區塊鏈技術於國防人事文件保存與驗證可行性研究
—以國軍軍士官任官令為例

蘇品長　王永志*

國防大學資訊管理學系

論文編號: NM-44-01-07
DOI: 10.29496/JNDM.202411_45(2).0001
來稿 2023 年 1 月 5 日→第一次修訂 2023 年 2 月 7 日→同意刊登 2023 年 2 月 26 日

摘要

區塊鏈為一種結合密碼學、數學與共識機制的劃世代技術。當「智慧合約」出現後，區塊鏈應用有了爆炸性突破，一舉飛躍至其他領域。各國亦開始針對國防的區塊鏈進行研究，如無人機管理等。目前國防人事文件仍多以紙本呈現，易因各種因素導致遺損，造成後續補發、查驗困難。本研究以國軍軍官士官任官令為例，提出以區塊鏈技術特性，設計將任官令導入區塊鏈後的作業流程，有效解決前述紙本文件產生之保存與換(補)發輔助驗證等問題，節省國防預算、增進人事文件處理效益並提升便民效益與國軍形象。

關鍵詞：區塊鏈、任官令、密碼學、智慧合約

*聯絡作者：王永志 email: yjwang980204001@gmail.com

The Feasibility Study on Blockchain Technology for Preservation and Validation of National Defense Personnel Documents: Commission Certificate of ROC Armed Forces Officer/NCO

Su, Pin-Chang Wang, Yeong-Jyh*

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

Abstract

Blockchain is a groundbreaking technology that combines cryptography, mathematics, and consensus mechanisms. With the emergence of "smart contracts", blockchain applications have made an explosive breakthrough and leapt into other fields. Countries are also starting to research blockchain for defense, such as drone management. At present, most of the national defense personnel documents are still presented in paper form, which are easily lost due to various factors, making it difficult to reissue and check them later. In this study, we propose a blockchain technology to design the operation flow of the blockchain after the commission certificate of ROC Armed Forces officers/NCOs, which can effectively solve the problems of preservation and replacement of paper documents, saving on national defense budget, improving the efficiency of the national defense personnel documents processing, and enhancing the image of ROC Armed Forces.

Keywords: Blockchain, Commission Certificate, Cryptography, Smart Contract

* Corresponding Author: Wang, Yeong-Jyh email: yjwang980204001@gmail.com

一、前言

近幾十年來，隨著電腦資訊科技快速發展，不論是有形的硬體設備及有無線網路裝置、線路，抑或是無形的軟體系統及程式語言，均呈現爆炸性的速度增長，可謂「一日千里」。上開技術的成長，亦帶動了網際網路的發展，許多可在網際網路上直接操作的應用軟體與系統也如雨後春筍般地出現，而這更帶動了「主從式架構（Client-Server Model）」、「多層式架構（N-Tiers）」等線上系統架構的發展。這些系統通常會有「應用程式伺服器」、「中央資料庫」等特色，所有資訊均須透過一個中心角色來處理、儲存，形成一個「中心化」的樣態。

隨著網際網路持續發展，有別於使用者只能被動瀏覽網頁、透過中心化的角色來存取、搜尋資料，慢慢有人開始針對「中心化」進行反思。因為都要透過一個中介的角色來進行處理，如果說每一台電腦（或其他設備）就是一個節點，這樣就不需要只向單一個中心化節點存取、查詢，達到「資料共享」、「去除中心化的限制」等目的。在這樣的情形下，點對點（Peer-to-Peer; P2P）型式的網路架構便應勢而生。點對點特性簡言之，即「沒有一個固定的中心節點」，任何節點都能當做「中心節點」，交易結束後即變回一般的節點。點對點可應用在資料傳輸、共享，如著名的 FOXY 等。而點對點的概念，亦對後來的區塊鏈（Blockchain）發展，奠下一定的基礎。2008 年爆發的金融海嘯，對於全球金融體系帶來了巨大的衝擊，也讓「區塊鏈」的概念，正式誕生於世人眼前。經過十餘年的發展，區塊鏈應用從原始的加密貨幣領域，擴展到其他領域，如供應鏈、證書證明、電子投票等。而區塊鏈除在民間應用上大放異彩外，國防實務運用上亦有部分國家已開始進行相關研究。如軍用補給品供應鏈、作戰無人機管理、軍事文件證明資料保存等。由於國防軍事上產製的表單、訊息、文件等資料，多半涉及軍事行動與機敏性，甚至可能有個人隱私資料（如身分證字號等），在選擇區塊鏈的種類時，更要慎加考量與評估。

我國人事證明文件種類繁多，舉凡獎懲令、任官令、退伍令均屬其一環。相關法規律定，國軍軍（士）官於初任、晉任官等時，應依法給予任官令以茲證明，其樣式、署名長官均有特別規定。任官令除可輔助人事單位辦理俸級登載錯誤更正，計算其正確現役年資、俸級數據以外，於退伍後應部分公職、學業考試尚有加分優待外，另再任公職時亦可充作「比（提）敘」公職俸級時的證明文件，提升起始薪資，效益極其龐大。惟現行任官令仍以紙本型式發給受領人自行存管，容易因自然與人為因素而導致破損或遺失，加上前述業務仍須以繳驗紙本資料，尚未有一整合平台讓各方驗證機關得以直接查驗申請人相關任官證明資料，造成當事人需奔波往返各地申領，浪費寶貴時間與金錢，同時對政府施政印象打上不便民的負面觀感。而區塊鏈的特性，正能有效解決上開所述之問題。因此，如何利用區塊鏈的特性，構建一套能夠整合發證、保存、驗證、查詢的數位任官令平台，為本研究之動機。

本研究將以國軍軍官士官任官令為範例，探討運用區塊鏈導入國防人事文件之可行性研究，其餘人事文件部分，後續可參考本研究之架構，進行套用與結合。本研究探討將容易遺失的紙本任官令，轉化成為「永久保存」、「快速驗證」的「數位化任官令」，除

可提供當事人查詢，及作為任官令換（補）發、軍職資料查註、再任公職辦理比（提）敘時的重要、快速取得之輔助依據外，針對發證、受領、驗證等不同用戶執行作業時，以數位簽章方式實施驗證，防止非授權節點參與及無效交易影響系統，並結合智慧合約設計完整的發、驗證流程，不同用戶即給予不同權限的資訊查詢功能。透過強化區塊鏈技術與改進，使系統更加自動化、資訊化與更加安全可信，有效解決現行紙本任官令管理、換（補）發等問題，提升便民效益。

二、區塊鏈基礎知識暨相關研究領域應用

針對區塊鏈技術相關知識進行說明，分段詳述如下：

2.1 區塊鏈概述

本節將介紹區塊鏈定義、特性、類型，並針對相關內容進行細部說明與區塊鏈類型差異進行分析。

2.1.1 區塊鏈定義

區塊鏈，可被視為新的「記帳方式」(林佳賢，2018)。起源於由中本聰（Nakamoto Satoshi）於 2008 年提出之論文。文中提及之電子貨幣即「攜帶加密作用」的「比特幣」，而比特幣的源頭核心技術，即為「區塊鏈」。區塊鏈也可說是一種分散式帳本技術（Distributed Ledger Technology, DLT），由密碼學、數學、演算法、經濟模型，以及共識機制結合而成的（Lin and Liao, 2017），提供使用者一套具有「安全」、「穩定」、「可被稽核」且「具有高效率」的紀錄與資訊交換機制（黃步添與蔡亮，2020）。每個區塊均含有前一個區塊的雜湊資料、時戳以及交易資料。

2.1.2 區塊鏈特性

從比特幣開始，區塊鏈均有下列特性：去中心化、共識機制、不可篡改、公開透明，而後續提出的區塊鏈亦遵循著這些特性。現就上開特性進行細部說明：

2.1.2.1 去中心化：

相對於「中心化」的觀念，區塊鏈因其為運用「點對點」技術的開放式系統，並沒有「集中化管理」的「中央伺服器」或「資料庫」，而是每個節點來共同實現系統的維護、資料運算與維持資訊傳遞的「真確性」、「不可否認性」，這消除了中介機構的干預並降低交易的成本。

2.1.2.2 資訊透明化：

所有存在區塊鏈上的資訊，除了交易方的私有訊息有透過各種方法加密之外，餘下的資訊均能在系統的公開平台查詢，且任何人都可以透過公開的介面查詢區塊鏈資料及開發相關之應用（如智慧合約等），因此整個區塊鏈系統資訊係屬於高度透明化。

2.1.2.3 共識機制：

區塊鏈最顯而易見與彰顯「民主」的特性，非「共識機制」莫屬。因區塊鏈節點分散各處且均為平行，沒有上下隸屬關係，此時必須設計一套制度，來維持運作與公正，以及在一定時限內對交易進行驗證與確認；而該筆交易若能得到其他多數節點認可，即視為全網節點達成共識。共識機制的提出，係為解決「去中心化」後，各節點之間的信任問題，因為每個節點互不相識，亦彼此之間互不信任，且並不知道對方是否故障或是

遭到惡意入侵。各類型的區塊鏈系統均有「共識機制」的演算法，常見的有「工作量證明（Proof-of-Work, PoW）」、「權益證明 （Proof-of-Stake, PoS，或稱「持有量證明」)」、「代理權益證明（Delegated Proof-of-Stake, DPoS，或稱「代理持有量證明」、「股份授權證明」)」、「權威證明(Proof-of-Authority, PoA)」、實用拜占庭容錯機制(Practical Byzantine Fault Tolerance, PBFT）等（匯商君，2021)。

2.1.2.4 不可篡改：

區塊鏈另一個顯而易見的特性即「不可篡改」,其核心在於它的加密方法採取「密碼學」的「雜湊函數（Hash)」。該函數具「單向不可逆」特性，即運算完畢後無法反向推導，因此存於鏈上的資料是無法被更改，以及永久被保存於鏈上的。意圖要單方面更改節點生成的資料並被承認，幾近於「不可能達成」,除非有辦法控制鏈上 51%的節點。

2.1.3 區塊鏈類型：

區塊鏈可依照「去中心化」、「參與者」、「節點身分」、「編寫或閱覽權限」等程度差異，劃分為三種類型（蘇品長與蘇泰昌，2021)：

2.1.3.1 公有鏈：

向全世界完全公開，所有使用者均可在鏈上執行瀏覽其規則與機制，及發送、接收與交易認證。其特點為所有交易過程均為透明、去中心化程度最高，但交易速度相對較慢。

2.1.3.2 私有鏈：

不開放給一般人使用，只有獲得預先授權才能成為節點，進行發送、接收與交易認證。其特點為交易速度最快、隱私保障程度最高，但去中心化程度最低、較容易受到駭客攻擊。

2.1.3.3 聯盟鏈：

本質上與私有鏈接近，去中心化程度介於公有鏈與私有鏈之間，對特定的組織團體開放。參與區塊鏈的節點是事先決定好的，節點間可能有很好的網路連接、結算或清算等 「企業對企業（Business to Business, B2B)」架構，其發送、接收、讀寫、記帳等權利，均由管理組織決定，適用於機構間的交易行為。三種區塊鏈類型之差異表如表 1 所示。

表 1　區塊鏈類型差異表

類型	去中心化程度	參與者	節點身分	安全性	認證速度	規格變更	成本	權限(編寫或閱覽)
公有鏈	高	任何人	匿名	低	慢	難	高	完全開放
私有鏈	低	單一組織	可識別	高	快	易	低	須經授權
聯盟鏈	中	多個機構	可識別	中	中	易	高	須經授權

資料來源：參考自蘇品長與蘇泰昌（2021）

2.2 區塊鏈發展歷程

區塊鏈自比特幣問世以來，打破原有金融與科技「中心化」局面，形成最早期的「區塊鏈 1.0」。然而，原有的區塊鏈技術，限制了其應用與發展，一開始僅侷限於加密貨

幣領域、專門電腦科學和密碼學社群討論（Sillaber and Treiblmaier, 2021）。直至「智慧合約（Smart Contracts）」、「智慧資產（Smart Assets）」、「以太坊（Ethereum）」、「分散式應用程式（Distributed App, DApp）」等機制的問世，使得區塊鏈技術從「加密貨幣領域（幣圈）」的「區塊鏈 1.0」，跳脫至加密貨幣與其他領域結合的「區塊鏈 2.0」。而近期區塊鏈更是與其他技術集合，如人工智慧（Artificial Intelligence, AI）、物聯網（Internet of Things, IoT）等，形成「區塊鏈 3.0」（學界亦有稱之為「區塊鏈 2.5」，因「完全第三方公證人 DApp 技術」尚未成熟）。由於區塊鏈特性，可將蒐集到的資料經過整理、分析後進行上鏈，這使得資料得以保持透明、公開，且永遠不消失與被篡改，對於某些行業或工作亦有莫大幫助，如司法機關、農林漁牧業界、藥品供應鏈事業、非同質化代幣（Non-Fungible Token, NFT）市場等。區塊鏈發展簡史，如圖 1 所示。

圖 1　區塊鏈發展歷程簡圖

2.3 區塊鏈其他相關技術介紹

如前節所述，由於「比特幣區塊鏈」特性只可進行記帳，導致其運用於僅限加密貨幣領域，無法真正使用其技術進行其他領域的應用。而以太坊與智慧合約的問世，改變了此一問題，使區塊鏈不但可以記帳，還能記錄與執行程式指令碼，等於將程式寫在區塊鏈上，實現加密貨幣外的應用目的。以下為以太坊與其相關技術介紹：

2.3.1 以太坊

以太坊最早現於由俄裔加拿大籍程式設計師維塔利克・布特林（Vitalik Buterin）於 2013 年所提出的「以太坊白皮書（Ethereum White Paper）」，前者後於 2014 年與英國籍科學家加文・伍德（Gavin Wood）等人共同創立「以太坊」。

以太坊是一個基於區塊鏈分散式帳本技術的開放源碼平台，其與比特幣相同，將區塊鏈技術作為其運作的底層紀錄，是當前被廣泛利用之基於區塊鏈的開放源碼智慧合約應用平台，通過提供圖靈完備的編程語言，使用者可以便利的在鏈上構築去中心化應用。

2.3.2 智慧合約

智慧合約的概念，於 1994 年由美國電腦科學家暨法學家 Nick Szabo 提出，以一套數位型式定義的認可，包含合約參與者可在合約上執行這些認可的協議。同時，將相關協議用程式碼編纂呈現，交由電腦運作，經過交易會自動執行合約內所預設的定義與規

則。與傳統簽約方法相較，智慧合約更具安全性，因此可降低與合約相關的交易成本。另所有智慧合約均為公開資料，任何人都能查閱。首個將「智慧合約」納入大量應用的區塊鏈的平台為「以太坊」。

2.3.3 星際檔案系統

星際檔案系統（Inter-Planetary File System, IPFS），是一種「點對點」的分散式檔案儲存與共享系統。其旨在建立永久且分散式儲存和共用檔案的網路傳輸協議，取代現行運作的「超文字傳輸協定（HyperText Transfer Protocol, HTTP）」。

2014 年，IPFS 利用比特幣區塊鏈技術和網路基礎設施的優勢來儲存不可更改的資料，移除網路上的重複檔案，以及取得儲存節點的位址資訊，資料是以「檔案內容」作為其獨一無二的位址儲存，在其全球網路相連的裝置當中，每上傳一個檔案到 IPFS 網路上，系統將會為檔案分配一個永久不變的地址（一個與內容關聯的唯一加密雜湊值），IPFS 會將這個地址寫在不可篡改的區塊鏈主鏈上，解決了現行網路上存在許多重複性檔案的問題（蘇品長與潘詩婷，2021）。

IPFS 整合了 P2P、BitTorrent、GIT 等技術，具有可靠、容錯高、擴展性佳、快速等特點，其主要大部分資料都是以默克爾有向無環圖（MerkleDag）結構存在，使達到內容定址、防篡改及去重複等功能，用以解決將所有資料都存在區塊鏈上，導致主鏈區塊空間浪費及效能降低等問題，同時亦可達成檔案分散儲存及共享的功用（潘詩婷，2022）。

2.3.4 超級帳本

超級帳本，英文全名為「Hyperledger」，是一個旨在推動區塊鏈能夠跨業界應用「開放源碼專案」，以及改進原本僅能適用比特幣、以太坊等加密貨幣應用的主流區塊鏈技術，最早於 2015 年 12 月由 Linux 領銜發起，成員囊括了製造、金融、科技、物聯網、物流、供應鏈的大型國際企業。Hyperledger 推出至今已有多達 9 個以上正式專案在使用中，框架與專案工具架構如圖 2 所示，其中以 Burrow、Fabric、Indy、Iroha、Sawtooth 較廣為知曉與應用（洪嘉隆，2018）。

主流區塊鏈技術，因其「無需許可（Permissionless）」、「排序-執行模型（Order-Execute Model）」及「主動複製（Active Replication）」等特性，以致有「缺乏效率、隱私」的情形產生，在企業的應用上較不利。而企業網路通常為「半開放至封閉」的架構，除了參與者固定、採取實名認證之外，還帶有權限控管，形成天生的「許可制」環境。而一個採用「許可制」的網路具有比較寬鬆的信任模型。換句話說，參與者不作惡的機率是比較大的，這帶給了共識機制模型更大的設計彈性。基於上述的背景，超級帳本被設計出一種「執行-排序-驗證」模型（Execute-Order-Validate Model），流程敘述如下：

I. 交易會交由一部分預先指定的節點各自「執行」，執行結果一致就可形成共識，未形成共識的交易會被捨棄。
II. 接著來自不同節點、已形成共識的交易會經由一個特定服務進行「排序」並打包至區塊中。
III. 最後，這個特定服務再將區塊傳播給所有節點，收到區塊的節點僅需對交易進行少量「驗證」，若驗證結果無誤便可以更新自身狀態。

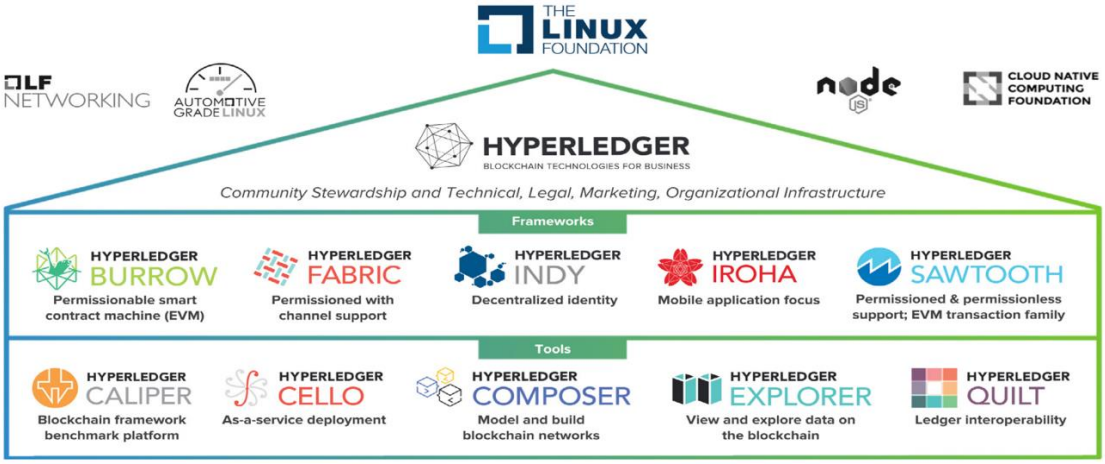

圖 2　超級帳本框架與專案工具架構簡圖

資料來源：參考自洪嘉隆（2018）

2.4 區塊鏈於學歷（專業技能）與證明文件領域相關應用

當吾人有任何疑難雜症時，都會尋求解方來處理。此時，具有該問題方面知識的權威人士就會被視為專家，可以替人來處理與解決問題（葉羅堯，2017）。然而，隨著時代的進步，人們為追求「一眼便知是否專業」，此時專家就需要拿出更有公信力的方式來證明自己的專長或技能，因此，證書與證明文件的需求油然而生（葉羅堯，2017）。而吾人在學習任何知識或技能時，必脫離不了各式各樣的考核，以檢視所學是否融會貫通或熟練專精，如能通過考核，亦有相對的證明文件發給，以昭公信與告訴其他人自己已具備文件上所載之知識或技能。

然而，現行的學歷或專業技能證明文件多數仍以紙本樣式發給，雖有各種防偽措施，如傳統的「證書號碼」、「鋼印」、「關防（印信）」到現代的「防偽標籤」、「特殊油墨印刷」、「管制用紙」等，在網際網路發達下，取得上開技術破解方式並非難事，加上紙本證明文件驗證不易，有心人士仍可藉此漏洞矇混過關。以學校發放畢業證書流程為例，教務處首先依畢業生名冊進行編碼，印製紙本證明與逐張黏貼相片後，鈐蓋鋼印與關防（印信）並裝入證書夾，於畢業典禮上由校長頒發給畢業生，上述過程需要耗費大量的時間、金錢與人力（葉羅堯，2017），但對於畢業生來說，卻是屬於一種榮耀的表現，彰顯學術研究、課業上努力的成果。但在前述發證過程中，有部分人士為一己私利，從中協助不法份子製造假學歷的案件出現（葉羅堯，2017）。有鑑於此，如何運用科技來達到有效防偽與檢驗證書的真實性與持有人之間的關係，便成了一個許多專家學者研究與實驗的目標。

而區塊鏈技術「不可篡改」、「公開透明」的特性，正好能對前述問題進行有效的處理。現行國內外已有學術機關採行運用區塊鏈技術來頒發學歷證明文件的案例，如美國麻省理工學院運用區塊鏈技術開發的「Blockcerts」（邱珮嘉，2019）、我國臺中市政府的「具 QR Code 驗證之區塊鏈證書檢測平台」（葉羅堯，2017），國立清華大學「區塊鏈畢業證書」（清華大學秘書處，2021）以及法務部「律師證書區塊鏈驗證系統」（Hsu, 2020）等。另亦有提出區塊鏈於戶籍謄本申辦（曾郁翔，2022）、以達到雙重辨識真偽保險、

防杜矇騙與損害他人權益，以及提升建築履歷與電子執照檔案商業價值等領域的應用（方成楓，2021）。

然軍事證明資料（如人事派令、軍事技能專長簽證書表、各類補給品撥補憑單等）亦不例外，除了容易衍生造假的問題外，也可能產生保存與保全的問題。傳統上，因軍隊組織分官設職、分層授權，以及閱讀習慣與「蓋印驗證」等文化，紙本迄今仍在軍事證明資料中佔有一定比例，而要保存這些紙本，就需有大型的空間來儲存，且紙本型式的「檔案」存管亦需要保持一定的溫、濕度，否則容易產生泛黃、蟲蛀等自然損毀情形。依據我國相關法規律定，除永久保存的檔案外，其餘均有保存年限，期滿必須依規定執行銷毀（國防部，2016），常見銷毀作業方式有水銷與火銷。但無論是哪種方式，均需要耗用大量時間與精力來作業，且需要額外經費來添購相關設備，如碎紙機、火銷爐等。目前雖已實施公文電子化方式儲存，大幅減低紙本存管成本與節省儲存空間，然數位設備的維運與舊有紙本轉檔至儲存媒體的工作，對機關單位來說亦是一個新的挑戰。

而前述之區塊鏈技術特性，對於資料保存上提供了極佳的契機。由於資料寫入區塊鏈後，即會永久留存在該區塊上。對於惡意破壞者來說，除非有極大資源掌握鏈上 51% 的節點，否則將無法修改。以公有鏈如比特幣、以太坊等來說，現行網路與硬體技術而言，目前尚無人能做到修改已產生既定區塊的資料，這對某些個人、團體或組織想要保存相關紀錄而言，不失為一個極佳的良方。從求婚內容、私人訊息，到學校、政府事件紀實，上鏈保存的資料可謂五花八門、無奇不有。而這種資料保存方式，對於某些「有言論管制的國家、政體」，更是突破封鎖的一道密鑰。如 2018 年中國大陸北京大學發生的「申訴事件」（李忠謙，2018），當事人將其揭發之事件始末，以中、英文方式寫入以太坊區塊鏈上，任何人均可查詢與閱讀，校方或當局均無法消除與封禁，而該事件始末紀錄，迄今仍留存於區塊上（李忠謙，2018）。

由上開案例可知，區塊鏈在資料保存上，擁有極佳的優勢，只要電力與網路不斷，資料就能一直存在且永遠不會消失，既可省下大量印製紙張的金錢與紙本儲存空間，又能隨時進行資料的查驗。然而，目前區塊鏈技術雖能解決前述紙本證明文件「防偽」與「驗證」的問題，但對於「證書與持有人關係驗證」、「原始數位發證資料檔案保存」，以及軍事證明資料機敏性等問題，目前尚無一套完整與標準的作法，仍由產官學界持續研究與開發中。

三、國軍軍士官任官令導入區塊鏈研究

國軍軍士官任官令（以下簡稱任官令），為我國政府依據「陸海空軍軍官士官任官條例」與其施行細則等法規，授予因具備各級軍官、士官任官之學、經歷與條件，而經審查並核准獲得官階的軍人之證書。依據相關規定，任官業務範圍可分為初任、晉任、轉任、敘任、追晉（贈）、免（復）官、俸級晉支及降階改敘等（國防部，2022），本研究所提之任官令以「初任」、「晉任」為限。任官令於早期為 B5 紙張尺寸，現則修正為與一般人事命令相同，為 A4 紙張尺寸。同時依類型可區分為軍官任官令與士官任官令兩大類，作業權責劃分、最高層級長官署名亦有不同，軍官任官令為「總統署名」、士官任官令為「國防部部長署名」。惟相同處在於任官令上均會有「任官令字號」、「區分」、「姓

名」、「兵籍號碼」、「軍種」、「官科」、「晉任官階」、「原任官階」、「生效日期」、「服務單位」、「備考」等欄位，詳實記載當事人的任官紀錄資料。

3.1 發給流程暨應用

依據前揭所提規定，國防部或司令部對於各層級單位呈報候任人員進行審查、核覆（閱）後，除依權責發布相關任官命令公文或呈報 總統核定後再行發布外，尚需另行製頒紙本型式任官令，發給相關當事人收執，以昭當事人獲得新任官階殊榮與布達他人週知，相關發給作業流程示意詳如圖 3 所示。

圖 3 任官令發給作業流程示意圖

任官令之應用，除可證明當事人所獲之官階，在早期國軍兵籍資料尚未電子化前，為人事作業上用以計算官階停年、薪俸俸級正確與否的一項重要佐證資料。雖現代均已完成兵籍資料電子化、資訊化，部分極少數人員仍有發生因單位人事承辦人員晉任換敘計算錯誤，導致俸級與同條件晉任之人員產生不一致現象，造成權益損失問題，此時即需要人工資料進行輔助認定，修正錯誤。而在退役後，任官令亦有其特別用處，即為後備軍人轉任公務人員「考試優待」、「任用比（提）敘」。

依照我國「後備軍人轉任公職考試比敘條例」等相關規定，依法退伍之軍、士官參加公務人員考試時，如有相關任官證明文件，在應考資格、成績加分、體格檢驗及應繳規費等方面，可酌予優待。而考取公務人員各官等任用資格後，可優先任用及依照比敘該官等內相當職等，亦即在職位核定上，將高於其他於同一時間任公職的同梯考生。

另我國「公務人員俸給法」、「公務人員曾任公務年資採計提敘俸級認定辦法」等相關法規亦提及，公務人員如有「曾任依法令任官有案之軍職年資」，並符合「與現任職務職等相當」、「性質相近且服務成績考核列乙等或七十分或相當乙等以上，繳有證明文件」之情形，得按年核計加級提敘至其所銓敘審定職等之本俸最高級；如尚有積餘年資，且其年終（度）考績（成、核）合於或比照合於「公務人員考績法」晉敘俸級之規定，得按年核計加級，再提敘至其所銓敘審定職等之年功俸最高級。換句話說，在薪俸等級上將遠亦高於其他於同一時間任公職的同梯考生。

由於律法的明文規定，政府對於後備軍人再任公職的權益保障上有一定的水準。然而，前提是必須要繳交前述的「依法令任官有案的證明文件」，而蒐整這些證明文件，對於部分當事人來說容易遇到麻煩與阻礙，如遺失、損毀，而要申請補發，又必須向國防部或原屬司令部提出，公文往返亦耗費當事人時間與精力，如有一個能資料登錄後即不可篡改、可公開查詢有無此任官紀錄、透過需許驗證即可以特殊方法讀取此紀錄的詳細資訊的系統，對於當事人、任官令發證方（國防部等），以及第三驗證方（其他公務機關或事業單位）來說，將是一大福音。

3.2 導入後流程與業務說明

上節說明任官令作業流程與應用，可得知任官令與國軍其他人事證明文件相同（如勳獎章證書等），仍以紙本型式發給當事人收執，而任官令在收藏上的重要性不比勳獎

章證書，可能會與其他紙本人事證明文件混儲，僅有部分人士會分門別類，存放於不同的檔案卷夾，但仍脫離不了紙本文件的普遍性問題：自然或人為因素的遺失或損毀。

本節將說明以區塊鏈技術導入任官令作業流程，並將資料加密、透過智慧合約上傳至鏈上進行保存之研究與探討。該作業流程除可確保作業中雙方身分得被安全驗證，縮短作業執行時間，並運用區塊鏈底層技術及智慧合約執行交易流程，後再納入數位簽章技術保證數位任官令交付流程可驗證性。另針對不同參與者（發證方、受領人）制定不同的資訊查詢功能，令參與者得完整查詢權限內可得的數位任官令相關資料。另對於驗證方則提供「臨時任官令檔」驗證方式，可驗證原始任官令檔與受領人持有關係。另當任官令驗證出現問題時，可快速掌握狀況與通報主管機關進行處置。以下將說明本研究所提出之數位任官令作業架構及其運作流程。

本文之研究運作架構如圖 4 所示，線條顏色分別表示各階段流程（紅色：身分註冊、藍色：智慧合約部署、黃色與綠色：任官令資料製作與上鏈、棕色：任官令資料驗證、紫色：查詢任官令狀態及部分公開資訊等）。

作業流程部分，依照順序分別為：身分註冊、智慧合約部署、任官令資料製作與上鏈、任官令資料驗證、查詢任官令狀態及部分公開資訊等 5 大階段。

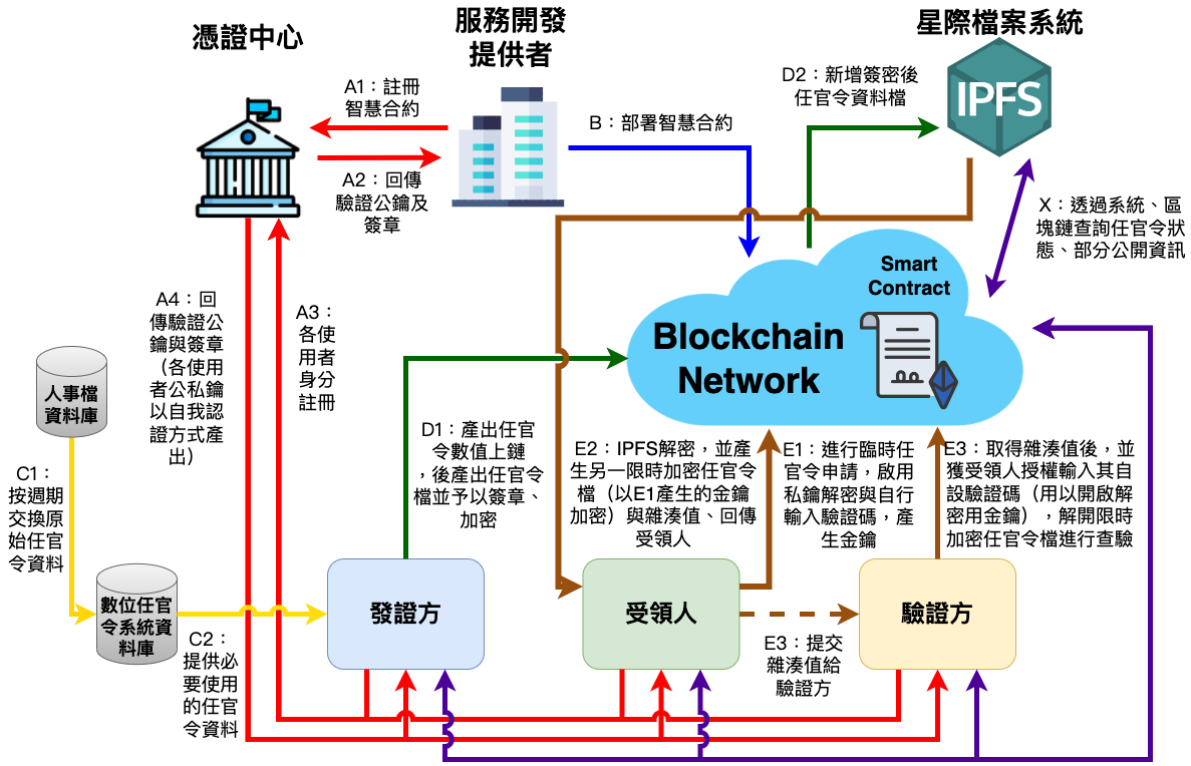

圖 4　區塊鏈技術導入任官令作業流程圖

此研究設計數位任官令作業流程參與者有「發證方」、「受領人」、「驗證方」等，參數說明表如表 2。

詳細作業流程暨各階段運作虛擬碼分述如下：

I. 身分註冊：首先所有參與者（發證方、受領人、驗證暨服務受理方）分別向憑證中心提交位址與簽名檔，進行註冊作業，以便取得驗證公鑰及憑證簽章，後各自

表 2　數位任官令作業流程參數符號說明表

項次	參數代碼	說明
1	CA、SD、IS、RC、VD、BN	憑證中心、服務開發提供者、發證方、受領人、驗證方、區塊鏈網路
2	SC	服務開發提供者編製的智慧合約
3	ID_i	參與者身分 ID，其中 i∈ *CA*、*SD*、*IS*、*RC*、*VD*、*SC*
4	S_i	參與者簽名檔，其中 i∈ *CA*、*SD*、*IS*、*RC*、*VD*、*SC*
5	$voSig_i$	參與者簽章，其中 i∈ *CA*、*SD*、*IS*、*RC*、*VD*、*SC*
6	$addr_i$	參與者區塊鏈位址，其中 i∈ *CA*、*SD*、*IS*、*RC*、*VD*、*SC*
7	$VPBK_i$	參與者驗證公鑰，其中 i∈ *CA*、*SD*、*IS*、*RC*、*VD*、*SC*
8	PBK_i、pvk_i	參與者獲取的公鑰和私鑰，其中 i∈ *CA*、*SD*、*IS*、*RC*、*VD*、*SC*
9	psw_{tempcc}	臨時任官令自設驗證碼
10	K_{tempcc}	臨時任官令驗證用金鑰
11	$data_{cc}$	任官令原始資料
12	$searchData_{cc}$	查詢所需資料（如身分證字號、姓名、任官令種類等）
13	$code_{cc}$、$code_{nullcc}$	任官令數值、原任官令「註銷資訊」
14	$file_{cc}$、$enFile_{cc}$	原始任官令檔、簽密後任官令檔
15	$tempFile_{cc}$、$enTempFile_{cc}$	臨時任官令檔、簽密後臨時任官令檔
16	$vdHash_{cc}$	任官令驗證用雜湊值
17	t_{stamp}	時間戳記
18	reg（）	使用者向憑證中心註冊的過程
19	Calculate（）	計算各自公私鑰過程
20	createCode（）	產出任官令數值過程
21	createBlock（）	送出任官令數值上鏈過程
22	createFile（）	製作任官令檔過程
23	createNullifiedCode（）	產出任官令「註銷資訊」數值過程
24	createNullifiedBlock（）	送出原任官令「註銷資訊」數值上鏈過程
25	createIPFS（）	新增任官令檔至 IPFS 過程
26	createTempKey（）	製作驗證用臨時任官令金鑰過程
27	createTempFile（）	製作驗證用臨時任官令檔過程
28	encrTempFile（）	加密、簽章臨時任官令檔過程
29	decrTempFile（）	驗證、解密臨時任官令檔過程
30	msg（）	智慧合約回傳事件是否成功執行等相關訊息
31	search（）	查詢任官令資料過程
32	dnld（）	下載與解密任官令過程
33	DB_{mip}、DB_{dcs}	人事檔資料庫、數位任官令系統資料庫

執行公私鑰（PBK_i, pvk_i）計算，確保後續各階段流程中，流程參與者均為合法授權的使用者，得獨立進行身分上的自我認證。

A1：服務開發提供者 SD 向憑證中心 CA 提交智慧合約 SC 的簽名檔 *S*、位址 *addr* 進行註冊。

A1′：SD→CA: Reg（ID_{SC}, S_{SC}, $addr_{SC}$）

A2：憑證中心 CA 回傳智慧合約 SC 的驗證公鑰 *VPBK* 與簽章 *voSig* 給服務開發提供 SD，並計算出智慧合約 SC 之公鑰 *PBK*。

A2′：CA→SD（SC）:（$VPBK_{SC}$, $voSig_{SC}$）、SD:Calculate（SC（$VPBK_{SC}$））→（PBK_{SC}）

A3：各參與者（發證方 IS、受領人 RC、驗證方 VD）向憑證中心 CA 提交簽名檔 *S*、位址 *addr*，進行註冊。

A3′：IS, RC, VD→CA: reg（S_i, $addr_i$）, i∈*IS*、*RC*、*VD*

A4：憑證中心 CA 回傳驗證公鑰 *VPBK* 與簽章 *voSig*，並由各使用者自行計算出公、私鑰。

A4′：CA→IS, RC, VD:（$VPBK_i$, $voSig_i$）、IS, RC, VD: Calculate（$VPBK_i$）→（PBK_i,pvk_i）, i∈IS、RC、VD

II. 智慧合約部署：服務開發提供者將製作完成的智慧合約部署至區塊鏈上，接著依照數位任官令作業流程由各參與者執行。

B：服務開發提供者 SD 將智慧合約 SC 部署至區塊鏈網路 BN 上。

B′：SD→BN:（SC）

III. 任官令資料製作與上鏈：發證方負責任官令資料處理與數位任官令檔製作，並透過合約將原始任官令資料產出任官令數值，並以發證方私鑰簽密後，新增至區塊鏈（任官令數值）及 IPFS（任官令檔）上。

C1：人事檔資料庫 DB_{mip} 定期轉錄任官令原始資料 $data_{cc}$ 至數位任官令系統資料庫 DB_{dcs}。

C1′：DB_{mip}→DB_{dcs}:（$data_{cc}$）

C2：發證方 IS 登錄系統，取用任官令原始資料 $Data_{cc}$。

C2′：DB_{dcs}:（$data_{cc}$）→IS

D1：發證方 IS 透過系統，將任官令原始資料 $data_{cc}$ 轉換成任官令數值 $code_{cc}$、原始任官令檔 $file_{cc}$，並以自身私鑰 pvk_{IS} 將原始任官令檔 $file_{cc}$ 簽章、受領人公鑰 PBK_{RC} 加密為簽密後任官令檔 $enFile_{cc}$，觸發智慧合約 SC 將任官令數值 $code_{cc}$、時間戳記 t_{stamp} 傳送至區塊鏈網路 BN。

D1′：IS: createCode（$data_{cc}$）→IS:($code_{cc}$, $file_{cc}$）、IS:（$file_{cc}$, pvk_{IS}, PBK_{RC}）→（$enFile_{cc}$）、IS: createBlock($code_{cc}$, t_{stamp}）（via SC）→BN

D2：發證方 IS 將簽密後的簽密後任官令檔 $enFile_{cc}$ 傳送至星際檔案系統 IPFS。

D2′：IS: createIPFS（$enFile_{cc}$, t_{stamp}）→IPFS

IV. 任官令資料驗證：驗證方則可透過「臨時任官令檔驗證」功能，由受領人主動提交申請，並輸入自設驗證碼產生金鑰，後由 IPFS 解密原始任官令檔並產生一個新的「限時任官令檔」並用前述之金鑰加密，併同「雜湊值」回傳給受領人，驗證

方取得受領人授權後，將其「雜湊值」與輸入「自設驗證碼」開啟金鑰解密，即可解開「限時加密任官令檔」進行驗證。

E1：受領人 RC 發起發起「驗證用臨時證書」申請，並送出自行輸入的臨時任官令自設驗證碼 psw_{tempcc}，啟用受領人私鑰 pvk_{RC} 與製作臨時任官令驗證用金鑰 K_{tempcc}。

E1′：RC: createTempKey（psw_{tempcc}, pvk_{RC}）→RC:（K_{tempcc}）

E2：IPFS 解密 $enFile_{cc}$，同時產生有存在時間限制的臨時任官令檔 $tempFile_{cc}$ 後再行加密，並利用 K_{tempcc} 產生任官令驗證用雜湊值 $vdHash_{cc}$ 並回傳給 RC。

E2′：IPFS: createTempFile（K_{tempcc}, pvk_{RC}, $enFile_{cc}$）→ IPFS:（$tempFile_{cc}$）、IPFS:encrTempFile（$tempFile_{cc}$）→IPFS:（$enTempFile_{cc}$）、RC:（$vdHash_{cc}$）

E3：驗證方 VD 自受領人 RC 處取得任官令驗證用雜湊值 $vdHash_{cc}$，並由受領人 RC 親自或授權驗證方 VD 輸入 K_{tempcc}，下載與解開 $enTempFile_{cc}$ 進行查驗。

E3′：RC:（$vdHash_{cc}$）→VD、VD:decrTempFile（$vdHash_{cc}$, K_{tempcc}, $enTempFile_{cc}$）→VD:（$tempFile_{cc}$）

V. 查詢任官令狀態及部分公開資訊：另其他參與者可於系統查詢介面輸入相關資訊，如身分證字號、任官令字號等進行比對，並回傳驗證結果（任官令狀態、部分公開資訊等）。另受領人可透過系統下載與解密任官令檔進行閱覽。

X：發證方 IS、受領人 RC、驗證方 VD 透過系統，輸入「查詢所需資料」$searchData_{cc}$，透過智慧合約 SC 啟用 search（），查詢鏈上有無相符資訊，再由系統回傳結果。如有，受領人 RC 可進行下載 $enFile_{cc}$，並以受領人私鑰 pvk_{RC} 解密與發證方公鑰 PBK_{IS} 驗證，一致即可解開閱覽。

X′：IS,RC,VD:Search（$searchData_{cc}$）（via SC）→BN:msg（success or fail）、RC:（ pvk_{RC},PBK_{IS}）→IPFS:dnld（$enFile_{cc}$）→RC:（$file_{cc}$）

四、安全性分析

本章將針對上節所述基於區塊鏈技術加上智慧合約設計之任官令作業流程，依據國際標準組織（International Standard Organization, ISO）所頒定之 ISO/IEC: 27001: 2018 文件「資訊安全管理需求」、區塊鏈技術特性所可能面臨的安全挑戰（Stephen and Alex, 2018），並與現行國軍人事系統之任官令作業流程比對，進行安全性分析，計有「機密性」、「隱匿性」、「不可否認性」、「不可篡改性」、「系統可擴展性」、「持有關係驗證性」、「原始檔上鏈儲存性」等 7 項，結果如表 3 所示，分述如下：

4.1 機密性

機密性是指文件、資料不得被未經授權之個人、實體或程序所取得或揭露的特性，且文件在傳遞過程中，內容都是被加密的，不被傳送及接收雙方以外的人獲知內容之特性。在本研究中，模擬可能遇到惡意使用者意圖攔截任官令檔並窺視其中內容之情境，而解決方法為發證方將任官令檔透過受領人的公鑰加密與自己的私鑰進行簽章，如無相對應的私鑰與公鑰而想要解開加密檔案，則須面臨暴力破解非對稱式金鑰的問題，故本

研究機制在實際安全上可確保任官令檔機密性。

4.2 隱匿性

「隱匿性」係於區塊鏈中非執行當筆交易的參與者，僅能證明此筆交易存在，無法獲知其交易內容，本研究以區塊鏈技術為基礎，參與者透過智慧合約執行交易程序，區塊與區塊之間是以雜湊值相互鏈結。另因雜湊函數為單向與不可逆，且傳送方將交易明文資訊以接收方公鑰加密，接收方取得密文後以私鑰解密還原為明文，因此除了接收方可以知道交易訊息，其他鏈上的參與者僅可知該筆交易確實存在，以確保鏈上資料的隱匿性。

4.3 不可否認性

「不可否認性」係為每一筆數位任官令資料與檔案的製作、傳送與頒授等「資料製作程序」，發證方不能否認其「行為」。在本研究中，模擬可能遇到某機關因承辦人疏失，登錄任官令數據錯誤導致後續俸級換算脫漏情事，引起受領人怨懟與申訴，某機關推諉不願處理之情境，而解決方法為在「發證階段」時，發證方於每筆任官令資料與檔案上鏈前均完成簽章，故受領人能以「驗證」方式確認其簽章的有效性，發證方無法否認其簽章，達到不可否認性。

4.4 不可篡改性

「不可篡改性」係指所有的紀錄及資料均不可被任何人篡改。在本研究中，模擬可能遇到惡意使用者意圖篡改鏈上紀錄，並將篡改後的資料強行上鏈之情境。本研究基於區塊鏈技術與智慧合約建構任官令作業流程，鏈上所有紀錄均採行區塊鏈技術之特性，以雜湊函數將每一區塊串接鏈結，因此若有任何參與者篡改內容，原有的雜湊值也會改變，進而影響整個鏈且被發現與棄用重算，且所有使用者執行作業前均需交由智慧合約驗證是否經過合法授權，否則將無法進行，故具有不可篡改性。

4.5 系統可擴展性

區塊鏈技術雖有資料透明公開，且記錄不可變之特性，然現行法規律定，所有的人事紀錄均必須留存用以驗證，在區塊大小有限的情況下，將會產生區塊容量變小導致交易被延遲或收取更高的交易手續費，因此本研究提出之方案運用 IPFS 分散式檔案儲存系統，將發證方發行之原始數位任官令檔完整記錄在 IPFS，於鏈上僅留存任官令數值等紀錄，可減少大量資料留存在鏈上的造成系統效能降低，亦可達到任官令紀錄可被驗證之優點，增加了系統的可擴展性。

4.6 持有關係驗證性

部分區塊鏈數位證書系統對於「證書與持有人關係」的驗證方式尚無統一作法，造成數位區塊鏈證書持有人不易，衍生「冒用證書」的問題。在本研究中，模擬可能遇到惡意使用者意圖冒用非屬於當事人之任官令進行不法行為之情境，而解決方法為採用「臨時任官令檔驗證」功能，由受領人主動提交申請，輸入自設驗證碼產生金鑰，後由 IPFS 解密原始任官令檔並產生一個新的「限時任官令檔」並用前述之金鑰加密，併同「雜湊值」回傳給受領人，驗證方取得受領人授權後，將其「雜湊值」與輸入「自設驗證碼」開啟金鑰解密，即可解開「限時加密任官令檔」進行驗證，可有效驗證「證書與持有人關係」。

4.7 原始檔上鏈儲存性

現行區塊鏈數位證書系統因區塊所能儲存空間仍有一定限制，加上其「公開透明」特性，多半不會將原始明文資料寫入區塊，而是一串經過雜湊函數或其他演算法處理後的數值，雖然可達到保密效果，但亦只能證明曾有寫入過這筆交易資訊，如需加驗原始證書檔案，就會衍生「無實體檔案可驗證」之問題。本研究提出將發證方產出之原始數位任官令檔案經過簽密後，上傳至「IPFS」儲存，受領人如需下載閱覽必須輸入私鑰方能開啟；驗證方則可透過前開項次「臨時任官令檔驗證」功能，進行驗證原始數位任官令資料檔，可有效解決前述「無實體檔案可驗證」之問題。

表 3　本研究與國軍人事系統之安全性分析比較表

比較項目	國軍人事系統（任官令作業）	本研究
機密性	△	O
隱匿性	△	O
不可否認性	△	O
不可篡改性	△	O
系統可擴展性	△	O
持有關係驗證性	X	O
原始檔上鏈儲存性	X	O

註：O 表完全符合、△表部分符合、X 表不符合、-表無相關

本研究設計之區塊鏈技術導入任官令作業流程之研究，在安全上的挑戰與資訊安全要求規定之範圍內，可滿足「機密性」、「隱匿性」、「不可否認性」、「不可篡改性」、「系統可擴展性」、「持有關係驗證性」、「原始檔上鏈儲存性」等特性，同時與現行國軍人事系統（任官令作業）機制進行比較。現行國軍人事系統（任官令作業）機制雖於封閉式內網進行，然僅使用帳號、密碼等進行使用者管控，傳輸資料時亦以明文逕行，無透過加解密金鑰；資料來源無法有效驗證，且任何人均能更改、觀看，造成部分專業人士得以運用技術與工具進行相關資料的窺探、竊取，形成資安漏洞，如上開人員帶有進一步之惡意目的，更有造成國家安全風險疑慮（錢利忠，2020）。再來所有資料均集中儲存於國防部的本地端資料庫，資料量日益龐大造成維護成本增加，且現行驗證任官令仍須以紙本為主，造成當事人保存負擔，以及因遺失或毀損所衍生之申辦時間、精力與金錢浪費。本研究除運用區塊鏈特性，將紙本任官令轉為數位檔案，改善保存、管理與資料整合問題，另採用橢圓曲線簽密法與自我認證機制，可有效達到機密性等特性，強化任官令管理與作業機制之安全性，解決區塊鏈技術中之節點權限控管等問題。

五、結論、國防領域應用與未來研究方向

區塊鏈自誕生迄今，無論在民用或是軍用領域上，各方勢力或團隊無不投入大量的重金來進行研究，逐漸脫離其初始創造目的。利用其去中心化、不可篡改且資料永久保存等特性，以及與其他諸如人工智慧、物聯網等技術結合，讓區塊鏈在各領域上有了更深、更廣的應用。而在國防實務上，區塊鏈應用的研究也未曾缺席，除民間的各式證書（明）、履歷資料等文件、投票（投標）等領域可直接或經過適當的修正後變成軍事上應

用的方案外，另諸如無人機等軍事裝備也能運用區塊鏈進行註冊、運用智慧合約輸入指令，降低敵方篡改、破壞資料的可能性，保護我方裝備不為敵所摧毀或虜獲。

另在軍事證明資料保存上，由於區塊鏈之特性，對於紙本文件的保存空間與成本政策考量上，有了顛覆性的變革。除可直接減少紙本儲存空間、購置相關設備的成本外，資料也能永久存在區塊鏈上，不需擔心保存年限、銷毀、轉檔的問題，也能隨時進行查詢，惟在開發前仍需進行相關的機敏性、限閱性等機制進行評估、增設。

本研究設計之區塊鏈技術數位任官令作業機制，運用區塊鏈技術具有去中心化、不可篡改且資料永久保存等特性，將發證方等各參與者交易過程及資訊完整保留，紀錄永久保存、可追溯且不可更改，並且運用密碼學簽章技術及非對稱金鑰加解密方式，解決發證、受領、驗證等流程上機密、隱匿性問題，並結合智慧合約設計完整的發、驗證流程，不同用戶即給予不同權限的資訊查詢功能；另採用 IPFS 分散式檔案儲存與共享系統方案，將完整的原始核發數位任官令檔保存，除可供使用者透過智慧合約隨時查詢外，亦可減輕鏈上區塊儲存空間，確保系統運作效能；本研究基於區塊鏈技術建構數位任官令作業機制除具持有關係驗證性與原始檔上鏈儲存性，在安全性上滿足機密、隱匿、不可否認、不可篡改等特點。透過強化區塊鏈技術與改進，使系統更加自動化、資訊化與更加安全可信，有效解決現行任官令換（補）發、軍職年資查註輔助驗證、查詢等問題，提升便民效益。

本研究近程於可應用於國防人事領域，在人事勤務方面，可應用在「國軍軍官士官任官業務」上。在「任官令管理」方面，任官令保存主管機關可以利用該系統進行原始核發任官令檔保存，多一處「存放位置」且可永久保存。在「任官令查詢與取得」方面，受領人可透過系統進行任官令的查詢、亦可隨時下載任官令原始檔進行閱覽，毋需擔心因自然或人為因素導致紙本任官令損毀或遺失的問題。而在「任官令換（補）發作業」及「作為軍職資料查註與審核輔助驗證」上，則可多一道快速查驗當事人是否曾有「依法令任官有案」紀錄，加速後續相關申請作業，提升便民效益與國軍單位形象。

另本研究設計著重於任官令發證、原始令狀數位檔案保存與驗證等資訊作業流程與安全，解決紙本任官令容易遇到的相關問題。於未來研究與運用方向上，則可結合政府部門公開金鑰基礎建設（Government Public Key Infrastructure, GPKI）、國軍現有憑證卡（國軍智慧卡）、內政部戶政系統數位身分識別證（New eID），強化金鑰與身分認證的機制，並可提供其他政府機關進行更多的運用，如提供其他公家機關人事部門針對「再任公職辦理比（提）敘」時加速查驗的依據、典試單位可用以快速審查退伍軍官士官考生之條件，並判定是否給予特別待遇（如可加若干分數等），有利未來軍隊、政府部門及社會實務應用。

參考文獻

方成楓（2021）。*運用區塊鏈技術於建築履歷暨電子證照管理之可行性研究*。天主教輔仁大學資訊管理學系未出版碩士論文，臺灣，新北市。

李忠謙（2018 年 4 月 26 日）。*被寫進「區塊鏈」的北京大學醜聞：無視教授性侵、說謊迫害聲援學生*。取自 2023 年 5 月 29 日 https://www.storm.mg/article/429991?page=1

林佳賢（2018 年 7 月 3 日）。*不懂技術沒關係！圖解告訴你區塊鏈可以這樣用*。取自 2023 年 5 月 29 日 https://www.cw.com.tw/article/5090842

邱珮嘉（2019）。*以區塊鏈技術建構畢業證書系統之研究*。銘傳大學資訊管理學系碩士論文未出版碩士論文，臺灣，桃園市。

洪嘉隆（2018 年 10 月 17 日）。*Hyperledger 技術介绍與 Fabric、Sawtooth 對比*。取自 2023 年 5 月 29 日 https://ithelp.ithome.com.tw/articles/10202324

清華大學秘書處（2021 年 6 月 24 日）。*清華發出全國首張區塊鏈加密數位畢業證書*。取自 2023 年 5 月 29 日 https://www.nthu.edu.tw/hotNews/content/1028

曾郁翔（2022）。*適用於區塊鏈資料存儲機制於戶籍謄本之可行性研究*。天主教輔仁大學資訊管理學系未出版碩士論文，臺灣，新北市。

國防部（2022）。*陸海空軍軍官士官任官作業程序*。臺灣，臺北市：國防部。

國防部（2016）。*國軍文書檔案作業手冊*。臺灣，臺北市：國防部。

黃步添、蔡亮（2020）。*區塊鏈改變未來的倒數計時*，臺北市：清文華泉事業有限公司。

匯商君（2021 年 9 月 22 日）。*一文讀懂區塊鏈的共識機制 PoW,PoS,DPoS,PoA 有何不同*。取自 2023 年 5 月 29 日 https://www.toutw.com/crypto/powsa/

葉羅堯（2017 年 5 月 22 日）。*智慧校園區塊鏈應用*。取自 2023 年 5 月 29 日 https://da.taichung.gov.tw/media/207141/712816251671.pdf

潘詩婷（2022）。*以區塊鏈技術強化供應鏈產品履歷機制之研究*。國防大學管理學院資訊管理學系未出版碩士論文，臺灣，臺北市。

錢利忠（2020 年 5 月 27 日）。*駭客分黑白灰 3 類 軍方電軍 5 士官從「白帽」變「黑帽」*。取自 2023 年 5 月 29 日 https://news.ltn.com.tw/news/society/breakingnews/3178726

蘇品長、潘詩婷（2021）。強化區塊鏈技術建構供應鏈產品生產履歷系統。*國防大學管理學院 2021 第二十九屆國防管理學術暨實務研討會*，35-49，臺灣，臺北市。

蘇品長、蘇泰昌（2021）。基於區塊鏈技術設計且強化安全之多樣化電子投票機制。*國防大學管理學院 2021 第二十九屆國防管理學術暨實務研討會*，50-68，臺灣，臺北市。

Jenny, H.（2020 年 2 月 3 日）。*杜絕《無照律師》真實上演，法務部 2020 年元旦推出「律師證書查驗系統」的下一步是什麼？*。取自 2023 年 5 月 29 日 https://medium.com/kryptogo/杜絕《無照律師》真實上演，法務部 2020 年元旦推出「律師證書查驗系統」的下一步是什麼-16584f707a93

Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653-659.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved on October 24, 2022, from https://bitcoin.org/bitcoin.pdf

Sillaber, C., & Treiblmaier, H. (2021). The impact of blockchain on e-commerce: A framework for salient research topics. *Electronic Commerce Research and Applications*, *48*(101054), 1-14

Stephen, R., & Alex, A. (2018). A review on blockchain security. *Proceedings of the IOP Conference Series: Materials Science and Engineering*, *396*, 1-7