Blockchain: A Panacea for Logistics Information Systems?

A Monograph

by
Major Julie A. Pearce
Australian Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2019

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-05-2019	Master's Thesis	JUN 2018 - MAY 2019

4. TITLE AND SUBTITLE
Blockchain: A Panacea for Logistics Information Systems?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Julie Pearce

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Advanced Operational Arts Studies Fellowship, Advanced Military Studies Program.

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Throughout history, military commanders have identified their supply chains as vulnerable. In times of war, the supply chain is a soft underbelly, rarely protected, and yet when targeted by the enemy it produces catastrophic results. The recent recognition of cyberspace as a warfare domain has provided adversaries with a new way of targeting logistics.

Digitization and technological improvements led militaries to adopt lean logistical approaches, often replicating commercial practices. These automated systems promised efficiencies in time and money. These promises rarely eventuated, and while technologies were introduced the underlying logistics structure remained mandraulic, centralized, and vulnerable.

Blockchain is the latest technological solution promised to deliver efficiencies to supply chains. This monograph examines the impact of incorporating blockchain technology within the Australian Army's Logistic Information Systems, including whether it can make Logistic Information Systems more efficient and more resilient to cyber attacks. This research uses the Rapid Technology Assessment Framework for Land Logistics to assess blockchain technology to determine how it can be of use, and whether it is better than current systems. It also identifies potential barriers to adoption and required Fundamental Inputs to Capability required to support the implementation of blockchain technology.

Like previous technological advancements, Blockchain is not a panacea. It is not the only answer to mitigating vulnerabilities to Logistics Information Systems (LogIS) in cyberspace, and it is not the complete solution to a lean, efficient, and effective supply chain. However, it has the potential to enhance the existing supply chain and make it more resilient against cyberspace attacks. While blockchain is unlikely to solve all vulnerabilities faced by LogIS, it should be part of the solution.

15. SUBJECT TERMS
Australian Army; Logistics; Blockchain; Information Systems; Cyberspace; Supply Chain; Logistics Information Systems

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MAJ Julie Pearce
(U)	(U)	(U)	(U)	50	19b. PHONE NUMBER *(include area code)*

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

Monograph Approval Page

Name of Candidate: Major Julie A. Pearce

Monograph Title: Blockchain: A Panacea for Logistics Information Systems?

Approved by:

_____, Monograph Director
Dan G. Cox, PhD

_____, Seminar Leader
Andrew J. Watson, COL

_____, Director, School of Advanced Military Studies
Kirk C. Dorr, COL

Accepted this 23rd day of May 2019 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

Blockchain: A Panacea for Logistics Information Systems? by Major Julie A. Pearce, Australian Army, 57 pages.

Throughout history, military commanders have identified their supply chains as vulnerable. In times of war, the supply chain is a soft underbelly, rarely protected, and yet when targeted by the enemy it produces catastrophic results. The recent recognition of cyberspace as a warfare domain have provided adversaries with a new way of targeting logistics.

Digitization and technological improvements led militaries to adopt lean logistical approaches, often replicating commercial practices. These automated systems promised efficiencies in time and money. These promises rarely eventuated, and while technologies were introduced the underlying logistics structure remained mandraulic, centralized, and vulnerable.

Blockchain is the latest technological solution promised to deliver efficiencies to supply chains. This monograph examines the impact of incorporating blockchain technology within the Australian Army's Logistic Information Systems, including whether it can make Logistic Information Systems more efficient and more resilient to cyber attacks. This research uses the Rapid Technology Assessment Framework for Land Logistics to assess blockchain technology to determine how it can be of use, and whether it is better than current systems. It also identifies potential barriers to adoption and required Fundamental Inputs to Capability required to support the implementation of blockchain technology.

Like previous technological advancements, Blockchain is not a panacea. It is not the only answer to mitigating vulnerabilities to Logistics Information Systems (LogIS) in cyberspace, and it is not the complete solution to a lean, efficient, and effective supply chain. However, it has the potential to enhance the existing supply chain and make it more resilient against cyberspace attacks. While blockchain is unlikely to solve all vulnerabilities faced by LogIS, it should be part of the solution.

Contents

Acknowledgments

Every AMSP student knows that words matter, unless written in passive voice or the Queen's English. However, despite my fights with Grammarly and Microsoft Word, my time at CGSC and AMSP has made me realize that writing also matters. It has been an amazing, albeit daunting opportunity to conduct independent research on a topic of my choosing. If nothing else, it gave me no one to blame except myself. That being said, there are plenty of people that deserve credit and acknowledgement. My monograph director Dr. Cox, who read pages and pages of research written in passive voice, but who also remained enthused about my research even when I was not. My Seminar Leader COL Watson, who had to endure a future focused monograph when his passion is history, I know that this was probably just short of torture for you. Although, as always, your counsel was insightful and contributed not only to the development of my monograph, but also towards my development as an officer.

The people you work with have a disproportionate effect on the amount of fun you have. I have been lucky to share this opportunity with an excellent group of international students, who have become my extended family in the absence of my own. You have all been excellent ambassadors for your countries, and I hope we have the opportunity to meet again. My classmates in Seminar 2 helped me to develop my intellectual rigor and an appreciation for timely memes, all of which helped make the course more rewarding and enjoyable.

To my husband, Trent, you have supported me in every aspect of this adventure. While this monograph might have been written even without your input, I am not sure the family would have been fed, clothed, or schooled at the same time. Jasmine, Annalise, and I are so lucky we have you in our lives. You have been a constant source of support, and thank you seems wholly inadequate to describe my appreciation.

Acronyms

ADF	Australian Defence Force
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSS	Combat Service Support
DDoS	Distributed Denial of Service
DSTO	Defence Science and Technology Organisation
FIC	Fundamental Inputs to Capability
JLC	Joint Logistics Command
MILIS	Military Integrated Logistics Information System
LogIS	Logistics Information Systems
P2P	Peer to Peer
PoS	Proof of Stake
PoW	Proof of Work
RTAF	Rapid Technology Assessment Framework

Illustrations

Tables

Introduction

> An adversary doesn't have to stop us. All they have to do is slow us down. All they have to do is make us doubt the accuracy of our own data. Once we've lost the veracity, how do you get it back? We will check double-check and triple-check every piece of data. By the time we figure it out, it may be too late. Our adversaries may have already won. They will not have used one bomb or one bullet. Instead, they will use ones and zeros. That is the reality of our time; it does not matter if we have the most lethal military in the world if we can't get it where it needs to go when it needs to get there. It just doesn't matter.
>
> — General McDrew, Logistics Officer Association Symposium

The dominant narrative regarding technology is that of interconnectedness. The digitization of economic, government, social, and communications systems has resulted in a dependence on digitized data to facilitate decision-making. In 2018, there were 2.5 quintillion bytes of data created each day. Ninety percent of all data in existence was created in the last two years.[1] Digitization led to an increased focus on creating efficiencies, and logistics and supply chains have not been exempt. These efficiencies failed to acknowledge or defend against vulnerabilities from cyber threats. These threats are pervasive, non-discriminatory, far-reaching and difficult to stop, with logistic systems being both one of the most obvious and vulnerable potential targets.[2]

Logistics is an essential component in enabling warfighting. Logistics can extend the operational reach of a combat unit, or conversely, can force a combat unit to culminate. With the advent of cyberspace as a warfighting domain, most literature focuses on the advantages that network-centric warfare can provide or cautions against the impact of a communications denied environment at the tactical level. Logistics Information Systems (LogIS) operate at all levels of

[1] Bernard Marr, "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, May 21, 2018, accessed August 12, 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/.

[2] Ksenia Ivanova and Guy Edward Gallasch, *Rapid Technology Assessment Framework for Land Logistics* (Fishermans Bend: Land Division, Defence Science and Technology Organisation, Commonwealth of Australia, March 2015), 7.

war and are reliant on interoperability with unclassified commercial logistics networks, as well as highly classified information systems. These considerations identify LogIS as a high payoff target, vulnerable to confidentiality, integrity or availability motivated attacks in cyberspace.[3]

The interconnectedness between Australian Army logistics and commercial or civilian logistics providers is threefold. Firstly, the Australian Army procures materiel from commercial logistics providers to supply the demands of the force. Multiple companies provide these materiels, who in turn, source their products from a combination of national and international logistics suppliers. Secondly, strategic-level logistics is increasingly reliant on and connected with, commercial logistics providers and contractors, mainly through the Joint Logistics Command (JLC). Functions performed by commercial logistics providers include heavy transport convoys, provisioning, maintenance, and warehousing. Lastly, Australian Army logistics is increasingly reliant on private military contractors to perform logistics functions from the tactical through to the strategic level.[4] Underpinning all these functions is a requirement for the sharing of information through a transparent medium. This medium is LogIS.

In 2015, the Defence Science and Technology Organisation (DSTO) identified the domination of the technological environment by the increased digitization and complexity of interconnected systems and emerging and disruptive technologies. The effects on the operational environment include an increasing dependence on Information and Communication Technology (ICT) systems that are not under the control of the Australian Defence Force (ADF) and an increasing reliance on satellite technology. The related effects on logistics include the dependence

[3] Julie Pearce, "Identifying an Achilles' Heel: The Vulnerabilities of the Australian Army's Logistics Information Systems in Cyberspace" (Master's Thesis, US Army Command and General Staff College, 2018), 106.

[4] David Beaumont, *Transforming Australian Army Logistics to Sustain the Joint Land Force*. Australian Army Occasional Paper, Future of Army Series (Canberra: Commonwealth of Australia, October 2017), accessed August 16, 2018, https://www.army.gov.au/sites/g/files/net1846/f/transform_logistics_b5_faweb.pdf.

on a constant connection to LogIS, requirements for secure design and supply chain process for ICT hardware and software, and the ensuing challenges in data security.[5]

Wildcard scenarios refer to low probability – high impact events that occur rapidly, giving the system little chance to adapt.[6] The Rapid Technology Assessment Framework for Land Logistics wildcard scenarios include attacks on networks and physical routes leading to a global supply chain crisis, targeted infiltration of military LogIS, and the falsification of information. With an increasing dependence on LogIS and without the ability to transition back to an analog system, it is imperative that the Australian Army invests in emerging technology, doctrine, training, and cyber hygiene to decrease the vulnerability of LogIS in cyberspace.[7]

Blockchain technology is one emerging technology that is demonstrating the potential for the security of data through a decentralized distributed ledger construct. It combines cryptographic, data management, networking, and incentive mechanisms to support the checking, execution, and recording of transactions between parties.[8] Historically, the creation and maintenance of a ledger was the responsibility of a single person responsible for the accurate and timely record keeping of activities. With the advent of technology and the internet, most of these ledgers are now digital. Despite the introduction of digitization, the centralization of ledgers still dominates common practice, with a central organization or person responsible for the accuracy and version control of the data.[9]

---

[5] Ivanova and Gallasch, *Rapid Technology Assessment Framework for Land Logistics*, 61.

[6] Ibid., 25.

[7] Ibid., 61.

[8] M. Staples, S. Chen, S. Falamki, A. Ponomarev, P. Rimba, A. B. Tran, I. Weber, X. Xu, and J. Zhu., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts* (Canberra: Commonwealth Scientific and Industrial Research Organisation, May 2017), 2.

[9] R.T. Hanson, A. Reeson, and M. Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades* (Canberra: Commonwealth Scientific and Industrial Research Organisation, May 2017), 2.

The rise of threats from cyberspace has led to the development of a trust deficit. How can you be sure that the data on the digital ledger is correct and has not suffered from interference? Blockchain decentralizes and distributes the ledger, with multiple people having access to the data simultaneously. This blockchain forms a consensus mechanism which when combined with cryptographic tools results in untrusted participants on an untrusted network being able to trust their transactions.[10]

Blockchain became prominent as the technology underpinning Bitcoin, the most popular and well-known cyber currency. However, many see that blockchain technology has significant applications outside of cyber currency. Considering that logistics and supply chains originated from an original physical ledger system, it is not surprising that commercial logistics and supply chain companies are interested in the applicability of blockchain technology. Commercial logistics providers hope to use blockchain to enhance visibility, transparency, and data security while aiming to increase efficiencies and embrace the subsequent profits. In an interconnected, data reliant environment, blockchain appears to be the solution to the trust deficit caused by potential cyber interference.[11]

Military organizations, the Australian Army included, have continually sought technological solutions to reduce the friction and fog of war while increasing the efficiency and effectiveness of the supply chain. Despite this, the Australian Army has struggled to integrate emerging technologies successfully into its organization, and in some instances has been unable to deliver the promised efficiencies. Operations in East Timor, Afghanistan, and Iraq identified that LogIS were inadequate and poorly implemented, often increasing instead of reducing the

[10] Hanson, Reeson, and Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*, 2.

[11] Ibid., 3.

workload of logistics operators. These systems and processes duplicated functions and failed to integrate emerging technology for the benefit of the organization.[12]

There is an increasing trend for commercial logistics providers to promote the adoption of blockchain within LogIS. However, the translation of blockchain from crypto-currency to LogIS remains conceptual and unproven. It may not be the promised panacea, and even if it is an ideal solution for commercial logistics providers, it is not automatically a perfect solution for the Australian Army.[13]

It is therefore imperative that the Australian Army analyze these technological solutions based on a framework specific to the organization and the environment before committing to these solutions. Given the interdependency of transparent LogIS between the Australian Army LogIS and the LogIS of commercial logistics providers, it is essential to identify the impact of blockchain incorporation on Australian Army logistics operations. Regardless of whether or not the Australian Army wants blockchain technology, it will affect their operations.

Literature Review

The internet has had an immeasurable impact on the transfer of data within and between organizations and people. It has contributed significantly to the efficiency of business but has had a remarkably little impact on the conduct of business. The design of the internet facilitated high-availability messaging between trusted parties. However, as the internet evolved, it has resulted in "a network designed for resilience and high availability, accessed by untrusted individuals . . . with limited inbuilt functions for ensuring accuracy and secrecy."[14]

---

[12] Allison Sonneveld, "Logistics and Emerging Technology," in *On Ops*, ed. Tom Frame and Albert Palazzo (Sydney: UNSW Press, 2016), 169–171.

[13] Ken Cottrill, "The Benefits of Blockchain: Fact or Wishful Thinking?" *Supply Chain Management Review* (February 2018), accessed August 14, 2018, http://www.scmr.com/article/the_benefits_of_blockchain_fact_or_wishful_thinking.

[14] Hanson, Reeson, and Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*, 2.

While the internet has improved the abundancy and transparency of data and information, it has resulted in information that is unreliable and perishable. Undesirable consequences eventuate when an individual sends information via the internet. This information is a copy, not the original. Anyone receiving that information can copy, modify, and distribute the information. Multiple copies of the same document, with differing information, decrease the amount of trust that a user has in the digital documents received.[15]

Trusted organizations responded to this environmental change and acted as intermediaries to validate data transferred through the internet. Banks provide a good example of trusted intermediaries, although other examples include retail corporations and lawyers. Securing data and maintaining the validity and integrity of the data has increasingly become a problem for these trusted intermediaries. Increased data breaches, cyber-attacks, and data spills have gradually decreased the trust individuals have in these intermediaries, leading individuals to investigate methods to overcome the trust deficit.[16]

Blockchain – The Technology

When "Satoshi Nakamoto" published a Bitcoin white paper in 2008, and released the prototype of Bitcoin two months later he disrupted the reliance on trusted intermediaries to transfer data between people and organizations through the internet. This technology offered a low-cost decentralized, distributed, and anonymous currency that enabled the exchange of financial transactions between parties that might be unknown to each other. A peer-to-peer network that validated transactions and removed the need for trusted intermediaries or centralized control overcame the trust deficit.[17]

---

[15] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World* (New York: Portfolio, 2018), xxiv.

[16] Ibid., 1–14.

[17] Ghassan Karame and Elli Androulaki, *Bitcoin and Blockchain Security*, Artech House information security and privacy series (Boston: Artech House, 2016), 1.

The cryptocurrency Bitcoin is reliant on a number of elements and foundational technologies. The amalgamation of these technologies is referred to as blockchain. The underlying components include the distributed ledger, a consensus mechanism, and cryptographic measures. These components result in a blockchain that is secure and immutable.[18] It is best to consider Bitcoin as one case study of blockchain technology in order to understand the potential for blockchain adoption outside of cryptocurrency environment.

Bitcoin

Nakamoto's system facilitated "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[19] Bitcoin does not store its data centrally. Instead, it records transactions using the blockchain, a distributed ledger. According to Nakamoto, the Bitcoin system utilizes a "peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."[20]

In less technical terms, the Bitcoin ledger runs on computers of volunteers, known as nodes. This structure results in there being no central server or database to target, hack, or compromise. Every ten minutes miners verify transactions and store them in a block. Each block links to the preceding block, which forms a chain. These blocks are encrypted using private and public keys. Groups of miners verify the transactions using a consensus mechanism. Figure 1 provides a graphical representation of this system.

---

[18] Michael Casey, Bill McBeath, Brigid McDermott, Sam Radoccia, Dan Doles, and Dan Harple. "Emerging Applications of Blockchain for Supply Chains" (PowerPoint Presentation, MIT Enterprise Forum, Cambridge, September 12, 2017), accessed September 27, 2018, http://www.mitforum cambridge.org/2017/12/video-using-blockchain-supply-chains/.

[19] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, White Paper, accessed February 5, 2019, http://bitcoin.org/bitcoin.pdf, 1.

[20] Ibid.

DUE TO COPYRIGHT RESTRICTIONS,

IMAGES ARE NOT INCLUDED

IN THIS ELECTRONIC EDITION.

Figure 1. What is Blockchain? Image from Blockgeeks, "What is Blockchain Tecchnology," accessed December 05, 2018, https://blockgeeks.com/guides/what-is-blockchain-technology.

In the case of Bitcoin, miners verify transactions through a proof of work consensus mechanism. Miners compete to solve complex computational puzzles to generate sufficient proof of work. The reward of Bitcoins incentivizes these miners to complete these computations. This reward mechanism combined with the computational power expended through the proof of work concept to achieve consensus makes it difficult for nefarious nodes to outnumber the honest nodes within the network. In order for dishonest nodes to control the consensus mechanism of the blockchain, they would have to control over sixty-six percent of the nodes in the network. They would also need to possess an asymmetric advantage relative to computational power to ensure that a dishonest node was able to solve the proof of work computation before an honest node and have the block verified by other dishonest nodes in the network. This scenario is improbable due to the combination of these variables.[21]

[21] Adam Rothstein, *The End of Money: The Story of Bitcoin, Cryptocurrencies and the Blockchain Revolution* (London: John Murray Learning, 2017), 187– 188.

Distributed Ledger Technology

According to the Commonwealth Scientific and Industrial Research Organisation (CSIRO), a distributed ledger is "replicated, shared and synchronized data geographically spread across multiple parties who may be in different sites, institutions, or countries. There is no central administrator or centralized data storage."[22] Multiple nodes store the history of the entire blockchain. This concept is not new; a simplified example includes individuals providing a copy of their will to multiple people. When executing a will, it is evident if one member has attempted to modify the contents of the will because multiple copies exist. When trying to validate these copies the forgery is easily identified and discarded as invalid. Figure 2 depicts the difference between centralized, decentralized and distributed ledgers.

DUE TO COPYRIGHT RESTRICTIONS,

IMAGES ARE NOT INCLUDED

IN THIS ELECTRONIC EDITION.

Figure 2. The Idea of Decentralization, Image from What is Blockchain? Image from Blockgeeks, "What is Blockchain Tecchnology," accessed December 05, 2018, https://blockgeeks.com /guides/what-is-blockchain-technology.

[22] Hanson, Reeson, and Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*, 61.

Consensus Mechanisms

Bitcoin's design relies on incentivized cooperation between nodes in the Peer-to-Peer (P2P) network. All nodes on the network receive and validate transactions in order to achieve consensus. These nodes confirm transactions in blocks on the distributed ledger, or blockchain by solving computational puzzles. The node that succeeds in solving the puzzle receives a financial reward and confirms the transaction. This type of consensus mechanism is referred to as Proof of Work (PoW).[23]

The PoW protocol means "the probability of mining a block is dependent on how much work is done by the miners."[24] While the PoW consensus protocol is the most well-known, it is not the only option to achieve consensus on a blockchain. Peercoin and NXT use alternate consensus protocols, such as the Proof of Stake (PoS) protocol where "the probability of mining a block is dependent on how much digital currency is controlled by the miners."[25] In a PoS blockchain, miners receive transaction fees instead of cryptocurrency incentives.

The design of PoS consensus mechanisms mitigates concerns raised regarding the excess energy expended in a PoW blockchain. While PoW and PoS remain the primary consensus mechanisms, variations are in existence. Proof of activity combines PoW and PoS, requiring a random number of miners to sign off on the verification of a block prior to adding it to the chain. These alternative consensus mechanisms have enabled the conceptualization of permissioned blockchains.[26]

---

[23] Karame and Androulaki, *Bitcoin and Blockchain Security*, 2.

[24] Hanson, Reeson, and Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*, 64.

[25] Ibid.

[26] Tapscott and Tapscott, *Blockchain Revolution*, 32.

Security and Immutability

Blockchain technology uses a hash algorithm, to make data within the blockchain cryptographically secure. Hash functions manipulate an input of arbitrary length and provide a fixed size output. The inputs include multiple forms, raw data, excel spreadsheets, a database, or files of any size. Figure 3 and figure 4 depict this process. Figure 3 provides an example of two data inputs of different length that produce different outputs of the same length (236 bits), referred to as the hash. Figure 4 provides an example of how small changes to data input create large differences in the hash generated. Additionally, it is impossible for two different inputs to have the same hash output. It is also impossible to decrypt the hash input from the hash output alone.

Figure 3. The Hash Process, Image from Blockgeeks, "What is Hashing? Under The Hood of Blockchain," accessed December 05, 2018, https://blockgeeks.com/guides/what-is-hashing/.

Figure 4. The Hash Process (Modified Input, Modified Output) Image from Blockgeeks, "What is Hashing? Under The Hood of Blockchain," accessed December 05, 2018, https://blockgeeks.com/guides/what-is-hashing/.

In blockchains, the transactions within a block pass through the hash function, as is the header (unique identifier) for each block. Each new block includes the hash of the previous block, forming the blockchain.[27] Figure 5 represents the use of hash functions within a simplified blockchain.

[27] Karame and Androulaki, *Bitcoin and Blockchain Security*, 35.

DUE TO COPYRIGHT RESTRICTIONS,

IMAGES ARE NOT INCLUDED

IN THIS ELECTRONIC EDITION.

Figure 5. Simplified Bitcoin Blockchain, Image from Blockgeeks, "What is Hashing? Under The Hood of Blockchain," accessed December 05, 2018, https://blockgeeks.com/guides/what-is-hashing/.

Through this use of hash functions, blockchains are immutable, or not alterable. Any attempt to modify a block within the blockchain would change the hash of that block, making the modification identifiable to the other nodes within the distributed network, invalidating the transaction in question. In reality, attempts to change data are feasible. However, the other nodes in the network will reject the change and interpret the amendment as an integrity attack. It is best to think of a blockchain or distributed ledger as tamper evident.[28]

In discussing blockchain security, confidentiality and privacy are important issues. The addition of public and private security keys to either public or permissioned blockchains is quite common. Traditional Public Key Infrastructure (PKI) examples include Common Access Cards (CAC) in the US Military and Defence Remote Electronic Access and Mobility Services (DREAMS) for the Australian Defence Force. In simpler terms, a public key is like the address of a mailbox, information that the owner of the mailbox shares with the public. In this analogy, the

[28] Hanson, Reeson, and Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*, 62.

private key is the physical key used by the owner to access the mailbox, which the owner keeps secure and does not share with the public.[29]

Other Blockchain Examples

Identifying the applicability of blockchain technology outside of the cryptocurrency environment has led to the development of permissionless (public) and permissioned blockchains. Bitcoin is a public blockchain; this means that any participant can read and write data. However, this means that all data in the blockchain is accessible to all participants, a concept that does not resonate well with corporations who want to protect commercially sensitive information and intellectual property. These concerns led to the creation of permissioned blockchains where access to the blockchain requires authorization and permissions create various levels of accessibility. These restrictions do require an oversight function, where a participant or group of participants to create these permissions and authorizations.[30]

Following the launch of Bitcoin in 2008, the technology expanded, and blockchain technology now supports a number of applications including multiple cryptocurrencies, smart contracts, as well as other applications. While Bitcoin remains the largest cryptocurrency, Ethereum and Hyperledger have taken the blockchain technology outside of the cryptocurrency environment and are of sufficient maturity that they are also worthy of discussion. Hyperledger is of importance to this monograph, as IBM secured a billion dollar contract to integrate information and technology functions including blockchain to the Australian government, including the Australian Defence Organisation in 2018.[31]

Ethereum is a decentralized platform that runs applications or smart contracts on a blockchain. It incorporates its own cryptocurrency, Ether. Vitalik Buterin, a Canadian of Russian

---

[29] Matthias Heutger and Markus Kuckelhaus, *Blockchain in Logistics* (Troisdorf, Germany: DHL Customer Solutions and Innovation, 2018), 5.

[30] Cottrill, "The Benefits of Blockchain," 22.

[31] Asha McLean, "IBM Scores AU$1b for Whole-of-Government IT," *ZDNet*, accessed October 11, 2018, https://www.zdnet.com/article/ibm-scores-au1b-for-whole-of-government-it/.

descent established Ethereum in 2013. Ethereum used a proof of work consensus mechanism but transitioned to a proof of stake consensus mechanism to reduce wasted computational and energy wastage. Contracts automatically enforced by computer contracts are Smart Contracts. Ethereum has generated a lot of interest due to its programmable platform capabilities. Ethereum is already powering a wide range of early applications in areas such as governance, autonomous banks, keyless access, crowdfunding, financial derivatives trading, and settlement, all by using Smart Contracts.[32]

Ethereum inspired IBM's Open Blockchain. However, unlike Ethereum, it enforces authorization for participation and confidentiality for transactions and is a permissioned blockchain. Open Blockchain was renamed Hyperledger when it became the candidate to become the Linux Foundation's blockchain platform.[33] Hyperledger aims to produce business blockchains using an open architecture and a defined set of layers. Once the nodes achieve consensus, the consensus layer adds a new block to the chain. This method uses far less computational energy to achieve consensus and implementation is possible due to the permissioned nature of the blockchain.[34]

Blockchain – The Shortcomings

Any emerging technology is not without its limitations. Shortcomings for blockchain focus on throughput limitations, data latency, size and bandwidth, security, resource wastage, usability, and forked chains.[35] The use of a permissioned blockchain that does not use PoW as a

---

[32] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman,"BlockChain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2 (June 2016): 13.

[33] Karame and Androulaki, *Bitcoin and Blockchain Security*, 185.

[34] Peter J. Denning and Ted G. Lewis, "Bitcoins Maybe; Blockchains Likely," *American Scientist; Research Triangle Park* 105, no. 6 (December 2017): 4.

[35] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander "Where Is Current Research on Blockchain Technology?—A Systematic Review," ed. Houbing Song, *PLoS One;* 11, no. 10 (October 2016): 13, accessed September 26, 2018, https://search.proquest.com /docview/1825439028/abstract/77028882087408EPQ/1.

consensus mechanism can mitigate the resource wastage and usability limitations that occur in a public blockchain. Likewise, the negation of the usability limitation occurs through training that can be provided to users of a permissioned blockchain, as users of the blockchain have known identities. Therefore, this research does not discuss these concerns.

Throughput and data latency are limitations of blockchain performance concerning transactional speed. According to the CSIRO, throughput is the total number of transactions a system can process within a time window, whereas latency is the time required to respond to a single transaction. Blockchains such as Bitcoin and Ethereum are unable to match the network throughput of conventional transaction processing systems. The VISA network, for example, can process 56,000 transactions a second compared to Bitcoin that can process four per second.

The time taken to access historical data from the blockchain, referred to as read latency is superior when compared to conventional, centralized database systems. This superiority is due to the user storing the database, resulting in no network delays. The time taken to verify a transaction within a block, added to the blockchain, and confirmed is referred to as write latency. Experiments using the Ethereum public blockchain identified that the write latency was 3 minutes on average.[36]

Data61 within CSIRO and the University of Sydney have proved that they have been able to overcome both read and write latency concerns through the development of the Red Belly Blockchain. Tests conducted in 2017 and 2018 demonstrated the ability to process 440,000 transactions per second. The ability to incorporate Amazon Web Services (AWS) cloud infrastructure resulted in read latency of only three seconds. These recent demonstrations prove that scalability of blockchain technology is feasible outside of a cryptocurrency context.[37]

---

[36] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 40–41.

[37] Jesse Hawley, "Red Belly Blockchain: Faster, More Secure and Energy Efficient," *CSIROscope*, last modified September 24, 2018, accessed October 29, 2018, https://blog.csiro.au/red-belly-blockchain-faster-more-secure-and-energy-efficient/.

As blockchains retain all previous transactions, the size of the distributed ledger becomes larger the longer the blockchain has been in existence. The size of the blockchain may potentially affect the performance in the future, as the size of the blockchain prevents its usage by participants on more mobile platforms with less storage. Some analysts fear that the size of the Bitcoin file will become unmanageable and "[eclipse] the capabilities of the network that was originally supported by its emergence."[38] Sharding is a proposed solution to this problem, which involves separating the database on the blockchain into independent pieces. Processing of these independent pieces can occur concurrently, improving the throughput of the whole system.[39] Within a permissioned blockchain network, nodes may participate in the consensus mechanism, although not all nodes participate in all aspects of the consensus. Major Barnas proposes that the US Air Force divide their nodes into three categories depending on relative capability (processing speed, storage capacity, and method of network access). This separation would result in nodes that can verify new records as well as generate and transmit new records without needing to store a complete copy of the ledger on all devices.[40]

It might seem ironic that one of the areas of concern regarding the use of blockchain technology includes security. The main concerns revolve around public breaches of both Bitcoin and Ethereum blockchains. Security vulnerabilities include a 51 percent attack, data malleability problems, authentication, and cryptography issues.

As previously discussed, the consensus mechanism achieves data integrity within a blockchain. In a 51 percent attack, nefarious elements gain control of 51 percent (or more) of nodes within the network. In a public PoW blockchain, this would enable adversaries to

---

[38] Hanson, Reeson, and Staples, *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*, 10.

[39] Ibid., 7–10.

[40] Niel B. Barnas, "Blockchains in National Defense: Trustworthy Systems in a Trustless World" (Air University, 2016), 24–25.

authenticate invalid transactions, corrupting the data held within the blockchain.[41] In a permissioned blockchain, mitigation of this risk occurs through identity verification. The Ripple blockchain explores this further. In the Ripple blockchain, a limited number of trusted intermediary nodes complete transactions. All nodes communicate with the wider user base to share transaction information submitted by all users. However, when a new block is required, they refer to a 'Unique Node List' of trusted nodes. If eighty percent of the list agrees, then the transaction is included in the blockchain.[42]

The use of private and public encryption keys is pivotal to the data integrity achieved on a blockchain. Data malleability concerns describe the fact that the digital signatures attached to a transaction do not provide a guarantee that the signatures themselves are authentic. An attacker attempts to intercept, modify and rebroadcasts a transaction, causing the party initiating the transaction to believe that the original transaction was not confirmed. This problem links to that of authentication and cryptography concerns, which the Mt. Gox attack against a Bitcoin wallet company highlights. Researchers have already been able to propose solutions to these problems including the integration of a hardware token, two-factor authentication, or a certification system. Both of these solutions are easier to apply to a permissioned blockchain than compared to a public blockchain. [43]

The basis of Blockchain technology relies on the very fact that it is mathematically impossible to reverse engineer hash functions and the individuality of every hash function generated. However, with the future advent of Quantum Computers, cryptographic keys may be vulnerable to decryption. The counter-argument would be that the advent of Quantum Computers

[41] Yli-Huumo et al., "Where Is Current Research on Blockchain Technology?" 15.

[42] Rothstein, *The End of Money*, 187.

[43] Yli-Huumo et al., "Where Is Current Research on Blockchain Technology?" 15.

would likewise generate new cryptographic functions that can applied retrospectively to the blockchain to maintain its immutability.[44]

Blockchain – The Potential

The potential uses of blockchain technology are numerous. Realization of the transformative power of this emerging technology has not yet occurred. However, the underlying benefits of blockchain, including data transparency, security, asset management, and smart contracts have led to research and investment from a number of industries. Current industry research has centered on citizen services, the retail sector, life sciences, and healthcare systems, manufacturing, as well as supply chains across multiple industries.[45]

Klaus Schwab contends that we are in the midst of a fourth industrial revolution underpinned by digital connectivity enabled by software technology that will fundamentally change society. Using data collected from the World Economic Forum's Global Agenda Council on the Future of Software and Society in 2015, he asserts that blockchain is one technological shift experienced as part of this revolution. From the perspective of technological adoption, he believes the tipping point will be when government collects tax for the first time using blockchain technology. Seventy-three percent of forum attendees anticipated that this tipping point will occur by 2025. Indeed, considering Estonia has already adopted blockchain technology to enhance national identification cards, this timeframe appears feasible.[46]

Blockchain and the Supply Chain/Logistics – The Environment

A supply chain refers to "a network of organizations (including suppliers, manufacturers, warehouses/distribution centers, and retailers) providing a series of value-added activities to

[44] Crosby et al., "BlockChain Technology: Beyond Bitcoin," 17.

[45] Heutger and Kuckelhaus, *Blockchain in Logistics*, 8–11.

[46] Klaus Schwab, *The Fourth Industrial Revolution* (New York: Crown Business, 2017), 160.

transform raw materials into finished products and deliver for consumption."[47] In the context of increased globalization over the past two decades, the supply chain has become increasingly more complex and segregated, as it involves multiple entities who control parts of the supply and very few who have complete ownership. Organizations have looked to technological innovations to help decrease the complexity of the supply chain. Logistics Information Systems (LogIS) encompass the automated systems used to communicate with other units on vertical and horizontal flow of logistics and maintenance information and status.[48] LogIS including Electronic Data Interchange (EDI), warehouse management system (WMS), and radio-frequency identification (RFID) technology have all helped to improve the management of the supply chain.

Globalization of supply chains offers multiple advantages including economies of scale, broadening of the customer and supplier base with geographical diversification, reducing market uncertainty, and increasing revenue. However, the downfalls of a globalized supply chain are acknowledged and documented. Longer lead times, higher risk of disruption, additional inventories (stock redundancy), limited visibility of operations, quality control issues, and supplier issues all lead to the potential for higher overall cost.[49] Within this context, organizations gravitate towards technology in the anticipation that gains in efficiencies occur without losses in effectiveness.

The lack of integration between the LogIS of different organizations inhibits the efficiency and effectiveness of digital supply chains in a globalized environment, which use a range of technological platforms, among numerous organizations while preserving intellectual property. A trust deficit inhibits transparency in between organizations. Don and Alex Tapscott

---

[47] Jose Arturo Garza-Reyes, Arturo, Vikas Kumar, Juan Luis Martinex-Covarrubias, and Ming K. Lim, *Managing Innovation and Operations in the 21st Century* (Boca Raton: CRC Press, Taylor & Francis Group, 2018), 58.

[48] US Department of the Army, *Army Regulation 750-1, Army Materiel Maintenance Policy* (Washington, DC: Government Printing Office, 2013), 203.

[49] Garza-Reyes et al., *Managing Innovation and Operations in the 21st Century*, 59.

posit that global supply chains are the next candidate for the adoption of blockchain to enhance operations. They believe that "decentralizing traditional supply chains and combining them with artificial intelligence, additive manufacturing, and the growing Internet of Things [will] produce new value networks that scale to the demand of both machines and human beings."[50]

The CSIRO used the adoption of blockchain within supply chains as one of its three case studies in its report *Risks and Opportunities for Systems Using Blockchain and Smart Contracts.* Their research contends that supply chains are a highly promising domain for the adoption of blockchain technology. Blockchain provides the industry with the opportunity to integrate information exchange, improve supply chain quality, demonstrate provenance, and reduce the cost of regulatory approvals.[51] In summary, blockchain has the potential to help organizations within global supply chains to overcome the trust deficit and achieve transparency of information.

Methodology

This thesis will use qualitative research methods to identify the impacts of incorporating blockchain technology within the Australian Army's LogIS. Qualitative research is appropriate because the problem requires further exploration.[52] While qualitative research is available analyzing the impact of blockchain technology for commercial logistics providers, there has not been research conducted into the impact on military LogIS. Rigor is integrated into the qualitative research by reducing bias and achieving fourth generation evaluation parallel criteria as proposed by Guba and Lincoln in their work, *Fourth Generation Evaluation.* These criteria are credibility, transferability, dependability, and confirmability.[53]

---

[50] Tapscott and Tapscott, *Blockchain Revolution*, viii.

[51] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 46.

[52] John W. Creswell, *Qualitative Inquiry & Research Design: Choosing among Five Approaches*, 2nd ed. (Thousand Oaks: Sage Publications, 2007), 39–40.

[53] Egon Guba and Yvonna S. Lincoln, *Fourth Generation Evaluation* (Newbury Park: Sage Publications, 1989), 228–251.

The use of an academically recognized methodology for conducting research under the supervision of a monograph director helps the author achieve credibility. "How one determines the extent to which the findings of a particular inquiry have applicability in other contexts"[54] defines transferability. The use of previous research focusing on the impact of blockchain on commercial supply chains establishes transferability. This research is transferred and assessed within a military context using the *Rapid Technology Assessment Framework for Land logistics* (RTAF), developed by the Australian Defence Science and Technology Organisation (DSTO). This framework produced a list of enduring logistic effects that helps to transfer research from the commercial logistics environment into the military context. This framework also assists with the dependability and confirmability of the research conducted, enabling a subsequent researcher to be able to follow the same decision trail used by the initial researcher, and assisting the author to remain objective throughout the conduct of the research.[55]

Limitations

The primary limitations of this thesis are time to complete research, availability of information, and the accessibility of information in the unclassified realm. The time available to research, this topic was limited to eight months. This time limitation has restricted the author's ability to research, analyze, and synthesize the information available in the time available. The time available has affected the scope of the research conducted.

Despite the concept of blockchains originating with Nakamoto's white paper in 2008, the amount of peer-reviewed literature and publications is relatively minimal. Most credible sources have originated since 2016, which is logical given the emerging nature of blockchain technology outside of the context of cryptocurrency. While no literature exists on the use of blockchain

[54] Eileen Thomas and Joan Kathy Magilvy, "Qualitative Rigor or Research Validity in Qualitative Research," *Journal for Specialists in Pediatric Nursing* 16, no. 2 (April 1, 2011): 151.

[55] Susan L. Morrow, "Quality and Trustworthiness in Qualitative Research in Counseling Psychology," *Journal of Counseling Psychology* 52, no. 2 (April 2005): 252.

within the military logistics information systems, the proportion of research focused on the applicability of blockchain technology to supply chains, in general, is favorable. The inclusion of a supply chain case study within the CSIRO 2017 reports is evidence that blockchain technology is suited to this environment.[56]

This thesis is limited to information that is publicly available at the unclassified level. For this reason, there is a reliance on CSIRO publications that indicate general acceptance and direction for the adoption of blockchain technology both within society in general as well as within Australian government agencies. Given the numerous variations of blockchains in existence, the research has primarily focused on permissioned blockchains based on models proposed by IBM, as they commenced the contract for the provision of Australian Government blockchain services in 2018.[57]

Analytical Framework

Although primarily aimed at assessing the suitability of physical objects for adoption into the Australian Army, the broad framework is generally transferable to evaluate the appropriateness of incorporating emerging technology into Australian Army LogIS. The RTAF assists analysts to select technologies for further development based on a requirements-driven perspective. The framework acknowledges that the operational context impacts logistics effects, and solutions for logistics systems need to alleviate identified operational constraints and vulnerabilities. Adoption of technical solutions also needs to ensure that the benefits of adoption outweigh the costs.

The RTAF generated a list of enduring logistics effects required by the Australian Army in support of a spectrum of operations.[58] The utility of adopting blockchain technology within the

[56] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 11.

[57] McLean, "IBM Scores AU$1b for Whole-of-Government IT."

[58] Ivanova and Gallasch, *Rapid Technology Assessment Framework for Land Logistics*, 2.

Australian Army logistics information systems is determined by applying this structure to generalized research on blockchain. The benefits of a blockchain enabled LogIS platform is then compared to the existing centralized network to provide a cost-benefit analysis The sub-questions within question two have been modified to reflect the CSIRO's non-functional requirements for supply chain information systems.[59] Table 1 depicts the original RTAF, and the modifications made by the author. These modified sub-questions are more relevant to blockchain as a technology rather than a physical object. The case study will conclude by considering what investment the Australian Army would need to make to develop blockchain technology into an effective capability, noting that specific financial costs for adopting blockchain are unknown. To enhance the depth of the research, question three also includes the barriers to the adoption of blockchain. This overarching framework was developed by an independent Australian government agency, which further enhances the rigor of research, reduces bias, and enhances the dependability of the research.

[59] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 12.

Table 1. Blockchain Assessment Criteria

RTAF Assessment Criteria	Blockchain Assessment Criteria
1. Is the technology useful?	
a. Does the new technology enable required logistic effects?	
b. Does it help achieve required capacity?	
c. Does it alleviate or work within specific operational constraints?	
d. Does it work within or alleviate key vulnerabilities?	
2. Is it better than the current solution?	
a. Does the new technology increase responsiveness of logistic operations?	a. Does blockchain increase interoperability of LogIS?
b. Does it reduce costs of logistic operations?	b. Does blockchain increase the latency of LogIS?
c. Does it increase flexibility and agility?	c. Does blockchain increase data integrity within LogIS?
d. Does it reduce or optimize the logistic footprint?	d. Does blockchain increase data confidentiality within LogIS?
e. Does it improve sustainability and robustness?	e. Does blockchain increase scalability of LogIS?
f. Does it facilitate situational awareness and total asset visibility?	
g. Does it enable decentralized execution of mission?	
h. Does it improve interoperability and deployability?	
3. What are the costs and Fundamental Inputs to Capability (FIC) for the new technology?	**3. What are the barriers to adoption and Fundamental Inputs to Capability (FIC) for blockchain?**
a. How mature is the technology?	a. How mature is blockchain?
b. What are the initial acquisition costs?	b. What are the barriers to adoption from the perspective of organization and environment?
c. What are the FIC and integration costs?	c. What are the FIC and integration costs?

Source: Created by author using data from Ksenia Ivanova and Guy Edward Gallasch, *Rapid Technology Assessment Framework for Land Logistics* (Fishermans Bend: Land Division, Defence Science and Technology Organisation, Commonwealth of Australia, March 2015), 2.

Research Questions and Hypothesis

The primary research question this research seeks to answer is "what is the impact of incorporating blockchain technology within the Australian Army's LogIS?" A secondary research question this research will answer is "can blockchain technology mitigate vulnerabilities faced by LogIS in cyberspace?" In answering these questions, the author can test the hypothesis that blockchain technology has the potential to decrease the vulnerability of Australian Army LogIS from cyber attacks while also making the supply chain more efficient at all levels of war.

Case Study Blockchain and Australian Army Logistics Information Systems

The Australian Army currently uses a centralized LogIS platform, Military Integrated Logistics Information System (MILIS). Understanding the impact of incorporating blockchain into Australian Army LogIS involves understanding the costs and benefits of the technology itself, a comparison of blockchain against MILIS, while identifying barriers that might prevent adoption and the resources required to realize potential capability. This approach considers technology, organization, and environmental factors when considering the suitability of blockchain within Australian Army LogIS.

How is blockchain useful to the Australian Army logistics function?

In order to ascertain the value that blockchain can provide Australian Army logisticians, it is essential to define the logistics effects that the Australian Army requires. The RTAF generated a list of enduring logistics effects, provided in Table 2. A panel of subject matter experts generated these effects and reviewed them in a workshop setting. Blockchain technology falls within the command and control logistic function, although effects on planning, forecasting, and the potential to facilitate automation would occur across all logistic functions.

Table 2. Enduring Logistic Effects

Logistic Function	Sub-functions
Supply	• Warehousing • Procurement • Demand forecasting • Inventory management and provisioning • Disposal of materiel • Waste disposal and management
Movements and Transport	• Preparation and planning • Terminal operations, including loading, unloading and cross-loading • Distribution: transport of personnel and materiel
Materiel Engineering and Maintenance	• Control of design, inspection, testing • Condition monitoring, calibration, servicing • Classification as to serviceability/engineering certification • Repair • Rebuilding • Modification • Reclamation • Overhaul • Recovery • Salvage/cannibalisation • Evacuation
Infrastructure Engineering and Maintenance – Sustainability Support	• Vertical and horizontal construction: planning, constructing and maintaining infrastructure • Provision of essential services • Obtaining resources in theatre • Waste disposal and recycling
Personnel Support Services	• Personnel administration • Postal services • Welfare services • Management of prisoners of war (POW) • Messing • Accommodation • Catering • Laundry • Shower services • Support to mortuary affairs
Health Services	• Prevention of injuries • Treatment of injuries • Casualty evacuation
Command and Control	• Logistic intelligence analysis in support of the Common Operating Picture (COP) • Maintaining situational awareness • Business intelligence and modelling for decision support • Tactical/operational/strategic planning • Tactical/operational/strategic communication • Control and coordination of specific logistic functions through Logistic Information Systems (LIS) • Development, application and measurement of doctrine, policy, structures, processes • Contract management
Capability Life-Cycle Management (in support of force modernisation and preparedness)	• Identifying capability gaps • Defining capability requirements • Acquiring and integrating capability • Managing fleet in service: rotation, deep maintenance, modification, monitoring fleet health status • Disposal of capability

Source: Ksenia Ivanova and Guy Edward Gallasch, *Rapid Technology Assessment Framework for Land Logistics* (Fishermans Bend: Land Division, Defence Science and Technology Organisation, Commonwealth of Australia, March 2015), 5.

The Chief of Defence Force (CDF) appoints the Commander Joint Logistics, responsible for command and control of logistics at the strategic level. This scope of responsibility includes directing logistics governance and assurance compliance, conducting strategic logistics engagement, negotiating Logistics Support Agreements (LSA), managing and coordinating the delivery of support to an agreed point during operations, and managing the effectiveness of the supply chain.[60] Therefore, at the strategic level, blockchain has tremendous potential to revolutionize logistics processes.

Blockchain can revolutionize the contract management aspect of the logistics function. Smart contracts can streamline LSA negotiations and provide enhanced transparency of the contents of the LSA to all nodes at the tactical and operational levels with permission to access that information. Smart contracts will also be able to remove manual contract management processes and assist in automating contract processes. Smart contracts, in turn, remove the requirement for contract management expertise at every level in all locations of the theatre, as well as reducing the chance of human error in contract management or contract negotiation.[61]

Smart contracts will also remove barriers to participation for service providers. By overcoming the trust deficit, blockchain can remove the current structure of third-party logistics providers coordinating services with sub-contractors. Instead, sub-contractors can enter a smart contract with the Joint Logistics Command directly. The ability to integrate LogIS platforms between suppliers and the ADF should help to flatten the current hierarchy of third-party logistics providers. This integration should result in processes that are more streamlined, economic efficiencies, and data transparency.[62]

---

[60] Commonwealth of Australia, *Land Warfare Doctrine (LWD) 4-0, Logistics* (Canberra: Australian Army, 2018), 44.

[61] Tapscott and Tapscott, *Blockchain Revolution*, lvii–lix.

[62] Heutger and Kuckelhaus, *Blockchain in Logistics*, 17–18.

Commercial research into the benefits of blockchain within the supply chain focuses on the establishment of product provenance. It is not immediately clear how this concept would apply to the military or the Australian Army in particular. However, in looking at the Repair Parts (RPS) supply chain, it is clear that confirmed provenance assists the military in sourcing parts, which comply with high safety standards, particularly from an Army Aviation perspective. It is often difficult to source alternative part providers or buy parts from other nations due to the lack of provenance of parts. The provenance benefit also helps to recall parts and enables the Army to forecast interruptions to the supply chain caused by national disasters or war.[63]

At the operational level, the Director-General Support and the J4 on the Joint Task Force Headquarters execute responsibility for the provision of logistics. These officers are responsible for logistic outcomes from the point of origin to the destination. This responsibility includes the establishment of logistics priorities to enable the operational commander's plan.[64]

Blockchains can improve transparency and traceability in supply chains as well as enable the automation of functions. System transparency facilitates the interoperability of systems and the sharing of information. Ideally, this would result in a reduction of systems, and therefore less data redundancy. Currently, users on operations are required to use MILIS, LNIDS, and CVS to manage necessary inventory.[65] However, these systems are limited to the information available within Defence. Data enters the system at the point that a strategic logistics unit receives it. Blockchain would enable suppliers to enter data into the LogIS once the manufacturer or supplier receives the order. This enables a user to track their demand from the point of production or procurement.

Improved transparency and traceability provide a clear link to improved situational awareness of logistic throughput in support of operations. In turn, this enables logistics

[63] Heutger and Kuckelhaus, *Blockchain in Logistics*, 14–16.

[64] Commonwealth of Australia, *LWD 4-0, Logistics,* (2018), 45.

[65] Sonneveld, "Logistics and Emerging Technology," 163.

commanders to improve planning and coordination in support of operational plans and an enhanced ability to communicate the CSS common operating picture to a broader audience. This improvement helps to prevent culmination and extend operational reach while mitigating risk. Blockchain enabled supply chains have the potential to leverage automated provisioning and data analytics supported by the availability of big data. Once captured, this data analysis has the potential to improve forecasting, provisioning, and CSS simulation in support of operational planning.

"Operational logistics orients on fulfilling the commander's requirement for manoeuvre, fires and effects at decisive points in an operation. This translates into the requirement to predict and replenish operational rates of resource consumption."[66] Throughout history, technical innovations have assisted logisticians in this task. The use of the railroad in conjunction with the telegraph in the American Civil War[67] and the Franco Prussian war greatly improved logistical throughput and greater understanding of logistical requirements.[68]

These same technologies enabled the Prussian mobilization in the Franco-Prussian War and German mobilization at the commencement of World War One. However, in the Battle of the Marne, Moltke the Elder was unable to capitalize on his technical superiority, in part, due to increased consumption, a lack of data transparency at the tactical level, and a capacity differential between the railhead and the front line.[69] Arguably, this problem is similar to that faced today. RFID and other technical solutions have been adopted, but they still rely on a user initiated centralized network in order to respond to demand. Blockchain's decentralized nature provides

[66] Commonwealth of Australia, *Land Warfare Doctrine 3-0, Operations*, (Canberra: Land Doctrine Centre, Australian Army, 2018), 59, accessed September 23, 2017, https://www.cove.org.au/doctrine/lwd-3-0-operations/.

[67] Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York: Free Press, 2002), 26–27.

[68] Martin Van Creveld, *Supplying War: Logistics from Wallenstein to Patton*, 2nd ed. (New York: Cambridge University Press, 2004), 84.

[69] Ibid., 132–134.

the capability to respond to horizontal and vertical demands, finding the most efficient solutions to satisfy demands.

Combat Service Support (CSS) at the tactical level is the remit of the deployed Land Force Component Commander. Sustainment of operations relies on the coordination of tactical CSS with the operational level higher headquarters. Commanders at all levels are responsible for the efficient employment of CSS assets and capabilities while the CSS force element commander is responsible for executing CSS in support of the entire land force in theatre.[70]

From the research available on the commercial applications of blockchain, it is at the tactical level that blockchain would appear to have the least versatility. However, it is through blockchain's distributed and decentralized structure that tactical level logistics has the most to gain. While command relationships can and should remain hierarchical, it is possible for logistics functions to be decentralized. Tasks supported by mission command could translate to smart contracts. For instance, a task to a transport section requires supplies to move from point A to point B, returning to their unit location no later than 1800h. After moving supplies to point B, it might be possible for those transport assets to accept a task of opportunity, potentially moving personnel or stores en route to their unit location, assuming time is permitting. The two units in question do not need to have a command relationship, as long as the task is within the restrictions of their smart contracts.

Similarly, a blockchain supported by data analytics would be able to identify the closest logistics node to satisfy a demand. This approach may mean that the integral logistics node for the Engineer unit satisfies a demand from a nearby infantry unit, without them requiring a command relationship. In these ways, the latent capacity of the supply chain supports the operation, increasing efficiency without inhibiting effectiveness.

[70] Commonwealth of Australia, *LWD 4-0, Logistics* (2018), 46.

The RTAF identifies operational constraints specific to the operation type. However, there are also some common generalized constraints for LogIS platforms regardless of operation type. These generalized constraints include situational awareness for asset tracking, unpredictable supply chains, degraded capacity for local contracts and purchases, collaboration with multi-national and non-governmental agencies, leading to a strong desire for standardization and interoperability.[71]

The previous discussion on how blockchain can enhance logistics operations at the strategic, operational, and tactical level already identifies that blockchain is capable of achieving or alleviating a number of these operational constraints. Blockchain provides transparency, interoperability, and smart contracts that are the mechanisms used to realize these constraints. However, it is worth discussing connectivity constraints and node responsibilities in order to demonstrate that by implementing a tiered approach, responsibilities of nodes should not exceed communication capacity at the tactical level.

The size of the blockchain over time has the potential to cause concern at the tactical level. However, in the model proposed by Neil Barnas, nodes have layers of responsibility. At the tactical level, nodes would be able to verify new records, as well as generate and transmit new records. At the operational level, nodes would hold a partial version of the blockchain, consisting of only headers of each block. These partial nodes are also able to verify new blocks, new records, and generate and transmit new records.

At the strategic level, with the assurance of bandwidth and connectivity, nodes can complete a full range of actions including storage of complete copies of the blockchain. These nodes can generate blocks, verify blocks, verify new records, and generate and transmit new

[71] Ivanova and Gallasch, *Rapid Technology Assessment Framework for Land Logistics*, 8–17.

records.[72] Implementation of a tiered system helps to alleviate concerns about connectivity and bandwidth restrictions within the theatre.

Australian Army LogIS are vulnerable to cyber attacks motivated to achieve confidentiality, integrity or availability objectives using malware, zero-day exploits, and Distributed Denial Of Service (DDoS) attacks. Confidentiality attacks include gaining access to a network and extracting information and monitoring activities. Examples range from theft to espionage. Integrity attacks involve entering a network to modify data as opposed to extracting information. Availability attacks aim to prevent access to the network; achieved through a Distributed Denial of Service (DDoS) in cyberspace, or through a kinetic effect, that takes the network offline.[73] Blockchain affords an organization the ability to control data through a permissioned blockchain. However, this technology does not help to mitigate against confidentiality motivated cyber attacks, and as such, are not discussed further.

Blockchain technology helps to mitigate an integrity attack on LogIS through its distributed, decentralized network structure and its immutability. As previously discussed, multiple copies of the database prevent the modification of data without the consensus of other nodes within the network. If a node were to attempt to modify the blockchain, it would identify that node as nefarious, providing the Australian Army information on adversaries and their intentions. Blockchain removes a central server or database that is vulnerable to an attack through cyberspace. Instead of denying adversaries access to the network blockchain denies adversaries the ability to modify the data contained in the database.

A DDOS attack prevents authorized users from accessing the network. Attackers accomplish the effect by flooding bandwidth or servers with e-mails or website-access requests. The volume of traffic, usually measured in millions of hits per second, overwhelms the servers

[72] Barnas, "Blockchains in National Defense: Trustworthy Systems in a Trustless World," 24–26.

[73] Pearce, "Identifying an Achilles' Heel: The Vulnerabilities of the Australian Army's Logistics Information Systems in Cyberspace," 87.

causing them to crash.[74] As blockchain technology is decentralized, no single server is vulnerable to a DDOS attack. Multiple nodes in several geographic location, all with a complete copy of the blockchain, make it difficult for an adversary to attack the blockchain writ large. However, it is possible for an adversary to achieve a localized effect by denying access to the blockchain in a specific theatre of operations. This risk is no greater than that within the existing centralized solution.

Is blockchain better than the current solution?

The CSIRO identified that supply chains are complex systems and it is unlikely that a single system will ever encompass the entirety of an industry's supply chain. However, a number of non-functional requirements are essential when considering supply chain systems (or LogIS). These non-functional requirements are interoperability, latency, integrity, confidentiality, and scalability.[75] These requirements determine if blockchain technology is an improvement on the Australian Army's current LogIS platform.

In 2008, the Australian Army introduced the Military Integrated Logistics Information System (MILIS) as part of Joint Project 2077. Australian-developed software application called Mincom Ellipse1 forms the basis of the MILIS platform. It incorporates track and trace capability, RFID technology, is deployable in the field environment, and performs in a communications interrupted environment. MILIS overcomes LogIS duplication and data redundancy identified during deployments to East Timor, Iraq, and Afghanistan.[76] MILIS

[74] Craig Stallard, *At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force* (Maxwell Air Force Base: School of Advanced Air and Space Studies, 2011), 43.

[75] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 12.

[76] Ian Peek, "Military Logistics: Defence Pioneers New Generation of Integrated Logistics - Australian Defence Magazine," *Australian Defence Magazine*, last modified June 1, 2007, accessed October 31, 2018, http://www.australiandefence.com.au/D5C98930-F806-11DD-8DFE0050568C22C9.

processes more than 16 million transactions a year, is fully NATO-compliant, and supports more than 9,000 users across 160 logistics sites.[77]

MILIS is a single point of record for ADF inventory. It is a centralized database, stored on a tier-3 primary data center in Sydney. This data center is capable of system recovery within 24 hours, and holds over a million gigabytes of data, across 153 applications, 412 environments, and 3,363 servers.[78] The data center holds information up to the security classification of secret, and the Australian Signals Directorate certifies its gateway. Following a strategic partnership agreement between Aldersgate and the Chinese multinational Huawei in April 2017, the ADF has announced that once the current contract expires in 2020, the ADF data center will transition back into a facility owned by the Australian government.[79]

Currently, information systems supporting supply chains are unique to the organizations employing them. This structure means that LogIS in the supply chain is organization focused instead of product focused, making it impossible to track products from creation through to consumption. This structure also results in data duplication, as the same product enters multiple LogIS as it progresses through the supply chain. LogIS integrate to varying degrees, from no integration through to partial integration where organizations use common barcodes or RFID tags. Very rarely is there full system integration. Barriers to integration include confidentiality concerns, the lack of standardized information formats and LogIS compatibility problems.[80]

---

[77] "Australia Deploys New Logistics System," *United Press International*, last modified August 19, 2010, accessed October 31, 2018, https://www.upi.com/Australia-deploys-new-logistics-system/70261282227413/.

[78] "Client Case Study: Accenture and Australia's Department of Defence," Accenture, accessed October 31, 2018, https://www.accenture.com/us-en/success-acn-australia-department-defence.

[79] Chris Uhlmann, "Australian Defence Files to Be Moved out of Privately Owned Data Hub after Chinese Buy-In," *ABC News*, last modified June 19, 2017, accessed October 31, 2018, https://www.abc.net.au/news/2017-06-20/security-concerns-over-defence-files-in-data-centres/8632360.

[80] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 12–18.

MILIS is a partially integrated system. MILIS is good at providing transparency and visibility from the strategic level through to the tactical level. However, it is unable to provide information on the supply chain outside of Defence. This lack of interoperability prevents situational awareness, planning, and provisioning primarily at the strategic and operational levels of the Defence organization. Defence barcoding standards conform to GS1 Electronic Product Code Information Services (EPCIS) standards.[81] Blockchain technology would be able to transform this system into a fully integrated system. In a permissioned blockchain, all users on the blockchain would be able to view information on products relevant to them, with commercial competitors unable to view information that does not pertain to their products. Overcoming the trust deficit is essential in expanding the interoperability of LogIS.

In this context, latency is not limited to the transaction or processing time of the information system. It also includes the time taken for documentation exchange to take place. Fundamental to the concept of latency is the concept of data duplication and the number of manual transactions that take place within a LogIS platform.[82]

MILIS has improved the number of automated transactions conducted. However, the proportion of automated transaction is highest at the strategic level and is lowest at the tactical level. Particularly when considering automated transactions conducted in a field environment. This research was unable to compare the transaction processing speed for MILIS and blockchain, as the data for MILIS was unavailable. Concerning latency, blockchain does not provide enhanced capability as it is the software platform that causes latency, data redundancy and manual entry, and physical hardware integration and availability. Therefore, regarding latency, the benefits of blockchain are negligible.

---

[81] Daniel Edwards, *Defence Inventory: Bar-Coding and Packaging Requirements Booklet* (Joint Logistics Command), accessed February 5, 2019, http://www.defence.gov.au/casg/Multimedia/barcode_booklet_supplier_edition-9-8805.pdf.

[82] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 12.

Data integrity, trust that the data held within the database is accurate is essential in being able to conduct logistics operations in the military. An adversary that can modify data held within a LogIS might be able to force culmination or generate enough friction and uncertainty that decision paralysis occurs. While manual demand procedures exist at the tactical level, downtime procedures are less viable at the operational and strategic level. At these levels, downtime procedures generally focus on keeping a manual record of transactions and conducting a bulk upload on the restoration of connectivity. If data in the database is corrupt, these processes cease to be effective.

MILIS is a centralized network; therefore, while restoration of a backup copy of the database can occur within 24 hours, if gradual data manipulation has occurred, it would be difficult to identify with any certainty which version of the database to restore. In a decentralized distributed network, blockchain technology prevents the amendment of historic transactions, and requires the verification of new transactions, making data compromises difficult, while maintaining data integrity. Data integrity is a key vulnerability in a centralized database system, and a key strength within a blockchain enabled database.

Confidentiality in this context refers to the privacy of information shared between participants within the same supply chain. The tradeoff for collaborators is the benefit in sharing data compared to the cost of competitors gaining access to commercial-in-confidence information. This information can include identities of participants, trade volume, prices, and delivery times.[83]

The current system protects the confidentiality of information, at the cost of transparency and integration. Actors within digital supply chains are thus indicating that they place a high value on the confidentiality of their information, even at the cost of efficiency. However, blockchain may be able to remove the dichotomy of this situation and enable both confidentiality

[83] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 18.

as well as transparency and integration. Even using blockchain technology, the design structure of the blockchain needs to identify confidentiality of information as a primary requirement. A permissioned or private blockchain does not automatically protect commercial-in-confidence information. The encryption of confidential data can still occur; this requires participants to exchange keys off the chain in order to access data and maintain confidentiality and comes at the cost of latency.[84] Therefore, a permissioned blockchain provides part of a solution towards a transparent, integrated supply chain that can maintain data confidentiality. However, identification of this requirement during the formulation of the blockchain structure is essential. It is an improvement on the current system but does not solve all problems for all participants in the supply chain.

Any LogIS platform needs to be able to conduct transactions at speeds comparable to the throughput requirement. This requirement refers to scalability. In a fully integrated supply chain, there would be many supply chain processes, conducted by multiple parties in progress at any time; this requires LogIS to be able to conduct a much larger volume of transactions than are currently conducted by a single LogIS system within an isolated or partially integrated network.

There is no data to indicate that scalability is a concern within MILIS, and as there is no intention for MILIS to increase its scope through integration with other LogIS platforms, there is no benefit in discussing its ability to scale outside of its current capacity. Scalability has been a prominent concern within research conducted on blockchains. As previously discussed, these concerns have their roots within the cryptocurrency realm where blockchains are public, and a proof of work consensus mechanism verifies the transactions. Recent tests conducted by the CSIRO on the Red Belly blockchain indicate that a permissioned blockchain using a proof of stake algorithm removes concerns regarding blockchain scalability.[85] Both MILIS and a

[84] Staples et al., *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*, 18.

[85] Hawley, "Red Belly Blockchain."

blockchain technology enabled databases appear capable of conducting transactions commensurate with the throughput required by the network in which they operate. Therefore, there appears to be no benefit to a blockchain enabled system pertaining to scalability.

The key non-functional requirements for supply chains of interoperability, latency, integrity, confidentiality, and scalability provide insight when comparing blockchain enabled LogIS networks against a hypothetical blockchain enabled LogIS network. Against these criteria, blockchain is an improvement over current LogIS platforms, based on the interoperability, integrity and confidentiality criteria. Furthermore, even if the whole supply chain does not adopt blockchain, it would appear that blockchain is worthy of adoption within the Australian Army in order to benefit from the immutability and integrity assured by blockchain technology.

What are the barriers to adoption and Fundamental Inputs to Capability (FIC) required to implement blockchain?

As blockchain is an underlying technology, it is appropriate to look at the intangible costs to the adoption of blockchain. Kirk Patterson, Curtis Grimm, and Thomas Corsi modeled the key factors influencing the adoption of supply chain technology. They identified the following set of variables as having a significant impact upon the pace of technology adoption: firm size, organizational structure, integration of supply chain strategy with overall corporate strategy, past financial performance, supply chain partner pressure, transaction climate, and environmental uncertainty.[86] The RTAF identifies the costs of new capability regarding Fundamental Inputs to Capability (FIC). FIC requirements include incorporating personnel, organization, collective training, major systems, supplies, facilities, support and command and control mechanisms.[87] These factors identify any barriers to the adoption of blockchain as well as identifying the FIC

[86] Kirk A. Patterson, Curtis M. Grimm, and Thomas M. Corsi, "Adopting New Technologies for Supply Chain Management," *Transportation Research Part E: Logistics and Transportation Review* 39, no. 2 (March 2003): 95.

[87] Ivanova and Gallasch, *Rapid Technology Assessment Framework for Land Logistics*, 34.

requirements needed to support the Australian Army in adopting blockchain technology within its LogIS networks.

Barriers to the Adoption of Supply Chain Technology

The Australian Bureau of Statistics quantifies a large business as those comprising 200 or more employees.[88] The Australian Army is small compared to its allies and operational partners. However, with 30,410 members[89] the organization meets the definition of a large organization. This distinction is important as Patterson et al. argue that the larger the organization, the more likely it will be to adopt supply chain technology. [90]

Research suggests that the more decentralized the organization, the more likely it will be to adopt supply chain technology.[91] It would be difficult to argue that the Australian Army is not a hierarchical, centralized organization. Indeed, the First Principles Review of the Department of Defence in 2015 that identified as many as twelve layers of management compared to a best practice standard of seven. However, the Australian Army is progressing toward a leaner hierarchical structure. Importantly, Patterson et al. also suggest that firms that allow decentralized decision-making throughout their organization may engage in environmental scanning, leading to greater awareness and appreciation of potential innovations. According to this measure, the

[88] Jan A. Swanepoel and Anthony W. Harrison, *The Business Size Distribution in Australia* (Canberra: Economic and Analytical Services Division, Department of Industry, Innovation and Science, 2015), 4.

[89] Greg Moriarty and Angus Campbell, *Defence Annual Report 2017-18: Chapter 7 - Strategic workforce management*, (Canberra: Department of Defence, October 2, 2018), 81, accessed November 1, 2018, http://www.defence.gov.au/annualreports/17-18/Chapter7.asp.

[90] Patterson, Grimm, and Corsi, "Adopting New Technologies for Supply Chain Management," 99.

[91] Ibid.

inculcation of a mission command philosophy[92] as well as a renewed focus on innovation,[93] the Australian Army is demonstrating that its organizational structure would not prohibit the adoption of supply chain technology.

Research indicates that less successful organizations are more likely to adopt supply chain technology. Integral to this theory is that the alignment of an integrated supply chain and logistics strategy with firm strategy is also vital for firm success.[94] It is beyond the scope of this research to determine the relative success of the Australian Army. However, it is possible to make a historical assessment of the success of the Australian Army to align its logistics strategy within its overarching organizational strategy.

David Beaumont argues, "the chronically low priority afforded to the Army's logistics over the last 15 years has created an inappropriate level of risk in the force's operational sustainability."[95] Indeed, the Australian National Audit Office study into the Management of Australian Defence Force Deployments to East Timor confirmed the limitations on the ADF at the time to sustain forces in 'low intensity' conditions. Through this lens, it would appear that logistical performance on operations in 1999 needed improvement.[96] These assessments indicate that alignment between logistics strategy has not aligned with organizational strategy in the past and the Australian Army might be predisposed to adopting supply chain technology to improve its logistical performance.

---

[92] Commonwealth of Australia, *Land Warfare Doctrine (LWD) 1, The Fundamentals of Land Power* (Canberra: Land Doctrine Centre, Australian Army, 2017), 34, accessed September 23, 2017, https://www.cove.org.au/doctrine/lwd-1-the-fundamentals-of-land-power/.

[93] Mick Ryan, *The Ryan Review: A Study of Army's Education, Training and Doctrine Needs for the Future* (Commonwealth of Australia, April 2016), 35, accessed September 23, 2017, https://www.army.gov.au/our-work/publications/our-work/publications/the-ryan-review.

[94] Patterson, Grimm, and Corsi, "Adopting New Technologies for Supply Chain Management," 100.

[95] David Beaumont, "Logistics and the Failure to Modernise," in *On Ops*, ed. Tom Frame and Albert Palazzo (Sydney: UNSW Press, 2016), 137.

[96] Commonwealth of Australia, *Management of Australian Defence Force Deployments to East Timor*, Performance Audit (Canberra: Australian National Audit Office, 2002), 88.

Organizations subjected to greater pressure from supply chain partners will be more likely to adopt supply chain technology. Furthermore, where the transaction climate between supply chain partners is positive, supply chain members will be more likely to adopt supply chain technology.[97] The CSIRO is leading the support for blockchain adoption within Australia, as evidenced by Data61's reports and involvement with the Red Belly blockchain. However, there is a lack of evidence to demonstrate that large logistics providers such as Toll and Linfox are adopting blockchain technology. There is evidence that the US government is investing in blockchain research,[98] although there has been no announcement of the adoption of blockchain within its military LogIS. It is assumed, that military partners and allies, as well as logistics partners still view blockchain technology as 'emerging' and that no external pressure exists for the Australian Army to adopt blockchain technology in the near future.

Organizations that face higher environmental uncertainty will be more likely to adopt supply chain technology. More specifically, demand uncertainty positively relates to technology adoption. The appetite to adopt technological solutions derives from a desire to improve information exchange and manage uncertainty between organizations and their environment.[99] The Australian Army identifies uncertainty as one of the enduring themes of warfare.[100] Operational uncertainty causes demand to fluctuate; this premise is factored into the principles of logistics, requiring logisticians to "balance the need for efficiency with the need for effective support, often characterized by friction, uncertainty, fluidity, and disorder."[101] However, it is

---

[97] Patterson, Grimm, and Corsi, "Adopting New Technologies for Supply Chain Management," 101–102.

[98] US Congress, *The 2018 Joint Economic Report* (Washington, DC: Joint Economic Committee Congress of the United States, March 13, 2018), 236, accessed November 1, 2018, https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf.

[99] Patterson, Grimm, and Corsi, "Adopting New Technologies for Supply Chain Management," 102.

[100] Commonwealth of Australia, *LWD 1, The Fundamentals of Land Power* (2017), 9.

[101] Commonwealth of Australia, *LWD 4-0, Logistics* (2018), 10.

possible that Australian Army logisticians will normalize the constant uncertainty and unpredictability of fluctuating demand. This situation would thus negate the impetus for adopting technological solutions to respond to the uncertain environment.

Overall, the Australian Army demonstrates some factors that indicate the organization should adopt new technology well. However, a previously poor record in adopting technological solutions within the supply chain[102] indicates that barriers to implementation may lie elsewhere. With this in mind, it is essential to look at the Fundamental Inputs to Capability requirements, as technology implementation may hold the key to improving the results of adopting technology within the Australian Army supply chain.

Fundamental Inputs to Capability (FIC) Requirements

The doctrinally established FIC framework is applied to understand the holistic costs associated with implementing blockchain technology within Australian Army LogIS. This framework includes personnel, organization, collective training, major systems, supplies, facilities, support, and command and control to consider potential integration costs for the adoption of new technologies.[103] It is the FIC requirements that enable the Australian Army to achieve the capability potential demonstrated by new technologies.[104] Failure to incorporate FIC into planning may result in the purchase of new technology without realizing the full capability potential of blockchain.

Recruiting, training and retaining personnel with the requisite skill sets is a fundamental enabler required to adopt any new technology. Personnel with specialized blockchain qualifications are required within the strategic logistics agency, Joint Logistics Command. They

---

[102] Sonneveld, "Logistics and Emerging Technology," 169.

[103] The FIC requirements are similar in concept to the US Joint Capabilities Integration and Development System, DOTMLPF-P.

[104] Commonwealth of Australia, *Defence Capability Development Handbook 2014* (Canberra: Director Skilling, Knowledge, Improvement and Policy. Capability Development Group, 2014), 2, accessed November 1, 2018, http://www.defence.gov.au/publications/docs/Defence%20Capability%20Development%20Handbook%20(DCDH)%202014%20-%20internet%20copy.pdf.

would also be required in the Chief Information Officer Group (CIOG) as well as within the Australian Signals Directorate (ASD). Given the Australian Government's focus on blockchain, it is likely that these agencies are already targeting personnel with blockchain skills, knowledge, and experience. It is unlikely that specialized skill sets would be required at the operational and tactical levels of the logistics organization, as blockchain will remain 'unseen' by regular users of the system. Regular users of the LogIS would continue to interact with the database interface, most probably unaware that the blockchain is recording transactions.

From an organizational perspective, personnel establishment, balance of competencies or structure would need not need modification in order to continue to accomplish Defence tasks and to ensure appropriate command and control. However, in order to realize the full capability of a decentralized, distributed database, a review is required into the command and control arrangements and relationships for logistics units. It is illogical to retain a rigid hierarchical supply chain when a blockchain database enables decentralized execution of logistics function. Alternative command status and relationships for decentralized logistic support are worthy of further research in its own right.

The requirement for additional collective training is minimal due to the low requirement for technical expertise at the tactical and operational levels. However, as part of the benefit of blockchain technology is to mitigate vulnerabilities faced by LogIS in cyberspace, the focus for collective training needs to be cyber hygiene from a generalized point of view. Awareness of cyber threats and the technologies in place to mitigate them help to create a layer of defense against exploitation in cyberspace.

Creation of the decentralized distributed network is the critical consideration regarding the major systems requirements to adopt blockchain technology. Given the ICT contract awarded to IBM for the whole of government services, including blockchain, it is likely that the Australian Army will outsource the creation of the network and logical layers in support of the adoption of blockchain. The contractor will thus determine the supply requirements as well as the facilities

and training areas required to support the emerging capability. Therefore, this research excludes these FIC components. While the cost of outsourcing is unlikely to impact specifically on Australian Army Logistics, it is important to capture LogIS blockchain requirements to inform contracted support.

Support criteria are essential enablers that influence the adoption of blockchain technology. Further research into providing tactical nodes with the communications connectivity and bandwidth to make demands on the database is required. Similarly, exploration of the computational cost and procedures associated with a proof of stake consensus mechanism is necessary. In order to realize the full blockchain potential, consultation with commercial logistic providers is essential for planning of blockchain adoption. Without this enabler, the benefits of integration and thus planning and forecasting will not eventuate.

From a command and control perspective, decisions on the blockchain structure and permissions are need to be made early in the adoption process. If integration with commercial partners is an aspiration, then keeping confidentiality as a primary concern is essential. The incorporation of these permissions into doctrine, process, and procedures are essential to ensure security. In a permissioned blockchain, one of the key components is the trusted nodes list, as well as the participants in the blockchain; incorporation of these matters into the design of the blockchain is likely to result in a more successful adoption strategy.

The FIC construct enables comprehensive analysis and planning of capability aimed at focusing attention on the combination and integration of the inputs rather than on the individual inputs separately.[105] This FIC analysis identifies that system analysis and integration requirements are essential components to the adoption of blockchain. LogIS is one part of an ICT network, and integration with internal and external ICT systems is essential. LogIS blockchain requiremnts need to influence contracted support arrangements for the establishment of blockchain within the

[105] Commonwealth of Australia, *Defence Capability Development Handbook 2014*, 2.

ADF as an element of major system requirements. ICT support is a clear enabler for blockchain technology, and ensuring sufficient connectivity and bandwidth needs to be a primary consideration for the adoption of blockchain. Finally, permissions and blockchain structure is fundamentally important, and these command and control considerations need to be incorporated early into the adoption process. The FIC analysis indicates that if the Australian Army executes a comprehensive and coordinated adoption plan, the benefits of blockchain technology will eventuate.

Conclusions and Recommendations

> War is inherently asymmetric and wise opponents rarely target each other's strengths. Every logistic problem that is left as a risk by the Army is a short step from becoming and exploitable vulnerability. If the Army doesn't invest time to properly understand logistic factors that are so fundamental to its combat power, someone with ill intent in mind undoubtedly will.
>
> — David Beaumont, "Logistics and the Failure to Modernise"

Blockchain is not a panacea, it is not the only answer to mitigating vulnerabilities to LogIS in cyberspace, and it is not a holistic solution to develop a lean, efficient, and effective supply chain. However, it has the potential to enhance the existing supply chain and make it more resilient against cyberspace attacks. While blockchain is unlikely to solve all vulnerabilities faced by LogIS, it should be part of the solution.

Blockchain technology has significant potential to revolutionize the supply chain for the Australian Army. This research suggests that blockchain has significant application within the command and control logistics effect function. These applications include enhanced visibility and tracking ability, which facilitates more effective provisioning and planning at the strategic, operational, and tactical levels. Blockchain has the potential to enhance the Australian Army supply chain, specifically concerning interoperability, data integrity, and confidentiality. Therefore, this research has answered the primary research question, 'what is the impact of incorporating blockchain technology within the Australian Army's LogIS?'

LogIS in cyberspace are vulnerable to a whole range of confidentiality, integrity, and availability cyberattacks. Blockchain has the potential to become part of the solution to mitigate these vulnerabilities. Blockchain is key to protecting against cyber attacks that threaten data integrity, and when incorporated with cloud technology it can mitigate the effects of a DDOS attack. However, there is no evidence to suggest that blockchain provides a mitigation effect against a confidentiality motivated cyberattack. This assessment answers the secondary research question, 'can blockchain technology mitigate vulnerabilities faced by LogIS in cyberspace?'

The original hypothesis for this research was that blockchain technology has the potential to decrease the vulnerability of Australian Army LogIS from cyber attacks while also making the supply chain more efficient at all levels of war. The research conducted partially supports this hypothesis, with some types of cyber attacks mitigated by blockchain technology. The adoption of blockchain technology does not indicate that the supply chain would become more efficient, there were no identified cost or time-saving indications. However, it is likely that the supply chain would become more effective at all levels of war, primarily in response to increases in interoperability and data transparency.

The research conducted recommends the implementation of a permissioned blockchain utilizing a proof of stake or proof of activity consensus mechanism to mitigate vulnerabilities of LogIS within the cyber domain. Blockchain also demonstrates significant potential to enhance transparency, interoperability, confidentiality, and data integrity. It provides the mechanism to overcome the digital trust deficit, enabling enhanced cooperation with commercial supply chain partners. However, despite the significant technological potential that blockchain provides "it may be that the most significant challenges in implementing IT are not technical in nature, but human."[106]

[106] Dawn M. Russell and Anne M. Hoag, "People and Information Technology in the Supply Chain: Social and Organizational Influences on Adoption," *International Journal of Physical Distribution & Logistics Management* 34, no. 2 (February 2004): 103.

Bibliography

Accenture. “Client Case Study: Accenture and Australia’s Department of Defence.” Accessed October 31, 2018. https://www.accenture.com/us-en/success-acn-australia-department-defence.

Barnas, Niel B. “Blockchains in National Defense: Trustworthy Systems in a Trustless World.” Air University, 2016.

Beaumont, David. “Logistics and the Failure to Modernise.” In *On Ops*, edited by Tom Frame and Albert Palazzo, 136 - 54. Sydney: UNSW Press, 2016.

———. *Transforming Australian Army Logistics to Sustain the Joint Land Force*. Australian Army Occasional Paper. Future of Army Series. Canberra, ACT: Commonwealth of Australia, October 2017. Accessed August 16, 2018. https://www.army.gov.au/sites/g/files/net1846/f/transform_logistics_b5_faweb.pdf.

Blockgeeks. “What is Blockchain Tecchnology.” Accessed December 05, 2018, https://blockgeeks.com/guides/what-is-blockchain-technology.

———. “What is Hashing? Under The Hood of Blockchain.” Accessed December 05, 2018, https://blockgeeks.com/guides/what-is-hashing/.

Casey, Michael, Bill McBeath, Brigid McDermott, Sam Radoccia, Dan Doles, and Dan Harple. “Emerging Applications of Blockchain for Supply Chains.” PowerPoint Presentation, MIT Enterprise Forum, Cambridge, MA, September 12, 2017. Accessed September 27, 2018. http://www.mitforumcambridge.org/2017/12/video-using-blockchain-supply-chains/.

Cohen, Eliot A. *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime*. New York: Free Press, 2002.

Commonwealth of Australia. *Defence Capability Development Handbook 2014*. Canberra: Director Skilling, Knowledge, Improvement and Policy. Capability Development Group, 2014. Accessed November 1, 2018. http://www.defence.gov.au/publications/docs/Defence%20Capability%20Development%20Handbook%20(DCDH)%202014%20-%20internet%20copy.pdf.

———. *Land Warfare Doctrine (LWD) 4-0, Logistics*. Canberra: Australian Army, 2018.

———. *Management of Australian Defence Force Deployments to East Timor*. Performance Audit. Canberra: Australian National Audit Office, 2002.

———. *Land Warfare Doctrine (LWD) 3-0, Operations*. Canberra: Land Doctrine Centre, Australian Army, 2018. Accessed September 23, 2017. https://www.cove.org.au/doctrine/lwd-3-0-operations/.

———. *Land Warfare Doctrine (LWD) 1, The Fundamentals of Land Power.* Canberra: Land Doctrine Centre, Australian Army, 2017. Accessed September 23, 2017. https://www.cove.org.au/doctrine/lwd-1-the-fundamentals-of-land-power/.

Cottrill, Ken. “The Benefits of Blockchain: Fact or Wishful Thinking?” *Supply Chain Management Review* (February 2018). Accessed August 14, 2018. http://www.scmr.com/article/the_benefits_of_blockchain_fact_or_wishful_thinking.

Creswell, John W. *Qualitative Inquiry & Research Design: Choosing among Five Approaches*. 2nd ed. Thousand Oaks, CA: Sage Publications, 2007.

Crosby, Michael, Nachiappan, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. “BlockChain Technology: Beyond Bitcoin.” *Applied Innovation Review*, no. 2 (June 2016): 16.

Denning, Peter J., and Ted G. Lewis. “Bitcoins Maybe; Blockchains Likely.” *American Scientist; Research Triangle Park* 105, no. 6 (December 2017): 335–339.

Edwards, Daniel. *Defence Inventory: Bar-Coding and Packaging Requirements Booklet.* Joint Logistics Command, Accessed February 5, 2019. http://www.defence.gov.au/casg/Multimedia/barcode_booklet_supplier_edition-9-8805.pdf.

Garza-Reyes, Jose Arturo, Vikas Kumar, Juan Luis Martinex-Covarrubias, and Ming K. Lim. *Managing Innovation and Operations in the 21st Century*. Boca Raton: CRC Press, Taylor & Francis Group, 2018.

Guba, Egon, and Yvonna S. Lincoln. *Fourth Generation Evaluation*. Newbury Park: Sage Publications, 1989.

Hanson, R. T., A. Reeson, and M. Staples. *Distributed Ledgers - Scenarios for the Australian Economy over the Coming Decades*. Canberra: Commonwealth Scientific and Industrial Research Organisation, May 2017.

Hawley, Jesse. “Red Belly Blockchain: Faster, More Secure and Energy Efficient.” *CSIROscope*. Last modified September 24, 2018. Accessed October 29, 2018. https://blog.csiro.au/red-belly-blockchain-faster-more-secure-and-energy-efficient/.

Heutger, Matthias, and Markus Kuckelhaus. *Blockchain in Logistics*. Troisdorf, Germany: DHL Customer Solutions and Innovation, 2018.

Ivanova, Ksenia, and Guy Edward Gallasch. *Rapid Technology Assessment Framework for Land Logistics*. Fishermans Bend: Land Division, Defence Science and Technology Organisation, Commonwealth of Australia, March 2015.

Karame, Ghassan, and Elli Androulaki. *Bitcoin and Blockchain Security*. Artech House information security and privacy series. Boston: Artech House, 2016.

Marr, Bernard. “How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read.” *Forbes,* May 21, 2018. Accessed August 12, 2018. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/.

McLean, Asha. “IBM Scores AU$1b for Whole-of-Government IT.” *ZDNet*, July 4, 2018. Accessed October 11, 2018. https://www.zdnet.com/article/ibm-scores-au1b-for-whole-of-government-it/.

Moriarty, Greg, and Angus Campbell. *Defence Annual Report 2017-18: Chapter 7 - Strategic workforce management*. Canberra: Department of Defence, October 2, 2018. Accessed November 1, 2018. http://www.defence.gov.au/annualreports/17-18/Chapter7.asp.

Morrow, Susan L. "Quality and Trustworthiness in Qualitative Research in Counseling Psychology." *Journal of Counseling Psychology* 52, no. 2 (April 2005): 250–260.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. White Paper. January 11, 2008. Accessed February 5, 2019. https://bitcoin.org/bitcoin.pdf.

Patterson, Kirk A., Curtis M. Grimm, and Thomas M. Corsi. "Adopting New Technologies for Supply Chain Management." *Transportation Research Part E: Logistics and Transportation Review* 39, no. 2 (March 2003): 95–121.

Pearce, Julie. "Identifying an Achilles' Heel: The Vulnerabilities of the Australian Army's Logistics Information Systems in Cyberspace." Master's Thesis, U.S. Army Command and General Staff College, 2018.

Peek, Ian. "Military Logistics: Defence Pioneers New Generation of Integrated Logistics - Australian Defence Magazine." *Australian Defence Magazine*. Last modified June 1, 2007. Accessed October 31, 2018. http://www.australiandefence.com.au/D5C98930-F806-11DD-8DFE0050568C22C9.

Rothstein, Adam. *The End of Money: The Story of Bitcoin, Cryptocurrencies and the Blockchain Revolution*. London: John Murray Learning, 2017.

Russell, Dawn M., and Anne M. Hoag. "People and Information Technology in the Supply Chain: Social and Organizational Influences on Adoption." *International Journal of Physical Distribution & Logistics Management* 34, no. 2 (February 2004): 102–122.

Ryan, Mick. *The Ryan Review: A Study of Army's Education, Training and Doctrine Needs for the Future*. Commonwealth of Australia, April 2016. Accessed September 23, 2017. https://www.army.gov.au/our-work/publications/our-work/publications/the-ryan-review.

Schwab, Klaus. *The Fourth Industrial Revolution*. New York: Crown Business, 2017.

Sonneveld, Allison. "Logistics and Emerging Technology." In *On Ops*, edited by Tom Frame and Albert Palazzo, 155 – 72. Sydney: UNSW Press, 2016.

Stallard, Craig. "At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force." Master's Thesis, School of Advanced Air and Space Studies, 2011.

Staples, M., S. Chen, S. Falamki, A. Ponomarev, P. Rimba, A. B. Tran, I. Weber, X. Xu, and J. Zhu. *Risks and Opportunities for Systems Using Blockchain and Smart Contracts*. Canberra: Commonwealth Scientific and Industrial Research Organisation, May 2017.

Swanepoel, Jan A., and Anthony W Harrison. *The Business Size Distribution in Australia*. Canberra: Economic and Analytical Services Division, Department of Industry, Innovation and Science, 2015.Accessed February 5, 2019. https://www.industry.gov.au/sites/g/files/net3906/f/June%202018/document/pdf/the_business_size_distribution_in_australia.pdf.

Tapscott, Don, and Alex Tapscott. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*. New York: Portfolio, 2018.

Thomas, Eileen, and Joan Kathy Magilvy. "Qualitative Rigor or Research Validity in Qualitative Research." *Journal for Specialists in Pediatric Nursing* 16, no. 2 (April 1, 2011): 151-5.

Uhlmann, Chris. "Australian Defence Files to Be Moved out of Privately Owned Data Hub after Chinese Buy-In." *ABC News*. Last modified June 19, 2017. Accessed October 31, 2018. https://www.abc.net.au/news/2017-06-20/security-concerns-over-defence-files-in-data-centres/8632360.

United Press International. "Australia Deploys New Logistics System." Last modified August 19, 2010. Accessed October 31, 2018. https://www.upi.com/Australia-deploys-new-logistics-system/70261282227413/.

U.S. Congress. *The 2018 Joint Economic Report*. Washington, DC: Joint Economic Committee Congress of the United States, March 13, 2018. Accessed November 1, 2018. https://www.congress.gov/115/crpt/hrpt596/CRPT-115hrpt596.pdf.

US Department of the Army. *Army Regulation 750-1 Army Materiel Maintenance Policy*. Washington, DC: Government Printing Office, 2013

Van Creveld, Martin. *Supplying War: Logistics from Wallenstein to Patton*. 2nd ed. Cambridge: Cambridge University Press, 2004.

Yli-Huumo, Jesse, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. "Where Is Current Research on Blockchain Technology?—A Systematic Review." Edited by Houbing Song. *PLoS One*; 11, no. 10 (October 2016). Accessed September 26, 2018. https://search.proquest.com/docview/1825439028/abstract/77028882087408EPQ/1.