10.6326/NDJ.202212_37(4).0004

區塊鏈技術應用於國防採購之研究
The Application of Blockchain Technology in ROC National Defense Procurement

蘇品長 (Pin-Chang Su)　　黃琬玲 (Wan-Ling Huang)
國防大學管理學院資訊管理學系教授兼系主任　國防大學管理學院資訊管理學系少校研究生

摘　要

隨著資訊科技快速發展，區塊鏈是近年來具前瞻及革命性的一種技術，被國際研究暨顧問機構列爲10大科技趨勢，並廣泛應用於金融、供應鏈、物聯網、公共事務等諸多領域，部分先進國家更是致力將技術發展於國防事物，有助於達成安全、可信任之國防服務。臺灣透明組織於2020年公布政府國防廉潔指數(Government Defense Anti-Corruption Index, GDI)，我國軍事廉潔度與德國並列全球第六名，然而在執行反貪腐與採購得分相對較低，且具中、高度風險，本研究將利用區塊鏈「去中心化」、「不可竄改」、「公開透明」特性，應用於國防採購作業，降低採購過程中，因資訊無法透明化，進而肇生投標文件遭竄改、官商勾結、廠商賄賂、收受回扣等貪瀆弊案之風險，達成國防採購安全及廉潔軍風要求。

關鍵詞：區塊鏈、國防採購、軍事事務革新、廉潔軍風

Abstract

With the rapid development of information technology, blockchain is a forward-looking and revolutionary technology in recent years. It has been listed as 10 major technology trends by international research and consulting institutions, and is widely used in many fields such as finance, supply chain, Internet of Things, public affairs, etc. Some advanced countries are even committed to developing the technology in defense matters, which can help achieve a secure and trustworthy defense service. Taiwan Transparency Organization announced the Government Defense Anti-Corruption Index (GDI) 2020, our country's military integrity ranks sixth in the world with Germany, However, the implementation of anti-corruption and procurement projects scored relatively low, with medium and high risk. This study will utilize the "decentralized", "non-tamperable", and "open and transparent" characteristics of blockchain to apply to national defense procurement operations. It can reduce the risk of tampering with bid documents, collusion between government and business, bribery and kickbacks, and other corruption and abuses in the procurement process due to the lack of transparency of information, and meet the requirements of security and integrity of national defense procurement.

Keywords: Blockchain, National Defense Procurement, Revolution of Military Affairs, Military Integrity

壹、前　　言

國防轉型通常伴隨著「軍事事務革新」(Revolution in Military Affairs, RMA)而來，依「國際戰略研究所」(International Institute for Strategic Studies, IISS)將「軍事事務革命」或「軍事科技革命」(Military Technical Revolution, MTR)定義為：「將新科技融入一個具有軍事意義系統，新科技結合創新的作戰概念與組織調整，進而增進軍事效能。」[1]，資訊科技的發展決定了軍事轉型的能力，每當科技出現重大突破與進展時，經常會驅動人類的社會轉型、軍隊變革發展，建立以資訊化為主的軍事核心能力，提升作業效率、效能及正確性，將是軍事轉型的重點工作，[2]資訊科技的革新，將可能在軍事作戰指揮體系上形成革命性的改革。[3]

2008年中本聰所發表的一篇名為「比特幣：一種點對點的電子現金系統」的白皮書，首次提到區塊鏈的概念，然而在加密貨幣外，區塊鏈技術更已被廣泛應用於金融、供應鏈、物聯網、公共事務、醫療保健、政府組織等諸多領域，取得令人難以置信的成就，[4]成為近年來一項具前瞻及革命性的技術；美國市場數據研究公司(International Data Corporation, IDC)在2021年4月發布一份最新預測報告，根據技術、行業、應用場景等潛在機會，預測全球使用區塊鏈技術的總體支出將在2024年達到近190億美元，並在2020至2024年期間內，總支出將以強勁的速度增長。[5]而國際研究暨顧問機構高德納諮詢公司(Gartner)也發表2020年10大策略性科技趨勢，分別為超級自動化、多重體驗、專業知識的全民化、增進人類賦能、透明化與可追溯性、強大的邊緣運算、分散式雲端、自動化物件、實用性區塊鏈及人工智慧安全性，其中在區塊鏈部分可以建立雙方信任，透明化地進行跨生態系統價值交換，因此極具發展潛力。[6]另預估將於2030年，區塊鏈可能帶來高達3.1萬億美元的新商業價值，並

1 謝之鵬，〈美軍軍事變革對兩次波灣戰爭影響—兼論兩岸之對應作為〉，《國防雜誌》，第20卷第11期，2005年11月，頁103-115。

2 彭錦珍，〈科技對世界軍事革新及其發展的影響〉，《復興崗學報》，第84期，2005年9月，頁55-80。

3 王崑義，〈非傳統安全與臺灣軍事戰略的變革〉，《臺灣國際研究學會臺灣國際研究季刊》，第6卷第2期，2010年6月，頁1-43。

4 David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, & Yaser Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, Vol.58, No.1, January 2021.

5 Stacey Soohoo, "Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024, According to New IDC Spending Guide," *International Data Corporation*, 2021/4/19, <https://www.idc.com/getdoc.jsp?containerId=prUS47617821>（檢索日期：2022年4月15日）

6 李淑惠，〈2020年十大科技趨勢：以人為本的智慧空間將持續推動科技發展〉，《中時新聞網》，2019年10月31日，<https://www.chinatimes.com/realtimenews/20191031003646-260410?chdtv>（檢索日期：2022年5月7日）

估計在2025年時，其中一半的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。[7]

區塊鏈技術一旦成功應用，並與人工智慧、物聯網、雲端運算和大數據相互結合，應用於軍事事務管理、訊息安全乃至於指揮管制，未來將打破傳統軍事指揮管理，帶來軍事發展和作戰方式的革命性變革，許多科學家預測，有效挖掘區塊鏈技術的軍事應用潛力，將對提高軍隊戰鬥力，促進軍隊轉型發展具有重要意義。[8] 美國國防部(United States Department of Defense, DoD)也在2019年7月12日發表了一份名為《數位現代化戰略(Digital Modernization Strategy)》的報告，內容描述了幾項美國數位防禦的戰略重要計畫，其中包含整合興新科技如人工智慧、量子計算、雲端運算及透過分散式帳本技術(Distributed Ledger Technology, DLT)強化通訊安全等，而美國國防高等研究計畫署的研究部門，為了開發網路安全防護系統，保護國防訊息在傳遞過程中的機密性，並提高國防事務處理的安全性，已試圖利用區塊鏈技術來創建一個「更高效、強大及安全的平臺」。美國國防部更指出，利用區塊鏈公開透明且不可竄改的特性，能有效降低危害國防安全的可能性，更增加了敵人的攻擊成本。[9]

國防部於2021年發布新聞稿說明，國際透明組織所屬國防暨安全小組（簡稱TI-DSP）於2021年11月16日公布第三次「政府國防廉潔指數(Government Defence Integrity Index, GDI)」評鑑成績，我國三度獲得「B」等級（低度貪腐風險）的優異評價，與德國並列全球第六名，是亞洲國家中唯一擠進全球前十名者，表示我國國防廉潔受國際肯定，[10] 而臺灣透明組織指出，政府國防廉潔指數合計77項指標，涵蓋「政治」、「財務」、「人事」、「執行」及「採購」等5大領域的貪腐風險，我國在人事領域的風險為最低，其次為財務和政治，然而執行反貪腐與採購的得分較低，具中、高度風險，未來在執行反貪腐方面，應建立前瞻性的策略規劃，而非停留在教條式的口號規定，在採購契約控管方面應朝更公開透明的方向努力，並針對採購流程加強貪腐風險管理。[11] 目前國軍辦理工程、財務及勞務採購，從計畫申

7 Gartner, "Blockchain Technology: What's Ahead?", <https://www.gartner.com/en/information-technology/insights/blockchain>（檢索日期：2022年4月20日）

8 Y Zhu, X Zhang, Zh Y Ju, & Ch Ch Wang, "A study of blockchain technology development and military application prospects," *Journal of Physics: Conference Series*, Vol.1507, No.5, April 2020.

9 Jason Liu，〈美國國防部正透過區塊鏈技術，開發網絡安全防護系統〉，《動區動趨BlockTempo網》，2019年7月30日，<https://www.blocktempo.com/us-department-of-defense-is-developing-a-blockchain-cybersecurity-shield/>（檢索日期：2022年5月2日）

10 中華民國國防部，〈國防部發布新聞稿說明「我國國防廉潔指數評鑑為『B』等級，世界排名第6」〉，《中華民國國防部全球資訊網》，<https://www.mnd.gov.tw/Publish.aspx?p=79317&title=%E5%9C%8B%E9%98%B2%E6%B6%88%E6%81%AF&SelectStyle=%E6%96%B0%E8%81%9E%E7%A8%BF>（檢索日期：2022年5月4日）

11 臺灣透明組織協會，〈臺灣透明組織公布2020年世界各國「政府國防廉潔指數」我國得分70分與德國並列全球第六名，歸類為B級，屬低度風險國家〉，《臺灣透明組織協會全球資訊網》，2021年11月16日，<https://

購、尋商訪價、小額下訂或招標訂約、履約驗收、付款到最終會計入帳等層層環節，每個階段雖然都由各業管部門獨立作業，但稍有不慎，仍可能肇生舞弊的風險。[12] 國防採購部門通常被認為是最有可能發生貪污的領域，因此對於採購從需求、招標到驗收等各階段，都必須建立嚴格的管理機制，以防止貪污情形發生。[13]

本研究將利用區塊鏈「去中心化」、「不可竄改」、「公開透明」特性，結合橢圓曲線密碼學、自我認證及盲簽章等技術原理，應用於國防採購系統，有效提高監管能力並消除不必要的中介，達成資訊傳遞、數據儲存及管理方式轉型，提供更快速的運作模式，進而促成國防採購過程安全、可信任，有效防止舞弊、貪污情形發生，達成國軍廉潔軍風之要求，其具備以下優點：

一、透過區塊鏈技術，於鏈上每個區塊除交易資訊外，還包含前一個區塊的雜湊值，由各個節點共同維護和更新，每個節點中都包含完整的採購歷史紀錄，如果資料或文件遭到竄改，則雜湊值將與其他區塊不同，於開標決標時可達成資料透明化及可驗證性，提升採購機關與投標廠商的信任度，並降低人為賄賂、舞弊所帶來的投標文件遭竄改之風險。

二、藉由盲簽章技術並結合橢圓曲線密碼學架構，利用較短位元長度的金鑰，可達到與RSA非對稱加密演算法相同等級的安全強度，提升系統效能、降低負荷，並達到運算成本低，符合機密性、完整性、鑑別性及不可否認性等資安特性，強化國防採購安全度。

三、導入自我認證機制，避免製發憑證的過程中，肇生憑證中心偽冒用戶身分的安全性問題，可使採購過程中參與人員身分資料達到完整性、不可否認性及真實性，同時降低公鑰儲存、計算與管理的成本與風險。

貳、區塊鏈本質與特色介紹

本章節分類整理、歸納區塊鏈之文獻，並針對「區塊鏈起源與核心技術」、「區塊鏈的分類與特性」、「智慧合約與去中心化應用程式」，另簡述「自我認證」概念介紹，加以彙整做為本研究的基礎。

一、區塊鏈起源與核心技術

2008年爆發全球金融海嘯，金融業者

www.tict.org.tw/%E5%8F%B0%E7%81%A3%E9%80%8F%E6%98%8E%E7%B5%84%E7%B9%94%E5%85%AC%E5%B8%832020%E5%B9%B4%E4%B8%96%E7%95%8C%E5%90%84%E5%9C%8B%E3%80%8C%E6%94%BF%E5%BA%9C%E5%9C%8B%E9%98%B2%E5%BB%89%E6%BD%94%E6%8C%87/>（檢索日期：2022年5月2日）

12 孫志宏，〈淺談維護海軍後勤採購的廉潔環境〉，《海軍學術雙月刊》，第55卷第5期，2021年10月，頁87-99。

13 陳俊明、莊文忠、李宗模、郭宗城，〈政府國防廉潔指數於國防政策之應用與實踐〉，《國防部政風室》，2019年12月16日，<https://ethics.mnd.gov.tw/userfiles/files/%E6%94%BF%E5%BA%9C%E5%9C%8B%E9%98%B2%E5%BB%89%E6%BD%94%E6%8C%87%E6%95%B8%E6%96%BC%E5%9C%8B%E9%98%B2%E6%94%BF%E7%AD%96%E4%B9%8B%E6%87%89%E7%94%A8%E8%88%87%E5%AF%A6%E8%B8%90%E8%AA%BF%E6%9F%A5%E6%A1%88-%E6%9C%9F%E6%9C%AB%E5%A0%B1%E5%91%8A%E5%AE%8C%E6%88%90%E7%89%88-20191223.pdf>（檢索日期：2022年4月17日）

擔任第三方中介角色明顯受到質疑，從那時起，對於傳統建立的第三方保證已無法滿足彼此交易的信任基礎。中本聰(Satoshi Nakamoto)所發表的一篇名為「比特幣：一種點對點的電子現金系統」論文，內容描述比特幣的電子貨幣及相關演算法，成為人類文明歷史上第一套去除第三方中介的點對點支付系統，也堪稱全球權威帳本，在2009年1月比特幣正式流通誕生，比特幣是一種利用加密技術來管理貨幣發行量及交易有效性的一種電子貨幣及線上支付系統，其中可以涵蓋三種層面：區塊鏈的底層技術、協議與進行交易的客戶端，或者指實際流通的比特幣，即所有加密貨幣的統稱。[14] 比特幣底層技術即為區塊鏈，區塊鏈是一種透過對等式網路架構(Peer to Peer, P2P)，並由一連串的數學及密碼學所原理組成，又稱分散式帳本技術(Distributed Ledger Technology, DLT)，其中各節點之間透過共識機制達成協議，每個區塊內都包含了區塊的容量大小、區塊的表頭（版本號、前一個區塊的加密雜湊Hash值、梅根樹根節點的加密雜湊Hash值、時間戳記、當前難度值及隨機數）及交易的資料內容（如圖1所示），Lin與Liao曾指出區塊鏈包含演算法、密碼學、數學及經濟模型，並結合點對點網路，使用分散式的共識演算法，有效解決傳統的分散式資料庫同步問題。[15] 透過各節點之間共同維護一個具時序性的帳本，達到分散式儲存，資料長久保存，無法被任意竄改，且具有可信任的特性。任兩個節點都可以進行交易，每筆交易由單個節點廣播到全網所有節點，[16] 由於區塊鏈沒有特定的中央伺服器，在沒有中介的情況下可以進行安全的線上交易，[17] 可以降低溝通成本，並提高交易的效率，快速確立雙方信任感或在雙方交互尚未建立信任關係時即完成交易，滿足金融的本質屬性和內在要求。[18]

二、區塊鏈的分類

區塊鏈以應用的規模大小及其去中心化的程度差異，可區分為「公有鏈」（又稱為公開鏈）、「私有鏈」及「聯盟鏈」，合稱為許可鏈，相關特性比較表如表1。

(一)公有鏈

完全公開透明的區塊鏈，任何參與人員都可以在公有鏈上進行資料存取、接收、發送與交易認證，因此公有鏈通常被認為是完全去中心化；具不可竄改性、匿名

14 Dmitry Efanov and Pavel Roschin, "The all-pervasiveness of the blockchain technology," *Procedia computer science*, Vol.123, 2018, pp. 116-121.

15 Iuon Chang Lin and Tzu Chun Liao, "A Survey of Blockchain Security Issues and Challenges," *International Journal of Network Security*, Vol.19, No.5, September 2017, pp. 653-659.

16 Ming K.Lim, Yan Li, Chao Wang, & Ming-LangTseng, "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Computers & Industrial Engineering*, Vol.154, April 2021.

17 Praveen Vijaya Raj Pushpa Raj, Sunil Kumar Jauhar, M.Ramkumar, & Saurabh Pratap, "Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts," *Computers & Industrial Engineering*, Vol.167, May 2022.

18 黃步添、蔡亮，《區塊鏈改變未來的倒數計時》（臺北：清文華泉事業有限公司，2020年），頁2-18。

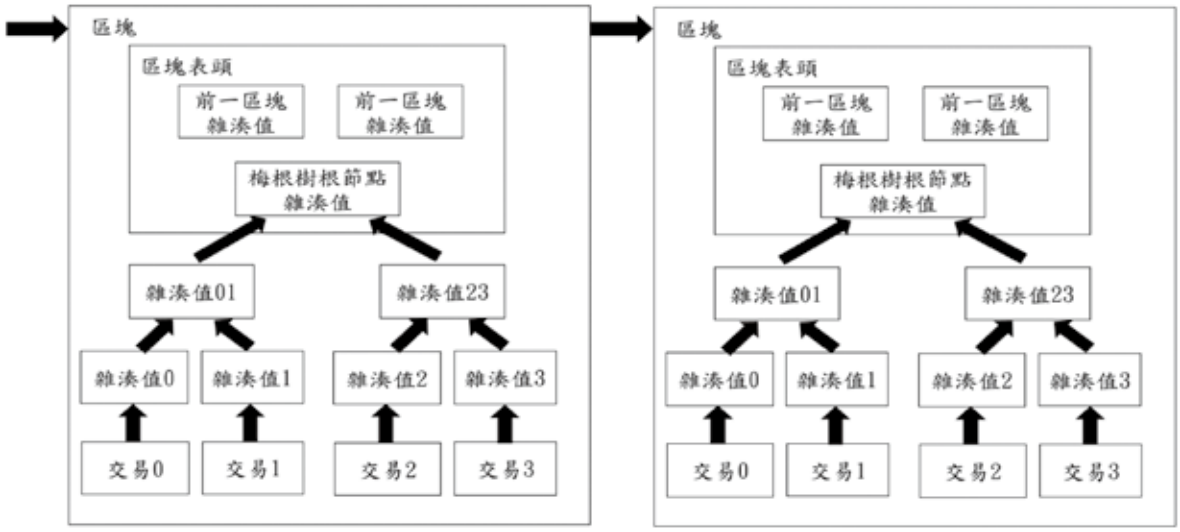

圖1　區塊鏈結構 [19]

表1　區塊鏈特性比較表

類別	公有鏈	聯盟鏈	私有鏈
參與者	任何人	多個機構	單一機構
身分	匿名	可識別	可識別
安全性	低	中	高
去中心化程度	高	中	低
交易效率	低	中	高
權限	不須授權，開放式閱覽、編寫	須經授權才能編寫、閱覽	須經授權才能編寫、閱覽
典型代表	比特幣、以太坊	Hyperledger	Multichain

資料來源：余庭儀，《植基於智慧合約的數位內容交易電子支付方法》（臺北：國防大學資訊管理學系研究所碩士論文，2020年）。

公開特性，採共識決機制，交易速度相對較慢。

(二)聯盟鏈

聯盟鏈是介於公有鏈和私有鏈之間，其中包含了兩者的特點，相較於公有鏈不屬於完全開放系統，任何人都可以驗證區塊，需要經過許可才能執行存取動作，相較於私有鏈屬於一個封閉的系統，聯盟鏈讀寫權、記帳權則由管理組織決定。

(三)私有鏈

私有區塊鏈建立了授權的規則，規範誰可以檢視和存取區塊鏈（需要經過許可的環境），參與私有鏈的節點受到嚴格的控制，節點與節點之間仍然共同維護區塊鏈的副本。私有鏈適合企業內部、單一公司內部使用，可以在不讓外部網路訪問的狀況下，

19 Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, <https://bitcoin.org/bitcoin.pdf>（檢索日期：2021年12月11日）

享有區塊鏈技術帶來的優點，保有內部隱私，並提升公司內部交易效率。

三、區塊鏈的特性

區塊鏈並非僅單一領域的新技術，包含數學、密碼學、經濟模型及演算法，並結合點對點網路，是一個綜合運用多領域技術之基礎設施構建，其主要具備五大特性：

(一)去中心化

區塊鏈最大的特性就是「去中心化」，採用點對點分散式儲存技術，無須第三方驗證機構單位，亦無統一的中央伺服器，資料是由節點與節點之間共同維護，並驗證訊息真實性，避免對單一或少數中心節點的高度依賴問題。

(二)匿名性

在區塊鏈上各節點以不具名方式參與，透過密碼學原理，並使用一組「英文＋數字」的代碼作為名稱，節點與節點之間遵循共識機制演算法，共同維護帳本，各節點之間可以基於交易錢包與交易地址而非個人身分進行資料交換。

(三)不可竄改性

區塊鏈上的資料採用密碼學雜湊函數原理，該函數具有不可逆之單向性，因此存在於鏈上產生的數據資料是無法被任意修改的，透過共識演算法機制，每個區塊鏈上的節點都共同維護總帳的副本，而副本分布式存儲在不同的位置，[20] 單一節點亦無法任意竄改交易紀錄。

(四)公開透明永久保存

區塊鏈網路上各節點都可以參與共享數據的記錄、維護，同一區塊鏈上資料均相同，所有成員都可以查看交易的完整記錄，[21] 具有公開透明性。另區塊鏈上資料依據時間順序環環相扣，屬於區塊鏈式數據結構，使得區塊鏈資料具有可追溯性，並且永久保存。

(五)共識機制

為了解決資訊同步與防止竄改的問題，每一種區塊鏈系統須採用某一種共識機制使安全性和唯一性有共同管制規範，當新的區塊被廣播到整個區塊鏈網路，節點必須驗證並接受或拒絕新區塊，如果多數人能夠達成協議，就可以達成共識，[22] 目前較成熟的共識機制區分為工作量證明、權益證明及股份授權證明，摘述如下：

1.工作量證明(Proof of Work, PoW)

比特幣和最初期的以太坊採用PoW協議，是一種依賴機器進行數學運算，各節點透過大量消耗電腦資源、來解決一道數學難題，最先解決難題的節點獲得記帳權，計算時間取決於機器的雜湊運算速度，每次達成共識需全區塊鏈共同參運算，共識機制高，性能效率低，[23] 如圖2所示。

20 Tonghe Wang, Haochen Hua, Zhiqian Wei, Junwei Cao, "Challenges of blockchain in new generation energy systems and future outlooks," *International Journal of Electrical Power & Energy Systems*, Vol.135, February 2022.

21 Nicola Friedman and Jarrod Ormiston, "Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains," *Technological Forecasting and Social Change*, Vol.175, February 2022.

22 同註20。

23 Sarah Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Systems with Applications*, Vol.168, April 2021.

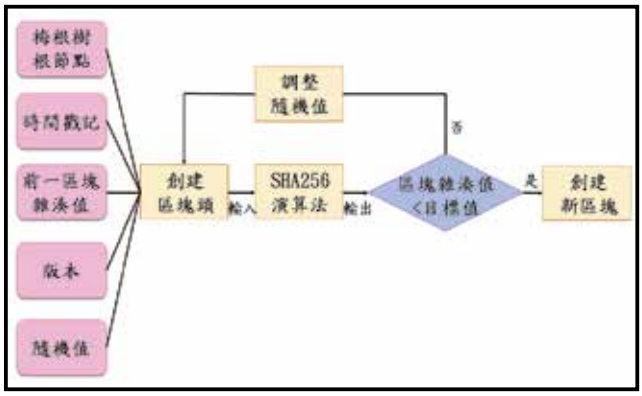

圖2　工作量證明流程圖 [24]

2.權益證明(Proof of Stake, PoS)

獲得節點記帳權的難度與節點持有的權益成反比，根據節點持有權益（幣）的比例，等比例降低挖礦難度，相較PoW減少了數學運算帶來的資源消耗，性能方面相對提升，但仍然是基於雜湊運算競爭獲取記帳權，[25] 如圖3所示。

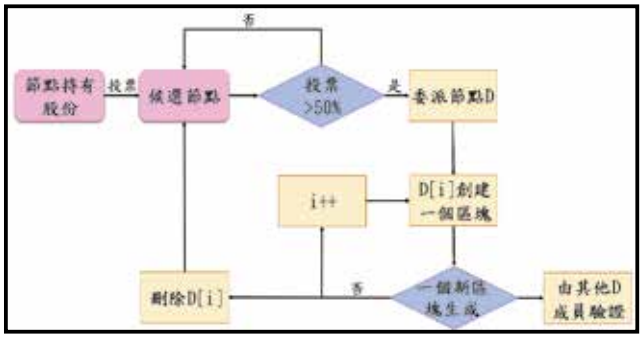

圖3　權益證明流程圖 [26]

3.股份授權證明(Delegated Proof of Stake, DPoS)

為了加快交易速度，DPoS機制原理類似於董事會投票，持有貨幣者投票選出一定數量的節點，進行代理驗證和記帳，參與者將權利授權給受託人，每個股東根據持有比例擁有相對應的影響力，縮小參與驗證和記帳節點的數量，加速共識驗證，與PoS主要區別在於節點選取代理人，由代理人進行驗證和記帳，[27] 如圖4所示。

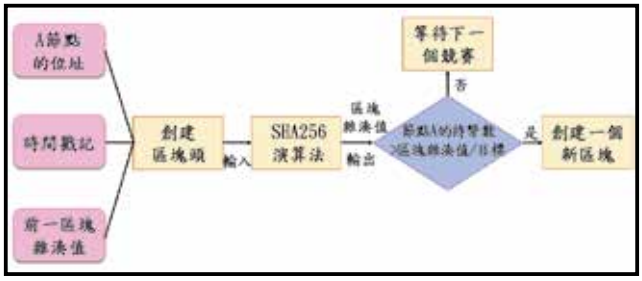

圖4　股份授權證明流程圖 [28]

四、智慧合約與去中心化應用程式

於1994年由一位法學家、電腦科學家及密碼學專家的學者尼克．薩博(Nick Szabo)提出智慧合約(Smart Contract)的概念，並定義為：「一套以數位形式之承諾，合約參與方可以在此執行協議」，將此協議程式化，透過電腦自動執行，[29] 而以太坊的創辦者維塔利克．布特林(Vitalik Buterin)於2014年發

24 Shijie Zhang and Jong-Hyouk Lee, "Analysis of the main consensus protocols of blockchain," *ICT express*, Vol.6, No.2, June 2020, pp. 93-97.

25 Sunny King and Scott Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," 2012/8/19, <https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf>（檢索日期：2022年3月21日）

26 同註24。

27 徐明星、田穎、李霽月，《圖解區塊鏈》（臺北：碁峰資訊股份有限公司，2017年），頁96-102。

28 同註24。

29 Szabo Nick, "Smart Contracts," 1994, <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>（檢索日期：2022年5月14日）

表了一份以太坊白皮書「下一代智慧合約和分散式應用平臺」，希望能將區塊鏈技術應用在加密貨幣以外之領域，書中說明以太坊提供一種完全成熟且圖靈完備的編程語言，相容各種區塊鏈的運用，允許用戶編寫智慧合約和分散式應用程序。[30] 利用Solidity編程語言編寫函數、事件和狀態，在編譯過後，智慧合約代碼被轉換為EVM代碼執行，並透過智慧合約建立交易，被識別為唯一的合約地址存儲在以太坊區塊鏈上。[31] 可以為所有權、交易格式和狀態轉換函數制定規則，透過智慧合約可建構一個無需信任基礎的去中心化應用程式平臺，並使區塊鏈的相關技術及其應用更為豐富多元化及自由。[33] 一份智慧合約通常由合約主體、數位簽章、合約條款及去中心化平臺等四要素所組成，[34] 使用程序邏輯來實現交易的合約條款，並減少例外情況，[35] 其中各種不同的區塊鏈平臺所執行的智慧合約會有部分差異，然而智慧合約運作的概念，皆是以「事件驅動」的模式運行，[36] 工作原理如圖5所示。

圖5　智慧合約工作原理 [32]

一般Web應用程式App是運行在TCP/IP四層模型上的中心化服務器的應用程式，而去中心化應用程式(Decentralized Application, DApp)主要是運行在區塊鏈技術所開發的應用程式，應用程式必須開源且可以自動運行，結合智慧合約和前端介面，不依賴中心化的伺服器，透過該程式能使用戶直接與區塊鏈互動，[37] DApp結合智慧合約和前端介面，不依賴中心化的伺服器，具有區塊鏈去中心化的特性，可以自動運行，所有的數據皆公開透明且不可竄改。當去中心化應用程式在區塊鏈點對點網路上運作時，必需花費燃料執行，這些燃料通常是使用DApp上流通的加密貨幣，例如以太坊(Etherum)。

五、自我認證

馬克．吉奧特(Marc Girault)於1991年提

30 Vitalik Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, 2014, <https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf>（檢索日期：2021年11月18日）

31 Satpal Singh Kushwaha, Sandeep Joshi, Dilbag Singh, Manjit Kaur, & Heung-No Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, Vol.10, January 2022, pp. 6605-6621.

32 吳銳、劉導，《區塊「鏈」接智能》（北京：電子工業出版社，2018年），頁46-50。

33 吳壽鶴、馮翔、劉濤、周廣益，《比特幣out、以太坊in超越交易實作區塊鏈技術》（臺北：佳魁資訊，2018年），頁18-39。

34 夏君和，《建構具安全性的智慧合約共享方案—以房屋共享為例》（臺北：國防大學資訊管理學系研究所碩士論文，2021年）。

35 蘇品長、夏君和、蘇泰昌，〈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》，第29卷第3期，2022年7月，頁253-275。

36 陳英倫，《區塊鏈與智慧合約在數位學習平台上之應用》（臺中：東海大學資訊工程研究所碩士論文，2018年）。

37 Zigui Jiang, Kai Chen, Hailin Wen, & Zibin Zheng, "Applying blockchain-based method to smart contract classification for CPS applications," *Digital Communications and Networks*, September 2022.

出自我認證公開金鑰密碼系統，於授權階段由憑證中心與使用者雙方共同參與公開金鑰的計算，於驗證階段可進行自我驗證的演算法；由於公鑰是由憑證中心及使用者兩方計算所得，可透過雙方傳送之公開資訊，達成身分的確認，無須透過公正第三方即可達成身分的確認，此種身分認證方式相較一般以憑證授權中心為基礎的公開金鑰密碼系統，先決條件須建立在憑證中心的安全性與公正性。

在自我認證機制中，由於私鑰是由使用者自行建立，憑證中心無法得知使用者私鑰，可避免憑證中心偽冒使用者問題；在運作上，使用者先利用自己的私鑰驗證公鑰之正確性，驗證無誤後，再以私鑰與通訊方之公鑰進行金鑰協議，可降低系統在公鑰儲存、計算與管理之成本與風險，並提升安全性。[38]

參、區塊鏈技術應用於國防採購

隨著網路普及發達，為了鼓勵中、小型企業參與公共採購、招標，近年來政府機關單位積極提倡電子化採購(E-Procurement)作業，是一個利用網際網路作為基礎交易的平臺，由行政院公共工程委員會建置「政府電子採購網」，包含「公開取得電子報價單」、「公開閱覽、徵求公告」、「共同供應契約系統」、「領標管理系統」、「投標管理系統」、「開標管理系統」、「決標管理系統」、「流廢標管理系統」等相關系統開發，[39]電子採購流程（如圖6所示），快速傳遞訊息、設計完善的安全演算法及安全管控機制，並配合電子簽章法使其具備法律的效力，並受法律規範，減少採購所需的大量人力、繁雜的文書往返及作業流程。[40]國防採購為支援國軍建軍備戰之重要手段，亦屬於政府採購之一環，主要目的是依照戰備演訓任務所需，在依法行政之體制下，以經濟有效之方式，整體衡量與評估品質、時效與價格等因素，以期能如期、如質、如預算獲得建軍整備之工程、財物、勞務，支援國軍戰備需求。[41]

「肅貪防弊、依法行政」是國軍各級持續要求的重點工作，為使國軍各級辦理採購作業，均能依法行政，維持廉潔軍風，各

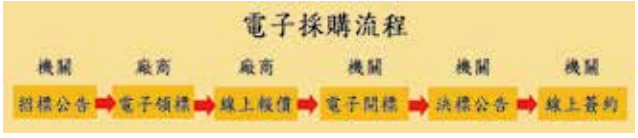

圖6　未達公告金額之工程、財物採購流程圖[42]

38 Marc Girault, "Self-certified public keys," In Workshop on the Theory and Application of of Cryptographic Techniques (Berlin: Heidelberg, 1991), pp. 490-497.

39 行政院公共工程委員會，《政府電子採購網》，<https://web.pcc.gov.tw/pis/>（檢索日期：2022年5月28日）

40 蘇品長，〈適用於國軍電子採購的盲簽章系統設計〉，《國防管理學報》，第29卷第2期，2008年11月，頁51-62。

41 蘇品長、蕭柏薰、陳明心，〈強化團軍電子採購業務—具自我認證暨多文件盲簽章機制之設計〉，《國防管理學報》，第36卷第1期，2015年5月，頁47-64。

42 行政院公共工程委員會，〈第三代政府電子採購網教育訓練簡報〉，《政府電子採購網》，<https://web.pcc.gov.tw/pis/prac/downloadGroupClient/getClientDownloadForDownloadFile?id=60000076>（檢索日期：2022年6月20日）

級主官管須三令五申一再宣導採購人員勿因一時貪念與廠商有不當往來、收受賄賂或其他不正當之利益，並定期由業管部門舉辦採購講習，要求承辦採購相關人員熟悉作業規定，秉持「毋枉毋縱」之精神，另由監察、保防部門擔任監管角色，降低貪瀆等違法情事肇生，惟國軍仍有部分人員因心存貪念、圖利廠商、收受賄賂等，進而肇生多起涉嫌採購弊案。研究中顯示，區塊鏈技術有助於提高招標流程的效率，並降低中、小型企業、供應商參與政府採購的成本，並確保承包商和分包商按照採購契約履行合約標的。[43] 負責監督日本行政制度、管理地方政府的總務省自2017起即開始利用區塊鏈系統處理政府標案，並藉此將各政府承辦單位連結，彼此共享數據，提高現有招標流程的效率；[44] 另美國總務署(General Services Administration, GSA)也正積極投入研究，如何透過區塊鏈技術改善中、小型供應商參與政府合約競標的審查方式，期望能建立一套系統，簡化審查流程；[45] 惟使用區塊鏈系統架構需要考慮一些因素，如區塊生成率、交易速度和區塊大小，目前比特幣在公有鏈上平均每秒處理7筆交易，而在區塊鏈交易性能方面，2020年由多名學者提出一份研究調查基於區塊鏈安全電子投票系統的性能限制中，分別在公有鏈及私有鏈建立了一個測試平臺，並監測相關實驗數據，包含區塊可以容納的最大投票交易數，區塊當前可以承載的平均投票交易數，投票交易大小，最大交易處理速度及系統當前的操作交易處理速度，結果顯示在公有鏈上每分鐘可達16,000筆投票交易，在私有鏈上模擬222,000筆交易從7個不同的客戶端發送，計算單個交易花費的平均時間大約是0.1秒，證明區塊鏈在公有鏈及私有鏈上交易速度對投票過程是穩定的，[46] 而國防部每年依照年度施政目標，配合核定預算額度，編定年度施政計畫，在近五(2017～2021)年度，公開招標案件平均計520件，[47] 如表2所示，案件交易量相較投票系統而言，在區塊鏈網路中具可擴展性。

故本研究提出以區塊鏈技術為底層架構，結合橢圓曲線離散對數難題之盲簽章技術、自我認證及密碼學原理，設計一個符合國軍所需之安全可信任電子採購機制，根據區塊鏈去中心化的程度及參與者類型之間的差異，採用私有鏈為本研究設計之原型，以符合國軍採購系統中參與者身分及權限控制的要求，憑證系統負責身分驗證，產生公鑰和私鑰，提供簽章、加密及驗證功能，並

43 Maxat Kassen, "Blockchain and e-government innovation: Automation of public information processes," *Information Systems*, Vol.103, January 2022.

44 威少，〈日本正為政府招標系統測試區塊鏈技術〉，《區塊客》，2017年8月1日，<https://blockcast.it/2017/08/01/japan-to-test-blockchain-for-government-contract-system/>（檢索日期：2022年1月28日）

45 許裕佳，〈區塊鏈促進微中小企業參與國際貿易之機會與挑戰〉，《經濟前瞻》第187期，2020年1月，頁100-105。

46 Kashif Mehboob Khan, Junaid Arshad, & Muhammad Mubashir Khan , "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, Vol.105, April 2020, pp. 13-26.

47 環通資訊股份有限公司，〈單位別年度招標決標案件統計〉，《臺灣採購公報網》，<http://www.taiwanbuying.com.tw/ShowOrgStat.asp?orgid=6729>（檢索日期：2022年6月25日）

表2　國防部歷年招標案件數量及金額統計表

項次	年度	案件數量	年度總金額	備考
1	2017	540	NT$70,701,198,341	民國106年
2	2018	498	NT$101,158,250,524	民國107年
3	2019	525	NT$350,662,721,074	民國108年
4	2020	542	NT$102,790,201,466	民國109年
5	2021	499	NT$130,420,274,682	民國110年

資料來源：環通資訊股份有限公司，〈單位別年度招標決標案件統計〉，《臺灣採購公報網》，<http://www.taiwanbuying.com.tw/ShowOrgStat.asp?orgid=6729>.（檢索日期：2022年6月20日）

透過Remix開發環境以Solidity語法將國防採購運作各階段流程之邏輯，開發轉換為智慧合約，利用Visual Studio Code編輯器，結合HTML和CSS代碼來開發DApp，編寫前端網頁JavaScript及Web3.js，來實現前端網頁的交互邏輯，終端使用者可以透過該前端網頁呼叫智慧合約功能來執行各階段步驟，使系統可自動化執行採購流程，最後採用橢圓曲線盲簽章技術確保投標廠商在投標過程的隱私性受到安全的保護機制，並運用加密技術傳送，於開標決標階段達到可驗證性、不可偽造性及不可否認性，以下將針對系統架構及作業流程實施說明：

一、系統架構

本研究以區塊鏈、智慧合約、盲簽章及自我認證機制為設計基礎，根據區塊鏈去中心化的程度差異，可區分為公有鏈、聯盟鏈及私有鏈，為符合國防採購身分驗證的需求，本研究機制採用私有鏈，規劃於國防採購相關單位、投標企業及廠商設立節點，共同維護鏈上資料，而區塊鏈上每筆交易採用橢圓曲線數位簽章演算法(Elliptic Curve Digital Signature Algorithm, ECDSA)加密，並運用雜湊函數(Hash Function)，將長度不一的訊息輸入，演算成固定長度的雜湊值輸出，將雜湊值廣播給各節點，確保交易資料不被竄改，而每個帳戶擁有一對「私鑰」(Private Key)和「公鑰」(Public Key)，交易發起人使用私鑰對交易簽章，區塊鏈上任何人都可使用公開的對應公鑰，對交易進行驗證。

在憑證申請階段系統導入Girault所提出的公開金鑰密碼系統中安全等級3的自我認證機制，取代中心化的憑證伺服器，所有參與者向憑證中心實施身分註冊，取得公、私鑰及簽章憑證，接續由採購機關將設計之智慧合約部署至區塊鏈上，並依照國軍電子採購作業流程透過智慧合約於區塊鏈上進行招標、領標、投標、開標及簽約交易，並運用密碼學盲簽章機制，達到可驗證性、不可偽造性及不可否認性，本機制之參與者均可透過DApp上之智慧合約查詢招標文件資訊檔案，並於開標後可驗證鏈上所有投標交易紀錄，系統運作架構如圖7所示。

二、協定參與者

執行採購作業流程參與者包含憑證中心、承辦單位、採購機關、投標廠商及區塊鏈網路，分別說明如下：

(一)憑證中心：為身分憑證核發單位，負責產生公鑰和私鑰，使系統中參與者可透過公鑰進行加密，私鑰進行解密。

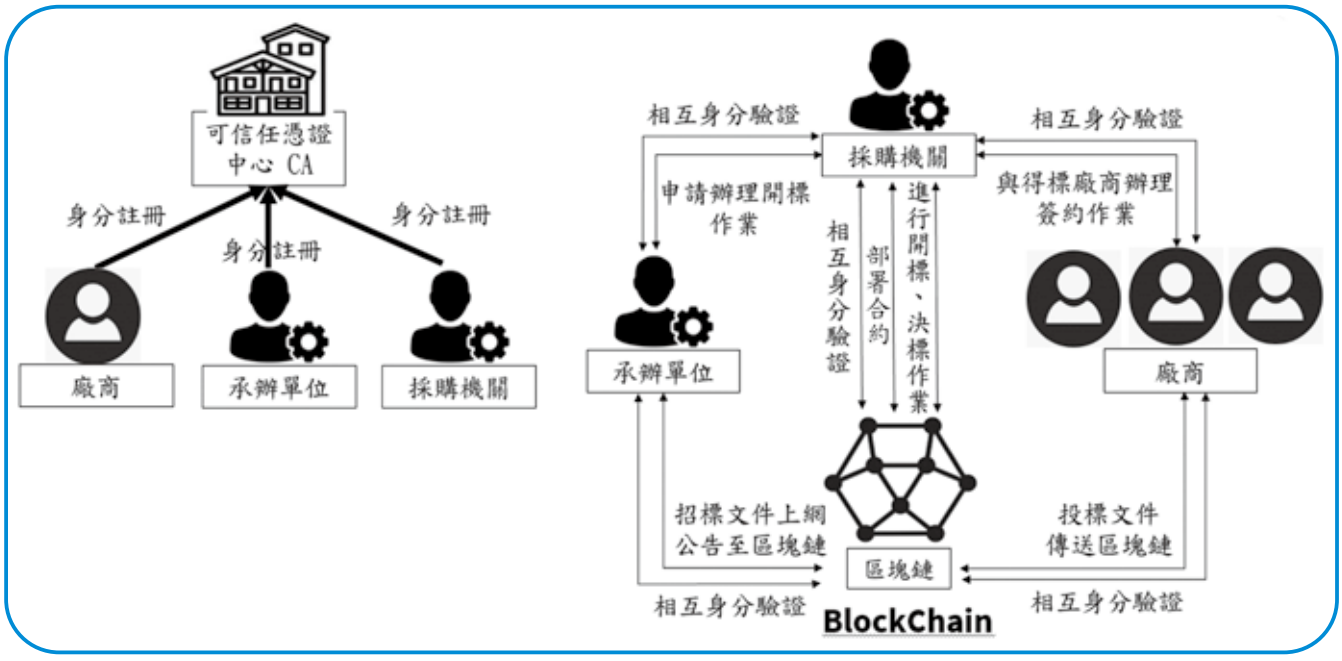

圖7　本研究提出之系統架構圖

資料來源：本研究整理

(二)承辦單位：為採購需求方，於身分註冊後，以其公鑰加密標案資訊及價格，並將採購案件，傳送至採購機關。

(三)採購機關：為辦理採購開標服務單位，並將智慧合約程式部署至區塊鏈網路，負責執行開標、決標作業。

(四)投標廠商：為欲投標之廠商，在系統中找到欲投標之標案，並經身分核對無誤後，即可透過智慧合約執行投標作業。

(五)區塊鏈網路：具有去中心化、各參與節點共同維護、數據透明及不可竄改等特性，有助於建立公開、透明及彼此信任之國防採購機制，並透過智慧合約，來查詢儲存於區塊鏈網路之資訊。

三、作業流程

系統作業流程區分身分註冊階段、部署智慧合約、招標階段、領標階段、投標階段、開標階段、簽約階段等7階段，分述如下：

(一)身分註冊階段

首先由採購作業參與人員透過自我認證方式分別向憑證中心申請憑證，參與者以自身身分資訊及隨機參數產生簽名檔，傳送至憑證中心註冊，憑證中心傳回驗證公鑰及憑證簽章，並由參與者自行計算公鑰與私鑰，可避免憑證中心產生偽冒使用者的問題，同時可降低系統公鑰儲存、計算與管理的風險，藉由該電子憑證可相互識別用戶之身分，確保身分合法性，並將憑證資料作為後續收受電子招標文件、領標、電子投標文件、電子押標金、電子保證金之保證書、開標、決標、訂購及付款等之憑據。

(二)部署智慧合約

採購機關取得憑證中心橢圓曲線公開參數，將所設計之智慧合約部署至區塊鏈上，相關協議編碼程式化，由電腦自動執行，建構一個無需信任基礎的去中心化應用平臺，使參與者透過分散式應用程序完成採

購過程中招標、領標、投標、開標及決標等相關作業，達成系統自動化。

(三)招標階段

於承辦單位於完成採購作業程序簽核後，將採購案向採購機關申請完成招標作業，並將招標文件公告上傳至區塊鏈系統，由於區塊鏈具備「公開透明」、「不可竄改」之特性，所有參與人員均可公開閱覽招標文件、驗證並防止竄改，並避免廠商任意重製、轉載或篡改電子招標文件。

(四)領標階段

廠商於電子採購系統中搜尋相關標案，完成標案領標費用繳費，並於完成繳費後，透過系統下載領標憑據電子檔及標案文件，後續以此電子憑據作為電子投標之依據。

(五)投標階段

廠商將投標文件透過盲簽章、數學演算法及加密技術傳送，並由採購機關系統賦予電子投標文件編號、完成數位簽章、附加時間戳記、最後將投標文件封存，並製作投標文件電子憑據給予投標廠商作為證明，透過電子簽章及加密技術可確保投標文件真實性及保密性，並於區塊鏈系統中，透過「去中心化」特性，防止遭受暴力威脅恐嚇，避免投標文件在傳輸過程中資訊遭攔截、竄改，影響投標結果。

(六)開標階段

於投標期限截止時，由採購機關觸發智慧合約，停止投標作業，並以開標用之憑證取得廠商投標之對稱式金鑰，再以該對稱金鑰將電子投標文件解密，核對簽章及廠商身分後，將投標結果公告於區塊鏈，執行電子開標、決標，過程中均於區塊鏈上執行並記錄，可確保資訊達到完整性、不可否認性及真實性，可加強其安全強度。

(七)簽約階段

系統發予得標廠商合約書，依照招標文件中所訂之規範，由採購機關與得標廠商於期限內完成電子投標文件簽約，並驗證簽章正確性及檢視廠商完成合約書內容填製。

肆、區塊鏈應用於國防採購安全性分析

藉由區塊鏈「去中心化」、「防竄改」且「資訊公開透明」等技術應用於國防採購作業進行安全性探討與檢視分析，預期可達到ISO組織所提出之資訊安全管理需求之安全特性，其中包含資訊之機密性、完整性、不可偽造性、不可否認性、不可竄改性、不可追蹤性、鑑別性、資料可追溯、抗中間人攻擊等安全需求，並針對國軍現行電子化採購系統與本研究比較各項安全性（如表3所示），分述如下：

一、機密性

機密性是指在傳輸或交易期間，不得被未經授權之個人、實體或程序所取得或揭露的特性，只有經授權的人或程序才可以取得資訊，內容都是被保密的，不被傳送及接收雙方以外的人獲知內容之特性，以避免資料外洩，在本研究中投標文件內容明文訊息經由雜湊運算得，若第三方竊取這些加密資訊，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投標文件機密性。

二、完整性

完整性是確保資料在傳遞過程中不會被任意變更竄改或破壞，其內容保持完整且正確一致，在區塊鏈系統傳遞過程中內容不能被任意增減或修改，並且可確認是由傳送方

表3　電子採購系統比較表

項目	國軍現行電子採購系統	本研究提出
機密性	○	○
完整性	○	○
不可僞造性	○	○
不可否認性	○	○
不可竄改性	X	○
不可追蹤性	○	○
鑑別性	○	○
資料可追溯性	X	○
抗中間人攻擊	X	○
註：○：符合、X：不符合		

資料來源：本研究整理

所發出，因此投標文件上傳至區塊鏈系統，可確保資料完整一致。另在本研究中，採購機關簽章之投標文件是利用單向雜湊函數雜湊出來的，因單向雜湊函數具不可逆推之性質，若途中遭攔截所發送之密文並修改，產出之密文摘要則不一致，於比對驗證時將無法通過，如此可以確保招標及投標文件內容是正確且完整的。

三、不可偽造性

不可偽造性是指只有授權方才能簽署投標文件，資料在傳遞的過程中，不會遭到惡意第三方偽造資料內容。在本研究中，第三方若想自行偽造文件或偽造簽章，必須得到採購機關之私密金鑰，然而想獲得密鑰將會面臨橢圓曲線離散對數的問題；另於決標後簽約階段，任何人能夠經由參數驗證得知文件或簽章是否遭偽造。

四、不可否認性

不可否認性是指在交易的過程，對一個已經發生的行動或事件之證明，傳送方無法否認其交易行為。本研究參與交易各方之公、私鑰對皆是經由向憑證中心註冊所得，僅有採購機關才能簽署合法的盲化投標文件訊息，而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，達到不可否認性。

五、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。在本研究中基於區塊鏈技術建構電子採購系統，所有合法的參與者均須透過區塊鏈上完成身分認證及執行電子招標、投標、開標、決標等交易動作，區塊鏈特性上資料公開透明，並以雜湊函數將每一區塊鏈結，因此如資料遭竄改，內容雜湊值將遭發現，故具有不可竄改性。

六、不可追蹤性

不可追蹤性是指投標文件內容，不可被任何人知道。本研究透過盲簽章機制，採購機關（簽章者）僅知道這些文件是經由自己簽署的，因盲因子是由廠商（送簽者）隨機產生的，因此採購機關無法得知其投標文件真正的內容，達到不可追蹤性。

七、鑑別性

鑑別性是指接收方可利用公開參數驗證訊息來源的合法性，以確保訊息是由傳送方所傳送的，使用者的公鑰與密鑰有唯一的對應關係，只有使用者的密鑰才能對應使用者的公鑰，因此藉由金鑰對可達到鑑別使用者身分的功能。在本研究中各成員皆已完成身分註冊，在執行各項採購作業階段時，均能由公鑰及相關參數進行相互身分驗證。

八、資料可追溯性

可追溯性是指電子招標、領標、投標等交易資訊可以溯源，每一筆紀錄儲存於區塊鏈系統中，都可以完整追溯其過程，進而打造完整的電子採購系統，當出現採購爭議時，可透過智慧合約查詢相關紀錄，確保交易合法性。

九、抗中間人攻擊

中間人攻擊指的是當攻擊者假冒或偽造數據身分，攔截通訊雙方的訊息並插入新的內容，破壞整個運作流程，而不被其他終端識破。本研究設計以自我認證方式，確認每一參與者在交易前均須完成相互認證，確保參與者合法身分，始可執行交易動作，另於電子投標過程均由需求方完成簽章，由接收方執行驗證，可有效抵抗中間人攻擊。

伍、結　　語

區塊鏈是一種「去中心化」、「不可竄改」、「公開透明」的分散式帳本，提供一套安全、透明、可驗證、穩定且高效的交易模式。近年來技術已紛紛導入各項產業鏈，如數位身分、醫療、供應鏈、學歷證書等，並成為10大科技趨勢，而國軍採購系統基礎建設經過多年努力已相當完善，並全面電子化，本研究運用區塊鏈安全特性，應用於國防採購作業之應用，所有資訊皆公開於區塊鏈上，使開標作業無人員干涉且無法竄改，可供查詢及驗證，強化國軍內部系統安全，另將智慧合約部署於區塊鏈上，使國軍人員可依循規範及流程實施採購作業，透過資訊技術大幅減少第三方惡意干涉之風險，建立一個公開、透明及安全的國軍電子化採購流程，並透過密碼學盲簽章及自我認證機制，降低系統運算成本，提高效能，達到ISO組織所提出之機密性、完整性、鑑別性、不可竄改、不可追蹤、不可偽造、不可否認性等資安特性，符合「資安即國安」之國防戰略。相較現行國軍電子採購系統，除可滿足政府採購法之資訊公開透明外，亦可保護投標人隱私、降低第三方參與度、抵抗中間人攻擊，達成軍事採購資料保密安全的原則，杜絕圍標、綁標之不法情事，強化國軍電子化採購作業安全性。

國防採購為支援國軍建軍備戰之重要手段，而國防科技為軍事作戰核心力量，在目前經濟衰退及不景氣的嚴峻環境下，國防預算日益緊縮，如肇生國軍採購弊端，將嚴重損害人民對國軍的信賴，並可能延遲獲得國軍建軍作戰所需之裝備及後勤補給，進而使國防安全遭到嚴重威脅，因此將區塊鏈技術應用於國防採購作業，一旦成功應用，未來將打破傳統軍事採購作業流程，帶來軍事發展的革命性變革，國軍於辦理各項工程、財務及勞務採購，從計畫申購、尋商訪價、上網公告、公開招標、簽約、履約驗收、付款到最終會計入帳，將大幅降低採購弊端與人力管理成本，有效提升整體戰力，達到廉潔軍風及支援建軍備戰之目標。

（收件：111年7月4日，接受：111年9月9日）

參考文獻

中文部分

專書

吳壽鶴、馮翔、劉濤、周廣益，2018。《比特幣out、以太坊in超越交易實作區塊鏈技術》。臺北：佳魁資訊。

吳銳、劉導，2018。《區塊「鏈」接智能》。北京：電子工業出版社。

徐明星、田穎、李霽月，2017/11。《圖解區塊鏈》。臺北：碁峰資訊股份有限公司。

黃步添、蔡亮，2020/03。《區塊鏈改變未來的倒數計時》。臺北：清文華泉事業有限公司。

期刊論文

王崑義，2010。〈非傳統安全與臺灣軍事戰略的變革〉,《臺灣國際研究學會臺灣國際研究季刊》，第6卷第2期，頁1-43。

孫志宏，2021。〈淺談維護海軍後勤採購的廉潔環境〉，《海軍學術雙月刊》，第55卷第5期，頁87-99。

許裕佳，2020/01/12。〈區塊鏈促進微中小企業參與國際貿易之機會與挑戰〉，《經濟前瞻》，第187期，頁100-105。

彭錦珍，2005。〈科技對世界軍事革新及其發展的影響〉，《復興崗學報》，第84期，頁55-80。

謝之鵬，2005。〈美軍軍事變革對兩次波灣戰爭影響—兼論兩岸之對應作為〉,《國防雜誌》，第20卷第11期，頁103-115。

蘇品長，2008。〈適用於國軍電子採購的盲簽章系統設計〉，《國防管理學報》，第29卷第2期，頁51-62。

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》，第29卷第3期，頁253-275。

蘇品長、蕭柏薰、陳明心，2015。〈強化國軍電子採購業務—具自我認證暨多文件盲簽章機制之設計〉，《國防管理學報》，第36卷第1期，頁47-64。

學位論文

余庭儀，2020。《植基於智慧合約的數位內容交易電子支付方法》。臺北：國防大學資訊管理學系研究所碩士論文。

夏君和，2021。《建構具安全性的智慧合約共享方案—以房屋共享為例》。臺北：國防大學資訊管理學系研究所碩士論文。

陳英倫，2018。《區塊鏈與智慧合約在數位學習平台上之應用》。臺中：東海大學資訊工程研究所碩士論文。

網際網路

Liu Jason，2019/07/30。〈美國國防部正透過區塊鏈技術，開發網絡安全防護系統〉，《動區動趨BlockTempo網》，<https://www.blocktempo.com/us-department-of-defense-is-developing-a-blockchain-cybersecurity-shield/>。

Sphinx，2021/11/16。〈臺灣透明組織公布2020年世界各國「政府國防廉潔指數」我國得分70分與德國並列全球第六名，歸類為B級，屬低度風險國家〉，《臺

灣透明組織協會全球資訊網》，<https://www.tict.org.tw/%E5%8F%B0%E7%81%A3%E9%80%8F%E6%98%8E%E7%B5%84%E7%B9%94%E5%85%AC%E5%B8%832020%E5%B9%B4%E4%B8%96%E7%95%8C%E5%90%84%E5%9C%8B%E3%80%8C%E6%94%BF%E5%BA%9C%E5%9C%8B%E9%98%B2%E5%BB%89%E6%BD%94%E6%8C%87/>。

中華民國國防部，110/11/17。〈國防部發布新聞稿說明「我國國防廉潔指數評鑑為『B』等級，世界排名第6」〉，《中華民國國防部全球資訊網》，<https://www.mnd.gov.tw/Publish.aspx?p=79317&title=%E5%9C%8B%E9%98%B2%E6%B6%88%E6%81%AF&SelectStyle=%E6%96%B0%E8%81%9E%E7%A8%BF>。

行政院公共工程委員會，《政府電子採購網》，<https://web.pcc.gov.tw/pis/>。

行政院公共工程委員會，2022/06。〈第三代政府電子採購網教育訓練簡報〉，《政府電子採購網》，<https://web.pcc.gov.tw/pis/prac/downloadGroupClient/getClientDownloadForDownloadFile?id=60000076>。

李淑惠，〈2020年十大科技趨勢：以人為本的智慧空間將持續推動科技發展〉，《中時新聞網》，2019年10月31日，<https://www.chinatimes.com/realtimenews/20191031003646-260410?chdtv。

威少，2017/8/1。〈日本正為政府招標系統測試區塊鏈技術〉，《區塊客》，<https://blockcast.it/2017/08/01/japan-to-test-blockchain-for-government-contract-system/>。

陳俊明、莊文忠、李宗模、郭宗城，2019/12/16。〈政府國防廉潔指數於國防政策之應用與實踐〉，《國防部政風室》。<https://ethics.mnd.gov.tw/userfiles/files/%E6%94%BF%E5%BA%9C%E5%9C%8B%E9%98%B2%E5%BB%89%E6%BD%94%E6%8C%87%E6%95%B8%E6%96%BC%E5%9C%8B%E9%98%B2%E6%94%BF%E7%AD%96%E4%B9%8B%E6%87%89%E7%94%A8%E8%88%87%E5%AF%A6%E8%B8%90%E8%AA%BF%E6%9F%A5%E6%A1%88-%E6%9C%9F%E6%9C%AB%E5%A0%B1%E5%91%8A%E5%AE%8C%E6%88%90%E7%89%88-20191223.pdf>。

臺灣透明組織協會，2021/11/16。〈臺灣透明組織公布2020年世界各國「政府國防廉潔指數」我國得分70分與德國並列全球第六名，歸類為B級，屬低度風險國家〉，《臺灣透明組織協會全球資訊網》，<https://www.tict.org.tw/%E5%8F%B0%E7%81%A3%E9%80%8F%E6%98%8E%E7%B5%84%E7%B9%94%E5%85%AC%E5%B8%832020%E5%B9%B4%E4%B8%96%E7%95%8C%E5%90%84%E5%9C%8B%E3%80%8C%E6%94%BF%E5%BA%9C%E5%9C%8B%E9%98%B2%E5%BB%89%E%BD%94%E6%8C%87/>。

環通資訊股份有限公司，〈單位別年度招標決標案件統計〉，《臺灣採購公報網》，<http://www.taiwanbuying.com.tw/ShowOrgStat.asp?orgid=6729>。

外文部分

期刊論文

Berdik, David, Otoum, Safa, Schmidt, Nikolas, Porte,r Dylan, & Jararweh, Yaser, 2021/1. "A survey on blockchain for information systems management and security," *Information Processing & Management*, Vol.58, No.1.

Bouraga, Sarah, 2021/4/15. "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Systems with Applications*, Vol.168.

Efanov, Dmitry and Roschin, Pavel, 2018. "The all-pervasiveness of the blockchain technology," *Procedia computer science*, Vol.123, pp. 116-121.

Friedman, Nicola, & Ormiston, Jarrod, 2022/2. "Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains," *Technological Forecasting and Social Change*, Vol.175.

Jiang, Zigui, Chen, Kai, Wen, Hailin, & Zheng, Zibin, 2022/1. "Applying blockchain-based method to smart contract classification for CPS applications," *Digital Communications and Networks*.

Kassen, Maxat, 2022/1. "Blockchain and e-government innovation: Automation of public information processes," *Information Systems*, Vol.103.

Khan, Kashif Mehboob, Arshad, Junaid, & Khan, Muhammad Mubashir, 2020/4. "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, Vol.105, pp. 13-26.

Kushwaha, Satpal Singh, Joshi, Sandeep, Singh, Dilbag, Kaur, Manjit, & Lee, Heung No, 2022/1. "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, Vol.10, pp. 6605-6621.

Lim, Ming K., Li, Yan, Wang, Chao, & Tseng, Ming-Lang, 2021/4. "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Computers & Industrial Engineering*, Vol.154.

Lin, Iuon Chan and Liao, Tzu Chun, 2017/9. "A Survey of Blockchain Security Issues and Challenges," *International Journal of Network Security*, Vol.19, No.5, pp. 653-659.

Raj, Praveen Vijaya Raj Pushpa, Jauhar, Sunil Kumar, Ramkumar, M., & Pratap, Saurabh, 2022/5. "Procurement, traceability and advance cash credit payment transactions in supply chain using blockchain smart contracts," *Computers & Industrial Engineering*, Vol.167.

Wang, Tonghe, Hua, Haochen, Wei, Zhiqian, & Cao, Junwei, 2022/2. "Challenges of blockchain in new generation energy systems and future outlooks," *International Journal of Electrical Power & Energy Systems*, Vol.135.

Zhang, Shijie and Lee Jong-Hyouk, 2020/06. "Analysis of the main consensus protocols

of blockchain," *ICT express*, Vol.6, No.2, pp. 93-97.

Zhu, Y., Zhang, X., Ju, Zh Y, & Wang, Ch Ch, 2020/04. "A study of blockchain technology development and military application prospects," *Journal of Physics: Conference Series*, Vol.1507, No.5.

研討會論文

Girault, Marc, 1991. "Self-certified public keys," In Workshop on the Theory and Application of of Cryptographic Techniques, Berlin: Heidelberg. pp. 490-497.

網際網路

Buterin, Vitalik, 2014. "A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, <https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf>.

Gartner, "Blockchain Technology: What's Ahead?" <https://www.gartner.com/en/information-technology/insights/blockchain>.

King, Sunny and Nadal, Scott, 2012/8/19. "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," <https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf>.

Nakamoto, Satoshi, 2008. "Bitcoin: A peer-to-peer electronic cash system," <https://bitcoin.org/bitcoin.pdf>.

Soohoo, Stacey, 2021/4/19. "Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024, According to New IDC Spending Guide," <https://www.idc.com/getdoc.jsp?containerId=prUS47617821>.

Szabo, Nick, 1994. "Smart Contracts," <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.