

淺析「區塊鏈」技術之軍事應用

Analysis of Blockchain Technology for Military Applications

海軍少校 黃琬玲、蘇品長 教授

提 要：

- 一、隨著科技快速發展，作戰型態也隨之轉變，資訊化作戰成為提高戰場致勝的重要因素之一，透過資訊科技整合戰場情資、快速蒐集與分析作戰情報，協助指揮官決策下達；而在軍事領域善用資訊科技，不僅帶來眾多優點，同時也可以減少風險和提高安全性，成為一項非常重要的議題。
- 二、在國軍各式資訊系統中，多已具備備援機制，亦建立資安防護設施監控，然而在有線與無線結合之數據鏈路中，仍有資料損毀、遺失、與遭竄改之風險；透過新的「區塊鏈」技術與「密碼學」原理結合，可滿足「不可竄改」、「去中心化」、「可追溯」等特性，強化訊息安全與數據完整性。
- 三、昔日美軍致力於各項先進科技、武器技術發展，故能在「波灣戰爭」中，迅速掌握優勢，並獲取勝利。借鑑此一致勝經驗，本文蒐整「區塊鏈」發展現況，並探討如何運用區塊鏈技術優點，輔助軍事作戰(包括作戰指管、武器裝備全壽期管理、軍事後勤管理及人力資源等項目)，期能提供國軍各單位做為資訊作戰建軍備戰參考運用。

關鍵詞：區塊鏈、軍事戰力、資訊安全、作戰指揮管制、全壽期管理

Abstract

1. With the rapid development of emerging technologies, the information technology warfare model has also changed. Information technology is one of the key factors to improve the success of warfare. How to integrate combat information through information technology, quickly collect and analyze warfare intelligence, and provide commanders with the ability to make decisions. The use of IT in the military sector has become a very important issue as it brings many benefits, but also reduces risks and improves security.
2. In the various information systems of the military, although there is a system redundancy mechanism and information security facilities to

monitor and control. However, there is still a risk of data destruction, loss and tampering in wired and wireless integrated data links. Through blockchain technology and cryptographic principles, it can satisfy the characteristics of “immutability”, “decentralized,” and “traceable” to strengthen information security and data integrity, which can ensure information security.

3. During the Gulf War, the U.S. Army was committed to the development of advanced technologies, weaponry and techniques, thus maintaining a strategic advantage. Drawing on this experience, this study will collect the current status of blockchain development and explore the advantages of using blockchain technology in military warfare, including the operational command and control system, military equipment life-cycle management system, military logistics management system, and human resources management system, which can provide reference for all units of the military to build and prepare for war.

Keywords: blockchain, military combat effectiveness, information security, operational command and control, total life cycle system management

壹、前言

隨著「人工智慧」(Artificial Intelligence)、「區塊鏈」(Blockchain)、「物聯網」(Internet of Things)、「大數據」(Big Data)、「雲端運算」(Cloud Computing)等資訊科技快速發展和應用，連帶推動許多產業的轉型和創新，也逐漸地影響著人類的生活，而資訊作戰的型態也隨之不斷改變。近年來，「區塊鏈」技術已被國際研究暨顧問機構「Gartner公

司」列入「十大趨勢科技」¹，可望於2025年發展成熟，成為主流應用科技，²並預估有望在2030年創造高達3.1兆美元(折合新臺幣約94兆4,800餘億元)的產值。³由於「區塊鏈」技術日益成熟且逐漸受到各界關注，其提供金融行業的「去中心化支付系統」⁴，除有效降低交易成本，亦使交易過程透明可信，其影響涵蓋金融、商業、隱私、安全等多個層面，達成更透明、高效、可信和安全的交易模式。

許多專家學者陸續提出利用「區塊鏈

註1：國際研究暨顧問機構在2020年所列十大趨勢科技，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」、「更強大的邊緣運算」、「分散式雲端」、「自動物件」、「實用性區塊鏈」及「人工智慧安全性」。

註2：〈Predicts 2022: Prepare for Blockchain-Based Digital Disruption〉, Gartner, December 6, 2021, <https://www.gartner.com/en/documents/4009108>, 檢索日期：2023年9月23日。

註3：iThome, 〈跟上區塊鏈列車！學習實用的區塊鏈技術〉, <https://www.ithome.com.tw/pr/142417>, 2021年1月23日, 檢索日期：2023年9月22日。

註4：「去中心化支付系統」是一種不依賴中央機構(如銀行或政府)的支付方式，是一種將信任基礎建立於區塊鏈或分散式帳本技術來達成的交易，這種系統允許交易雙方直接進行交易，無需通過中間機構進行處理或授權。

其他研究

」技術的發展，除可以改變既有的作業模式外，更有望帶來軍事領域技術革新，並能在未來幾年內普及應用。「軍以戰為主，戰以勝為先」，作戰是軍事核心任務，而勝利為最終目標，傳統的軍事作戰命令下達是採用口頭、紙本傳遞方式，指揮官則需要確保指令快速、準確地傳送到每個單位，據以執行任務。隨著資訊技術發展，透過數據系統改變信文傳遞方式，建立共同的戰場圖像，方能迅速應敵接戰；⁵然未來戰場指管之需求，需要更緊密聯合的指揮機制，才能應對複雜的戰爭環境和挑戰，達到最大化的戰鬥效果。目前本軍艦艇、陸岸站臺均已具備數據指管與鏈路通信系統，如何運用先進資訊科技，將作戰部隊與作戰支援單位連結，強化共同作戰圖像功能，實現載台與作戰部隊即時訊息交換，提高戰場透明度，⁶使各階層指揮官可以同步掌握戰場動態，增強聯合作戰的實效性和可靠性，⁷這些都將是國軍指管通信系統必須持續努力的目標。

在「波灣戰爭」中，美軍致力於各項先進科技與技術的發展，因此保持戰略優勢，並迅速擊退伊拉克軍隊；然隨著現代戰爭日趨複雜，敵方的威脅也越來越趨多樣化，亦增添應對困難度。依我國《110

年國防報告書》內容提及，國軍官兵弟兄除秉持前瞻性的思維外，更應思考在面對嚴峻的敵情威脅下，如何採取積極的防禦措施、建軍備戰，並以快速提升戰力為當前首要目標，⁸其中就論述到須透過發展新的技術和戰術。因此，本文期望探討近年興起之先進技術-「區塊鏈」如何應用於軍事作戰中，俾保持戰略優勢，其中含括領域如作戰指管、武器裝備全壽期管理、軍事後勤管理及人力資源管理系統等項目；另一方面，透過分析「區塊鏈」技術的特性與其優點，導入於國軍軍事應用，並提供各單位系統運作效能升級和增強安全性之參考。

「水能載舟，亦能覆舟」，在實際運用區塊鏈技術上，仍需綜合考慮導入該技術的成本效益、安全性，以及國軍現行制度相容特性等因素。換言之，國軍在導入「區塊鏈」技術前，必須審慎的進行需求、技術評估、效益分析、風險管控等，以確保「區塊鏈」技術應用於軍事上能真正發揮最大效益與可持續性，這也是撰寫本文主要目的。

貳、認識區塊鏈技術

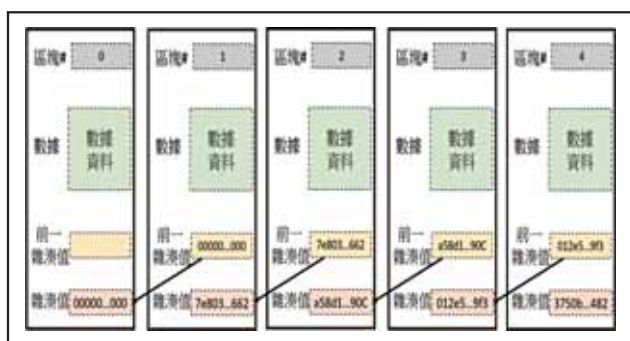
隨著「區塊鏈」技術發展飛速，除可

註5：姚樂輝，〈從美海軍戰術信文系統(MTMS)談戰場指管〉，《海軍學術雙月刊》(臺北市)，第52卷，第3期，2018年6月1日，頁19-30。

註6：曾國政，〈海軍建置「協同作戰能力」(CEC)與現行數據鏈路之研究〉，《海軍學術雙月刊》(臺北市)，第56卷，第6期，2022年12月1日，頁87-104。

註7：國防報告書編纂委員會，《中華民國110年國防報告書》(臺北市：國防部，2021年10月)，頁52-75。

註8：同註7。



圖一：「區塊鏈」結構示意圖

資料來源：參考Wang, T., Hua, H., Wei, Z., & Cao, J., "Challenges of blockchain in new generation energy systems and future outlooks," International Journal of Electrical Power & Energy Systems, Vol.135, 107499, (February 2022), p.3, 由作者彙整製圖。

提高管理效率、確保資訊安全外，並具有內容可追溯性；代表國軍如能善用「區塊鏈」技術與特性，將有助於保護機密資訊安全、降低系統資料遭竄改之風險，並可增進後勤補給管理時效與提高戰場指揮效率。以下就「區塊鏈」之起源、原理與特性，進一步探討其所能達到的特殊功效，臚列介紹如后：

一、區塊鏈緣起與原理

(一)「區塊鏈」起源於2008年，由一位自稱日裔美國人，網路化為中本聰(Satoshi Nakamoto)所提出的一篇〈點對點的電子現金協定機制〉(Bitcoin: A peer-to-peer electronic cash system)論文，⁹概念係透過一個「去中心化」(De-

centralization)平臺，將「密碼學」(Cryptology)和「分散式帳本」(Distributed Ledger Technology)技術結合至數位貨幣，在交易的過程中，無須第三方機構進行履約保證，並能讓所有成員都能參與交易的驗證和記錄；尤其若在軍中封閉的環境下，可以讓資訊更具公信力，防止不當行為和操作。

(二)區塊鏈上的資料採用密碼學「雜湊函數」(Hash Function)原理¹⁰，每個區塊內都包含容量大小、交易的資料數據內容、前一個區塊的雜湊值及該區塊雜湊值等內容，資料依據時間順序環環相扣，屬於「鏈式」(Chain Rule)數據結構(如圖一)。¹¹由於每一個區塊包含前一個區塊的雜湊值的鏈式結構，依照時間順序排列，區塊間環環相扣；當某一個區塊上的資料遭竄改時，所得到的雜湊值將會隨之改變，影響整個區塊鏈上的數據；因此，鏈上資料無法竄改，此一特性可以改善現行軍事中心化系統，可能因資料儲存不安全而遭竊取，抑或攻擊者駭入系統管理者的權限時，即能竊取大量敏感數據或對系統數據進行控制、修改等潛在風險。

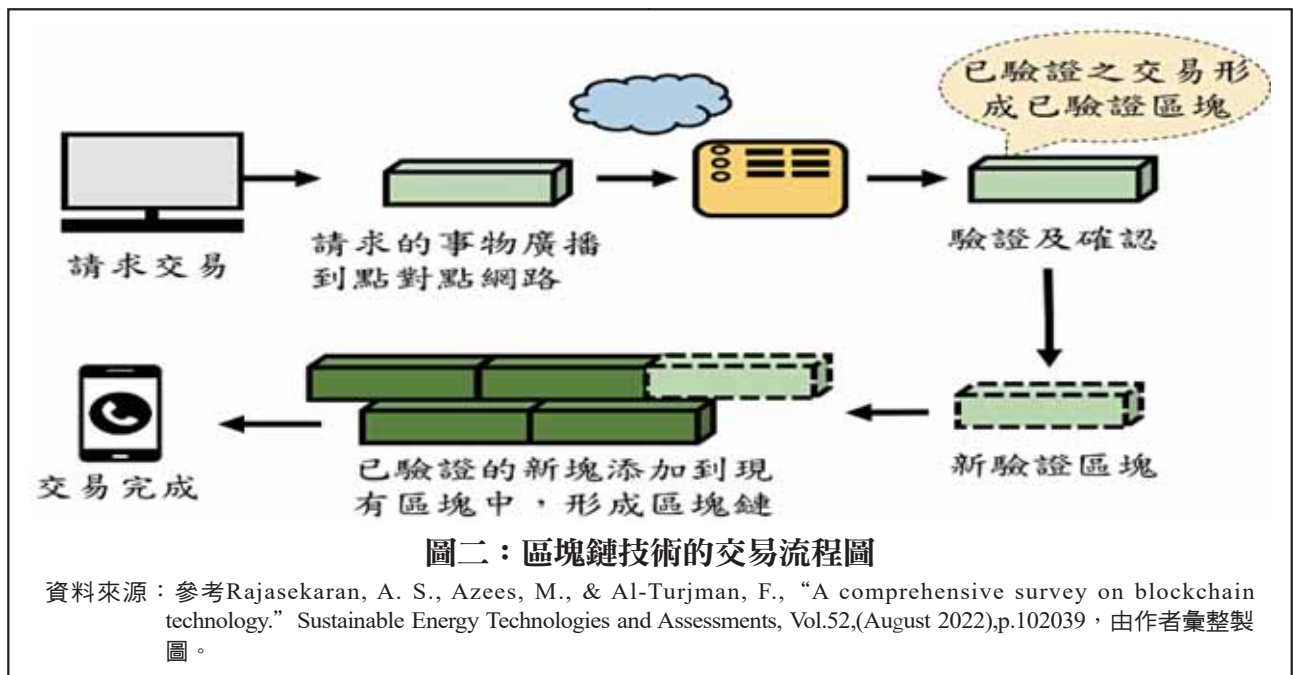
二、區塊鏈技術

(一)區塊鏈並非僅單一領域的新技術

註9：Nakamoto, Satoshi, 〈Bitcoin: A peer-to-peer electronic cash system〉, <https://bitcoin.org/bitcoin.pdf>, 2008, 檢索日期：2023年9月25日。

註10：「雜湊函數」是一種資料處理的方法，可以將任意訊息長度或資料輸入之後，轉換成為固定格式輸出的演算法，經常用於識別資料是否有被竄改。

註11：謝圓富，〈資訊戰的矛與盾 蘇特系統與區塊鏈技術〉，《海軍學術雙月刊》(臺北市)，第53卷，第2期，2019年4月1日，頁131-142。



，而是透過「對等式」(Peer to Peer)網路架構¹²，結合一連串的數學與密碼學原理所組成，又可稱為「分散式帳本技術」(Distributed Ledger Technology)，透過將資料分散儲存到每個網路節點，避免集中儲存在單一的伺服器或資料庫中，減少資料一次性遺失可能產生之風險。整個交易流程可區分為交易發起、交易驗證、完成交易。首先由交易發起者將資訊輸入到「區塊鏈」網路中，當新的資料請求加入時，「區塊鏈」上的各節點會依照「共識機制」(Consensus)¹³對新生成的資料進行驗證，檢查交易的合法性、可用性和範圍等，最後，一旦達成共識，新的區塊將被

添加到區塊鏈中，並且透過密碼學「雜湊函數」技術，成為一筆不可修改、永久保存的交易紀錄(如圖二)。

(二)透過此一運作技術的資料是經過共識機制驗證的，因此可以快速確立雙方信任感，提高交易的效率；另一方面，由於資料是同步儲存在各個節點中，可以滿足資料的長久保存，更無法被任意竄改。在國軍部隊中，利用此技術可以改善現行中心化系統資料儲存不安全，及具有最高管理者權限之問題；另於國軍現行伺服器如遇故障，可以接替啟動緊急備援機制。

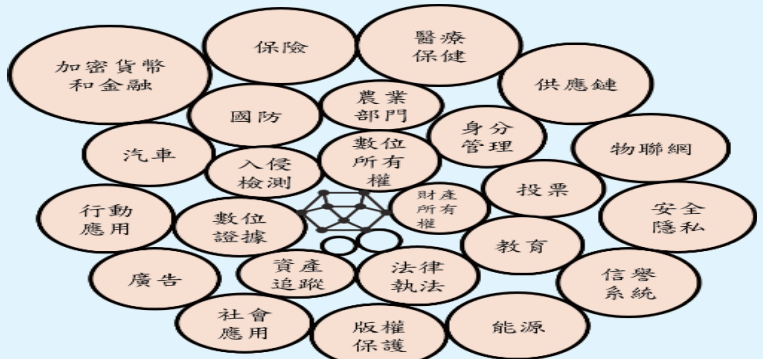
三、區塊鏈特性

(一)區塊鏈技術憑藉其不可竄改、「

註12：「對等式」網路架構是一種平等的網路架構，在網路上各個參與節點彼此可以直接進行資料及數據交換，無中央伺服器管理。

註13：在區塊鏈上每個參與者都是平等的，「共識機制」即是當新的資料上傳到區塊後，各參與者必須對這項資料進行驗證，決定接受與否，達成資訊同步。

附表：「區塊鏈」技術演進一覽表

演進	區塊鏈1.0	區塊鏈2.0	區塊鏈3.0
年代	2009-2014年	2014-2017年	2017年-
代表項目	比特幣	以太幣、超級帳本	應用於各商業項目
發展特色	以比特幣為主之數位貨幣，達成去中心化支付系統。	將「智能合約」部署至區塊鏈，主要應用於金融業。	<p>各行各業均可導入區塊鏈之應用。</p> 

資料來源：參考Guo, H., & Yu, X., "A Survey on Blockchain Technology and its security." Blockchain: research and applications, Vol.3, No.2, (June 2022), p.100067；曾偉誌，〈以智慧合約為設計基礎之新穎政府採購招標方法〉，國防大學資訊管理學系研究所碩士論文，2021年，<https://hdl.handle.net/11296/3b8rdc>，頁16，由作者彙整製表。

去中心化」、公開透明、分散式帳本、匿名性及自動化的特性，能夠大幅提升交易的安全性和效率；其不可竄改的性質，可以確保組織單位的機密資訊安全，透過「雜湊函數」單向性與抗碰撞性，保護各式資訊，避免遭人為因素竄改。由於區塊鏈的系統具備「去中心化」特性，可以提升系統的穩定性與可靠性，即使在遭受敵方網路攻擊的情況下，由於系統不再依賴單一的中心化儲存，因此可以降低整體通信系統被摧毀的風險。

(二)由於區塊鏈的交易和紀錄是公開透明的，其中的參與者都可以查看和驗證交易的資訊，且區塊鏈的分散式帳本資料儲存在各節點中，每個節點都有一個完整

副本，有助於建立一個可全程追蹤的物資管理系統，不僅追蹤物資的來源、運輸流程和生產履歷，亦進一步提升資訊的安全性與可信度。區塊鏈也具備匿名特性，可以保護人員的身分，使用「英文+數字」的代碼做為名稱，同時避免敏感數據外洩之虞。

(三)區塊鏈透過「智能合約」(Smart Contract)¹⁴，讓指揮者可以利用設計和預先編寫一系列行動指令，當符合特定條件時，該合約將自動觸發相應的行動，並在無人為干預的情況下節省時間和成本。例如，當特定的情報數據達到預定的標準時，「智能合約」可以自動發出特定的命令，啟動行動進程，並通知相關人員，使軍

註14：「智能合約」是一段由程式碼編寫的協議，其中包含合約的條款、條件和執行規則，可在特定的條件觸發下並自動執行，不會受到第三方的干預。

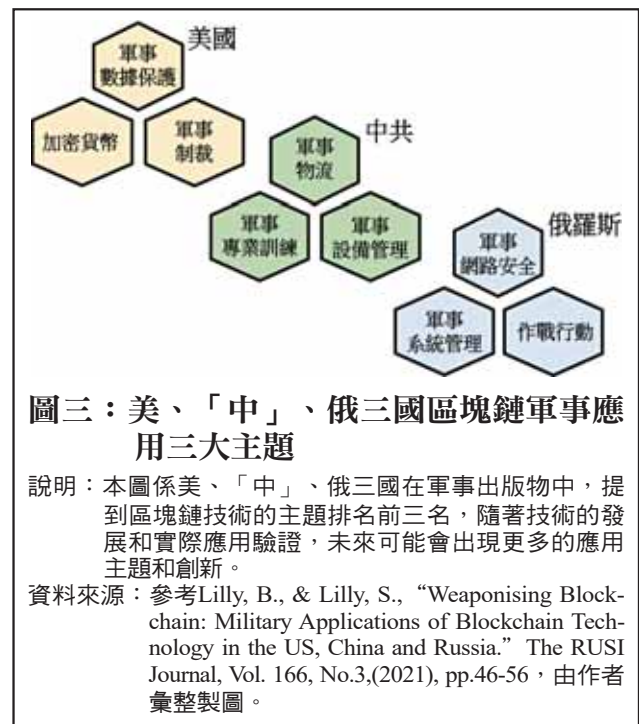
其他研究

事行動命令和過程得以同步，為指揮者提供即時且準確的行動進程。因此，區塊鏈技術在軍事應用上具有重大潛力，並且能提高國軍整體作戰指揮能力。¹⁵

善用區塊鏈的特性可以為軍事應用領域帶來一定的潛力與優勢，亦有助提升作戰效能、後勤管理，以及整體軍事運作的可靠性。然而，同時也需要考慮網路攻擊、隱私保護和技術執行上的問題，才能確保其在軍事應用上安全有效。

參、「區塊鏈」技術之軍事應用

近年來，「比特幣(Bitcoin)」、「以太幣(Ethereum)」¹⁶的興起及區塊鏈技術的發展，讓其不在侷限於數位貨幣；且結合學術界的研究和發展現況，讓其技術演進也從傳統1.0、2.0進化到3.0，¹⁷並將此一技術廣泛應用物流、金融、供應鏈、物聯網及國防等領域(如附表)。當前美國、中共和俄羅斯三大軍事武器發展強國，均已將區塊鏈列為資訊技術發展至關重要的「核心技術」之一；各國國防機構也透過區塊鏈平臺進行相關軍事應用測試，其中「網路安全」和「軍事後勤」是主要的



圖三：美、「中」、俄三國區塊鏈軍事應用三大主題

說明：本圖係美、「中」、俄三國在軍事出版物中，提到區塊鏈技術的主題排名前三名，隨著技術的發展和實際應用驗證，未來可能會出現更多的應用主題和創新。

資料來源：參考Lilly, B., & Lilly, S., "Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia." The RUSI Journal, Vol. 166, No.3,(2021), pp.46-56, 由作者彙整製圖。

應用項目，並持續擴展更多的軍事用途(如圖三)。¹⁸有關此技術的軍事運用，摘整說明如后：

一、戰場管理

(一)區塊鏈在軍事應用研究中可以輔助戰場作戰管理、建立可信任之軍事管理架構，透過「分散式帳本」(Distributed Ledger Technology)與「星際檔案系統」(InterPlanetary File System, IPFS)¹⁹等進行戰場情報資料儲存、共享和傳遞。在

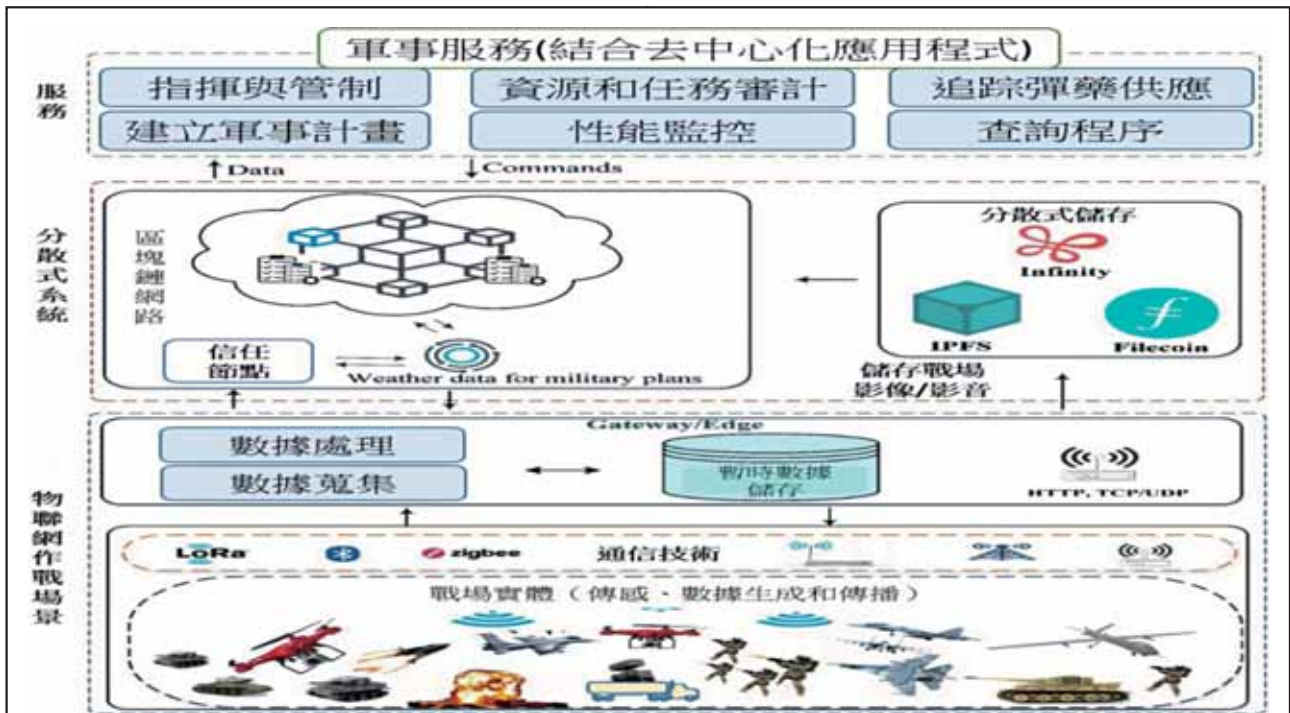
註15：Wang, T., Hua, H., Wei, Z., & Cao, J., "Challenges of blockchain in new generation energy systems and future outlooks." International Journal of Electrical Power & Energy Systems, Vol.135, (February 2022), 107499。

註16：「比特幣」是一種加密數位貨幣，無需中央管理機構(如政府或銀行)的數位幣，允許用戶進行「點對點」的交易，主要用途包括做為一種價值儲存和轉移工具。「以太幣」是以太坊區塊鏈平台的原生加密數位貨幣，做為交易時的主要支付方式；當用戶執行交易或智能合約時，需要支付一定數量的「以太幣」做為交易費用。

註17：Efanov, D., and Roschin, P., "The all-pervasiveness of the blockchain technology." Procedia computer science, Vol.123, (2018), pp.116-121。

註18：Lilly, B., & Lilly, S., "Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia." The RUSI Journal, Vol.166, No.3, (2021),pp.46-56。

註19：「星際檔案系統」是一種點對點的分散式檔案系統，建立一個檔案共享和儲存平台，取代傳統的中心化檔案儲存和傳輸模式，資料分散儲存在眾多電腦的IPFS節點中，不依賴單一伺服器，當主系統發生無法存取問題時，仍可從其他節點取得資料，避免服務中斷。如「數位發展部」的全球資訊網，即是利用此系統將資料分散儲存在全球眾多電腦的



圖四：區塊鏈之戰場管理架構示意圖

說明：透過「區塊鏈」技術可以建立一個分散式系統，在物聯網組成的作戰場景中，提供安全、即時和可信的戰場訊息共享平台，提供指揮管制與軍事服務，也確保數據完整性與安全。

資料來源：參考Ahmad, R. W., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. "Blockchain for aerospace and defense: Opportunities and open research challenges." Computers & Industrial Engineering, Vol.151, (January 2021), 106982, 由作者彙整製圖。

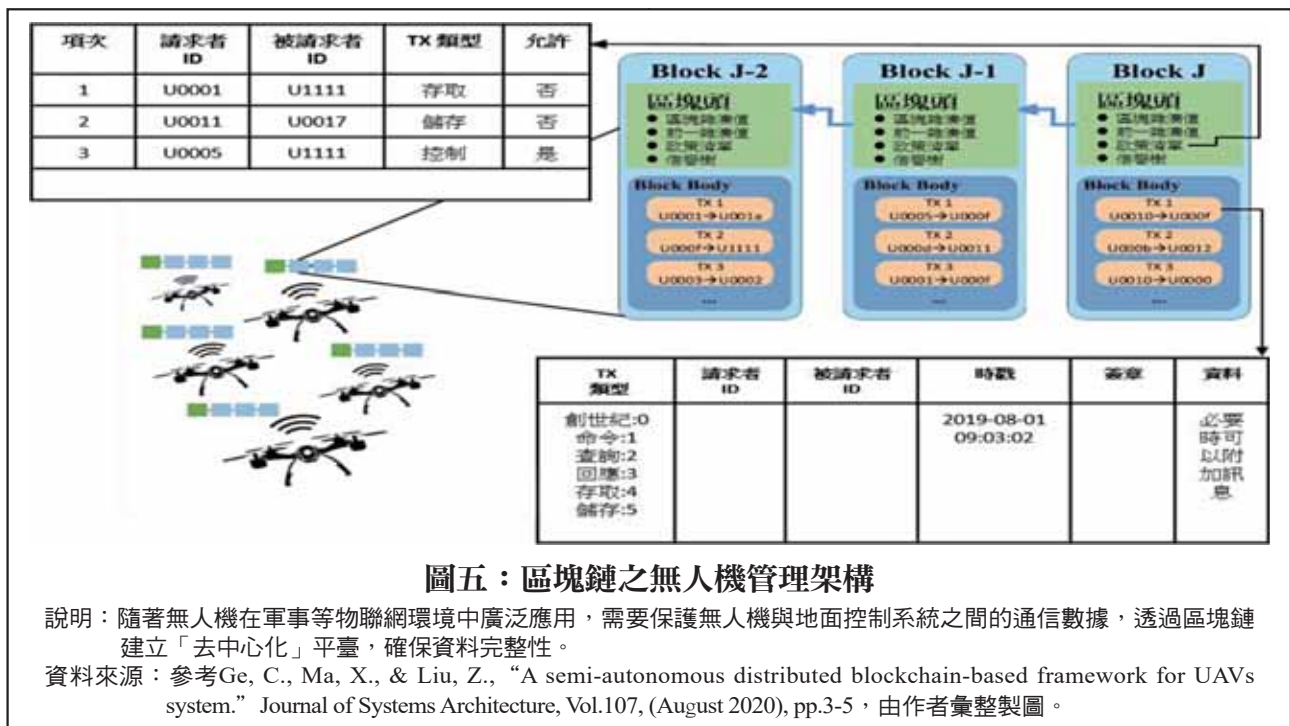
系統安全性上，即可律定各階層官、士、兵資料存取權限，再運用非對稱密鑰、密碼技術，進一步驗證資料的真實性和完整性。在資料傳輸部分，透過「Wi-Fi」無線網路、「ZigBee」短距離及「LoRa」遠距離傳輸²⁰等無線網路協定技術的相互構聯，就能輕易整合戰場資訊，包含陸地、海上與空中各式傳感器、無人機、作戰設備、通信車、戰鬥機、武器和作戰人員的

戰場訊息。

(二)國軍透過此系統可以建立戰場即時資訊共享平台，整合軍事作戰計畫，讓指揮官能隨時存取作戰動態，並監控整個作戰計畫執行；或整合戰場後勤資源，讓後勤補保資源進行統一分配、調度。此外，系統亦能建立官士兵個人戰場績效，分析官兵的專長、技能和能力，對其戰場績效與表現進行客觀評估，同時做為後續獎

IPFS節點中，可有效避免服務中斷。

註20：「ZigBee」是一種低功耗、低速率的無線通信技術，主要用於建立低成本、低功率的短距離無線傳輸網路，透過此一技術，網路上的每個設備都可直、間接與其他設備相互通信。如「宜家家居(Ikea)」公司的Tradfri無線調光燈泡，就使用該通信技術做為「飛利浦智慧照明系統(Philips Hue)」的一部分。「LoRa」是一種遠距離無線傳輸技術，具低功率和低數據傳輸速率的特點，同時此技術可以應用在物聯網(IOT)的場景，連接許多不同種類的設備，遠程監控設備的運作、讀取和控制相關設備等。如企業在貨物上裝設LoRa追器，讓業者在運送過程中可以隨時掌握物品，避免遺失。



圖五：區塊鏈之無人機管理架構

說明：隨著無人機在軍事等物聯網環境中廣泛應用，需要保護無人機與地面控制系統之間的通信數據，透過區塊鏈建立「去中心化」平臺，確保資料完整性。

資料來源：參考Ge, C., Ma, X., & Liu, Z., "A semi-autonomous distributed blockchain-based framework for UAVs system." Journal of Systems Architecture, Vol.107, (August 2020), pp.3-5，由作者彙整製圖。

勵的依據(如圖四)。²¹

二、無人飛行載具控制

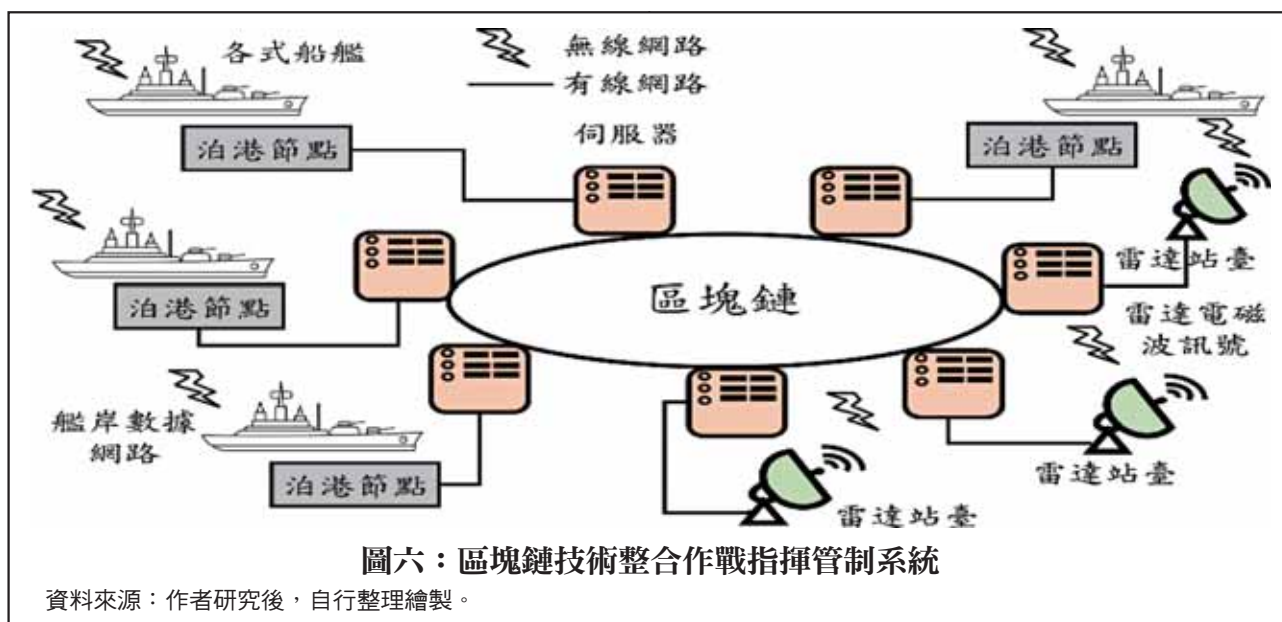
(一)運用區塊鏈技術組成的「無人飛行載具」(Unmanned Aerial Vehicle, UAV)架構，可以解決當前UAV管理中的信任和安全問題。²²典型的無人機系統由多個物聯網設備組成，包含無人機、地面控制站和通信數據鏈路(衛星鏈路、無人機鏈路和無線電通信鏈路)等，每種鏈路都承載不同的訊息；其中，政策清單為法律、規定和標準，政策的具體內容和要求會根據不同國家和地區的法律和規定而有所不同，內容包含律定無人機飛行限制區域

、最大飛行高度、速度限制、碰撞規則、優先等級分配等，可以用來指導和規範無人機操作的規則和限制，並確保無人機在運行過程中遵守相應的規範。而無人機在訊號相互構聯時，訊息交換結構包含類型(可標識訊息是一筆交易、請求、回應還是其他類型的訊息)、請求方和回應方的識別ID(讓其他無人機可以識別訊息的來源和目的地)、請求方的簽章(可由發送方驗證簽章，以確保訊息未被篡改，並確實由該請求方發送)，以及必要時可以附加通訊數據內容。

(二)UAV在物聯網傳輸過程容易遭受

註21：Ahmad, R. W., Hasan, H., Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M., "Blockchain for aerospace and defense: Opportunities and open research challenges." Computers & Industrial Engineering, Vol.151, (January 2021), 106982。

註22：Ge, C., Ma, X., & Liu, Z., "A semi-autonomous distributed blockchain-based framework for UAVs system." Journal of Systems Architecture, Vol.107, (August 2020), 101728。



各種網路攻擊，導致傳輸數據資料遭竊取及竄改之風險；因此，利用區塊鏈架構於軍事UAV系統中，可以提升系統的數據安全、降低威脅；用戶端可以透過區塊鏈取得UAV的真實位置、狀態和歷史軌跡，確保情資傳遞過程的完整性、機密性和可用性要求，並改善現行倚賴中央服務器可能發生單點伺服器故障或導致訊號中斷之情形(如圖五)。

肆、「區塊鏈」技術於我國軍事應用

未來區塊鏈技術一旦成功應用，必將帶來軍事發展和作戰方式的革命性變革，超越傳統軍事指揮管理範圍，提高軍隊戰鬥力，促進軍隊轉型發展，並在作戰指揮管制系統、武器裝備全壽期管理系統、軍

事後勤管理系統及人力資源管理系統等各方面，提高指揮管制和決策安全。以下針對區塊鏈技術與各系統整合運用概況，分別探討如後：

一、區塊鏈整合作戰指揮管制系統

(一)我國發展C4ISR系統以國防部為核心，整合各軍種的系統，使戰場指揮官能夠更迅速、有效地作出決策。近年來，系統已建構完成戰場資訊化，讓各級指揮體系相互構連，以建立情資共享及共同作戰為目標；然在實際運用上，仍發現存在有體系及組織困境，資源分散且資訊透明度不足等現象，運用上仍待持續精進。²³由於國軍是一個分工綿密的軍事組織，各部隊資訊系統和設備並不一致，在數位化指揮及資訊共享領域仍有很大的進步空間；故現階段仍以滿足未來戰場訊息量爆炸

註23：陳育正，〈美國網路安全防護經驗對我國網路安全情勢之啟示〉，《國防雜誌》(桃園市)，第30卷，第3期，2015年5月1日，頁73-87。

其他研究

的傳遞需求為目標。另一方面，當前作戰多以「網路戰」、「資訊戰」為主要攻擊手法，包括利用電腦封包流量攻擊、釣魚郵件等手段對敵方資訊系統進行干擾、控制，破壞網路安全，進而影響國軍各項以資訊網路服務為基礎的重要軍事系統，²⁴此點證諸當前「俄烏戰爭」就是最好的例子，亦值得國軍省思。²⁵

(二)透過區塊鏈分散式帳本特性、共識機制、自治特性和非對稱加密演算法機制，建立自動化、安全的指揮管制系統，可確保訊息真實性，並解決作戰場景中，指揮管制系統資訊共享之問題。由於作戰指管系統涉及到高度機敏的軍事訊息；因此，在架構整合時必須特別注意系統的安全性(整合架構，如圖六)。當近、中、遠程雷達站接收各式訊號、資料分析和目標識別，可以透過「區塊鏈」整合各艦透過「艦岸數據鏈路網」回傳指揮中心之數據，進行即時共享情報數據、目標追蹤、戰術圖像等，並可避免遭敵方利用網路攻擊，惡意竄改數據而導致指揮官做出錯誤決策、下達錯誤命令或虛假命令之風險。其優點概述如后：

1. 系統可靠性提高：

作戰指揮系統需要處理大量的戰場資訊，區塊鏈提供一種「去中心化」資料管

理方式，能夠增強資料的可靠性和安全性，所有交易紀錄都會被永久保存在鏈上，實現資料的完整性、可追溯性和不可竄改性，進而提高作戰指揮系統的可靠性。

2. 加強資料的即時監控和追蹤能力：

區塊鏈技術能夠提供即時的存取紀錄和監控系統，作戰指揮系統需要提供指揮官立即的戰場資訊與情資，並可即時監控和追蹤作戰動態，以便將其轉化為作戰指令和決策。

3. 提高資料的安全性和防竄改能力：

作戰指揮系統機敏資訊需要完整保護，以避免被駭客攻擊和情資遭敵方竊取竄改；而透過區塊鏈技術並採用加密和「去中心化」的資料管理方式，能提高資料的安全性和防竄改能力。

4. 加速決策過程：

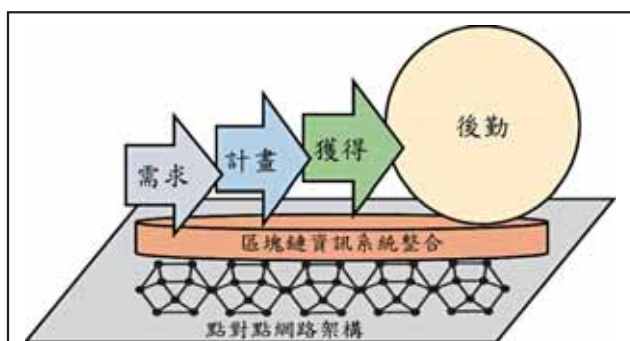
作戰指揮系統必須能輔助指揮官快速做出決策，以應對戰場情況變化，在「對等式」網路架構下，迅速蒐整各單位情資，並共享戰場訊息，可以實現更快速的決策過程，提供指揮官決心下達。

二、區塊鏈整合武器裝備全壽期管理系統

(一)國軍軍事裝備及武器系統自需求階段即應導入全壽期管理概念，包含計畫、保修、補給、構型、能量建立、成本管

註24：蔡志銓，〈我國應用C4ISR系統強化作戰整合之研究〉，《國防雜誌》(桃園市)，第35卷，第2期，2020年6月1日，頁107-128。

註25：2022年俄羅斯對烏克蘭的入侵，即透過「資訊戰」進行大規模「分散式阻斷服務」(DDoS)攻擊，並發布假消息，干擾及誤導對方，造成混亂並影響重要決策。李建興，〈歐盟研究發現科技公司自2022年來都未能有效阻擋俄羅斯資訊戰〉，iThome，2023年9月5日，<https://www.ithome.com.tw/news/158575>，檢索日期：2023年10月30日。



圖七：區塊鏈技術整合全壽期數位化管理系統

資料來源：作者研究後，自行整理繪製。

控等多個面向，需要各業務之間緊密協調、環環相扣，內容繁雜、缺一不可。目前國軍後勤資訊系統雖已完成全盤規劃，然由於系統各自獨立，分系統無法構連及資料庫版本問題導致發展受限，需要透過人工進行資料交換來彌補其缺陷。另外，因單位上下隸屬關係、人為疏失及未明確規範相關作業程序等，可能導致資料修訂、異動、回饋有缺漏情形，進而影響後續分析、統計結果失真，也會導致資料正確性遭到質疑。²⁶

(二)利用區塊鏈資料永久保存且可追溯技術，可以構建一個由開發者、生產者和管理者共同營運、相互監督的軍事武器、裝備全壽期管理系統(整合架構，如圖七)，可追蹤和管理軍事武器裝備從需求研製、計畫生產、交付獲得到服役及除役的所有設計參數、測試數據、作戰技術狀態和維護記錄，綜整其優點如后：

1. 提高資料可靠性和安全性：

武器裝備全壽期管理系統必須要能迅速處理大量的資料，包括武器裝備的開發、生產、測試、使用和維護等，透過區塊鏈「去中心化」的管理方式，能夠增強資料的可靠性和安全性，所有的交易都會被記錄在區塊鏈上，並保存軍事武器、裝備的設計參數、測試數據、技術文件和維護記錄等相關資料，以確保這些資料永久保存且不被竄改，實現資料保存必需的完整性、可追溯性和不可竄改性。

2. 提高全壽期管理效率和節省成本：

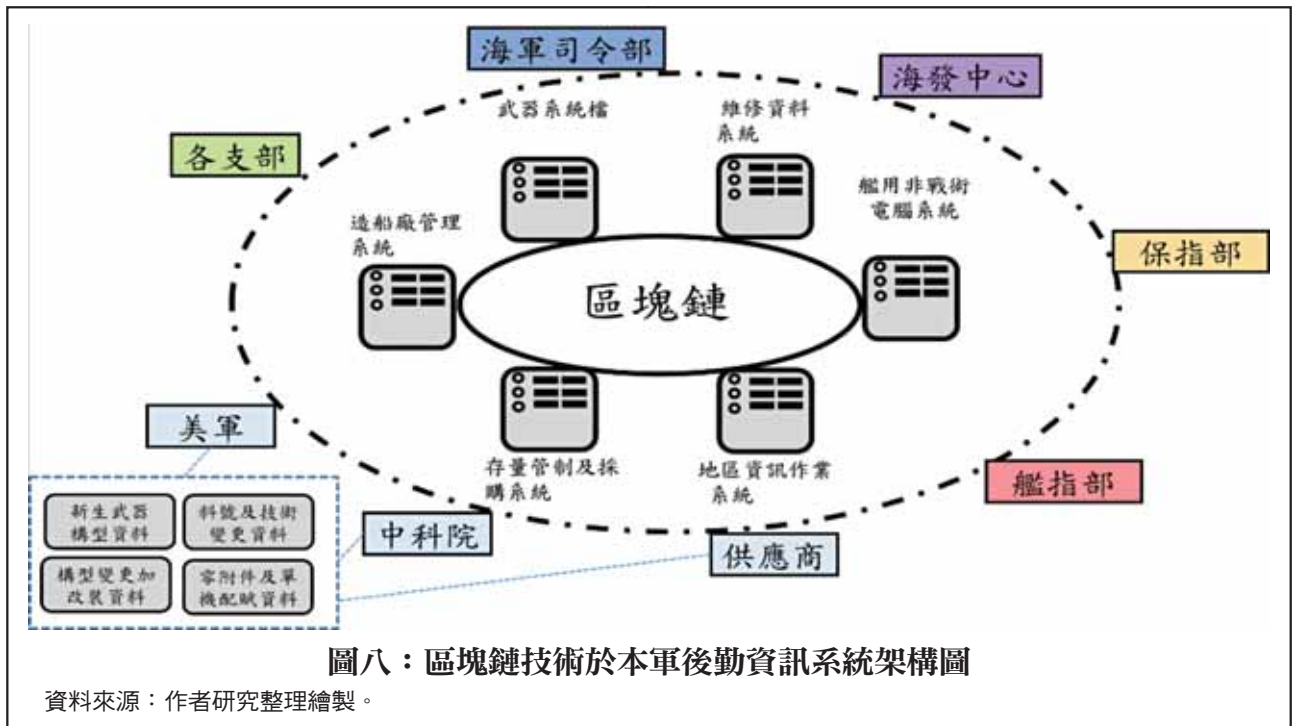
武器及重要軍事裝備從開發、生產、測試、使用和維護需要耗費龐大的人力成本和時間，透過區塊鏈技術能夠自動化進行武器裝備的全壽期管理流程，從研製、生產、交付、服役到除役的全壽期階段，確保所有過程履歷都可以追溯，並永久保存無法竄改，再透過「去中心化」系統，使過程減少「第三方」干預之風險。

3. 增強管理效能及資源利用：

軍事武器裝備全壽期管理系統需要由業管部門監控指揮武器裝備的開發、生產、測試、使用和維護等過程，以保證武器裝備的品質和效能，透過區塊鏈分散式帳本技術，能夠達成交易紀錄永久保存和不可竄改，增強管理效能。再者，當區塊鏈用於武器裝備的生產和供應鏈，可以達成資源共享及提高資源的有效分配與利用。

三、區塊鏈技術整合後勤管理系統

註26：黎立珊，〈整合型後勤資訊系統執行武器裝備全壽期管理之規劃〉，《海軍學術雙月刊》(臺北市)，第52卷，第2期，2018年4月1日，頁68-81。



圖八：區塊鏈技術於本軍後勤資訊系統架構圖

資料來源：作者研究整理繪製。

(一)國軍後勤管理良窳攸關部隊持續戰力發揮，其重點在於補給與保修，現行通用零附件庫儲管理中，各層級庫房管理多數仍透過人工方式進行庫儲清點，耗費大量人力及時間，部分庫房之間庫儲資訊亦無法流通。²⁷另從補給品獲得、入庫、造冊、建立帳卡、清點、登帳管制、出庫、銷帳等繁鎖之工作，管理人員容易因一時疏忽，而發生帳物不符情形，日積月累，造成呆帳、呆料，亦造成部分有心人士認為「有機可乘」，並利用承辦或管理時機，勾結廠商不當得利，致發生偷盜、賣軍品等危害軍隊名譽之情事。²⁸本軍現行

主要後勤資訊系統區分為武器、存量管制、採購、維修、造船廠管理等，在系統整合方面，由各後勤單位依後勤業務各自發展，導致各子系統之間無法即時共享資料，另由於資料庫建置軟體亦不同，無法互相構聯，需以人工方式實施各系統資料轉出與轉入，浪費人力與資源耗損。²⁹

(二)利用區塊鏈建構軍事後勤管理系統，將本軍各單位現行各系統進行整合，達成後勤軍品、倉儲、物流管理到採購、維修、修艦備料管理、運輸及配送相關的數據資料共享(架構，如圖八)；另該系統在資料共享時，須注意區塊鏈系統的可擴

註27：蔡曜任，〈國軍以ERP系統導入自動倉儲模式之研究-以臺北聯保廠為研究標的〉(健行科技大學電機工程系碩士論文，2018年)。

註28：陳俊旭，〈從貪瀆行為論強化海軍後勤採購防弊之具體作為〉，《海軍學術雙月刊》(臺北市)，第52卷，第2期，2018年4月1日，頁110-120。

註29：同註26。

展性，以應對不斷增長的資料量和數據。當在修艦零附件、武器裝備進出倉庫或運輸環節等相關記錄，均完整儲存在區塊鏈上，將能提高軍品、料件等後勤紀錄的完整、一致與安全性；尤其當發生帳物不符、呆帳情況時，其不可竄改之特性，將有利紀錄追蹤及核對，減少錯誤和遭盜竊的風險，讓後勤補給及支援作業能即時滿足各軍種和基層部隊的需求，迅速支援作戰所需。統整系統優點如后：

1. 增強資料真實性和安全性：

鑒於國軍各種零附件及料件琳瑯滿目，因此後勤管理系統需要處理大量的資料，其中包含物資調配、運輸、儲存、分配、清點等。透過區塊鏈技術整合，讓鏈上所有交易紀錄均彼此鏈接，且因無法任意竄改，進而增強資料的真實與安全性，並可隨時追蹤歷史紀錄，有助於後勤資料安全與管理。

2. 提高管理效率和節省成本：

國軍後勤武器裝備種類數量龐大，透過區塊鏈技術能夠實現自動化的後勤管理，利用智能合約條件化進行日常工作系統建置，例如庫存盤點、零附件管理、調配物資等，提高後勤管理的效率和準確性，並可以減少手動操作的人為疏失，及中介環節出錯的可能。

3. 增強後勤管理資料可追溯性：

在各式軍品裝備使用、清點、維護、

保修等日常工作，可以透過區塊鏈記錄和追蹤所有相關的數據，例如清點紀錄、維修紀錄、保養日誌、損耗情況等，確保軍品裝備的歷史紀錄是真實、可靠和不可竄改的，強化管理效率和確保資料可信度。

4. 加速資訊共享：

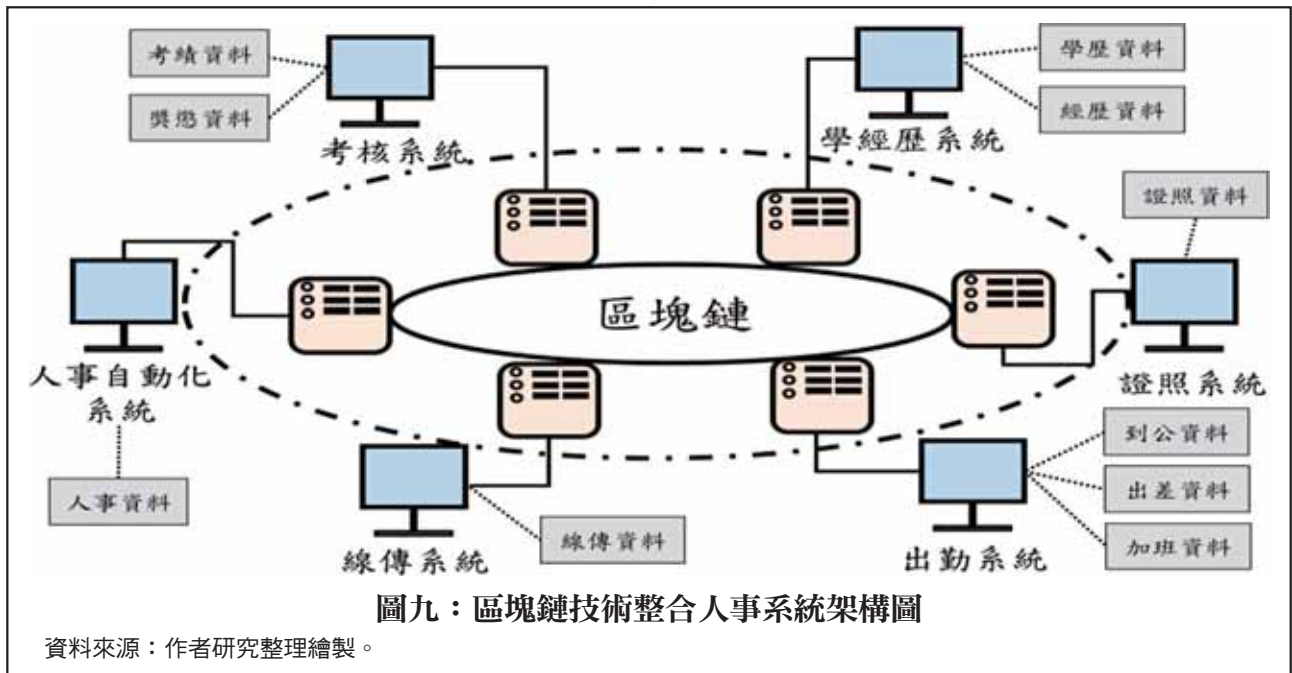
區塊鏈也可以建立共享平臺，讓不同後勤單位、部門及維護商等可以共享資訊，提高物資、裝備調配運用，例如軍方、裝備生產商、維修商和供應商等可以透過區塊鏈共享資訊，提高裝備生態系統的保修效率和生產效能，確保後勤資訊及管理工作順利進行。

四、區塊鏈技術於人力資源管理系統

(一)人力資源(Human Resources)被廣泛認為是企業營運中至關重要的因素之一，因為它們直接關係到企業的運作效率、生產力和競爭力，包括一個組織或企業中所有人員與其所擁有的相關資源，如員工所擁有的技能、知識、經驗和能力。而人力資源管理即是指企業內部人力資源的管理方式，包含組織內所有人力資源的獲得、調用和維護，進行有效的規劃、控制和管理的過程。³⁰國軍自推動人事資料自動化起，系統必須定期備份及更新人事資料庫，再透過人事自動化系統及人事線傳系統產生線傳碼後，將資訊上傳至國防部伺服器。³¹然而獨立伺服器容易發生單點故障及最高管理者擁有完全的控制權之問

註30：楊立中、賴焜燦，〈以《美國退伍軍人權利法案》(GI Bill)為基礎論國軍募兵制度-運用人力資源管理策略〉，《國防雜誌》(桃園市)，第23卷，第3期，2008年6月1日，頁43-55。

註31：蘇品長、王仁志、蕭雅尹，〈設計具安全機制之國軍人事資料管理系統〉，《國防管理學報》(臺北市)，第39卷，第1期，2018年5月1日，頁1-18。



資料來源：作者研究整理繪製。

題，系統管理者擁有存取伺服器上的所有資料和系統設定的權限，若管理者濫用或疏忽，均會對伺服器 and 其中重要數據造成損害，也有可能讓其帳戶也成為被攻擊者的目標。

(二)一旦最高管理者的帳號遭到駭客攻擊或者濫用，整個系統將受到威脅；另可能肇生人事學歷、經歷、專長、證照、考績、教育等機敏性資料被竄改的問題。國防人力資源管理攸關國軍整體戰力基礎，若能將區塊鏈技術導入人力資源管理系統，透過不可竄改及永久保存之特點，能將人事學歷、經歷、專長、證照、考績、教育等機敏性資料易被竄改之風險降至最低，同時解決長時保存的問題。尤其區塊鏈技術的系統整合人員出、缺勤、加班、外勤與薪資作業流程，達成數據同步、安

全及可信任(整合架構，如圖九)，然而同時也須注意個人隱私保護之問題。其優點如后。

1. 增強資料透明度和可靠性：

區塊鏈技術提供了一種「去中心化」的資料管理方式，能夠增強資料的透明度和可靠性，當人事資料記錄上鏈，保證數據真實可信，避免人為竄改，增加數據的可信度與可靠信。

2. 提高效率 and 節省成本：

區塊鏈技術能夠自動化和優化各種人力資源管理過程，自動化進行加班、外勤、缺勤和薪資的計算，減少了人為計算失誤與繁瑣的操作和審核流程，進而提高效率並節省成本。

3. 增強安全與隱私性：

區塊鏈上進行數據驗證時，需要透過

複雜的數學算法來驗證，保證節點之間的通信和交易是安全和保密的；所有的交易記錄透過加密機制進行加密與驗證，防止資料洩漏和不當使用。

4. 人力資源共享：

利用區塊鏈技術建立人力資源共享平臺，共享各單位人員招聘、調職、出缺、離職等相關兵力資訊，進而達成人才匹配和資源配置，並更利於戰時人事運用、指揮、協調和調度。

伍、省思-代結語

區塊鏈技術已逐漸發展成熟，有助於建構自主化、安全、可信任之資訊系統，且鑑於該技術的軍事應用潛力，預期可能帶來之效益，包括提高系統工作效率、降低人為出錯風險、促進系統間整合運作及增強安全性；另一方面，亦對提高軍隊戰鬥力，促進軍隊轉型發展，賦予新的重要意義。省思國軍在區塊鏈技術之軍事應用上，仍有以下努力方向：

一、安全性和保密性

在區塊鏈上雖可以將數據雜湊並加密儲存，限制只有授權的使用者才能存取資料，保護各項軍事系統的數據儲存及驗證機制安全，並防止未經授權的第三方進行竄改或竊取資料，同時改善現行國軍資訊系統單點伺服器遭攻擊肇生資料遭竄改之問題。此方式將可保障軍事戰力之機密性和防範敵方滲透攻擊，使系統更加安全。

二、性能和擴展性

現有的區塊鏈平台在性能和擴展性方面仍然存在限制，如區塊的生成率、交易速度。在軍事系統中，需要高效率的系統來處理大量的數據和交易。因此，未來將區塊鏈導入時，須進行系統的性能和效率評估，是否能滿足國軍現行系統要求。

三、系統整合

區塊鏈技術透過分散式帳本，讓不同的系統之間進行數據交換和互動，建立共享平臺，達成不同軍事單位資訊共享、協同合作與系統整合；然而在導入區塊鏈於提升國軍戰力的同時，仍需進行全面的統籌規劃，包含軟硬體設置、新舊系統相容介接及技術培訓等，以確保有足夠的專業人員能夠設計、維護和管理區塊鏈系統。

四、法律和監管挑戰

區塊鏈技術跨足了傳統法律和監管框架，我國現行法規中針對加密貨幣尚未開放，在使用上將有許多限制；因此未來系統建置時須配合國家政策，避免引發法律和監管問題。

綜上所述，儘管區塊鏈技術存在諸多優點，但「水能載舟，亦能覆舟」，由於仍是在雲端中進行，同樣存在如「分散式阻斷服務攻擊(Distributed-Denial-of-Service)」、「中間人攻擊(Man-in-the-Middle Attack)」、「進階持續性威脅(Advanced-Persistent-Threat)」、「跨網站指令碼攻擊(Cross-Site-Scripting)

其他研究

」³²等各式網路攻擊，可能導致資訊服務中斷、重要機敏訊息遭竊。因此，國軍建置區塊鏈系統後，可結合現行網路流量分析及封包檢測等設備，進行相關數據監測；另在系統中落實IP控管、身分驗證(如結合多因子身分查驗手續)，加強網路防火牆功能、限制特定IP位址等，確保只有授權的用戶可以存取系統。當發現網路異常立即採取相對應的策略進行修正，降低系統服務中斷或資料遭竊取之機率，俾確

保區塊鏈技術能夠發揮最大價值。



作者簡介：

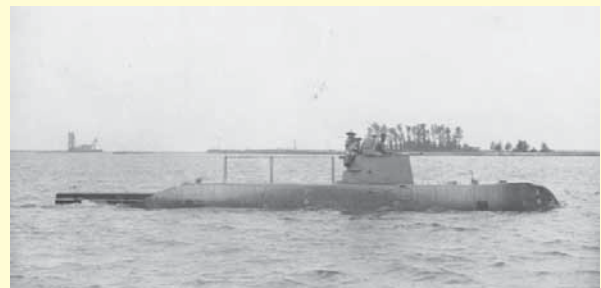
黃琬玲少校，國防大學管理學院資訊管理學系101年班、國防大學管理學院資訊管理研究所碩士112年班。曾擔任海軍司令部人事軍務處程式設計官、海軍左營後勤支援指揮部程式設計官、海軍馬公通信隊副隊長，現服務於海軍司令部。

蘇品長教授，長庚大學電機工程研究所博士。曾擔任國防大學管理學院資訊管理學系教授、副教授、助理教授、主計局電資中心資訊督導官，現服務於國防大學管理學院。

註32：「分散式阻斷服務攻擊」是一種常見網攻手法，攻擊者利用多個來源發起大量的請求或流量，超出目標系統的處理能力，導致系統不可用或緩慢。「中間人攻擊」是攻擊者偽裝成合法的通信方，並監控、竄改或截取通信的內容，並在不被察覺到的情況下干擾通信流量。「進階持續性威脅」是一種複雜且持續存在的威脅，通常由具高度專業的攻擊者發起，以進行長期的持續監視、滲透和控制為目標，並進行有組織、有計畫和隱蔽的攻擊活動。「跨網站指令碼攻擊」是一種常見的網站安全漏洞，攻擊者利用漏洞在目標網站的網頁中注入惡意代碼，並執行各種惡意操作，包括竊取敏感訊息、獲取登錄憑證、操縱網頁內容，甚至引導用戶到惡意網站。

老軍艦的故事

海蛟潛艇S-1 & 海龍潛艇S-2



民國54年我海軍在義大利造船廠的協助下，於當時的「海三廠」淡水分廠裝配海蛟及海龍潛艇，並於民國56年遷至左營完成裝配及試航。民國58年10月8日，前總司令馮啟聰上將主持海蛟及海龍兩艘潛艇的成軍典禮，而這是我國海軍擁有的第一代潛艇兵力。該兩艘潛艇於民國62年11月1日除役。(取材自老軍艦的故事)