

數位支付之技術、模式與監理

陳佑任

中華民國 113 年 6 月

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

摘 要

在各項支付手段多元發展的背景下，電子支付、行動支付、第三方支付等各種支付，以及 Apple Pay、Google Pay、Line Pay 等各種 Pay，已成為耳熟能詳的名詞。為有助理解不同支付間使用的技術或營運模式，本文首先分析數位支付的基本運作模式，並從中歸納出有助理解數位支付的 4 個構面：清算機制、數位技術、商業模式與法律基礎。

本文挑選網路銀行、信用卡、行動支付、加密貨幣等 4 項數位支付方式，並根據清算機制、數位技術、商業模式與法律基礎構面，分別介紹與分析這些支付方式的技術與模式。基於這些說明，彙總與比較各種支付方式的主要特色，並進一步說明各個構面在各種數位支付中，扮演的角色與彼此的關係。

目 次

一、 緒論	4
二、 數位支付概述	5
三、 網路銀行與 ATM 轉帳.....	9
四、 信用卡	11
五、 行動支付	13
(一) 行動銀行.....	13
(二) NFC 與 HCE 感應支付.....	14
(三) 電子支付／第三方支付與掃碼支付	16
六、 加密貨幣	17
七、 綜合比較	21
八、 結論	22
參考文獻	23

一、緒論

支付（payment）是指付款人將金錢或其他形式之有價值物轉移給受款人的行為或過程。支付涉及之手段十分多樣，如現金、支票、信用卡、轉帳、行動支付等。相對於以實物媒介為基礎的現金支付，非現金支付手段如行動支付，隨著各種技術與商業模式的演進，例如通訊裝置的普及、資訊服務的發展，業者的整合等，非現金支付的占比及重要性與日俱增，已極大程度地改變了日常生活與金融服務的樣貌。

在大多數非現金支付的背後，依賴資訊系統作為傳遞支付訊息的管道，這類型支付手段常被稱為電子支付，然而我國已有「電子支付機構管理條例」，為避免混淆，本文以數位支付一詞指涉較為廣義、依賴數位科技為基礎之支付方式與支付系統。

數位支付涉及許多科技之整合與應用，如行動裝置、網路設備、資訊服務、技術協定等，這些技術彼此間關係本就十分複雜，而不同支付方式與數位技術間的關係又不盡相同，若僅以特定角度說明，實不易理解不同數位支付的關鍵差異與發展重點。

本文將以支付的核心流程出發，梳理出數位支付的主要構面，並以這些構面分析幾種主要的數位支付方式。希望透過本文的介紹與分析，能夠幫助讀者理解數位支付與數位技術在其中扮演的角色，對於各種支付方式乃至於對未來新的支付手段之理解、評估與決策提供幫助。

二、數位支付概述

數位支付從付款人的觀點出發，通常是透過電腦或手機操作軟體，傳達支付指令後，將資金移轉至收款人，例如消費者透過街口、Line Pay 在商家掃碼，或是使用網路銀行轉帳。這些看似平常的支付行為，背後常隱藏了複雜的資訊流與資金流。

為協助分析數位支付背後的運作，最佳的方式是以現金支付作為對照。在現金支付中，移轉價值或資金的手段，是透過交付具有價值的實物，亦即實體貨幣本身。與之相對，在非現金、非實體支付中，在不攜帶及移轉實物的前提下，付款人僅能靠著發出支付指令，由支付機構代為將款項交付給收款人。

透過上述的對比，可以發現非現金支付包含幾項關鍵要素：

1. 付款人必須有發出支付指令的方法。
2. 必須存在能夠代為處理付款事宜的付款機構。
3. 付款機構必須能動用付款人的資金。

而付款機構若能不透過實物移轉，將付款人的資金交付給收款人，代表：

4. 必須存在能夠代為處理收款事宜的收款機構。
5. 收款人能夠向收款機構取得資金。

為了滿足要素 1-3，最簡單的機制是付款人將資金預先存放於付款機構，並透過雙方約定的方式，發出支付指令，付款機構接到指令後，即動用付款人存放的資金，交付給收款人。為了滿足要素 4-5，最簡單的機制即是收款機構暫時保管收到的款項，收款人可以透過約定的方式取出資金。

綜合以上情境，並進一步考量付款機構如何交付款項給收款機構，為了達到非現金支付，最為簡單的機制為：存在一機構同時作為付款及收款機構，付款人與收款人皆在此一機構開戶，付款人發出支付指令後，該機構同

時減少付款人的帳戶餘額、並增加收款人的帳戶餘額。

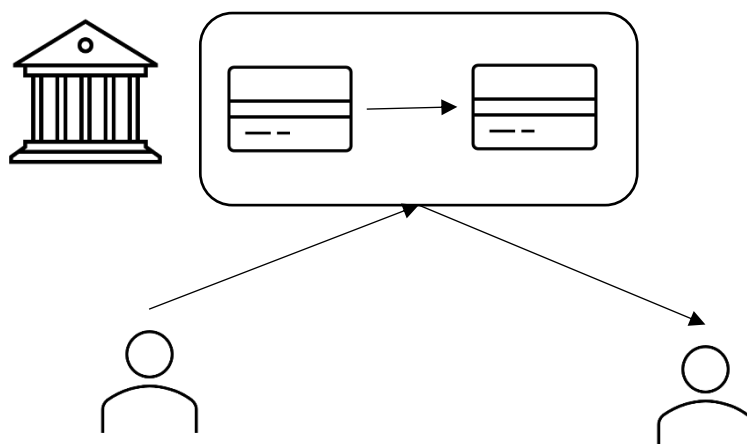


圖 1：支付流程：單一支付機構

接下來進一步探討，當付款機構與收款機構不是同一機構，付款機構要如何以非實物的方式，將資金移轉給收款機構呢？將此問題與前述非現金支付的分析對照，若將付款機構與收款機構，視作前述討論中的付款人與收款人，則可得知要完成付款機構 A 與收款機構間 B 的支付，最簡單的機制即是存在另一個機構 C，而機構 A 與機構 B 皆在機構 C 開戶，當機構 A 發出支付指令後，機構 C 即透過機構 A 與機構 B 之帳戶餘額的增減，完成資金的移轉。

上述機構 A 與機構 B 間的資金移轉，亦可以由機構 B 在機構 A 開戶，或是機構 A 在機構 B 開戶的方式來完成，此兩類情形可視作由機構 A 或機構 B 同時扮演機構 C 與其客戶的角色，因此在概念上，可將此兩類情形視作機構 A、B 皆在機構 C 開戶的變形，而不加以細分。

若再加入一機構 D，想要為它的客戶款項移轉至機構 B 的客戶，這時可能有許多種做法可以完成資金移轉，較具代表性的方式包含：

1. 機構 D、機構 A、機構 B 都成為機構 C 的客戶。在這種情境中，機構 C 作為提供多家機構支付服務的組織，通常被稱為清算

(Settlement)機構。

2. 機構 D 成為機構 A 的客戶，機構 D 向機構 A 發出支付指令後，機構 A 再作為機構 D 的代理，透過機構 C 將資金移轉給 B。

綜合以上分析，付款人若要透過非現金支付的手段將資金移轉給收款人，必須有提供接收指令移轉資金及接收資金之服務的機構。付款人可以將資金移轉給該機構的其他客戶，或是透過該機構作為更上層機構的客戶，將資金移轉給其他機構的客戶。因此，數位支付通常是透過階層式的支付網路，亦即透過機構間的資金移轉，完成付款人到收款人的資金移轉。

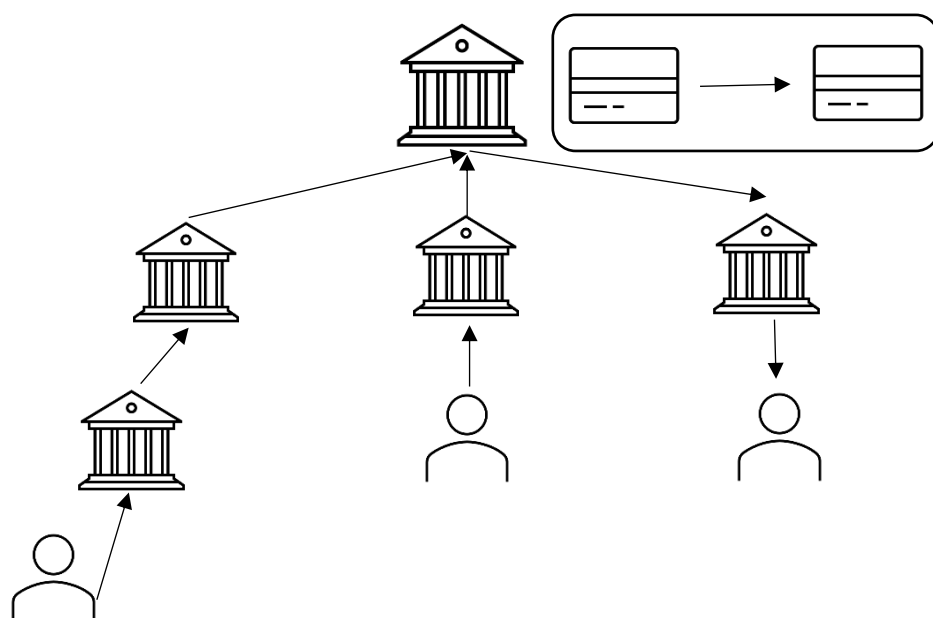


圖 2：支付流程：跨支付機構

換句話說，若要分析與解釋數位支付的運作原理，首先，須識別哪個機構扮演了清算機構的角色。清算機構的作用，是基於客戶指令，透過增減客戶帳戶的餘額的方式完成清算，亦即完成一項交易所涉及的權利義務關係。而識別了支付過程中的清算機構，以及它們之間的關係，也就瞭解了支付過程中最核心的資金移轉機制與流程。因此分析數位支付的第一個構面，是支付的清算機制。

其次，相對於現金支付的實體交換，非現金支付改以傳遞交易指令的方

式移轉資金，在支付過程中所涉及的資訊傳遞、處理、儲存，通常也依賴各種不同的數位技術。而要確保支付過程的安全性、交易指令的不可否認性，也須仰賴不同數位科技。因此分析數位支付的第二個構面，是數位支付過程中運用的主要技術。

再者，為了因應各種交易需求與交易情境，在技術演進的背景下，不同的支付方式被發展出來。一方面交易情境的需求會促進技術的應用與發展，但技術的選擇同時也會形塑支付手段的面貌。因此分析數位支付的第三個構面，是支付方式的商業模式與使用情境。

最後，清算機構能基於支付指令，完成權利義務的清算，是基於參與機構與其客戶及與其他支付機構間的協議，以及法律的授權，使各機構的行為及支付過程具備法律效力，因此，本文分析數位支付的第四個構面，是支付方式的法律基礎及其監管。

三、網路銀行與 ATM 轉帳

網路銀行與 ATM 轉帳是行之有年的數位支付手段，民眾可以登入網路銀行後，透過轉帳功能，輸入轉出帳戶、轉入帳戶與轉帳金額後，將資金從轉出帳戶移轉至轉入帳戶；或可以利用 ATM 提款機，插入金融卡後將資金轉出。

轉帳通常又分自行轉帳及跨行轉帳。自行轉帳之轉入帳戶與轉出帳戶屬於同一家銀行，此時僅需銀行自行清算即可完成此筆交易。另一方面，跨行轉帳之轉出銀行與轉入銀行不同，如同第二章的分析，需要由涉及交易的兩家銀行都在另一個機構(即清算機構)開戶，以完成跨機構間的資金移轉。

在台灣，銀行間轉帳與 ATM 等跨銀行交易訊息係透過財金資訊股份有限公司(以下簡稱財金公司)之跨行金融資訊系統(以下簡稱財金系統)傳遞。為協助財金公司跨行清算作業順利進行，做為我國支付清算體系樞紐的中央銀行，同意各銀行在央行共同開立跨行業務結算擔保專戶，以作為財金系統逐筆結計跨行支付之擔保，財金系統記錄各銀行在跨行業務結算擔保專戶之餘額(以下簡稱跨行基金)，並以跨行基金進行逐筆結計跨行支付。付款銀行發送支付指令至財金系統，由財金系統減少付款銀行之跨行基金，增加收款銀行之跨行基金，並將資金移轉交易訊息送到收款銀行，最後在由收款銀行確認交易後，將資金匯入收款人在該行的帳戶。

銀行如果需要調節跨行基金，係透過中央銀行營運的同業資金調撥清算作業系統(以下簡稱同資系統)，將存款準備金帳戶與跨行業務結算擔保專戶之資金互轉；若是增撥資金，銀行於同資系統發送支付指令，將增撥之資金自該銀行存款準備金帳戶轉入跨行業務結算擔保專戶，同資系統會自動將相關訊息通知財金系統，財金系統再據以增加該銀行之跨行基金；若是回撥資金，則自財金系統發送減提指令給同資系統，該筆資金即自跨行業務結算擔保專戶轉入該銀行存款準備金帳戶。

因此在清算機制層面，轉帳支付的主要機構包含銀行、財金公司與中央

銀行。而從銀行法、基於銀行法訂定之金融機構間資金移轉帳務清算之金融資訊服務事業許可及管理辦法、中央銀行同業資金電子化調撥清算業務管理要點、金融機構在中央銀行業務局開立及使用跨行業務結算擔保專戶應注意事項等法規，亦可看出上述主要機構之關係。

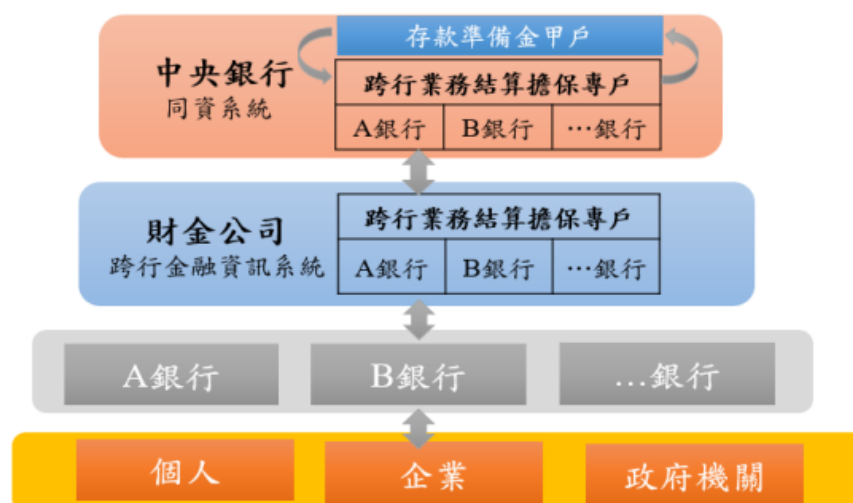


圖 3：銀行跨行轉帳機制
(來源：中央銀行)

從支付清算機構的構面來看，網路銀行與 ATM 並無太大的差異。而從數位技術的角度分析，兩者皆是以銀行端的資訊系統來接收與處理支付指令，而最大的差異則是驗證使用者的方式不同。網路銀行是透過事先約定的帳號密碼來識別與驗證客戶，並可能搭配多因子驗證機制(如手機 OTP)。ATM 則是透過嵌入在金融卡內的安全晶片搭配儲存於銀行端的晶片資訊來驗證使用者。

從商業模式或使用情境的構面來觀察，金融卡與網路銀行主要差異亦來自其驗證技術的差異。由於金融卡主要依賴安全晶片，安全性雖高，但需搭配特定硬體(如晶片讀卡機或是 ATM)，而 ATM 的硬體亦可搭配生物識別等裝置，達成更多元便利的操作體驗。相對來說，網路銀行只需要有上網裝置即能存取，網路銀行因為主要依賴軟體，其安全性較低，能執行的交易類型亦受限。但隨著行動裝置的普及，伴隨多因子驗證之規範逐漸成熟，行動銀行能執行的交易類型，基本上也與晶片卡接近。

四、信用卡

手持信用卡到特約商店以接觸方式刷卡，或是以非接觸方式感應刷卡，是許多人十分熟悉的消費場景，信用卡的交易流程可參考圖 4：消費者刷卡後，由特約商店發動，透過收單銀行經由授權網路，向發卡行請求授權後，完成在店內的消費。後續則由發卡行向消費者收取刷卡帳款後，透過清算機制將款項撥轉給收單銀行後，再由收單銀行支付給特約商店。

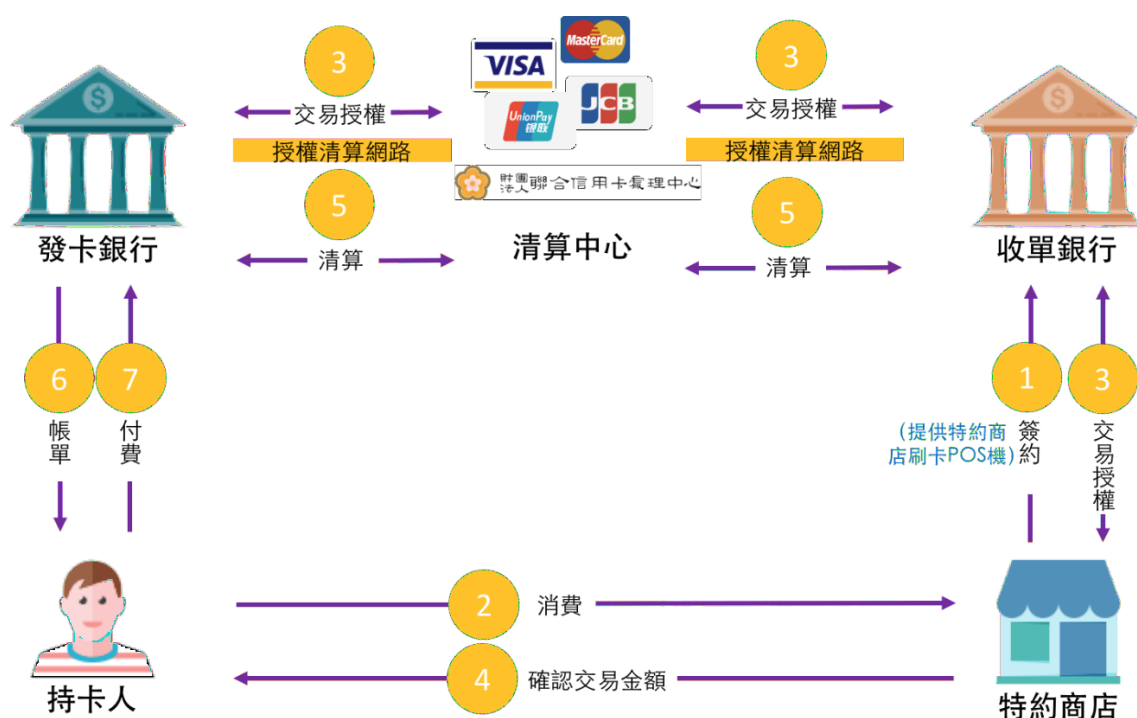


圖 4：信用卡支付機制
(來源：<https://www.mypay.com.tw/>)

若收單銀行與發卡銀行為同一家銀行，則清算機制類似自行轉帳，由銀行自行處理刷卡消費者與特約商店間的資金移轉，即可完成此筆交易。若兩者為不同銀行，則由收單行與發卡行，各自將涉及特約商店與消費者的消費與退款款項之所有資訊送交聯合信用卡中心(以下簡稱聯卡中心)結算(Clearing)¹，結計各銀行之應收、應付差額，集中送至中央銀行同資系統辦理清算，因此聯卡中心在央行有開立清算專戶，有應付差額之銀行透過同資

¹ 財金公司亦辦理信用卡之發卡收權、結算、收單等業務，惟為簡化說明，本文省略財金公司辦理之信用卡業務

系統將款項轉至聯卡中心之清算專戶，聯卡中心亦透過同資系統將款項自其清算專戶撥給有應收差額之銀行。

基於上述說明，在清算機制層面，信用卡支付的主要機構包含發卡銀行、收單銀行、聯卡中心與中央銀行。而主要法律依據為信用卡業務機構管理辦法。

相對於網路銀行的情境，使用者使用自有的聯網裝置，透過開戶銀行提供的功能完成支付。而信用卡的消費情境，消費者持有的信用卡並不具備通訊功能，必須透過刷卡機向支付系統發出支付指令，同時佈建刷卡機的收單銀行不一定是發卡銀行。因此僅靠發卡行的資訊服務無法讓其持卡者完成消費，而是需要組織訂定標準，以達成下列關鍵的資訊交換：1.信用卡具安全晶片，讀卡機可讀取並發送經安全晶片授權之交易訊息。2.收單行可透過授權網路取得發卡銀行的交易授權。

結合清算機制與數位技術之分析，信用卡支付的商業模式主要依賴信用卡組織建立下列機制：

1. 主要參與者：信用卡組織、發卡行、收單行。
2. 信用卡組織訂定卡片技術標準，使所有發卡行發行之卡片皆可被與收單銀行簽約之特約商店讀取與接受。
3. 信用卡組織建立授權網路服務，使收單銀行能與發卡銀行確認卡片授權。
4. 信用卡組織建立清算機制，使發卡銀行能將消費款項移轉至收單銀行。

由於讀取卡片的設備由特約商店準備，消費者除卡片外不須攜帶其他設備，且搭配先消費後付款的結帳模式，實使信用卡的使用門檻降到最低，且具誘因。在行動裝置尚未普及的年代，信用卡就能成為主要的非現金支付工具，顯見是技術與商業模式結合之成功範例。

五、行動支付

在行動裝置普及的基礎上，各家業者亦開始發展行動支付，時至今日，各種「Pay」已深入生活，成為耳熟能詳的名詞與品牌，例如較為著名的 Google Pay、Apple Pay、Samsung Pay、台灣 Pay、Line Pay、街口等。顧名思義，行動支付代表利用行動裝置進行支付的服務。然而除了利用手機裝置是唯一的共通點外，各種行動支付背後的支付網路與核心技術卻可能差異甚大，包含基於銀行支付網路、信用卡支付網路、電子支付業者等，分別介紹如下：

（一）行動銀行

若觀察銀行提供的服務，一般會將以網頁形式提供的銀行服務稱作網路銀行，以手機 App 形式提供的服務則稱作行動銀行。因此客戶透過手機行動銀行轉帳，亦是行動支付的一種類型。行動銀行在本質上是網路銀行的另一種形式，僅是強調其透過行動裝置作為連接設備，網路銀行的清算機制及相關技術已在第二章介紹，此處不再贅述，以下僅強調行動銀行利用行動裝置的特性，可發展出不同的使用場景，如：

1. 手機設備有許多與安全相關的硬體或功能，包含內建的安全晶片、生物識別(如指紋、臉孔)，或是手機本身可以作為多因子驗證中的使用者持有裝置，這些基於手機裝置特性的安全功能，可以加強行動銀行的安全性，並增加銀行客戶能透過網路服務進行的交易，提升客戶體驗。²
2. 可以利用手機相機的掃碼功能，介接其他支付服務，這可視作網路銀行的附加服務。例如銀行 App 可支援台灣 Pay 掃碼，手機相機讀取的二維碼內容發送給網路銀行系統，由網路銀行系統與台灣 Pay 系統介接後，完成資金的移轉。

² 依據金融機構辦理電子銀行業務安全控管作業基準，除少數例外(如辦理約定帳戶排除使用簡訊 OTP)，行動銀行可達到之安全強度已十分接近金融卡。

(二) NFC 與 HCE 感應支付

行動支付其中一種常見的場景，是消費者拿出手機感應店家的刷卡機後就完成付款。這樣的支付應用整合了既有的清算機制及新的技術，茲先就涉及的關鍵技術說明：

1. NFC 近場通訊 (Near Field Communication)

又稱近距離無線通訊，是一種短距離的高頻無線通訊技術，由非接觸式射頻識別 (RFID: Radio-Frequency Identification) 演變而來，允許電子設備之間進行非接觸式點對點資料傳輸，在 10 公分 (3.9 英吋) 內交換資料，其傳輸速度有 106 Kbit/秒、212 Kbit/秒或者 424 Kbit/秒 3 種，目前已成為 ISO/IEC IS 18092 國際標準、EMCA-340 標準與 ETSI TS 102 190 標準。

在 NFC 的各種運作模式中，卡模擬模式 (Card emulation mode) 相當於一張採用 RFID 技術的 IC 卡，可以替代現在大量的 IC 卡 (包括信用卡)、悠遊卡、門禁管制卡，車票，門票等等，卡片透過非接觸讀卡器發射的無線電磁場來供電，即便是裝置 (如手機) 沒電也可以運作。

2. 主機卡類比 HCE(Host Card Emulation)

若從實體支付卡片的发展來看，從前的磁條卡片容易被複製，因此催生了晶片卡。晶片卡將金鑰、憑證、交易機制等機敏性資料儲存在一個無法被竄改的硬體晶片上，然後再透過晶片所加密、簽章的訊息來保證交易的安全性。非接觸式支付卡片亦是從接觸式晶片卡演化而來，只是傳輸機制變成無線傳輸。

當行動裝置欲利用 NFC 進行支付時，由於 NFC 主要是一種傳輸技術，可讓支援 NFC 的兩設備互相傳輸資料。但純粹的資料傳輸機制並不能保證電子交易所需的安全性，因此 NFC 的標準中還納入安全

元件 SE(Secure Element)或 HCE(Host Card Emulation)的機制。SE 或 HCE 的角色類似於晶片卡上的晶片。POS 讀卡機與行動裝置溝通時，透過 NFC 無線傳輸與存放在 SE 或 HCE 中的卡片機制溝通。從 POS 機的角度來說，一個將 Visa 信用卡片機制存於 SE 或 HCE 中的行動裝置，與一張實體的非接觸式 Visa 信用卡是相同的。

SE 是硬體式的安全元件，其部署卡片機制的權限在發行安全元件的業者手中(如手機製造商或電信業者)，對支付服務業者來說，因為涉及較複雜的生態系，此種卡片部署機制難以普及。

HCE 則是軟體式的卡片模擬機制，讀卡機與作業系統溝通，由作業系統與 App 儲存卡片個人化資訊以扮演卡片的角色，支付服務提供者因此可以直接向行動裝置部署卡片機制。但由於 HCE 模式缺少如 SE 的硬體設備來確保卡片資訊不會被竊取，因此 HCE 需要配合其他機制來加強安全性。

因此，利用 NFC 與 HCE 技術，行動裝置可以模擬實體信用卡，並與店家的刷卡機以無線的方式感應付款。模擬實體卡片機制的優點在於，行動裝置與店家設備通訊時，傳輸的交易內容與使用信用卡交易時的格式相同，因此可以利用既有的信用卡支付網路完成資金的移轉。例如消費者在手機 App 中註冊了一張 A 銀行發行的信用卡，到透過 B 銀行收單的特約商店消費。此時資金的移轉、清算過程，就與拿出一張 A 銀行發行的實體卡片消費的相關過程相同。

但正如同 HCE 一節中說明，HCE 的技術是透過軟體的方式模擬卡片，其安全防護不如實體卡片上的晶片。因此為了提升安全性，行動支付通常還會搭配如代碼化(Tokenization)等機制，僅將最低限度的資訊放在裝置端，並在信用卡授權機制中增加額外的解碼與安全機制。例如增加虛擬卡號的管理服務，使用者在手機上綁卡僅儲存虛擬卡號，再由發卡銀行確認授權時，向虛擬卡號管理服務確認卡號的合法性與真實卡號。

(三) 電子支付／第三方支付與掃碼支付

由於網際網路與行動裝置普及，使資訊服務業者直接向終端使用者提供服務變得更容易，若將這樣的技術發展應用在支付領域，代表支付服務業者若要直接對商家與消費者提供資訊服務都變得更容易，使得業者獨立提供支付服務的門檻下降，也因此促成了各種行動支付的蓬勃發展。

依據電子支付機構管理條例，所謂電子支付機構，指的是經營代理收付實質交易款項³或收受儲值款項等業務之業者。電子支付業者須經金管會許可始得經營，但因同法亦許可未經營業收受儲值款項之非電子支付業者，在其所保管代理收付款項總餘額未逾一定金額(目前為日均 20 億元)的條件下，可經營代理收付實質交易款項業務，因此相對於依據電子支付機構管理條例成立之電子支付機構(如街口、全支付)，經營代理收付實質交易款項業務之非電子支付機構，一般又稱為第三方支付業者(如 Line Pay、蝦皮)。

在技術層面，由於電子支付/第三方支付同時服務店家與消費者，因此對交易流程有較高的掌控程度，得以降低店家與消費者的進入門檻，並提升消費者體驗。以目前最為普及的二維碼掃碼支付方式為例，若由消費者主掃，則店家僅需列印出二維碼陳列；若由消費者被掃，則店家之 POS 系統須與行動支付業者整合。在兩種模式中，消費者均僅須下載 App 並註冊即可使用。掃碼支付過程得以簡化，關鍵在於二維碼的產出與處理，皆由電子支付業者一手包辦，店家與消費者僅需產生條碼或是掃描條碼，後續的交易處理均由業者負責整合，使業者得以在持續增加各種服務與功能的同時(例如整合電子發票載具)，仍然維持交易過程的便利性。

在清算機制層面，電子支付業者可以整合既有的支付手段。例如一方與收單銀行簽約，作為特約商店以接受消費者的信用卡款項，另一方則透過銀行轉帳將款項移轉給店家，以達成代理收付交易款項的目的。

³ 依據電子支付機構管理條例，代理收付實質交易款項指接受付款方基於實質交易所移轉之款項，並經一定條件成就、一定期間屆至或付款方指示後，將該實質交易之款項移轉予收款方之業務。

六、加密貨幣

自 2009 年比特幣(BitCoin)誕生，至 2024 年美國 SEC 批准比特幣現貨 ETF 上市，加密貨幣已經經過 15 年的發展，市場從一開始陌生，現今對加密貨幣的接受度已越來越高。目前最主流的加密貨幣為比特幣及乙太幣，以下將從支付工具的角度介紹加密貨幣的運作。

比特幣及乙太幣的特性，是開放的、去中心化的支付系統，其底層機制，是運用區塊鏈(BlockChain)技術的分散式帳本(Distributed Ledger Technology, DLT)。如第二章所述，支付機構的核心機制之一，是透過增減其客戶的帳戶餘額，達成資金移轉的功能，傳統在支付系統或其他應用中，記錄帳戶餘額、交易紀錄的所謂帳本，通常都由負責該項業務的組織以集中的方式自行儲存與管理，而分散式帳本，指的是不同節點儲存與管理同一套帳本。不同節點可能由單一組織或一群特定組織營運，而在加密貨幣的場景中，則是開放由任何人都可成為節點，使加密貨幣不依賴任何組織，得以去中心化的模式營運。

區塊鏈是實作分散式帳本的一種方式，其將多筆交易包裝成一個區塊，每一個區塊都透過密碼學機制，串聯前一個區塊的資訊，區塊鏈與加密貨幣因此得名。由於後產生區塊的資訊包含先前區塊的資訊，導致已經發生的交易資訊若要被修改，必須一併修改之後所有區塊的資訊，大幅增加修改的困難度。然而，僅靠區塊鏈，在資料可以被輕易複製與修改的網路世界，並不足以保證交易的內容無法被修改，因此不同加密貨幣會設計不同的共識機制，以確保發送至區塊鏈上的合法交易能被所有參與的節點承認。結合區塊鏈與共識機制，可以在沒有中心組織的條件下，使交易被所有參與者承認且難以被修改。

比特幣所採用的共識機制稱為工作量證明(Proof of Work, POW)，其機制為生成新的交易區塊時，必須執行複雜數學運算並將結果附加於區塊內，成功產出區塊的節點亦可因此獲得比特幣。數學運算的困難度會根據區塊

產生的速度動態調整，因此越多節點競爭區塊的產出，會導致區塊運算的難度上升，這種依賴電腦執行複雜運算產出區塊，並因此獲得獎勵的機制，被類比稱之為挖礦，區塊產生者被稱為礦工。由於區塊的產出難度隨所有節點運算能力(算力)上升，因此特定節點若想要竄改區塊鏈中的交易內容，需要重新運算所有區塊並廣播其結果與其他節點的運算結果競爭，因此僅有在特定節點的算力佔比達 51%，即超過其他節點算力的總和的條件下，才有可能竄改區塊鏈內容(即所謂 51% 攻擊)。也因此比特幣實質上是透過各參與節點的算力總和，作為交易資料的保護機制。

乙太幣初期亦使用工作量證明，後為了節省運算的能源消耗，於 2022 年改採權益證明(Proof of Stake, POS)，各節點可以透過質押乙太幣獲得參與產生區塊的機會，質押數量越多、時間越長，獲得產生區塊及獎勵權利的機會就越高。由於產生區塊必須先擁有並質押一定數量的乙太幣，此機制實質上是由乙太幣的利害關係人以他們的資產為區塊的正確性背書。

乙太幣與比特幣另一個重大差別，乙太幣區塊鏈(即以太坊，Ethereum)所支援的智能合約是圖靈完備的，亦即能完成電腦可能執行的所有運算，而比特幣的智能合約僅支援與支付相關的部分功能。除此之外，以太坊的功能升級亦較為積極，這使得基於以太坊的各種去中心化金融應用(Decentralized Finance, DeFi)蓬勃發展，例如各種同質、非同質化代幣(Non-Fungible Tokens, NFTs)、去中心化交易所、甚至遊戲(Game Finance, GameFi)等。

從清算機制的角度分析，各種加密貨幣背後的區塊鏈，既然是由眾多節點共同使用、共同維護單一帳本，因此可以將區塊鏈看成是單一支付機構，而支付服務使用者的資金移轉，實際上是此機構內的自行轉帳。同樣的，基於區塊鏈的各種 DeFi，本質上也可以視作同一機構提供的不同服務。傳統金融在各種業務通常有不同的服務機構，如財金公司、證券交易所、集保結算所等，而帳本則由各機構自行集中管理，因此從服務網路的觀點，可視作分散式的組成結構。相對來說，加密貨幣的單一帳本，可以視作是不同金融

服務機構的集中化與中心化，但在資料的儲存及機構的治理結構上進行分散。

因此若僅就清算機制觀之，區塊鏈是透過將資金移轉或其他交易都納入單一機構、單一帳本來完成清算，與傳統金融並無根本差異。加密貨幣或區塊鏈最值得觀察的，是技術與商業模式的結合與演變。例如比特幣除了運用整合既有的加密技術建構分散式帳本，還利用具有獎勵性質的工作量證明，並且設計了比特幣的數量上限。這種模式的設計，提供區塊產生者足夠的誘因營運節點、處理交易，並利用區塊產生者的算力保護交易安全性。比特幣的模式確保了正向循環的發展：比特幣的價值與挖礦獎勵吸引足夠的礦工挖礦，足夠的礦工保證比特幣的安全性，比特幣的安全性及稀缺性又確保比特幣的價值。此種商業模式的設計，正是使比特幣得以不依賴特定機構，僅靠著網際網路上不特定的參與者，就得以發展至今的關鍵。

以太坊基於上述的基礎，進一步完善智能合約的機制。因此只要具備程式設計能力，就能在以太坊上發布智能合約並開啟新的金融服務，例如發行各種代幣、非同質化代幣。又例如去中心化交易所 Uniswap，即是具有代幣兌換功能的智能合約，其程式設計回饋機制，獎勵參與者質押代幣提供流動性，並根據流動性的資金供應情形，自動調整代幣間的兌換比率，可以說是 DeFi 的極佳案例。也因為前述的技術與機制特性，比特幣被視作數位黃金，偏向價值儲存與資金移轉的定位，而以太坊則被視作去中心化金融的創新平台。

金融服務的商業模式必須長期可維持，並對服務使用者產生價值。若與傳統金融對比，加密貨幣並沒有提供傳統金融不能提供的服務，而是其營運機構從傳統的金融機構變成網路上的節點與加密貨幣服務提供機構。由於加密貨幣仍是快速發展的領域，其優缺點尚無定論，加密貨幣是否能發展出普及的服務，可以從以下角度思考與觀察：

1. 加密貨幣之營運機制仰賴演算法，技術面上未知的漏洞或風險對平台穩定性有何影響？
2. 由於程式碼可以複製，開發社群發展、行銷策略與大眾認知等因素對於特定加密貨幣的價值之影響程度有多大？
3. 除了價值儲存，是否還有甚麼領域的金融服務？
4. 若結合分散式的處理技術，其商業模式是否具競爭力，又可從下面兩點觀察：
 - a. 從社群、去中心化的營運與管理模式的角度來看，哪一種服務在金融監管逐漸完善後，仍具競爭力？加密貨幣是否可作為金融創新的平台，持續為金融產業提供價值？
 - b. 加密貨幣屬於泛用且分散式的儲存與處理平台，與特定業務、集中式的資訊平台相比，哪一種服務在吞吐量、營運成本上更具競爭力？

七、綜合比較

基於第三至第六章對各種數位支付的介紹，以表格簡單比較如下：

表 1：各種數位支付綜合比較

		清算機制主要參與者	主要技術	商業模式特點	法律基礎
網路銀行、ATM 轉帳		收付款方開戶銀行、財金公司、中央銀行	主要參與者建置之資訊系統	交易類型多元，支援多種裝置，依據裝置特點提供不同的體驗	銀行法、中央銀行同業資金電子化調撥清算業務管理要點
信用卡		特約商店、收單行、發卡行、信用卡組織、聯卡中心、中央銀行	主要參與者建置之資訊系統、晶片卡	消費者僅需持卡，學習門檻極低	信用卡業務機構管理辦法
行動支付	行動銀行	同網路銀行	行動裝置	透過行動裝置的普及與安全機制提升網路銀行的體驗	同網路銀行
	感應支付	同信用卡	行動裝置、NFC、HCE	利用既有特店，消費者可免攜卡	同信用卡
	電子支付	電子支付業者、及網路銀行、信用卡之參與者	行動裝置	消費體驗由同一家業者整合	電子支付機構管理條例
加密貨幣		分散式帳本節點營運者	區塊鏈、共識機制、智能合約	去中心化	2024 年成立虛擬通貨公會，專法研擬中

八、結論

分析清算機制有助於界定特定支付方式中的重要參與者及其扮演角色，也因此能夠描繪出特定支付方式的整體結構。另外，法律與監管機制通常不會限制技術的使用，但新技術與支付方式的發展，若演變出既有法規無法有效管理的營運模式，則須制訂新的法規。因此透過法規，能更深入理解支付參與者間權利義務關係。基於清算機制與法律層面對支付參與者的關係，有助理解各種技術在支付過程中扮演的角色，並進一步分析支付方式得以實現的關鍵技術基礎。

例如在網路銀行中，其關鍵技術是銀行、清算機構的資訊系統及其相連的網路。在信用卡中，是晶片卡與發行組織的技術規格，使支付指令可以基於實體卡片發動。在行動支付中，是行動裝置的安全機制、感應軟硬體及聯網特性，使不同類型的行動支付得以實現。而在加密貨幣的單一帳本清算機制中，是區塊鏈作為實現分散式帳本的關鍵技術。

另一方面，透過對商業模式或使用情境的分析，也有助於從另一角度理解技術在支付過程中扮演的角色。這是因為技術的發展可以創造新的使用情境，並且新發展的商業模式，也受到技術的制約。例如在沒有行動支付的年代，卡片技術的發展，使消費者能以最輕便的設備-卡片，實現便利的非現金支付。而等到行動裝置普及後，因為已有現成的卡片支付體系，也使感應支付方式應運而生。

綜上所述，基於第二章對數位支付基本運作機制的分析，本文歸納出清算機制、數位技術、商業模式及法律監管等構面，並利用各構面在第三章至第六章介紹與分析網路銀行、信用卡、行動支付、加密貨幣等支付工具。而透過對各種支付工具的分析，亦有助於理解各構面在數位支付中扮演的角色，進一步得以運用上述各種構面，深入理解各種支付工具的技術與模式。

參考文獻

- 中央銀行 (2023), 中華民國支付及清算系統 (更新版), 中央銀行, 台北。
- 林政雄 (2011), 「信用卡收單共用業務系統經驗分享」, 財金資訊季刊, 第 68 期, 頁 37-44。
- 洪國峻、陳廷豪 (2014), 「消費金融—卡片支付業務發展新趨勢」, 財金資訊季刊, 第 77 期, 頁 2-9。
- 范姜群暉 (2015), 「從『電子支付機構管理條例』展望國內電子金融服務發展」, 財金資訊季刊, 第 83 期, 頁 2-16。
- 徐憶玫 (2014), 「支付系統營運管理新思維—管理走在第一線」, 財金資訊季刊, 第 79 期, 頁 22-28。
- 財金資訊股份有限公司 (2016), 財金公司「跨行通匯及 ATM 系統」遵循 PFMI 之揭露報告, 財金資訊股份有限公司, 台北。
- 陳恭 (2023), 全球數位貨幣發展及趨勢介紹 (Crypto 篇)。
- 國立台灣大學資訊管理學系 (2019), 新型態零售支付結算平台模式分析之研究, 中央銀行委託研究計畫, 台北。
- 黃麗蓉 (2020), 因應全球化電子商務之我國非銀行業者涉入傳統金流服務之發展, 台北外匯市場發展基金會委託計畫, 台北。
- 蘇偉慶 (2016), 「雲端行動支付利器—HCE 之金融應用」, 財金資訊季刊, 第 85 期, 頁 7-13。
- Bank for International Settlements (2003). *A Glossary of Terms Used in Payments and Settlement Systems*. Available at: https://www.bis.org/cpmi/glossary_030301.pdf
- Bank for International Settlements (2012). *Principles for Financial Market Infrastructures*. Available at: <https://www.bis.org/cpmi/publ/d101a.pdf>
- Reserve Bank of Australia. *Payments System*. Available at: <https://www.rba.gov.au/payments-and-infrastructure/payments-system.html>