以聯盟鏈導入電子公文交換機制之研究

蘇品長 劉亭萱 謝宛蓁*

國防大學資訊管理學系

論文編號：NM-44-02-01

DOI:10.29496/JNDM.202505_46(1).0001

來稿 2023 年 4 月 7 日→第一次修訂 2023 年 5 月 13 日→第二次修訂 2023 年 11 月 19 日→同意刊登 2024 年 2 月 28 日

摘要

在網際網路快速發展下，電子公文交換系統打破了時間與空間之限制，大幅減少公文交換作業時間及人力成本；然而，在公文交換過程中，仍需建構中心化伺服器及可信賴的第三方機構，若設備產生單點故障，則會導致系統不穩定，影響公文儲存及交換作業；此外，當資料發生濫用或誤用的情況時，亦需依賴第三方機構執行爭議仲裁作業；本研究設計將區塊鏈及智慧合約導入電子公文交換機制，將智慧合約程式部署於區塊鏈，透過智慧合約向憑證中心完成使用者註冊，驗證收發文身分並自動執行電子公文交換，具體貢獻簡述如後：（1）透過自我認證機制產生之公、私鑰，使用者可自行驗證公鑰的正確性，防竄改並降低第三方之參與度。（2）透過智慧合約函式自動解決交易衝突，確保電子公文交換作業的正確性。（3）電子公文交換作業紀錄皆分散儲存於區塊鏈各節點，達到去中心化的目的，以確保資料的安全與完整性。

關鍵詞：區塊鏈、智慧合約、電子公文交換、自我認證

* 聯絡作者：謝宛蓁 email: yaya99887@gmail.com

A Study of Introducing Consortium Blockchain into Electronic Official Document Interchange Mechanism

Su, Pin-Chang Liu, Ting-Hsuan Hsieh, Wan-Chen*

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

Abstract

With the rapid development of the Internet, the electronic official document interchange system breaks the constraints of time and space. It can greatly reduce the time and manpower cost of official document interchange process. However, in the process of document interchange, the centralized servers for the system and a reliable third-party organization still need to be constructed. If the equipment has a single point of failure, it will lead to system instability and affect document storage. In addition, when data is abused or misused, it is also necessary to rely on third-party organizations to perform dispute arbitration operations. This research introduces blockchain and smart contract into the electronic official document exchange mechanism and deploys smart contract programs in the Blockchain. It can complete user registration with the certificate center through smart contracts and verify the identities of documents senders and recipients. Finally, it automatically executes electronic official document interchange. The specific contributions of this research are briefly described as follows: (1) Through the public and private keys generated by the self-authentication mechanism, system users can verify the correctness of the public key by themselves to prevent tampering and reduce third party involvement. (2) Automatically resolve transaction conflicts through smart contract functions to reduce the participation of third parties. (3) The records of electronic official document interchange are distributively stored in each node of the blockchain to achieve the purpose of decentralization to ensure the security and integrity of the data.

Keywords: Blockchain, Smart Contract, Official Document Exchange System, Self-Certification

* Corresponding Author: Hsieh, Wan-Chen email: yaya99887@gmail.com

一、前言

電子公文交換系統以電子化作業取代傳統的人工紙本作業，係政府各機關公文傳遞的核心系統，隨著資訊科技不斷發展，資安威脅層出不窮，而電子公文系統也歷經多次改革，除了強化資安防護外，也提升使用者的便利性。然而，現行使用的系統仍以分層集中式管理架構，萬一引發單點故障問題，會提高駭客入侵、竄改或竊取資料的可能性，楊耿瑜（2019）曾提出當某機關資料被濫用或誤用時，須耗費龐大的人力、物力及時間，比對各機關間資訊系統的存取紀錄；當由公正第三方建立跨機關資訊系統介接平臺，銜接各機關的資訊系統，平臺會儲存所有跨機關資料交換的紀錄，若發生爭議，則由此平臺提出相關資料執行仲裁工作；另現行公文交換系統係透過政府憑證中心（Government Certificate Authority, GCA）所簽發的憑證來確認身分，且現行的電子公文交換地址簿傳遞採用公開金鑰基礎架構（Public Key Infrastructure, PKI），因技術限制及考量安全問題，系統採集中式管理，新增或異動均須辦理相關申請流程，並透過主管機關審核方式進行，無法即時更新資料；而 PKI 系統面臨的最大挑戰，就是憑證中心不可信，若憑證中心未做好安全管控，可能會被駭客入侵，引發中間人攻擊，而集中式的憑證中心故障，將會導致認證無法進行等問題，亦需耗費資源及儲存空間來管理金鑰目錄及憑證。

自虛擬貨幣出現後，社會開始關注區塊鏈的實際應用，從金融業到智慧合約，得以讓使用者進行去中心化的交易，不必再仰賴第三方機構，且具備不可竄改的特性。區塊鏈衍生出不同類型的鏈以符合需求，例如公有鏈、私有鏈與聯盟鏈，聯盟鏈結合公有鏈與私有鏈的特性，將部分少數的參與者視為驗證者，不像公有鏈如此開放透明，任何人都可以驗證區塊，也不像私有鏈如此封閉；而聯盟鏈可以讓許多有價值或機密的資料，不須公開分享，藉由設定參與者權限，避免資訊暴露，但又同時具備區塊鏈去中心化及資料不可竄改的特性。因區塊鏈具備去中心化、高度安全及不可竄改的特性，並且能確保資料在安全的狀況下傳遞，歐盟認為區塊鏈技術能促進政府數位化，歐洲 105 個組織在 2019 年簽署加入「國際共信區塊鏈應用協會（International Association for Trusted Blockchain Applications, INATBA）」，期許透過協會組織的成員，以區塊鏈技術達成公開透明、可信任的應用模式。

本研究希望利用區塊鏈去中心化、分散式帳本及不可竄改的特性，改善現行電子公文交換系統的集中式管理風險，由於區塊鏈上資料不可竄改，可避免電子公文交換紀錄不被承認或遭到偽造，增加其可信度；此外，為降低現行電子公文交換系統對於憑證中心的依賴性，並減輕金鑰管理負擔及達到不可否認性，蘇品長等（2014）提出基於橢圓曲線之密碼系統，來設計及實作具有自我驗證能力之 PKI 架構，除了可以確保憑證中心在註冊階段不能偽造用戶的公鑰，也可以降低對憑證中心的依賴度。透過提出一套「以聯盟鏈導入電子公文交換機制之研究」，以期透過聯盟鏈執行電子公文資料交換作業，導入智慧合約及自我認證機制，並利用橢圓曲線加密系統建立安全、完善的機制，實現自動化作業流程，確保系統流程的正確性，避免公文遭到竊取或是偽冒使用者，唯有合法的受文者才能取得電子公文；此外，所有的公文交換紀錄都可以透過許可制的區塊鏈保存，無須仰賴第三方跨機關資訊系統平臺追查交換資料的存取紀錄，大幅降低時間、

人力及物力成本，且在無須以第三方跨機關資訊系統平臺介入之前提下，可解決資料交換信任的難題，使分散的使用者達成共識。

二、文獻探討

本章提出以聯盟鏈導入電子公文交換機制之研究，並介紹「電子公文系統發展現況」、「區塊鏈技術」、「密碼學技術」及「電子公文系統相關之研究」等研究議題。

2.1 電子公文系統發展現況

推動電子化政府促進公文交換系統的架構調整，我國電子化政府發展分為 5 個階段（行政院研究發展考核委員會，1997），而各階段的電子化政府發展對於公文交換系統都有重大的影響。自 1998 年至 2020 年電子化政府的 5 個重要階段歷程，電子公文系統也從第 1 代的前置交換處理器(Front End Processor, FEP)、第 2 代的閘道系統(Gateway)、第 3 代跨閘道及點對點交換系統、第 4 代的終端用戶交換系統（eClient）到第 5 代的公文收發模組功能（jAgent）都在系統架構改革歷程中逐步奠定穩固基礎（陳美蓉與林其範，2020）。

楊耿瑜（2019）認為電子公文交換系統的分層管理、分散式集中架構來說，交換中心負責轄下機關電子公文交換工作，可讓電子公文交換機制運作之複雜度，維持可控制的範圍（系統運作效能考量），且能讓電子公文交換營運模式維持在一定水準（營運成本考量），且在此架構的運作下，只要交換中心故障，將會影響該部會、機構及所屬機關之內、外部電子公文交換機制之可用性，存在集中式系統的單點故障影響整體電子公文交換系統的風險，另因技術限制，現行交換系統的地址簿新增與異動作業，不利於資料即時性更新，均須透過申請流程且經過主管機關審核進行（陳美蓉與林其範，2020）。

2.2 區塊鏈技術

Szabo（1994）首次提出智慧合約的概念，並將其定義為：「一個智慧合約是一套以數據形式定義的承諾，包含合約參與者可以在合約執行這些承諾的協議。」Szabo 訂定智慧合約的基本運作原理，相較於傳統契約，智慧合約具備更高的安全性，也能降低交易成本，是一種自動化合約。

Wood（2014）發表以太坊黃皮書，並說明在以太坊系統中，提供一個去中心化的以太坊虛擬機（Ethereum Virtual Machine, EVM），而在此虛擬機內部運行合約代碼，與外部完全隔離，每一個節點都會透過以太坊虛擬機來執行智慧合約的運算，而使用 Solidity 程式語言定義智慧合約的規則條件，再經編譯後轉換為以太坊虛擬機可以執行的程式碼，為此奠定智慧合約開發的基礎。以太坊智慧合約透過外部擁有帳戶發起交易，傳送客戶端節點呼叫的函數及參數，在所有的節點接收到這筆交易後，再從區塊鏈中讀取已儲存之智慧合約運行程式。由於智慧合約在經過本地 EVM 運算後，再與其他節點的運算結果互相驗證通過後，才會將結果寫進區塊鏈中，因此智慧合約可以減少人為操作的弊端。

綜上所述，智慧合約可以理解為一個自動執行的電腦程式，它能自動接收及執行外部的指令，智慧合約的內容皆為公開透明，將智慧合約發佈到區塊鏈上後，所有人都無法更改其程式，此一特性使智慧合約擁有極高的安全性，並確保上鏈的智慧合約會照著

函式邏輯自動執行。智慧合約通常具備四大元素：合約主體、數位簽章、合約條款及去中心化平台。智慧合約主體存在才能執行或取消合約中的服務或商品，交易執行的過程中須利用參與者的私鑰進行認證，當智慧合約中的程式條件被觸發時，將會自動推送到待驗證的狀態，並經過區塊鏈上的各分散的節點進行簽署認證，獲得共識後，才能成功執行智慧合約，並自動完成交易（吳銳與劉導，2018），智慧合約運作原理如圖 1。

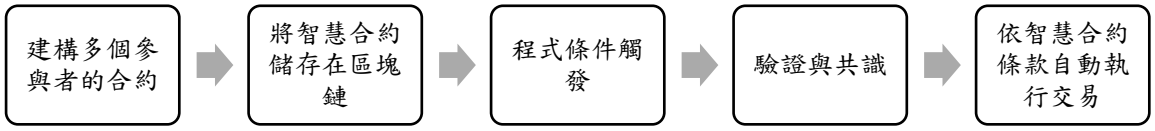

圖 1 智慧合約運作原理
資料來源：吳銳與劉導（2018）

區塊鏈網路因其授予網路用戶的權限及中心化的程度差異可區分三種類型：公有鏈、私有鏈及聯盟鏈。公有鏈是任何人都能參與共識過程和觸及資訊的區塊鏈，因此可以被視為「完全去中心化」；而私有鏈是完全私有的區塊鏈，由特定組織或機關控管寫入許可權的區塊鏈，亦可任意限制讀取權限之程度，由於節點間具高度信任，可排除節點互相驗證之交易過程，提高交易速度，且成員需要進行身分認證，降低惡意攻擊的可能性。為保有私有鏈的隱私性，同時維持公有鏈多節點共識機制的特性，聯盟鏈即是兩種區塊鏈的混合，是由若干機構的節點共同參與及管理區塊鏈，每個機構都運行著一個或多個節點，只允許系統內不同的機構進行讀寫與發送交易資料，並共同記錄交易數據（鏈習生，2022），其透明和去中心化程度有所限制，區塊鏈類型比較如表 1 所示。

表 1 區塊鏈類型差異表

項目	公有鏈	聯盟鏈	私有鏈
參與組成	任何節點	多個組織或機構	特定組織或機構
身分識別	匿名	可識別	可識別
權限	開放式閱覽、編寫	經授權才能編寫或閱覽	經授權才能編寫或閱覽
信任與安全程度	低	中	高
去中心化程度	去中心化	部分中心化(弱)	部分中心化(強)
典型示例	比特幣、以太坊	Hyperledger、R3	組織內區塊鏈

2.3 密碼學技術

基於公開金鑰密碼系統的身分驗證，是目前較為普遍應用且成熟的認證機制。Girault（1991）年提出自我認證公開金鑰密碼系統。在授權階段，使用者會參與憑證中心之公鑰計算，且憑證中心的憑證會內嵌於使用者公鑰中，讓其他使用者藉此驗證該使用者公鑰的正確性，且私鑰是由各使用者自行建立，因此憑證中心無法得知使用者私鑰，可避免產生憑證中心的偽冒使用者的可能性。在驗證過程中，使用者先利用自己的私鑰

驗證公鑰之正確性，驗證正確後，再以私鑰與通訊方之公鑰進行金鑰協議。

Girault（1991）提出公開金鑰密碼系統三個層次的安全等級，其中等級 3 即為自我認證公開金鑰密碼系統，其可降低系統上公鑰的管理、計算與儲存上的風險及成本（梁榮哲，2012），具備較高的安全性、較低的管理負擔及進行身分認證的高效率特性，特別適合應用在點對點網路或無線網路的環境（胡國新，2001）。陳文彬（2012）提出基於隨機背包難題及橢圓曲線離散對數之動態存取控制方法，在使用者註冊憑證階段，即採用自我認證公開金鑰機制，使其具備較高的安全性及效率，而宋宜芳（2018）年亦以國軍某電腦兵棋系統為例，以橢圓曲線自我驗證機制，設計具高可靠度之存取控制，以強化身分驗證機制，而余庭儀（2020）年以數位內容電子支付為例，藉由橢圓曲線自我驗證機制產生公、私鑰，使協定參與者可於交易期間進行身分驗證及數位商品加密。

2.4 電子公文系統相關研究

電子公文交換系統用戶涵蓋各級政府機關（構）、公司企業及人民組織團體，迄至 2021 年底止用戶數已逾 35,000 個，用戶間網網相連、息息相關，進行公文交換作業，建立資訊安全強化措施的重要性更是無庸置疑，行政院亦將之納為國家關鍵資訊基礎設施（Critical Information Infrastructure, CII）之一，檔案局資通安全責任等級亦核定提升為 A 級，足見其對政府運作的重要性（邱菊梅與林其範，2020）。然而，在系統運行的過程中仍伴隨著諸多資安課題及挑戰，下表彙整近 3 年各研究學者針對電子公文系統所做之相關研究，詳如表 2。

表 2 電子公文系統相關研究列表

發表年份	研究學者	研究內容
2013 年	胡家銘 醒吾科技大學	發展出電子公文之文件進行數位簽名且有加密及解密功能的公文管理系統。
2018 年	張守群 臺灣科技大學	透過聯盟區塊鏈的技術來讓企業間或者是企業內的檔案交換機制更完善，藉由區塊鏈的特性解決以往中心化架構的缺點以及透過 Quorum 的資料隱私處理，確保只有相關的受文者可以收到交易資料，保障交換雙方的隱私。
2019 年	郭靜瑋 國防大學	以橢圓曲線密碼系統為基礎，及具自我認證機制及隨機背包密碼系統管控電子公文系統內密件公文之安全性。
2019 年	翁紹宏 國防大學	將國軍現行電子公文處理與傳遞流程的弱點及文件控管的安全缺失，應用數位浮水印嵌入技術，分辨電子公文之真實性，達成系統維運之文件安全管控方式。

此外，近年來許多國家正試圖應用區塊鏈的技術改善醫療保健、金融應用、基礎設施、資產管理、教育、數據管理及供應鏈溯源等範疇，進而強化數位政府的運作，以提升運作效能（Clavin et al., 2020）。我國行政院於 2019 年核定「智慧政府推動策略計畫」，其中推動之策略：創新科技導入客製化民生服務，即要求政府應秉持「科技脈動、服務原力」原則，創新政府為民服務型態，改造政府服務企業模式，加速政府運作效率，善用人工智慧、區塊鏈等技術，改善政府運作程序，聚焦於政府內部管理之應用。

學者陳美蓉與林其範（2020）提出未來區塊鏈導入新一代交換系統的可行性，為考量交換系統的資料保護需求及使用者認證安全性，應以許可制方式管理使用者會員，且

交換系統地址簿應採用聯盟鏈模式，藉此達到資料分散保存且避免單點故障所引發的問題，而每一位使用者都可取得並驗證區塊鏈內容的資料，以確保其資料透明及可靠性，解決資料即時性的問題，另現行系統僅能透過地址簿維護機關提供佐證資料，若加入區塊鏈技術，未來可經由公開透明第三方認證，提高資料可信度，並同時降低集中式管理的維護成本。

三、交易協定設計

本研究提出由以太坊智慧合約所建構之去第三方且具資料隱私之電子公文交換協定設計，為符合電子公文交換之身分驗證的要求，本研究採用聯盟鏈為原型，將參與區塊鏈的憑證中心、發文者、受文者及管理平台為各個節點，共同維護區塊鏈的分散式帳本，且因區塊鏈不可竄改資料的特性，可提升電子公文交換系統的可信度，以下將說明本研究所提出之電子公文交換系統架構及其運作流程。

本研究交易協定區分為初始、註冊、收文及發文階段（各階段設計如圖 2 所示）。憑證中心負責組織身分認證、各簽章及驗證之功能，並對電子公文及隱私數據進行加解密。智慧合約區分為部署及執行兩部分，先將智慧合約程式部署到區塊鏈網路中儲存，再經由智慧合約的呼叫，實現區塊鏈網路中公文交換管理的功能，本文主要由兩個智慧合約組成，分為收文智慧合約$ReSC$及發文智慧合約$SeSC$，其中$ReSC$包含交換管理XM，而$SeSC$則包含檔案管理FM及交換管理XM。收發文代理服務$SAgent$包含收文代理服務$RSAgent$及發文代理服務$SSAgent$，為電子公文交換之重要角色，負責和區塊鏈節點溝通與收發文作業，同時負責將公文交換檔案儲存至檔案管理區。區塊鏈網路是一個由多方參與且共同維護的分散式數據庫，透過分散式節點、不可竄改的密碼系統及共識機制等技術，使系統具有較高之安全性，而去中心化的特性可強化電子公文交換安全及完整性。

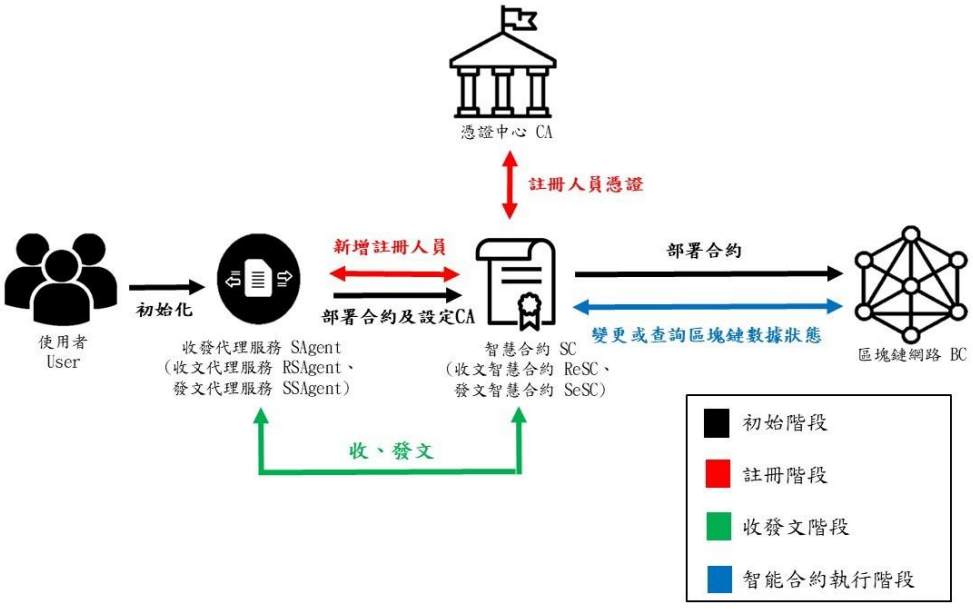

圖 2 各階段設計圖

3.1 交易流程架構及符號

本研究智慧合約設計之流程主要分為初始、註冊、收文及發文階段。各階段使用之符號參數，如表 3 所示。

表 3 符號參數說明表

項目	符號	說明
1	CA、$SAgent(RSAgent$、$SSAgent)$、$SC(ReSC$、$SeSC)$、BC、$User$	分別表示為憑證中心、收發文代理服務（收文組織、發文組織）、智慧合約（收文智慧合約、發文智慧合約）、區塊鏈網路、使用者。
2	XM、FM、$ReSC$、$SeSC$	分別表示為交換管理、檔案管理、收文、發文的智慧合約。
3	Pk_x、W_x	憑證中心、收發文代理服務、發文組織、收文組織及使用者的公鑰和簽章，其中x代表參與者身分。
4	add_x	外部擁有帳戶（Externally Owned Account, EOA）之位址，其中x代表參與者身分。
5	$E_k(d)$、$h(d)$	透過金鑰k對公文d進行加密、對公文d進行雜湊運算。
6	$Deploy$、$Initialization$	部署智慧合約、初始化交換網路。
7	$RegisterEvent()$、$RegisteredEvent()$、$RegisterPermitEvent()$、$QueryRecipientEvent()$、$DocExchangeEvent()$、$sendDocEvent()$、$recieveDocEvent()$	人員註冊事件、人員已註冊、人員註冊成功、查詢受文者資料、觸發公文交換、發文成功、觸發收文事件
8	$modifierSAgent()$、$modifierCA()$、$modifierUser()$、$modifierSender()$、$modifierRecipient()$	分別限制為只有收發代理服務、憑證中心、使用者、發文組織或收文組織可以執行。
9	$setCAPk()$、$setCAAdd()$	收發文代理服務設定憑證中心憑證及位址資訊。
10	$setCA()$	在智慧合約中將憑證中心位址設立為產生憑證單位。
11	$registerCert()$	使用者呼叫智慧合約執行註冊功能。
12	$setRegister()$	CA提供註冊人員公鑰及憑證資訊。
13	$Existed$	為註冊人員狀態，$true$為已註冊成員，$false$則反之。
14	$ListInfo$	受文者清單，包含公文名稱、內文描述、檔案雜湊值、受文者編號、發文者及受文者位址。

表 3 符號參數說明表（續）

項目	符號	說明
15	$createRecipientList()$	建立受文者清單
16	$recipientInfo$	受文者資訊，包含受文者編號、名稱、公鑰及位址。
17	$decrptDoc()$、$encrptDoc()$、$createDoc()$、$UploadDoc()$、$saveDoc()$	解密檔案、加密檔案、建立發文資訊、上傳檔案、儲存檔案
18	$queryRecipient()$、$queryDocAddress()$、$requestDoc()$	查詢受文單位、查詢檔案之 API 位址、請求檔案下載

3.2 初始階段

收發代理服務部署智慧合約於區塊鏈網路上，接著設定憑證中心之位址、公鑰及憑證資訊（如圖 3）。

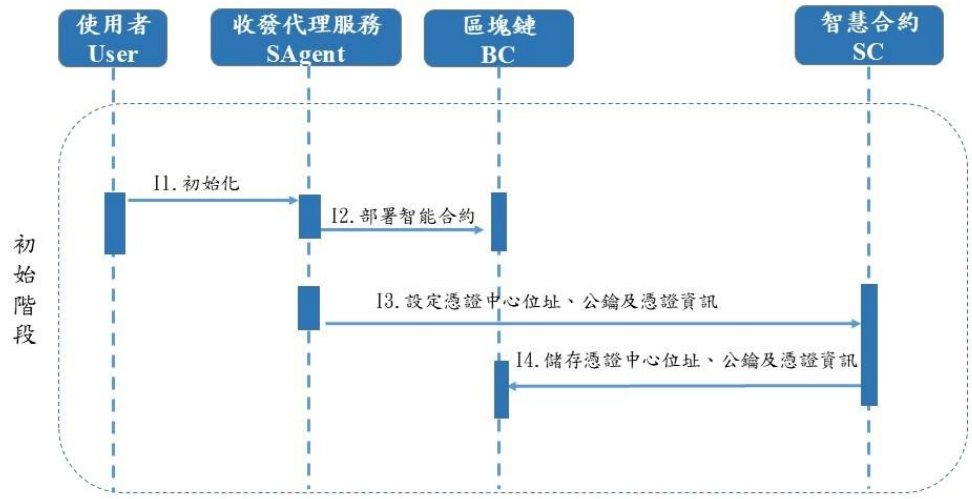

圖 3 初始階段循序圖

I1. 初始化：使用者將自身單位資訊存入收發代理服務的設定檔，完成初始化。

$$User \xrightarrow{Initialization} SAgent \quad (1)$$

I2. 部署智能：合約收發代理服務部署智慧合約。

$$SAgent \xrightarrow{Deploy} BC：\mathrm{SC} \quad (2)$$

I3. 設定憑證中心位址、公鑰及憑證資訊：收發代理服務設定憑證中心位址、公鑰及憑證資訊。

$$SAgent \rightarrow SC：modifierSAgent\left(setCA(add_{CA}, Pk_{CA}, Cert_{CA})\right) \quad (3)$$

I4. 儲存憑證中心位址、公鑰及憑證資訊：智慧合約儲存憑證中心位址、公鑰及憑證資訊於區塊鏈網路上。

$$SC \rightarrow BC：add_{CA}, Pk_{CA}, Cert_{CA} \quad (4)$$

3.3 註冊階段

憑證中心及註冊者透過自我認證機制演算法產生一組公、私鑰對，再運用 CA 的私鑰與參與者的公鑰加上數位簽章，來製作憑證。註冊者資訊將儲存於區塊鏈網路，並觸發新增成員事件。最後，改變人員存在狀態，完成註冊，並將資訊儲存於區塊鏈網路上（如圖 4）。

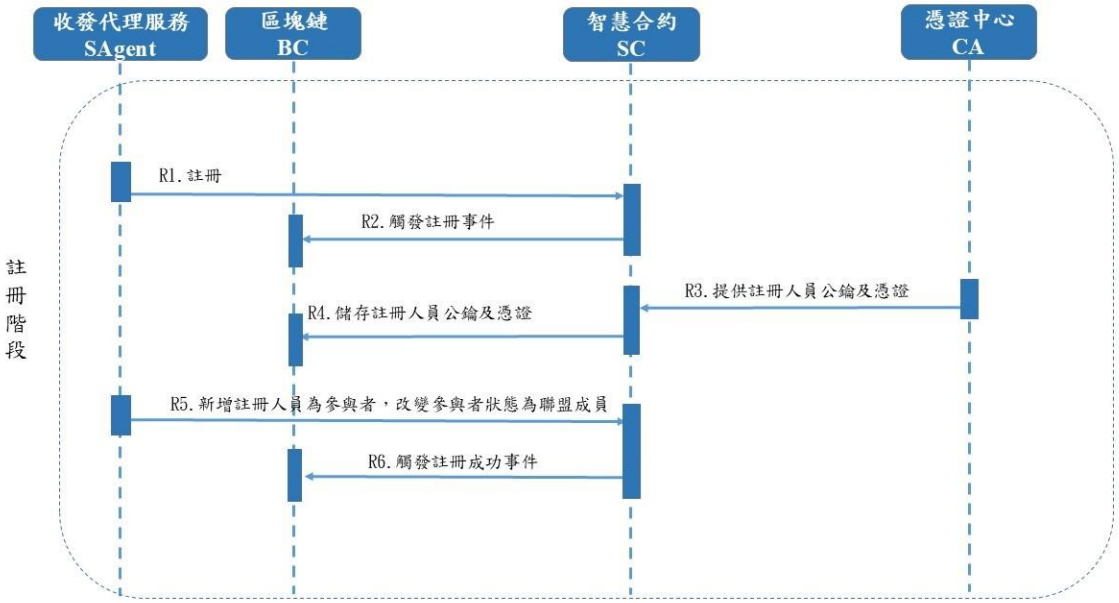

圖 4 註冊階段循序圖

R1. 註冊：使用者透過收發代理服務呼叫智慧合約註冊功能，提交註冊位址。

$$SAgent \rightarrow SC：register(add_{User}) \quad (5)$$

R2. 觸發註冊事件：智慧合約SC觸發人員註冊事件。

$$SC \rightarrow BC：RegisterEvent \quad (6)$$

R3. 提供註冊人員公鑰及憑證：憑證中心透過基於橢圓曲線之自我認證公開金鑰系統，與註冊之參與者建立其公、私鑰，並透過智慧合約設定註冊參與者公鑰及憑證資訊。

$$CA \rightarrow SC：modifierCA\big(setRegister(add_{User}, W_{User}, PK_{User})\big) \quad (7)$$

R4. 儲存註冊人員公鑰及憑證：檢查註冊事件狀態，若狀態為$true$則回傳該位址已註冊，若為$false$則儲存註冊人員公鑰及憑證於區塊鏈網路上，並觸發新增人員事件。

$$SC \rightarrow BC：(add_{User}, W_{User}, PK_{User}, RegisteredEvent) \quad (8)$$

R5. 新增註冊人員為參與者，改變參與者狀態為聯盟成員：檢查$Existed$狀態，狀態為$true$則回傳已為系統成員，如為$false$則收發代理服務可將成員狀態改變為$true$。

$$SAgent \rightarrow SC：modifierSAgent\big(addAccount(add_{User})\big) \quad (9)$$

R6. 觸發註冊成功事件：檢查成員是否已存在，若存在則觸發註冊成功事件。

$$R6：SC \xrightarrow{isExisted(true)} BC：RegisterPermitEvent \quad (10)$$

3.4 收文階段

使用者透過收文代理服務進行收文作業，而收文代理服務透過監聽交換網路取回公文交換地址，並將簽章及檔案雜湊值傳給發文代理服務用以請求檔案下載，發文代理服務驗證簽章以確認收文代理服務的身分，並驗證該其是否為合法受文者清單成員，此步驟可以避免身分偽造問題，驗證通過後將從隔離區取得交換檔案，再加簽檔案雜湊值及交換檔案回傳至收文代理服務，經驗證無誤後，再以雙方共產的金鑰解密檔案(如圖 5)。

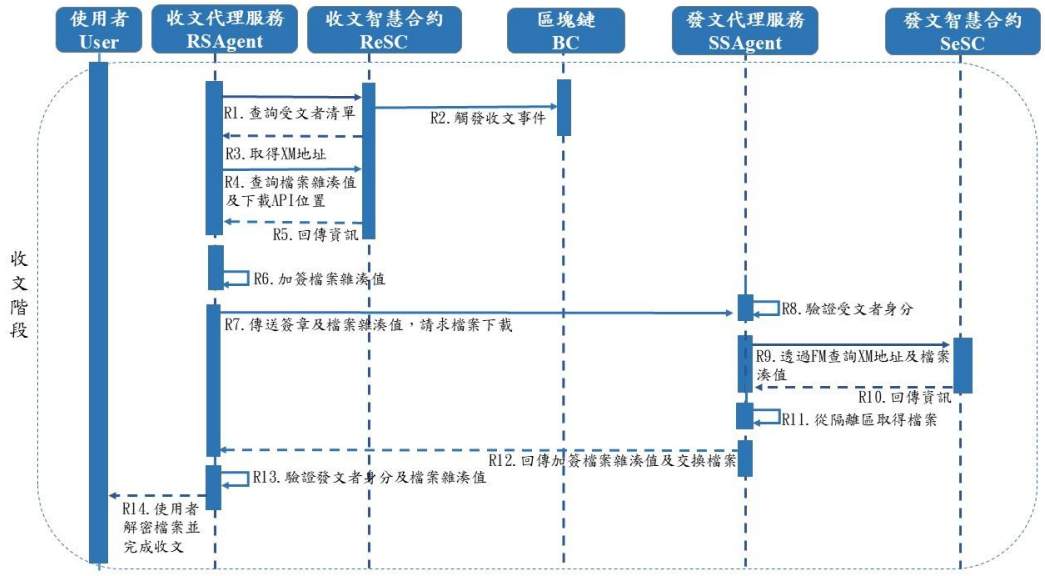

圖 5 收文階段循序圖

R1. 查詢受文者清單：收文代理服務廣播查詢受文單位。

$$\boldsymbol{RSAgent \rightarrow ReSC：modifierSAgent(queryRecipient(recipientInfo))} \quad (11)$$

R2. 觸發收文事件：收文智慧合約觸發收文事件。

$$ReSC \xrightarrow{isRecipient(true)} BC：recieveDocEvent \quad (12)$$

R3. 取得XM地址：收文代理服務取得公文交換位址。

$$ReSC \rightarrow RSAgent：modifierSAgent\big(getDocExchange(XMaddress)\big) \quad (13)$$

R4. 查詢檔案雜湊值及下載API位置：收文代理服務查詢檔案雜湊值及API位址。

$$RSAgent \rightarrow ReSC：modifierSAgent(queryDocAddress(XMaddress)) \quad (14)$$

R5. 回傳資訊：收文代理服務透過位址取得檔案雜湊值及API位址。

$$ReSC \rightarrow RSAgent：modifierSAgent\big(getDocExchange(h(d), dataHostUrl)\big) \quad (15)$$

R6. 加簽檔案雜湊值：收文代理服務加簽公文檔案雜湊值。

$$RSAgent：modifierSAgent\big(signatureDochash(W_{User})\big) \quad (16)$$

R7. 傳送簽章及檔案雜湊值，請求檔案下載：收文代理服務傳送簽章及檔案雜湊值給發文代理服務，以請求檔案下載。

$$RSAgent \rightarrow SSAgent：modifierSAgent\big(requestDoc(W_{User}, h(d))\big) \quad (17)$$

R8. 驗證受文者身分：發文代理服務驗證受文者身分。

$$SSAgent：modifierSAgent(isRecipient(true)) \quad (18)$$

R9. 透過FM查詢XM地址及檔案雜湊值：發文代理服務查詢檔案雜湊值及API位址。

$$SSAgent \rightarrow SeSC：modifierSAgent(queryDocAddress(XMaddress)) \quad (19)$$

R10. 回傳資訊：發文代理服務透過位址取得公文檔案雜湊值及API位址。

$$SeSC \rightarrow SSAgent：modifierSAgent\big(getDocAddress(h(d), dataHostUrl)\big) \quad (20)$$

R11. 從隔離區取得檔案：發文代理服務取出公文檔案。

$$SSAgent：modifierSAgent\big(getDoc(file, dataHostUrl, PK_{User}, h(d))\big) \quad (21)$$

R12. 回傳加簽檔案雜湊值及交換檔案：發文代理服務回傳公文檔案。

$$SSAgent \rightarrow RSAgent：modifierSAgent\big(sendDoc(file, W_{User}, h(d))\big) \quad (22)$$

R13. 驗證發文者身分及檔案雜湊值：收文代理服務驗證發文者身分及檔案雜湊值。

$$RSAgent：modifierSAgent\Big(isSender(true), h(d)\Big) \quad (23)$$

R14. 解密檔案並完成收文：使用者以E_{User}密鑰解密公文檔案，完成收文。

$$RSAgent \rightarrow User：modifierUser\big(decrptDoc(E_{User})\big) \quad (24)$$

3.5 發文階段

發文過程中發文代理服務利用公文交換管理合約來查詢受文單位資訊，使用者上傳公文前檔案透過橢圓曲線加密法完成加密，並產出受文者清單使合法受文者擁有下載公文及檔案之權利，後由發文代理服務寫入相關發文資訊且觸發公文交換事件，將雜湊值與合約地址存入檔案管理合約，以完成發文作業（如圖 6）。

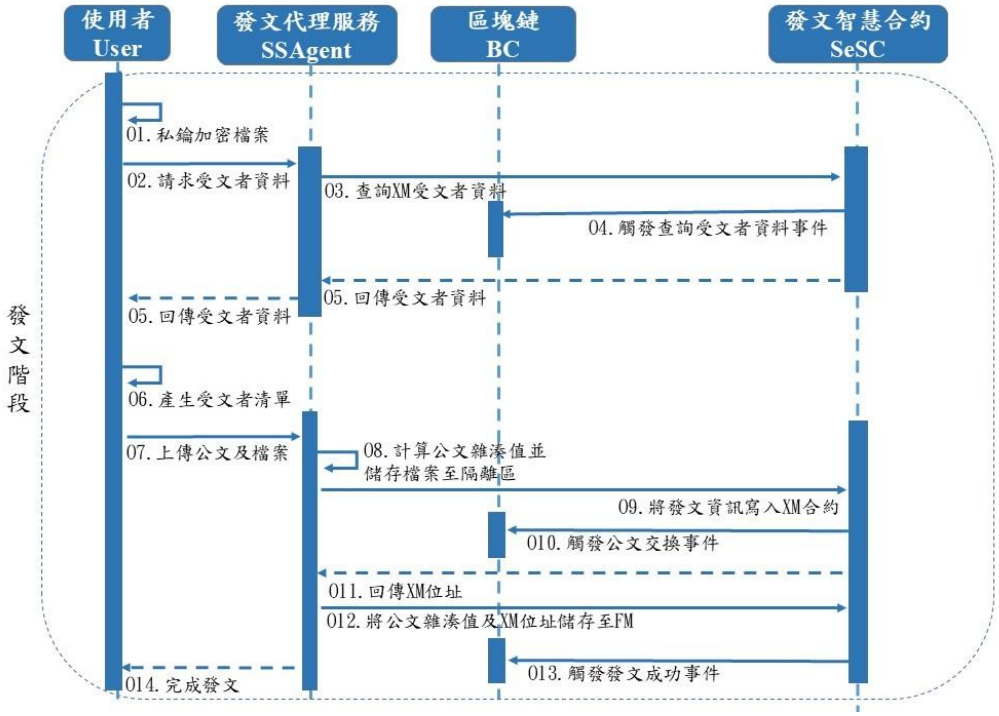

圖 6 發文階段循序圖

O1. 私鑰加密檔案：使用者以E_{User}密鑰加密公文檔案。

$$User：modifierUser\big(encrptDoc(E_{User})\big) \quad (25)$$

O2. 請求受文者資料：使用者請求發文代理服務查詢受文者資料。

$$User \rightarrow SSAgent：modifierUser(queryRecipient(recipientInfo)) \quad (26)$$

O3. 查詢XM受文者資料：發文代理服務利用公文交換管理合約查詢受文單位資訊。

$$SSAgent \rightarrow SeSC：modifierSAgent(queryRecipient(recipientInfo)) \quad (27)$$

O4. 觸發查詢受文者資料事件：發文智慧合約觸發查詢受文者資料事件。

$$SeSC \xrightarrow{isExisted(true)} BC：QueryRecipientEvent \quad (28)$$

O5. 回傳受文者資料：使用者取得受文者資料。

$$SeSC \rightarrow User：modifierUser\big(getRecipientAddress(recipientInfo)\big) \quad (29)$$

O6. 產生受文者清單：使用者建立交換檔案時的受文者清單。

$$User：modifierUser(createRecipientList(listInfo)) \quad (30)$$

O7. 上傳公文及檔案：使用者將交換檔案及受文清單傳遞給發文代理服務。

$$User \rightarrow SSAgent：modifierUser(UploadDoc(file, listlnfo, PK_{User}, W_{User})) \quad (31)$$

O8. 計算公文雜湊值並儲存檔案至隔離區：發文代理服務將交換檔案及檔案雜湊值儲存至檔案隔離區。

$$SSAgent：modifierSAgent\big(saveDoc(file, dataHostUrl, PK_{User}, h(d))\big) \quad (32)$$

O9. 將發文資訊寫入XM合約：在公文交換管理合約中建立發文資訊。

$$SSAgent \rightarrow SC：modifierSAgent\big(createDoc(listInfo, dataHostUrl, PK_{User}, h(d))\big) \quad (33)$$

O10. 觸發公文交換事件：發文智慧合約觸發公文交換事件。

$$SeSC \xrightarrow{isAvailable(true)} BC：DocExchangeEvent \quad (34)$$

O11. 回傳XM位址：發文代理服務取得公文交換位址。

$$SeSC \rightarrow SSAgent：modifierSAgent\big(getDocExchange(XMaddress)\big) \quad (35)$$

O12. 將公文雜湊值及XM位址儲存至FM：儲存公文及檔案雜湊值至檔案管理隔離區。

$$SSAgent \rightarrow SeSC：modifierSAgent\big(saveDoc(XMaddress, h(d))\big) \quad (36)$$

O13. 觸發發文成功事件：儲存發文資訊至區塊鏈上。

$$SeSC \xrightarrow{isAvailable(true)} BC：sendDocEvent \quad (37)$$

O14. 完成發文：使用者完成發文。

$$User：modifierUser(sendDoc(true)) \quad (38)$$

四、安全性分析與評估

本研究提出基於聯盟鏈的電子公文交換系統機制，而本章節將針對協定中的各項流程及機制，透過 BAN-Logic 邏輯分析及非正規之情境分析，並探討相關安全性指標滿足

情形，藉以評估本研究機制之安全性。

4.1 BAN-Logic

透過 BAN 邏輯分析模式（符號表如表 4），來證明註冊及收、發文階段參與者 Participant（本章節定義為使用者 User 及收發代理服務 SAgent）與智慧合約 SC 雙方能否信任彼此的共享金鑰，以確保機制的安全性及自我認證等特性（如表 5）。

表 4　BAN-Logic 符號表

符號	定義
$P \mid \equiv X$	P相信X為正確。
$P \lhd X$	P看到X這個訊息，也就是當有人傳送訊息給P時，P就會看到X。
$P \mid \sim X$	P曾經傳送過X這個訊息。
$P \mid \Rightarrow X$	P對X有管轄權。
$\#(X)$	X是新生成的。
(X, Y)	X或Y皆屬於(X,Y)的一部分。
$\langle X \rangle_Y$	X被與Y結合。
$\{X\}_Y$	X是訊息，用Y金鑰加密。
$\mid \xrightarrow{key} P$	P擁有一把公鑰叫做key，也就是P也會有一把相對的私鑰。
$\mathrm{P} \overset{k}{\leftrightarrow} Q$	P、Q之間交換一把金鑰叫做k，且k不會被第三方所得知或使用。
$\mathrm{P} \overset{s}{\leftrightarrow} Q$	P、Q 之間交換一個秘密叫做 s，例如密碼等。
$KEY_{(P,Q)}$	為P 與Q 之間的共享金鑰。

表 5　本研究 BAN-Logic 協定內容表

訊息	符號表示	訊息	符號表示
訊息一	$Participant \rightarrow SC：(PK_{\mathrm{Participant}}, P_{\mathrm{Participant}}, id_{\mathrm{Participant}})$	訊息二	$SC \rightarrow Participant：(PK_{\mathrm{SC}}, P_{SC}, id_{SC})$
目標一	$SC \mid \equiv PK_{Participant}$	目標三	$Participant \mid \equiv Participant \overset{k_{(\mathrm{Participant},SC)}}{\longleftrightarrow} SC$
目標二	$Participant \mid \equiv PK_{SC}$	目標四	$SC \mid \equiv Participant \overset{k_{(\mathrm{Participant},SC)}}{\longleftrightarrow} SC$

接著對所提出的機制進行一些假設，之後進一步透過 BAN-Logic 證明假設的推論結果，假設如表 6：

後續，BAN-Logic 依據上述邏輯規則和假設，來證明本研究的完整性。相關證明過程如后：

在SC獲取訊息一時，可以證明SC可看到$Participant$傳送之的訊息：

$$SC \lhd (PK_{Participant}, P_{Participant}, id_{Participant}) \quad (39)$$

並可推論出：

$$SC \lhd (PK_{Participant}) \quad (40)$$

表 6　本研究 BAN-Logic 證明假設表

假設	符號表示	假設	符號表示
假設一	$Participant\| \Rightarrow d_{Participant}$	假設六	$\mathrm{SC}\| \equiv Participant\| \equiv (n_{Participant}, CA\| \sim P_{\mathrm{Participant}})$
假設二	$SC\| \equiv Participant\| \sim (id_{Participant}\ , d_{Participant})$	假設七	$Participant\| \equiv id_{SC}$
假設三	$SC\| \Rightarrow d_{SC}$	假設八	$SC\| \equiv id_{Participant}$
假設四	$SC\| \equiv CA\| \sim w_{Participant}$	假設九	$Participant\| \equiv CA\| \sim w_{SC}$
假設五	$Participant\| \equiv SC\| \equiv (n_{SC}, CA\| \sim P_{SC})$	假設十	$Participant\| \equiv SC\| \sim (id_{SC}\ , d_{SC})$

由假設一、假設二及假設四我們可以得知：

$$SC\| \equiv Participant\| \Rightarrow PK_{Participant} \quad (41)$$

且$$SC\| \equiv Participant\| \equiv PK_{Participant} \quad (42)$$

並可推論出：

$$SC\| \equiv PK_{Participant}（目標一） \quad (43)$$

基於本研究註冊階段程序，SC的n_{SC}及PK_{SC}與參與者註冊程序相同，故同理可證當 Participant 獲取訊息二後，依據假設三、假設八及假設十，亦可得證：

$$Participant\| \equiv SC\| \Rightarrow PK_{SC} \quad (44)$$

且$$Participant\| \equiv SC\| \equiv PK_{SC} \quad (45)$$

並可推論出：

$$Participant\| \equiv PK_{sc}（目標二） \quad (46)$$

因此可滿足自我認證之特性，無須透過CA憑證中心即可驗證雙方身分，且因參與者對自行選取之隨機值 d 具有管轄權，避免第三方假冒身分。

基於假設八，我們可以證明：

$$SC\| \equiv CA\| \sim P_{\mathrm{Participant}} \quad (47)$$

基於假設五及目標一，我們可以證明：

$$SC\| \equiv Key_{(SC,Participant)} \quad (48)$$

$$SC\| \equiv \mathrm{Participant} \xleftrightarrow{key_{(SC,Participant)}} SC（目標四） \quad (49)$$

基於假設七，可以證明：

$$Participant\| \equiv CA\| \sim P_{\mathrm{SC}} \quad (50)$$

基於假設六及目標二所得證，我們可以證明：

$$Participant\| \equiv Key_{(SC,Participant)} \quad (51)$$

$$Participant\ | \equiv Participant \xleftrightarrow{key_{(SC,Participant)}} SC（目標三） \quad (52)$$

經過上述邏輯推導所得四項目標，證明本研究所提出之自我認證機制，以及所產生之共享密鑰，在合法性、可靠性及機密性上，對於參與者及智慧合約而言都是可以相互信任。

4.2 相關安全性指標分析

本研究透過情境分析法，針對可能發生之情境，研擬出相關對策，並依國際標準組織（International Standards Organization, ISO）所提出的資訊系統安全性管理需求，一個安全的資訊系統應該要達到的機密性（Confidentiality）、完整性（Integrity）、鑑別性（Authentication）、不可否認性（Non-repudiation），本研究設計以區塊鏈及智慧合約達

成第三方最小參與度，並導入自我驗證機制，使各使用者間無須透過憑證中心，即可相互驗證身分，本研究針對各項安全指標之定義、情境及解決方法進行探討。

4.2.1 機密性

機密性係指在適當的安全機制下，保護資料和資源以避免暴露於無權限人員或程式之下，而危害到資訊安全目標，也是為維護資料在傳輸、儲存與處理狀態時，不被非授權人員之存取及使用。

- 情境：駭客意圖攔截發文者及收文者之間的電子公文交換訊息。
- 解決方法：發文者與收文者在收發文進行過程中，會傳送身分資訊（步驟 O9、$R7$）。由發文者與受文者產生共享密鑰 $Key_{(P,Q)}$，電子公文檔案經過加密後才進行傳送，雖然身分資訊$(ID_{user}、S_{user}、PK_{user})$公開，但只有發文者與受文者可產生共享密鑰$Key_{(P,Q)}$，並由受文者以共享密鑰解密，故即便駭客從中攔截，仍無法解密。

4.2.2 完整性

完整性係指確保資料在傳遞過程中不會被任意變更、竄改，其內容均維持一致，且可確認是由傳送方所發出（Stallings and Brown, 2018）。

- 情境：駭客意圖竄改電子公文內容。
- 解決方法：於發文者透過智慧合約，建立發文資訊並儲存檔案雜湊值（參數為 h(d)）於區塊鏈網路上（步驟 O9）；而受文者於驗證發文者身分及檔案之雜湊值確認相符後才會完成收發文（步驟 R12）。

4.2.3 鑑別性

鑑別性係指能確認網路使用者或資料傳送者身分之特性。在公開金鑰系統中，可藉由公鑰鑑別身分（Stallings and Brown, 2018）。

- 情境：駭客攔截發文者傳送給收文者的電子公文交換資訊。
- 解決方法：參與者均需透過憑證中心進行註冊，由憑證中心設定參與者至區塊鏈網路（步驟 R3）且在發文者發文階段和受文者確認收文時，會傳送交易雙方身分資訊，並檢查雙方身分驗證資訊是否相符，並透過$Key_{(P,Q)}$產生之共享密鑰，對電子公文進行加密，故駭客無法偽裝身分從中攔截並對所獲之資訊進行解密。

4.2.4 不可否認性

不可否認性係指對已經發生之事件或行動的證明，使該事件或行動於日後無法被否認。簽章具有不可否認性，只有發文者知道自己的私密金鑰，因此發文者無法否認簽章的產生及公文傳送的事實。

- 情境：收文者聲稱未收到發文者電子公文資訊，要求重新發文。
- 解決方法：發文過程中（步驟 O1至步驟 O14），發文資訊均公開儲存於區塊鏈網路，當發文資訊產生時，亦將受文者清單及公文檔案暫存於智慧合約位址當受文者驗證發文者身分及檔案完整性後，會由智慧合約直接交換電子公文（步驟 R11、R12）且收發文紀錄會儲存於區塊鏈網路上，該過程具備不可否認性。

4.2.5 不可偽造性

不可偽造性指的是在資料傳遞的過程中，不會遭到惡意的第三者竄改資料的內容，確保資料可以完整無誤的傳送至接收端。

- 情境：駭客試圖偽造收文資訊以取得電子公文檔案。
- 解決方法：因公文資訊加密後使用單向雜湊函數運算產生密文摘要，且由於單向雜湊函數有無法逆推的特性，駭客無法透過密文摘要取得公文資訊，且偽冒的密文訊息在簽章驗證階段時無法通驗證，故不會受到第三方偽造的可能。

4.2.6 自我驗證機制

自我驗證機制係指使用者在授權階段會參與憑證中心之公鑰計算，且憑證中心的憑證會內嵌於公鑰中，可讓使用者獨立進行身分驗證，而不需再透過第三方。

- 情境：系統安全機制須整體考慮人員安全、實體安全及軟體安全，各流程須考量資料安全性及正確性，於各使用者的溝通管道，規劃適當之安全性協定。
- 解決方法：交換系統的登入介面，機關層登入必須透過相容於憑證管理中心所製發之憑證卡及地址簿設定進行雙重認證；當檔案傳送時，傳送方須將檔案進行簽章，接收方需驗證簽章，以驗證檔案是否為遭竄改及確認傳送者身分；而本研究是從系統註冊使用者時，即可利用憑證中心授予的公鑰等參數進行互相的身分認證，不須與憑證中心隨時保持連線，達到自我認證機制之安全性。

4.2.7 小結

本研究設計之機制整體流程，在資訊安全方面可達到機密性、完整性、鑑別性與不可否認性；在公文交換方面具備不可偽造性及自我認證機制。以本研究流程而言，以智慧合約的條件設置降低後續第三方調解機制之需求，預防問題爭議的發生，且因智慧合約透明而公開於區塊鏈網路，將有利後續具有公信力之監管單位使用；由於本研究架構以區塊鏈為底層技術，公文檔案均儲存於檔案隔離區，採分散式儲存架構，具有無法竄改且永久保存之特性；因此，在公文檔案已儲存至檔案隔離區的情況下，即便發文者將公文刪除或銷毀，收文者仍能透過收文組織，依程序請求發文組織自檔案隔離區取得公文檔案，另本研究電子公文交換機制搭配橢圓曲線密碼學演算法，公鑰與私鑰均透過橢圓曲線加密演算法產生，如有意圖不軌第三方企圖竊取或竄改公文資料，則需面對如何破解橢圓曲線離散對數之難題。

本研究參考先前研究，針對機密性、完整性、鑑別性、不可否認性、不可偽造性及自我認證機制等 6 個安全性指標進行分析（如表 7）。胡家銘（2013）研究公文透過加密方式，達到在傳遞公文過程中的完整性及不可否認等特性，但由於內部人員仍可能透過中心化伺服器取得資料，甚至竄改資料，故僅符合部分不可偽造性；此外，仍須仰賴機關之交換中心及文檔人員參與公文電子交換之流程，資料採集中式架構管理，且相關認證仍須透過憑證中心進行，故不符合第三方最低參與度及自我認證特性。翁紹宏（2019）透過數位浮水印技術導入公文電子交換系統，以確保機密性、完整性與不可否認性，然而，研究中未提及資料之不可偽造性，且仍須透過憑證中心進行身分驗證，亦未提出自我認證之特性，故無法符合第三方最低參與度。張守群（2018）提出藉由聯盟區塊鏈的技術，使企業間或者是企業內部檔案交換機制更完善，透過區塊鏈的特性解決中心化架構的缺點，確保只有經授權的受文者可以收到交易資料，故具不可偽造、完整、不可否認等特性，另該設計框架以去中心化公開金鑰基礎建設（Decentralized Public Key Infrastructure, DPKI）服務處理身分確認機制，以系統設計而言，部分符合最低第三方參與度，而該設計在憑證中心離線狀態下，無法進行身分認證，表示無自我認證特性。

表7 本研究與其他研究之安全性分析比較表

安全性分析比較項目	機密性	完整性	不可否認性	不可偽造性	第三方最低參與度	自我認證機制
電子化公文系統（胡家銘，2013）	○	○	○	X	X	X
以數位浮水印技術提升電子公文交換系統安全機制（翁紹宏，2019）	○	○	○	X	X	X
基於區塊鏈之電子訊息交換（張守群，2018）	○	○	○	○	△	X
本研究	○	○	○	○	○	○

○：符合

△：代表部分符合特性

X：不符

五、結論與未來研究方向

本章就本研究之結論、在國防領域的應用及未來研究方向三個部分詳述說明。

5.1 結論

本研究以區塊鏈技術為基礎，發展植基於聯盟鏈之電子公文交換系統。除建立自我認證之身分驗證機制外，區塊鏈技術建構的智慧合約保有公開式記錄及去中心化的運行特性，佈署於區塊鏈平台後，此平台之使用者分散式執行觸發智慧合約條件，自動觸發電子公文交換；本研究去中心化的交換架構，大幅降低傳統電子公文系統單點失效的風險，且經由許可制的區塊鏈網路來進行電子公文交換作業，藉此限制僅合法受文者才能取得交易中的資料，因加密的公文資料存放於發文者的系統內，僅供相關受文者存取下載，提高資料的機密性及安全性。本研究所提出之電子公文交換機制，除安全性可達資訊安全原則，還具備下列優點：（1）本研究透過自我認證機制產生公、私鑰，可在與憑證中心離線狀態下，進行身分驗證，使第三方參與程度降低。（2）本研究透過智慧合約自動執行，確保公文交換作業流程的正確性，建立完善的控制機制。（3）本研究交換記錄均分散儲存於區塊鏈各節點，具可驗證性、永久保存且公開透明，建立可信任的服務，並避免爭議。

5.2 國防領域之應用

本研究透過智慧合約之程式條件完成電子公文交換系統各項流程，並加入自我認證機制達到去中心化的目的，強化系統安全性；然而，電子公文交換系統已為國軍單位廣泛使用，成為國軍人員每日使用且重要的資訊系統之一，為有效控管電子公文的安全性，

此項技術可運用於國防領域。以管理層面而言，本研究機制導入智慧合約及自我認證機制，相較於現行公文系統的運作，可降低人力成本及管理負擔，無須再進行人工收發文；另外，以實務層面而言，現行公文系統採集中式架構，易有單點故障風險，藉由分散式系統的特性，開發出一套可對抗單點攻擊的國軍電子公文交換系統，確保系統可用性。

5.3 未來研究方向

本研究已符合預期之成果，結合區塊鏈技術、智能合約、自我認證機制強化電子公文交換系統的資安強度，本研究設計之協定符合國際標準組織所提出的資訊系統安全性管理需求機密性、完整性、鑑別性及不可否認性，結合區塊鏈技術，減少第三方的依賴性；然而，本研究僅採用邏輯推導及演算法分析，且智能合約之安全性及效率問題，亦須經設計及探討，若未來可導入實際系統測試，可大幅增加此研究之可信度。

參考文獻

行政院研究發展考核委員會(1997)。*電子化/網路化政府中程推動計畫(87 至 89 年度)*。5-6。

宋宜芳（2018）。*設計具高可靠度之存取控制-以國軍某電腦兵棋系統為例*。國防大學資訊管理學系未出版碩士論文，臺灣，臺北市。

余庭儀（2019）。植基於智慧合約的數位內容交易電子支付方法。國防大學資訊管理學系未出版碩士論文，臺灣，臺北市。

吳銳、劉導（2018）。*區塊「鏈」接智能*（36-40）。北京：電子工業出版社。

邱菊梅、林其範（2020）。全國共用公文電子交換政策制定與推動策略之探討。*檔案半年刊，19*（2），4-23。

胡家銘（2013）。*電子化公文管理系統加解密之研究*。醒吾科技大學資訊科技學系未出版碩士論文，臺灣，新北市。

胡國新（2001）。*設計植基於自我驗證公開金鑰系統之安全線上電子拍賣機制*。大葉大學資訊管理學系未出版碩士論文，臺灣，彰化縣。

陳文彬（2012）。*運用動態存取控制方法於雲端服務之研究*。國防大學資訊管理學系未出版碩士論文，臺灣，臺北市。

陳美蓉、林其範（2020）。我國公文電子交換系統回顧與展望。*檔案半年刊，19*（1），78-95。

郭靜瑋（2019）。*適用於國軍密件電子公文處理之機制設計*。國防大學資訊管理學系未出版碩士論文，臺灣，臺北市。

翁紹宏（2019）。*以數位浮水印技術提升公文電子交換系統安全機制之研究*。國防大學資訊管理學系未出版碩士論文，臺灣，臺北市。

梁榮哲(2012)。*多重文件盲簽章機制之設計*。國防大學資訊管理學系未出版碩士論文，臺灣，臺北市。

張守群（2018）。*基於聯盟區塊鏈之使用者導向電子訊息交換框架*。臺灣科技大學資訊管理學系未出版碩士學位論文，臺灣，臺北市。

楊耿瑜（2019）。公文電子交換機制新契機。*檔案半年刊，18*（2），106-117。

鏈習生（2022 年 11 月 23 日）。*公鏈、私有鏈、聯盟鏈是什麼?區塊鏈的三大分類介紹*。取自 2023 年 3 月 26 日 https://chainee.io/what-is-public-blockchain-private-blockchain-consortium-blockchain/

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設計與實作。*電子商務研究，12*（1），73-92。

Clavin, J., Duan, S., Zhang, H., Janeja, V. P., Joshi, K. P., Yesha, Y., Erickson, L. C., & Li, J. D. (2020). Blockchains for Government: Use Cases and Challenges. *Digital Government: Research and Practice, 1*(3), 22.1-22.21.

Girault, M. (1991). Self-Certified Public Keys, *Advances in Cryptology-Eurocrypt '91, 547*, 490-497.

Szabo, N. (1994). *Smart Contracts: Building Blocks for Digital Markets.* Retrieved on November 2, 2022, from https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Stallings, W., Brown, L. (2018). *Computer security: principles and practice* (4th ed.). London, England: Pearson.

Wood, G. (2014). *Ethereum: A secure decentralized generalised transaction ledger.* Available online at https://gavwood.com/paper.pdf.