

出國報告（出國類別：實習）

參加 SEACEN 研訓中心
支付及清算系統監管課程報告

服務機關：中央銀行

姓名職稱：楊鎰鴻 業務局辦事員

詹凱傑 發行局辦事員

陳永祚 資訊處辦事員

派赴國家：菲律賓

出國期間：2019 年 10 月 20 日至 10 月 26 日

報告日期：2020 年 1 月 15 日

目次

壹、前言	1
貳、菲律賓支付系統	3
一、大額支付系統	3
二、零售支付系統	9
三、支付系統之監管	15
參、分散式帳本技術、區塊鏈及其應用	18
一、分散式帳本技術	18
二、區塊鏈技術及其應用	20
三、分散式帳本技術的風險	23
四、分散式帳本技術的優劣勢與 CBDC	26
肆、央行數位貨幣之議題	29
一、CBDC 的類型	29
二、CBDC 的技術方案	33
三、國際間 CBDC 的發展與試驗案例	36
伍、心得及建議	41
一、心得	41
二、建議	43
參考資料	46

壹、前言

本次奉派參加由東南亞國家中央銀行(The South East Asian Central Banks, SEACEN)研訓中心與日本央行(Bank of Japan)於菲律賓馬尼拉舉辦之「支付及清算系統監管課程」，參與學員除來自我國外，尚包括不丹、汶萊、柬埔寨、印度、印尼、寮國、馬來西亞、蒙古、緬甸、尼泊爾、巴布亞紐幾內亞、菲律賓、新加坡、斯里蘭卡、泰國及越南等國。

主辦單位邀請來自國際清算銀行(Bank for International Settlements, BIS)、日本央行、新加坡金管局(Monetary Authority of Singapore)、馬來西亞央行(Bank Negara Malaysia)、菲律賓央行(Bangko Sentral ng Pilipinas)、VISA 等機構中高階主管，以及 SEACEN 研訓中心資深人員擔任講師。授課內容包括：

一、大額與零售支付系統之監管

說明支付系統潛在的風險來源，以及英國、菲律賓、馬來西亞等國對於支付系統之監管方式及央行扮演之角色，另針對近期興起之網路犯罪及駭客攻擊，闡述其型態及應對策略。

二、分散式帳本技術(distributed ledger technology, DLT)的應用與風險

簡介 DLT 特性與應用場景，探討加密資產之定義及其與通貨的差異，並提出各國對發展央行數位貨幣(Central Bank Digital Currency, CBDC)的態度與使用 DLT 的試驗案例，闡述發展 CBDC 可能帶來的益處與挑戰，以及使用 DLT 尚需考量的風險。

本報告內容分為 5 章，主要係根據本次課程內容，分別說明主辦國菲律賓之支付系統、分散式帳本技術之發展及央行數位貨幣議題。除第壹章前言外，第貳章概述菲律賓支付系統及監管方式；第參章說明分散式帳本技術、區塊鏈及其應用；第肆章探討央行數位貨幣之相關議題；第伍章為心得與建議。

貳、菲律賓支付系統

一、大額支付系統¹

菲律賓大額支付系統名為「菲律賓支付清算系統(Philippine Payments and Settlements System, PhilPaSS)」，於2002年上線，由菲律賓央行營運，採即時總額清算(Real-Time Gross Settlement, RTGS)機制，透過增減參加單位於央行開立之準備金帳戶(Demand Deposit Account)餘額，辦理大額支付指令之即時清算，已完成之交易不可撤銷，具有最終清算效力；另針對美元及政府債券之交易，提供款對款同步收付(payment versus payment, PvP)及款券同步交割(delivery versus payment, DvP)服務。

(一)營運單位

PhilPaSS 之營運單位為菲律賓央行的支付清算辦公室(Payments and Settlements Office, PSO)，其隸屬於企業服務部門(Corporate Service Sector)，直接向督導該部門之副總裁報告。PSO 的主要職責為維持 PhilPaSS 之健全性，並消除相關風險，業務內容包含：

1. 確保參加單位遵循相關規範
2. 實施適當且有效的營運不中斷計畫
3. 促使 PhilPaSS 符合國際支付清算相關標準
4. 持續精進支付流程及作業方式

(二)營業時間

¹ Bangko Sentral ng Pilipinas (2019a)、Bangko Sentral ng Pilipinas (2019b)

PhilPaSS 營業時間為營業日之 9:00 至 17:45，若國內有部分地區放假，PhilPaSS 仍會接受未放假地區之交易，參加單位除可辦理當日之即時交易外，亦可辦理 4 個日曆日內之期約交易。

(三)交易類型

PhilPaSS 主要用於辦理參加單位間大額交易、金融市場及零售支付之最終清算，處理之交易類型包含：

1. 央行公開市場操作
2. 參加單位間大額資金移轉
3. 參加單位準備金調整
4. 零售支付²的最終清算
5. 銀行客戶的支付指令³
6. 美元交易的菲律賓披索部分⁴
7. 政府債券交易的款項部分⁵
8. 參加單位與央行間之交易(例如存提現金、重貼現、融通等)
9. 參加單位向央行繳交透支息、監管年費、罰鍰、申請其他業務之手續費等

² 包含民眾利用 ATM、支票、ACH、快捷支付系統等辦理之零售支付交易。

³ 菲律賓之銀行得代其客戶以 PhilPaSS 進行跨行支付，且該支付指令之受款人為最終受款人，銀行可自訂手續費及服務截止時間(通常僅開放上午時段)。

⁴ 菲律賓央行將 PhilPaSS 與菲律賓證券清算公司(Philippine Securities Settlement Corporation)營運之菲律賓國內美元移轉系統(Philippine Domestic Dollar Transfer System)介接，提供 PvP 服務。

⁵ 菲律賓央行將 PhilPaSS 與財政部系統介接，提供 DvP 服務。

10. 銀行代收稅款匯回財政部

(四) 清算機制

PhilPaSS 採 RTGS 機制，若參加單位準備金帳戶餘額不足，支付指令將納入佇列，並依參加單位指定之優先順序⁶或先進先出原則，於餘額足夠時自動清算；當存在 2 個以上來自不同參加單位的佇列支付指令時，系統每 30 分鐘會啟動 1 次資金互卡解決方案(gridlock resolution)；另 PhilPaSS 於 17:45 會自動剔除尚未清算之佇列指令。

(五) 參加單位及連結方式

截至 2019 年 12 月 4 日，PhilPaSS 參加單位共 168 家，分別為 43 家商業銀行、3 家國有銀行(specialized government bank)、37 家儲蓄銀行(thrift bank)、74 家農村銀行(rural bank)、8 家具有部分銀行功能之非銀行⁷(non-bank with quasi-banking functions)、2 個菲律賓央行內部單位，以及財政部。

參加單位得透過 SWIFT 傳送支付指令至 PhilPaSS，或透過網頁版的「PhilPaSS 參加單位瀏覽器(PhilPaSS Participant Browser, PPB)」連結 PhilPaSS，PPB 亦作為 SWIFT 故障時的備援機制。

PhilPaSS 藉由與多家第三方系統提供商(third party systems provider, TPSP)介接，提供零售支付、金融市場交易的最終清算服務。TPSP 負責驗證支付交易之正確性(accuracy)，完整性(completeness)及有效性(validity)，並將結算結果傳輸至 PhilPaSS 辦理清算。目前與 PhilPaSS 介接的 TPSP 如表 1。

⁶ 向政府單位(央行、財政部及國有銀行)之支付指令優先於其他銀行間交易。

⁷ 例如信用卡公司、租賃公司、車貸公司等。

表 1、PhilPaSS 介接之第三方系統提供商

第三方系統提供商	結算交易類型
BancNet	ATM
	快捷支付(fast payment)系統
菲律賓結算所公司(Philippine Clearing House Corporation, PCHC)	媒體自動轉帳(Automated Clearing House, ACH)
	支票
財政部	政府債券
PDS 集團*	美元交易中涉及 菲律賓披索款項部分

*PDS 集團(PDS Group)提供菲律賓國內多項重要金融基礎設施，旗下包含菲律賓交易所(Philippine Dealing & Exchange Corp.)、菲律賓集中保管結算所(Philippine Depository & Trust Corp.)等，其中菲律賓證券清算公司提供美元即時轉帳服務。

資料來源：菲律賓央行、PDS 集團

(六)手續費

PhilPaSS 參加單位無須支付年費等固定費用，僅依照完成清算之交易支付手續費，且手續費視交易類型及交易金額而定，費率結構之調整須由菲律賓央行之理事會(Monetary Board)批准，目前費率如表 2。

PhilPaSS 之交易手續費依交易金額高低採階梯式收費，單筆手續費最高為 400 菲律賓披索(約新台幣 260 元)，若因參加單位系統故障或連線中斷等異常事件，導致須人工處理銀行間交易，則收取最低 5,000 菲律賓披索(約新台幣 3,250 元)之手續費。

表 2、PhilPaSS 交易手續費

單位：菲律賓披索

交易類型	手續費	
1.交易手續費	交易金額	每筆交易手續費
● 銀行間交易	1-100 101-500,000 500,001-1,000,000 1,000,001-40,000,000 40,000,000 以上	免費
● 美元交易的菲律賓披索部分		5
● 政府債券交易		10
● 支票及 ACH 交易		交易金額×0.00001*
● ATM 交易		400
● 人工處理銀行間交易	MIN(5,000；1,000+交易金額×0.00001)	
2.其他手續費		
密碼卡申請	每張 1,200	
線上交易查詢	經由 SWIFT—每次 100 經由 PPB—免費	
對帳單申請	經由 SWIFT—每次 100 經由 PPB—免費	

*四捨五入至個位數。

資料來源：菲律賓央行

(七)流動性管理

PhilPaSS 以 RTGS 機制辦理資金清算，搭配佇列及資金互卡解決方案，降低信用、流動性及清算風險。此外，參加單位亦可透過日間流動性工具(Intraday Liquidity Facility)及日間透支機制(Overdraft Credit Line)，避免臨時性的流動性不足，分述如下：

1. 日間流動性工具：參加單位事先以政府債券作為抵押，於準備金帳戶餘額不足時向央行進行附買回交易取得資金，原則上當日 17:00 便須償還。
2. 日間透支：參加單位以政府債券足額擔保，當其準備金帳戶餘額低於支票結算之應付款項時，由央行提供臨時流動性，

以避免資金互卡。

(八)風險管理

菲律賓央行已將 PhilPaSS 相關風險納入企業風險管理架構 (Enterprise Risk Management Framework) 中定期審視，另為確保營運不中斷，PhilPaSS 已建立異地備援系統，並要求參加單位建立緊急應變程序。

為確保 PhilPaSS 遵循國際支付清算相關準則，菲律賓央行於 2007 年根據「重要支付系統之核心準則(Core Principles for Systemically Important Payment Systems)」辦理自我評估；2014 年由亞洲開發銀行 (Asian Development Bank) 根據金融市場基礎設施準則 (Principles for Financial Market Infrastructures, PFMI) 進行第三方評估；目前菲律賓央行每年會執行 1 次 PhilPaSS 遵循 PFMI 的自我評估。

(九)營運量

2018 年 PhilPaSS 處理之交易筆數約 163 萬筆，金額約 260 兆菲律賓披索，其中交易金額以銀行間交易及公開市場操作為大宗(如表 3)；2018 年交易筆數及金額分別較 2017 年下降約 9.0% 及 1.2%，其中筆數大幅下降係因菲律賓央行於 2018 年年中，停止提供海外移工匯款功能「PhilPaSS-Remit⁸」，致該類別交易筆數減少約 3 成。

⁸ PhilPaSS-Remit 係菲律賓央行為使該國海外移工可更安全、快速地將資金匯回國內，開放 PhilPaSS 可用於即時清算海外移工匯款；具體方式為海外移工將資金存入參與此服務之商業銀行的外國據點，再由該銀行之菲律賓總行透過 PhilPaSS 匯入受益人銀行。惟隨著新興零售支付系統蓬勃發展，本服務功能逐漸被取代，故菲律賓央行於 2018 年 6 月 30 日停止 PhilPaSS-Remit 服務。

表 3、PhilPaSS 交易筆數及金額

單位：筆、兆菲律賓披索、%

交易類別	2018		2017		成長率	
	筆數	金額	筆數	金額	筆數	金額
銀行間交易	648,756	40.28	599,756	46.55	8.17	-13.47
支票	23,816	6.28	25,566	5.85	-6.85	7.35
零售支付系統*	46,462	1.21	29,909	0.84	55.34	44.05
美元交易	161,711	32.55	142,170	26.91	13.74	20.96
政府債券**	47,161	2.04	43,172	1.88	9.24	8.51
PhilPaSS-Remit	601,764	0.02	851,237	0.03	-29.31	-33.33
公開市場操作	56,632	171.72	58,201	179.33	-2.70	-4.24
其他	43,639	6.24	40,910	2.18	6.67	186.24
合計	1,629,941	260.34	1,790,921	263.57	-8.99	-1.23

*包含 ACH、ATM、快捷支付系統等。

**包含初級及次級市場交易。

資料來源：整理自 Bangko Sentral ng Pilipinas (2019c)

二、零售支付系統

菲律賓央行為提升該國電子支付比率，於 2017 年發布國家零售支付系統(National Retail Payment System, NRPS)⁹框架，並在此框架下陸續推出 ACH 及快捷支付等快速且便利的零售支付服務。

(一)國家零售支付系統框架

NRPS 是菲律賓央行制訂之政策方向及監管框架，旨在透過確立相關原則及標準供支付服務提供商(Payment Service Provider, PSP)遵循，使其能夠提供更安全、高效且可靠的零售支付服務，目標是將該國電子支付比率自 2013 年的 1%，提升至 2020 年的 20%。

NRPS 主要原則是「促進互通性」、「建立公平且開放的競爭基礎」及「激發產業競合」，內容涉及該國境內以菲律賓披索進行之零售支

⁹ Bangko Sentral ng Pilipinas (2017)

付相關活動、機制、機構及使用者；而零售支付之定義為符合以下條件之一的支付行為：

1. 未直接與金融市場交易相關
2. 清算不具時間急迫性
3. 付款人、受款人或兩者皆為自然人或非金融機構
4. 付款人、受款人或兩者皆非支付系統直接參與者

(二)菲律賓電子資金移轉系統及營運網路(PESONet)

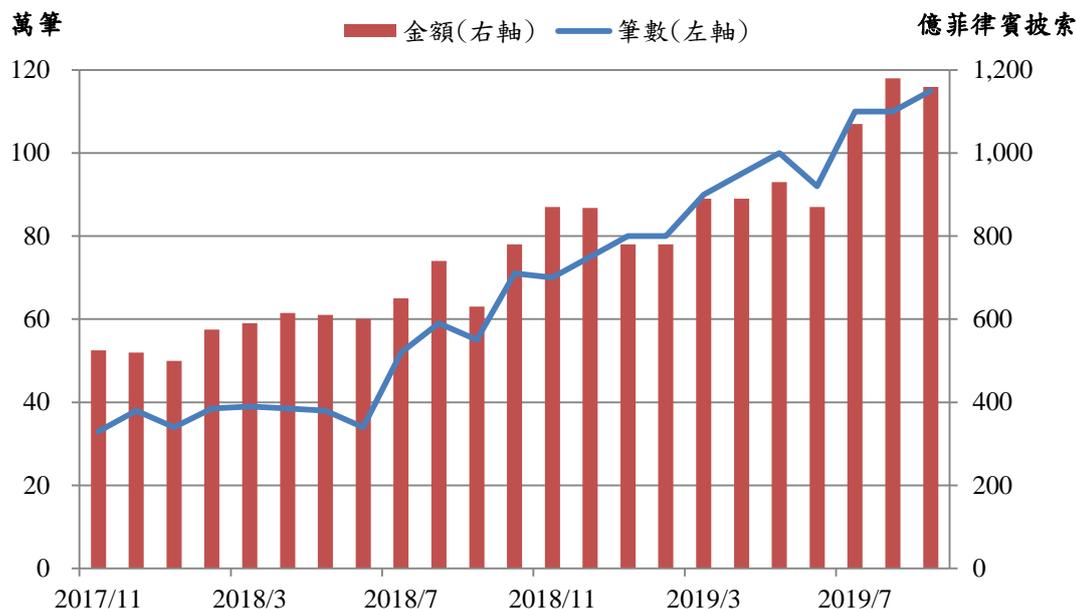
PESONet 是首個根據 NPRS 推出的 ACH 服務，交易時間、金額及次數均無限制，若付款人在特定截止時間前發送交易指令，資金將於同一營業日全額到帳，可供個人、企業及政府用於支付員工薪資、政府補助金、供應商貨款或其他不具時間急迫性之交易。本服務於 2017 年 11 月 8 日上線，截至 2019 年 11 月底共有 55 家支付服務提供商加入。

PESONet 以定時、批次、淨額清算方式處理跨行轉帳交易，由菲律賓結算所公司辦理結算，並於每個營業日的 16:30 將結算結果送交 PhilPaSS 辦理清算，款項將於 PhilPaSS 清算完成後方移轉至受款人帳戶。

PESONet 自推出以來交易金額及筆數持續上升，如圖 1。2019 年 9 月之單月交易筆數達 115 萬筆，金額 1,159 億菲律賓披索¹⁰(約新台幣 753 億元)。

¹⁰ 我國同期 ACH 業務交易筆數 130 萬筆，金額新台幣 3,238 億元。

圖 1、PESONet 交易金額及筆數



資料來源：菲律賓央行

(三) InstaPay

1. 簡介

InstaPay 是 2018 年 4 月 23 日上線的快捷支付系統，可供使用者全天候都能以銀行帳戶或電子貨幣帳戶進行購物、繳交醫療費、學費等，交易金額上限為 50,000 菲律賓披索，且資金即時到帳，使用者不受交易時間及次數之限制，商家亦無須架設刷卡機便可接受電子支付。

2. 清算方式¹¹

InstaPay 的清算方式係採預撥資金(prefunding)制，參加單位須於央行開立擔保清算專戶(Secured Settlement Account, SSA)，並於 PhilPaSS 營運時間內，將資金自準備金帳戶預先撥付至 SSA，

¹¹ Bangko Sentral ng Pilipinas (2018b)

作為 InstaPay 交易的擔保。此外，SSA 之餘額得全數作為法定準備金。

結算機構 BancNet 每個營業日將 InstaPay 交易之結算淨額傳送至央行 3 次，若參加單位為應付方，則扣減其 SSA 餘額，若為應收方，則增加其準備金帳戶餘額，清算時程如表 4；非營業日之交易將整併至次一營業日的第 1 次清算。

表 4、InstaPay 清算時程

InstaPay 交易時段	央行清算時間
前一日之 15:00~本日 8:00	9:00~9:15
8:00~11:00	12:00~12:15
11:00~15:00	15:15~16:00

資料來源：菲律賓央行

3. 參與者

截至 2019 年 11 月底，共有 31 家支付服務提供商提供 InstaPay 收付服務，另有 14 家僅提供收款服務。參加單位可依有無參加 PhilPaSS 細分為直接參加單位及間接參加單位，後者須透過前者之準備金帳戶及 SSA 辦理 InstaPay 的款項清算。例如當間接參加單位為應收方時，資金會先撥付至直接參加單位的準備金帳戶，再由直接參加單位將資金撥付至間接參加單位於自身開立之帳戶。

4. 風險管理方式

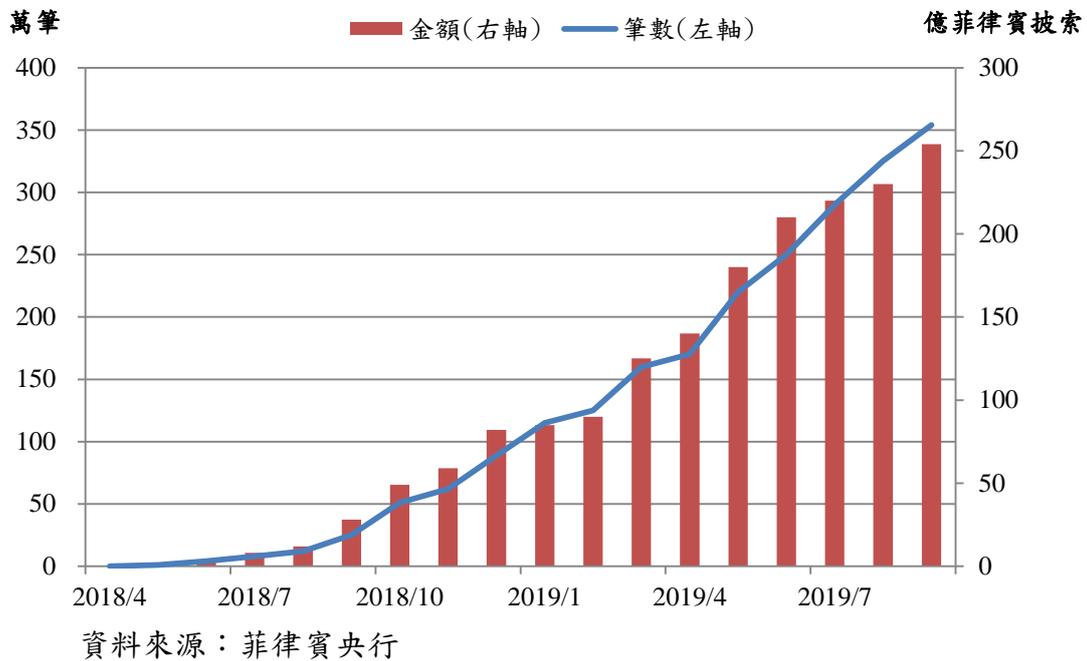
由於 InstaPay 之清算係採預撥資金制，故參加單位應於假日前增加預撥之資金，以因應假期間的交易需要；若參加單位之擔保清算專戶資金水位下降 50%、70%、90% 及 100% 時，將收到

警示 E-mail；當資金水位為負時，BancNet 將拒絕交易。

5. 營運量

InstaPay 自推出以來，交易金額及筆數持續高速成長，如圖 2。2019 年 9 月之單月交易筆數達 354 萬筆，金額約 254 億菲律賓披索(約新台幣 165 億元)。

圖 2、InstaPay 交易金額及筆數



(四) 菲律賓各種零售支付方式之比較

PESONet 及 InstaPay 等新興零售支付方式推出後，由於服務時間及手續費透明度等皆對消費者更為友善，故已部分取代原先透過支票或資金移轉機構等傳統支付方式，目前菲律賓各種零售支付方式之比較如表 5。

表 5、菲律賓零售支付方式一覽表

支付方式	到帳時間	金額上限	辦理方式	服務時間	手續費
PESONet	當日	無	電子	營業日 24/7	付款人支付、資金全額到帳
InstaPay	即時	5 萬披索	電子	365/24/7	付款人支付、資金全額到帳
支票	次日	無	臨櫃	營業時間內	手續費支付方式未統一，資金全額到帳
透過資金移轉機構*辦理	當日	無	臨櫃	營業時間內	付款人支付，受款人亦可能須付手續費

*非銀行的匯款公司，例如西聯匯款(Western Union)。

資料來源：菲律賓央行

(五) 菲律賓零售支付近期發展

菲律賓央行以 PESONet 及 InstaPay 為基礎，持續推動 NRPS 相關計畫，包含：

1. QR Ph

QR Ph 為菲律賓之 QR Code 共通支付標準，目前正由 6 家銀行及支付機構進行先導試驗(pilot)，其背後之金流係透過 InstaPay 辦理；菲律賓央行為提升國內支付工具的互通性，於 2019 年 10 月 17 日發布公告，要求 PSP 若提供 QR Code 支付方式，皆應採用 QR Ph。

2. EGov Pay

EGov Pay 於 2019 年 11 月 20 日正式上線，供民眾可以數位方式進行政府款項(如稅款、補助款)之收付，而其背後之金流係透過 PESONet 辦理，目前已有 9 個中央機關及地方政府加入。

三、支付系統之監管

根據菲律賓的第 11127 號共和國法(Republic Act 11127)，菲律賓央行有權營運及監管該國支付系統；此外，NRPS 中亦包含多項有關零售支付系統之監管原則。

(一)法源依據

2018 年 10 月生效的第 11127 號共和國法，又稱國家支付系統法(National Payment System Act, NPSA)，明定菲律賓央行應監管菲律賓的支付系統，以確保其穩定性及有效性。

菲律賓支付系統之監管由菲律賓央行的「支付系統監管局(Payment System Oversight Department, PSOD)」負責，包含制定相關規範、指定具系統重要性之支付系統、監管經指定的支付系統營運商等，且菲律賓央行有權對支付系統參加單位進行實地檢查，且可要求參加單位提交相關營運報告或統計資料，必要時得實施行政制裁。

(二)零售支付系統之監管¹²

為促進零售支付市場自由且公平的競爭、互通性、效率性及網路效果，NRPS 要求 PSP 須遵守以下規範：

1. **結算方式**：PSP 應透過結算機構辦理之多邊結算，將資金移轉至其他 PSP，不允許個別 PSP 訂定具排他性的雙邊結算協議。
2. **結算機構**：每一種支付方式(例如 ACH、快捷支付)僅能由單一結算機構辦理結算，惟單一結算機構可辦理多種支付方式

¹² Bangko Sentral ng Pilipinas (2018a)

之結算¹³。此外，各種支付方式之結清算規則應由參加單位共同決定，而非由結算機構決定，結算機構亦不得對參加單位施加不公平的標準或規則。

3. **手續費**：為提高透明度及競爭性，金融機構應向菲律賓央行提交其向客戶收取之手續費定價標準，央行彙整後再於官方網站向大眾揭露。此外，受款人不應支付手續費，且應全額到帳；付款人支付之手續費不得高於臨櫃辦理之手續費。
4. **到帳時間**：快捷支付部分，受款銀行應於接獲結算成功訊息後 3 秒內，將款項撥付至受款人帳戶；而 ACH 部分，受款銀行應於接獲結算成功訊息後 2 小時內(或不晚於下次清算時間)，將款項撥付至受款人帳戶。
5. **支付管道**：只要可行，經授權提供電子支付服務的金融機構，應於特定時限前讓消費者得透過電子管道(網路或行動裝置)進行 PESONet 及(或)InstaPay 資金移轉。
6. **其他要求**：金融機構應符合風險管理、互通性、資訊安全、消費者保護、反洗錢、反資恐等相關要求。

(三)零售支付產業自律

為促進產業合作，菲律賓之銀行及電子貨幣發行商¹⁴共同成立菲律賓支付管理公司(Philippine Payments Management Inc., PPMI)，負責

¹³ 例如，該國 ACH 業務僅得單由一個結算機構(即菲律賓結算所公司)辦理結算，其他結算機構不得辦理同項業務；惟菲律賓結算所公司除 ACH 結算業務外，尚可辦理其他種類支付方式之結算業務(如支票結算)。

¹⁴ 電子貨幣發行商須向菲律賓央行申請營業執照，並受該行之監管；截至 2019 年 11 月 20 日，菲律賓共有 49 家電子貨幣發行商，其中 31 家為銀行兼營。

制定自律規範、將結算合約標準化及協調業者彼此合作等。截至 2019 年 10 月 28 日，該公司共有 88 家會員。

菲律賓央行於 2018 年 1 月 12 日，指定 PPMI 為支付系統管理機構(Payment System Management Body)，並要求其須確保會員法遵情形、陳報相關報表資料予央行，且符合以下條件之零售支付系統參加單位皆須成為其會員：

1. 有銀行或非銀行電子貨幣發行商的執照
2. 持有客戶資金
3. 參與結算機構辦理之多邊結算
4. 直接或間接以準備金帳戶與央行進行款項清算
5. 符合結算機構的技術要求

參、分散式帳本技術、區塊鏈及其應用

一、分散式帳本技術

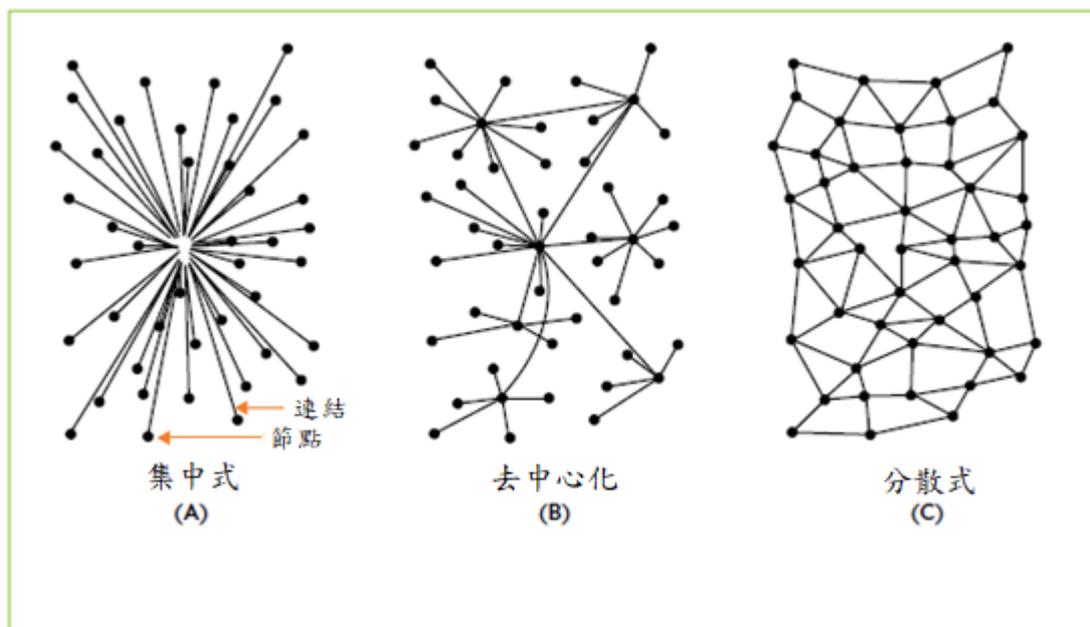
新技術與創新應用的出現，通常伴隨著令人難以理解的詞彙，以及各種人們對於它的不同看法，對於分散式帳本技術、區塊鏈和它的應用，最好的理解方式就是從了解它背後所使用的技術開始。

「分散式帳本」是一個資料庫，它在網路上由共同參與的節點透過共識演算法同步、更新和維護，「區塊鏈」是實作它的參考技術，分散式帳本的樣貌就是一個個的交易區塊透過密碼學及數位簽章技術串起的區塊鏈。

(一)集中式帳本與分散式帳本

透過下圖 3，可以比較容易理解集中式與分散式的概念。

圖 3、集中式、去中心化、分散式概念圖



資料來源：Asian Development Bank (2019)

集中式帳本是目前應用在金融領域最常見的資料儲存方式，由一個信任的中心機構儲存與維護資料，並且記錄資產的轉移，例如：大部分的證券結算與清算系統、許多國家中央銀行的大額支付系統，以及傳統的資產登記系統等。集中式帳本系統可以專注在單一實體系統的安全保護，也能夠兼顧運行的速度效能。

然而，集中式帳本系統仍然面臨風險，一個單一存放於網路伺服器上的帳本可能被惡意破壞、竊取或竄改，有許多數學方法可以量測需要花費多少電腦運算能力就足以攻破一台伺服器。

集中式帳本系統於是專注於網路安全與管理，例如相關的中央結算機構及證券交易所將交易集中於信任中心機構處理與管理，以減少與外部連結的風險。然而這種作法反而更將風險集中了，於是 BIS 等相關機構提出了一系列的監管方法與措施，為了防範金融市場基礎設施的系統性風險。

分散式帳本系統透過提高竄改資料的困難度來對付這些問題，在分散式帳本架構下，許多節點互相連結且同時記錄所有的資料，共同維護一個相同的帳本，分散式帳本需要透過共識來同步這些節點，有許多不同的共識演算法發展出來完成這個同步過程，例如：工作量證明 (proof-of-work)、權益證明 (proof-of-stake)、權威證明 (proof-of-authority) 等。

舉例來說，如果要攻破一台伺服器的困難度假設為 E ，那麼要攻破一個由 N 個節點組成的分散式帳本系統，就等於 $N \times E$ 的難度，所以分散式帳本系統較集中式帳本系統安全。然而這個假設的計算有點過於簡化，現實的情況攻破單一集中式帳本系統的伺服器，其困難

度可能遠大於攻破一個分散式帳本的節點，而且還有許多其他的變數會影響攻擊的難度，例如：不同的共識演算法、不同電腦的運算能力等，而在非認許式(permissionless)的分散式帳本系統又更難以計算其難度，因為任意網路上的電腦都可以隨時加入成為節點。

(二)認許式與非認許式系統

分散式帳本系統同樣也有許多種不同的樣貌，它可以是認許式(permissioned)或是非認許式的，認許式的系統運行在一個具有治理規範的私有領域網路當中，參與的網路節點需要被這個網路的治理規範認可才能加入，例如：金融領域的 Corda 平台就是透過 R3 組織的治理。

相反地，非認許式分散式帳本系統如：Bitcoin，在公開的網路上運行，允許任何人只要下載運行相應的軟體就能成為其中的一個網路節點，而它的軟體也是公開放在網路上供大眾共同開發。這種非認許式分散式帳本系統的參與者，可能無法隨時得知目前有哪些人正在運行軟體成為節點，而這部分的「未知」也可以成為一種安全的元素，因為如果節點總數是可知的，攻擊者就可以計畫一個確定的大量節點或運算能力來突破系統。其他非認許式分散式帳本系統的範例還有如：Ethereum。

非認許式系統透過公開以及永續運作的設計，無疑地展示了一個創造不同信任機制的極大可能，然而，它也暴露出治理與控制的問題與風險。在金融領域的應用中，認許式的系統設計較為尋常且合適。

二、區塊鏈技術及其應用

區塊鏈指的是資料如何被儲存在帳本上的方式，不同於一般資料的直接儲存，區塊鏈的資料是儲存於一個區塊中並且與一些其他的資訊綁定在一起，一個區塊包含許多的交易資料，而所有的區塊以一個固定的順序串聯成為一個區塊鏈，區塊中包含有時間戳記和前一個區塊的關聯。一個網路攻擊者若要竄改一筆交易，就必須修改整個區塊，以及與它相關聯的區塊，就是整條區塊鏈。這個防禦竄改能力的差異與前一個區塊的關聯設計有關，舉例來說，在 Bitcoin 區塊鏈中，這個關聯是透過取得前一個區塊的雜湊值(hash)來達成，也就是說，攻擊者不只要竄改當前區塊中的資料，也必須改動之後的每一個串在它後面的區塊，而修改一個區塊的困難度等於所有 Bitcoin 區塊鏈節點算力的總和。

區塊鏈的一個關鍵優點就是難以竄改，在一個以雜湊值作為關聯的區塊鏈資料庫中，任何對於資料的改動都會產生一個完全不同的雜湊值，而任何的更動都可以被輕易地偵測出來，只要透過比對存在下一個區塊中的關聯雜湊值即可。所以，區塊鏈特別適合使用於需要強力防止竄改的產品和服務，例如：加密資產與智能合約。這樣，區塊鏈技術就被使用來發行、儲存和轉移加密資產(如：Bitcoin)。

除了 Bitcoin 是有原生加密資產的區塊鏈以外，Ethereum 也是以區塊鏈技術設計的系統平台，它也有原生的加密資產 Ether，Ethereum 區塊鏈是一個非認許式的區塊鏈平台，其平台的目的是讓使用者可以透過智能合約在其上開發出各樣的應用。而 Corda 平台則是一個分散式帳本系統，但它的資料並不是以區塊鏈的方式儲存，所以狹義來說它並不是一個區塊鏈系統，同時它也沒有原生的加密資產，但它可以用來發行各樣的數位貨幣。另外，Hyperledger 平台是被廣泛認識的

區塊鏈系統，同樣地，它也沒有原生的加密資產。

智能合約指的是一種在區塊鏈上自動執行的軟體協定，當合約上的條件達成，它會根據合約上的指令自動完成交易。這類型的智能合約允許交易於各種不同的對象之間直接進行，而不需要第三方外部單位的介入(如：上級機構或中央結算機制)，其背後所倚靠的便是不可逆的執行程序，以及交易透明、可追蹤的區塊鏈技術。

智能合約所帶來的影響就是在個體與機構間的去中介化，人為的合約在執行上需要大量的人工介入，這通常需要耗費許多的時間，相反的，如果透過電腦來自動執行，可以節省許多時間。舉例來說，如果有一個合約交易的條件依賴於另一個合約交易的結果，透過電腦程式自動檢查條件並執行，可以大幅減少人為的失誤與時間的耗費，智能合約可以應用的場景相當地廣泛，可以用於借貸、貿易和證券交易等等。

圖 4 以使用者的數量與創新的複雜度及時間 2 個維度，展示了貨幣、制式服務、智能合約、去中心化自治組織 4 個區塊鏈應用的領域。

貨幣應用領域包含了支付、小費、群眾募資，它的應用相關使用者涵蓋了數十億的使用者，而制式服務、智能合約與去中心化自治組織則是更複雜的應用，需要更多的時間來發展，同時，它們涵蓋的終端使用者也較少。

圖 4、區塊鏈應用領域維度圖



資料來源：Asian Development Bank (2019)

三、分散式帳本技術的風險¹⁵

隨著許多基於分散式帳本技術的應用推出，各界對它的興趣也逐漸提升，紛紛開始探討分散式帳本技術應用是否會改變整個金融體系，從貨幣到基礎建設，甚至到募資。先撇開分散式帳本技術可以帶來的效益，值得注意的是，過去在日本與香港等地都有虛擬貨幣交易所被網路攻擊導致數十萬的客戶蒙受鉅額的損失，面對如此巨大的變革，我們需要更詳盡地對分散式帳本技術可能面臨到的風險進行分析。

(一) 資訊透明風險

分散式帳本其中的關鍵技術之一就是將資料同步到所有的網路節點上，這代表的是資料在各節點之間透明，並且可以進行驗證，也因此保障了安全性，這個特性相當適合拿來作為防制洗錢或是追蹤異常交易使用，因為交易歷史資料完整地儲存於區塊鏈之中，同時也能

¹⁵ Asian Development Bank (2019)。

夠證明資料的可信度。但資料的透明也同時暴露了隱私，也帶來相應的風險，雖然可以透過一些方式來保護機敏資料，例如：資料加密，但資料仍然存在於各節點之中。

分散式帳本技術能夠透過匿名或假名的方式來進行隱私保護，但是透過大數據分析再配合一些外部的資訊(例如：IP 地址)，仍然可以重新組合推知使用者的身分，這樣的數據分析甚至成了一門生意，許多公司提供這樣的數據分析服務。

資訊透明的風險不僅止於交易者的身分，甚至交易的內容以及交易的行為都會涉及，將這樣的個人資訊分散發布於網路節點當中，可能觸及個資法律的問題，甚至將會面臨鉅額罰款。

這個問題在跨國際的情況更為複雜，每個國家對於隱私保護的程度和法規皆不同，甚至可能有衝突，資訊保護的問題在分散式帳本技術上尚需各界廣泛合作研議，提出一個可行的解決方案。

(二)網路攻擊風險

分散式帳本技術並不會減少網路攻擊的風險，在某些情況下甚至反而可能增加風險。首先，錯誤的資料一旦被發布於分散式帳本中，它就會被快速的擴散出去至所有節點上，甚至被拿來使用，分散式帳本技術並不會更正錯誤的資料。

其次，分散式帳本技術是透過將資料同步到多個節點上，藉此形成一個巨大的防護網來確保系統的安全以及提供韌性(resilience)，單一的節點被駭或者損毀並不會影響整體系統的營運，這個特點看似優於目前集中式帳本技術，然而事實上或許並非如此。集中式帳本的中

心節點通常有較高的網路安全防禦等級，且有許多的安全規範與作業流程保護，相較於分散式帳本的節點則通常較弱。另外，分散式帳本的節點也並非每個都有相同的安全等級及措施，攻擊者可以針對較低安全等級的節點進行攻擊，進而對分散式帳本系統進行破壞。

目前並沒有一套對於分散式帳本系統的安全認證方法，對於分散式帳本系統安全性優於集中式帳本系統的迷思，仍需看其系統的設計以及應用，才能進行風險的評估。

(三)作業風險

作業風險是另一個分散式帳本技術值得被探討的議題，它可能是一個顯著的缺點，設計不良的智能合約一旦被發布在分散式帳本上，就會被快速的複製並散布於所有的網路節點之中，攻擊者可能利用這個程式弱點進行攻擊，而區塊鏈防止竄改的特性再加上智能合約的自動執行，反而更加重了此風險的影響。

即使 Bitcoin 區塊鏈被證實相當安全，但這並不表示所有的分散式帳本技術應用也同樣安全，有許多的錢包服務以及 Bitcoin 的交易所都有被駭的案例。現今區塊鏈技術相關的網路資源相當豐富，一般的資訊人員可以很容易地建置一個區塊鏈系統，然而，它可能一點都不安全。所以這個問題突顯出我們可能需要一個分散式帳本系統的認證組織，來確保其應用的作業風險能夠被有效控制。

(四)區塊鏈特性的風險

區塊鏈有一個獨特的特性就是不可更改，也就是說，資料只能不斷地新增上去，卻不能被刪除與修改，這樣的特性看似是區塊鏈的優

勢，但在某些國家中卻違反了當地的「資訊被遺忘權」。相同地，這樣的特性也使得某些回復機制難以實行，例如有錯誤資訊被登載於鏈上，則難以更正。

四、分散式帳本技術的優劣勢與 CBDC¹⁶

(一)分散式帳本技術的優勢

分散式帳本技術有兩個優勢：去中心化及高韌性。現行的集中式資料庫由信任的中心機構，透過大量的人為流程與規範，來進行重要資料的保護，為確保資料不被竄改，需要設計許多的作業流程，以及僱用許多的人力來執行資料保護，這通常需要花費大量的時間與金錢。分散式帳本技術的去中心化優勢是將資料分散儲存於網路上的各節點，然後透過密碼學與共識演算法來同步並防止資料的篡改，人工的作業流程以程式碼自動執行取代，資料的保護規範以密碼學來代替，這大幅降低了中心的維運成本。

另一個分散式帳本技術的優勢則是高韌性，每一個節點都處理所有的交易，而每一個節點都是平等的，沒有一個節點是特別重要的，彼此透過網路連結溝通，如果節點暫時損毀，當節點重新回復後，仍可從其他的節點回復資料，保持整體資料的一致性，如此，系統可以維持高韌性，不會因為單一節點毀損，導致整體系統暫時停止服務或是資料喪失。

(二)分散式帳本技術的劣勢

分散式帳本技術也有兩個劣勢：隱私性以及處理效能。分散式帳

¹⁶ MultiChain (2016)、Bank Underground (2017)

本技術需要透過共識演算法來同步帳本資料，所以必須公開其交易資訊內容來供各節點驗證其資料的真偽。相對於集中式帳本技術，可以透過簡單的權限控管來限制對於機敏資料的讀取，雖然分散式帳本技術也發展出處理隱私保護的相關技術，如：資料加密、零知識證明 (zero-knowledge proofs, ZKP)，然而，這卻會大幅降低處理效能，同時也犧牲了部分的系統高韌性特性。

分散式帳本技術的另一個劣勢是處理效能較集中式帳本技術低，因為分散式帳本技術的每一個節點都要處理所有相同的交易，每個節點做一樣的事，藉此確保安全性及高韌性，所以增加節點個數並不能提升處理效能，而分散式帳本技術每個節點又需要與彼此同步，再加上網路的延遲以及密碼學演算法的數位簽章運算，整體的處理效能明顯較集中式帳本技術緩慢。

(三)分散式帳本技術與 CBDC

CBDC 系統的特性是需要有高韌性，同時也要能夠避免網路攻擊導致單點失靈(single point of failure)，採用分散式帳本技術可以滿足這些需求，另外，透過密碼學與共識機制防止竄改的特性也可以節省人力與成本。然而，採用分散式帳本技術來發展 CBDC 系統也會面臨隱私保護的問題，目前有部分針對隱私性開發的技術平台被發展出來，例如：Corda 平台節點僅記錄與自身相關的交易，也僅傳遞交易資料給相關的節點，來保障交易資料不被不相關的第三方窺視，但這樣的作法將會犧牲部分的資料高韌性特性，因為如果有任兩個節點毀損，對作的交易資料將無法回復。Quorum 平台則透過零知識證明技術來進行隱私保護，然而，ZKP 技術需要耗費大量運算資源，將導致

處理效能大幅降低。

雖然採用分散式帳本技術來發展 CBDC 系統仍存在許多挑戰，但確實能夠為 CBDC 系統帶來相當的效益，所以許多國家也開始進行相關的研究與試驗。分散式帳本技術目前仍在持續發展中，或許未來這些挑戰能夠一一被克服。

肆、央行數位貨幣之議題

近年，為因應分散式帳本技術及加密資產等金融科技的崛起，加以部分國家電子支付比率逐年提高，國際間央行¹⁷與學術單位已開始研究發行央行數位貨幣的可行性。以下說明 CBDC 的類型與技術方案，以及國際間 CBDC 的發展與試驗案例。

一、CBDC 的類型

傳統上，中央銀行貨幣(central bank money)包括實體形式之鈔券，以及數位形式之準備金帳戶，而 CBDC 係為一種新的數位形式中央銀行貨幣。

支付暨市場基礎設施委員會(Committee on Payments and Market Infrastructures, CPMI)¹⁸將上述這種由「央行發行」並採「數位形式」的貨幣，依據「使用對象」(有限制或普遍使用)及「應用技術」(帳戶、代幣)等兩個特徵，分為 4 種類型(如表 6)。其一是傳統金融機構存於央行準備金帳戶的存款，屬於廣義的 CBDC；其餘三者則是近期所熱議的 CBDC，包括採用代幣技術的批發型(wholesale)與通用型(general-purpose)¹⁹央行數位代幣，以及開放帳戶給大眾使用的通用型央行帳戶，差異詳如後述。

¹⁷ Barontini and Holden (2019)調查全球 80 家央行，有 69%正進行相關研究。

¹⁸ CPMI (2018)。

¹⁹ 通用型 CBDC 有時亦可稱為零售型(retail)CBDC。

表 6、央行發行之數位形式貨幣的類型

	帳戶基礎	代幣基礎
限制使用對象 (如僅供銀行)	央行準備金帳戶 或清算帳戶	批發型央行數位代幣
普遍可用 (大眾均可使用)	通用型央行帳戶	

資料來源：CPMI

(一)使用對象

在使用對象方面，CBDC 可依是否有所限制分為批發型及通用型。前者僅開放給特定對象使用，如銀行等機構；後者則不限制使用對象，如社會大眾均可使用。

一般而言，批發型 CBDC 相較於通用型者，單筆交易金額大而每秒交易量(transactions per second)低。

(二)應用技術

在技術選擇方面，國際間²⁰將 CBDC 可分為帳戶基礎(account-based)及代幣基礎(token-based)。前者係將 CBDC 價值連結至中心化帳本記載的帳務餘額，後者係以代幣直接表示價值；茲將其中差異分說如下。

1. 交易流程及驗證機制

- (1) 帳戶基礎 CBDC 的用戶直接在央行開立帳戶。其交易流程與商業銀行開立的存款帳戶類似：付款人登入帳戶後，系統驗

²⁰ Bech (2017)、Kahn (2018)、IMF (2018)、CPMI (2018)、Norges Bank(2019)。

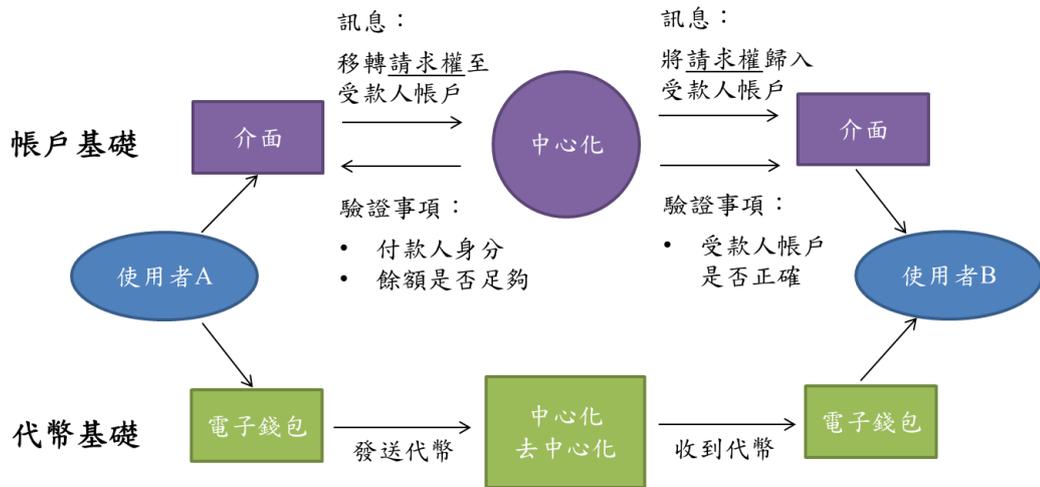
證付款人身分、確認帳戶餘額是否足夠、受款人帳戶是否正確，便將金額自付款人帳戶餘額移轉至受款人帳戶餘額，如圖 5。

- (2) 代幣基礎 CBDC 係以數位化的物件表示價值，例如一串數字代碼²¹，而數位代幣可能存於手機或卡片。數位代幣的移轉，係倚賴密碼學中的金鑰技術，如用戶需動用自身私鑰以控制特定數位代幣；背後的清算機制可能為中心化或去中心化(如圖 5)。
- (3) 這二種基礎的主要差異，在於交易驗證機制。在帳戶基礎之下，驗證事項係確認付款人身分是否就是發動交易的人，而帳戶提供者或系統營運者須控管詐欺交易的風險；在代幣基礎之下，驗證事項係其真實性²²，如特定的數位代幣是否曾發生雙重支付(如表 7)。
- (4) 交易驗證機制的不同，也對隱私產生影響。帳戶基礎 CBDC 的交易雙方彼此都知道對方的帳號，而帳號可連結至真實身分；在代幣基礎之下，付款人無需知道受款人身分，且也無需向受款人揭露該代幣以外的其他資訊。

²¹ 在非數位形式下，代幣基礎的央行貨幣包括鈔券及硬幣。

²² 現金也是代幣基礎的貨幣，只是為實體形式。為了驗證其真實性，受款人需要檢驗券幣本身是否係偽造貨幣，但不用確認付款人身分。

圖 5、帳戶及代幣基礎下之交易流程及驗證機制



資料來源：IMF

2. 與私部門金融支付工具的差異：

- (1) 商業銀行所提供的存款帳戶，為現行層級化金融體系之一種帳戶基礎的商業銀行貨幣，其清算機制倚賴商業銀行在央行開立的帳戶；而帳戶基礎的 CBDC 因交易雙方都直接持有央行帳戶，故交易即完成清算(如表 7)。
- (2) 交通票證等具預付性質的電子貨幣，係一種以代幣為基礎的傳統支付工具。若代幣基礎的 CBDC 係將價值存於卡片、手機等裝置，則其與交通票證等傳統支付工具非常類似，差異僅在於發行人是否為央行(如表 7)。

表 7、CBDC 設計選擇之比較

	帳戶基礎	代幣基礎
交易驗證	驗證用戶身分，包括： <ol style="list-style-type: none"> 1. 確認付款人是否有權支付 2. 餘額是否足夠 3. 受款人帳戶真確性 	驗證數位化物件，例如是否該數位代幣是否有合格的數位簽章
清算機制	中心化	去中心化 / 中心化
價值儲存位置	價值連結至帳戶餘額	以代幣表示價值
傳統金融體系支付工具	商業銀行提供的存款帳戶	預付性質的電子貨幣，如交通票證
CBDC 與傳統支付工具之差異	CBDC 交易雙方都在央行開戶，故交易直接清算	CBDC 發行人是央行，而非私部門

資料來源：整理自 IMF (2018)、Kahn (2018)、Norges Bank(2019)

二、CBDC 的技術方案

由於採用技術的不同，CBDC 的架構也將有所差異。一些國家根據「帳戶基礎」及「代幣基礎」，進一步提出發展 CBDC 的解決方案，以下以挪威央行(Norges Bank)的提案²³為例說明(如表 8)。

(一)帳戶基礎 CBDC

1. 開放式

- (1) 交易雙方之一方持有央行帳戶。例如，付款人可將其在央行帳戶的資金，移轉到受款人的商業銀行帳戶。

²³ Norges Bank (2019)。

- (2) 用戶所持有的央行帳戶，類似於現行商業銀行帳戶；亦即，用戶的資金可在央行帳戶及商銀帳戶之間互轉。
- (3) 央行需要為此發展相關的支付工具，以使用戶以 CBDC 進行支付，也需要涉入銀行間支付系統與相關的支付服務系統。
- (4) 央行可透過利率調控社會大眾對 CBDC 的需求；然而，在金融危機發生時，該類 CBDC 可能成為價值儲存工具，大眾資金可能轉入這種開放式的央行帳戶。

2. 封閉式

- (1) 交易雙方均持有央行帳戶，資金僅可在央行帳戶之間互轉，付款人無法將其央行帳戶的資金轉到受款人的商業銀行帳戶。
- (2) 用戶所持有的央行帳戶，類似於目前電子支付機構提供的電子貨幣帳戶，例如 Paypal。
- (3) 與開放式帳戶類似，央行也需要付出高昂營運成本，並提供客戶相關服務。
- (4) 對社會大眾而言，封閉式央行帳戶與一般商業銀行帳戶有別，對商業銀行貨幣的替代性較低。
- (5) 為防止金融危機發生時大量資金湧入，央行可藉調控利率，亦可對帳戶餘額設定限額。換言之，央行對這類 CBDC 的掌控能力較開放式帳戶強。

(二)代幣基礎 CBDC

1. 存於裝置

- (1) 透過實體設備儲存 CBDC，例如卡片、手機 SIM 卡、手機晶片等。
- (2) 用戶將卡片或手機接觸終端機或讀卡機以進行支付，且交易即完成清算，此與現金相似。
- (3) 由於 CBDC 存於離線設備，故不支付利息。
- (4) 倘若設備遺失或損壞，則儲存於其中的 CBDC 將無法取回。為了降低此損失，每台裝置可儲存的金額可能有所限制(也因此其對銀行存款的影響有限)。

2. 基於註冊

- (1) CBDC 儲存於線上平台，而非實體設備，為避免雙重支付，系統需設有註冊(register)功能，其負責登載相關的金鑰(但不記錄用戶的真實身分)，並持續記錄發生的交易。
- (2) 可設計使用者介面的手機 app，以使用戶連結至平台以動用 CBDC。
- (3) 由於平台記載用戶持有之 CBDC 相關資訊，而手機 app 的功能僅在於連結至平台，故手機遺失並不意味 CBDC 遺失。

表 8、CBDC 設計方案之比較

類型	方案	
帳戶基礎	開放式	<ul style="list-style-type: none"> • 付款人的央行帳戶餘額，可轉到受款人的商銀帳戶 • 類似一個商銀帳戶
	封閉式	<ul style="list-style-type: none"> • 付款人的央行帳戶餘額，只能轉到受款人的央行帳戶 • 類似電子支付機構提供的帳戶，如 Paypal 帳戶
代幣基礎	存於裝置	<ul style="list-style-type: none"> • 在實體設備(卡片、手機等)儲存 CBDC • 實體設備防止雙重支付 • 去中心化，類似現金
	基於註冊	<ul style="list-style-type: none"> • 帳本記錄交易 • 帳本防止雙重支付 • 帳本是由央行控制與管理 • 商銀等中介機構將代幣分配給用戶，並提供使用者介面

資料來源：挪威央行

三、國際間 CBDC 的發展與試驗案例

國際間，央行所探索的 CBDC 依批發型及通用型分為 2 類²⁴。前者包括日本與歐洲央行、南非、泰國、加拿大、新加坡等；後者包括厄瓜多、烏拉圭、柬埔寨、瑞典、丹麥、挪威、巴哈馬、以色列及中國大陸等。

²⁴ IMF (2018)。

以下介紹這 2 種類型 CBDC 的發行動機，以及部分國家已試驗的 CBDC 案例²⁵：

(一)發展 CBDC 的動機

一些央行研究應用於銀行間支付清算使用的批發型 CBDC，嘗試透過 DLT 改善傳統大額支付系統的安全及效率，如單點失靈及跨境支付的效率性問題，並且倘若未來金融市場部分資產被「代幣化」，則以 DLT 為基礎的支付系統將能發揮效益²⁶。研究通用型 CBDC 的央行，則期望透 CBDC 的發行，促進金融普惠化及市場競爭，或減少實體現金生產、運送及管理成本等²⁷。

(二)CBDC 試驗案例

1. 日本央行與歐洲央行²⁸

2016 年 12 月起，此 2 家央行針對 DLT 於批發型 CBDC 進行試驗，聯合發布一系列的 Stella Project 報告：

- (1) Phase I：採用 Hyperledger Fabric(版本為 0.6.1)平台，測試大額支付系統(BOJ-NET 及 TARGET2)及流動性節省機制(liquidity saving mechanism)是否能運行在 DLT 環境。試驗結果發現 DLT 的效能與網路規模大小及節點距離有關，且 DLT 有強化支付系統韌性的潛力，但鑒於 DLT 技術相對未成熟，暫不適合用於大額支付系統。

²⁵ 一些國家已積極研擬 CBDC，但尚並未發布試驗結果，例如中國大陸的數字貨幣。其他一些國家雖有類似研究，但並不能算是真正的 CBDC，例如突尼西亞的 e-Dinar 系統係由郵局而非央行創建。

²⁶ OMFIF and IBM (2018)。

²⁷ OMFIF and IBM (2019)。

²⁸ ECB and BoJ (2017)、ECB and BoJ (2018)、ECB and BoJ (2019)。

- (2) Phase II: 採用 Hyperledger Fabric(版本為 1.1.0-alpha)、Elements、Corda 等 3 個平台，設立單鏈(單一帳本)、雙鏈(2 個不同帳本)2 種架構，以原子交換(atomic swap)技術測試有價證券款券同步機制的可行性。試驗結果發現 DLT 平台可運行 DvP；此外，跨鏈交易未必需要特定中介者在雙鏈之間傳遞資訊，而可透過雜湊時間鎖合約(Hash Time Lock Contract, HTLC)實現，惟該技術也可能使交易雙方面臨本金風險(principal risk)²⁹。
- (3) Phase III: 採用 Hyperledger Fabric(版本為 1.2.1)平台，測試跨境交易在不同支付架構下的安全性³⁰，包括支付是否在鏈上清算、資金在清算前是否被圈存(或交由第三方託管)、滿足預定條件時是否可強制執行支付、是否支援 HTLC 或支付管道(payment channel)³¹機制等設計。試驗結果認為，透過將資金圈存及帳本之間清算的同步化等技術，可能提高跨境支付的安全性。然而，要實施這種新的支付架構，仍須考慮相關法規議題、技術成熟度，以及進行成本效益分析。

2. 厄瓜多³²

- (1) 厄瓜多央行於 2000 年將美元採納為法定貨幣，每年為美鈔汰舊換新的成本高達 3 百萬美元。2015 年 2 月，由厄瓜多央行發行的通用型 CBDC「dinero electrónico」正式營運，期能降低管理實體美元的成本，從而提高經濟成長。

²⁹ DvP 機制應使交易雙方避免本金風險。

³⁰ 在現行跨境支付下，付款銀行可能面臨信用風險，如中轉行收到付款銀行的資金後(尚未轉付給受款銀行)隨即倒閉。

³¹ 「支付管道」係合併交易雙方之間的多筆支付，僅以最後的淨部位進行清算。

³² Shirai (2019)及 IMF(2018)。

- (2) 個人以身分證字號開立 dinero electrónico 帳戶，並透過手機 app 移轉數位帳戶的資金。
- (3) 然而，可能因為當地民眾對央行缺乏信任，以及對美元的信心超過這種新的數位代幣，使用者的接受度很低，僅少數實際用於購買商品及服務或支付，結果該計畫業於 2017 年終止。

3. 烏拉圭³³

- (1) 烏拉圭央行(Banco Central del Uruguay)認為通用型 CBDC 或可降低實體現金的相關成本，包括印製、運送、防偽技術研究。此外，央行為能因應數位時代的來臨，並促進健全金融體系發展，有探索 CBDC 的需要。
- (2) 為累積更多 CBDC 相關的經驗與技術，烏拉圭央行於 2017 年 11 月，進行了一項為期 6 個月「e-Peso」的先導試驗。e-Peso 係數位化鈔券，設有電子鈔券管理平台(Global e-Note Manager Platform)記錄每張數位鈔券的所有權。系統以烏拉圭披索為擔保發行等值 e-Peso，社會大眾可以手機 app 進行交易，且交易即時清算。
- (3) 該計畫已於 2018 年 4 月結束，並收回所有 e-Peso(共發行 2 千萬烏拉圭披索)。試驗結果顯示成功，無任何意外事件發生，該國央行正評估技術方案及商業模式等議題。

4. 柬埔寨³⁴

³³ Bergara (2018)。

³⁴ OMFIF and IBM (2019)。

- (1) 目前該國人口僅有 22%擁有銀行帳戶或行動貨幣帳戶，為完善支付系統基礎設施、提升金融普惠化，並互通不同支付方式，柬埔寨央行(National Bank of Cambodia)於 2019 年 7 月以區塊鏈為基礎，進行通用型 CBDC 計畫「Bakong」。
- (2) Bakong 計畫將柬埔寨銀行業者及支付服務提供者串接在單一平台上，減少該國支付體系的零碎化現象與提高支付效率，民眾得以當地貨幣及美元進行即時零售支付。

伍、心得及建議

一、心得

(一)我國與菲律賓大額支付系統之差異比較

我國與菲律賓皆係由中央銀行負責營運大額支付系統，進行銀行間交易、零售支付、金融市場交易之最終清算，惟因國情不同而發展出各自的特色，茲比較我國中央銀行同業資金調撥清算作業系統(下稱同資系統)與菲律賓 PhilPaSS，如表 9。

表 9、我國與菲律賓大額支付系統比較

比較項目	我國同資系統	菲律賓 PhilPaSS
開始採行 RTGS	2002 年	2002 年
清算機制	即時總額清算	混合清算
帳戶類型	準備金甲戶 跨行業務結算擔保專戶	準備金帳戶 擔保清算專戶
清算交易類別	銀行間交易、證券、政府債券、票券、外匯、支票、信用卡、ACH、ATM 等	銀行間交易、政府債券、美元、支票、ACH、ATM 等
營運時間	09:00-17:40	09:00-17:45
期約交易期限	1 年	4 個日曆日
參加單位 (2019/12/4)	85 家	168 家
參加單位類型	銀行、票券金融公司、央行內部單位、結算機構	商業銀行、國有銀行、儲蓄銀行、農村銀行、具有部分銀行功能之非銀行、央行內部單位及財政部
一般交易手續費	單一費率	依交易金額 採階梯式費率
2018 年交易筆數	76 萬筆	163 萬筆
2018 年交易金額	新台幣 526 兆元	260 兆菲律賓披索 (約新台幣 171 兆元)

資料來源：作者整理

(二)我國與菲律賓對支付系統之監管比較

1. 法源依據

相較於菲律賓藉由訂定專法，給予中央銀行監管支付系統之法源依據，我國有關支付系統之法律，則是分別規定於金管會組織法第 2 條(金融支付系統，由中央銀行主管)，以及銀行法第 47 條之 3(涉及大額資金移轉帳務清算之業務，應經中央銀行許可)。

2. 主管機關

菲律賓央行為該國銀行業主管機關，同時監管大額支付與零售支付，而我國由央行擔任大額支付主管機關，至於零售支付部分，主要由金融監督管理委員會(下稱金管會)監管，央行則對透過同資系統辦理款項清算之零售支付系統加以管理，並就零售支付涉及外匯或金融穩定等議題時協助金管會。

3. 大額支付系統監管權責劃分

菲律賓央行將大額支付系統之營運及監管業務，分別由「支付清算辦公室」及「支付系統監管局」負責，並由不同副總裁督導；我國則係由央行之「業務局」及「資訊處」辦理大額支付系統之營運及監管。

4. 零售支付產業自律

菲律賓零售支付產業參與者透過建立菲律賓支付管理公司來確保產業自律，我國則是透過銀行公會及其轄下之電子支付業務委員會訂定自律規範及協助政府推行金融政策等。

(三)深入了解 DLT 技術，有助於掌控相關應用的風險

透過對於 DLT 技術與區塊鏈的深入了解，我們能夠更清楚其設計的原理，以及所產生的難以竄改、高韌性等特性與效果，進而藉由探討它與不同系統架構的比較，能夠探知 DLT 技術的優勢與劣勢。

近來由於 Bitcoin 帶來的風潮，DLT 的相關應用蓬勃發展，透過深入了解 DLT 技術，能夠有助於評估相關金融應用的風險，進而採取相對措施來因應。

(四)各國 CBDC 發展漸有與其他公私部門合作之趨勢

近來，一些央行彼此合作，研擬以 DLT 進行跨境支付的研究，俾提升國際匯款效率並降低成本，包括日本央行與歐洲央行的 Stella (phase III)、加拿大央行與新加坡金管局的 Jasper-Ubin、泰國央行與香港金管局簽立合作備忘錄(Memorandum of Understanding, MOU)、柬埔寨央行與馬來亞銀行(Maybank)簽立 MOU。

對於通用型 CBDC，根據官方貨幣與金融機構論壇(Official Monetary and Financial Institutions Forum, OMFIF)及 IBM 於 2019 年發布的聯合調查報告³⁵，受訪央行中有 64%認為該類 CBDC 仍須依賴私部門的中介功能，特別是在分配 CBDC 給大眾的層面，如同目前實體現金的分配方式也是透過銀行等中介機構。亦即，未來通用型 CBDC 的發展或許係朝向公私協力模式，特定中介機構可使用央行準備金或清算帳戶，並向大眾分配 CBDC，以及負責 KYC 與反洗錢等事宜。

二、建議

³⁵ OMFIF and IBM (2019)針對全球共 23 家央行進行調查。

(一)研議未來中央銀行法修正時，可納入監管支付系統之法源

菲律賓的國家支付系統法於 2018 年 10 月生效，提供菲律賓央行監管系統性重要支付系統更堅實的法源基礎，另根據本次學員分享各國監管經驗之簡報，包含新加坡、汶萊、柬埔寨、印尼、寮國、蒙古、緬甸、斯里蘭卡及泰國等，皆藉由訂定專法或於該國央行法內明文規範，使央行得據以監管支付系統，例如將發展高效率的支付清算系統列為央行經營目標，或央行有權執行適當措施以促進支付系統健全運作等；而我國有關支付系統之法律，則分別規定於金管會組織法及銀行法，央行另訂定「中央銀行同業資金電子化調撥清算業務管理要點」，作為管理同資系統連線機構之依據；未來研議修改中央銀行法時，似可納入本行監管支付系統之法源依據。

(二)持續關注 DLT 發展，培養多元人才因應金融創新應用

DLT 仍在持續發展階段，許多問題正逐漸被解決，例如：資源浪費、處理量能等問題，且有更多的 DLT 創新應用在支付、貨幣、有價資產、身分認證等領域。為了維護金融穩定並促進經濟成長，本行宜持續關注 DLT 發展，並積極培養多元人才，在業務、技術、法規、監理等層面累積相關知能，裨益因應未來各式新型態的金融創新應用。

(三)謹慎關注國際間 CBDC 的發展，並與產學界合作

為持續提升支付系統效率性，各國央行透過尋找及測試新興技術，以解決該國在支付領域的痛點。央行基於各國情形不同，目前已對不同類型的 CBDC 進行研究。

支付系統為國家重要金融基礎設施，在是否引入 CBDC 的議題上，除非央行能確保其將促進支付系統安全及效率，並不損及金融穩定與貨幣政策有效性，否則不宜貿然發行。鑑於 DLT 等新興科技日新月異，相關應用場景及創新亦可能與日俱增，為提升公共利益，本行宜持續關注他國央行及國際機構在 CBDC 領域的研究，並與產學界合作以累積更多經驗，俾便研究發行 CBDC 的可行性。

參考資料

1. Asian Development Bank (2019), “Distributed Ledger Technology and Digital Assets: Policy and Regulatory Challenges in Asia,” June.
2. Bangko Sentral ng Pilipinas (2017), “Adoption of National Retail Payment System (NRPS) Framework,” November.
3. _____ (2018a), “Guidelines on the National Retail Payment System (NRPS) Key Principles and Specific Rules,” March.
4. _____ (2018b), “Guidelines on the Settlement of Instant Retail Payments,” April.
5. _____ (2019a), “The Philippine Payment and Settlement System,” May.
6. _____ (2019b), “Rules and Regulations Governing the Philippine Payment and Settlement System,” May.
7. _____ (2019c), “Annual Report 2018,” March.
8. Bank Underground (2017), “Central Bank Digital Currency: DLT, or not DLT? This is the Question,” June.
9. Barontini, Christian and Henry Holden (2019), “Proceeding with Caution a Survey on Central Bank Digital Currency,” BIS Papers, No.101, January.
10. Bech, Morten and Rodney Garratt (2017), “Central bank cryptocurrencies,” BIS, September.
11. Bergara, Mario and Jorge Ponce (2018), “Central Bank Digital Currency: The Uruguayan e-Peso Case,” June.

12. CPMI (2018), “Central Bank Digital Currencies,” BIS, March.
13. ECB and BoJ (2017), “Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment,” September.
14. _____ (2018), “Securities Settlement systems: Delivery-versus-Payment in a Distributed Ledger Environment,” September.
15. _____ (2019), “Synchronised Cross-border Payments,” June.
16. IMF (2018), “Casting Light on Central Bank Digital Currency,” November.
17. Kahn, Charles, Francisco Rivadeneyra and Tsz-Nga Wong (2018), “Should the Central Bank Issue E-money?” December.
18. MultiChain (2016), “Blockchains vs Centralized Databases,” March.
19. Norges Bank (2018), “Central Bank Digital Currencies,” May.
20. _____ (2019), “Central Bank Digital Currencies,” June.
21. OMFIF and IBM (2018), “Central Bank Digital Currencies,” September.
22. _____ (2019), “Retail CBDCs: The Next Payments Frontier,” October.
23. Shirai, Sayuri (2019), “Money and Central Bank Digital Currency,” February.