基於區塊鏈技術建構多銀行數位交易機制之芻議

蘇品長 黃琬玲*

國防大學資訊管理學系

論文編號：NM-44-01-06

DOI：10.29496/JNDM.202405_45(1).0003

來稿2022年9月22日→第一次修訂2023年2月3日→第二次修訂2023年4月10日→

同意刊登 2023 年 4 月 19 日

摘要

近年來網際網路及資訊科技日益發展，區塊鏈已成為全球新興科技趨勢，一旦成功應用於軍事事務，將有助於提高部隊戰鬥力，並促成軍隊轉型發展。其中區塊鏈技術已在金融行業進行了廣泛的實驗、研究和應用，本研究透過區塊鏈分散式帳本、去中心化、資料難以竄改、匿名性等技術及密碼學理論基礎，並運用智能合約導入多銀行數位交易支付機制，解決目前電子商務中跨銀行及第三方來進行支付存在之安全性及信任問題，透過去中心化的系統，降低第三方參與，免除實體貨幣兌換程序並避免電子現金重複消費之問題，有效提升買賣雙方信任度，增強支付機制安全性，可適時導入國軍數位電子現金發行構想，強化數位交易安全機制，提升整體國防財務及後勤管理戰力。

關鍵詞：區塊鏈、智能合約、多銀行數位交易、金融服務、電子支付

*聯絡作者：黃琬玲 email: florence9839@gmail.com

Discussion on the Construction of Multi-Bank Digital Transaction Mechanism Based on Blockchain Technology

Su, Pin-Chang Huang, Wan-Ling*

Department of Information Management, National Defense University,
Taiwan, R.O.C

Abstract

In recent years, the Internet and information technology have developed rapidly, blockchain has become a global emerging technology trend. Once it is successfully applied to military affairs, it will help to improve the combat effectiveness of the troops and facilitate the transformation and development of the military. Blockchain technology has been extensively experimented, researched and applied in the financial industry. This research uses the technology and cryptography theoretical foundation of the blockchain, such as distributed ledger, decentralization, data hard to tamper, anonymity, and uses smart contracts to import multi-bank digital transaction payment mechanism. It can solve the security and trust problems existing in the current e-commerce for payment across banks and third parties. Through a decentralized system, it can reduce third-party participation, eliminate physical currency exchange procedures, and avoid the problem of double consumption of electronic cash. It can effectively improve the trust between buyers and sellers, and enhance the security of the current payment mechanism. Introduce it into the ROC Armed Forces digital electronic cash issuance concept can strengthen the digital transaction security mechanism and improve the overall defense financial and logistics management capabilities.

Keywords: Blockchain, Smart Contracts, Multi-bank Digital Transactions, Financial Services, Electronic Payments

*Corresponding author: Huang, Wan-Ling email: florence9839@gmail.com

一、前言

因應數位時代的變革，我國傳統金融體系已於 2019 年逐步朝向「開放銀行」(Open Banking)及「開放應用程式介面」(Open Application Programming Interface; Open API)方向轉型，使金融服務的使用者可以取得資料的自主權，而未來趨勢將很有可能結合區塊鏈(Blockchain)技術，實現去中心化的金融服務(彭思遠，2021)，國際研究暨顧問機構 Gartner 也發表，預估於 2030 年，區塊鏈可能帶來高達 3.1 萬億美元的新商業價值，並估計在 2025 年時，其中一半金額所帶動的附加商業價值是為了改善現行營運作業流程而產生的(Gartner, 2022)；另分析師 Avivah Litan 表示區塊鏈將成為未來金融體系的主流，讓交易變得更加安全。

在區塊鏈技術興起之前，網路交易大部分都必須仰賴金融機構作為可信賴的第三方，然而在這種基於信用的模式下，消費者所有交易資訊、機敏資料均儲存及掌控在第三方手上，消費者對於第三方必須完全信任，並且無法參與驗證（李宛蓁與黃杭浔，2016)。近年來，區塊鏈技術不斷發展，利用其去中心化、分散式帳本、不易竄改、智能合約(Smart contract)及共識機制等特性，逐漸影響到各行各業，其中在金融服務領域中，最令人關注和期待(黃敬翔，2019)，主要是因為透過區塊鏈技術可以有效降低交易及營運成本，提高監管能力並消除不必要的中介，建立分散式信任，並促進銀行間交易支付過程(Ramchandra et al., 2022)，而去中心化金融服務和商業模式，使的金融體系得以跨國界、交易自由，並更加透明化及創新發展(Chen and Bellavitis, 2020)。

在傳統支付過程中，多以實體貨幣(現金、紙鈔、硬幣)作為支付工具，隨著數位產業及電子商務發展，我國消費型態逐漸改變，電子支付日益普及，根據金融監督管理委員會(金管會)統計，截至 111 年 6 月底止，使用人數已多達 1 千 7 百餘萬人(金管會，2022)，未來電子支付將會成為支付工具的主流；常見的電子支付機制包含信用卡型、帳戶型與電子現金型三種方式，其中電子現金的概念與傳統貨幣較為接近，使用上的風險與交易成本相對較低，因此深受消費者喜愛，另在向金融機構申購時會留下申請開戶紀錄，在使用上具有匿名性，可保障消費者的隱私與帳戶的安全（郭木興，2003)。然而在眾多發行電子現金的銀行中，各個機構彼此為封閉體系，電子支付系統亦屬於封閉體系，無法進行跨機構間款項轉移(楊金龍，2019)；集中式的數據儲存具有單點故障、傳輸中斷、資料遺失的風險(Liao et al., 2022)，商家在收到不同銀行所發行之電子現金須有發行銀行之公開金鑰或是驗證資訊，才能驗證所收到電子現金的合法性(曹偉駿與蔡欣潔，2010)，在管理上造成不便；跨銀行進行電子現金款項轉移時，因系統無法互通，需透過存放在中央銀行的準備金，負擔交易清算成本，進行跨銀行清算(楊金龍，2019)；另在電子商務中，為了確保消費者與商家雙方交易的安全性、完整性、不可否認性及驗證用戶身分，必須透過公開金鑰基礎建設(Public Key Infrastructure; PKI)來實現，由憑證中心(Certificate Authority; CA)確認身分資訊，使用公鑰來簽發憑證，然而當憑證中心系統遭受駭客攻擊入侵竄改時，將對用戶身分資料保密性、完整性、不可否認性及真實性等造成極大的危害(蘇品長等，2014)。

因此本研究規劃將運用區塊鏈技術結合智能合約與密碼學原理，設計一個具安全性數位交易支付機制，由多銀行組成聯盟鏈，共同維護帳本，透過區塊鏈即時完成跨銀行清算，達到金流互通、資訊流同步一致與資料長時保存的效益，改善銀行之間系統介接及系統維運的成本，提升商家與消費者便利性；而在區塊鏈架構下之多銀行共同參與支付機制需考慮在區塊鏈上匿名監管問題，建立完善的信任機制，因此導入自我認證機制，解決憑證中心可能無法信任導致資訊安全的問題，使銀行、消費者、商家等電子商務中的參與人員身分資料達到完整性、不可否認性及真實性，有效提升交易安全；透過部份盲簽章方式實施電子交易支付，於交易過程確保電子現金有效性，

避免交易內容遭洩漏，亦可解決已簽署之電子現金難以辨識其額度或時效的問題，進而達成電子商務交易安全性，促進電子支付的發展，具備以下優點：

（一）透過區塊鏈結合智能合約設計，達成多銀行金流互通、資訊帳本同步一致及系統自動化，避免資料偽冒及遭竄改之風險。

（二）應用橢圓曲線部份盲簽章技術於電子支付過程，避免交易資訊在傳送過程遭有心人士非法竊取，並可確保電子現金有效性。

（三）運用橢圓曲線特殊點加法運算及其在與 RSA 相同的安全複雜度之下，僅需較小的密鑰長度，可以避免大量的指數運算，有效降低系統負荷，並達到機密性（Confidentiality）、完整性（Integrity）、不可竄改（Immutability）及不可否認性（Non-repudiability）等資安特性，強化電子商務交易安全度。

二、文獻探討

本章節分類整理、歸納分析與本研究相關聯之文獻，並針對區塊鏈、金融服務、電子支付及密碼學等與本研究相關的技術，加以彙整作為本研究的基礎，分述如后：

2.1 區塊鏈介紹

區塊鏈技術日新月異，隨著比特幣問世後，持續不斷演進，如今已成為一項具前瞻性和獨立研究的技術領域，目前在金融、能源、物聯網、健康、供應鏈、保險、媒體等不同領域中快速發展與應用（Chen et al., 2020），本章節彙整區塊鏈緣起與發展、區塊鏈技術與架構、區塊鏈特性與類型實施介紹，分述如后：

2.1.1 區塊鏈緣起與發展

在 2008 年爆發全球金融風暴，中心化的機構已無法被完全相信，而由中本聰於是年所發表的論文，一篇名為「比特幣：一種點對點的電子現金系統」的白皮書，內容描述比特幣及相關演算法，提出一種新的電子現金系統，採用點對點網路（Peer-to-Peer; P2P），不須倚賴可信任的第三方執行交易（Nakamoto, 2008），於 2009 年比特幣誕生，成為一種新型態的數位貨幣；而比特幣即是採用區塊鏈技術為底層架構的加密貨幣，區塊鏈在本質上是一種去中心化的分散式帳本資料庫，透過密碼學演算法，由一串鏈接的區塊所組成，確保區塊內的交易數據不可竄改，在沒有中心的節點控制下，保證資料一致性（鄒均等，2018）。而區塊鏈系統的三個重要屬性，去中心化、安全性和可擴展性，需達成平衡與兼顧，因此在區塊鏈去中心化架構下，尚需考慮安全及效率之問題，如區塊交易速度、智能合約安全性等問題等，目前針對學術界的發展現況和研究，和將區塊鏈的演進區分為區塊鏈 1.0、2.0 及 3.0 三種層次，摘述如后：

（一）區塊鏈 1.0

區塊鏈 1.0 為數位貨幣應用，它指的是透過區塊鏈分散式帳本技術為基礎，利用共識和挖掘機制來交換數位貨幣的概念，打造一個不需仰賴第三方的金流系統，如匯款、轉帳及數位支付系統等，將交易從一個用戶直接轉移到另一個用戶，其中最具代表性為比特幣，自 2009 年比特幣推出以來，相較傳統貨幣它證明了其可靠性、獨立性和安全性（Lee et al., 2021），而在區塊鏈支付系統中，Hu 等學者（2019）提出一種基於以太坊區塊鏈的支付方案，在偏鄉地區實際驗證金融交易是可以穩定運行，確認區塊鏈在交易支付上具可擴展性。

（二）區塊鏈 2.0

區塊鏈 2.0 是數位經濟，被稱為是在數位貨幣之外的金融應用，利用智能合約，依照預先指定的概念和規則，可以自動執行各種業務流程，徹底改變傳統金

融交易和支付系統，此類應用包含去中心化金融(DeFi)、證券交易、供應鏈金融等，是更廣泛的經濟和更金融應用(Cheng et al., 2021)，由於智能合約程式碼是開源的，因此在開發時需透過相關工具(如 FSolidM、KEVM、MAIAN、Securify、Mythril)，進行漏洞和安全性檢測，避免遭受惡意攻擊(Di Angelo, 2019)。

(三)區塊鏈 3.0

區塊鏈 3.0 是在數位貨幣和金融以外，一種以信任為核心價值的新型經濟形式，推廣至政府、健康、科學、文化和藝術等各領域的應用，並側重於對社會去中心化的監管和治理(Swan, 2015)，各領域可透過區塊鏈技術改善原有的業務模式及生活，區塊鏈最具未來性的前景應用是智慧城市，包含智慧治理、智慧生活、自然資源智慧利用、智慧市民、智慧經濟等要素(Sun et al., 2016)。

2.1.2 區塊鏈技術與架構

一個完整的區塊鏈系統並非單一技術，其中包含儲存數據的區塊、數位簽章、時間戳、點對點網路架構及共識演算法等，而區塊鏈的核心技術是在沒有中心化的控制及無信任基礎的情況下，透過共識機制達成共識，並由節點之間共同維護分散式資料庫(鄒均等，2018)，每個區塊包含多筆交易，而每個區塊中包含前一個區塊的雜湊值、此次區塊的雜湊值、隨機數、當前困難度、區塊產生的時間戳、交易紀錄、挖掘礦工及礦工獎勵(李耕銘，2021)，區塊鏈架構如圖 1 所示。

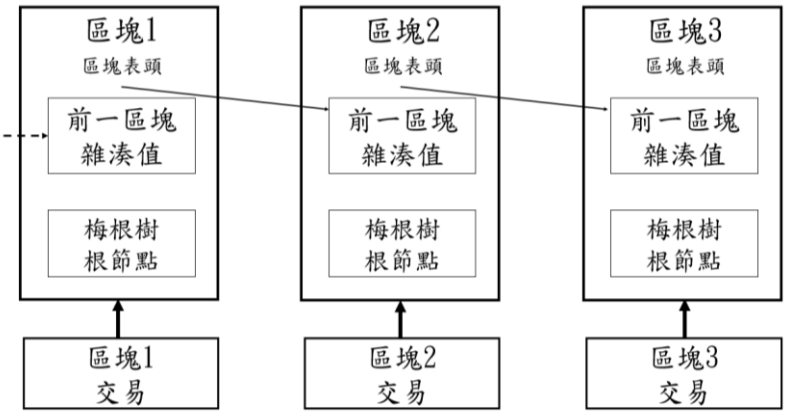

圖 1 區塊鏈架構示意圖
資料來源：鄒均等(2018)

2.1.3 區塊鏈特性與類型:

區塊鏈是由數學、密碼學原理及演算法所組成，其主要具備五大特性，其一為匿名性，各節點在區塊鏈上以不具名方式參與，使用代碼作為名稱，各節點之間是基於交易錢包與交易地址而非個人身分進行資料交換。其二為不可竄改性，當交易紀錄打包成區塊，並同步至各節點，當節點欲竄改區塊鏈資料，則需具備 51%全節點算力，因此任一節點無法任意竄改資料，交易資料具備高可信度。其三為去中心化，無第三方驗證機構單位，採用點對點分散式儲存機制，資料由節點與節點之間共同維護，並驗證訊息真實性。其四為可追溯性，區塊鏈上資料環環相扣並，資料上區塊鏈後都會被記錄，交易紀錄時間序列無法更動，具備可追溯性。其五為共識機制，當新的區塊被廣播到整個區塊鏈網路，節點將交易打包成一個區塊，並加入區塊鏈中，交易紀錄被鏈上的其他參與者確認並接受。

依據區塊鏈的參與者、去中心化程度及應用規模，可分區為「公有鏈」、「私有鏈」

及「聯盟鏈」，其特性如表 1 所示。

(一)公有鏈

公有鏈是高度去中心化的，帳本完全公開透明，參與節點無需經過授權，任何人都可以參與，並在公有鏈上進行資料發送、接收、存取及交易認證，其中比特幣和以太坊是兩個發展最著名的公有區塊鏈。

(二)聯盟鏈

聯盟鏈即是兩種區塊鏈的混合，由聯盟與多個組織共同構建，是需要經過授權的，可以滿足私有鏈的隱私性，又能達到公有鏈共識機制的特性，每個組織都是區塊鏈的一個節點，如果其他組織想要加入聯盟區塊鏈，需要聯盟的授權。

(三)私有鏈

私有鏈僅由一個組織控制，該組織建立並規範授權規則，控制誰可以參與、執行共識和維護共享帳本，參與私有鏈的節點受到嚴格的控制，資料發送、接收、存取及交易權限均受到限制，因此私有鏈交易速度較快，性能較佳。

表 1 區塊鏈特性

類別	公有鏈	聯盟鏈	私有鏈
公開程度	高	中	低
權限	不須授權	須經授權	須經授權
交易速度	低	中	高
可擴展性	低	中	高
去中心化程度	高	中	低
成本	低	中	高
典型代表	Bitcoin、Ethereum	Hyperledger Fabric、Corda	Quorum

資料來源：Zhang and Huang（2022）

2.2 區塊鏈導入金融服務介紹

在金融領域中，透過區塊鏈架構作為一種新的交易底層技術，有效整合金融資訊，提升系統的運行效率和服務質量(Zhang et al., 2020)，本章節介紹區塊鏈導入我國金融服務之發展潛力與效益，摘述如后：

2.2.1 貿易/供應鏈融資

中國信託銀行於 2016 年加入全球區塊鏈組織，發展數位金融，於 2019 年 10 月奇美實業出貨給波蘭的進口商，透過開發的「國際區塊鏈信用狀平臺」，擔任交易過程中的押匯行，完成我國首筆真實交易，利用區塊鏈去中心化、即時傳輸、無法竄改、公開透明及可溯源的特色，將作業流程從 5 天縮短至 1 天，並簡化實體文件傳遞流程，有效提升交易安全性及國際貿易效率(魏喬怡，2019)。

國泰世華銀行於 2021 年與 7 大銀行(上海商銀、台中銀行、新光銀行、陽信銀行、遠東商銀、元大銀行、永豐銀行)、2 大航運商(陽明海運、長榮海運）組成「環球貿易共享區塊鏈」，透過安全雜湊演算法技術，運用於現行進出口貿易融資，如圖 2 所示，將銀行貿易融資的資訊公開化，提高可信度，使各銀行可防範企業重複融資，並達成在保護雙方隱私的前提下，於區塊鏈上驗證供應商提供之交易文件及航運業者的貨運文件，比對各聯盟銀行傳送之交易資訊，增強風險控管作為(國泰金控，2021)。

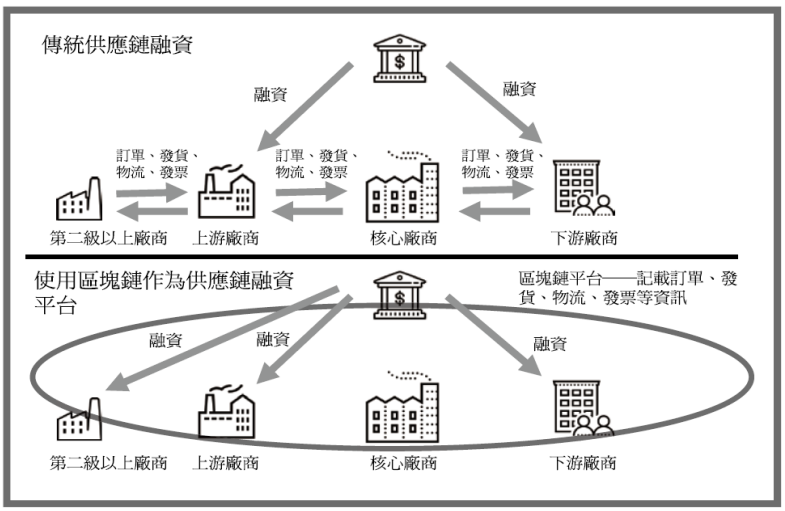

圖 2 區塊鏈供應鏈融資架構

資料來源：黃敬翔(2019)

2.2.2 函證

函證(Confirmation)是指會計師事務所在稽查企業財務報表時，向金融業者發詢證函，並取得相關查核證據的審核程序，為了提高資訊透明化並以企業永續經營為目的，財金公司、財團法人中華民國會計研究發展基金會、金融機構及四大會計師事務所，共同制定統一資訊標準，於107年合力建置「區塊鏈函證服務平臺」(李于宏，2021)。透過區塊鏈函證平臺將銀行函證自動化及資訊化，將原本紙本郵寄方式改為透過區塊鏈平臺加密傳送，解決人工填寫易發生誤填、遺失、竄改及舞弊的問題，確保資料來源正確性及安全性；另於區塊鏈上記錄函證資料，相關紀錄均無法修改或遭竄改，解決傳統企業及銀行可能偽冒資料之風險，相關業管單位可隨時掌握執行狀況，提高審核作業時效(財金資訊股份有限公司，2021)，函證作業流程如圖 3 所示。

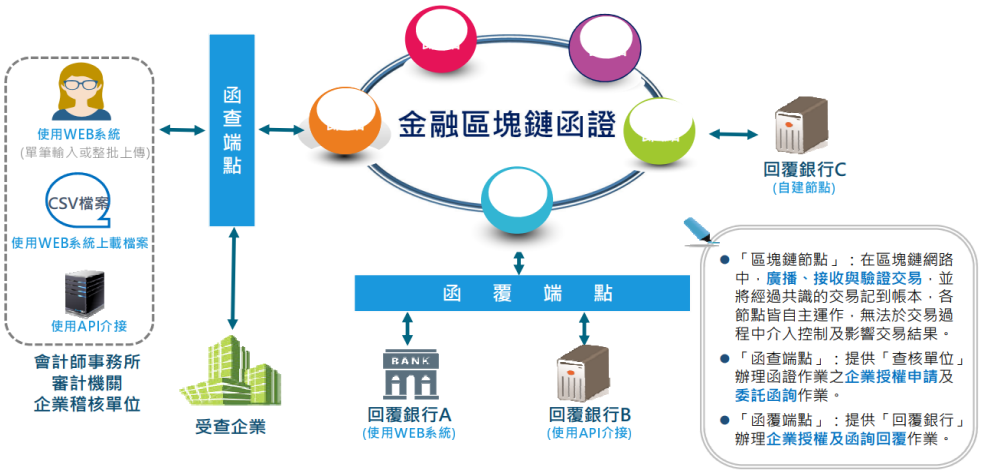

圖 3 金融區塊鏈函證作業流程

資料來源：財金資訊股份有限公司(2020)

2.3 電子現金相關研究

電子現金即是將傳統的紙本現金以電子數位的方式存在，並透過密碼學技術產生一序列的編碼資料，與傳統的貨幣一樣具有唯一性及不可偽造的特性，在交易階段利

用電子設備以網路連線傳送給商家完成支付作業，提供安全便利之資金移轉服務，現行貨幣比較如表 2。而在典型的電子現金系統包含客戶、銀行（發行方或收單方）和商家三個角色，交易內容包含開戶、提款、支付和存款協議，主要流程為客戶從銀行提取電子現金，使用電子現金交易支付給商家，最後商家將其電子現金存入銀行的過程（Chen et al., 2011），以下描述 Wang、Tsaur 和 Li 等學者所提出之電子現金支付之研究。

表 2 貨幣比較表

項目	傳統現金	電子現金	虛擬貨幣
來源	中央銀行貨幣	電子貨幣	虛擬貨幣
發行機構	中央銀行	金融機構	任一機構
存在形式	實體	數位	數位
轉移模式	硬幣/紙張	帳戶基礎	代幣基礎
耐久度	易損毀	永久保存	永久保存
攜帶便利性	不易攜帶	易攜帶	易攜帶
發行量	由中央銀行決定	限量發行	限量發行
法償效力	具備	具備	不具備

2.3.1 Wang 等學者電子現金支付機制

2007 年 Wang 等學者提出了一個基於群簽章的公平和可轉移的多銀行離線電子現金系統，由可信任的第三方擔任憑證中心，達成用戶的身分識別，防止舞弊勒索行為，確保電子現金公平交易，並由多個銀合組成一個群體，由中央銀行擔任群組管理者，透過群盲簽章達成聯合發行電子現金的目標，使消費者可以匿名消費，當商家取得群體之公開金鑰後，即可驗證由不同銀行發行之電子現金合法性，系統交易流程如圖 4 所示（Wang et al., 2007）。

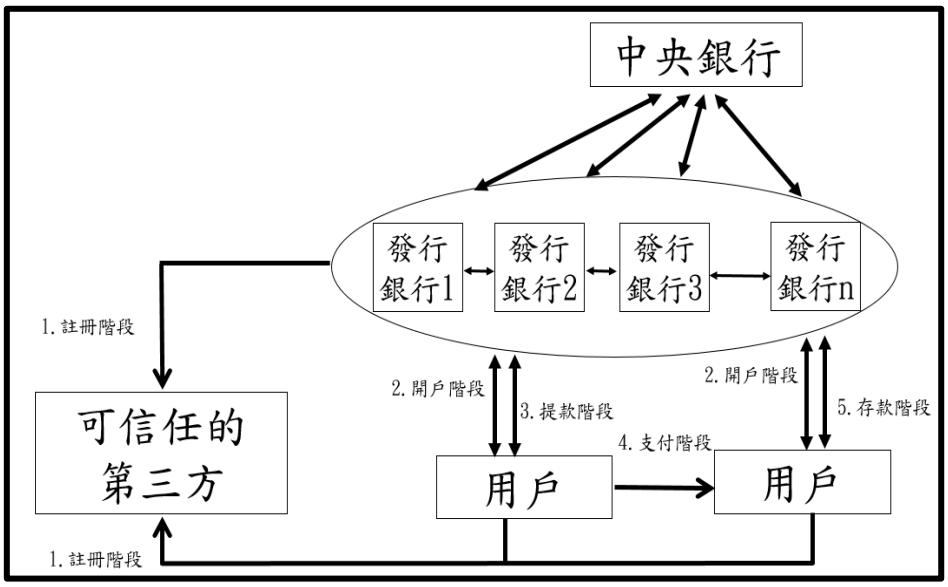

圖 4 多銀行發行離線電子現金系統交易流程

資料來源：Wang et al.（2007）

2.3.2 Tsaur 等學者電子現金支付機制

2018 年 Tsaur 等學者於提出的一種基於橢圓曲線的部份盲簽章電子現金系統，該研究方案由多銀行共同發行的行動電子現金系統，利用橢圓曲線設計之部份盲簽章技術，

解決已簽署之電子現金難以辨識額度與時效的問題，並可改善銀行資料庫迅速成長的情形，提高執行效率並降低計算和通信的成本，並透過自我認證公開金鑰密碼系統，使用者能自行驗算系統中心傳送的公鑰正確性，使得系統中心無法掌握公開金鑰的產生與驗證，系統交易流程如圖 5 所示(Tsaur et al., 2018)。

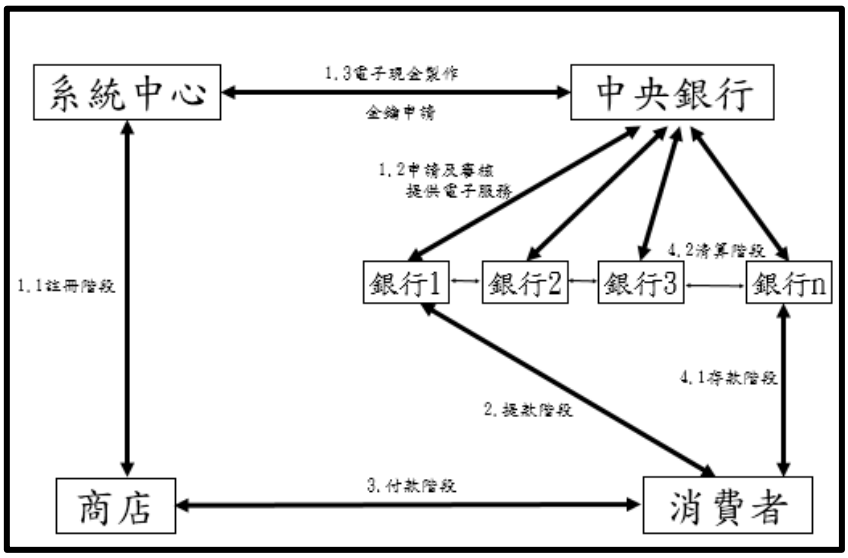

圖 5 多銀行發行電子現金系統交易流程
資料來源：Tsaur et al.（2018）

2.3.3 Li 等學者電子現金支付機制

2019 年 Li 等學者提出的一個高效的公平離線電子現金方案，該研究方案中由中央銀行擔任一個可信任的中央金融機構擔任憑證中心，負責發佈憑證，利用非交互式零知識證明技術，在不公開資訊的情況下，驗證身分及電子現金之合法性，可達成多個銀行發行電子現金之目的，在不受電子現金發行銀行的限制下，驗證電子現金合法性，並合乎電子現金匿名性、不可重複消費、不可偽造性和可追溯性相關的安全屬性，系統交易流程如圖 6 所示(Li et al., 2019)。

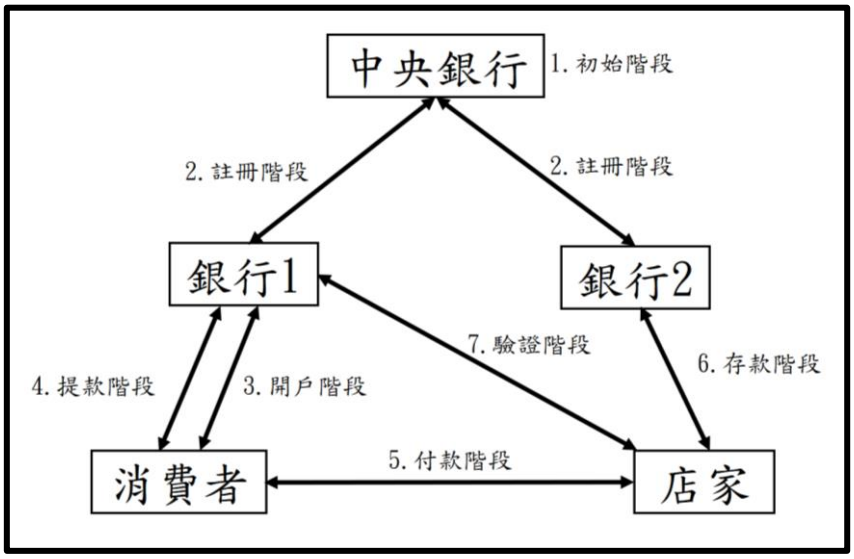

圖 6 標準模型下多銀行的公平離線電子現金流程圖
資料來源：Li et al.（2019）

2.4 密碼學理論

本章節彙整本研究應用之密碼學理論。

2.4.1 橢圓曲線密碼系統

由 Miller(1985)及 Koblitz(1987)兩位學者分別提出將橢圓曲線應用在密碼學上，主要是利用橢圓曲線特殊點加法及反元素的特性，將其運用在公開金鑰加密系統上，一般方程式為：$y^2 + axy + by = x^3 + cx^2 + dx + e$，其中 a、b、c、d、e 為實數，通常以$y^2 = x^3 + ax + b$方程式來表示，其優點是運用點加法運算，解密者必須窮舉所有可能的點才能破解密鑰，而此問題至今尚無法於多項式時間內求得解答，另在相同安全複雜度下，加密金鑰的長度較 RSA 短，現行依美國國家標準暨技術研究院(National Institute of Standards and Technology; NIST)所制定之國際標準，橢圓曲線簽章及驗證要求之金鑰長度皆大於或等於 224 位元(Barker and Roginsky, 2019)，金鑰比較如表 3 所示。

在 Galois Field 有限域 $GF(p)$ 中，取質數 p （p>3）同餘的橢圓曲線群，以$E: y^2 = x^3 + ax + b(modp)$來表示，其中 a、b 為小於 p 之正整數，且$4a^3 + 27b^2 \neq 0(modp)$，假設$M(x_1, y_1)$與$N(x_2, y_2)$為$GF(p)$上的點，在橢圓曲線上點加法其具有以下規則：

(一) $M + O = O + M = M$。

(二) 當$M = -N$，表式N為$(x_2, -y_1)$，則$M + N = (x_1, y_1) + (x_1, -y_1) = O$。

(三) 當$M \neq -N$，則$M + N = (x_3, y_3)$，且$x_3 = (\lambda^2 - x_1 - x_2)$，$y_3 = \lambda(x_1 - x_3) - y_3$，此處：

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ M \neq N \\ \dfrac{3x^2 + a}{2y_1} & if\ M = N \end{cases}$$

(四) 為了加速運算，橢圓曲線中利用加法運算達成乘法運算，如：$4M = 2M + 2M$，再計算$2M = M + M$即可。

(五) 反元素運算：當點$N = (x, y)$的反元素為$-N = -(x, y) = (x, -y)$。(因$N + (-N) = O$，O即為乘法單位元素)

表 3 橢圓曲線密碼系統與 RSA 在相同安全複雜度下金鑰長度之比較表

橢圓曲線密碼系統與 RSA 金鑰長度在相同安全複雜度下之比較					
長度 / 項目	金鑰長度				
橢圓曲線密碼系統	112	163	224	256	384
RSA	512	1024	2048	3072	7680
金鑰長度比	1：5	1：6	1：9	1：12	1：20

資料來源：蘇品長(2007)

2.4.2 部份盲簽章

盲簽章是 1982 年由 Chaum 所提出的一種基於 RSA 的電子簽章，其概念為使用者將訊息利用盲因子盲化後，傳送給簽章者進行簽名，而簽章者收到盲化過的訊息，故無法得知其訊息內容，最後驗證者可利用簽章者的公鑰，驗證簽章的正確性，具有保護使用者隱私的特性，所以可被應用於網際網路環境下的電子現金系統及投票場景保護用戶隱私的安全性問題。

然而，盲簽章後續在電子現金的應用上出現兩個問題，其一為銀行必需留存已使用的電子現金防止雙重支出，導致資料庫無限增長，其二為簽章者必須在無法確認電子現金面額之情況下，完全相信所簽署內容；為了解決上述問題，Abe 和 Fujisaki 於 1996 年提出植基於 RSA 部份盲簽章的概念(Abe and Fujisaki, 1996)，簽章者在簽章時，

可得知部份簽章內容，其餘隱私之內容簽章者無從得知，演算法區分 5 個階段：

(一) 初始階段：

銀行隨機選擇兩個大質數p,q，然後接著計算：

$$n = p \cdot q 及 \emptyset(n) = (p-1)(q-1)$$

決定一公開金鑰及私密金鑰對為e,d，滿足：

$$ed \equiv 1(mod\emptyset(n))及gcd(e,\emptyset(n)) = 1，且e,d < \emptyset(n)$$

銀行對外公佈公開金鑰(e,n)及單向雜湊函數$H()$，對內自行保有私密金鑰(d,p,q)，並且讓每筆發出的電子現金都價值w元。

(二) 盲化階段：

假若消費者決定向銀行提領電子現金，他隨機選擇隨機選取一盲因子r和亂數m，$m,r \in Z$，並計算：

$$\alpha \equiv r^{ev}H(m)modn$$

v為事先與銀行定義好的公開訊息，包含電子現金的面額和有效期限，並將部分盲訊息(α,v)傳給銀行。

(三) 簽章階段：

銀行收到(α,v)之後，先確認v是否正確，假如正確無誤，計算：

$$\beta \equiv \alpha^{(ev)^{-1}}modn$$

從消費者在銀行的帳戶內扣除w元，並傳送β給消費者。

(四) 去盲階段：

消費者收到β後，消除盲因子r，計算：

$$s = r^{-1}\beta modn$$

消費者即得到自己購買的電子現金(m,s,v)。

(五) 交易階段：

當消費者使用電子現金(m,s,v)時，商家獲得電子現金後，商家首先先確認v是否正確，商家使用銀行的公開金鑰e驗證電子現金是否滿足，若滿足則表示電子現金合法：

$$s^{ev}modn \equiv H(m)modn?$$

要求銀行檢驗電子現金(m,s,v)是否有重負支付，若無則銀行將該電子現金(m,s,v)儲存於資料庫中，以便對往後付費時的電子現金可執行重複付費檢查，並在商家帳戶內加入消費者實際消費總額。

2.4.3 自我認證

在安全的電子商務中，PKI 技術的建設是一項重要的系統工程，Girault 於 1991 年提出植基於 RSA 之自我認證公開金鑰密碼系統，不同於一般 ID-Based 由憑證中心製發憑證的作法，在授權階段由憑證中心與用戶雙方共同參與公開金鑰的計算，在驗證階段可以進行自我驗證的演算法，並可透過雙方傳送公開資訊，達成身分的確認，由於憑證中心的憑證內嵌於公鑰中，其他使用者可以驗證該使用者公鑰的正確性(蘇品長等，2014)，Girault 提出三種層次的安全等級如表 4 所示。

表4Girault提出之安全等級表

安全等級	說明	應用案例
初等	憑證中心因為擁有所有使用者的私密金鑰與公開金鑰，因此可以在任何時候偽冒任一個使用者而不被發現。	以身分為基礎的認證系統
中等	憑證中心在不知道使用者的私密金鑰的情況下，卻能偽造出一個未授權的使用者而不被發現。	電子憑證之認證系統
高等	1.授權中心透過使用者傳送之參數才能計算其公鑰，在授權階段，憑證中心不知道使用者的私鑰，所以無法自行產生或偽冒使用者的公鑰。 2.使用者可以自行驗算憑證中心傳送之公鑰，並驗證其正確性，故憑證中心無法主導使用者公鑰的產生與驗證。	自我認證公開金鑰密碼系統

資料來源：蘇品長等(2014)

2.5 小節

根據前述文獻探討得知區塊鏈技術具有不可竄改、可追溯及去中心化等特性，已在金融領域中快速發展與應用，可以解決交易雙方信任之問題，對比文獻中專家學者提出之多銀行數位交易機制，仍有電子現金難以辨識額度及資訊不對稱、資料遭竄改及身分偽冒之風險，故本研究提出運用區塊鏈技術結合智能合約與密碼學原理之多銀行數位交易機制，以區塊鏈技術為底層架構，利用分散式帳本技術結合智能合約，改善中心化伺服器最高者管理者權限及資料可能遭竄改之問題，達到金流、資訊流同步一致與資料可追溯性；透過橢圓曲線部份盲簽章方式實施電子交易支付，確保電子現金有效性，解決已簽署之電子現金難以辨識其額度或時效的問題；以自我認證為設計進行身分認證，不需透由第三方認證中心保證，使銀行、消費者、商家等電子商務中的參與人員身分資料達到完整性、不可否認性及真實性，進而達成電子商務交易安全。

三、電子交易機制設計

在本研究構想中，提出一個以區塊鏈為底層架構，利用智能合約建構安全電子交易機制，主要運用部份盲簽章和自我認證這兩種技術，首先，由服務開發者部署智能合約，由多個銀行業者組成聯盟鏈，可達成不同銀行金流互通及共享帳本之目的，接著利用植基於橢圓曲線離散對數難題之部份盲簽章技術，確保於交易階段銀行無法得知交易內容為何，確保交易內容及消費習慣隱蔽性，並達成電子現金驗證性，最後系統導入 Girault 所提出之公開金鑰密碼系統中安全等級 3 的自我認證機制，避免憑證中心在憑證製發的過程中產生偽冒消費者身分進行交易之問題，同時也可減輕憑證伺服器對所有參與人員在公鑰儲存、計算與管理的負擔，以下將說明本研究所提出之電子現金交易系統架構及其運作流程。

3.1 系統架構

本研究設計電子交易參與者計系統服務開發者、多銀行、消費者及商家，首先由服務開發者將智能合約部署至區塊鏈上，所有參與者向憑證中心實施身分註冊，並取得公、私鑰及簽章憑證，接著由消費者與商家各自向銀行完成開戶作業，接續由消費者與商家實施電子交易（商品瀏覽及訂購），由消費者向商家完成付款，商家將款項存

入，最後由商家進行出貨，寄出交易商品，系統整體運作架構如圖 7 所示。

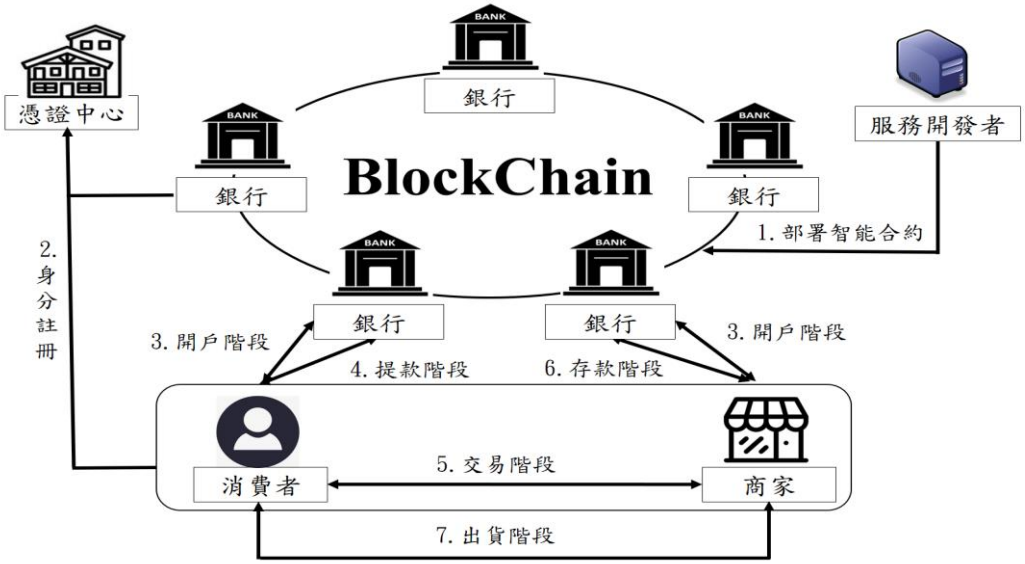

圖 7 系統整體運作架構圖

3.2 系統運作流程

本研究提出之系統作業流程區分系統初始、註冊、開戶、提款、交易、存款、出貨等七階段，參數說明如表 5 所示，首先由服務開發者設計智能合約並部屬至區塊鏈網路，參與者藉由憑證中心完成身分註冊，透過該電子憑證相互進行身分確認，確保為合法之用戶，消費者於後續提款、支付及商家進行存款階段中，將訂單及付款資訊透過部份盲簽章及加密技術傳送，確保資訊安全性。

表 5 系統各參數說明

項目	符號	說明
1	G	為橢圓曲線內之基點
2	$E(F_q)$	有限域F_q中之橢圓曲線
3	n	橢圓曲線上基點的階數(order)
4	q	$q > 2^{256}$之質數
5	$\|\|$	訊息連結符號
6	$CA、SD、EP、CS、SH$	憑證中心、服務開發者、銀行機構、消費者及商家
7	SC	服務開發者設計之智能合約
8	BC	區塊鏈網路
9	DG_{gid}	商品名稱，gid為其專屬的商品代號
10	Num	訂單編號，每筆交易自動產生的編號
11	$Price$	訂單上的金額
12	Key_{gid}	進行數位商品DG_{gid}加解密的對稱式金鑰。
13	ID_i	參與者身分 ID，i∈ $\{CA、SD、EP、CS、SH\}$
14	id_i	參與者匿名身分 id，i∈ $\{CA、SD、EP、CS、SH\}$
15	V_i	參與者簽名檔，i∈ $\{CA、SD、EP、CS、SH\}$
16	Add_i	參與者位址，i∈ $\{CA、SD、EP、CS、SH\}$
17	W_i	參與者計算之驗證值 i∈ $\{CA、SD、EP、CS、SH\}$

表 5 系統各參數說明(續)

項目	符號	說明
18	Ac_i	參與者帳戶，i∈ {CA、SD、EP、CS、SH }
19	d_i、k_i	隨機秘密參數值，i∈ {CA、SD、EP、CS、SH }
20	Pk_i、Sk_i	參與者獲得之公鑰及私鑰 i∈ {SD、EP、CS、SH }
21	Wk_i	CA 計算的參與者簽章 i∈ { SD、EP、CS、SH }
22	$Key_{i/j}$	雙方經過身分驗證後，建立之共享金鑰 i, j∈ {SD、EP、CS、SH }
23	ec	交易內容，包含訂單編號、訂單金額及商品名稱
24	t	電子現金之公開資訊，包含電子現金之面額與時限
25	Er	電子發票
26	ts_{ij}	由使用者i所選取之時間戳記，j為傳遞次數，$j = 1,2,\dots,n$
27	$Deploy()$	部署智慧合約，把合約儲存在區塊鏈上，並取得一個專屬的位址
28	$Oac()$	參與者透過智能合約向銀行開戶的過程
29	$Reg()$	參與者向憑證中心註冊的過程
30	$Cer()$	雙方互向認證的過程
31	$Check()$	檢查資料正確性
32	$CheckAc()$	檢查帳戶餘額

3.2.1 初始階段

在初始階段，服務開發者向憑證中心CA取得橢圓曲線公開參數寫入智能合約 SC，服務開發者將其智能合約部屬至區塊鏈上。

$$SD \rightarrow BC：Deploy(SC) \quad (1)$$

3.2.2 註冊階段

參與者(EP、CS、SH)各自向憑證中心註冊身分資料，由憑證中心驗證並產出公私鑰Pk_i及簽章Wk_i，憑證中心傳回給參與者(EP、CS、SH)，並由參與者各自計算其驗證值V_i，後續於交易可獨立進行身分自我認證。

$$EP \rightarrow CA: Reg(ID_{EP}, V_{EP}, Add_{EP}) \quad (2)$$
$$CA \rightarrow EP: (Pk_{EP}, Wk_{EP}) \quad (3)$$
$$CS \rightarrow CA: Reg(ID_{CS}, V_{CS}, Add_{CS}) \quad (4)$$
$$CA \rightarrow CS: (Pk_{CS}, Wk_{CS}) \quad (5)$$
$$SH \rightarrow CA: Reg(ID_{SH}, V_{SH}, Add_{SH}) \quad (6)$$
$$CA \rightarrow SH: (Pk_{SH}, Wk_{SH}) \quad (7)$$

3.2.3 開戶階段

銀行、消費者與商家完成身分認證後，確認雙方均為合法身分，消費者與商家透過智能合約分別向銀行申請開戶。

$$CS \rightarrow EP: Cer(ID_{CS/EP}, Pk_{CS/EP}, V_{CS/EP}) \quad (8)$$
$$CS \rightarrow EP: Oac(id_{CS}) \quad (9)$$
$$EP \rightarrow CS: Ac_{CS} \quad (10)$$
$$SH \rightarrow EP: Cer(ID_{SH/EP}, Pk_{SH/EP}, V_{SH/EP}) \quad (11)$$
$$SH \rightarrow EP: Oac(id_{SH}) \quad (12)$$

$$EP \rightarrow SH: Ac_{SH} \quad (13)$$

3.2.4 交易階段

消費者與商家完成身分認證後，確認雙方均為合法身分，消費者以 SSL 與商家建立彼此之間的安全通道，會議金鑰為$Key_{CS/SH}$；消費者瀏覽網站上的數位商品，選擇欲購買的數位商品，並發起電子交易。

$$CS \rightarrow SH: Cer(ID_{CS/SH}, Pk_{CS/SH}, V_{CS/SH}) \quad (14)$$

$$CS \rightarrow SH: (DG_{gid} \| ts_{CS1}) \quad (15)$$

$$SH \rightarrow CS: (Num, DG_{gid}, price \| ts_{CS1}, ts_{SH1}) \quad (16)$$

3.2.5 付款階段

在付款階段中，消費者與商家及銀行完成身分認證後，確認雙方均為合法身分，消費者將提款公開訊息 t(包含欲提款的電子現金之面額與時限）與帳戶資訊id，加密傳送給銀行，於雙方進行身分驗證後，銀行檢查公開資訊t之格式及帳號內是否有足夠餘額。接著，消費者將電子現金申請資訊進行盲化α，並由銀行於部分盲訊息上完成簽章S_α，並從消費者帳戶扣除與電子現金面額相等的金額，再將簽章傳回給消費者，消費者可在銀行機構無法獲得完整資訊的情況下取得其部份盲簽章之電子現金。最後，消費者以 SSL 與商家建立彼此之間的安全通道，會議金鑰為$Key_{CS/SH}$，並將訂單編號及電子現金加密傳送商家，商家收到加密訊息，解密後檢驗電子現金是否符合時限，如不符則拒絕。

$$CS \rightarrow EP: Cer(ID_{CS/EP}, Pk_{CS/EP}, V_{CS/EP}) \quad (17)$$

$$CS \rightarrow SH: Cer(ID_{CS/SH}, Pk_{CS/SH}, V_{CS/SH}) \quad (18)$$

$$CS \rightarrow EP: (id_{CS}, t \| ts_{CS1}) \quad (19)$$

$$EP: Check(t) \quad (20)$$

$$EP: CheckAc(id_{CS}) \quad (21)$$

$$CS \rightarrow EP: (\alpha \| ts_{CS2}) \quad (22)$$

$$EP \rightarrow CS: (S_\alpha \| ts_{EP1}) \quad (23)$$

$$CS: S'_\alpha \quad (24)$$

$$CS \rightarrow SH: (Num, (S'_\alpha, t) \| ts_{CS1}) \quad (25)$$

3.2.6 撥款階段

在撥款階段中，商家與電子機構完成身分認證後，確認雙方均為合法身分，商家以 SSL 建立與電子支付機構之間的安全通道，共同會議金鑰$Key_{SH/EP}$，可在傳輸資料時執行加/解密使用，商家將加密後的帳戶及電子現金資訊傳送給電子支付機構，電子支付機構解密並核對電子現金是否重複存款；如檢查正確，則傳給商家一個電子現金為合法的回應 Msg（$legal$），並將錢存入商家的帳戶中。

$$SH \rightarrow EP: Cer(ID_{SH/EP}, Pk_{SH/EP}, V_{SH/EP}) \quad (26)$$

$$SH \rightarrow EP: (id_{SH}, (S'_\alpha, t)) \quad (27)$$

$$EP: Check(S'_\alpha, t) \quad (28)$$

$$EP \rightarrow SH: Msg(legal) \quad (29)$$

3.2.7 出貨階段

在出貨階段中，商家與消費者完成身分認證後，確認雙方均為合法身分，商家以 SSL 建立與消費者之間的安全通道，共同會議金鑰為$Key_{CS/SH}$，商家傳送數位商品DG_{gid}之解密金鑰K_{gid}及電子發票Er給消費者，消費者透過解開Dg_{gid}，獲得數位商品。

$$CS \rightarrow SH: Cer(ID_{CS/SH}, Pk_{CS/SH}, V_{CS/SH}) \quad (30)$$

$$SH \rightarrow CS: (DG_{gid}, K_{gid}, Er) \quad (31)$$

3.3 系統演算法設計

考量文章篇幅，摘述身分註冊及電子現金核心技術，演算法如下。

3.3.1 身分註冊

憑證中心CA在有限域$E(F_q)$上選擇一個安全的橢圓曲線$E(F_q)：y^2=x^3+ax+b(modq)$且$4a^3+27b^2\neq 0(modq)$，q 為一個 256 位元以上之大質數，並在橢圓曲線$E(F_q)$上選一階數（order）為 n 的基點 G，使$n\cdot G=O$，接續由CA選擇一個單向無碰撞雜湊函數$h(\ )$，選擇私密金鑰並計算公鑰，$Pk_{CA}=Sk_{CA}\cdot G$，最後由CA公開參數E、G、q、$h(\ )$、Pk_{CA}。

參與者註冊：參與者$(EP、CS、SH)$首先選擇一隨機秘密參數值$d_i\in[2,n-2]$，以參與者位址Add_i與秘密參數值d_i計算產生簽名檔V_i，完成簽名檔計算後將V_i、Add_i傳送至憑證中心CA，計算如下:

$$V_i=h(d_i\parallel Add_i)\cdot G \tag{32}$$

憑證中心CA驗證回傳：憑證中心 CA 接收參與者之註冊資訊後，選擇一隨機秘密參數$k_i\in[2,n-2]$，與註冊資訊計算參與者的驗證公鑰W_i及簽章值Wk_i，憑證中心 CA 完成計算後將W_i及Wk_i回傳給參與者，計算如下:

$$W_i=V_i+\left(k_i-h(Add_i)\right)\cdot G=\left(q_{ix},q_{iy}\right) \tag{33}$$

$$Wk_i=k_i+Sk_{CA}\left(q_{ix}+h(Add_i)\right) \tag{34}$$

參與者產生公、私鑰階段:參與者接收憑證中心CA回傳之驗證公鑰W_i及簽章值Wk_i，計算自己的公、私鑰(Pk_i,Sk_i)，並驗證公鑰W_i的正確性，計算如下:

$$Sk_i=Wk_i+h(d_i\parallel Add_i) \tag{35}$$

$$Pk_i=Sk_i\cdot G \tag{36}$$

$$Pk_i=[Wk_i+h(d_i\parallel Add_i)]\cdot G \tag{37}$$

$$Pk_i=Sk_i\cdot G=k_i\cdot G+h(d_i\parallel Add_i)\cdot G+[q_{ix}+h(Add_i)]Pk_{CA} \tag{38}$$

3.3.2 電子現金

申請階段：消費者將提款資訊t與帳戶資訊id加密傳送給銀行，銀行檢查確認消費者帳戶金額足夠，隨機選取橢圓曲線上一點P_1和隨機數$af\in[2,n-2]$，並加密隨機數P_a和計算電子現金序號密文摘要 $\mathrm{P_Q}$，將加密隨機數$\mathrm{P_a}$，電子現金序號密文摘要$\mathrm{P_Q}$傳送給消費者。

$$P_a=af\cdot G \tag{39}$$

$$P_Q=P_1+af\cdot Pk_{EC} \tag{40}$$

盲化階段：消費者收到P_a及P_Q後，隨機選取橢圓取上一點P_2，盲因子$br\in[2,n-2]$和隨機數$bf\in[2,n-2]$，用自身的公開金鑰Pk_{CS}針對電子現金申請資訊進行盲化α，並傳送給銀行。

$$P_R=P_2+bf\cdot Pk_{CS} \tag{41}$$

$$\alpha=x_{P_2}\cdot br^{-1}\cdot h\left(ec\|x_{P_Q}\cdot x_{P_R}\right) \tag{42}$$

簽章階段：銀行收到α之後，隨機選擇亂數$cf\in[2,n-2]$，並使用電子現金私鑰Sk_{EC}進行簽章，計算S_1,S_2，接著把α、S_1,S_2、P_1傳給消費者。

$$S_1=t\cdot Sk_{EC}\cdot x_{p1}\cdot\alpha+cf \tag{43}$$

$$S_2=cf\cdot G \tag{44}$$

解盲階段：消費者收到α、S_1,S_2、P_1之後，進行解盲化，並可在銀行無法得知ec

之情形下，取得部份盲簽章(K, J, a, b, t)。

$$a = x_{P1} \cdot x_{P2} \quad (45)$$

$$b = x_{P_Q} \cdot x_{P_R} \quad (46)$$

$$K = br \cdot S_2 \quad (47)$$

$$J = br \cdot S_1 \quad (48)$$

驗證階段：商家收到其電子現金後，可驗證電子現金之有效性。

$$J \cdot \mathrm{G} \stackrel{?}{=} t \cdot Pk_{EC} \cdot a \cdot h \quad (49)$$

驗證說明如后：

$$J \cdot \mathrm{G} = br \cdot S_1 \cdot \mathrm{G} \quad (50)$$

$$= br \cdot [t \cdot Sk_{EC} \cdot x_{p1} \cdot \alpha + cf\,] \cdot \mathrm{G} \quad (51)$$

$$= br \cdot t \cdot Sk_{EC} \cdot x_{p1} \cdot x_{P_2} \cdot br^{-1} \cdot h\left(ec \| x_{P_{Q1}} \cdot x_{P_{Q2}}\right) \cdot \mathrm{G} + br \cdot cf \cdot \mathrm{G} \quad (52)$$

$$= t \cdot Pk_{EC} \cdot a \cdot h \quad (53)$$

四、安全及效益分析

4.1 安全性分析

理想的電子現金系統都應具備基本的安全屬性：不可偽造性-任何使用者都不能偽造或修改電子現金的價值；不可追蹤性-任何使用者都不能從電子現金中得知交易細節或使用者身分細節；防止雙花-任何使用者都不能多次花費同一筆電子現金(Barguil and Barreto, 2015)，本研究除滿足上述基本安全性外，另達到機密性等額外安全要求。

4.1.1 機密性

機密性是指在交易或傳輸期間，資料都是被保密的，無法遭未經授權的人員或程序所取得或透露的特性，只有經過核可的人或程序才能獲得相關數據資料，避免資料外洩(蘇品長等，2022)；在本研究交易中，使用非固定式交談金鑰$Key_{i/j}$，若資訊遭有心人士竊取，因無相對應的交談金鑰，須暴力破解橢圓曲線離散對數之難題，故在實際安全上可確保電子現金機密性。

4.1.2 完整性

完整性是資料在傳遞過程中，確保內容保持完整且正確一致，不會遭任意竄改，在本研究中由於區塊鏈上每個區塊之間以雜湊函數值鏈結，在傳遞過程中內容不能被任意增減或修改(Guo and Yu, 2022)，另銀行簽章之電子現金是由消費者利用雜湊函數演算法所得$\alpha = x_{P_2} \cdot br^{-1} \cdot h\left(ec \| x_{P_Q} \cdot x_{P_R}\right)$，若途中遭攔截並修改後發送給商家，產出之密文摘要不一致，可以確保電子現金內容之完整性。

4.1.3 匿名性

匿名性是在交易階段中，不想透露真實身分的一種不具名行為，本研究基於區塊鏈技術為基礎，在區塊鏈中的參與者，皆是以「英文+數字」的代碼為名稱，採匿名身分進行交易，於鏈上參與者僅能確認該筆交易存在(Rajasekaran et al., 2022)，無法知悉其交易內容，消費者在提領電子現金交易行為，銀行皆無法取得使用者之交易明細ec，因此無法調查消費者之習慣。

4.1.4 防止雙花

消費者在傳送電子現金給商家進行付款時，商家可先行檢查電子現金合法性$J \cdot \mathrm{G} \stackrel{?}{=} t \cdot Pk_{EC} \cdot a \cdot h$，驗證通過後，銀行於收到銀行存入該筆電子現金時，可檢查是否已被使用，若發生重複消費可進行追蹤。

4.1.5 不可否認性

不可否認性是指對已經產生的交易或事件的證明，無法否認其交易行為，在本研究中，參與交易各方之公、私鑰對皆是向憑證中心註冊所得，在電子現金提款階段，已由銀行完成簽章，故接收方能以驗證方式確認其簽章的有效性，各參與者皆無法否認所簽署之資訊，另在交易傳送訊息過程中，加入時戳ts_{ij}，可以達成電子交易時間證明，達到不可否認性。

4.1.6 不可偽造性

不可偽造性是指只有授權方銀行才能發行電子現金，在本研究中，第三方若想偽造發行電子現金，必須得到授權之金鑰，然而想獲得密鑰將會面臨橢圓曲線離散對數的問題；另在付款階段，商家可驗證消費者所支付的電子現金合法性，不需透過發行銀行，可達到電子現金之不可偽造性。

4.1.7 不可竄改性

不可竄改性是指資料及數據不可被任何人任意竄改，在本研究中利用區塊鏈技術建構電子現金系統，參與者均須透過區塊鏈上執行電子現金提款、存款等交易行為，而在區塊鏈上，每個區塊之間以雜湊函數值鏈結，而雜湊函數據不可逆且為單向性，因此存在於鏈中產生的數據是不可被任意竄改的(Rajasekaran et al., 2022)，故具有不可竄改性。

4.1.8 資料可追溯性

可追溯性是指電子現金交易申請資訊可以溯源，在本研究中，每一筆電子現金從銀行傳送至消費者，並由商家存入銀行，區塊鏈上都可以透過智能合約完整追溯其過程(Li et al., 2020)，銀行亦可透過區塊鏈共享帳本確認電子現金合法性，完整記錄溯源。

4.1.9 抗中間人攻擊

中間人攻擊指的是當攻擊者偽冒身分或偽造數據，在不被他人識破的情形下，破壞整體系統運作流程，大多數沒有良好身分驗證安全性的加密系統都面臨中間人攻擊的威脅(Mallik, 2019)，在本研究中以自我認證方式實施身分註冊，使用者可自行驗算憑證中心傳送之公鑰正確性$Pk_i = Sk_i \cdot G = k_i \cdot G + h(d_i \| Add_i) \cdot G + [q_{ix} + h(Add_i)]Pk_{CA}$，並於後續交易過程中，雙方先行完成身分驗證後，始可進行交易，確保參與者合法身分，可有效抵抗中間人攻擊。

4.2 方案比較

本研究設計基於區塊鏈建構多銀行數位交易機制，針對理論基礎與第二章文獻探討中所列學者提出之多銀行電子現金系統進行比較，並依據區塊鏈技術之優勢及特性，參酌相關文獻進行安全性分析與時間複雜度計算(Wang et al. 2007; Tsaur et al., 2018; Li et al., 2019; Tsai and Su, 2021)，可發現電子現金交易時所花費時間成本相對較低，並可滿足安全性要求，安全性比較結果如表 6，運算成本參考如表 7，時間複雜度比較如表 8。

4.2.1 Wang 等學者提出電子現金系統方案

該研究提出透過群盲簽章雖然能達到聯合發行電子現金的目標，惟未能解決銀行資料庫成長快速與已完成簽署之電子現金難以辨識額度及使用效期的問題，在設計中先決條件為可信任之第三方擔任憑證中心，無法避免憑證中心偽冒使用者問題，在計算量與傳輸量方面植基於 RSA 機制，相對需要大量的指數運算，導致系統運算負荷，另針對銀行集中式伺服器管理無法解決資料可能遭受竄改及清算系統故障導致金流及資訊流不對稱之問題及問題。

4.2.2 Tsaur 等學者提出電子現金系統方案

該研究方案設計基於部份盲簽章之多銀行聯合發行的行動電子現金系統，利用部

份盲簽章之技術應用於多銀行聯合發行的行動電子現金系統雖可改善銀行資料庫大量成長的衝擊，解決已簽署之電子現金難以辨識其額度與時效的問題，然而針對銀行集中式伺服器管理無法解決資料可能遭受竄改及清算系統故障導致金流及資訊流不對稱之問題。

4.2.3 Li 等學者提出電子現金系統方案

該研究方案中由中央銀行擔任一個可信任的中央金融機構擔任憑證中心，負責發佈憑證，然而未提及中央銀行可能無法信任之解決方案，銀行集中式伺服器管理無法解決資料可能遭受竄改及清算系統故障導致金流及資訊流不對稱之問題，另設計中未提出改善銀行資料庫大量成長的衝擊，解決已簽署之電子現金難以辨識其額度與時效的問題。

表 6 安全性比較表

項目	Wang 等學者提出之電子現金系統(2007)	Tsaur 等學者提出之電子現金系統(2018)	Li 等學者提出之電子現金系統(2019)	本研究機制
機密性	◯	◯	◯	◯
完整性	◯	◯	◯	◯
匿名性	◯	◯	◯	◯
防止雙花	◯	◯	◯	◯
不可否認性	◯	◯	◯	◯
不可偽造性	◯	◯	◯	◯
不可竄改性	Δ	Δ	Δ	◯
資料可追溯性	Δ	◯	◯	◯
抗中間人攻擊	X	◯	X	◯
系統便利性	X	Δ	Δ	◯
多銀行發行	◯	◯	◯	◯
註：◯：符合、Δ：部分符合、X：不符				

表 7 運算成本參考表

符號	定義
T_{ECMUL}	進行一次 ECC 乘法運算所需時間≈29 T_{MUL}。
T_{ECADD}	進行一次 ECC 加法運算所需時間≈5 T_{MUL}。
T_{BP}	進行一次雙線性對運算所需時間≈120 T_{MUL}。
T_{EXP}	進行一次模式指數運算所需時間≈240 T_{MUL}。
T_{INVS}	進行一次模式乘法反元素所需時間≈240 T_{MUL}。
T_{MUL}	進行一次模式乘法所需時間。
T_c	進行一次對稱式加密所需時間。
T_{ADD}	進行一次模式加法所需時間（可忽略不計）。
t_h	進行一次單向雜湊函數所需時間≈0.4 T_{MUL}。

資料來源：Tsai and Su（2021）

表 8 電子現金交易複雜度比較表

項目	Wang 等學者提出之電子現金系統(2007)	Tsaur 等學者提出之電子現金系統(2018)	Li 等學者提出之電子現金系統(2019)	本研究機制
時間複雜度	$1207.44T_{MUL}+6t_h+5T_c$	$409.92T_{MUL}+5t_h+7T_c$	$12T_{EXP}+14T_{ECMUL}$ $2T_{ECADD}+6T_{BP}$	$10T_{ECMUL}+3T_{ECADD}$ $+5T_{ADD}+12T_{MUL}+$ $1T_{INVS}+5t_h+5T_c$
合計	$\approx 1210T_{MUL}+5T_c$	$\approx 412T_{MUL}+7T_c$	$\approx 4016T_{MUL}$	$\approx 559T_{MUL}+5T_c$

五、結論

本研究設計基於區塊鏈建構具安全性數位交易機制，透過區塊鏈可達成各銀行業者共同維護帳本，即時完成跨銀行清算，達成金流互通、資訊流同步一致的目標，提高合作商家與消費者便利性，進而提升電子支付普及率，在本研究機制中，透過銀行帳本同步一致及資料長時保存，可解決現行電子現金易遭惡意竄改，易被複製及重複付款的安全性威脅；利用區塊鏈能監管溯源及匿名之特性，使電子支付能被商家及消費者信任；運用部份盲簽章技術解決電子支付中，電子現金難以辨識其額度或時效的問題，使商家可驗證其有效性，並能保障消費者隱私性；另在電子商務環境中，利用自我認證方式提高系統安全性，在使用者申請註冊及開立電子現金帳戶時，解決憑證中心可能偽冒使用者身分進行註冊及開立電子現金帳戶之情形，達到參與人員身分資料完整性、不可否認性及真實性，並可有效減輕憑證中心公鑰儲存的成本，始能兼顧使用者便利性及交易安全性之外，避免電子支付機構淪為金融犯罪的缺陷。

本研究在安全性上除滿足電子現金基本要求不可偽造性、不可追蹤性及防止雙重花費外，另外達到匿名性、機密性、不可否認、不可竄改、數據可追溯、抗中間人攻擊等特點，並運用智能合約使系統更加自動化，當電子現金出現重複消費爭議及問題時，可快速掌握並釐清責任歸屬，解決資訊不對稱及信任問題，有效提升電子商務中消費者對於電子支付之信心。

5.1 國防領域之應用

本研究可應用於國防採購及財務領域，在採購方面，可將此電子支付機制導入國軍福利站、國軍副食供應中心、國軍文具部、國軍服裝供售站等各項商品銷售支付，隨著電子化購物的消費型態改變，使國軍官兵弟兄姊妹在採購方式上，除了既有的現金支付外，提供更多樣性的選擇，強化國軍電子商務便利性，達成網路商店交易安全，符合現代科技多元支付服務範疇，另可使電子現金支付更具安全性。在財務方面，現行人員獎勵多採用發放獎金（現金）、禮卷等方式，惟紙本不易保存，且承辦單位常無法有效掌握核發對象，如未來可將其實體獎金改為發行電子現金構想，可避免紙本現金、禮卷丟失及重複領用等問題，並達到去中心化（第三方）之目的，同時強化交易之安全性，提升整體國防戰力。

5.2 未來運用方向

經過多年努力，我國電子支付的基礎建設已臻完備，隨著金融科技如大數據、區塊鏈、雲端運算及人工智慧等創新技術發展，各銀行及相關企業企圖透過資訊技術提高執行效率、增加交易安全性及降低成本，亦期望能帶來嶄新的機會，目前國內電子支付比率占消費支出比率仍低於鄰近亞洲國家，如日本、韓國、新加坡等，行政院已訂立目標，在本研究設計中，運用區塊鏈系統達成帳本同步一致，於電子現金開戶、

交易、付款與撥款之金流、資訊流皆不可竄改，可有效解決電子商務中電子現金安全性、雙重花費及信任等問題，並利用密碼學原理、植基於橢圓曲線部份盲簽章技術及自我認證公開金鑰系統技術，提高交易之安全性及提高執行效率，期望透過本機制可提升電子現金使用率，並達成 2025 年行動支付的普及率 90%之目標，達成無現金之數位化生活。

近年來國際間中央銀行正投入研究發展數位貨幣(Central Bank Digital Currency; CBDC)，而我國也正積極投入研究，於「111 年度金融資訊系統年會」中，中央銀行總裁楊金龍表示，央行數位貨幣(CBDC)跟現行電子支付是互補關係，未來俟 CBDC 發展成熟、完善系統營運安全機制，並於我國政府對於區塊鏈發展金融服務之監管與法規體制明確，完成相關系統建設後，可結合本研究支付機制，使支付整體機制更加完整，有利未來金融業者及相關企業金融服務之應用，另在雲端運算環境中存在各式網路攻擊，如側通道攻擊、分散式阻斷服務攻擊及區塊鏈技術上存在智能合約漏洞等安全威脅，可能導致網路服務中斷、私密訊息遭竊及鏈上資訊亦有被竄改之可能性，因此於系統建置後可結合流量分析及封包檢測等設備，監測相關數據，提早發現異狀進行修正，降低系統服務中斷或資料遭竊取之威脅。

六、國防相關應用

本研究可應用於國防採購、財務領域，並導入國軍各式支付機制，如國軍福利站、國軍副食供應中心、國軍文具部、國軍服裝供售站等，提供多元安全之電子支付方案。

參考文獻

李于宏（2021）。解構區塊鏈本質，*財金資訊*， 99。

李宛蓁、黃杭浔（2016）。區塊鏈及數位貨幣在金融業的影響與應用研究計畫，台灣金融研訓院。

李耕銘（2021）。區塊鏈生存指南：帶你用 Python 寫出區塊鏈！，臺北：博碩文化。

金融監督管理委員會（2022/8/11）。111 年 6 月份信用卡、現金卡及電子支付機構業務資訊，下載於 https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202208110001&dtable=News（2022 年 8 月 30 日）。

財金資訊股份有限公司（2020/12/11)。財會主管看「金融監理與銀行函證」研討會，下載於 https://www.ardf.org.tw/downloads/ppt/3.pdf（2022 年 9 月 3 日）。

財金資訊股份有限公司，金融區塊鏈函證服務，財金資訊股份有限公司資訊網，下載於 https://www.fisc.com.tw/TC/Business?Caid=7c31a87d-2b5f-42bf-aafd-3c2405f64e8b&CaStyleId=4（111 年 4 月 8 日）。

國泰金控（2021/9/23）。國泰世華銀行「環球貿易共享區塊鏈」獲金管會核准試辦攜手 7 銀行以區塊鏈打造台灣首例企業金融資料交換平臺，國泰金控，下載於 https://www.cathayholdings.com/holdings/information-centre/intro/latest-news/detail?news=aK1nGyfMkECqFdgCC-4kPQ&page=4（2022 年 4 月 2 日）

曹偉駿、蔡欣潔（2010）。基於部分盲簽章之多銀行聯合發行的行動電子現金系統，全國資訊安全會議，第 20 屆，145-150。

郭木興（2003）。*電子商務：觀念、策略與案例實作*，臺北：學貫行銷出版。

彭思遠（2021）。去中心化金融與區塊鏈的發展，*臺灣經濟研究月刊*，44（1），49-55。

黃敬翔（2019）。區塊鏈技術對金融發展之衝擊，*臺灣經濟研究月刊*，42（11），55-61。

楊金龍（2019）。「中央銀行貨幣與零售支付系統-兼論財金公司扮演之角色」，下載於 https://www.cbc.gov.tw/tw/cp-302-104572-883b0-1.html（2023 年 3 月 13 日）。

鄒均、張海寧、唐屹、李磊、劉天喜、陳暉、曲列、鄭曉明(2018)。*區塊鏈技術指南*，北京：機械工業出版社。

魏喬怡（2019/10/23）。中信奇美實創區塊鏈交易首例，中時新聞網，下載於 https://www.chinatimes.com/newspapers/20191023000292-260205?chdtv（2022 年 4 月 10 日）

蘇品長（2007）。植基於 LSK 和 ECC 技術之公開金鑰密碼系統，長庚大學電機工程研究所博士論文。

蘇品長、夏君和、蘇泰昌（2022）。建構具安全性的智慧合約共享方案-以房屋共享為例，*資訊管理學報*， 29（3），253-275。

蘇品長、張鈞富、黃棠建（2014）。適用於電子商務之自我認證公開金鑰架構之設計與實作。*電子商務研究*，12（1），73-92。

Abe, M., & Fujisaki, E. (1996). How to date blind signatures. *In International Conference on the Theory and Application of Cryptology and Information Security*, 244-251. doi:10.1007/BFb0034851

Barguil, J. M., & Barreto, P. S. (2015). Security issues in Sarkar's e-cash protocol. *Information Processing Letters*, *115*(11), 801-803. doi:10.1016/j.ipl.2015.06.007

Barker, E., & Roginsky, A. (2018). Transitioning the use of cryptographic algorithms and key lengths (No. NIST Special Publication (SP) 800-131A Rev. 2). National Institute of Standards and Technology.

Chaum, D. (1983). Blind signatures for untraceable payments. *In Advances in cryptology*, 199-203. Springer, Boston, MA. doi:10.1007/978-1-4757-0602-4_18

Chen, Q., Srivastava, G., Parizi, R. M., Aloqaily, M., & Al Ridhawi, I. (2020). An incentive-aware blockchain-based solution for internet of fake media things. *Information Processing & Management*, *57*(6), 102370.

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, e00151. doi: 10.1016/j.jbvi.2019.e00151

Chen, Y., Chou, J. S., Sun, H. M., & Cho, M. H. (2011). A novel electronic cash system with trustee-based anonymity revocation from pairing. *Electronic Commerce Research and Applications*, *10*(6), 673-682. doi:10.1016/j.elerap.2011.06.002

Cheng, H. K., Hu, D., Puschmann, T., & Zhao, J. L. (2021). The landscape of blockchain research: impacts and opportunities. *Information Systems and e-Business Management*, *19*(3), 749-755.

Di Angelo, M., & Salzer, G. (2019, April). A survey of tools for analyzing ethereum smart contracts. *In 2019 IEEE International Conference on Decentralized Applications and Infrastructures*, 69-78. doi: 10.1109/DAPPCON.2019.00018

Gartner., "Blockchain Technology: What's Ahead?", From https://www.gartner.com/en/information-technology/insights/blockchain （retrieved on April 11, 2022）.

Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: Research and Applications*, *3*(2), 100067.

Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2019). A delay-tolerant payment scheme based on the ethereum blockchain. *IEEE Access*, 7, 33159-33172.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, *48*(177), 203-209. doi:10.1090/S0025-5718-1987-0866109-5

Lee, S. W., Singh, I., & Mohammadian, M. (2021). Blockchain Technology for IoT Applications. Singapore: *Springer*.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, 107, 841-853.

Li, Y., Zhou, F., & Xu, Z. (2019). A fair offline electronic cash scheme with multiple-bank in standard model. *Journal of the Chinese Institute of Engineers*, *42*(1), 87-96.

Liao, C. H., Guan, X. Q., Cheng, J. H., & Yuan, S. M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future*

Generation Computer Systems, *135*, 450-466.

Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Journal Pendidikan Teknologi Informasi*, *2*(2), 109-134.

Miller, V. S. (1985). Use of Elliptic Curve in Cryptography, *In Conference on the Theory and Application of Cryptographic Techniques*, 417-426. doi:10.1007/3-540-39799-X_31

Nakamoto Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System [Online forum comment]. From https://bitcoin.org/bitcoin.pdf（retrieved on April 3, 2022）

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039.

Ramchandra, M. V., Kumar, K., Sarkar, A., Mukherjee, S. K., & Agarwal, K. (2022). Assessment of the impact of blockchain technology in the banking industry. *Materials Today: Proceedings*, *56*, 2221-2226.

Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1), 1-9. doi: 10.1186/s40854-016-0040-y

Swan, M. (2015). *Blockchain Blue print for a New Economy*, O'Reilly Media Publishing, United States.

Tsai, C. H., & Su, P. C. (2021). A robust secure self-certified concurrent signature scheme from bilinear pairings. *The International Arab Journal of Information Technology*, *18*(4), 541-553.

Tsaur, W. J., Tsao, J. H., & Tsao, Y. H. (2018). An efficient and secure ECC-based partially blind signature scheme with multiple banks issuing E-cash payment applications. *In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, 94-100.

Wang, C., Li, Q., & Yang, X. (2007). A fair and transferable off-line electronic cash system with multiple banks. *In IEEE International Conference on e-Business Engineering*, 189-194. doi:10.1109/ICEBE.2007.45

Zhang, L., Xie, Y., Zheng, Y., Xue, W., Zheng, X., & Xu, X. (2020). The challenges and countermeasures of blockchain in finance and economics. *Systems Research and Behavioral Science*, *37*(4), 691-698. doi:10.1002/sres.2710

Zhang, T., & Huang, Z. (2022). Blockchain and central bank digital currency. *ICT Express*, *8*(2), 264-270.