

國際間跨境支付 應用區塊鏈之試驗研究

陳永祚

中華民國 113 年 4 月

作者任職於中央銀行，本文內容純屬個人意見，與服務單位無關，如有錯誤概由作者負責。

摘 要

現今國際間的跨境支付效率不佳，採用新興的技術或許有可能改進跨境支付的效率，透過相互介接各國的央行數位貨幣(Central Bank Digital Currency, CBDC)系統，形成多幣別 CBDC(mCBDC)體系是一種可能改善的方法。本文探討國際間採用區塊鏈技術或分散式帳本技術(Distributed Ledger Technology, DLT)試驗跨境支付的各種方案，包括如何運用區塊鏈技術在系統中發揮可能的潛在效益，這些改進對於現行透過代理銀行服務的新興市場經濟體特別重要；各國中央銀行可以評估將其研究成果納入改善現行跨境支付系統的可能性。

BIS 對於 CBDC 跨境支付系統提出了 3 種可能的模型：相容型(compatible)、介接型(interlinked)及單一型(single)，本文將就各個模型的架構設計、系統特性及其優缺點進行探討。

近年來隨著加密資產的崛起，其背後所使用的區塊鏈技術亦備受矚目，國際間也開始了許多採用區塊鏈技術試驗跨境支付的專案，如：Inthanon-LionRock2、Jura、Dunbar、mBridge 等，本文亦詳細闡述各專案之系統架構、技術平台及業務流程，並就各專案之異同進行比較與探討。

目 次

壹、跨境支付系統模型	1
一、相容型 CBDC 系統(Compatible CBDC Systems).....	2
二、介接型 CBDC 系統(Interlinked CBDC Systems).....	3
三、單一型 mCBDC 系統(Single mCBDC System)	5
貳、國際間跨境支付試驗專案	7
一、Inthanon-LionRock2 專案.....	7
二、Jura 專案.....	11
三、Dunbar 專案	15
四、mBridge 專案	18
參、國際間跨境支付試驗專案之比較	22
肆、結語	24
參考文獻.....	25

圖 目 次

圖 1、模型 1：多幣別 CBDC 跨境支付安排基於相容型 CBDC 系統.....	2
圖 2、模型 2：多幣別 CBDC 跨境支付安排基於介接型 CBDC 系統.....	4
圖 3、模型 3：多幣別 CBDC 跨境支付安排基於單一型 mCBDC 系統.....	5
圖 4、Inthanon-LionRock2 跨境支付模型架構.....	8
圖 5、Jura 專案跨境模型架構.....	12
圖 6、Dunbar 專案跨境模型架構.....	15
圖 7、mBridge 專案跨境模型架構.....	19

表 目 次

表 1、跨境支付試驗專案之比較	22
-----------------------	----

壹、跨境支付系統模型

跨境支付對經濟發展越來越重要，尤其是在旅遊業、電子商務和匯款，這些交易在過去十年中都大幅增長，然而這樣的支付交易通常處理速度緩慢、不透明和費用昂貴。改進跨境支付系統是全球努力的重要事項，除了推動改進現有系統外，各國央行還在探索央行數位貨幣(CBDC¹)可能給跨境支付服務帶來的機會，這是對於提高跨境支付效率的重要動力。

多幣別跨境支付比國內支付更複雜，以不同貨幣清算會增加風險和成本。如今在大多數跨境支付中，貨幣轉換通常涉及多方，各國的規範和監管標準也可能不同，這增加了阻力和風險。

提升支付系統之間的互通性(Interoperability)有助於減少阻力，這是一個廣義的術語，它可能包含幫助系統交換信息等各種層面，現今支付系統透過三種不同方式實現了跨境和跨貨幣互通性：

- 1.相容的標準(例如類似的監管框架、市場慣例、訊息格式和資料要求)。
- 2.透過技術介接，採用共同的結算機制或相關方案。
- 3.透過建立單一的多幣別支付系統。

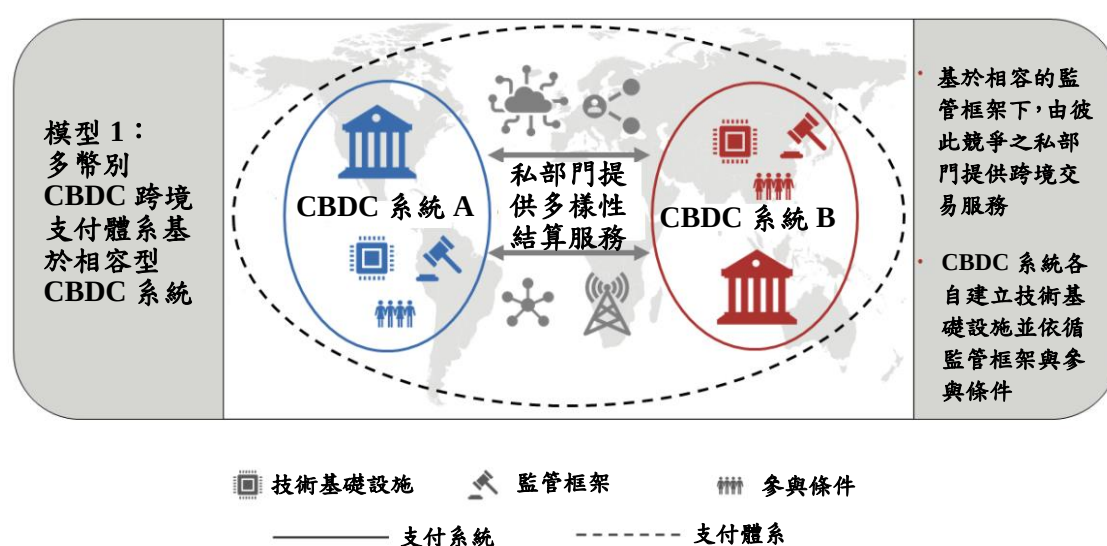
支付系統(system)和支付安排(arrangement)不同，支付系統具有營運機構維護一個單一的規則並控管整個系統，而支付安排則缺乏這種統一的協議，透過使用相容標準、相互介接或是單一的多幣別支付系統可以提升互通性以形成多幣別支付安排。

¹ CBDC 是一種被各國央行廣泛研究的新型數位貨幣，已有少數國家開始發行和試點。

一、相容型 CBDC 系統(Compatible CBDC Systems)

支付系統可採用相容的標準以減少阻力和障礙，並利用支付系統的多樣性，提供不同的選擇和競爭，使跨境支付更快、更便宜及更透明。許多國家選擇採用混合型 CBDC²架構進行試驗，其中私部門將處理面對客戶的所有交易，這種「分層」的設計使得第一種相容型 CBDC 系統看起來可能與傳統支付系統非常相似³(圖 1)。

圖 1、模型 1：多幣別 CBDC 跨境支付體系基於相容型 CBDC 系統



資料來源：Raphael Auer, Philipp Haene and Henry Holden (2021)

在相容型 CBDC 系統模型中，就像任何的支付方式一樣有通用技術標準，例如訊息格式、加密技術、資料要求和用戶界面，以減少參與多個系統的操作負擔，共通的合規和監管標準可以簡化 KYC 和交易監控流程。

然而，如果沒有在政治上的協調行動，推行相容的標準需要花費大量時間；協調龐雜的市場參與者移轉到通用訊息標準或調整法律框架，有時被銀行和支付服務提供商認為是最大的阻力來源。歷史已經

² Auer, Raphael and Rainer Böhme (2020)

³ 皆透過私部門來提供終端用戶服務。

證明，即使有央行和政治上的支持，任何形式的協調都可能需要數年時間，例如單一歐元支付區(SEPA)。

基於相容型的 CBDC 系統可按照國際標準設計，可能可從其簡潔的設計來獲益，並鼓勵私部門參與以提升多樣性，提供更多的選擇以及更廣泛的跨境支付生態系統競爭。然而，鑑於它們類似於傳統的跨境支付安排，面臨的一些問題可能相同，即使有更多樣性的潛力，現存有較多資源的銀行可能具有優勢，導致跨境支付服務的集中度。

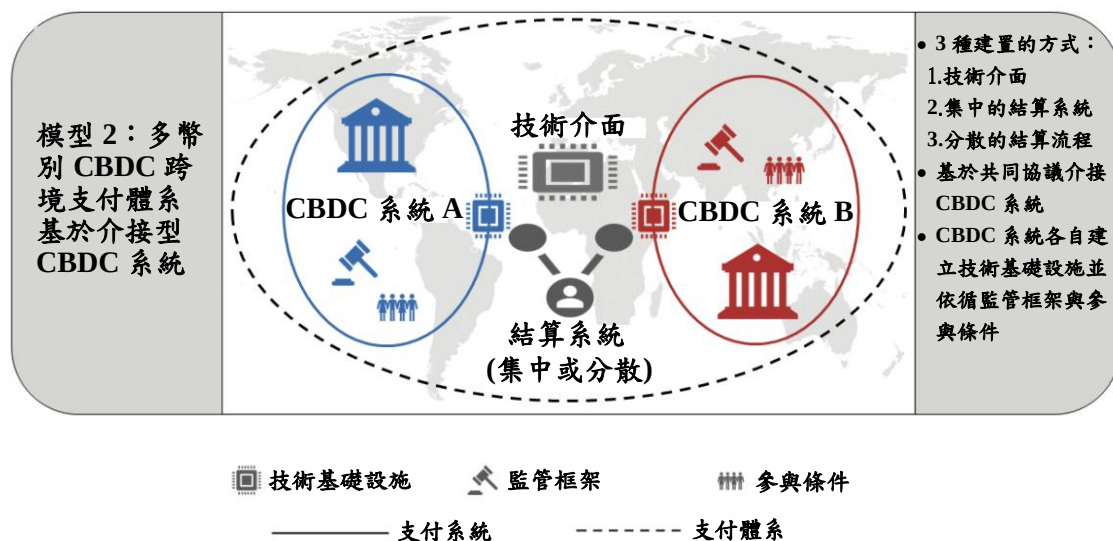
二、介接型 CBDC 系統(Interlinked CBDC Systems)

介接支付系統是一項複雜的任務，通常需要相應的措施，如果將支付比喻作支付系統的「管道」，那麼介接支付系統就是將水管與不同的壓力或流量的水管串接起來；簡單地將它們連接在一起是行不通的，其中的閥門和控制器是必須的，所以介接支付系統中的協議和營運安排相當重要，這可以藉由兩種形式實現：(1)共享技術介面；或(2)通用結算機制(可以透過去中心化的往來帳戶或中心化的結算系統處理)。

一個共享的技術介面，是經由雙方共同協議，允許一個系統的參與者向另一個系統的參與者付款(圖 2)，許多國家的 CBDC 試驗已經對這種方法進行了測試(例如歐洲央行和日本央行⁴)；通用結算機制則採用不同的方法，透過清算帳戶介接系統，清算帳戶可以是分散式或是集中式，例如東非支付系統(EAPS)，參與的中央銀行在對方系統中各持有一個帳戶，可以進行付款和收款；或例如歐洲 TARGET，各國央行集中參與系統並使用帳戶進行清算，另外更集中的方式可以採用受信任的中介機構作為各參與央行的清算中心。

⁴ European Central Bank and Bank of Japan (2019)

圖 2、模型 2：多幣別 CBDC 跨境支付體系基於介接型 CBDC 系統



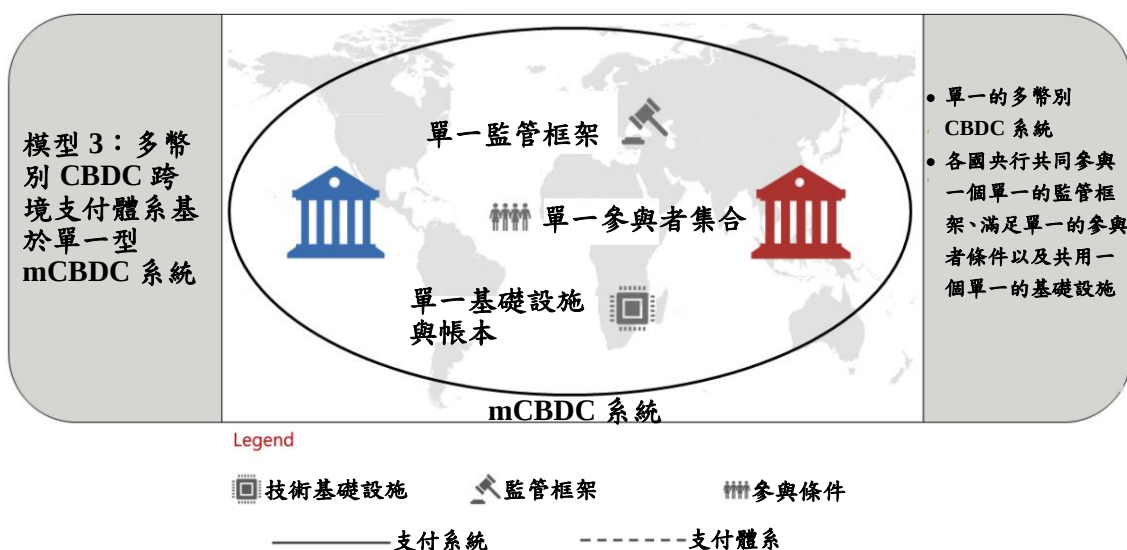
資料來源：Raphael Auer, Philipp Haene and Henry Holden (2021)

儘管存在多種介接選項，但沒有一個是容易實現的，過去的歷史顯示，許多項目並沒有帶來預期的收益，甚至即使進行了大量投資仍無法進入運營階段。雖然透過試驗證實了介接 CBDC 系統的技術可行性，然而，介接一個真正的支付系統不僅須確保營運基礎設施更具可擴展性、安全性和彈性，也須協調許多利害相關者和參與者，就像在傳統系統中一樣，這些工作會隨著每一 CBDC 系統的增加而倍增。建立健全的生態系統，並採取多種激勵措施，讓其中的參與者能以安全有效地使用系統是一項的重要任務，若僅介接系統而沒有投入更廣泛的協調與引入法規的相容性，不足以實現高效的跨境支付。

三、單一型 mCBDC 系統(Single mCBDC System)

除了介接雙方國內 CBDC 系統的方法，跨境支付系統也可以是涉及多方多幣別的 CBDC 系統（圖 3）。mCBDC 系統(單一型多幣別 CBDC 系統)採用傳統的多貨幣類別，有單一的監管框架和存取限制，與介接型的最大差異是參與者直接連接到他們的「共用系統」，這種更深入的系統整合可能可以實現更多的操作功能和提高效率，但也增加了治理和掌控的困難，例如，更多的連結可能會提高清算效率，但會增加其他風險。

圖 3、模型 3：多幣別 CBDC 跨境支付體系基於單一型 mCBDC 系統



資料來源：Raphael Auer, Philipp Haene and Henry Holden (2021)

mCBDC 系統的設計可能與傳統的支付系統差異很大。針對不同的業務特性，可能也可以存在多個 mCBDC 系統；例如，更多以「零售」為重點的 mCBDC 系統，可以專注於更高的交易量能、較小額度的跨境支付，以及允許更多的參與者使用；而以「批發」為重點的 mCBDC 系統，則優先考慮大額的即時支付。另外，也可以採用新技術，例如 CBDC 可以透過區塊鏈技術採用一個分散式的帳本，在技

術上比介接不同的系統更簡單；然而，一個單一的 mCBDC 系統產生了一系列的治理問題，管理共用的系統監管框架和治理事務只是一方面，各國央行可能都需要在最終設計中，對於貨幣政策、金融穩定和支付規範進行權衡，例如，各國央行將需要評估他們是否願意放棄一些對於系統運營的控制和監管。因此在多個中央銀行之間就這些治理協議進行權衡與談判，將是一個挑戰。

mCBDC 系統理論上可以採用新技術來探索以前無法做到的複雜功能，例如通過分散式帳本系統中的監控、管制和分割，代幣化形式的 CBDC 可以存在於中央銀行之外，因此理論上可以實現和傳統不同且更具整合性的模型，其中所有貨幣可以在一個分散式帳本上清算。雖然使用私人的加密資產清算也是可以做到的，但它的安全性可能不如使用 CBDC 系統來清算交易。

貳、國際間跨境支付試驗專案

CBDC 可以幫助提供更好的跨境支付服務，因此全球超過 90% 的國家央行都在探索 CBDC，無論是在概念上還是從技術上，或是零售型以及批發型。批發型 CBDC 的研究工作更是受到越來越多的跨境支付效率相關的因素驅動，G20 已將加強跨境支付作為優先事項，批准了一項由 19 個項目組成的綜合計畫，來應對這項關鍵挑戰，其中一項具前瞻性項目便是考量如何以國際角度來設計 CBDC 以解決跨境支付效率問題，國際清算銀行創新中心(BISIH)亦響應 G20 號召協調各國進行試驗，近期已經完成了數個與世界各地中央銀行和私部門合作的跨境 CBDC 項目，包括：Inthanon-LionRock2(ILR2)、Jura、Dunbar 和 mBridge 等專案，分別說明如次：

一、Inthanon-LionRock2(ILR2)專案

2021 年 9 月，BISIH 香港中心與香港金融管理局（HKMA）和泰國央行(BoT)共同完成 ILR2⁵專案，ILR2 是建立在 HKMA 和 BoT 最初的 Inthanon-LionRock 項目之上，該項目的目標是探索使用區塊鏈技術或是分散式帳本技術(DLT)，促進跨國之間的資金移轉效率，實現具有原子性⁶的即時外匯(FX)交易 PvP⁷機制。

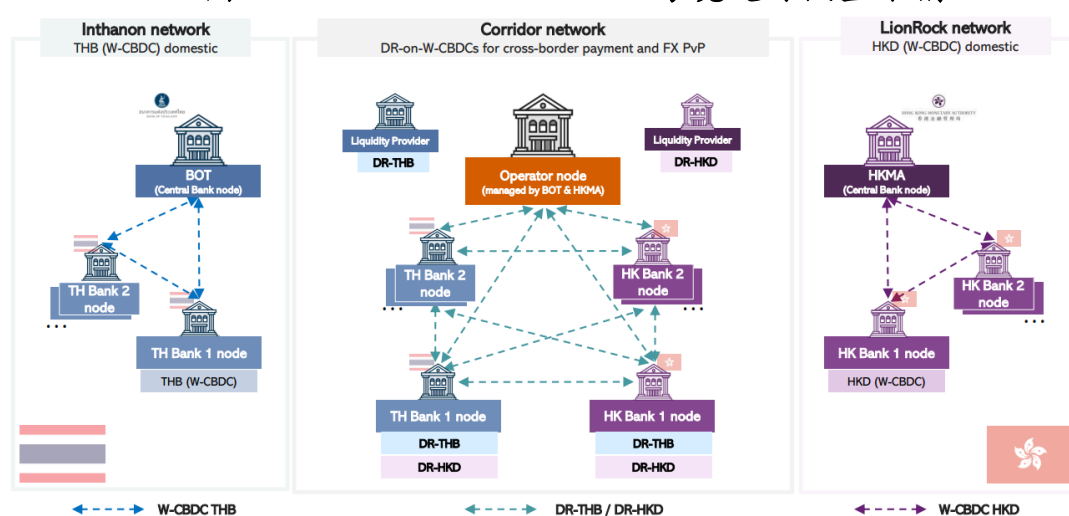
⁵ BISIH, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates (2021)

⁶ 原子性 (Atomicity)，即一個交易 (transaction) 中的所有操作，或者全部完成，或者全部不完成，不會結束在中間某個環節，例如款與券的交易同時交割，不會只有單邊完成。

⁷ Payment vs. Payment(PvP)，於外匯交易時進行的雙邊同步支付清算機制。

該試驗展示了使用 CBDC 和 DLT 技術提供即時、更低成本和更安全的跨境支付清算，系統平台實現了「秒級」跨境轉帳，相對於過去需要幾天的時間；它也展示了降低多項成本的潛力，代理銀行的業務成本最多可以減少到一半，這部分可以透過使用區塊鏈技術中的智能合約來實現，運用演算法來實現流動性節省機制，以減少往來的流動性、資金運作、外匯交易和合規成本。

圖 4、Inthanon-LionRock2 跨境支付模型架構



資料來源：Hong Kong Monetary Authority and Bank of Thailand (2020)

試驗採用的跨境系統模型屬於單一型的 mCBDC 系統，模型架構如圖 4，模型中有三個網路系統，分別是兩個國內的 CBDC 網路系統：Inthanon(泰國)與 LionRock(香港)，以及一個跨境的 mCBDC 走廊 (Corridor)網路系統。在國內的網路系統中，央行負責發行及贖回本國的批發型 CBDC(wholesale CBDC, wCBDC)代幣，國內的系統與跨境系統是完全分離的，跨境交易及非本國銀行是無法存取國內的網路系統。

模型中有一個特別為跨境交易設計的網路系統稱為「走廊 (Corridor)」，各國的銀行可以加入這個網路進行跨境交易，在這個網

路中，交易的代幣稱為存託憑證(DR)，參與的銀行可以持有不同幣別的 DR 並進行交易。另外，還設計了一個流動性節省機制可以處理交易僵局⁸(Gridlock)的問題。

在走廊網路中包含了幾個角色，分別是：營運節點(Operator node)、參與銀行節點及流動性提供者節點。營運節點是由兩國央行共同管理，它負責發行與贖回各幣別的 DR 代幣，以及提供處理交易僵局的服務和交易的合規監管；參與銀行節點則提供跨境交易服務，可以進行跨境轉帳、換匯等交易，同時也負責管理自行各幣別代幣的流動性；流動性提供者節點則是可以提供暫時性的借款，當交易流動性不足時，提供國外代幣的流動性。

國內的 wCBDC 和走廊網路上的 DR 轉換則是透過各自的央行來處理，例如泰國本地的銀行想要進行跨境支付向央行請求轉換，將 wCBDC 移轉至央行，央行銷毀對應的 wCBDC 並於走廊網路系統上發行 DR-THB 給對應的銀行做為跨境交易使用，反之亦然。

在走廊網路上各參與銀行可以自由的進行各幣別的跨境支付，例如：用本地代幣支付給外國銀行、用外國代幣支付給本國銀行或是用外國代幣支付給外國銀行，同時，換匯交易也可以在這個網路上進行。

ILR2 模型系統背後所採用的技術是區塊鏈技術，其中的交易處理、代幣發行、贖回、記錄帳本等功能皆是透過區塊鏈上的智能合約實作，交易區塊的驗證則是透過去中化的各驗證節點以共識完成；區塊鏈技術平台是使用 ConsenSys 公司的 Hyperledger Besu，它是一個認許制的企業版以太坊(Ethereum)區塊鏈，該專案選擇 Hyperledger Besu 的目的是評估如何透過以太坊區塊鏈去建構一個單一帳本多幣

⁸ 指參與之交易間產生資金互卡問題。

別的網路系統，而採用 Hyperledger Besu 是因為其技術平台的特性，包含隱私設計、靈活有彈性的共識機制以及技術支援的社群。

在試驗模型中，每個中央銀行都是一個驗證節點，負責驗證交易並透過共識生成區塊，每個商業銀行參與者則都是標準節點，可以讀取區塊鏈上的資訊並且發送交易。除此之外，所有的交易都會透過一個交易管理模組，這個模組負責系統中節點之間的隱私通訊，這樣網路中交易以外的所有其他參與者，都無法看到所涉及的機敏資訊。

交易的清算最終性是通過權威證明(Proof of Authority, PoA)共識機制實現的，PoA 是一種共識機制，可以有很多不同的實作，ILR2 模型系統選擇了伊斯坦堡拜占庭容錯⁹2.0 (IBFT 2.0)，IBFT 2.0 是適用於快速處理大量交易的企業級共識演算法，使用此共識機制，驗證節點向參與者提供清算最終性，將最終交易區塊發佈到區塊鏈網路上，這就是為何要將標準節點與驗證節點區分開來的原因，PoA 共識機制確保每筆交易必須得到三分之二的驗證節點的批准以完成交易最終性。

實現業務邏輯的方式是使用區塊鏈技術中的智能合約，在 ILR2 模型系統中所有的交易都是透過智能合約實現，系統中的 CBDC 資產是透過代幣來表示，它是採用公開的通用標準設計，通用標準提供了適應未來功能的靈活性，例如嵌入式合規設計或代幣化證券等功能，並允許模型系統與其他使用以太坊網路系統互通。

該專案透過 ILR2 模型系統，驗證了區塊鏈技術可以顯著增加速度、降低成本，並為複雜的跨境支付業務流程提供運營系統的效率和韌性，該專案進一步顯示，透過創新的技術解決方案可以管理流動

⁹拜占庭容錯(Byzantine fault tolerance, BFT)機制是在資訊科技領域的一種確保系統高可用性的容錯演算法，它容許一個分散式系統中在有 1/3 的節點毀損或惡意攻擊，系統仍可正常運作。

性、解決交易僵局，並提供有競爭力的外匯交易，同時滿足合規和監管，並支援未來的服務。

然而，值得注意的是，區塊鏈技術仍然存在一些局限性，例如隱私的設計會導致跨多個國境的 PvP 交易無法確保其原子性，同時也沒有一個單一國家可以查看所有的待處理外匯交易；平台上如果再增添更多的國家或幣別，仍需要進一步評估區塊鏈技術在處理大量交易時的可擴充性和效能，此外，完善的風險治理機制也需要被建立。

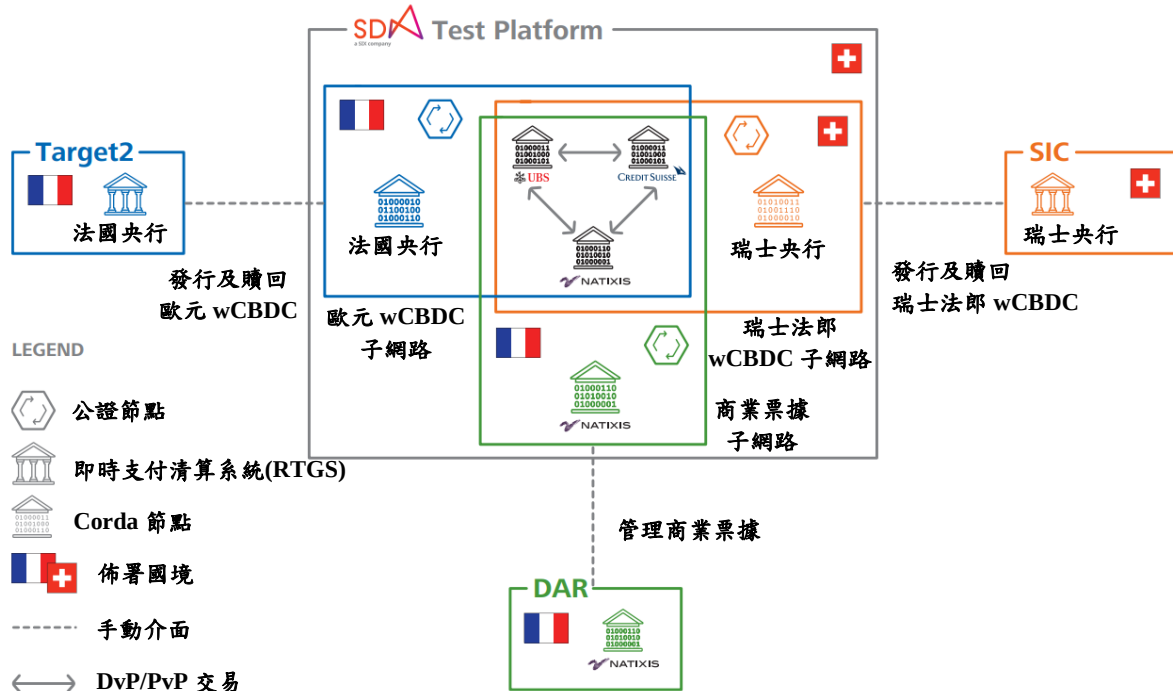
二、Jura 專案

BISIH 瑞士中心、瑞士央行、法國央行及 SIX Digital Exchange (SDX)公司共同合作在 2021 年 12 月發布了 Jura 專案¹⁰的試驗報告(圖 5)，Jura 專案探索了法國和瑞士的商業銀行以 wCBDC 在歐元和瑞士法郎之間的直接跨境轉帳，採用的系統是由第三方運營的單一 Corda DLT 平台，代幣化資產和外匯交易使用 PvP 和款券同步(DvP)機制進行清算，該試驗是在近乎真實的環境中進行的，使用真實的價值進行交易並遵守現行監管要求。

在第三方的平台上發行 wCBDC，並給予外國金融機構直接存取中央銀行貨幣會引發複雜的政治問題，Jura 專案探索了一種新方法，採用子網路和雙重公證機構的數位簽章技術，這可能可以讓央行安全的在第三方平台上發行 wCBDC 並授權外國金融機構存取 wCBDC。

¹⁰ BIS Innovation Hub, Bank of France and Swiss National Bank (2021)

圖 5、Jura 專案跨境模型架構



資料來源：BIS Innovation Hub, Bank of France and Swiss National Bank (2021)

Jura 專案的模型架構是由 4 個基礎設施組成：(1)法國央行 TARGET2 支付清算系統；(2)瑞士央行 SIC 支付清算系統；(3)DAR(Digital Assets Registry)數位資產管理機構；(4)SDX 試驗平台。其中 SDX 試驗平台是以 Corda DLT 技術建構的平台，該平台以去中心化點對點網絡上的各節點所構建而成，在「僅知原則 (need-to-know)」的基礎上運行，交易資料僅在交易雙方之間通信及保存，平台上的其他成員無法查看；但基於監理法規要求，可以部署「觀察節點」來查看交易數據。Corda 的共識模型基於交易驗證和確保唯一性，在交易驗證過程中交易雙方獨立確認交易是否遵守業務規則，並在交易上附上數位簽章，而公證節點則確認交易的唯一性避免雙重支付。

在 SDX 試驗平台上，有 3 個商業銀行參與成為節點，可以進行

wCBDC 與商業票據的移轉交易。另外，SDK 試驗平台被分割成 3 個子網路，每一個子網路上處理一種代幣，例如：歐元 wCBDC、瑞士法郎 wCBDC 或商業票據，每一個子網路有唯一的公證節點及發行者，法國央行為歐元 wCBDC 的公證節點，瑞士央行為瑞士法郎 wCBDC 的公證節點，而商業票據則由 SDX 公司擔任公證節點，涉及兩種代幣的 PvP 或 DvP 交易則通過需要雙方的公證節點驗證後才能完成，這種需要 2 個子網路同時完成的交易採用了 HTLC¹¹技術以確保交易的原子性。

wCBDC 的發行與贖回是透過央行的即時支付清算系統(RTGS)來完成，商業銀行透過 RTGS 將款項移轉至央行的保管帳戶，央行則於子網路中發行對應的 wCBDC 給該商業銀行，贖回流程亦同。而商業票據則是透過數位資產管理機構發行。

PvP 交易流程，例如以歐元 wCBDC 交換瑞士法郎 wCBDC，首先交易雙方先於系統平台上將交易資訊細節輸入並發動交易指令，在歐元 wCBDC 子網路中，歐元 wCBDC 移轉交易經過雙方數位簽章後，提交至法國央行公證節點驗證，而在瑞士法郎 wCBDC 子網路中，瑞士法郎 wCBDC 移轉交易經過雙方數位簽章後，提交至瑞士央行公證節點驗證，系統便會自動並確保原子性執行交易；最終交易雙方再將各自收到的 wCBDC 贖回，透過央行的 RTGS 完成清算。

DvP 交易流程，例如以歐元 wCBDC 交易商業票據，首先交易雙方先於系統平台上將交易資訊細節(商業票據數額、交易金額等)輸入並發動交易指令，在歐元 wCBDC 子網路中，歐元 wCBDC 移轉交易

¹¹ Hash Time Lock Contract(HTLC)是一種使用於區塊鏈智能合約上的跨鏈支付技術，將支付款項以收款者提供的秘密字串之 Hash 值鎖住並設定一個時間限制，如果逾期不解鎖則返還支付者；只要收款者將其秘密字串公布則可經由智能合約驗證將款項解鎖收入帳戶。

經過雙方數位簽章後，提交至法國央行公證節點驗證，而在數位票據子網路中，數位票據代幣移轉交易經過雙方數位簽章後，提交至 SDX 公證節點驗證，系統便會自動並確保原子性執行交易，最終收到款項的商業銀行贖回 wCBDC，透過央行的 RTGS 完成清算，而收到數位票據代幣的商業銀行則透過數位資產管理機構進行資產的交付與登記。

Jura 專案成功的展示了一種新方法來清算代幣化的金融資產和跨境外匯交易，它透過結合 DLT 的技術，將不同國境的多種資產整合在單一平台系統上，同時保留了央行的關鍵監管能力；DvP 和 PvP 交易可以即時和原子性的進行，這也顯示將 wCBDC 交易和代幣化資產整合到單一第三方平台上是可行的。

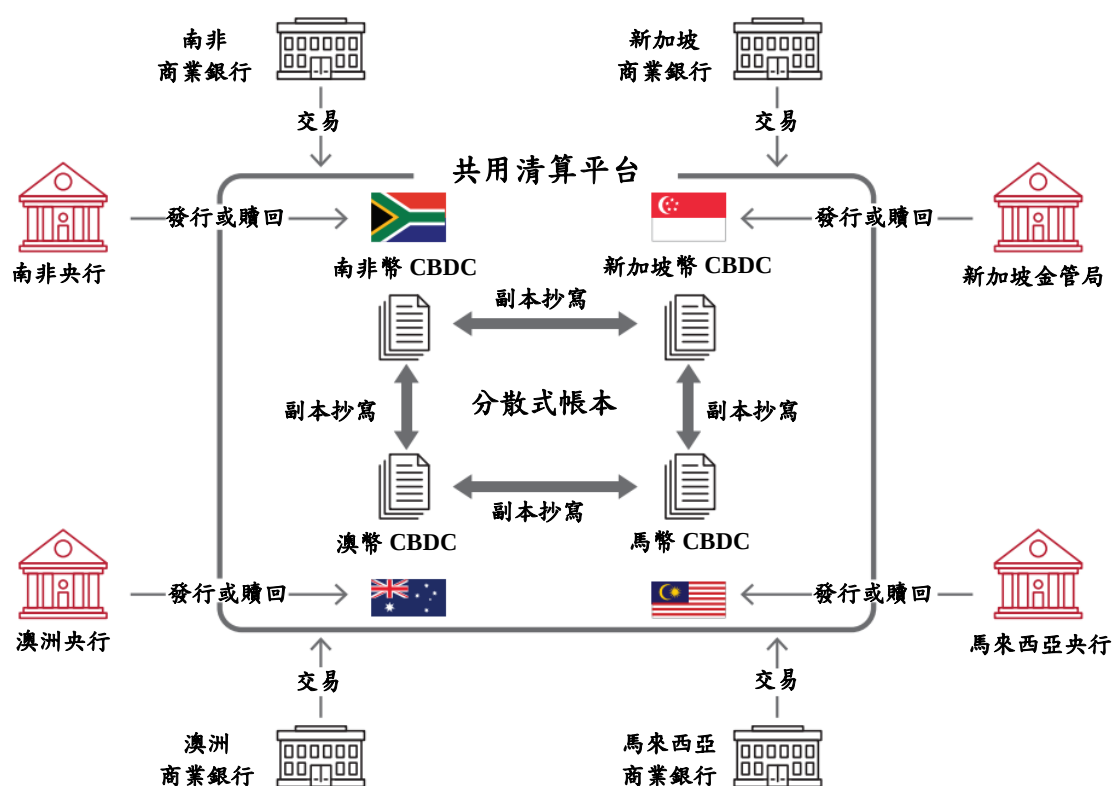
專案設計了一種靈活的方法來分配管控功能至不同的國家，這可能有助於實現更安全、更高效的跨境清算，從而促進金融穩定，外國金融機構可以在單一的平台進行資產和資金管理，有助於提高效率和節省成本。

Jura 專案也展示了中央銀行與私部門之間的合作方式，同時也表明代幣化和 DLT 技術或區塊鏈技術在跨境支付方面的潛力，未來可以繼續探索不同的設計選擇，以及更廣泛的對其相關的政策問題進行探討；雖然初步試驗證明了技術可行性，但仍將由各國中央銀行決定是否進一步探索 wCBDC 的發行。

三、Dunbar 專案

2022 年 3 月，BISIH 新加坡中心發布了 Dunbar 專案¹²的報告(圖 6)。Dunbar 專案召集了澳洲央行 (RBA)、馬來西亞央行 (BNM)、新加坡金融管理局(MAS)和南非央行(SARB)與 BISIH 一起測試多種幣別 wCBDC 的國際清算，文內表明使用二種不同的 DLT 技術：(1)Corda (2)Quorum。

圖 6、Dunbar 專案跨境模型架構



資料來源：BIS Innovation Hub, Reserve Bank of Australia(RBA), National Bank of Malaysia (NBM), Monetary Authority of Singapore(MAS), and South African Reserve Bank(SARB) (2022)

每個參與平台的國家央行都以本國貨幣發行自己的 CBDC，而參與平台的商業銀行能夠直接持有這些 CBDC，從而獲得外國貨幣資金，而無需在代理銀行開立帳戶，當所有參與的商業銀行可以直接持

¹² BIS Innovation Hub, Reserve Bank of Australia(RBA), National Bank of Malaysia (NBM), Monetary Authority of Singapore(MAS), and South African Reserve Bank(SARB) (2022)

有不同的 CBDC 時，他們就能夠直接以不同的貨幣進行交易。

該專案基於不同的 DLT 技術(Corda 和 Quorum)開發了兩個原型系統，實現國際間使用由多國央行發行的各幣別 wCBDC 以進行跨境清算，該系統設計直接使用不同的貨幣在金融機構之間進行跨境交易，在降低成本並提高清算速度上具有潛力。

以 Corda 技術開發的原型系統網路由各個節點組成，每個節點運行一個 Corda 底層系統和多個 CorDapps¹³，節點之間的通信是點對點並不依賴全局廣播¹⁴，每個節點都有安裝一個憑證代表其網絡身份，用以對應其現實世界的合法身份；Corda 網路還包括其他的服務，例如：網絡地圖服務(Network map service)，管理並記錄每個已知節點的 IP 位址與身份；身分管理服務，管理網絡上各節點的參與權限；簽名服務作為網絡地圖服務、身份管理服務、公鑰基礎設施(PKI)和硬體安全模組(HSM)基礎設施之間的橋樑；公證服務(Notary service)透過驗證確保交易的唯一性；Oracle 服務¹⁵將 Corda 網路連接到網路外的世界。

一個 Corda 網路上有多個 Corda 節點，每個節點屬於一個網路參與者；一個 Corda 節點負責管理與其他節點的通訊、運行 DLT 中的智能合約應用程式，以及儲存內部數據，Corda 節點由 Corda 核心系統、Corda 儲存空間(Corda vault)以及 CorDapps 組成，Corda 儲存空間就像一個資料庫來儲存帳本上的共享資訊；CorDapps 是應用程式運行在 Corda 核心系統之上，由以下這些組件組成：(1)狀態(States)：代表已經完成的事實；(2)合約(Contact)：定義何為有效的交易；(3)

¹³ CorDapp 是安裝於 Corda 底層系統上的應用程式，可以針對不同的使用案例設計不同的應用。

¹⁴ 全局廣播是一種資訊傳遞的方式，節點透過連鎖的方式向相連接的節點傳遞訊息。

¹⁵ Oracle 服務提供網路外界的資訊，例如現實世界中的股價、匯率等資訊。

流程(Flows)：定義進行交易的流程。

另一個以 Quorum 技術開發的原型系統網路，則由多個 Quorum 節點組成，其中節點有兩種類型：(1)參與節點(Participant nodes)：負責共同記錄網路間的交易細節，在 Quorum 去中心化的系統中，每個節點都有一份區塊鏈的副本；(2)驗證者節點(Validator nodes)：負責驗證交易，並透過共識將驗證過的交易更新到區塊鏈上，各國央行節點被配置為驗證節點，需要以點對點的方式連接到所有其他的驗證節點，而參與者節點則不需要連接到所有的網絡節點。

Quorum 是企業版的以太坊(Ethereum)區塊鏈，它提供隱私保護、新的共識機制、節點參與許可管制和更高的處理量能，一個 Quorum 節點的組成元件有：(1) Quorum 系統核心：為企業版的以太坊區塊鏈系統；(2) dApps(去中心化應用程式)：作為傳統系統與區塊鏈技術之間的中間層，負責轉譯用戶的交易指令為所需的智能合約交易格式；(3) Tessera：為一個 Java 應用程式，負責加密與解密具隱私的交易資訊和隱私訊息的傳遞，其中還包含兩個元件：交易管理器以及 Enclave；交易管理器是負責處理與傳遞加密的隱私交易數據，Enclave 則負責私鑰的管理及交易數據的加密和解密。

雖然上述兩種原型系統已經成功在專案中開發和試驗，但它們是建立在初步的設計基礎上，在進行測試的時候，是基於一種最具可能性且理想的預設場景，透過後續專案的推進及試驗的反饋，原型系統和設計將持續改善，以更清楚地了解其他需要解決的問題。

在設計原型系統時，通常有一些技術的權衡考量，這樣的權衡在試驗中可能由於試驗範圍有限，所以影響並不明顯，例如專案只模擬了五家商業銀行參與的情況，若銀行家數增加可能會面臨擴展性的技

術挑戰。

此外，該專案多聚焦於 CBDC 平台上的交易，然而，平台上的交易僅是完整支付流程的一部分，可能尚需與中央銀行的系統介接，以支援 CBDC 的發行，以及與商業銀行的客戶交易系統介接，藉此提供客戶服務。此外，跨境支付交易可能也只是國際貿易中的一個小環節，進一步與外部系統整合介接的開發與測試也是格外重要的。

多幣別的 CBDC 平台除了需與其他外部系統連接外，為實現跨境和多幣別的全球支付，平台系統將需要連接由其他國家或地區所建立的多幣別 CBDC 平台，建立一套全球通用的系統互通性標準或規範，將這些系統無縫介接至關重要。

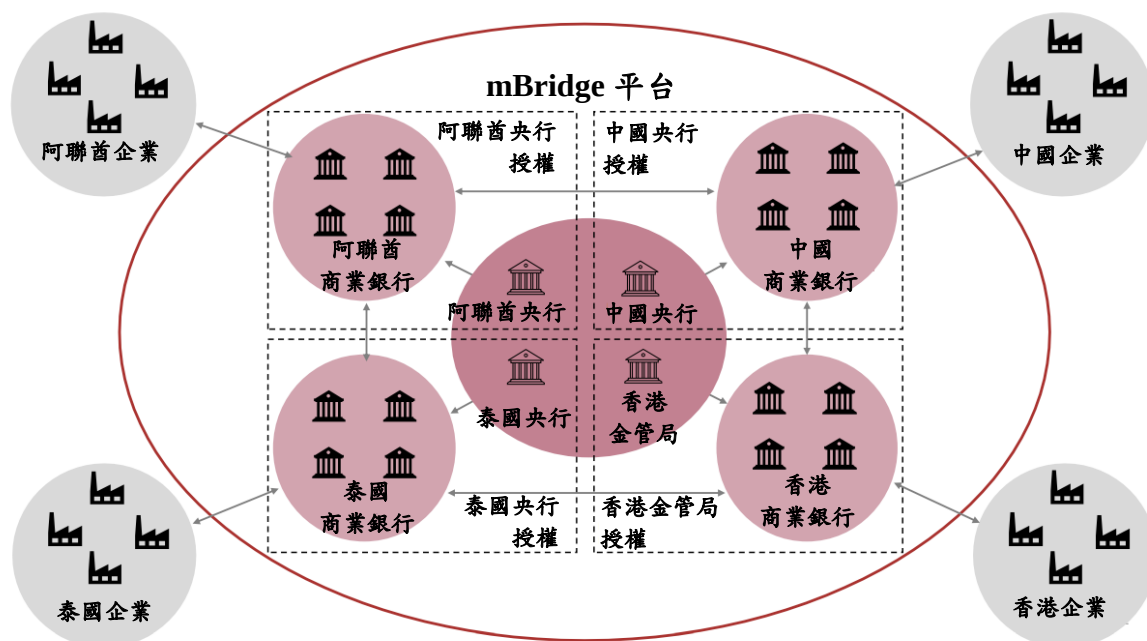
四、mBridge 專案

2021 年 2 月，在 BISIH 香港中心的推動下中國人民銀行與阿聯酋央行以及 ILR2 的原始成員一起創建了該項目的第三階段，並更名為 mBridge 專案(圖 7)，該專案擴展了之前 ILR2 基於 DLT 的概念驗證(PoC)模型系統，以探索多國貨幣的跨境支付能力，並開發一個 DLT 平台系統，多國中央銀行透過參與系統，可以發行自己本國的 CBDC 及分發給其他參與者，這些參與者可以用不同幣別的 CBDC 進行點對點付款，也可以將 CBDC 贖回轉換為對央行的準備金。

mBridge 平台採用模組化「樂高積木」方式構建，以實現在不同參與者間跨境應用功能的靈活性，專案試驗的重點是更進一步精進技術，並深入地研究法律和治理方面議題，透過試點取得真實的數據資料，以優化不同模組並擴展其交易量，以支援更多的參與者和交易。

考量到一些國家可能還沒有本國的 CBDC 系統，並且透過 API 介接系統需要花費大量時間，mBridge 平台在發行與贖回功能上支援

圖 7、mBridge 專案跨境模型架構



資料來源：BIS Innovation Hub (2022)

手動與自動兩種模式，手動模式為國內支付系統提供了互通性以及共存能力，使得 CBDC 系統和傳統支付系統都可以輕鬆的連接到平台，而若能夠以自動模式介接 mBridge 平台，對於商業銀行在效率與流程自動化上可以取得相對的優勢。

在手動模式下，各國央行可以在 mBridge 平台上發行及贖回他們的 CBDC，而無需更動他們現有的支付機制；商業銀行首先提交發行 CBDC 請求，並於平台外透過國內支付系統，進行手動資金轉移到央行(例如透過 RTGS 或國內 CBDC 系統)，央行一旦收到資金和完成內控檢查後，在 mBridge 上發行等量的 CBDC 存入商業銀行的錢包；同樣地，贖回也是由商業銀行的請求觸發，在 mBridge 上發送給央行的要贖回的 CBDC 數額，央行再手動將等額的資金透過國內支付系統轉移到商業銀行，完成贖回交易。

在自動模型中，mBridge 平台直接介接國內支付系統或 CBDC

系統，允許在兩個系統之間以高度自動化的方式處理交易，該過程涉及商業銀行透過本地支付系統匯款到指定的帳戶，然後在 mBridge 平台上自動觸發 CBDC 的發行；同樣，商業銀行在 mBridge 上發起贖回將自動觸發支付將款項匯回到本地支付系統的商業銀行帳戶。

在 mBridge 平台上可以實現兩種跨境支付：單一幣別跨境支付與雙幣別外匯 PvP 交易。單一幣別跨境支付首先由付款方設定幣別、金額和交易對象，然後於平台外進行合規性檢查，其中包括 AML/CTF 等，並於平台上向收款方發送付款請求，當收款方收到此請求，它也要於平台外進行自己的合規性檢查，並於平台上確認支付，付款方收到確認後，透過平台支付介面執行智能合約向收款方支付指定的貨幣金額；而雙幣別外匯 PvP 交易，它們是原子性的，透過 PvP 智能合約完成交易，交易涉及三個不同的階段：啟動、提交和執行：啟動階段，發起方於 PvP 智能合約上設定一組幣別、金額、匯率(於平台外談定)和交易對象，然後，就像單一幣別跨境支付一樣，發起方於平台外先進行合規性檢查，再向交易對象發送支付請求，一旦交易對象確認後，便進入提交階段，在此期間 FX 交易的一個方向已經完成，然後等待交易的另一個方向被對方觸發並確認；最後，進入執行階段，由 PvP 智能合約執行並完成 FX 交易。

mBridge 平台的核心是中央銀行，每個央行都運行一個驗證節點並進行共識，每個央行驗證節點之間都有連接，形成一個完整的連接圖，每個央行都可以將其國內商業銀行加入平台，每個國家的商業銀行都連接到該國的央行，如此，商業銀行就可以代表他們的客戶進行交易，藉此延伸平台的服務。

mBridge 平台是認許制的 DLT 系統，參與系統的節點必須透過組織認許才能加入，是否接受或拒絕提交的交易到分散式帳本上，須透過驗證節點的共識機制完成。共識機制有很多種，其中最為大眾熟悉的是工作量證明(Proof of Work)和權益證明(Proof of Stake)，它們分別被使用在比特幣和以太坊區塊鏈中，然而，認許制的 DLT 系統不同於非認許制的區塊鏈公鏈系統，認許制的 DLT 系統不需要為驗證者提供經濟獎勵，比較理想的共識機制是拜占庭容錯(BFT)或能夠提供系統韌性的機制，mBridge 平台使用名為 HotStuff¹⁶的共識機制，HotStuff 是 BFT 的一種實作，有很多優越的性能，特別是它的運算速度、演算法的複雜度以及與驗證節點數量成線性關係的優勢。

透過 mBridge 專案的探索可以瞭解，採用多幣別 CBDC 平台來解決現今跨境交易支付系統的局限性，可能是一個務實且可行的解決方案；通過提供單一共用平台，參與者可以在其上直接且安全地進行點對點的跨境支付。mBridge 專案的試驗結果也證實，一個通用的多幣別 CBDC 平台可以改進跨境支付的速度和效率，降低清算風險並能支援在跨境支付中使用本地貨幣。

後續 mBridge 專案將繼續改進現有功能及添加新功能，進而從當前的試驗階段逐步邁向最終能成為真實上線的系統。

¹⁶ HotStuff 是 BFT 的一種實作，不同於其他的實作方法受驗證節點數量的限制，在大量的驗證節點數的情況下，運算時間以級數等級上升，HotStuff 則以線性等級上升。

參、國際間跨境支付試驗專案之比較

在過去，要在傳統系統中實現的效率的提升，並允許中央銀行維持對其貨幣和清算的管控，必須介接彼此分離的集中式系統，然而這種方法充滿挑戰。本報告所提四個試驗專案都專注在批發(Wholesale)金融市場，提供功能讓不同幣別的 CBDC 可以進行單一移轉，也可以與另一個 CBDC 幣別兌換，這些試驗案例中，具有許多相似之處，例如每個試驗專案的技術平台皆採用 DLT 構建，並採用「於單一系統內的實現多種幣別交易」的創新做法，大幅改變了現今支付系統，也展現了提升效率的潛力。

這四個跨境支付的試驗專案在幾個方面也有所不同，包括真實程度、不同幣別的數量和試驗場景，以致技術和實驗設計的一些差異(表 1)。

表 1、跨境支付試驗專案之比較

項目	Inthanon LionRock2	Jura	Dunbar	mBridge
BISIH 中心	香港	瑞士	新加坡	香港
參與央行	香港金管局 泰國央行	法國央行 瑞士央行	新加坡金管局 南非央行 澳洲央行 馬來西亞央行	香港金管局 泰國央行 中國央行 阿聯酋央行
產出	概念驗證	原型系統	原型系統	原型系統
wCBDC 類型	日間	日間	隔夜(無息)	日間與隔夜
貨幣	港幣、泰銖	歐元、瑞士法郎	新幣、南非幣 澳幣、馬幣	港幣、泰銖、人民幣、阿聯酋迪拉姆
交易類型	模擬	真實	模擬	真實

介接模型	共用平台	共用平台 (透過子網路)	共用平台	共用平台
DLT 技術平台	Hyperledger Besu	Corda	Corda、Quorum	mBridge Ledger(MBL)
外國銀行 使用 wCBDC	持有與移轉	持有與移轉	持有與移轉	持有與移轉
平台營運者	各國央行	私人	各國央行	各國央行
境內支付	支援(無試驗)	支援(無試驗)	支援(無試驗)	支援(無試驗)
跨境支付	支援(有試驗)	支援(有試驗)	支援(有試驗)	支援(有試驗)
境內外幣支付	不支援	支援(有試驗)	支援(有試驗)	不支援
PvP	支援(有試驗)	支援(有試驗)	支援(有試驗)	支援(有試驗)
DvP	不支援	支援(有試驗)	不支援	不支援

資料來源：BIS Innovation Hub (2022)

四個試驗專案的成果證明皆具初步可行性，顯示在一個 mCBDC 平台上，可進行多種貨幣和資產清算。除了滿足跨境支付的核心要求外，各試驗系統也顯示出與現今系統相比更具潛力的運營效率；將多種貨幣和資產整合到一個系統中，採用一個共用的 DLT 平台，允許智能合約自動執行預定的交易規則，降低相關的合規與人工成本；同時，也減少對中介代理機構的需求，並實現參與者之間的直接交易，提高了清算的效率；在系統中，交易紀錄在一個單一的帳本上一步到位，參與者可以即時了解自己的資金狀態，也增加了營運透明度。

肆、結語

提供更好的跨境支付服務是各國央行共同努力的目標，透過 CBDC 可能有助於實現這個目標，但中央銀行需了解相關的系統與流程應該如何建立，以及將如何為未來貨幣體系開拓更廣闊的前景，通過結合試驗所學得的技術經驗和教訓，中央銀行可以對系統及跨境支付市場有更好的了解。

目前國際間的試驗是在有局限的情境下進行，雖然初步結果顯示採用區塊鏈技術或 DLT 技術建立一個共用的 mCBDC 平台，可以降低成本、加快清算速度並增加運營透明度，可能是一個改善跨境支付服務的方法，然而區塊鏈技術仍有許多難題尚待探討，例如：如何和現存系統進行介接、可能存在的擴展性問題，以及如何確保系統的強韌性和安全性等，仍需要後續更多的探索及試驗研究。

參考文獻

1. Auer, Raphael and Rainer Böhme (2020), “The Technology of Retail Central Bank Digital Currency”, *BIS Quarterly Review*, March.
2. BIS Innovation Hub, the Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People’s Bank of China and the Central Bank of the United Arab Emirates (2021), “Inthanon-LionRock to mBridge: building a multi CBDC platform for international payments”, September.
3. BIS Innovation Hub, Bank of France and Swiss National Bank (2021), “Project Jura: cross-border settlement using wholesale CBDC”, December.
4. BIS Innovation Hub, Reserve Bank of Australia(RBA), National Bank of Malaysia (NBM), Monetary Authority of Singapore(MAS), and South African Reserve Bank(SARB) (2022)”, Project Dunbar: international settlements using multi-CBDCs”, March.
5. BIS Innovation Hub (2022), “Using CBDCs across borders: lessons from practical experiments”, June.
6. European Central Bank and Bank of Japan (2019), “Project Stella – Synchronised cross-border payments”, June.
7. Hong Kong Monetary Authority and Bank of Thailand (2020), “Inthanon-LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments”, Jan.
8. Raphael Auer, Philipp Haene and Henry Holden (2021), “Multi-CBDC arrangements and the future of crossborder payments”, *BIS Monetary and Economic Department*, March.