軍事管理

DOI:10.29683/AFOB.202202_222.0005

國軍人事作業自動化系統導入區塊鏈技術之研究

空軍少校 歐喜誠

提要

國軍人事作業自動化系統研發之目標係促使人事業務導入資訊化、自動化、標準化，在使用該系統的過程中可以發現一些問題，像資料庫操作繁瑣、資料庫不同步、異地備份需求及管理者的可靠性等等，美國知名顧問管理資詢公司麥肯錫曾在2017年提出「以區塊鏈技術，改善政府資料管理」的論點，指出政府機關各部門所掌握資訊的交流與個資保密的重要性，利用區塊鏈的相關特性來改善系統的缺陷，而在實作及導入前，評估其可行性尤其重要，因此本研究利用分析層級程序法(AHP)找出影響國軍人事作業自動化系統導入區塊鏈技術之關鍵成功因素。

區塊鏈技術於2008年10月由中本聰在發明比特幣的論文中提出，其使用到的技術包含了分散式帳本、點對點傳輸、非對稱式加密、雜湊函數、默克爾樹、時間戳記等，而這些技術讓區塊鏈具備了去中心化、資料竄改不易及可追溯性等特性，另外，對區塊鏈這種分散式帳本的技術而言，如何讓區塊鏈各個節點，在互不信任且沒有中央機構的情況下達成共識，這種共識機制是非常重要的，因此也衍生出多種共識機制，如工作證明、權益證明、權威證明等等，目前區塊鏈以類型而言可區分成公有鏈、私有鏈及聯盟鏈，以發展階段而言可區分為1.0–數位貨幣、2.0–數位經濟(智能合約)、3.0–數位社會，應用範圍越來越廣泛。

從區塊鏈的技術特性可歸納出「安全層面」、「資料紀錄內容」及「技術功能層面」等3個構面及10項準則來分析導入區塊鏈技術的影響因素，再分別針對管理、執行及技術等各階層人員進行評估，透過分析層級程序法綜合分析，發現安全性及其相關技術(雜湊函數)仍為國軍各階層最為重視的環節，其次為可靠性及來源真實性，因此，導入區塊鏈的關鍵成功因素在於其安全性、可靠性及來源真實性的相關技術，若技術發展成熟即可提升國軍人事作業自動化系統導入區塊鏈之可行性，並提升國軍人事作業的效能。

關鍵詞：分析層級程序法(AHP)、區塊鏈、共識機制、雜湊函數

壹、前言

一、研究背景與動機

國防部人次室因應國軍精進案人事行政人員精簡及公文書改革，責由空軍司令部研發新一代人令系統，並於民國93年8月完成系統開發，並逐項完成人令製作及線傳系統程式研改，國軍人事作業自動化系統開發的範圍共分為以下四項：

(一)資料庫採集中管理，由資料庫主機依人事權責切割各單位權限內人員資料，再將資料封包加密置於主機等候預約者下載。

(二)本系統係運用網際網路架構提供使用者預約下載介面與建置。

(三)以Deliphi程式語言開發，結合後端Access資料庫，提供各類人事命令(人令、獎懲、專長、俸級晉支、退除等)製作及查詢(編現、人員資料)功能。

(四)各項人事命令均採Word套表，由系統將資料直接轉為Word格式，並逐欄置入資料及排版換頁。

從資料庫的角度而言，新興的主流技術為「區塊鏈」，自從2008年Satoshi Nakamoto首次發表論文【註1】提出區塊鏈技術後，區塊鏈技術即蓬勃發展，在許多方面都有其應用，美國知名顧問管理資詢公司麥肯錫公司曾在2017年提出「以區塊鏈技術，改善政府資料管理」的論點，指出政府機關各部門所掌握資訊的交流與個資保密的重要性，而我國行政院也在近年通過了國發會提出的智慧政府規劃報告，要推動兩大基礎建設，包括全面發行數位身分證來串連政府服務，將要利用區塊鏈技術，來介接不同政府機關的資料庫【註2】，以上種種都相當值得深入探究區塊鏈在各領域導入的價值及關鍵成功因素。

二、研究動機

觀察現行國軍人事作業自動化系統的運作方式，可以發現以下幾個問題：

(一)資料庫操作繁瑣：由於國軍人事作業自動化系統為單機版，因此，必須定期下載最新的人事資料庫，須透過過一連串的程序後，始可使用。

(二)資料庫不同步：由於單機版的系統需要手動匯入更新資料庫，因此，所使用的並非最新資料，而且，現行國軍人事資料庫有以下區分：

1.「人事資訊系統」資料庫一由通次室維管，是完成線傳作業後，最即時也

註1　Satoshi Nakamoto, Bitcoin A Peer-to-Peer Electronic Cash System, 2008。

註2　許明恩，2019/3/10，區塊鏈走入台灣政府，https://medium.com/@astromnhsu/139-區塊鏈走入台灣政府-3f78fafad567，檢索日期：2020/12/15。

最完整的人事資料；

2.「電子兵資」資料庫一由人次室維管，每日與通次室的人事資料庫同步一次；

3. 各軍種人事資料庫一由各軍種司令部人軍處維管，每日與通次室人事資料庫同步一次，內容僅含該軍種單位及該軍種人員；

4. 各單位人事資料庫一由各單位人事人員定期下載更新用，內容僅限該單位(含所屬單位)人員。

5. 由國軍人事資料庫分類可知，各資料庫的更新時間不同，內容也會有所差異，經常造成人事人員線傳作業錯誤及查證上的耗時。

表1.　智慧車輛自動駕駛6等級分類標準資料

資料庫分類	維管單位	更新頻率	資料來源	內容範圍
人事資訊系統	通次室	每小時	各單位線傳資料	全國軍
電子兵資	人次室	每日	通次室資料庫	全國軍
各軍種	司令部 人軍處	每日	通次室資料庫	軍種單位或軍種人員
各單位	各單位	5~7日	通次室資料庫	單位內人員

資料來源：自行整理。

(三)異地備份：由於通資機房一直是作戰攻擊的重要目標之一，為了確保資訊的可用性與完整性，國軍資安政策一直要求資訊機房的資料必須異地備份，以免遭到摧毀癱瘓，而國防部的人事資料庫主要存放在通次室伺服器，並由人次室伺服器定期同步，通次室與人次室的伺服器均存放在同一個機房，並不符合異地備份的條件。

(四)管理者的可靠性：在軍中資料庫的管理集中在少數管理者，而由於政策、程式或作業等種種因素造成的錯誤或修訂需求，管理者具有最大的權限可讀寫所有資料庫內容，甚至連增修欄位、資料表及權限設定都在同一個人手上，倘若該管理者稍有不慎或私心，就會造成無可彌補的錯誤或不公，這也是電子兵資無法完全電子化的原因之一。

由於區塊鏈的目的就是為了解決信任問題，讓貨幣交易(資料)的儲存不須透過第三方達成，具有透明公平的性質，如果導入區塊鏈，就沒有第三方也就是管理者，就消除了管理者可靠性的問題，而其主要特性包含了「去中心化」、「不可竄改性」、「加密安全性」及「可追蹤性」等等[註3]，剛好適合解決國軍人事自動化系統所遭遇異地備份及同步性的問題，並且符合國軍對於資安上的需求，此外，導入區塊鏈技術後，各節點都具有相同的資料庫，使用者本

註3　徐南煌，《區塊鏈技術發展與應用之研究》(國立台灣科技大學資訊管理系EMBA碩士論文)，2019年5月，第17頁。

身即可成為節點，無需再依繁瑣費時的程序更新下載資料庫，可大幅提升作業效率，因此將在後面的章節透過各種文獻研究，深入探討區塊鏈技術，及其導入後對於國軍人事作業自動化系統的助益，並歸納出導入區塊鏈的評估準則及關鍵成功因素。

貳、文獻探討

一、區塊鏈簡介

(一)區塊鏈的起源

2008年10月，Satoshi Nakamoto在一個私密的密碼學群組上發表了一篇論文「Bitcoin: A Peer-to-Peer Electronic Cash System」[註4]，俗稱「比特幣白皮書」，其研究目的正是希望交易無須透過第三方執行，他提出了一種基於密碼學而非信用的電子支付系統，所使用的核心技術概念正是區塊鏈[註5]，而這種技術也逐漸擴展應用至其他領域。

(二)區塊鏈的技術與特性

1. 去中心化[註6]：

比特幣的交易紀錄不用透過銀行保存，而是每個使用者都會保存一份完整的交易紀錄，這就是所謂的「分散式帳本」，只要擁有一個網路帳戶，即可在線上完成「點對點」傳輸交易，無需銀行中介，如果有新的交易，每個使用者的交易紀錄也會自動更新，假如某人不小心遺失了交易紀錄，他可以跟其他人複製一份，達成「去中心化」的目的。

2. 非對稱式加密(真實性)：

在區塊鏈的分散式帳本裡，並沒有實際記錄每個帳戶的餘額[註7]，帳戶的用途是「存取交易紀錄」，再從每筆交易紀錄統計餘額[註8]；對交易雙方及區塊鏈上的各個節點而言，要確認交易的真實性，則是採用「非對稱式加密」的公私鑰來判別，好處是，公鑰可以公開，如果別人用你的公鑰加密訊息後傳給你，只有你能用私鑰解密，相反地，若你要發布訊息給

註4　同註1。
註5　同註3。
註6　林佳賢，2018/7/3，不懂技術沒關係！圖解告訴你區塊鏈可以這樣用，https://www.cw.com.tw/article/5090842(天下雜誌651期)，檢索日期：2020/12/17。
註7　同註5，第13頁。
註8　詹雨安，2018/9/17，淺談區塊鏈與比特幣，https://medium.com/sheracaolity/淺談區塊鏈與比特幣-898581543d96，檢索日期：2020/12/17。

其他人時，可以用私鑰加密訊息，其他人若能用你的公鑰解開密文，就能確定訊息是由你發出的【註9】。數位簽章是非對稱式加密的應用，區塊鏈中的每一筆交易都要有當事者的數位簽章，確認該筆交易為當事人發起的【註10】。

圖1.　對稱式加密

圖2.　非對稱式加密

圖片來源：https://medium.com/@RiverChan/基礎密碼學–對稱式與非對稱式加密技術–de25fd5fa537

3. 雜湊函數(安全性)：

區塊鏈最重要的技術就是雜湊函數(Hash function)，它具有以下幾個特性【註11】：

(1) 固定長度：一個任意長度的值可以透過雜湊函數計算出固定長度的hash值。

(2) 不可逆：透過雜湊函數計算出的hash值無法計算回推出原值。

(3) 發散性：透過雜湊函數計算出hash值後，如果改變原本的值，計算的結果就大不相同。

區塊鏈中的每個區塊都包含兩個部份：「區塊頭」與「交易紀錄」，而區塊頭的長度是固定的，其組成就包含上一個區塊的雜湊值與當下區塊的Merkle Root值。

4. 資料竄改不易：

(1) 默克爾樹(Merkle Tree)：區塊頭裡的Merkle Root值，是Merkle Tree唯一的終止節點，是從打包區塊的交易資料經過多次雜湊函數計算出的Top Hash值，此參數能確保區塊中的交易紀錄未經竄改；假如有人竄改了內容，那麼根據雜湊函數的發散性，產出的Hash值會大不相同

註9　賴忠建，《植基於區塊鏈技術之物聯網資訊安全》(國立高雄科技大學電子工程系碩士論文)，2018年7月。
註10　https://know.zombit.info/加密與簽章，檢索日期：2020/12/21。
註11　同註8。

，所產出的Merkle Root值也會大幅改變【註12】。

(2)從「去中心化」的特性中，我們得知在區塊鏈裡，每個節點都有完整而且相同的交易紀錄，若某個節點的使用者偷偷竄改交易紀錄，那這個節點的交易紀錄就會與其他節點不同，我們就能輕易地發現該節點的交易紀錄是否被竄改【註13】。

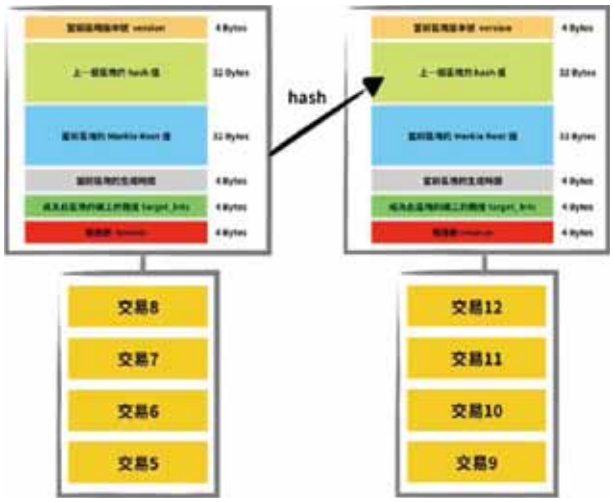

圖3.　區塊鏈組成與關連

5.可信的時間戳記(Timestamp)：

可信的時間戳記是確立電子紀錄具法律效力的重要技術之一，利用時間戳記，把每個區塊依時間順序進行排列，形成鏈狀【註14】。在「比特幣白皮書」中提出時間戳記伺服器的概念，把很多項目組成的區塊經過雜湊函式計算後加上時間戳記，並進行廣播，每個時間戳記會將前一個時間戳記一起進行雜湊運算，接續形成一條鏈，而且每個時間戳記都強化了前一個時間戳記【註15】。每筆交易依序建立時間戳記，系統就能回溯之前任何一個時間點的交易紀錄【註16】，讓區塊鏈兼具了可追溯性的特性。

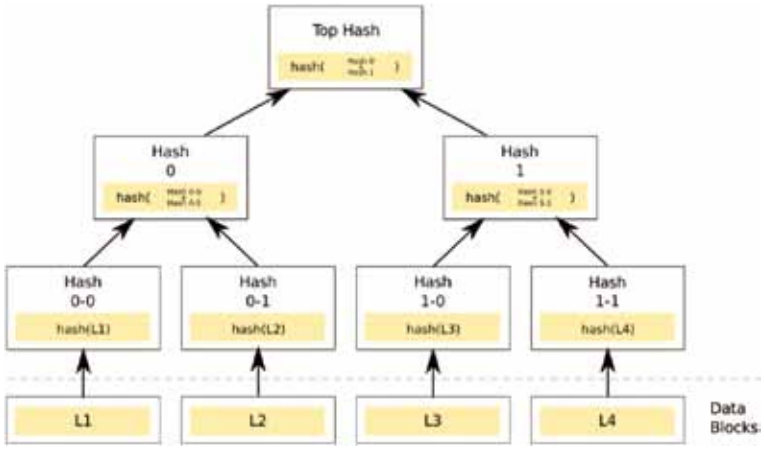

圖4.　交易資料Hash值產出Merkle Root過程

圖片來源：https://medium.com/sheracaolity/淺談區塊鏈與比特幣-898581543d96

註12　同註8。
註13　同註9。
註14　https://chainnews.com/zh-hant/articles/528240183491.htm，檢索日期：2020/12/22。
註15　同註1。
註16　同註3。

二、區塊鏈的發展趨勢與應用

台灣IBM公司技術長徐文暉認為區塊鏈從實驗走向商營已經成為主流趨勢【註17】，而區塊鏈的趨勢可以從共識機制、區塊鏈類型及區塊鏈階段等三個層面的發展來討論：

圖5. 竄改交易紀錄

圖片來源：https://medium.com/sheracaolity/淺談區塊鏈與比特幣-898581543d96

(一)共識機制/共識演算法(Consensus algorithm)【註18】：

所謂「共識機制」就是參加區塊鏈記帳的規則，共識機制的主要目的是選出爭取到區塊記帳權的節點，為了讓區塊鏈中各個節點，在互不信任且沒有中央機構的情況下達成共識，一起維護區塊鏈，讓節點間的帳本達成共識，才能確保帳本的一致性和交易的有效性，常見的有以下幾種：

1. 工作證明(Proof of Work, PoW)：

1993年，由Cynthia Dwork和Moni Naor提出，在工作證明中，爭取記帳權的過程稱為「挖礦」，參與者就是「礦工」，為了吸引使用者成為礦工，需要一套公平的獎勵機制，爭取到記帳權的礦工會得到兩種獎勵：建立新區塊的加密貨幣，是無中生有的新創貨幣，另一種是區塊中交易紀錄的交易費【註19】。

2. 權益證明(Proof of Stake, PoS)：

2011年，在BitcoinTalk論壇中，Quantum Mechanic第一次提出了「權益證明」；隔年8月Sunny King首次將PoS應用在新發行的PPCoin上；2014年rat4以PPCoin為基礎使PoS演算法更加完善，並應用發佈了黑幣【註20】。權益證明的出現是為了取代工作證明，減少因挖礦大量運算所造成的能源耗損【註21】；權益證明則是根據權益，權益越高，獲得打包區塊

註17 徐文暉，從實驗走向商營區塊鏈技術成主流趨勢，電腦與通訊期刊，第169期。
註18 https://know.zombit.info/共識機制/，檢索日期：2020/12/21。
註19 https://easonwang.gitbook.io/blockchain/block，檢索日期：2020/12/23。
註20 https://www.samsonhoi.com/386/blockchain-proof-of-stake，檢索日期：2020/12/23。
註21 同註15。

的機率越高。

3. 權威證明(Proof of Authority, PoA)[註22]

2017年，由以太坊兼Parity Technologies公司聯合創始人Gavin Wood提出，是一種基於聲譽的共識機制，基於有限的驗證節點，使其成為擴展性高的系統，區塊和交易都由已認證過的帳戶當成系統管理者來實施驗證。權威證明的運作是藉由驗證者的工作範圍及聲譽大小實現的，每筆交易至少要得到兩個節點的驗證，而它們的權力必須大於初始節點。成權威證明驗證者的三個基本條件：

(1)有效可信的身份：驗證者必須在網路上正式驗證過身份。

(2)嚴苛的篩選條件：為了使驗證過程有價值並提供足夠的獎勵，應使資格很難獲得[註23]。(例如：一個候選公證員應取得國家證照才能成 正式公證員)

(3)檢查和程序一致：建立權威的檢查和程序應該保持一致。

(二)區塊鏈類型[註24]：

1. 公有鏈

公有鏈是所有人都可以查詢，並執行收發與認證交易，向所有人公開；任何人都能夠參與其共識過程的區塊鏈，經由共識過程決定哪個區塊可以加入區塊鏈，因此公有鏈通常是完全去中心化的。公有鏈的特點是不可篡改、使用者匿名、交易公開、技術門檻低，實際的去中心化；缺點是分散式管理依賴共識機制，更新同步慢，對企業而言，自行開發初期成本高昂，且受限在擴充相容的窒礙，無法滿足企業。

2. 私有鏈

私有鏈為完全私有的，其寫入權限掌握在所屬組織手裡，讀取權限有限制性的開放，整個網路由組織成員共同維護，共識過程由事先選定的節點控制，這種類型的區塊鏈屬於部分去中心化。私有鏈的特點是交易速度快、交易隱秘、成本低，並保持不可篡改的特性；缺點是權限由少數節點掌控，無法解決作弊的問題，背離去中心化的初衷，且數據可能被控制，代碼也可能遭修改。

註22 https://www.chainnews.com/zh-hant/articles/824457289655.htm，檢索日期：2021/1/12。

註23 https://kknews.cc/zh-tw/tech/562rbn8.html，檢索日期：2021/1/12。

註24 Ennio Y. Lu ，2018/12/12，https://www.blocktempo.com/which-blockchain-analysis/，檢索日期：2021/1/13。

3. 聯盟鏈

聯盟鏈適合用在機構之間交易、清算或結算等B2B架構，即企業與企業之間互動，做為同業機構之間交易的可信平台，通常外部使用者能夠查詢，但無法交易，其共識過程受預選節點掌控；聯盟鏈允許每個人讀取，區塊的Root Hash和API(應用程式接口)是開放的，屬於部分去中心化；聯盟鏈和私有鏈相似，開放程度及去中心化的程度有限，其記帳權、讀寫權是由組織決定，與私有鏈最大的不同在於，聯盟鏈是由一個聯盟組成，而私有鏈是由一個組織主導【註25】。

(三)區塊鏈階段【註26】：

1. 區塊鏈1.0-數位貨幣：

區塊鏈1.0主要用在數位貨幣，是虛擬貨幣的底層技術應用於去中心化的支付系統。

2. 區塊鏈2.0-數位經濟：

區塊鏈2.0是指各種經濟與金融的應用，在這個階段還涉及到區塊鏈技術的關鍵應用一智能合約，能自動執行合約條款，如果合約條件相符，合約協議的內容則會自動履行。智能合約是由電腦科學家暨密碼學專家Nick Szabo於1994年提出【註27】，擬訂了智能合約的運作方式，定義智能合約是一種以訊息化傳播、驗證及執行合約的電腦協議，在沒有第三方的情況下進行可靠交易，這些交易可追蹤且無法逆轉，智能合約能解決許多公司不履行合約的窘境，原因有以下3點：自動執行、可靠性、高效性【註28】。

3. 區塊鏈3.0-數位社會：

區塊鏈3.0是指金融經濟以外的應用，包含教育、科學、認證、健康、藝術、文化等各方面。參考許多文獻可以發現，有關區塊鏈3.0的定義，仍眾說紛云，可概分為兩種：第1種是將分散式帳本技術應用於更多場景(如結合物聯網應用IOTA)，第2種是解決區塊鏈2.0所遇到的問題(如擴容及儲存限制)【註29】。

註25 https://www.abmedia.io/consortium-blockchain，檢索日期：2021/1/14。
註26 陳慧君，《以AHP和ISM分析法應用於創業服務區塊平台投資評估因素關聯性之研究》(國立中興大學碩士論文)，第12頁，2019年7月。
註27 陳恭，《智能合約的發展與應用》(財金資訊季刊NO.90)，2017年10月。
註28 https://m.yicai.com/news/100926418.html，檢索日期：2021/1/14。
註29 https://www.joyso.io/from-bitcoin-to-blockchain-3-0/?lang=zh-hant，檢索日期：2021/1/14。

三、區塊鏈導入之各項評估準則

從文獻中我們可以歸納出區塊鏈的技術與特性：去中心化的分散式帳本、點對點傳輸交易、非對稱式加密(真實性)、數位簽章、雜湊函數(安全性)、資料竄改不易及可信的時間戳記(可追溯性)，而從區塊鏈的發展趨勢我們也了解到共識機制能確保分散式資料的一致性，區塊鏈2.0智能合約的可靠性；而這些特性大致上可從資料的「安全層面」、「資料紀錄內容」及「技術功能層面」等3個構面來分析導入區塊鏈技術的評估準則，可歸納出以下10項：

表2.　導入區塊鏈技術的各項因素

國軍人事作業自動化系統導入區塊鏈評估要項說明				
主要評估層面		次要因素		因素說明
1	安全層面	1.1	安全性(雜湊函數)	運用密碼學中的雜湊函數(Hash Function)將交易資訊轉換成**無法回推**的雜湊(hash)值。
		1.2	竄改不易	區塊鏈技術使用 Merkle Tree 技術，將交易數據**層層加密**，增加資料竄改的難度，且每個區塊都有相同完整的交易資料，除非同時修改超過半數的區塊資料，否則資料無法竄改。
		1.3	可靠性(智能合約)	智能合約在沒有第三方的情況下進行可靠交易，提供**驗證及執行**合約內所訂立的條件，這些交易可追蹤且無法逆轉。
2	資料紀錄內容	2.1	來源真實性(非對稱式加密)	加密與解密分別使用**公鑰與私鑰**，依加密方式的不同，來確定訊息來源或訊息接收者的身份，確保訊息的真實性及安全性。
		2.2	分散資料一致性(共識機制)	所謂「共識機制」就是參加區塊鏈**記帳的規則**，其主要目的是選出擁有記帳權的節點，為了讓區塊鏈中各個節點，在互不信任且沒有中央機構的情況下達成共識，確保帳本的一致性和交易的有效性。
		2.3	可追溯性	區塊鏈上每筆交易紀錄都含有**時間戳記與參考連結**，環環相扣且公開透明，是無法異動的，可靠且安全，能夠追溯之前任何一個時間點的交易紀錄。
3	技術功能層面	3.1	數位簽章	「數位簽章」屬於非對稱加密的應用，當事人以**私鑰加密簽名**過的紀錄，只能用當事人的公鑰打開，藉此可知該筆紀錄資料屬於當事人。
		3.2	紀錄方式(打包區塊的方式及內容)	區塊鏈將多筆交易內容、時間戳記及相關資訊，用雜湊函數演算加密，資料結構採 Merkle Tree 固定資料長度，並能**確保資料的完整性**。
		3.3	點對點傳輸	在區塊鏈點對點的網路架構中，每個使用者既是節點，也具有伺服器的功能，每個節點都能互相傳輸紀錄資訊，**解決了訊息不對等和信任問題**。
		3.4	可信的時間戳記	可信的時間戳記是**確立電子紀錄**具法律效力的重要技術之一，利用時間戳記，把每個區塊依時間順序進行排列，形成鏈狀。

資料來源：作者自行彙整。

參、研究方法與設計

一、 建立層級架構

為了確保問卷的專業性與可用性，本研究流程將以兩階段進行，第一階段透過文獻蒐集分析研擬出國軍人事作業自動化系統導入區塊鏈技術的主要層面及次要準則後，邀集專家學者提供意見，藉以篩選評估主、次準則，以確立層級架構；第二階段依照確立之層級架構設計AHP問卷，由各管理者、使用者及專家學者填寫問卷，針對各項準則兩兩比較後，再以軟體驗證結果的一致性，以確立準則的排序與權重。

(一)研擬主、次準則：

經由文獻探討歸納出區塊鏈的各項特點，做為國軍人事作業自動化系統導入區塊鏈技術的評估準則，以找出導入區塊鏈技術的關鍵成功因素，區分為「安全層面」、「資料紀錄內容」及「技術功能層面」等3個主要層面來評估，彙整如下表：

(二)專家訪談：

在文獻蒐集的過程中，發現許多專家學者的研究、指導與傑出成就，都提供了許多深入而寶貴的資料，第一階段遴選出10位較具代表性的專家，評選導入區塊鏈技術所應考量的因素並提供專業建議，結果回收7份有效問卷(專家背景資料如下表)。

表3.　關鍵成功因素彙整表

研究目的	主要評估層面	次要因素
國軍人事作業自動化系統導入區塊鏈技術	安全層面	安全性(雜湊函數)
		竄改不易(Merkle Tree)
		可靠性(智能合約)
	資料紀錄內容	來源真實性(非對稱式加密)
		分散資料一致性(共識機制)
		可追溯性
	技術功能層面	數位簽章
		紀錄方式(打包區塊的方式及內容)
		點對點傳輸
		可信的時間戳記

表4.　專家背景資料

項次	單位	職稱	經歷
1	巴克夏夫科技股份有限公司(BuckChaf)	執行長	英國媒體評為「2019 前十大潛力區塊鏈公司」BuckChaf 執行長
2	巴克夏夫科技股份有限公司(BuckChaf)	營運長	英國媒體評為「2019 前十大潛力區塊鏈公司」BuckChaf 營運長
3	台灣圖靈鏈股份有限公司(Turing Chain)	執行長	德國慕尼黑 ACM MobiSys CryBlock 2018 論壇發表區塊鏈技術論文「ERC860」榮獲最佳論文(Best Paper)
4	中華民國區塊鏈大學聯盟	理事長	富加 F.plus 平台負責人
5	BlockUnicorn	Founder	幣安台灣社區負責人
6	微進科技股份有限公司	合夥人	AppWorks Fellow
7	BDE	Founder	數位轉型科技限公司創辦人

(三)評估主、次準則：

由文獻探討分析所得國軍人事作業自動化系統導入區塊鏈技術應考量的3個主要層面及10個次要因素，經過專家審慎評估後，全數同意勾選自文獻歸納出的3個主要層面及10個次要因素均有其必須性。

(四)確立層級架構：

依據文獻探討分析及專家評估同意所得國軍人事作業自動化系統導入區塊鏈技術應考量之關鍵成功因素評估層級架構，確立由「安全層面」、「資料紀錄內容」及「技術功能層面」等3個構面主準則及其下10個次準則來分析歸納(如下圖)。

二、設計AHP層級分析問卷

本研究從第一階段研擬主/次準則、專家訪談、評估準則、確立層級架構

後，分別將各層級中的影響因素兩兩比較，目的在求得評估之主、次準則先後次序及權重的相對重要性，以確保對第一、二階段問卷內容瞭解程度及各主、次準則重要性評選無太大落差，研究對象以人事工作階層、管理階層及技術階層之專家為主體，共42位受訪者，以作為研究分析運用。

圖6.　層級架構圖

肆、研究分析與結果

一、權重分析

(一)一致性分析

採用AHP應用軟體「Expert Choice 11」分析回收問卷的一致性，經過兩兩比較後，可經由準則與準則間的比例運算出一致性指標(Consistency Index, C.I.)值，若C.I.值>0.1，表示受訪者所填寫的比例前後不一致，即無法採用；本次層級分析問卷區分管理、執行及技術等3個階層進行調查，從司令部到各聯隊層級人事單位，共發放42份，回收30份問卷，其中，計有7份C.I.值未達標準，為無效問卷；其餘23份均為有效問卷，因此採用23份有效問卷為本研究決策依據主體。

(二)主準則權重分析

1. 高階管理階層權重優先次序值畫面如下：
2. 基層執行階層權重優先次序值畫面如下：
3. 資訊技術階層權重優先次序值畫面如下：
4. 整體評估權重優先次序值畫面如下：

圖7.　管理階層主準則優先次序畫面

(三)次準則權重分析

1. 高階管理階層之次準則權重優先次序:

2. 基層執行階層之次準則權重優先次序:

3. 資訊技術階層之次準則權重優先次序:

4. 整體評估之次準則權重優先次序：

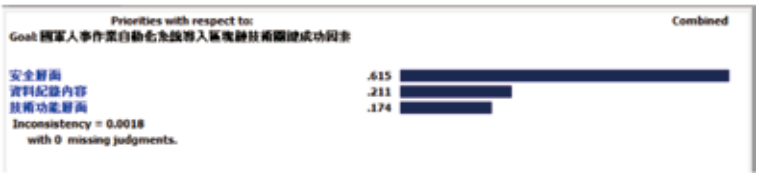

圖8.　執行階層主準則優先次序畫面

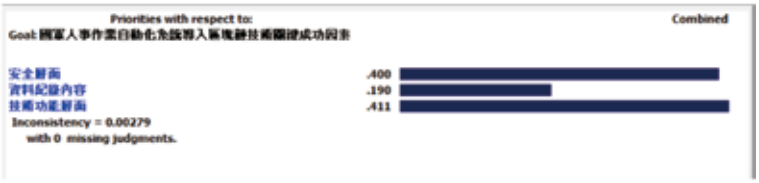

圖9.　技術階層主準則優先次序畫面

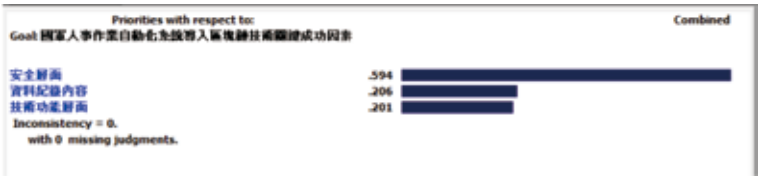

圖10.　整體主準則優先次序畫面

二、綜合分析

本次研究問卷共發放42份，回收30份，其中有效問卷計23份，區分管理階層8份、執行階層11份及技術階層4份，整體權重統計圖如圖23，針對各項統計數據綜合實施分析，並提出小結。

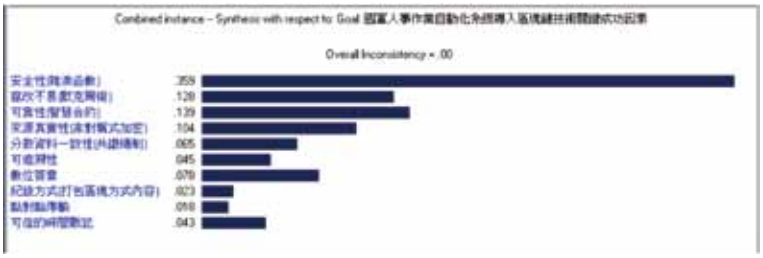

圖11.　管理階層次準則優先次序畫面

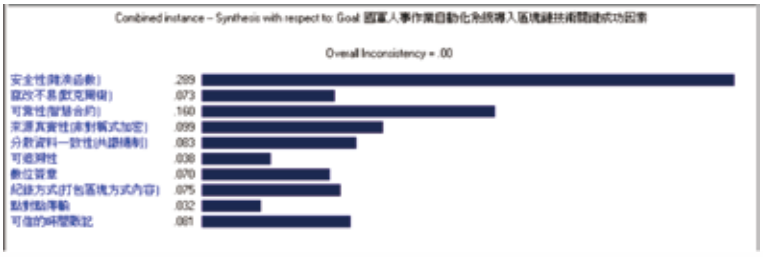

圖12.　執行階層次準則優先次序畫面

(一)主準則分析

整體而言，「安全層面」仍是大部份受訪者認為對於國軍人事作業自動化系統導入區塊鏈技術之關鍵因素，其中包含了雜湊函數加密所具備的「安全性」、默克爾樹使其「竄改不易」、智能合約提升的「可靠性」等次準則，隨著人員精簡、作業簡化的趨勢下，如何提升系統的「安全層面」是各級不容忽視的一環。

(二)「安全層面」次準則分析

管理、執行及技術等3個階層的受訪者一致認為「安全層面」中的次準則，以雜湊函數加密所具備的「安全性」權重最高，其次為智能合約提升的「可靠性」，因此，「安全性」是各階層最重視的部份，對於人事資料而言，由於作業的系統化，透過網路傳輸的加密安全更顯重要，國軍人事作業自動化系統可藉由雜湊函數加密傳輸人事資料，使得在網路中傳輸的資料更加有保障，即使遭到竊取，也無法輕易解密。

圖13.　技術階層次準則優先次序畫面

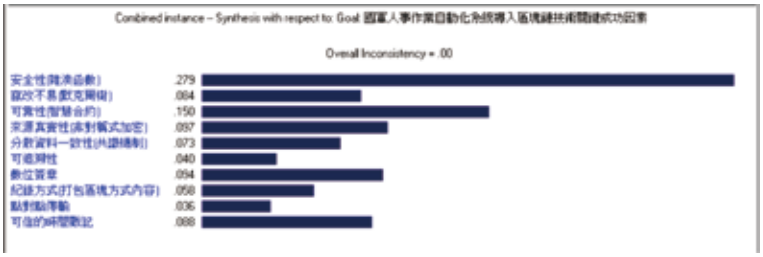

圖14.　整體次準則優先次序畫面

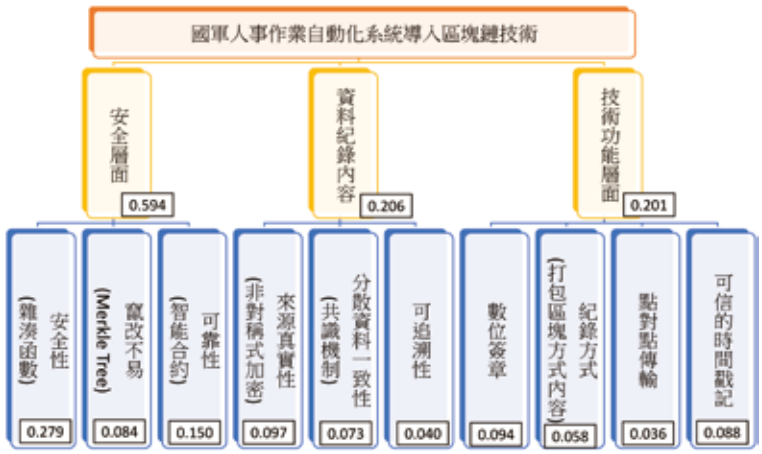

圖15.　整體主、次準則權重統計圖

(三)「資料紀錄內容」次準則分析

「資料紀錄內容」中的次準則，以非對稱式加密所能證實的「來源真實性」權重最高，其次為共識機制確保「分散資料一致性」，為了確保人事資料的真實性與安全性，系統應採用嚴謹的非對稱式加密技術，以確保相關的人事資料或人事命令，來源是合法且可靠的，若能透過區塊鏈導入非對稱式加密技術，即可降低偽冒造假的風險，確保人事資紀錄的內容的安全性與正確性。

(四)「技術功能層面」次準則分析

管理、執行及技術等3個階層的受訪者對於「技術功能層面」中的次準則權重優先次序均不同，但從整體評估統計中，以「數位簽章」為「技術功

能層面」中權重最高的次準則，其次為「可信的時間戳記」，而這兩個次準則所對應到的是人員及時間，就人事系統的技術面來說，是非常重要的兩項因素，人事命令要如何發布到當事人手中而不致於外流或外洩，就要依靠數位簽章來確保人事命令送達當事人手中，以保障當事人的權益及隱私，而時間戳記是確立電子紀錄具有法律效力的重要技術，因此透過評估也凸顯出受訪者對其重視程度。

伍、結論與建議

一、結論

為使國軍人事作業自動化系統資料庫的使用及維管能簡化，並符合安全規範與備援機制，藉由探討、蒐整相關區塊鏈特性與發展趨勢，歸納出導入區塊鏈技術之主、次準則，做為爾後系統改版更新或重新建構之參考依據，期能有效提升人事作業效率、正確性及安全性。本研究經由專家訪談及分析層級程序法結果所得之「安全性」、「可靠性」及「來源真實性」等前3項優序，其相關建議作法如后：

(一)安全性：

研究結果顯示，各項次準則中以雜湊函數加密所具備的「安全性」權重最高，表示各階層的受訪者認為以雜湊函數加密所具備的「安全性」在國軍人事作業自動化系統導入區塊鏈技術之研究中最受重視。可以採納台灣圖靈鏈股份有限公司(Turing Chain)執行長所提之建議，採用SHA256層級以上之雜湊函數，因MD5/SHA128等舊型函數有雜湊碰撞等資安風險，而國軍對於資安的要求及管控較為嚴格，因此可採用較嚴格之加密法，並培養或延攬加密程式及資料庫人才，以提升國軍各項系統資安防護能力。

(二)可靠性：

研究結果顯示，各項次準則中以智能合約提升「可靠性」權重排序第二，表示各階層的受訪者認為以智能合約提升「可靠性」在國軍人事作業自動化系統導入區塊鏈技術之研究中頗受重視。智能合約主要功能是在沒有第三方的情況下進行可靠交易，可避免管理者疏失或私心，並提供驗證及執行合約內所訂立的條件，在導入區塊鏈技術的過程中，必須再三檢視及驗證相關人事作業的程序、條件及特例，是否完備，才能讓系統執行人事資料更新時更加精準正確，提升人事作業的效率及正確性。

(三)來源真實性：

研究結果顯示，各項次準則中以非對稱式加密所能證實的「來源真實性」權重排序第三，表示各階層的受訪者認為以非對稱式加密所能證實的「來源真實性」在國軍人事作業自動化系統導入區塊鏈技術之研究中也很重要。以非對稱式加密證實「來源真實性」的技術是加密與解密分別使用公鑰與私鑰，依加密方式的不同，來確定訊息來源或訊息接收者的身份，確保訊息的真實性及安全性，因此除了資訊技術人才的培育外，公鑰與私鑰的管理方式也是導入區塊鏈技術的重要一環，若能搭配良好的管理機制，就能讓區塊鏈技術發揮更大的效能。

二、建議

(一)國軍人事自動化系統精進方向

1. 自動化：

國軍人事自動化系統為提供人事人員更方便、迅速且正確的發布人事命令，由於人事法規是固定的，如果做的好，甚至能讓系統自動完成人令的發布，尤其是定期產製的人令，例如俸級晉支，又或者是遇到狀況，系統也能自動判別，例如違反了資安法規，系統偵測到就能連線處理，依對應的懲處表發布懲處，如果導入區塊鏈，在可靠的情況下，是可以達成的願景。

2. 系統整合：

人事資料是許多系統都會需要建置的基本資料，就像公文系統、後勤系統甚至飛行系統都會用到，因此，系統的整合也是國軍人事自動化系統精進的方向之一，而要整合系統，最重要的就是資料庫的介接，因此，具有一個可靠、安全的資料庫環境很重要，而不能時時刻刻由人員去維護，否則資料庫越來越複雜且龐大，對於維管人員勢必成為不小的負荷，因此，導入區塊鏈技術，不但能減輕人員的負擔，提升資料庫的安全性、可靠性，也有助於系統的整合。

(二)適時引進新興技術與人才培育

資訊的提升，是需要硬體、軟體及人員三方面同時提升，才能發揮其最大的功效，對人事系統而言，其實很多作業是可以簡化、自動化的，如果能導入區塊鏈技術，並且培育新興技術的人才，除了能提升系統的效能，更能讓人員培養資訊實力，成為誘因吸引人才，而且區塊鏈本身其實就涵蓋了許多其他的新技術，像點對點傳輸、智能合約、雜湊函數及默克爾樹等多項技術，非常值得深入探究，相信導入後，能有更多領域的應用。

參考文獻

一、期刊：
1.徐文暉，從實驗走向商營區塊鏈技術成主流趨勢，電腦與通訊期刊，第169期
2.陳恭，《智能合約的發展與應用》(財金資訊季刊NO.90)，2017年10月
二、論文：
1.Satoshi Nakamoto, Bitcoin A Peer-to-Peer Electronic Cash System, 2008
2.徐南煌，《區塊鏈技術發展與應用之研究》(國立台灣科技大學資訊管理系EMBA碩士論文)，2019年5月
3.賴忠建，《植基於區塊鏈技術之物聯網資訊安全》(國立高雄科技大學電子工程系碩士論文)，2018年7月
4.陳慧君，《以AHP和ISM分析法應用於創業服務區塊平台投資評估因素關聯性之研究》(國立中興大學碩士論文)，2019年7月
三、網路：
1.許明恩，2019/3/10，區塊鏈走入台灣政府，https://medium.com/@astromnhsu/139-區塊鏈走入台灣政府-3f78fa-fad567，檢索日期：2020/12/15
2.林佳賢，2018/7/3，不懂技術沒關係！圖解告訴你區塊鏈可以這樣用，https://www.cw.com.tw/article/5090842(天下雜誌651期)，檢索日期：2020/12/17
3.詹雨安，2018/9/17，淺談區塊鏈與比特幣，https://medium.com/sheracaolity/淺談區塊鏈與比特幣-898581543d96，檢索日期：2020/12/17
4.https://know.zombit.info/加密與簽章，檢索日期：2020/12/21
5.https://chainnews.com/zh-hant/articles/528240183491.htm，檢索日期：2020/12/22
6.https://know.zombit.info/共識機制/，檢索日期：2020/12/21
7.https://www.samsonhoi.com/360/blockchain_proof_of_work，檢索日期：2020/12/23
8.https://easonwang.gitbook.io/blockchain/block，檢索日期：2020/12/23
9.https://www.samsonhoi.com/386/blockchain-proof-of-stake，檢索日期：2020/12/23
10.https://www.chainnews.com/zh-hant/articles/824457289655.htm，檢索日期：2021/1/12
11.https://kknews.cc/zh-tw/tech/562rbn8.html，檢索日期：2021/1/12
12.Ennio Y.Lu，2018/12/12，https://www.blocktempo.com/which-blockchain-analysis/，檢索日期：2021/1/13
13.https://www.abmedia.io/consortium-blockchain，檢索日期：2021/1/14
14.https://m.yicai.com/news/100926418.html，檢索日期：2021/1/14
15.https://www.joyso.io/from-bitcoin-to-blockchain-3-0/?lang=zh-hant，檢索日期：2021/1/14

作者簡介

空軍少校 歐喜誠
學歷：中正理工專93年班、航院通參正規99年班、空軍指參學院110年班。
經歷：曾任通信官、資網官、程設官。
現職：國防大學空軍指揮參謀學院學員。