不宜採用 DLT 技術：由央行發行但採去中心化多節點處理交易之央行數位通貨，較現有支付系統更不具效率。例如，該行 Jasper 1 概念驗證計畫，利用 DLT 發行央行加密通貨(CAD Coin)，進行銀行間跨行支付及結清算，結果顯示並未較現有央行之中心化處理系統有效益。
2. 發行央行電子貨幣可抑制大眾過度使用私部門加密通貨：比特幣等加密通貨如被廣泛使用，會影響央行貨幣政策有效性，如發行央行電子貨幣，可避免民眾過度依賴私部門加密通貨。
3. 央行可發行中心化驗證交易的電子貨幣，讓全民在央行開戶且附息，有利央行直接調整該等利率水準，加速貨幣政策傳遞機制。

(四) 挪威央行(Norges Bank)看法

2018 年 5 月挪威央行發布報告[17]指出，CBDC 發行方式有下列三種：

第 1 種：帳戶基礎模式或價值基礎模式擇一。

[16] Davoodalhosseini and Rivadeneyra (2018)。

[17] Norges Bank (2018)。

第 2 種：前揭 2 種模式並用。

第 3 種：使用 DLT 技術，惟該行指出 DLT 技術尚不成熟，不宜採用。

以下說明帳戶基礎模式與價值基礎模式：

- 帳戶基礎(account-based)模式(圖 3 左)

  開放大眾在央行開戶[18]，支付交易採中心化作業處理，由央行在雙方帳戶即時增減交易金額。以圖 3 左為例，用戶同時在銀行及央行開戶，可透過銀行網銀系統線上將存款撥轉至央行帳戶。

  大眾 CBDC 餘額均記錄在央行中心化系統，進行支付交易時，以其載具(例如綁定央行帳戶之手機)感應，資金即由央行中心化系統即時增減雙方帳戶餘額。

- 價值基礎(value-based)模式(圖 3 右)

  用戶 CBDC 餘額儲存與記錄在其所持之儲值卡或手機預付(SIM)卡晶片中。當用戶進行支付時，經由近端感應技術，直接在交易雙方載具晶片中增減餘額。此等餘額記錄之變更由個別載具直接分散式處理[19]，如同雙方以實體現金支付移轉般，屬於非中心化作業。

  雖然價值基礎模式之支付過程採匿名式交易，但在用戶以存款或現金法幣儲值時，應採實名制。

價值基礎模式 CBDC 之功能類似實體現金，而帳戶基礎模式 CBDC 則類似銀行存款。二種模式主要特色如次：

1. 帳戶基礎 CBDC
   - 可適用在所有支付方式，包括近端及遠端線上購物支付等。
   - 須提供安全的資金保管機制。
   - 依賴中心單位即時交易結清算處理作業，在使用上有其限制。

[18] 帳戶基礎模式亦可設計為二層級架構，由銀行在央行開戶，而大眾只能在銀行開立 CBDC 帳戶。銀行收取客戶存款並兌換 CBDC 給客戶後，銀行須確保所收存款與兌換出之 CBDC 金額一致，且所收存款須 100%存放央行或保存在帳上不得動用，形成 100%準備金制度之銀行體系。

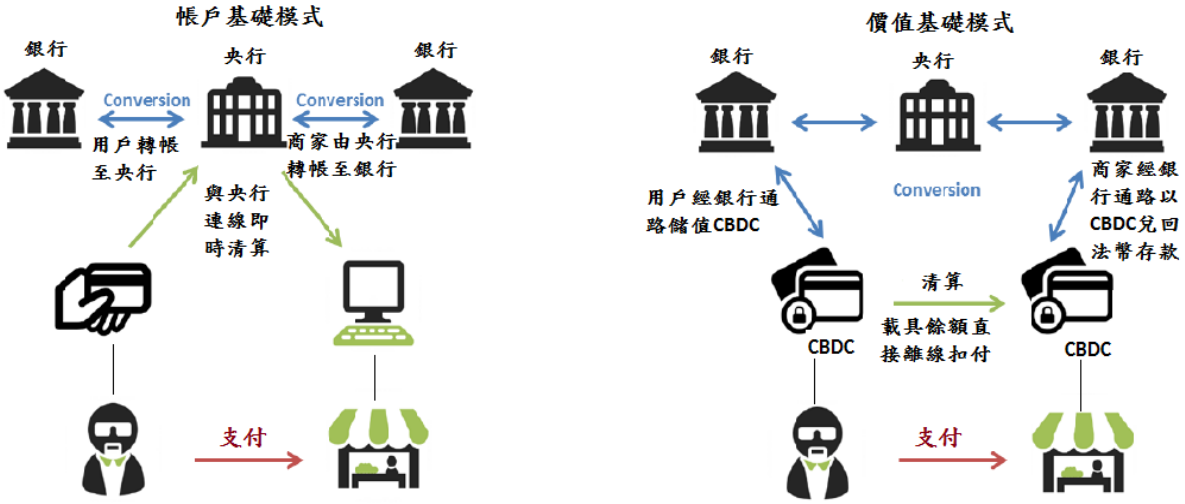
[19] 國內悠遊卡(預付儲值卡)公車費用支付案例即屬此模式，當乘客在公車上完成感應支付後，該筆交易金額立即記錄至雙方載具中晶片，屬離線且去中心化之交易處理機制，而非由中心化單位直接處理帳戶款項撥轉事宜。公車業者日終(或定期)彙整將各據點交易紀錄與金額，再向發卡機構批次請款，此時才會經由銀行處理款項撥付事宜。

- 對銀行、金融穩定、貨幣政策可能有較大的衝擊。

2. 價值基礎 CBDC

- 支付交易係直接記錄在各用戶載具上，不須依賴第 3 方中心單位處理交易。
- 支付交易未被追蹤或紀錄在中心化資料庫，可滿足交易匿名性之需求。
- 因載具(卡片或手機)內直接記錄儲值金額，一旦遺失載具就形同遺失現金，將造成用戶損失[20]。因此，不適合大額資金之儲存或交易。
- 不適合應用在線上購物等遠端支付場景。

圖 3 帳戶基礎模式與價值基礎模式



資料來源：Norges Bank (2018)

(五) 英格蘭銀行(BoE)看法

2018 年 5 月 BoE 發布報告[21]，提出發行 CBDC 之構想，其發行方式與前揭各國央行有所不同，主要差異在於客戶係以合格擔保品(如英鎊公債)向銀行換取 CBDC，如果客戶想以存款向銀行兌換 CBDC，銀行並不保證可全額兌換 CBDC，該報告認為此作法可減緩銀行存款流失情形。

[20] 如另外設計記名式之機制，則可避免此等損失。
[21] Kumhof and Noone (2018)。

此外，在使用技術部分，BoE 報告則質疑其他央行建議不宜採用 DLT 技術之見解。

在 CBDC 之運作架構設計，BoE 認為遵循下列原則，可適度減緩銀行體系存款流失：

1. CBDC 設計為附息，且利率可調整，在市場對 CBDC 需求高時，可調降利率，以避免資金大幅流向 CBDC，有利金融市場穩定。
2. 其他有關 CBDC 報告多設計為民眾可以存款向銀行兌換 CBDC，且無金額限制；惟 BoE 報告參考英國法規並未要求銀行必須提供足額現金供客戶提領存款之精神[22]，建議若發行 CBDC，銀行亦無須承諾客戶存款可兌換 CBDC，以減緩其存款流失壓力。
3. 為避免銀行存款流向他行，而產生金融不穩定之現象，銀行僅得以公債等擔保品向央行兌換 CBDC，不得以其在央行之準備金存款兌換 CBDC。

例如：若甲銀行保證其客戶存款均可無限制兌換 CBDC，但他行對客戶存款有限制兌換之情況下，一旦民眾對 CBDC 需求增加，將使他行客戶將存款轉至甲銀行並兌換成 CBDC，而他行須透過央行準備金帳戶清算並撥款至甲銀行準備金帳戶；若央行允許銀行可以準備金兌換 CBDC，甲銀行將有非常充裕的 CBDC 持續供應其客戶，從而導致他行存款持續大幅流失。因此，銀行僅得以合格擔保品(公債)向央行兌換 CBDC，不得以銀行準備金存款兌換 CBDC。

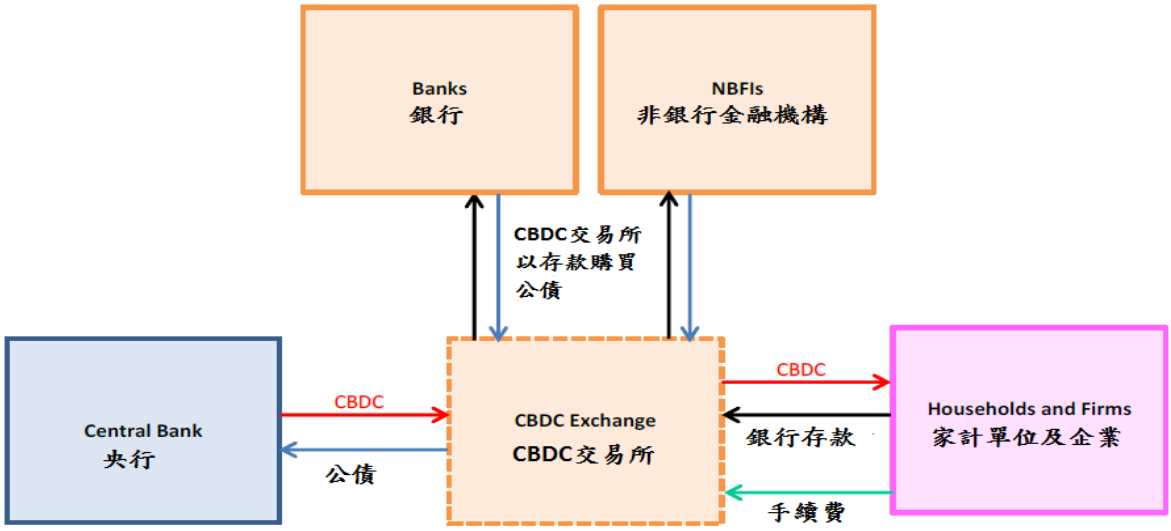
有關央行開戶對象範圍，BoE 報告提出 3 種模式，以下說明銀行等金融機構、CBDC 交易所、一般企業及大眾均可在央行開戶之 EW 模式(economy-wide access model)運作方式：

- 央行開戶對象：無限制，包括所有銀行、非銀行金融機構(non-bank financial institutions, NBFIs)、CBDC 交易所，以及企業與大眾均可在央行開戶。

[22] 詳 Kumhof and Noone (2018)，第 14 頁，附註 15。

- 銀行、非銀行金融機構及 CBDC 交易所可以公債等合格擔保品向央行兌換 CBDC(類似公開市場操作)。
- CBDC 交易所:(1)可接受大眾以存款兌換CBDC,並收取手續費;(2)為補足 CBDC 部位，交易所以存款向銀行或非銀行金融機構購買公債，再以取得之公債向央行兌換 CBDC(圖 5)。
- 企業與民眾如需要 CBDC，可透過下列方式取得：(1)以存款向 CBDC 交易所兌換 CBDC；(2)以公債向銀行兌換 CBDC，再由銀行以公債向央行兌換 CBDC；(3)以存款向銀行兌換 CBDC，但銀行不保證客戶可兌換到 CBDC。

圖 5 CBDC 交易所之運作架構



資料來源：Kumhof and Noone (2018)

BoE 以銀行資產負債表之變化分析，認為發行 CBDC 會使銀行存款流向央行 CBDC，導致銀行資產負債表規模縮減，但若能遵循前述發行 CBDC 原則，則可減緩銀行存款流失情況。

四、國際間對發行批發型 CBDC 之研究與看法

(一) 國際間之研究與測試結果

各國央行近年陸續就批發型 CBDC 進行測試並公布測試結果，主因批發型 CBDC 僅涉及技術層面問題，但不涉及過多前述零售型 CBDC 面

對的複雜問題。

國際間進行批發型CBDC研究測試時，主要係瞭解應用區塊鏈或DLT技術所發行之CBDC如何應用於跨行支付及結清算作業。測試內容包括：

- 銀行如何以法幣存放至央行帳戶作為擔保品，再由央行據以對銀行發行等值CBDC。
- 銀行如何進行跨行支付移轉。
- 銀行如何執行多邊淨額互抵結算(又稱流動性節省機制LSM[23])。
- 銀行如何執行境內與跨境款券同步交割(DvP)，以及不同幣別間之款項同步清算(PvP)等。

主要國家央行DLT作業測試結果指出之挑戰詳附錄1，重點如次：

- DLT在系統擴展性(scalability)、交易處理效能及效率性不及中心化作業系統：DLT 為使各節點對交易結果達成共識，須耗時進行共識決演算，同步驗證並儲存交易資料，導致交易處理速度與效率遠不及現有之中心化作業系統。
- DLT 雖宣稱可改善單點失靈問題，但實際上並無法完全解決問題：各節點功能皆相同之DLT作業模式雖具有降低單點失靈風險之優勢，惟各國測試結果顯示，部份作業過程如交易排序等，仍須依賴單一節點處理。若該節點運作失常，恐致系統無法運作，故其並無法發揮DLT原先宣稱可完全避免單點失靈之優勢。
- 跨不同DLT平台款券同步交割(DvP)作業尚存問題

  2018年3月ECB與日本央行(BoJ)公布聯合測試報告指出，若數位化後之款、券均屬同一DLT平台，款券同步交割作業速度及效率尚稱順暢[24]。

  惟款、券分屬不同DLT平台，當部分作業程序中斷或設定款、

[23] 流動性節省機制(Liquidity Saving Mechanism, LSM)係當銀行帳戶餘額不足支付指令扣付時，該指令不直接退回，而是佇列等候，待特定時間再將等待支付之指令進行雙邊或多邊互抵作業，以節省銀行流動性，並避免產生銀行間資金互卡(gridlock)現象。

[24] 2018年5月加拿大央行公布採用同一DLT平台之款、券同步交割作業，亦顯示同樣結果。

券圈存的時間不當時，會發生款、券移轉至同一交易方，導致另一方承受風險的異常狀況(附錄 2)。

(二) 我國央行主要測試研究結果

2017 年本行與票據交換所及學術機構共同合作，進行區塊鏈技術應用於跨行支付及清算作業之概念驗證，主要內容及結論如次：

- 測試內容:模擬以銀行持有的央行數位通貨進行跨行支付,並研究「即時清算」及「混合清算」兩種模式。前者係在銀行帳戶餘額足夠即時直接扣付款項，完成資金移轉，帳戶餘額如不足，則退回交易指令；後者則可在銀行帳戶資金不足時，將交易指令暫時佇列，再定時進行批次多邊淨額互抵，以節省流動性需求。
- 測試結果：採即時結清算模式且主要交易內容(如交易對象及金額)未進行遮蔽[25]之測試結果，平均每秒約處理 26 筆交易；若採用流動性節省混合結清算模式，並對主要交易內容遮蔽時，因為必須由單一節點先就遮蔽資料予以解密，再進行批次結清算作業，此種流程下，該單一節點可能產生單點失靈問題，且平均每秒處理之交易筆數僅約 4 筆。上述不論是即時或混合清算模式，處理速度皆遠低於現行票交所中心化作業系統[26]。

綜上，近年國際間已有多家央行利用批發型 CBDC 就跨行支付清算進行測試研究，包括加拿大、英國、日本、新加坡及歐洲央行等機構。截至目前為止，各國測試結果大多顯示，運用 DLT 在跨行支付及結清算作業方面，並未較現有央行之中心化作業系統具有優勢，且 DLT 仍面臨多項技術問題與挑戰。目前各國跨行支付系統均已電子化與高度自動化，且央行為受信賴主體，由央行負責之跨行清算作業深受市場信任，因此，應用多節點分散式記帳與交易驗證的 DLT 技術在跨行支付及結清算領域，尚難明顯看到效益，此結論與 BIS 看法一致。

[25] 交易內容如未遮蔽，其他節點可查看鏈上所有交易內容，將造成交易隱私未受保護，而被其他無關之參與者查看到交易內容。

[26] 現行 ACH 中心化作業系統平均每秒約處理 2,700 筆。

五、部分財政困窘國家透過 ICO 發行新數位貨幣

前述發行 CBDC 之型態，均假設央行向大眾或金融機構收取法幣或公債為擔保，並據以發行等值的 CBDC 給使用者[27]，此種方式較能取得民眾的信任。惟近期部分國家則透過 ICO 發行數位代幣，做為其主權貨幣，例如，馬紹爾群島共和國(RMI)與委內瑞拉。

(一) 馬紹爾群島共和國(RMI)之主權貨幣

RMI 為美元化國家，無自己的主權貨幣，為因應美國即將停止對該國提供每年 3 千萬美元之援助款[28]，該國爰於 2018 年 2 月 26 日頒布「主權貨幣發行法(Declaration and Issuance of the Sovereign Currency Act)」，立法通過發行本國數位化主權貨幣，以避免過度依賴美元。

因 RMI 財政困窘，無財源建置自己新的貨幣體系，因此，政府透過 ICO 方式向市場籌措資金，發行數位代幣，並宣稱以該代幣做為主權貨幣(Sovereign Currency, SOV)。前揭 ICO 籌得資金除部分充實國庫外，另一部分則用於建置主權貨幣(SOV)在市場使用之生態系統。主要特色如次：

- SOV 採用去中心化之區塊鏈技術驗證交易：以開放式的 DLT 技術，經各節點礦工爭相驗證交易，成功礦工可獲得報酬。
- 政府宣布 SOV 主權貨幣具法償效力：RMI 宣布 SOV 可用以支付國內各項負債、公共事業費用及稅捐支出等，將成為民眾除美元以外，另一個可選擇使用的法幣。

(二) 委內瑞拉

委內瑞拉因受到經濟制裁，除財政困窘外，國內亦發生惡性通膨，其貨幣玻利瓦(Bolivar)嚴重貶值，導致民眾對貨幣失去信心。該國總統未經國會授權下，於 2018 年 3 月間透過 ICO 方式向市場籌資，並發行數位代幣(Petro)。

委內瑞拉總統與 Petro ICO 白皮書雖宣稱以該國石油資產作為發行

[27] 央行如允許大眾直接在央行開戶，則使用者除金融機構外，亦包括大眾。

[28] 1940 至 1950 年代美國頻繁在 RMI 進行數十次核試爆，後續造成許多民眾健康問題，美國因此每年提供約 3 千萬美元資金援助 RMI，惟該等款項援助將到期。

Petro 準備，惟實際上 Petro 持有人無法向政府兌換石油。因此，Petro 實質上仍屬無擔保或無準備之發行機制。

Petro 透過開放式區塊鏈技術，由各節點礦工爭相驗證交易，並採用新經幣(NEM)區塊鏈之重要證明(proof-of-importance, PoI)[29]共識演算機制。

委國總統宣稱 Petro 可用以支付國內公共事業費與稅捐，但並無法強制民間商家接受 Petro。依外電報導，委國在受到經濟制裁情況下，尚能發行 Petro 募得資金，其背後主要有來自俄羅斯之協助[30]。

依上述 RMI 與委內瑞拉二國以 ICO 發行數位貨幣之經驗，均因無法以既有之本國貨幣做為發行數位貨幣之準備或擔保，且面臨財政困窘問題，才須利用 ICO 方式籌資充實國庫，並期以透過區塊鏈技術之去中心化交易驗證機制，建立一套該國新的貨幣體系。反觀一般經濟與財政均正常的國家，目前均無發表須以 ICO 方式籌資並建立新的貨幣體系之案例。

肆、對私部門加密通貨交易之監管

一、加密通貨之適當名稱

私部門加密通貨如比特幣，早期推出時係標榜低費率之支付工具，惟近年來已面臨部分技術上亟待克服的問題，包括交易處理速度慢、使用者需負擔高額手續費[31]等，故其不易成為主流支付工具；另因加密通貨價格波動甚大，實務上亦不適合作為價值儲存及記帳單位。

此外，BIS 近期報告[32]指出，虛擬通貨的系統設計存在瑕疵，例如透過全體節點同時對所有交易進行驗證之運作效率低、對電腦與電力之耗能高、系統不具擴展性無法同時處理大量交易、交易不具最終確定性、以及去中心化的共識決機制存在脆弱性等因素，可能導致虛擬通貨之運作機制瓦解，而使其價值歸零。

---

[29] 重要證明(PoI)係指重要性較高的節點擁有較高的投票權重，而重要性包括擁有愈多新經幣及驗證愈多交易之節點則愈重要(Petro 白皮書第 22 頁)。

[30] 參考 http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/。

[31] 2018 年 2 月，ECB 執董會董事 Yves Mersch 講稿指出，比特幣近期交易需負擔之成本約 25 歐元。

[32] BIS (2018)。

由於加密通貨並不具備傳統貨幣之三大功能，近期部分國際機構已陸續將加密通貨改稱為加密資產(crypto-assets)，其中 ECB 並直指虛擬通貨被稱作通貨(currency)一詞並不恰當(表 1)。

表 1 主要國際機構與國家近期改變對加密通貨之稱謂

機構	對加密通貨之稱謂
G20	2018 年 3 月，20 國集團(G20)發布財長及央行首長公報，以加密資產(crypto-assets)取代 virtual currency 一詞
ECB	2017 年 11 月及 2018 年 2 月，歐洲央行(ECB)均表示 virtual currency 不具貨幣三大功能，使用 currency 一詞不恰當(misnomer)
IMF	2018 年 4 月，國際貨幣基金會(IMF)主席 Lagarde 講稿使用 crypto-assets 一詞

資料來源：107 年 6 月央行理監事會後記者參考資料

二、加密通貨之交易平台類型

(一) 代購代售平台

此類平台[33]業者透過交易平台對客戶提供買、賣雙向報價，作為客戶之應買或應賣對象，而其作為應買或應賣之加密通貨部位，可能是自己持有之部位，或是客戶購入後存放在平台代客保管之部位。

當客戶款項轉至平台業者帳戶時，業者會即時將其加密通貨撥入買方在平台之帳戶，此部分之業者與買方交易並未經過區塊鏈系統，只在平台業者之帳內進行移轉紀錄。

只有當買方將其加密通貨轉出至平台以外之交易人時，該筆交易才由交易平台業者以其私鑰簽署，並發送至區塊鏈系統進行處理與驗證。若買方對加密通貨需求增加時，平台業者即批次在國外交易所買入加密通貨，以備客戶之需求。

[33] 此類型業者不僅是其所宣稱之僅為其客戶提供代購與代售服務，業者實際上係先以自己自有之加密通貨部位或是客戶存放之部位，提供買、賣雙向報價並與客戶成交。

(二) 交易撮合平台

此類平台[34]提供買、賣客戶下單之撮合交易，常見之撮合交易類型包括：

- 法幣對加密通貨之交易：例如以法幣買比特幣或其他加密通貨。
- 加密通貨對加密通貨之交易：例如以太幣對比特幣之交易，或比特幣對新掛牌之 ICO 代幣交易。
- 槓桿交易：部分交易平台(如 Bitfinex 等)對客戶提供融資與融幣功能，使其可進行槓桿交易，若平台客戶有閒置資產(加密通貨或法幣)，則可利用交易平台之 P2P 放貸功能收取利息[35]。

三、主要國家將交易平台納入反洗錢規範

私部門加密通貨不具備貨幣之三大特性，惟其與貨幣同樣具有匿名交易特性，故易成為犯罪及洗錢工具。因此，防制洗錢金融行動工作組織(FATF)於 2015 年即出具報告，建議將涉及提供法幣與加密通貨互換之交易平台、錢包業者納入洗錢防制監管範圍。

G20 並於 2018 年 3 月財長及央行首長會議發布公報允諾，FATF 之反洗錢標準將適用於加密通貨。IMF 亦呼籲各國有關當局與國際標準制定者，應共同監控加密通貨交易，並採較一致性的監管方法，加強國際合作。

表 2 整理主要國家對加密通貨交易平台之反洗錢監管情形，由於各國法例與國情不同，其實際執行之方式亦有所差異。

表 2 主要國家對加密通貨交易平台反洗錢之納管方式

國家/地區		主管機關	監理內容概要
美國	聯邦層級	金融犯罪執法網(反洗錢)	虛擬通貨兌換及支付處理業者屬「銀行秘密法」(Bank Secrecy Act，洗錢及資恐防制之聯邦法規)之「貨幣服務業」，應向金融犯罪執法網

[34] 國內主要交易撮合平台包括幣託設立之 BitoPro、Maicoin 設立之 Max 及日商 Bitpoint。

[35] 交易撮合平台如提供客戶融資融幣交易功能，所涉風險大，且可能屬於我國期貨交易法第 3 條定義之槓桿保證金契約，將引發同法第 13 條，非依本法不得經營期交所或期交所業務之疑慮。

國家/地區		主管機關	監理內容概要
			(FinCEN)註冊並遵守洗錢防制義務。
	州層級(紐約州等)	州金融服務署、金融局等(核發執照)	虛擬通貨相關業者須取得執照並受監理。
日本		金融廳 (核發執照與反洗錢)	1. 依「支付服務法」進行金融監理，該法主要規範虛擬通貨交易平台等業者。 2. 平台業者另依洗錢防制相關法令，須向警察廳犯罪收益移轉防止對策室(JAFIC)通報可疑交易。
南韓		金監會 金監局 (反洗錢)	1. 反洗錢部分，2018 年 1 月 30 日起客戶在交易平台及銀行開立之帳戶均採實名制，以利執行反洗錢作業。銀行應對虛擬通貨交易所進行高度盡職調查，並就涉及大額或疑似洗錢交易向金監會(FSC)[36]之金融情報局(KoFIU)[37]部門進行反洗錢通報。 2. 金監局(FSS)[38]、FSC、KoFIU 近年曾數次就平台對客戶虛擬通貨之保管與反洗錢等問題，對平台業者與銀行執行聯合檢查。
新加坡		警政署商業事務局 (反洗錢)	1. 虛擬通貨不致對金融穩定產生風險，金管局(MAS)未納管或禁止。 2. 平台業者應向警政署商業事務局(Commercial Affairs Department,

[36] 金融監督委員會(Financial Supervisory Commission, FSC)負責金融政策及法規監管之單位。
[37] 金融情報局(Korea Financial Intelligence Unit, KoFIU)為 FSC 內部單位，負責金融機構反洗錢業務。
[38] 金融監督局(Financial Supervisory Service, FSS)負責執行金融機構之監管。

國家/地區	主管機關	監理內容概要
		CAD)通報洗錢交易。
香港	警務處聯合財富情報組(反洗錢)	1. 金管局(HKMA)未納管或禁止。 2. 平台業者應向聯合財富情報組(JFIU)[39]通報洗錢交易。
澳洲	司法部澳洲交易報告與分析中心(反洗錢)	1. 澳洲央行(RBA)及證投會(ASIC)未納管或禁止。 2. 2018 年 4 月完成修法，將平台業者納入既有洗錢防制體系，由司法部澳洲交易報告與分析中心(AUSTRAC)監管。

資料來源：本文整理

四、各國對 ICO 之監管

(一) ICO 有高比例交易涉及詐騙

ICO 係向社會大眾發行數位代幣，並收取主流加密通貨(如比特幣或以太幣)之籌資行為，且多採用區塊鏈等新興技術，透過網路等非傳統籌資管道向投資大眾募資。

近期ICO市場成長快速，然而目前已有不法人士利用ICO進行詐騙。例如，以未實際發行之虛假代幣邀集投資人參與購買，標榜高報酬，並以多層次傳銷的龐氏騙局方式，吸收大眾資金。

BIS 在 2018 年度經濟報告引用麻省理工學院(MIT)研究，依據新聞報導示警、ICO 募資後網站是否停止營運、白皮書內容等三個指標進行評估，判斷 ICO 案是否屬於詐騙，結果顯示逾 2 成 ICO 案例涉及詐騙(圖 5)。

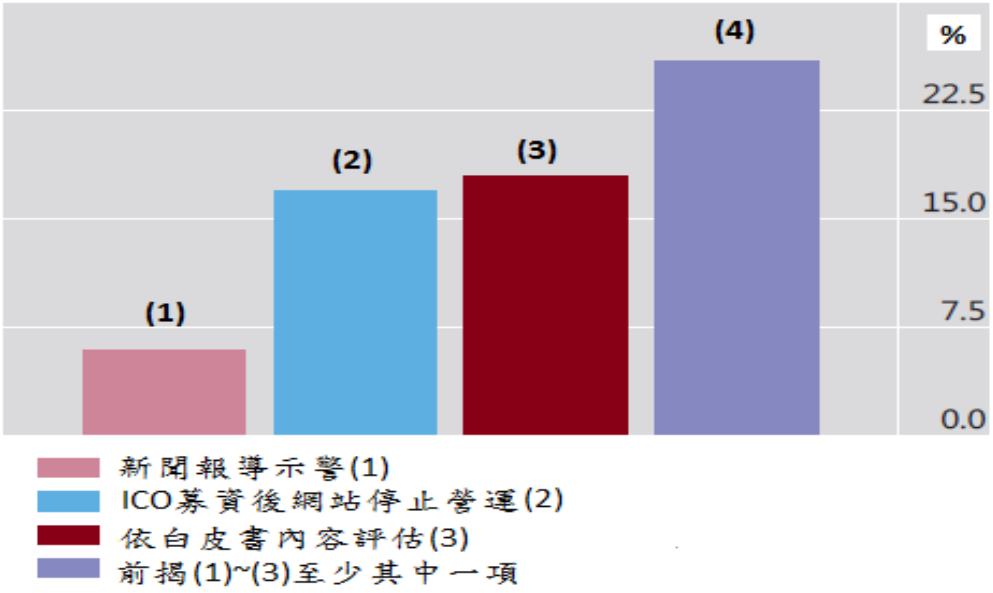
(二) ICO 監管

目前各國對 ICO 之監管方式不盡相同，除中國大陸及南韓[40]禁止外，少數國家採發布警示或加強宣導方式，部分國家則係採 ICO 個案認定其

[39] 聯合財富情報組(Joint Financial Intelligence Unit, JFIU)由香港警務處及海關人員共同組成。
[40] 惟近期部分外電報導南韓可能會解除 ICO 禁令。

發行代幣之性質及其應遵循何種法令。

圖 5 高比例 ICO 案件屬於詐騙



資料來源：BIS (2018)

瑞士金融市場監理局(FINMA)於 2018 年 2 月發布之指引函令，定義下列 3 種 ICO 類型，並認為實務上發行案例可能混合不同類型。

1. 資產型代幣(asset tokens)[41]：代幣持有人對 ICO 發行者之資產有請求權(如股權或債權)，例如，若代幣持有人可分享發行者之營運盈餘，則該代幣性質形同股權(equities)。
2. 效用型代幣(utility tokens)：代幣持有人可將代幣使用在發行者提供之應用與服務[42]。
3. 支付型代幣(payment tokens)：代幣持有人可將代幣作為廣泛支付商品與服務之工具，此類代幣對發行者無請求權。

另泰國在 2018 年 5 月頒布數位資產事業法(Digital Asset Business Law)，明定泰國證管會(SEC)為虛擬通貨與 ICO 之主管機關，虛擬通貨交易相關事業須在 90 天內向 SEC 登記，否則將受罰。在 ICO 規定部分，發行者僅限於有限公司，並須經 SEC 核准，且透過 SEC 認可的平台募資，

[41] 部分國家稱為證券型代幣。

[42] 例如，部分虛擬通貨交易平台以 ICO 發行自己的代幣，投資人在平台交易之手續費，如以該代幣支付，則可享優惠與折扣。

此外，ICO 發行者須定期向 SEC 提交財務及營運報告。

表 3　國際間對 ICO 之監管方式

監管方式	經濟體	主要內容
禁止	中國大陸、南韓	－中國大陸禁止 ICO 相關活動。 －南韓表示，若干 ICO 項目利用代幣進行股權募資，違反資本市場法案，將嚴懲違法平台。
發布警示或加強宣導	日本、歐洲、馬來西亞、香港、美國	－日本金融廳警示虛擬通貨價格變化劇烈，風險極大，且部分 ICO 可能是場騙局。 －歐洲證券與市場監理機關(ESMA)指出，ICO 對投資人的風險很高。 －馬來西亞央行(MAS)與證券委員會(SC)均表示，未經允許及從事 ICO 業務，恐觸犯 SC 轄下的證券相關法規及 BNM 轄下的金融服務相關法規。 －香港金管局運用多元的媒體管道強化宣導，提醒大眾留意投資虛擬通貨與 ICO 的風險。 －美國證管會(SEC)設置虛構的 ICO 網站，引誘民眾點閱，將其引導至宣導網站，並依實際經驗，提供反詐騙資訊。
個案認定	瑞士、泰國、美國、新加坡、加拿大、香港	－瑞士金融市場監理局(FINMA)於 2018 年 2 月發布指引，定義 3 種 ICO 類型，指出具證券屬性之代幣須遵循證券相關法令，以利市場遵循。 －泰國於 2018 年 5 月頒布數位資產事業法(Digital Asset Business Law)，規定 ICO 發行者僅限有限公司，且須獲證管會(SEC)核准，並透過 SEC 認可的平台募資；此外，ICO 發行者須定期向 SEC 提交財務及營運報告。 －美國證管會(SEC)、新加坡金融管理局(MAS)、加拿大證券管理局(CSA)及香港證監會(SFC)指出，ICO 須個案認定，若所發行的代幣實質上具證券屬性，則應遵循證券相關法規。

資料來源：本文整理

伍、心得與建議

一、 心得

(一) 採用 DLT 發行批發型 CBDC，仍有待克服之技術問題

Fed 主席 Powell 於 2017 年之「創新、科技與支付系統」講稿表示，目前區塊鏈技術之信任度(reliability)、可擴展性(scalability)、安全性(security)與跨系統互通性(interoperability)等問題，仍尚待克服。

ECB 與 BoJ 於 2017 年 9 月發布第 1 階段聯合測試報告表示，DLT 技術尚不成熟，現階段無法實際應用在日本或歐洲央行大額支付清算系統；其復於 2018 年 3 月發布第 2 階段聯合測試報告指出，若款、券分屬不同 DLT 平台，當部分作業程序中斷或設定款、券圈存的時間不當時，會發生款、券均移轉至同一交易方，導致另一方承受風險的異常狀況。

BIS 於 2018 年 3 月及 6 月分別發布報告指出，以區塊鏈技術或 DLT 發行之批發型 CBDC 進行跨行支付及結清算作業，其效能並未優於現有的中心化作業基礎設施。

(二) 央行是否發行通用型 CBDC 因涉及許多層面問題，宜審慎評估

通用型 CBDC 之發行，除涉及大眾均可在央行開戶之問題，從而產生央行對大眾帳戶之管理、銀行存款可能流向央行之存款流失問題、實體鈔券與 CBDC 可能並行甚長時間，或永遠並存問題，除降低央行負利率政策效果外，亦會增加央行對通貨之發行與管理成本。

由於尚有前述之挑戰與問題，各國對於發行通用型 CBDC 多抱著持續研究與觀望之態度，甚或表示無發行計畫，例如丹麥[43]、瑞士[44]等國央行。

世界經濟論壇(WEF)近期發布報告指出[45]，發行 CBDC 所帶來之風險

[43] 參考 http://www.nationalbanken.dk/en/publications/Pages/2017/12/Central-bank-digital-currency-in-Denmark.aspx。

[44] Central Banking (2018)。

[45] WEF (2018)。

將遠超過其效益；此外，允許所有人均可在央行開戶，將對目前央行對銀行、銀行對大眾之金融中介運作架構產生重大影響。WEF 建議，央行宜維持現有銀行與央行之傳統運作架構，並以其為基礎提供創新服務，主管機關可透過法規增修[46]，開放新競爭者與技術加入市場，以提高系統運作效率。

(三) 將私部門加密通貨納入洗錢防制體系，符合國際潮流

私部門加密通貨易成為犯罪及洗錢工具，因此，防制洗錢金融行動工作組織(FATF)於 2015 年即出具報告，建議將涉及提供法幣與加密通貨互換之交易平台、錢包業者納入洗錢防制監管範圍。此外，G20 並於 2018 年 3 月發布公報，允諾將 FATF 之反洗錢標準將適用於加密通貨。

二、 建議

(一) 持續掌握私部門加密通貨之發展及其與金融體系之連結

現行私部門加密通貨如比特幣及以太幣，一方面仍面臨多項待解決之技術性問題，如交易處理速度等，另一方面部分國家禁止銀行持有或辦理加密通貨相關業務，致加密通貨規模尚不致影響金融穩定。

然而，未來若加密通貨技術[47]大幅改善，民眾需求可能提高，進而使得加密通貨與金融體系之連結加深，本行宜持續關注其進展，以利掌握其對整體金融市場之可能影響。

(二) 密切關注各國央行業務應用 DLT 之情形

雖然應用 DLT 技術在通用型或批發型 CBDC 領域仍面臨技術層面及其他複雜的問題，惟本行仍須關注 DLT 應用之脈動與發展，並適時與國內外專家、學者持續交流，以利未來 DLT 技術成熟時，可適時應用在支付系統相關業務領域。

---

[46] 例如，近期歐洲通過第二代支付服務法(Payment Services Directive, PSD2)，其中一項即要求銀行應開放 API 予新競爭者，以該等業者能在客戶同意下，連結客戶帳戶並協助進行各帳戶間之整合與管理。

[47] 例如比特幣與以太幣提出之閃電(lightning)與分片(sharding)方案，均規劃先將交易在鏈外處理並產生摘要資訊後，再將該資訊傳送至區塊鏈記錄，以降低區塊鏈系統之負荷並提高其處理效能。

(三) 加強研議對加密通貨交易平台及 ICO 之監管規範

1. 加密通貨交易平台

配合國際組織之呼籲並因應年底之亞太洗錢防制組織(APG)之評鑑作業，國內宜儘早規劃研議將虛擬通貨交易服務提供者納入洗錢防制管理體系。

短期似可參考 2018 年 1 月南韓採取之措施，銀行對於以實名制開立帳戶之虛擬通貨業者與其用戶，應進行盡職審查，並就業者與用戶有大額或疑似洗錢交易通報相關單位。

長期則須思考是否需將交易平台直接納管，要求其遵循防制洗錢規範，並就其相關業務、財務與資安控制等進行適度管理。

2. ICO

由於 ICO 發行之代幣可能屬於有價證券，爰須由證券主管機關個案認定，以遵循證券交易相關法令。

國內部分加密通貨交易平台業者已進行 ICO 籌資，並作為交易平台營運資金，其中未來將提供交易平台客戶進行融資融幣之槓桿交易；此等槓桿交易是否涉及期貨交易法第 3 條及 13 條規定，非依該法不得經營期貨交易所或期貨交易所業務，建議主管機關宜儘早釐清。

(四) 研議提升國內零售支付系統運作效能之方案

WEF 報告認為發行 CBDC 所帶來之風險超過其效益，且將大大影響目前央行對銀行、銀行對大眾之金融中介運作架構。因此，建議維持既有銀行與央行之傳統運作架構基礎下，提供創新零售支付服務。

基此，本行策略上宜先發展具效率之零售支付系統，除前已督促財金公司發展金融卡與信用卡之 QR code 共通標準外，考量近期國際間部分央行陸續推出新型態之零售快捷支付系統，如澳洲快捷清算服務系統(fast settlement service, FSS)、美國零售即時支付(real-time payment, RTP)系統等，本行似可就國際間新型態零售支付結算平台之運作模式進行委外研究，以研議進一步提升國內零售支付系統運作效能之方案。

附錄 1 各國央行應用 DLT 於跨行支付清算之主要測試結論

測試單位	完成時間	測試平台	測試內容	主要結論
加拿大央行	2016.6 Jasper 計畫,階段 1	Ethereum 私有鏈 (Quorum)	1、發行批發型 CBDC 2、應用 CBDC 於銀行間支付	1、採「工作證明」共識機制較無效率，可能二個節點同時完成區塊製作，使區塊鏈暫時分叉(Soft Fork)，造成交易清算最終性不確定。 2、交易資料未進行隱私保護加密處理。
	2017.5 Jasper 計畫,階段 2	R3 Corda	1、應用批發型 CBDC 於銀行間支付 2、測試 LSM 作業	1、交易未傳送給不相關節點，其優點為兩造間金融交易隱私受保護；缺點為各節點彼此資料不同，若某節點失去功能要回復作業時，向其他節點複製自己歷史交易資料的過程很複雜。 2、LSM 機制由央行單一節點處理各銀行傳送之多邊互抵支付指令,有單點失靈之虞。
	2018.5 Jasper 計畫,階段 3	R3 Corda	測試隱私保護下之同一 DLT 平台款券同步交割(DvP)作業	1、交易雙方之資訊不會被無關第三方得悉，可達金融交易隱私保護效果。 2、代碼化後之款、券在同一 DLT 平台上之 DvP 交割，其即時款券同步交換作業可降低交易對手風險，並可活化圈存擔保品之運用。
英國央行	2017.10	Ripple	模擬兩個 RTGS 大額清算系統,進行雙幣別跨境移轉	1、採用 Ripple 的跨帳本協定 (Inter-Ledger Protocol) 技術尚能同步處理兩種貨幣間之跨境移轉。 2、惟銀行間跨境支付需存放外幣資金於對方銀行之流動性需求問題，仍待解決。
巴西央行	2017.8	Ethereum 私有鏈 (Quorum)	1、發行批發型 CBDC 2、就核心業務進行簡單備援作業測試	1、DLT 技術尚不成熟，技術服務廠商亦未達到服務水準。 2、交易隱私仍為最大的挑戰，如欲達到隱私保護，則會損及系統運作效率及作業處理速度。

測試單位	完成時間	測試平台	測試內容	主要結論
新加坡貨幣管理局	2016.12 Ubin 計畫階段 1	Ethereum 私有鏈 (Quorum)	1、發行批發型 CBDC 2、CBDC 應用於跨行支付	1、需適合的法律架構以確保法定數位通貨移轉的效力。 2、此階段僅作基本項目測試，未評估效益。
	2017.11 Ubin 計畫階段 2	Corda、Hyperledger Fabric、Ethereum 私有鏈 (Quorum)	測試隱私保護下之 LSM 作業	1、以多節點進行多邊互抵結算作業屬新的突破；惟 DLT 處理速度較傳統中心化系統慢。 2、測試過程如交易排序作業等，仍仰賴單一節點處理，有單點失靈風險，而失去採用 DLT 之原意。
歐洲央行與日本央行合作	2017.9 Stella 計畫階段 1	Hyperledger Fabric	1、發行批發型 CBDC 2、測試 LSM 作業 3、認證單位與銀行節點當機後之復原作業	1、採用單一節點對參加單位進行身分辨識及 LSM 作業，有單點失靈風險。 2、交易資料未進行隱私保護加密處理。 3、ECB 與 BoJ 認為 DLT 技術仍不成熟，現階段尚無法實際應用在大額支付系統。
	2018.3 Stella 計畫階段 2 (詳細說明如附錄 2)	Hyperledger Fabric、Corda、Elements	1、相同 DLT 系統，款券在同一帳本之 DvP 2、跨 DLT 系統，款券在不同帳本之 DvP	1、若款、券均使用相同 DLT 平台，同屬一套帳本時，對款、券設定不同圈存時間之去中心作業，測試結果尚稱順暢。 2、惟款、券若分屬不同 DLT 平台時，在部分作業程序中斷，以及設定款、券圈存時間不當時，會發生款、券移轉至同一交易方，導致另一方承受風險的異常狀況。
荷蘭央行 (DNB)	2018.6 Dukaton 計畫	使用修改自比特幣區塊鏈共識演算及驗證機制之 4 個 DLT 平台	發行批發型 CBDC，並應用於跨行結清算	1、區塊鏈雖能提高支付系統復原性(resilience)，但存在擴展性、交易處理效能與效率不佳的情況。 2、DBN 認為現有支付系統運作甚具效率，且區塊鏈系統尚無法處理大規模交易。
南非央行	2018.6 Khokha	Ethereum 私有鏈	1、發行批發型	1、以 6 個實際(非模擬)節點實測，70,000 筆交易在 1 小時

測試單位	完成時間	測試平台	測試內容	主要結論
	計畫	(Quorum)	CBDC，應用於跨行結清算作業。 2、以零知識證明[48]之去中心作業方式，進行銀行間交易隱私之保護。 3、未測試LSM。	30 分 41 秒完成交易，每秒平均處理 12 筆交易。 2、測試結果符合南非央行預定之目標，包括：交易可使用 ISO 20022 訊息格式執行、交易處理規模達標、區塊廣播速度在 95%信賴度下 1 秒可完成；99%信賴度下 2 秒可完成、交易隱私獲得保護、央行節點可監看交易。 3、此次測試成功，並不表示會以 DLT 系統取代現有中心化系統，因為中心化系統尚有其他功能包括 LSM、央行日中透支機制等，均未納入本次測試。

資料來源：本文整理

[48] 係指在付款方的帳戶餘額及支付金額均加密情況下，區塊鏈上的其他節點仍可藉由零知識證明的特殊機制，驗證對該筆支付交易。

附錄 2 歐洲央行與日本央行第 2 階段 Stella 計畫聯合測試結果

一、背景說明

ECB 與 BoJ 於 2018 年 3 月間公布第 2 階段跨行支付及結清算之測試報告，本次測試主要著重在利用相同或不同 DLT 平台之款、券同步交割作業。本研究測試 Corda、Elements 及 Hyperledger Fabric 三個 DLT 平台。各 DLT 平台對雙方交易節點之交易記錄、儲存作法略不同，如下表示。

表 1　ECB 與 BoJ 測試使用之 DLT 平台及其主要特色

Corda	Elements	Fabric
每個節點各自維護並儲存自己相關之交易，沒有一個節點保存 DLT 平台上總帳資料。	每個節點均保存相同的總帳資料。	● 交易雙方銀行節點以通道(channel)為基礎相互連結，相同的通道上之節點保存相同之帳本資料。 ● 單一排序節點負責 DLT 平台上所有交易之排序，並持有所有跨通道之資料。

二、聯合測試主要研究結論

- DLT 可提供款券同步交割(DvP)作業：經測試後，包括款券在相同帳本之單一 DLT 平台，以及款券分屬不同帳本之不同 DLT 平台，均可執行 DvP 作業(詳圖 1)。
- 即使二個 DLT 平台未相互連結時，亦可採用「原子互換 (atomic swap)」技術完成 DvP 作業。
- 跨平台 DvP 作業尚有待解決之問題:部分作業程序中斷或設定款、券圈存的時間不當時，會發生款、券移轉至同一交易方，導致另一方承受風險的異常狀況，爰有須要再改進。

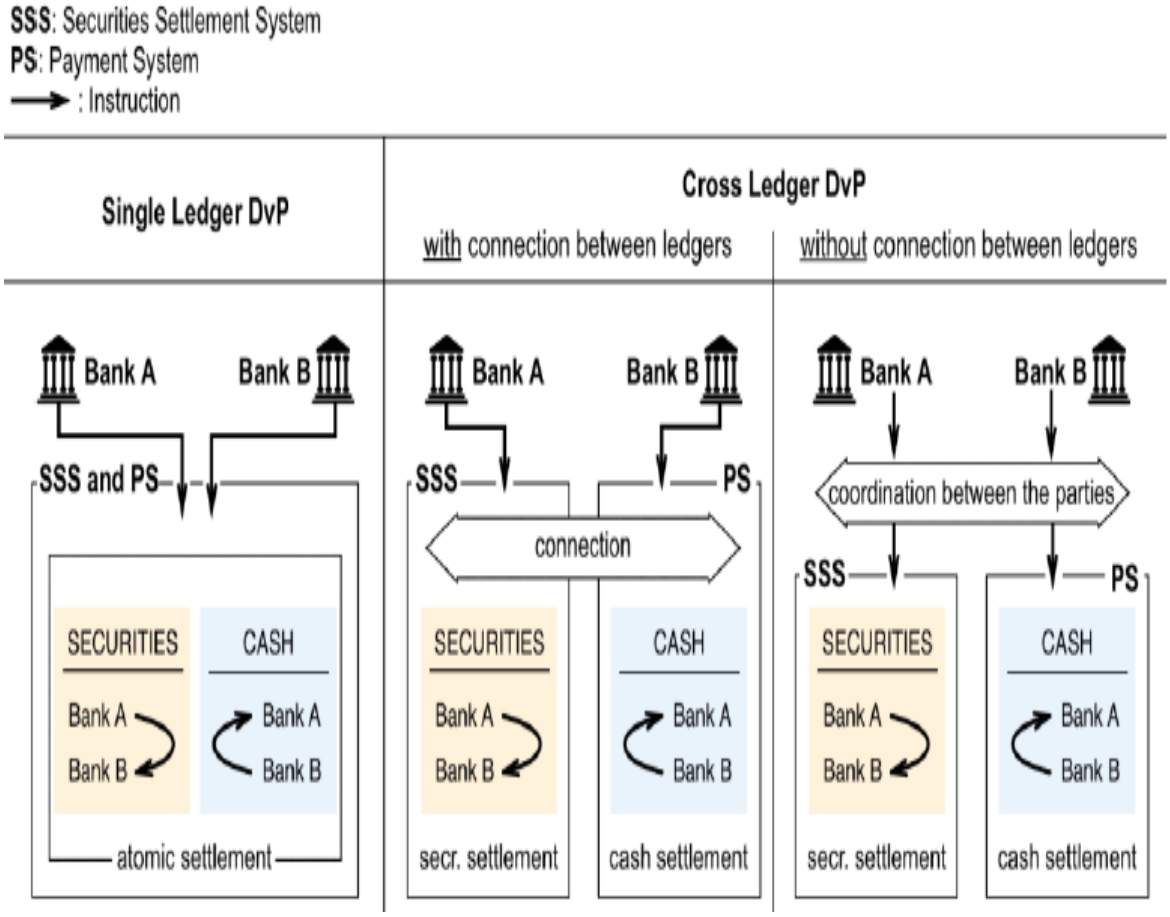
三、DvP 測試內容說明

本研究利用「原子互換(atomic swap)」技術進行二個不同平台間之 DvP 測試，該技術可執行二種不同虛擬通貨之自動化互換，無須經中

介機構處理。

原子互換係使用「鎖定時間雜湊合約」(Hashed Timelock Contracts，HTLC)」技術，主要係利用加密雜湊方式將雙方持有之資產個別圈存鎖定一段時間(如 1 小時與 2 小時)，如因故未完成正常作業程序時，會在鎖定時間終止時，將個別資產解除圈存，並退回給原持有人。

圖 1　款券在相同與不同 DLT 平台之同步交割示意圖

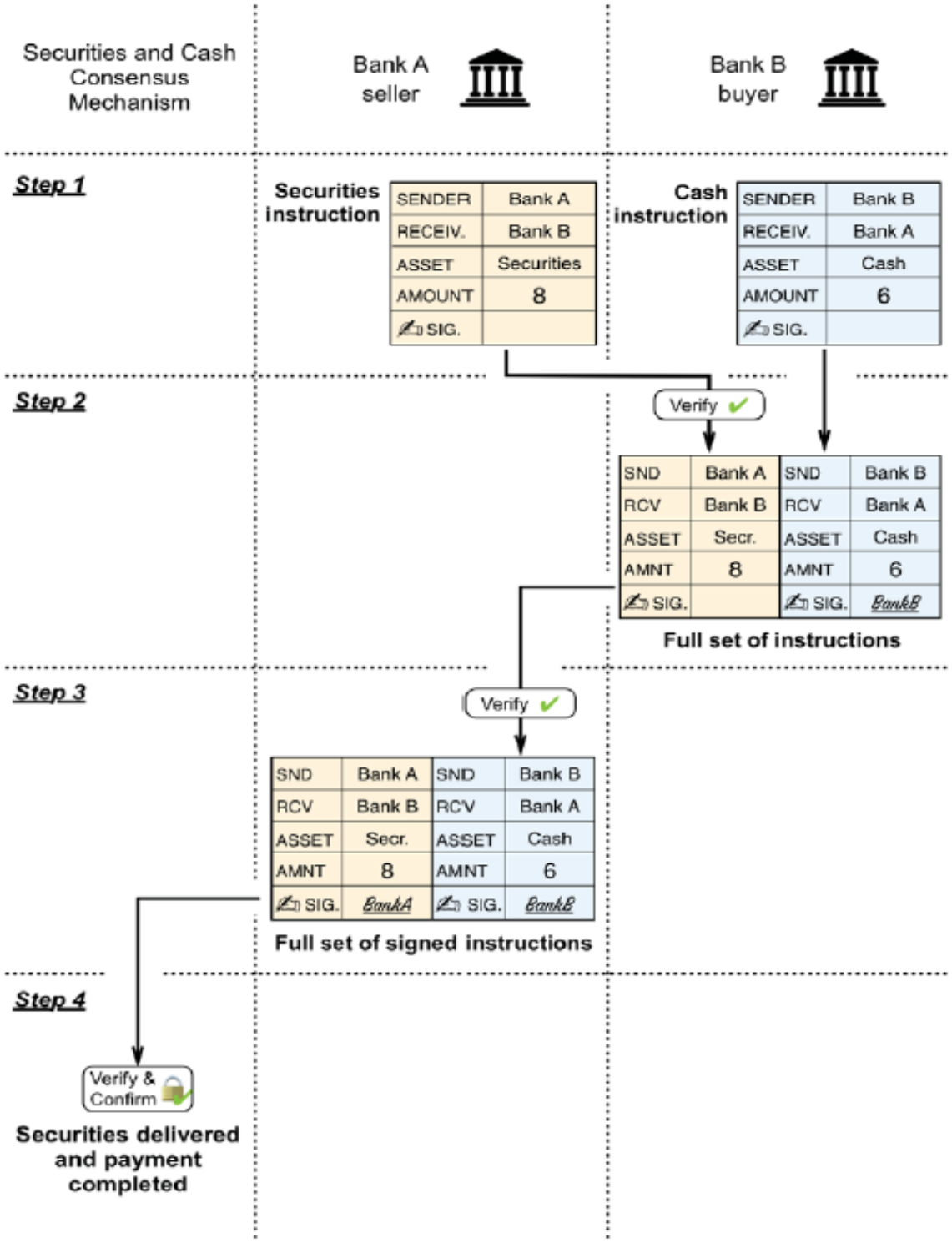


(一)款、券在同一 DLT 平台上之交割作業(詳圖 2)

- Step 1:A銀行(原持有證券)、B銀行(原持有款項)同時產生個別之券、款端支付指令，此階段雙方均尚未進行簽章。
- Step 2：A銀行傳送其證券支付指令給B銀行(A銀行先不簽章)，B銀行查驗A指令中之證券無誤後，將其款項支付指令與A之證券指令合併產生全套的DvP指令，由B簽章後發送給A。
- Step 3：A銀行查驗無誤並簽章後，傳送至DLT平台進行共識機制。

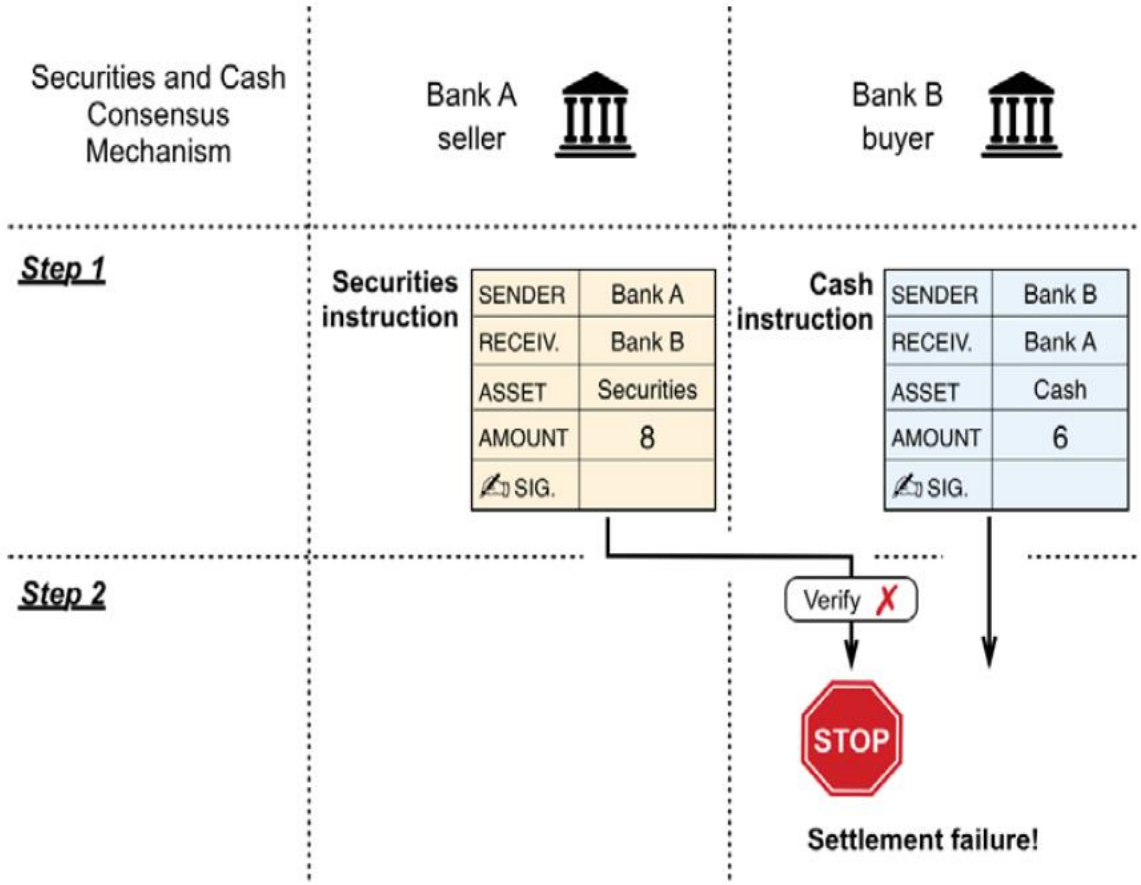
- Step 4：平台完成共識機制後，DvP指令被執行並寫入帳本(表示款、券完成相互移轉)。

圖2 款、券在同一DLT平台之交割流程



前述過程如有任何異常，而造成作業中止時，整個作業在 Step 2 會停住，款券會分別退回給原持有人(詳圖 3)，亦不會發生款、券均移轉至同一方之異常結果。

圖 3 款、券在同一 DLT 平台之交割流程



(二) 款、券在不同 DLT 平台之交割作業

1、成功 DvP 交割之作業流程

涉及兩個不同 DLT 平台之款、券同步作業時，因指令要傳送至其他 DLT 平台須完成共識後再送出，除跨鏈作業時間變長外，在部分假設情境下，會產生款、券同時移轉至單一交易方的不合理情況[49]。

若作業過程有問題，可能產生兩種交割失敗(settlement fails)情況，

[49] 現有具中間管理單位的中心化作業下，不會產生款、券都同時移轉至同一方之異常情況。

第 1 種情況款、券分別會退回原持有方，此情況尚不致產生本金風險(principal risk)[50]；第 2 種情況款、券可能均移轉至同一銀行，使另一方產生風險。

以下說明正常情況之作業流程，假設證券持有方 A 先發動交易指令，且 A 設定之資產圈存時間 2 小時，而款項持有方 B 設定之款項圈存時間為 1 小時。

- Step 1：產生第 1 次證券支付指令，A 銀行(原持有證券)產生一個密碼(secret)*x* 值及雜湊值 Y=H(*x*)，並將 Y[51]傳給 B 銀行。雜湊值 Y 為單向函數，B 銀行無法由 Y 值反推出 *x* 值。A 銀行產生證券支付指令，並載明以下 2 個條件：(1)若 B 能提出滿足 Y=H(*x*)的 *x* 值給 A，則可取得證券；或者(2)經 2 小時後，若 B 未回覆 *x* 值，證券退回給 A[52]。A 銀行將指令簽章，並傳送至證券端 DLT 帳本進行共識。
- Step 2：第 1 次證券支付指令經證券 DLT 平台共識、確認後，寫入帳本。
- Step 3：B 銀行(原持有現金)收到 Y=H(x)，並查驗 A 傳送之指令內容無誤後，產生第 1 次的款項端支付指令，並載明以下 2 個條件：(1)若 A 能提出滿足 Y=H(*x*)的 *x* 值給 B，則可取得現金；或者(2)經 1 小時後，若 A 未回覆 *x* 值，款項退回給 B。B 銀行將指令簽章，並傳送至款項端 DLT 帳本進行共識。
- Step 4：第 1 次款項支付指令經款項端 DLT 平台共識、確認後，寫入帳本。
- Step 5：A 查驗 B 銀行第 1 次款項支付指令內容無誤後，接著，A 產生第 2 次款項指令並提供 *x* 值給 B 而取得款項(但仍須待 Step 6 寫入 DLT 帳本才算確實取得)，再傳送至款項端 DLT 進行共識。

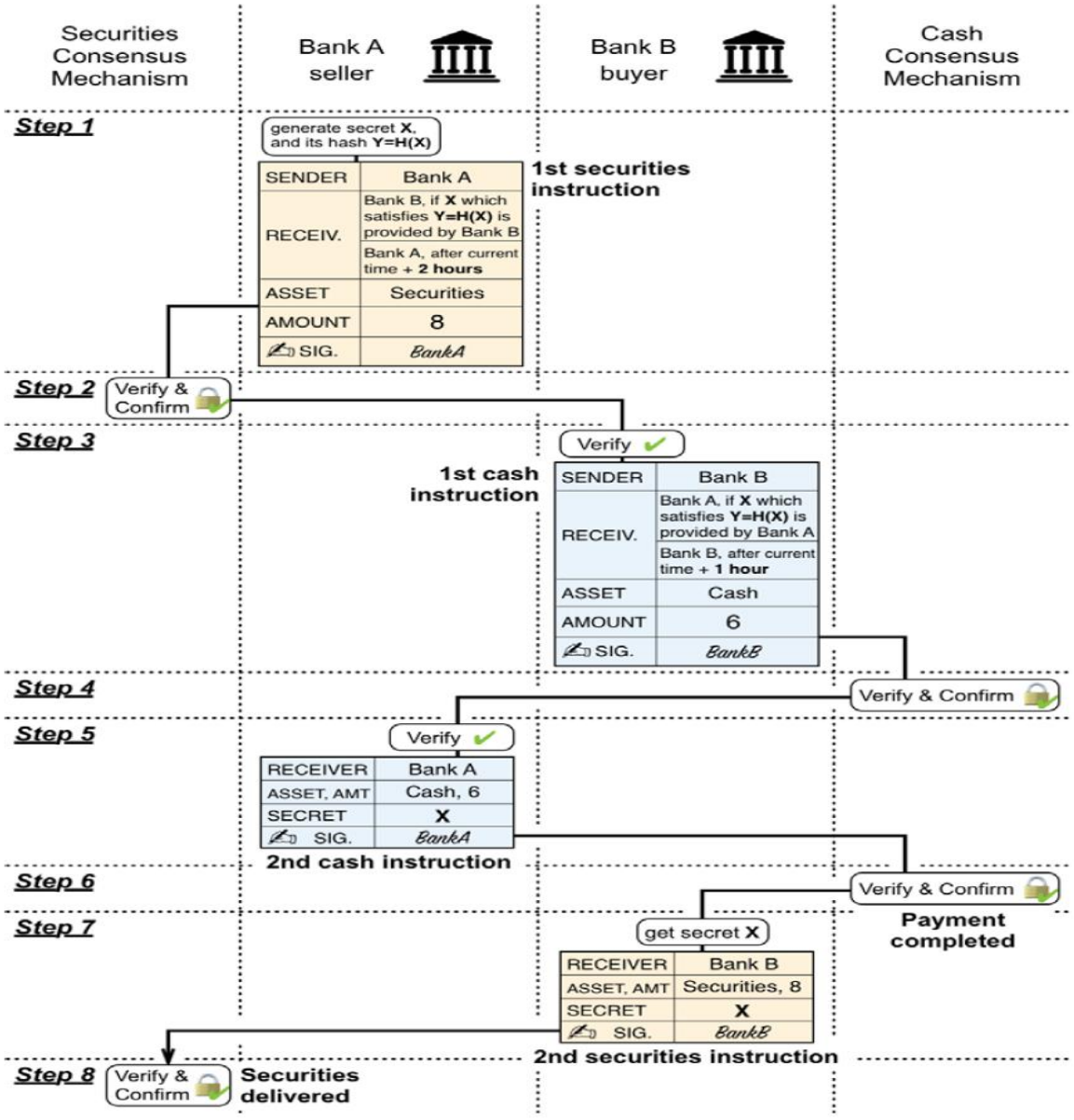
[50] 本金風險係指已付出資產但卻未收到 DvP 相對應收到之資產。

[51] 可想像成 Y 是一個密碼鎖頭，x 是解鎖的密碼值；而 A 買了二個密碼鎖頭 Y 並設定相同的密碼值 x 後，將其中一個鎖頭寄給 B，接著，A 及 B 均將款、券資產上鎖，以避免 DLT 上其他對手打開取得資產。

[52] 可能因為 B 提不出 x 值或其他作業因素導致交易中斷所致。

- Step 6：款項端 DLT 完成共識，將第 2 次款項指令寫入款項端 DLT 帳本，完成款項移轉。
- Step 7：B 銀行取得第 2 次款項指令中附帶之 *x* 值。接著，B 產生第 2 次證券指令，並提供 *x* 值給 A 而取得證券(但仍須待 Step 8 寫入 DLT 帳本)，再傳送至證券端 DLT 進行共識。
- Step 8：證券端 DLT 完成共識，將第 2 次證券指令寫入證券端 DLT 帳本，完成證券移轉。

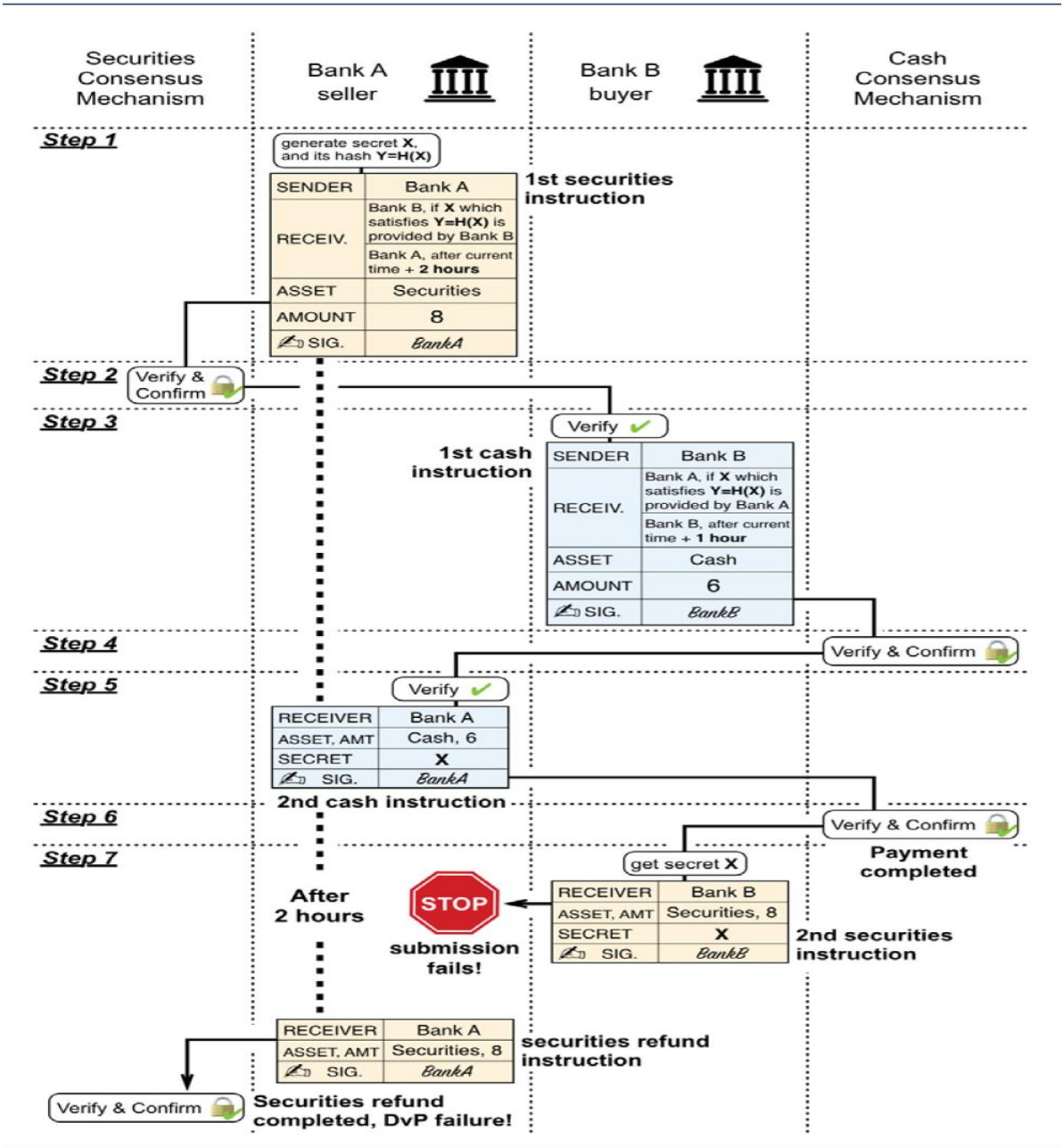
圖 4 款、券在不同 DLT 平台之正常交割結果



2、交割失敗情況款、券均移轉至同一方

如圖 5 示，若流程在 Step 7 作業中斷，將造成交割失敗。此時，A 銀行已完成 Step 6 送出 *x* 值並取得款項，但 B 銀行傳送第 2 次證券指令後，可能因 B 本身連線中斷，指令仍無法傳送至證券端 DLT 進行共識及查驗作業，因逾 2 小時，系統便將證券退回給 A 銀行。此情況下，將導致 A 銀行同時持有款與券，使 B 銀行承受風險。

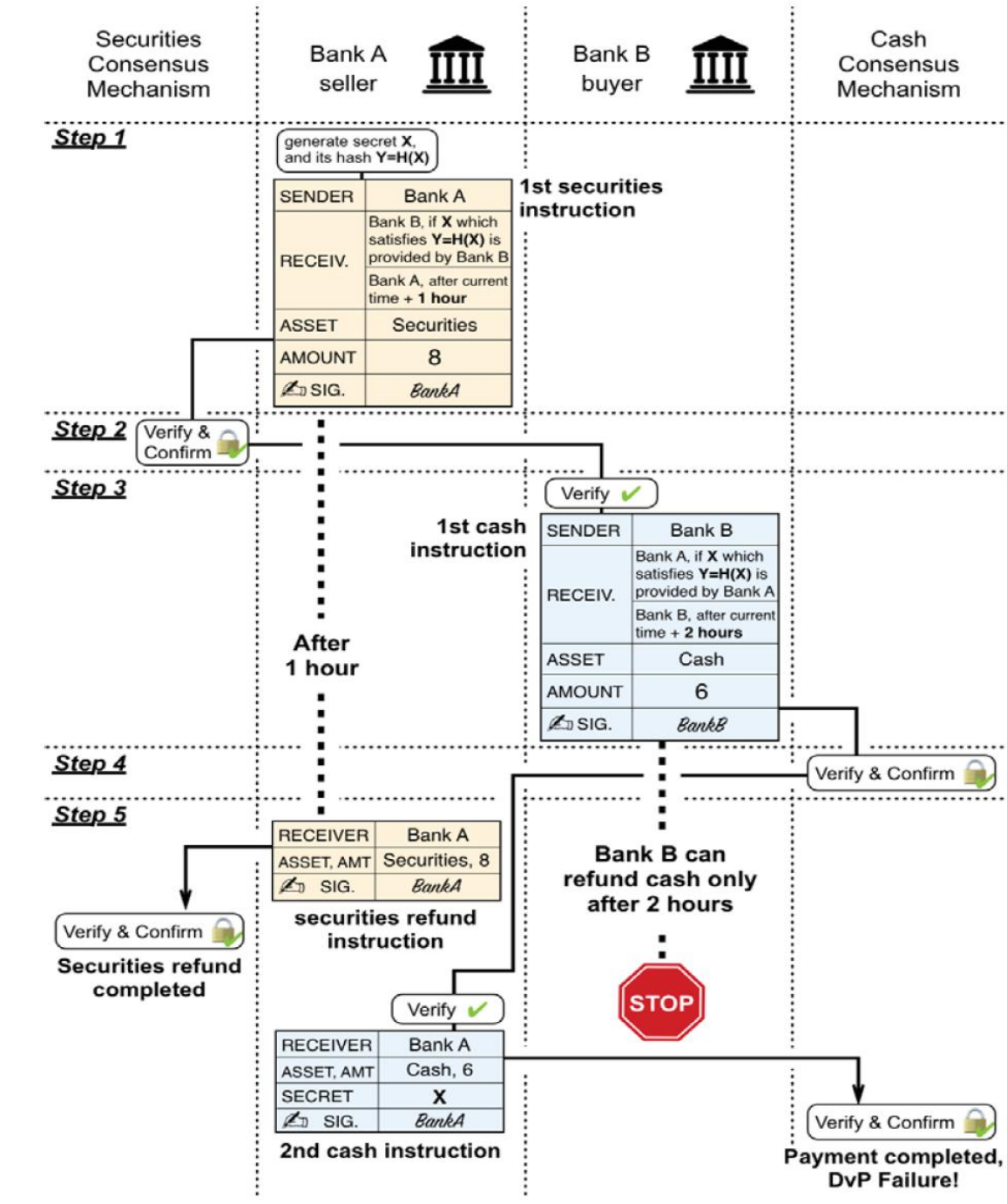
圖 5 款、券在不同 DLT 平台之異常交割結果-連線中斷



3、款、券圈存時間不對亦會發生均移轉至同一方的情況

以下案例說明證券與款項之圈存時間長度必須不同，且首次發送指令之資產圈存時間應較長，否則，即使系統未發生前揭連線中斷情況，亦會產生款、券都移轉至同一方的情況。

圖 6 款、券在不同 DLT 平台之異常交割結果-圈存時間設定不對



如圖 6 示，若 A 之證券指令圈存時間 1 小時，而 B 之現金指令圈存為 2 小時，只要 A 在介於 1 小時與 2 小時的任何時間才發送 step 5 指令將 x 給 B，即可同時取得款與券。因為逾 1 小時後，系統自動將證券退回給 A，若 A 再產生第 2 次款項指令並將 x 傳給 B，經款項端 DLT 完成共識決後，A 便會同時又持有款項。

- Step 1：產生第 1 次證券支付指令，A 銀行(原持有證券)產生一個密碼(secret)*x* 值及雜湊值 Y=H(*x*)，並將 Y 傳給 B 銀行。雜湊值 Y 為單向函數，B 銀行無法由 Y 值反推出 *x* 值。A 銀行產生證券支付指令，並載明以下 2 個條件：(1)若 B 能提出滿足 Y=H(*x*)的 *x* 值給 A，則可取得證券；或者(2)經 1 小時後，若 B 未回覆 *x* 值，證券退回給 A。A 銀行將指令簽章，並傳送至證券端 DLT 帳本進行共識。
- Step 2：第 1 次證券支付指令經證券 DLT 平台共識、確認後，寫入帳本。
- Step 3：B 銀行(原持有現金)收到 Y=H(x)，並查驗 A 傳送之指令內容無誤後，產生第 1 次的款項端支付指令，並載明以下 2 個條件：(1)若 A 能提出滿足 Y=H(*x*)的 *x* 值給 B，則可取得現金；或者(2)經 2 小時後，若 A 未回覆 *x* 值，款項退回給 B。B 銀行將指令簽章，並傳送至款項端 DLT 帳本進行共識。
- Step 4：第 1 次款項支付指令經款項端 DLT 平台共識、確認後，寫入帳本。
- Step 5：
  (1) A 查驗 B 銀行第 1 次款項支付指令內容無誤後，接著，A 產生第 2 次款項指令並提供 *x* 值給 B，經款項端 DLT 完成共識，A 即取得款項。
  (2) B 銀行取得前述 x 值後，原本需再產生第 2 次證券指令並傳送 x 值給 A，以使得 B 取得證券；惟因 A 圈存時間 1 小時內並未收到

B 回傳之 x 值[53]，系統自動在 1 小時後自動製作證券指令，將證券返還給 A，導致 A 同時持有款與券。

[53] 此案例顯示，A 只要在超過其證券圈存時間 1 小時以後發送 x 值給 B，即可同時持有款與券。

參考資料

中文部分

中央銀行理監事會後記者參考資料(民國 107 年 6 月)，「虛擬通貨與首次代幣發行(ICO)之發展近況、風險及監管重點」。

英文部分

1. Bech, Morten and Rodney Garratt (2017), "Central Bank Cryptocurrencies," BIS Quarterly Review, Sep.
2. Berentsen, Aleksander (2018), "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies," Economic Research, Federal Reserve Bank of St. Louis, Apr.
3. BIS Research (2017), "Blockchain Technology in Financial Services Market - Analysis and Forecast: 2017 to 2026," Jul.
4. BIS (2018a), "Central Bank Cryptocurrencies," Mar.
5. BIS (2018b), "Cryptocurrencies: Looking Beyond the Hype," BIS Annual Economic Report - Chapter V, Jun.
6. Central Banking (2018), "SNB Reject Idea of Retail Central Bank Digital Currency," Central Banking Newsdesk, Apr. 6.
7. Davoodalhosseini, Mohammad and Francisco Rivadeneyra (2018), "A Policy Framework for E-Money: A Report on Bank of Canada Research," Bank of Canada Staff Discussion Paper, 2018-5, April.
8. ECB and BoJ (2017), "Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment," STELLA - a joint research project of the European Central Bank and the Bank of Japan, Sep.
9. ECB and BoJ (2018), "Securities Settlement Systems: Delivery-Versus-Payment in a Distributed Ledger Environment," STELLA - a joint research project of the European Central Bank and the Bank of Japan, Mar.

10. Fatás, Antonio and Beatrice Weder di Mauro (2018), “Here’s Why Central Banks Shouldn’t Play Cryptocurrencies at Their Own Game,” WEF, May.
11. Financial and Technology Proposal (2018), “Petro White Paper,” Mar.
12. Hileman, Garrick and Michel Rauchs (2017), “Global Blockchain Benchmarking Study,” Cambridge Centre for Alternative Finance.
13. HKMA (2017), “Whitepaper 2.0 on Distributed Ledger Technology,” Oct.
14. IMF (2017), “Fintech and Financial Services: Initial Considerations,” Staff Discussion Note, Jun.
15. Jerome, Powell H. (2017), “Innovation, Technology, and the Payments System,” Remarks at Roundtable of Blockchain: The Future of Finance and Capital Markets, Board of Governors of the Federal Reserve System, Mar.
16. Kumhof, Michael and Clare Noone (2018), “Central Bank Digital Currencies – Design Principles and Balance Sheet Implications,” Bank of England Staff Working Paper, No. 725, May.
17. MAS and Deloitte (2017), “The Future Is Here Project Ubin: SGD on Distributed Ledger”.
18. Mersch, Yves (2018), “Virtual or Virtueless? The Evolution of Money in the Digital Age,” a lecture by member of the executive board of the ECB, Feb.
19. Norges Bank (2018), “Central Bank Digital Currencies,” Norges Bank Papers, No.1.
20. Risksbank (2017), “The Risksbank’s E-Krone Project,” Sep.
21. WEF (2018), “Here’s Why Central Banks Shouldn’t Play Cryptocurrencies at Their Own Game,” May.