

數位支付時代的央行角色與貨幣型態

本文係轉載 109 年 9 月 17 日「央行理監事會後記者會參考資料」

邁向數位時代，支付服務已不再只由銀行等傳統金融機構提供，非銀行支付機構的加入，以及支付科技的創新與貨幣型態可能的改變等，均使支付市場的發展更為多元、競爭。然而，在越來越錯綜複雜的市場分工與組成結構中，最終要能形成安全、效率的支付生態體系，並且營造出適合創新的環境，維持市場競爭的效率，則央行所扮演的角色（圖 1）與提供的貨幣信任基礎將是其中的關鍵。此外，央行也能善用數位科技帶來的契機進行創新，特別是近期國際間興起研究的央行數位貨幣（CBDC）^{（註 1）}，如經研究試驗可行，可望作為未來數位支付的新基礎。

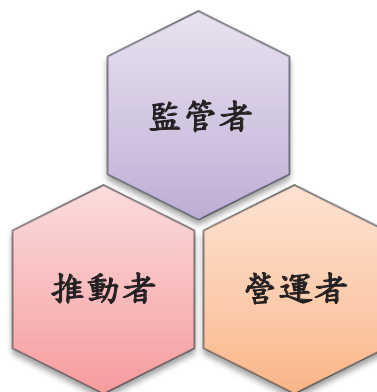
壹、央行在數位支付發展上扮演重要角色，並提供貨幣的信任基礎

一、央行在促進支付健全上的三個重要角色^{（註 2）}

（一）作為「營運者」，提供公共、中立的基礎設施

- 一 為滿足社會大眾的支付需求，多數央行亦營運該國重要的支付基礎設施，直接提供公共、中立的支付服務，以促進全民的公共利益為宗旨，而非追求商業利益。
- 一 零售市場上，央行發行的「現金」，被社會大眾普遍使用與接受，並可在電子支付未普及的場所或電子支付系統失靈時，作為基本且可靠的支付工具；此外，現金使用方便、無需手續

圖 1 央行在支付市場的重要角色



資料來源：本文整理

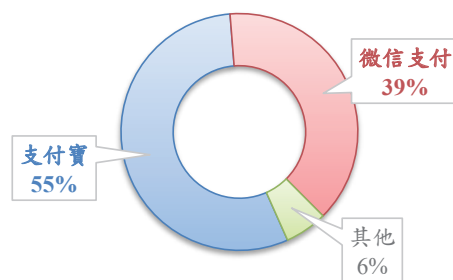
費且具支付的普及性，也促使電子支付必須朝向比現金更具吸引力的方向發展，以維持其競爭力。

- 批發（大額）市場上，央行營運的「即時總額清算（RTGS）系統」（如我國的央行同資系統），提供銀行等金融機構辦理跨行清算作業，並串接零售結算系統（如我國的財金公司跨行金融資訊系統），為民間支付業者佈建遍及全國支付網路的發展根基。

（二）作為「推動者」，促進支付互通，以利市場競爭

- 支付服務具有網路效應，越多人使用，就能提供使用者越高的價值。
- 支付系統理應儘可能容納更多的使用者，以充分發揮網路效應的效益，然而民間支付業者在營利及商業競爭的考量下，通常傾向於發展獨立、封閉的支付網路，不願與其他業者共享，以達成壟斷市場的發展目標，特別是以占中國大陸行動支付市場九成以上的支付寶與微信支付為效仿對象（圖2）。

圖2 中國大陸行動支付市占率
（2020年第1季）



資料來源：易觀智庫網路科技公司

- 支付市場如由少數業者寡占，固然能發揮極大的網路效應。但壟斷的市場結構，缺乏競爭對手的威脅下，恐逐漸喪失創新精進的動力，最終反而不利於市場長期的健全發展。
- 央行與其他主管機關，正致力於促進支付市場互通，打破支付網路間的隔閡，並降低市場的進入門檻，以維持市場的競爭性。例如，透過支持共通支付標準的發展、推動 Open API 等促進開放互通的措施。

（三）作為「監管者」，監管並指引市場的健全發展

- 數位科技的發展，正加速支付產業的變革，央行與其他主管機關的監管措施也與時俱進，特別是許多數位創新在提供更好支付體驗的背後，可能會潛藏對於消費者保護與個人隱私等的風險。此外，國際間日益重視的認識客戶（KYC）、反洗錢 / 反資恐（AML/CFT）等措施，亦是支付市場健

全發展的重要基礎。

- 政府也可訂定政策目標，指引支付市場發展的方向，例如，我國行政院訂定的 2025 年行動支付普及率達到 90% 目標等。

二、支付系統得以健全運作的基礎關鍵係央行提供受信任的貨幣

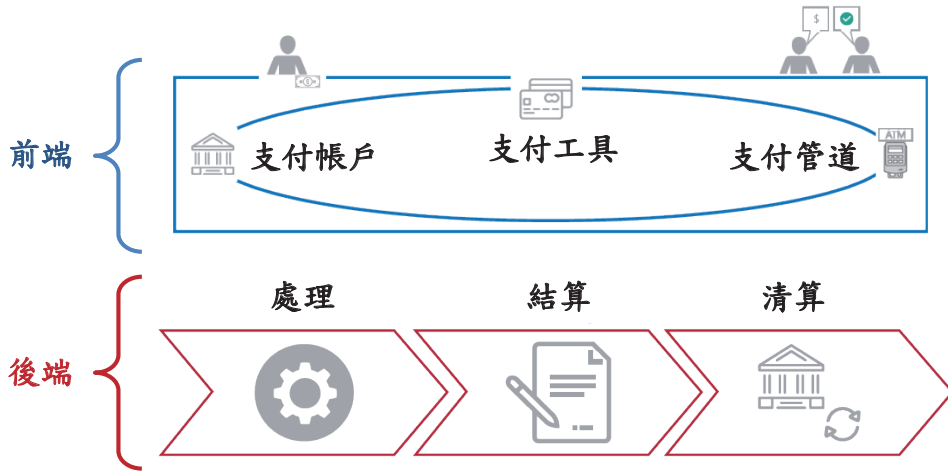
- 支付系統通常採雙層式的架構設計，由央行及銀行與非銀行中介機構（簡稱中介機構）共同合作：央行提供受信任的貨幣，中介機構則負責服務大眾並發揮創新；當中由央行提供最安全的系統（RTGS 系統）與支付工具（現金），用於清算批發與零售交易，中介機構則提供各式零售電子支付工具，讓大眾使用於各種支付場景。
- 近年數位支付的創新浪潮下，大眾接觸到的支付服務日新月異，例如卡式支付從刷磁條到近距離感應，甚至無實體化綁定到行動裝置上。然而，支付系統健全運作的基礎關鍵並未改變，依舊根植於央行提供受信任的貨幣。在此堅實的信任基礎上，讓中介機構可以專注於支付服務創新、發展，也提高大眾接受的意願。

貳、數位創新正在各方面重塑支付服務，亦試圖改變貨幣型態

一、數位創新正改變支付服務的體驗

- 數位創新正在全面地改變支付服務的提供與體驗，範圍涵蓋支付系統對使用者提供的「前端」及「後端」服務（圖 3）。
- 前端的「支付帳戶」已不僅限於銀行帳戶，資金也可保存在電子支付帳戶中，靈活應用於小額支付場景；「支付工具」除現金、支票、金融卡、信用卡、電子貨幣外，未來也有可能使用央行數位貨幣；「支付管道」除實體可用的 ATM、POS 機外，網路、手機 App 等已成為發展趨勢。
- 新科技的發展，也持續改善後端金流的處理、結算及清算作業，例如，運用大數據降低支付詐欺、洗錢等風險。此外，傳統系統係中心化架構，分散式帳本技術（DLT）興起後，已引發國際間探討以去中心化架構重新設計支付及結清算系統的可能性。

圖 3 支付系統之功能分工

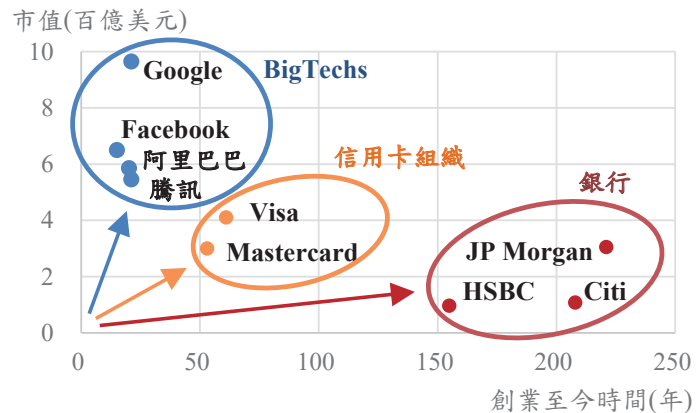


資料來源：主要參考自 BIS(2020)

二、大型科技公司可能影響支付市場的競爭結構

- 支付服務的網路效應顯著，非常適合已掌握大量使用者的大型科技公司（BigTechs）發展。
- BigTechs 憑藉優異的 DNA（data-network-activities）核心競爭力^(註3)，在規模化的速度與程度均遠遠超越傳統銀行與信用卡組織（圖4）^(註4)，如進入支付市場，將具備主導市場的潛力，進行不對等的競爭，最終可能使市場發生結構性變化。
- BigTechs 進入支付市場，雖讓消費者享受更好的服務，然而，資訊與金融的本質不盡相同，一旦處理不當，很可能會衍生重大風險，已引發各國主

圖 4 BigTechs 規模化速度超越傳統金融機構



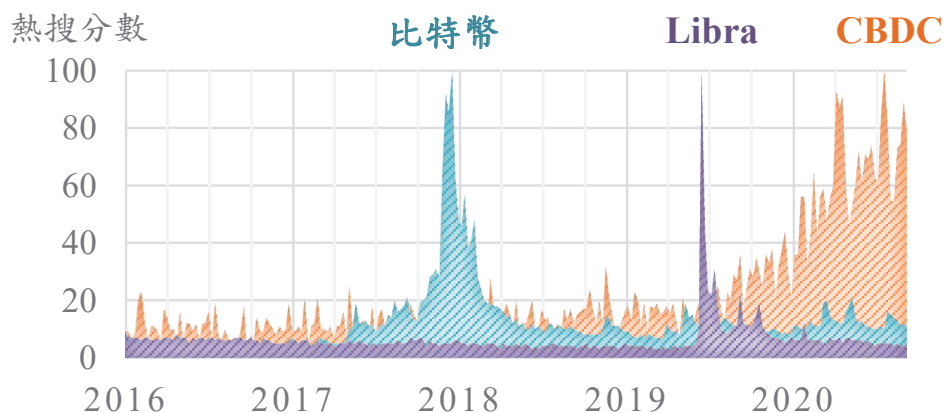
資料來源：BIS(2020)

管機關的密切關注。

三、民間業者正挑戰改變貨幣型態，國際間央行亦持續精進並擁抱創新

- 一 在支付服務與市場結構變化的同時，民間業者也開始嘗試挑戰支付系統的關鍵基礎，試圖改變貨幣型態。例如，比特幣與 Facebook 的 Libra，均曾短暫獲得市場大量的關注（圖 5）^{（註 5）}。

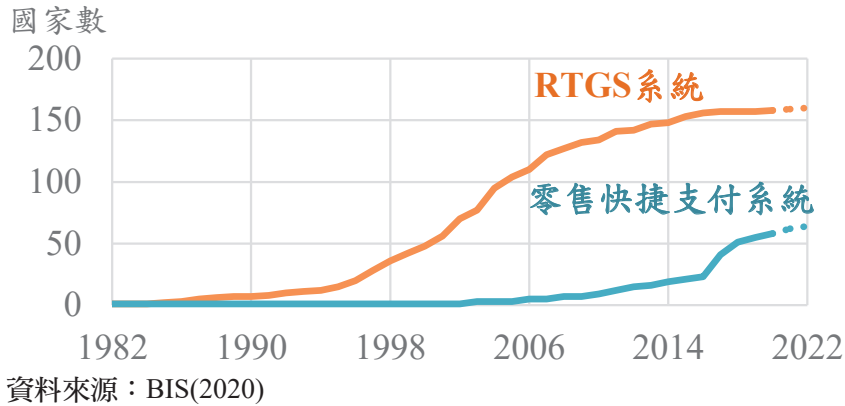
圖 5 比特幣、Libra 及 CBDC 的 Google 搜尋熱度



資料來源：Auer 等 (2020)、Google Trends

- 一 比特幣最初的設計理想係試圖建構出一種新型態的電子現金，惟其價值波動劇烈，並不具備貨幣的功能^{（註 6）}，至今多用於投機炒作，而非作為支付工具；國際間多視為是虛擬商品或數位資產。
- 一 Libra 希望能成為全球支付工具，然而，其信用不及國家貨幣，也缺乏國家主權與法律制度的保護。此外，Facebook 全球高達數十億的用戶數，致 Libra 影響範圍廣泛，除 G7 要求應符合國際間最高管理標準並受到審慎監管外，Libra 如要在各國合法經營亦需配合當地法規調整，是以此其迄今發展未如預期。
- 一 國際間央行面對民間的挑戰，一方面持續精進支付系統，例如多數國家已實施 RTGS 系統，並加速發展零售快捷支付系統（圖 6）^{（註 7）}；另一方面亦積極擁抱支付創新，目前全球約 80% 央行已著手 CBDC 研究工作^{（註 8）}。

圖 6 實施 RTGS 與零售快捷支付系統之國家數

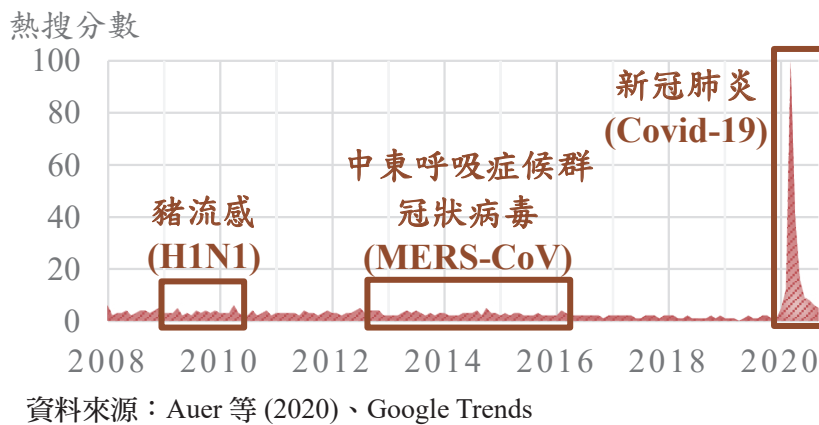


參、疫情加速數位支付時代的來臨，並影響國際間 CBDC 的研究規模

一、 疫情影響零售支付行為，加速電子支付發展，也推升對 CBDC 的期待

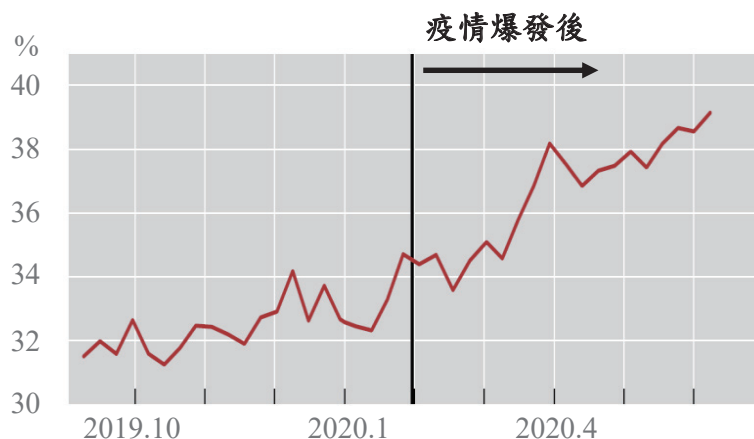
- 新冠肺炎疫情下，對於面對面直接接觸的擔憂，也影響民眾支付工具的選擇，特別是現金，曾一度被渲染成有傳遞病毒的可能，而在 Google 搜尋的熱度急升（圖 7）；惟至今並未傳出有人因使用現金而感染新冠肺炎之情事^{（註9）}。

圖 7 現金與病毒的 Google 搜尋熱度



- 一 當維持社交距離的生活型態開始成為新常態，電子支付等非接觸式的支付方式，很可能成為民眾面對面支付的新選擇，例如，卡片改以感應支付的交易行為，在疫情爆發後更趨明顯（圖 8）^{（註 10）}。

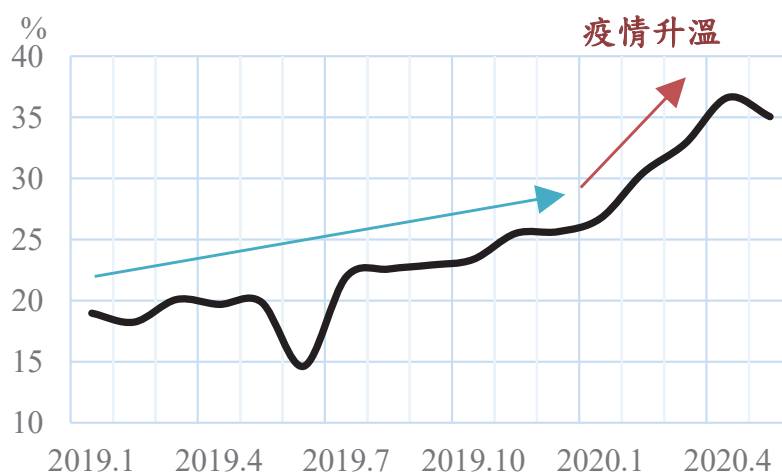
圖 8 全球面對面卡式支付採感應支付之比率



資料來源：Auer 等 (2020)

- 一 受疫情衝擊，實體店家關門，民眾在家隔離或減少不必要的外出時，多半只能仰賴電子支付完成網路購物等消費行為，例如，國人在疫情升溫後，信用卡用於網路購物的占比明顯上升（圖 9）^{（註 11）}。

圖 9 國人信用卡用於網路購物之筆數占比



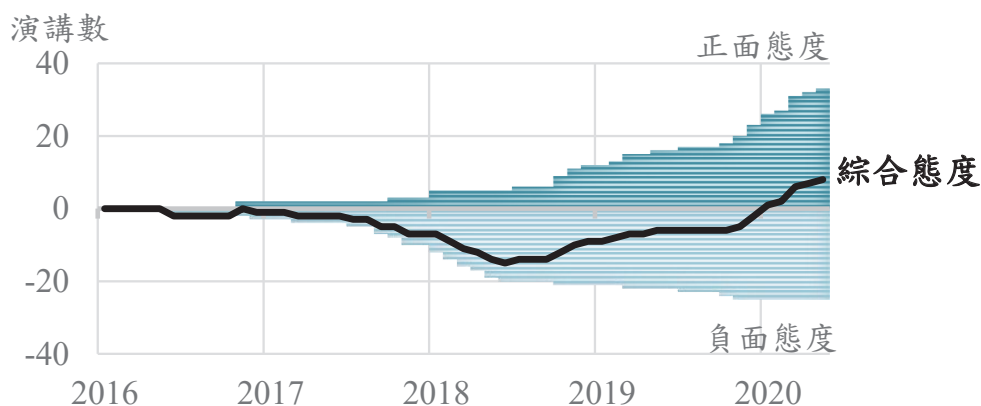
資料來源：聯卡中心 (2020)

- 一 假使疫情持續，民眾很可能養成新的支付習慣，逐漸減少現金的使用，最終恐衝擊社會中倚賴現金支付的族群。雖目前國際間尚無央行發行 CBDC，惟期望已逐漸加深，希望 CBDC 能延續過往現金使用的良好經驗，適用於社會中的各個族群，並能兼備電子支付的優點。

二、國際間央行日益重視 CBDC，正提升研究的規模與層級

- (一) 隨著 CBDC 研究的進展，國際間央行已陸續探討其可能的效益與風險，瞭解其潛力與局限。據 BIS 研究全球 175 國（或區域），現階段沒有任何一國（或區域）正式發行 CBDC^{（註 12）}，相關技術仍在研發之中，但展望未來，數位發展是必然的趨勢，必須正面看待 CBDC 未來應用於數位時代的可能性。
- (二) 近期國際間央行對 CBDC 的態度已轉趨正面（圖 10）^{（註 13）}，一些主要國家也開始提升相關研究的規模與層級，期望透過概念驗證（POC）或先導試驗（pilot）等方式，掌握技術的實際進展。

圖 10 國際間央行對 CBDC 的態度轉趨正面 *



* 針對國際間央行提及 CBDC 的演講，如內容正面計為 +1 次，負面為 -1 次，其他態度中立者則不計入。綜合態度為所有演講正負面相抵後之結果。

資料來源：Auer 等 (2020)

- 一 南韓央行已成立數位貨幣研究團隊與技術團隊，並在 2020 年 3 月展開為期 22 個月的 CBDC 先導試驗計畫，惟該行強調 CBDC 目前仍未成熟，且

在可預見的未來尚不會成真^(註 14)。

- 日本央行於 2020 年 7 月成立數位貨幣組，為隸屬於該行支付清算系統局的正式單位，負責推進支付系統的數位化及研究 CBDC，未來亦計畫與民間機構合作進行 CBDC 的概念驗證。該行強調目前並沒有發行 CBDC 的計畫，惟環境變化快速，需提前做好準備^(註 15)。
- 美國 Fed 於 2020 年 8 月宣布其科技實驗室（TechLab）正擴大數位貨幣及其他支付創新的實驗，Fed 波士頓分行亦與學術單位 MIT 合作研究計畫。美國目前雖然沒有計畫要發行 CBDC，惟 Fed 認為基於美元的重要地位，必須站在 CBDC 相關研究及政策發展的最前線，並與其他央行一同學習與合作^(註 16)。

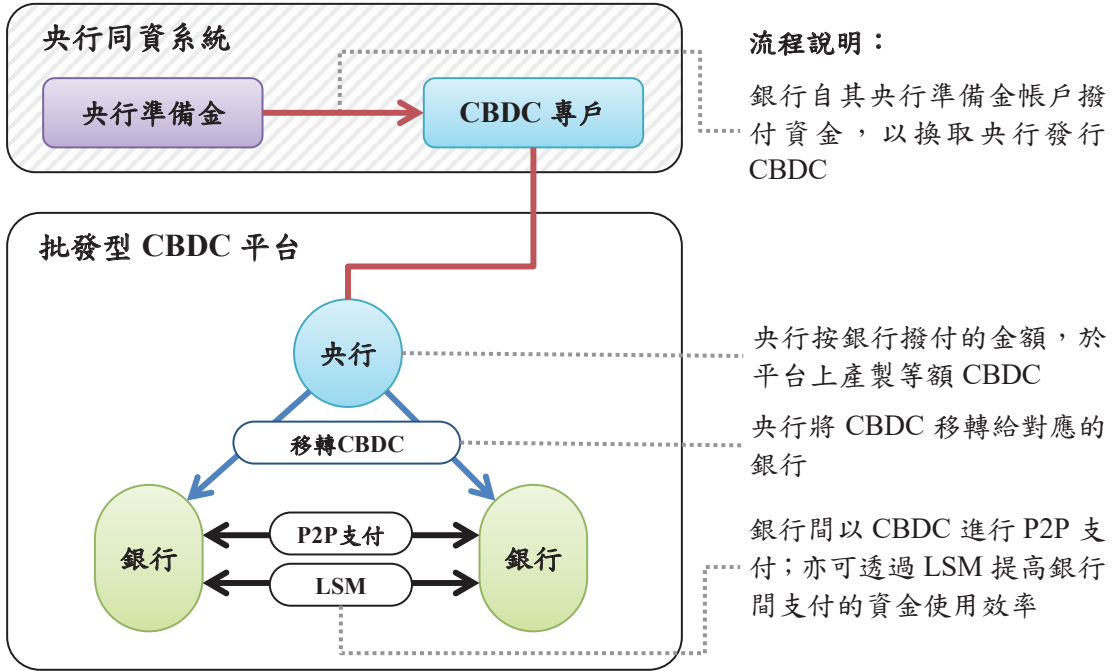
肆、本行已完成批發型 CBDC 的技術研究，下階段將進行通用型 CBDC 的試驗

為推動 CBDC 研究計畫，本行於 2019 年 6 月成立「CBDC 研究計畫專案小組」，下設「CBDC 工作小組」負責規劃與執行，已於 2020 年 6 月完成「批發型 CBDC 可行性技術研究」，透過與學術單位協作的方式，瞭解 DLT 應用在批發型 CBDC 的潛力與局限，並作為下階段通用型 CBDC 技術研究之參考，相關研究進度與國際腳步一致。

一、DLT 應用於批發型 CBDC 的研究分析

- 批發型 CBDC 要能發揮實質效益，在安全與效率上必須優於現行系統^(註 17)，以符合未來大額支付市場的需求：在運作上（圖 11）系統要能 7x24 運作^(註 18)、提供金融機構間點對點（P2P）支付功能，以及為降低參與者大額資金成本的需求，需有「流動性節省機制」（liquidity-saving mechanism, LSM）^(註 19)。特別是批發型 CBDC 如採用 DLT 等去中心化架構，須額外考量交易具清算最終性、隱私保護與監管等議題。
- 研究發現目前 DLT 的處理效能在實際應用上仍有其局限性，特別是在即時、大量、高頻的交易上，仍無法滿足現行電子支付系統的需求，主要是隱私保護的需求影響其運作效能。

圖 11 批發型 CBDC 運作架構



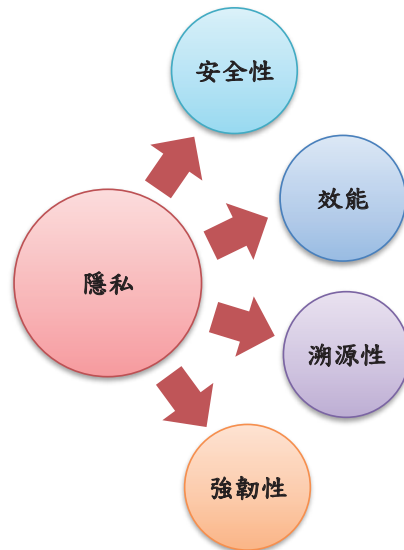
資料來源：本文整理

二、隱私保護是 DLT 應用於 CBDC 首要解決的課題

比特幣等傳統 DLT 並未考慮交易隱私，其網路上的所有節點會彼此共享交易資訊，透過共同的共識演算法，讓所有帳本保持一致，以防止雙重支付並確保交易具清算最終性。然而，CBDC 等金融應用特別注重隱私保護，不該與不相干的對象共享交易資訊，DLT 如要修改機制以兼顧隱私保護，通常會連帶影響安全性、效能、溯源性及強韌性（圖 12）。

— 安全性：為確保隱私，交易資訊僅

圖 12 隱私對 DLT 的重大影響



資料來源：本文整理

能交易雙方知曉，將使 DLT 網路上的其他節點沒有交易明細、無從驗證，可能衍生雙重支付等安全性疑慮。

- 效能：若要同時確保隱私性及安全性，並避免發生雙重支付，交易需透過「零知識證明」^(註 20)等特殊技術處理。然而，該等技術運算繁複，系統需耗費大量時間處理，顯著影響效能。
- 溯源性：對於隱私保護而施加的保護機制，可能無法滿足監管所需的溯源性，例如「一次性帳號」^(註 21)等去除關聯的技術，可能使交易無法被追蹤或追蹤成本過高。
- 強韌性：DLT 為兼顧隱私保護，可新增第三方的中立節點處理交易雙方的交易資訊，惟此節點將成為系統中較脆弱的部分，而衍生單點失靈等問題，限縮 DLT 原生的強韌性。

三、通用型 CBDC 在技術上需具備更高之效能，並宜採行雙層式運作架構

相較於批發型 CBDC 僅限銀行間的大額支付交易，需處理的交易量有限，通用型 CBDC 的使用者遍及社會大眾，並廣泛用於各種支付場景；因此，在技術上需具備更高的效能，並宜採行雙層式運作架構。

- (一) 通用型 CBDC 須保有現金的優點，並善用數位科技以滿足未來支付的額外需求（表 1）

表 1 通用型 CBDC 之設計考量

項目		說明
保有現金 優勢	普惠金融	允許任何人開立 CBDC 數位錢包使用
	保護隱私	匿名程度依交易金額及錢包等級有所區別
	隨時可用	提供 7x24 服務
	離線交易	支援離線支付，惟可能需限制金額以確保安全
善用數位 科技	遺失處理	具遺失處理機制
	利息設計	可支援利息設計
	未來數位支付需求	— 支付互通性 — 可程式化

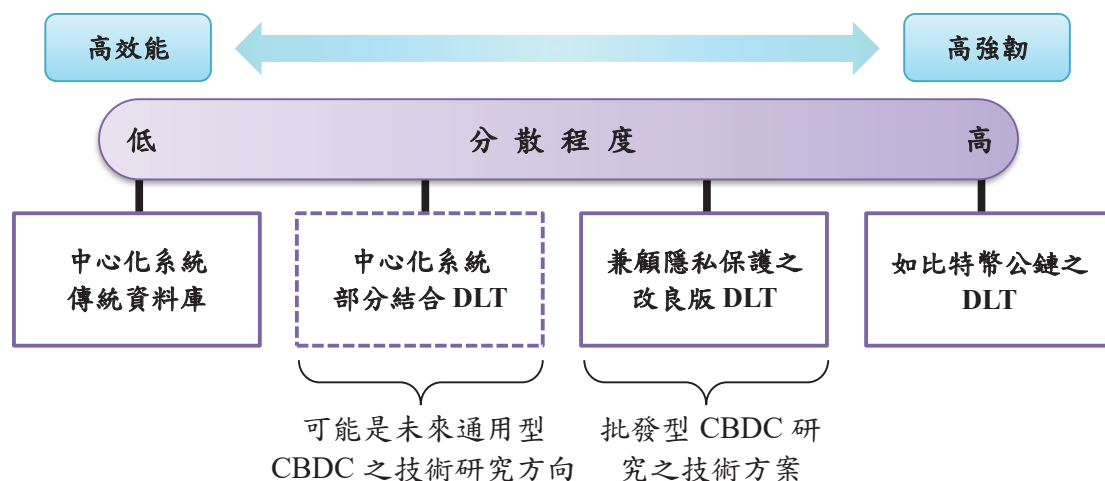
資料來源：本行 CBDC 工作小組

- 保有現金優點：通用型 CBDC 在使用上應比照現金，具備極低的使用門檻，允許任何人開立 CBDC 數位錢包，以利普惠金融；在遵循 AML/CFT 等法規的前提下，提供匿名支付的功能；系統能 7x24 運作，讓 CBDC 與現金一樣隨時可用；支援離線支付，以擴大到任何離線的支持場景。
- 善用數位科技：通用型 CBDC 可利用數位科技，實現過往現金無法提供的功能，例如，提供遺失處理機制、支援利息設計^(註22)、可程式化^(註23)等，以滿足未來數位支付的額外需求。

(二) 中心化系統部分結合 DLT 可能是通用型 CBDC 之技術方向

- 為因應支付交易的隱私需求，現行 DLT 發展出的改良方案^(註24)，主要是修改傳統 DLT 完全分散的設計（如比特幣），往中心化機制靠攏，以犧牲部分的強韌性為代價，換取更高的效能（圖 13）。

圖 13 分散程度不同之系統在效能與強韌上之比較



資料來源：本文整理

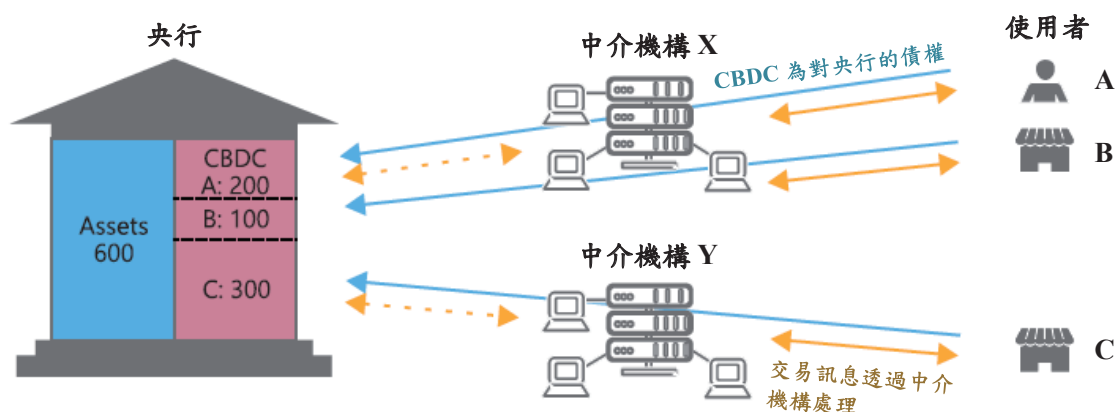
- 批發市場要求的效能較低，研究使用的改良版 DLT 方案大致能符合批發型 CBDC 的需求，但效能仍不及現行中心化作業之系統^(註25)。
- 未來通用型 CBDC 在設計上可以採取偏向中心化的設計，以滿足更高的效能需求。「中心化系統部分結合 DLT」是可能的技術方向，即以中心化

系統為基礎、部分功能（例如交易資料儲存等）結合 DLT，以提升系統強韌性，持續不間斷地提供交易與資料的服務。

（三）雙層式架構有助於通用型 CBDC 的健全發展

- 傳統貨幣體系採雙層式架構，例如現金由央行發行，但須仰賴銀行等中介機構擔當現金的分配者，讓大眾能透過銀行櫃檯、ATM 等管道取得現金。
- BIS 建議通用型 CBDC 可採用「混合型」（hybrid）CBDC 的設計（圖 14）^{（註 26）}，為一種雙層式架構，維持傳統公私合作提供貨幣的良好運作機制，並達到避免去金融中介化的目的。

圖 14 BIS 混合型 CBDC 的雙層式架構



資料來源：主要參考自 Auer 等 (2020)

- 使用者取得的每筆 CBDC，均為對央行的債權，如同現金，享有國家貨幣的各種保障；由央行作為 CBDC 的後盾，記錄所有 CBDC 的餘額；中介機構則居中辦理開戶、KYC、AML 等作業，並提供使用者相關創新支付服務。
- 央行確保大眾對於貨幣的信任，是支付系統最根本的基礎，雙層式架構讓中介機構在央行穩固的基礎上，能致力於發展業務、進行創新，使大眾能享有良好的支付服務而無需承擔額外的風險。在這樣的安排下，公私雙方均發揮最大的效益，有助於通用型 CBDC 的健全發展。

四、下一階段通用型 CBDC 試驗計畫之概要

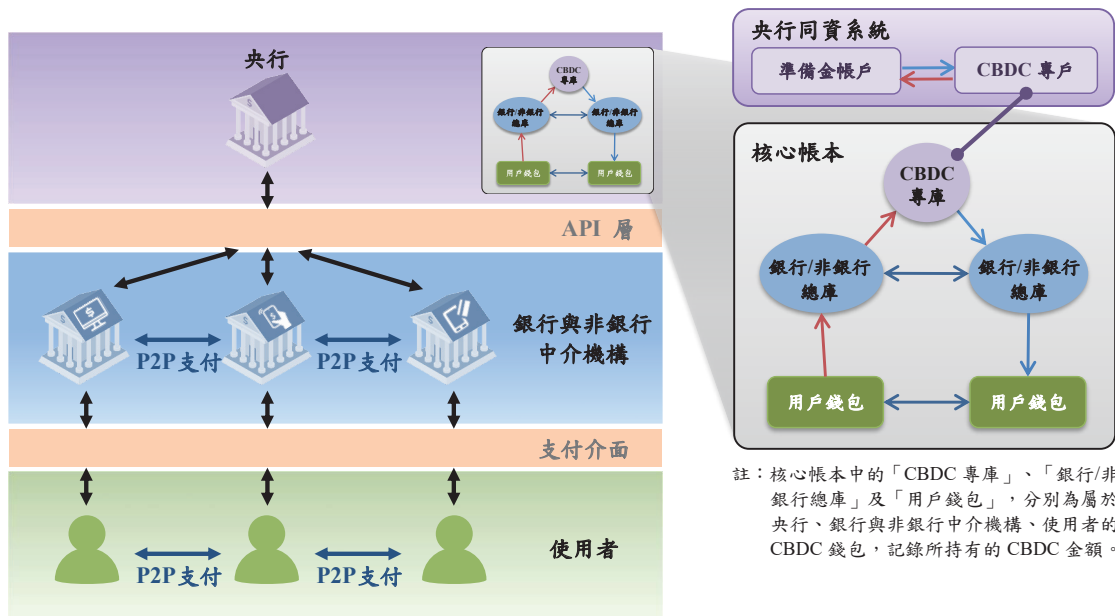
(一)通用型 CBDC 研究的目的，在探討現金數位化之可能性，預先為未來數位支付的發展做好準備

從本行已進行之批發型 CBDC 技術研究發現，以完全（或高度）去中心化 DLT 建構之批發型 CBDC 平台，其效能並未明顯優於現行中心化系統；然而，數位支付為未來發展趨勢，應持續研究並嘗試各種具有發展潛力的技術架構，同時探討在各種支付場景的可能應用，故本行將接續進行通用型 CBDC 試驗，探討現金數位化之可能性，預先為未來數位支付發展做好準備。

(二)通用型 CBDC 試驗計畫之平台架構

— 下一階段「通用型 CBDC 試驗計畫」，規劃將採雙層式架構（圖 15），由央行向中介機構發行 CBDC^{（註 27）}，再由中介機構提供給使用者；取得 CBDC 後，在銀行及使用者間就能以 CBDC 直接進行 P2P 支付。

圖 15 通用型 CBDC 平台整體運作架構



資料來源：本文整理

- 試驗用的通用型 CBDC 平台，在技術上將採「中心化系統部分結合 DLT」之設計，由央行^(註 28)維護 CBDC 的「核心帳本」，並運用 DLT 保存交易資料，以強化系統的強韌性；中介機構透過 API 介接核心帳本，負責 KYC 等使用者錢包開立作業，並可自行發展各種創新支付服務；使用者則透過中介機構提供的各種支付介面（如手機 App），將 CBDC 應用於各種支付場景。

伍、結語

一、貨幣的外在形式或有不同，卻都根植於央行提供的信任基礎上

- 現代支付系統的運作，是以具法償效力的中央銀行貨幣為基礎，支撐著商業銀行貨幣、電子貨幣等其他支付工具。換言之，貨幣的外在形式或有不同，然而，貨幣制度與支付系統均建立在對通貨的信任基礎上，而唯有央行可以確保其信任。
- 央行作為支付基礎設施的營運者、促進支付市場健全的推動者及監管者，提供支付系統發展的堅實基礎，在維護大眾對貨幣信任的同時，也支持民間部門的創新；央行亦站在科技創新的前端，積極研究 CBDC 作為未來的新支付工具，以因應數位時代的未來趨勢。

二、國際間 CBDC 研究的各種技術與架構，均未改變貨幣須具備信任的本質

- 國際間央行對 CBDC 的態度已轉趨正面，正逐步提升 CBDC 研究的量能，研究 CBDC 各種可能的技術與架構。然而，CBDC 無論是採用中心化或去中心化技術、以雙層式或更複雜的架構運作，只是外在形式的改變，均未改變貨幣須具備信任的本質。
- CBDC 如運用 DLT，其作用也是在提高系統強韌性，透過新技術強化系統安全，來進一步加深大眾對於貨幣的信任，並非以 DLT 取代貨幣的信任基礎。

三、本行將進行通用型 CBDC 試驗計畫，並視試驗情形與國際發展滾動式檢討期程

- 本行在第一階段「批發型 CBDC 可行性技術研究」發現，以完全（或高度）去中心化 DLT 建構之批發型 CBDC 平台，其效能並未明顯優於現行中心化系統，主要是因金融交易有隱私保護的需求，而影響其運作效能。
- 在瞭解 DLT 的潛力及問題後，本行將進行第二階段「通用型 CBDC 試驗計畫」^{（註 29）}。考量目前國際上尚無符合零售支付市場高頻交易需求之 CBDC 平台實例，再加上隱私保護的考量，未來在設計上可能以中心化系統為基礎、部分功能（例如交易資料儲存等）結合 DLT 之規劃，可能是較符合通用型 CBDC 需求的技術研究與發展方向。
- 未來的 CBDC 要能同時實現現金的普及性及電子支付的便利性，「通用型 CBDC 試驗計畫」亦以此作為研究的方向，在設計上希望能保有現金的優點，並善用數位科技，盡可能地符合現在及未來支付市場的需求。本試驗計畫預計於 2020 年 9 月底啟動，期程預定 2 年，並將視實際試驗情形及國際間 CBDC 發展趨勢，滾動式檢討期程的調整。

註釋

註 1：參見中央銀行 (2020)，「國際間央行數位貨幣之最新發展趨勢」，6 月 18 日央行理監事會後記者會參考資料。

註 2：主要取材自 BIS (2020), “Central Banks and Payments in the Digital Era,” *BIS Annual Economic Report*, Jun. 24.

註 3：參見中央銀行 (2019)，「FinTechs 與 BigTechs 在支付領域之發展及影響」，9 月 19 日央行理監事會後記者會參考資料。

註 4：BIS (2020), “Central Banks and Payments in the Digital Era,” *BIS Annual Economic Report*, Jun. 24.

註 5：Auer, Raphael, Giulio Cornelli and Jon Frost (2020), “Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies,” *BIS Working Papers*, No. 880, Aug. 24.

- 註 6：貨幣須具備的三大功能，包括：可作為價值儲藏的工具、可普遍被接受作為交易媒介、可普遍作為計價或記帳單位。
- 註 7：快捷支付系統 (Faster Payment System) 係指系統可即時處理支付訊息，讓付款人在付款時，收款人可近乎即時收到款項，並提供 24 小時全天候服務。
- 註 8：Boar, Codruta, Henry Holden and Amber Wadsworth (2020), “Impending Arrival – A Sequel to the Survey on Central Bank Digital Currency,” *BIS Papers*, No. 107, Jan. 23.
- 註 9：Auer, Raphael, Giulio Cornelli and Jon Frost (2020), “Covid-19, Cash, and the Future of Payments,” *BIS Bulletin*, No. 3, Apr. 3.
- 註 10：同註 9。
- 註 11：聯卡中心 (2020)，「COVID-19 對電子商務的行為改變－2019 年 vs. 2020 年 (1~5 月) 信用卡網路購物消費分析」，8 月 12 日。
- 註 12：Auer, Raphael, Giulio Cornelli and Jon Frost (2020), “Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies,” *BIS Working Papers*, No. 880, Aug. 24.
- 註 13：同註 12。
- 註 14：BOK (2020), “Situation of Major Countries’ Countermeasures to CBDC,” Feb. 5; Jung, Jun-ho (2020), “Bank of Korea to Establish a Digital Currency Organization for CBDC Research,” *Korea IT Times*, Feb. 6; BOK (2020), “Bank of Korea, Central Bank Digital Currency (CBDC) Pilot Test,” Apr. 2; Lee, Min-hyung (2020), “Bank of Korea Moves toward Issuance of Digital Currency,” *The Korea Times*, Apr. 6.
- 註 15：Kasai, Tetsuya and Kazuo Teranishi (2020), “Bank of Japan Speeds Up Work Toward Issuing Digital Currency,” *The Asahi Shimbun*, Jul. 29; Amamiya, Masayoshi (2020), “Japan’s Economy and Monetary Policy,” Speech at the Japan National Press Club, Jul. 29.
- 註 16：Brainard, Lael (2020), “An Update on Digital Currencies,” Remarks at the Federal Reserve Board and Federal Reserve Bank of San Francisco’s Innovation Office Hours, Aug. 13; Federal Reserve (2020), “Federal Reserve Highlights Research and Experimentation Undertaken to Enhance Its Understanding of the Opportunities and Risks Associated with Central Bank Digital Currencies,” Aug. 13.
- 註 17：例如，現行我國央行同資系統係採中心化架構，運作安全又有效率，且透過同、

異地備援機制，維持營運不中斷。

註 18：7x24 運作係指每周 7 天，每天 24 小時全時不中斷運作。

註 19：流動性節省機制係指當付款行帳戶餘額不足時，支付指令不是直接退回，而是進入佇列等候，待特定時間再將等待的多筆支付指令進行互抵作業，互抵後之應付淨額，如付款行帳戶餘額足數扣付，則完成該等支付指令的資金收付，以節省銀行流動性，並避免產生銀行間資金互卡 (gridlock) 現象。

註 20：零知識證明 (zero knowledge proof, ZKP) 係透過數學方法，可在不洩漏資訊的情況下，驗證所宣稱事項的真實性，例如：A 向 B 宣稱門口停的車是 A 擁有的，但 A 不想拿出鑰匙給 B 查驗，於是 B 向 A 提出挑戰，明日下午 3 點 15 分時，車要出現在後門，且車頭朝向右，如果挑戰成功，則可證明 A 擁有該車。ZKP 用於支付上，可用以證明付款人帳戶餘額足夠進行支付，且支付的款項正確反映在收付雙方的帳戶餘額上，而不會洩露任何有關帳戶餘額的訊息。

註 21：一次性帳號 (one-time address)，如比特幣每個帳號僅用於一次付款交易，交易時，付款帳號內所有款項會全額提出，一部分付給收款者帳號，剩餘的部分則回存至付款者新創的另一個一次性帳號，供下次使用。

註 22：實體現金沒有利息，CBDC 如做為現金的替代工具，很可能也不需要提供利息功能。但 CBDC 在設計上應儘可能保留未來發展的彈性，支援利息設計，以因應未來市場可能的變化。

註 23：可程式化 (programmable)，讓 CBDC 能依照程式設定的條件，自動執行交易，可能延伸應用的場景多樣，例如，債券在付息日及到期時，以 CBDC 自動支付利息及償還本金；CBDC 與其他代幣化資產 (無論實體資產或金融資產) 直接交易，完成款券同步交割 (DvP) 或款對款同步收付 (PvP)；可設定某筆 CBDC 款項的用途，專款專用，如限定只能用於支付營養午餐的費用；此外，交易也可與實體設備或物聯網 (IoT) 整合，如智慧型冰箱如偵測到特定食材快用完時，直接向廠商訂購，並以 CBDC 自動完成付款。

註 24：現行主要有「零知識證明技術搭配全網驗證」及「交易隔離搭配中立節點」等兩種改良方案：「零知識證明技術搭配全網驗證」方案，交易雙方的交易不公開，透過「零知識證明」產生對應的密文，並交由「全網驗證」，達到等同驗證原始交易的效果。此方案雖能保護隱私，但因交易資訊僅儲存於部分節點，需搭設備援機制，以兼顧溯源性與強韌性；惟其效能也因使用零知識證明而受影響。「交

易隔離搭配中立節點」方案，交易雙方使用專屬之交易通道將「交易隔離」，可確保通道內的交易內容不被外人得知，並設立第三方的「中立節點」負責驗證交易，以確保沒有雙重支付等問題。由於沒有使用運算耗時的零知識證明，效能較高。惟中立節點為中心化設計，仍有單點失靈的風險，須依賴備援機制。

註 25：研究使用的改良版 DLT 方案每秒約可處理 10 筆交易，不及現行已具高處理效能的央行同資系統，每秒可處理數百至數千筆交易，並可隨實際需求擴充效能。

註 26：Auer, Raphael and Rainer Böhme (2020), “The Technology of Retail Central Bank Digital Currency,” *BIS Quarterly Review*, Mar. 1.

註 27：如同批發型 CBDC 的設計，銀行需自其央行準備金帳戶撥付資金，以換取央行發行的 CBDC。

註 28：或央行指定的機構。

註 29：第二階段「通用型 CBDC 試驗計畫」係為 CBDC 研究的過程，並非表示本行即將要發行 CBDC；未來亦將評估該階段的試驗結果，如可行，將規劃進入下一階段，進行先導試驗。