National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE TALE OF TWO CHAINS: DEFENCE SUPPLY CHAIN MODERNIZATION AND SECURITY THROUGH BLOCKCHAIN

Lieutenant-Commander Ryan Van Poppel

JCSP 47

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 47

Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47
2020 – 2021

SOLO FLIGHT

THE TALE OF TWO CHAINS: DEFENCE SUPPLY CHAIN MODERNIZATION AND SECURITY THROUGH BLOCKCHAIN

By Major R.F. Van Poppel

THE TALE OF TWO CHAINS: DEFENCE SUPPLY CHAIN MODERNIZATION AND SECURITY THROUGH BLOCKCHAIN

Rapidly emerging technology is and will continue to change how warfare is conducted. What cannot be forgotten about is the sustainment of warfare. Technology is driving change in how supply chains operate, from the manufacturers and suppliers to the distribution to the end customers, the soldiers. Adversaries are seeing deficiencies in defence supply chains as opportune targets. The Department of National Defence (DND) and the Canadian Armed Forces (CAF) Defence supply chain (DSC) can be described as complex, inefficient, and disjointed. The risks to not modernizing and integrating the DSC are great, given the rapid evolution of technology's impact on supply chain management (SCM), dispersed warfare, and the evolving threats of cyber attacks to defence supply chains. The Vice Chief of Defence Staff (VCDS) also identified supply chain reformation within DND's top four force development priorities.[1] The inclusion of supply chain reformation along with data and digitalization cues the requirement for supply chain modernization. Current trends in SCM see a shift from linear and siloed supply chains to dynamic, integrated, open systems, which Deloitte has termed Digital Supply Networks.[2] What will enable this transition? Still, in the early stages of development and implementation, researchers and private industries indicate that blockchain technology, as an emerging enabling technology can be used in a wide array

[1] Vice-Chief of Defence Staff, *VCDS/DMA Planning Guidance Data and Digitization*: VCD2020-0015391, 02 Nov 2020.

[2] Adam, Mussomeli, Doug Gish, and Stephen Laaper. "The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains," Deloitte University Press, (2016): 2, https://www2.deloitte.com/content/dam/insights/us/articles/3465_Digital-supply-network/DUP_Digital-supply-network.pdf

of applications and industries, including SCM.[3] This paper will demonstrate that Canada's Defence supply chain is vulnerable to a range of threats, and although an emerging technology, blockchain can modernize and integrate the Defence supply chain, shifting it to a digital supply network(s), while also enhancing data and material security. The paper will provide a basic understanding of digital supply networks and blockchain. Next, the paper will examine the requirement for enhanced security within the DSC given the increased cyber threats and vulnerabilities throughout the supply chain. Finally, the paper will look at how blockchain is being integrated with other emerging technologies to improve efficiencies and asset visibility of supply chains, which can transform the DSC to be able to sustain Canada's future fighting force.

Digital Supply Networks Overview

With evolving and readily available technology, supply chains are seeing a transformation in processes and value creation. This transformation is from linear, sequential operations to interconnected, dynamic systems, one in which Deloitte has termed digital supply networks.[4] In traditional supply chains, similar to the DSC, information flows linearly, from X to Y, with each stage depending on the one before it. Inefficiencies created in linear processes have a cascading effect along the supply chain, as in most cases users have limited if any visibility into the other stages. Because of this functions further down the chain are restricted in their capacity to react to any disruptions

[3] Konstantinos,Christidis and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access* 4, (2016): 2292, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408

[4] Adam, Mussomeli, Doug Gish, and Stephen Laaper. "The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains." 2.

in other parts of the supply chain.[5] In digital supply networks data is driven from internal and external to the supply chain and is integrated to provide a holistic view of operations. Nodes throughout the system are interconnected allowing for data, communications, and interactions amongst functions that never existed. This allows for rapid responses to changes or disruptions, increased transparency, collaboration, as well as performance evaluations and forecasting, all of which enable strategic and operational planning and decision-making.[6] While several emerging technologies can enable the transformation from linear to a digital network, blockchain technology stands out as a key enabler to linking the physical and the digital, as its characteristics are similar in moving from siloed central data transactions to distributed networks.

Blockchain Overview

Blockchain is a digitally distributed database of records and transactions that operates through a peer-to-peer network. The data is stored decentralized on all nodes participating on the network; therefore, each participant (node) keeps and has access to a copy of the ledger of transaction information.[7] This structure provides the first two benefits of blockchain, namely, the availability of data and security. Everyone has access to changes to the data in near real-time. It also provides resiliency against a single point of failure. The second security feature is how a blockchain is constructed. Information of a transaction is contained in a 'block.' Each block is timestamped and signed with a cryptographic key or what is known as a hash function. The hash also has reference to the

[5] Ibid., 6
[6] Ibid., 2
[7] SAP Insights. "What Is Blockchain Technology?" (last accessed 03 March 2021) https://insights.sap.com/what-is-blockchain/

previous block, linking blocks together, retaining a complete history of instructions, transactions executed, thereby forming a chain.[8] The cryptographic key and reference to the previous block's hash form an immutable record. For anyone to manipulate the data, they would have to change all the previous blocks' hash functions, which makes it easy to identify an attempt to tamper with transactions. The decentralized and secure nature of blockchain is being seen and researched by several nations, including the U.S., China, and Russia as having incredible potential for defense applications, including modernizing logistics and supply chains.[9] In addition to the security and distribution of data, according to SAP, the other advantages blockchain provides to organizations are transparency, traceability, and automation.[10] These benefits will be expanded upon how they are impacting supply chain management and can modernize and integrate the DSC.

Some may argue that having an open decentralized network, where anyone can access information, does not suit government institutions such as defence that store and transmit secure data or materials. However, The evolution of blockchain allows networks and access to be configured in predominantly two ways, public or 'permissioned.'[11] Public blockchains allow any participants to join the network, as well as to conduct any transactions, including reading and sending transactions throughout the network, while

---

[8] Eric, Piscini, Mark Cotteleer, and Jonathan Holdowsky. "Blockchain: A technical primer." *Deloitte Insights*, 06 February 2018: 3. Last accessed 03 March 2021. https://www2.deloitte.com/global/en/insights/topics/emerging-technologies/blockchain-technical-primer.html

[9] Gilles, Wouters, A. Quintin, R. Vanholme, and G. Clementz. "Blockchain in defence: a breakthrough?" *FINABEL European Army Interoperability Center*, September 2020: 13 Last accessed 12 Feb 2021. https://finabel.org/blockchain-in-defence-a-breakthrough/

[10] SAP Insights. "What Is Blockchain Technology?" (last accessed 03 March 2021) https://insights.sap.com/what-is-blockchain/

[11] T.J., Willink, "On blockchain technology and its potential application in tactical networks," Defence Research and Development Canada Scientific Report – DRDC-RDDC-2018-R033, April 2018, Last accessed 03 March 2021. https://www-deslibris-ca.cfc.idm.oclc.org/ID/10101201

permissioned blockchains allow for the control of roles and access in the network by a central body or a group.[12] This configuration of blockchain seems best suited for military and defence sectors.

Defence Supply Chain Overview

According to DND's Supply Administration Manual (SAM), there are a vast number of stakeholders involved within the DSC, right down to the unit supply technician, base supply, and customer.[13] Figure 1 depicts the stakeholders at the institutional level and their overarching roles and responsibilities. In addition to stakeholders within DND and the CAF one must also take into consideration the entire supply chain, which can include manufacturers, distributors, private organizations that operate within the defence industry, and other government departments (OGDs).[14] With this many participants, there are bound to be friction points. Each step is insular, with little visibility of other parts of the chain. The requirement for trust and transparency amongst a wide array of stakeholders lends well to the benefits blockchain provides.[15] For example, South Korea's Defense Acquisition Program Administration (DAPA) collaborated with other agencies and private industry creating a single system on

[12] T.J., Willink, "On blockchain technology and its potential application in tactical networks," 6-7; SAP Insights. "What Is Blockchain Technology?" (last accessed 03 March 2021) https://insights.sap.com/what-is-blockchain/

[13] Department of National Defence, A-LM-007-100/AG-001, Supply Administration Manual (Ottawa: DND Canada, 2020), 1.3. Roles and Responsibilities: 9-37.

[14] Ibid., 1.3. Roles and Responsibilities: 4.

[15] "Accenture Technology Vision 2018: Intelligent Enterprise Unleashed," Accenture, 2018: 55, Last accessed 03 February 2021, https://www.accenture.com/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

blockchain for its supply chain as a means of transparency, interoperability, and increased efficiencies.[16]

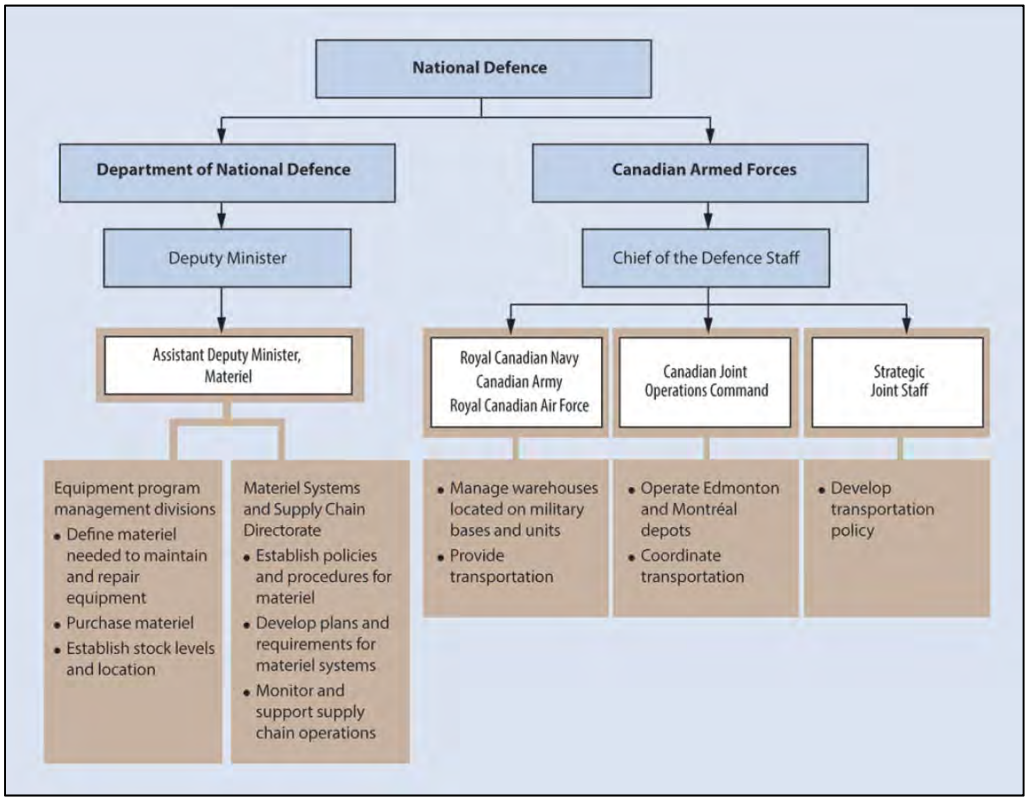

Figure 1 – Roles and responsibilities for supply material

Source: Office of Auditor General of Canada, "Supplying the Canadian Armed Forces – National Defence," Exhibit 3.1.

Examining how data is inputted and processed throughout the DSC, the DSC is very much siloed and not interconnected, unlike digital supply networks. The DSC operates predominately through six information systems. These are the Defence Resource Management Information System (DRMIS), which is one of two of DND's Enterprise Resource Planning (ERP) systems that is SAP-based and is responsible for financial and

[16] Miranda, Wood, "South Korea reveals blockchain plans for defense and arms procurement," *Ledger Insights*. Last accessed 04 March 2021. https://www.ledgerinsights.com/south-korea-blockchain-defense-arms-procurement/

supply/asset management, Ammunition Information Management System (AIMS), Defence Customs and Brokerage System (DCBS), National Movements and Distribution System (NMDS), and Fleet Management System (FMS). These systems have limited to no integration, and in some cases still require manual data inputs, or processes are done analog or through office suite programs (Excel). These systems also do not take into account, nor are integrated with DND's second ERP, Guardian, which is an Oracle-based ERP and is responsible for the Human Resource portion of DND's program. Operating off disjointed systems complicates decision-making as there is reduced visibility of other functions within the supply chain and business processes. Blockchain can connect these systems into a digital enterprise ecosystem and be a mechanism for the exchange of data. Imagine an integrated system in which data such as where people are posted, what are their uniforms, and other material entitlements were all shared throughout the DSC to better inform decision-makers of when resupplies were required, where they were required, and what step in the supply chain an item was located. Blockchain, fully integrated with other emerging technologies, is being touted as the connective tissue of evolving digital supply networks.[17]

Nothing precludes DND from augmenting or amending information infrastructures within the DSC, primarily their ERP, DRMIS. Prior to the introduction of DRMIS in 2012, DND's financial management and material management systems were

[17] Jason, Kilmeyer and Jonathan Holdowsky. "From siloed to distributed: Blockchain enables the digital supply network," *Deloitte Insights*, February 2019 :7 https://www2.deloitte.com/global/en/insights/topics/understanding-blockchain-potential/digital-supply-network-blockchain-adoption.html

separate.[18] According to the SAM changes to the DSC would require the Assistant Deputy Minister (Material) in concert with Director DRMIS under ADM (Data, Innovation, Analytics), and the Strategic Joint Staff (SJS) J4 to fully analyze options.[19] The modernization of Defence Resource Business is listed as one of the ADM Information Management's top issues, and major system upgrades will occur over the next several years.[20] Concerns of implementing a new ERP can be alleviated in that a growing number of information technology companies, including IBM, SAP, and Oracle, provide what is known as blockchain-as-a-service (BaaS). These providers help to develop and maintain blockchain technologies.[21] BaaS acknowledges the potential of blockchain when integrated with other emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Big Data, and Additive Manufacturing (AM), by providing platforms and applications that communicate and interact with each other.[22] Moving the DSC on a blockchain platform would provide an integrated system and connect all stakeholders in the DSC for information exchange, thus creating a trusted secure digital supply network. This secure digital supply network will be required for the evolving threats the DND and CAF will face.

---

[18] Jes Ellacott, "DRMIS: Resource Management at DND," *Frontline Defence*, Vol 9, No 4, 2012. Last accessed 22 February 2021. https://defence.frontline.online/article/2012/4/1235-DRMIS%3A-Resource-Management-at-DND

[19] Department of National Defence, A-LM-007-100/AG-001, Supply Administration Manual (Ottawa: DND Canada, 2020), 1.3. Roles and Responsibilities: 9.

[20] Department of National Defence, Canada. "Assistant Deputy Minister (Information Management) and Chief Information Officer," last modified 03 April 2020, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/defence-101/2020/03/defence-101/adm-im.html

[21] T.J., Willink, "On blockchain technology and its potential application in tactical networks," 16.

[22] T.J., Willink, "On blockchain technology and its potential application in tactical networks," 16; "SAP Galvanizes the Enterprise with Intelligent New Products and Choice," *SAP News Center*, June 6, 2018, https://news.sap.com/2018/06/sapphire-now-sap-intelligent-enterprise-products-choice/

Cyber Security Threat to Supply Chain

According to Canada's Defence policy, *Strong, Secure, Engaged*, "the cyber threat environment is evolving rapidly."[23] DND's platforms, systems, and personnel are highly networked, and vulnerable to adversary cyber actions. The DSC is no different and maybe more vulnerable due to globalization and the requirement of goods and services from around the world. Dr. Samantha Ravich, Chairman of the Foundation for Defense of Democracies' Centre on Cyber and Technology Innovation notes, "the complexity of global economic institutions and processes produces an ocean of transactional data in which supply chain hackers can hide."[24] Dr. Ravich further defines the threat as cyber-enabled economic warfare; this is "a hostile strategy involving non-kinetic attacks upon a nation's economic targets via cyber technology with the intent to weaken its economy and thereby reduce its political and military power."[25] The challenge stems from the globalization of supply chains and the emergence of attacks in which malicious electronic or counterfeit parts are introduced.[26] The attacks are towards the entire defence industry, which leaves hardware, parts, and even systems in which the CAF relies upon unreliable. Storing vast amounts of sometimes sensitive data in the same place is hazardous. Furthermore, manipulated or inaccurate data can have adverse effects on decision-

---

[23] Department of National Defence, Canada, "Strong Secure, Engaged: Defence Policy," (Ottawa: DND Canada, 2017), 72.

[24] Samantha Ravich, and Michael Hsieh. "Leveraging Blockchain Technology to Protect the National Security Industrial Base," *Foundation for Defense of Democracies*, July 10, 2017. 1, https://www.fdd.org/analysis/memos/2017/07/10/leveraging-blockchain-technology-to-protect-the-national-security-industrial-base/

[25] Samantha Ravich, "Cyber Enabled Economic Warfare: An Evolving Challenge (Vol. 2)," The Hudson Institute, November 2015. 29. https://s3.amazonaws.com/media.hudson.org/files/publications/20151117RavichCyberEnabledEconomicWarfareAnEvolvingChallengeVol2.pdf

[26] Samantha Ravich, and Michael Hsieh. "Leveraging Blockchain Technology to Protect the National Security Industrial Base," 1.

making. Blockchain's resiliency in its distributed, immutable audit trail characteristics provides a solution to defend against cyber attacks.[27] Canada's closest ally, the United States (U.S.) and the Department of Defence (DoD) also acknowledge the cyber threat by state and non-state actors towards their supply chain. Even as an emerging technology, blockchain was identified by the U.S. as a potential means to counter such threats. The U.S. Government directed within the National Defense Authorization Act for the fiscal year 2020 that the Secretary of Defense provided a report on the use of blockchain for defense purpose, one specific inclusion being use within defense logistics and supply chain operations.[28] From the National Defence Authorization Act and the follow-on report, the U.S. Defense Advanced Research Projects Agency (DARPA) has been aggressively working with industry partners in researching blockchain defence applications. As an example, Lockheed Martin, a major defence contractor incorporated blockchain into its supply chain risk management and software development processes to counter threats of "manipulation in networked and weapon systems embedded cyber physical systems."[29]

To build on the cyber threat towards the DSC, there is a significant threat of adversaries introducing malicious electronic hardware, software, or counterfeit components into the DSC. As stated in the U.S. DoD's report on potential uses of blockchain:

---

[27] Gilles,Wouters, A. Quintin, R. Vanholme, and G. Clementz. "Blockchain in defence: a breakthrough?": 3.

[28] "National Defense Authorization Act For Fiscal Year 2020," *U.S. Government Publishing Office*, Washington D.C. December 2019: 2793. https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf

[29] "Lockheed Martin Contracts Guardtime Federal For Innovative Cyber Technology," *Lockheed Martin*, 27 April 2017, Last accessed 04 March 2021. https://news.lockheedmartin.com/2017-04-27-Lockheed-Martin-Contracts-Guardtime-Federal-for-Innovative-Cyber-Technology

> However, U.S. adversaries understand that these [advanced weapon] systems are the final stage in an unimaginably vast production and supply network. They understand that it is far safer to surreptitiously alter the design of a rotor blade than to confront an attack helicopter. They understand that infecting the meals ready to eat (MRE) supply chain is infinitely more disruptive than surrounding an infantry squad. The most advanced enemies are skilled at sowing doubt in their adversaries and know that an untrusted supply line is effectively sabotaged.[30]

As early as 2012 the U.S. Senate Committee on Armed Services identified the threat and the importance of a secure trusted supply chain:

> Our committee's report makes it abundantly clear that vulnerabilities throughout the defense supply chain allow counterfeit electronic parts to infiltrate critical U.S. military systems, risking our security and the lives of the men and women who protect it.[31]

An example of the vulnerabilities the report identified was counterfeit electronic components for its Missile Defence Agency's Terminal High Altitude Area Defence missile. If the components would have been installed and failed, there was a strong possibility of the missile failing. Canada and the DND are not impervious to such cyber-enabled economic threats. In 2013 it was reported that counterfeit chips were installed in CC-130J Hercules aircraft that could have left pilots susceptible to blank instrument panels.[32] A further risk to Canada is being a source of counterfeit products, through resale, sub-contractors, as part of finished goods, etc. The 2012 U.S. Senate Committee report stated that China was the major source of counterfeit components, but Canada was

---

[30] "Potential Uses of Blockchain by the U.S. Department of Defense," *Value Technology Foundation*, March 2020. 20. https://www.crowell.com/files/Potential-Uses-of-Blockchain-Technology-In-DoD.pdf

[31] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," May 21, 2012: 1. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

[32] Greg, Weston,. "Fake parts in Hercules aircraft called a genuie risk." *CBC News*, 09 Jan 2013. Last accessed 03 Feb 2021. https://www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862

noted as the third largest reseller.[33] Not having a trusted, collaborative defence supply network from manufacturers and distributors to the end customers, that being soldiers or allies, can degrade relationships and interoperability with allies. As indicated by the U.S. DoD report earlier, there are significant threats to tampering with rations, medicines, and supplies that could undermine a fighting force and operations. For this reason, supply chain transparency is becoming increasingly important. As noted by Dr. Ravich, "The essence of the blockchain solution to supply chain security is the unification of all the transactional activities that constitute a supply chain into a single dataspace so that the transactional fog in which adversaries presently hide can be minimized."[34] It should be noted that blockchain is not ideally suited to identify individual bad actors that could be operating in an organization. Proper vetting and establishing protocols and procedures will still have to occur, but blockchain integrated with other emerging technology such as AI, ML, and or sensors, threats are expected to be significantly reduced.[35]

Blockchain enables transparency and security by establishing the provenance of every transaction, which cannot be altered. Manufactures can be invited on a permissioned blockchain to input every serial number or every step along the production line into the blockchain. Integrated with the Internet of Things, such as sensors, information on materials can be visible to all that have permission. This allows CAF and DND personnel access to a materials transactional history back to its origin preventing any counterfeit. It also enhances the ability to conduct recalls of parts or components. An

---

[33] U.S. Senate Committee on Armed Services, "Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts," 2.

[34] Samantha Ravich, and Michael Hsieh. "Leveraging Blockchain Technology to Protect the National Security Industrial Base," 6.

[35] Ibid., 6-7.

example of such a recall is identifying if a part of a fighting vehicle is thought to be defective. Members can use the blockchain to focus on where parts are located as well as where they originated from, to quarantine and investigate. This can apply to all sources of supplies, including food and medicine.

As militaries, including the CAF, look to modernize, increase efficiencies in their supply chainsand better sustain fighting forces in evolving operating landscapes, they are exploring a range of emerging technologies. One technology that is seen as being disruptive to supply chain management is additive manufacturing (AM), also known as 3D printing. It is seen as a disruptive technology as it will drastically change how the quote-in-quote business will be done. AM allows for the manufacturing of parts and components on an as-required basis and allows for the choice of where manufacturing occurs in the supply chain, for example, in or near operating environments. This could be especially valuable in dispersed, sometimes austere operating environments, or when parts or components are no longer produces or not readily available. AM can reduce costs and time to procure and transport mission-critical supplies to soldiers. Recently, the Canadian Joint Operations Command (CJOC) issued a tasking order to implement AM in a deployed context for such reasons mentioned. AM was to be trialed to mitigate sustainment and parts scaling issues for Op REASSURANCE in Latvia.[36]AM relies on printing from digital catalogs. To maximize the value of AM, militaries should look to decentralize access to digital catalogs. The opportunities for AM within the DSC are great, but there are also risks. As indicated by Nikhil Gupta, Professor of mechanical and

[36] CJOC Tasking Order – Deployed Additive Manufacturing, 3350-1 (A/J4) (RDIMS# 522660), Canadian Joint Operations Command, 18 Dec 2020: 1.

aerospace engineering at New York University, "The integration of digital thread with the physical supply chain increases the attack surface and makes AM supply chain vulnerable to cyber-attacks that lead to defects in physical products."[37] The CAF, in their implementation of deployable AM, must take into account the vulnerabilities in the DSC and how an attack towards AM could impact the security and safety of soldiers and the nation. Blockchain allows for secured decentralized access to the digital thread of parts and components by AM printers in areas of operations. Blockchain's attributes ensure designs from original equipment manufacturers (OEMs) have not been compromised, as the digital thread cannot be altered or deleted. Also, each step of the thread could be traced. The cryptographic decentralized characteristics are reasons why the U.S. Navy and Air Force are currently using blockchain as a platform to securely share AM digital threads to deployed forces. SIMBA Chain, a company born from a grant from DARPA, is providing a blockchain platform as part of a project called "Blockchain Approach for Supply Chain Additive Manufacturing Parts (BASECAMP)."[38] Blockchain can be a platform to fully integrate all aspects of the DSC modernizing it towards a digital supply network.

One of the earliest advantages to supply chains that blockchain has provided is traceability. Because data is immutable and distributed, it is ideal for tracking information

---

[37] Gupta, Nikhil, et al, "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks." *IEEE Access* 8, (2020): 47323, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9026901

[38] "U.S. Air Force extends blockchain supply chain project," *Ledger Insights*, June 2020. Last accessed 14 March 2021, U.S. Air Force extends blockchain supply chain project - Ledger Insights - enterprise blockchain; Jon LCDR, McCarter, "DON Innovator Embraces a New Disruptive Technology: Bitcoin." *Department of Navy*. 22 Jun 2017. Last accessed 14 Mar 2021. DON Innovation: Block Chain (navy.mil)

and materials from origin throughout complex supply chains. Material visibility over a product's path is essential, especially for mission-critical items. As blocks are timestamped, data can be updated as it transits through the supply network. Integrated with IoT such as sensors, blockchain can provide near-real-time visibility of materials. As Brigadier General Mark Simerly, the Commander of the U.S. Defence Logistics Agency Troop Support states:

> In a secure environment, blockchain has potential for military applications at each planning level…leaders can have greater confidence in knowing what resources are on hand, in-transit, or available to request…Having greater confidence in pre-positioned materials, movements of capabilities, and conditions improves operational planning visibility needed for success. Material traceability can be enhanced and can shape the battlefield for successful conditions.[39]

Blockchain's asset visibility can reduce duplication of orders, reduce transportation requirements and costs, and allow for decentralized decision-making, breaking down the siloes. A recent Auditor General's report on the DND's supply chain found that due to poor inventory management, inefficiency processing of requests, and inadequate control over transport costs, DND's "systems and processes often did not ensure timely and efficient delivery of military supplies to the Canadian Armed Forces."[40] Furthermore, 50% of the materials requested were delivered late.[41] DND can look towards private industry leaders like Walmart in how blockchain can improve asset traceability, and as a whole modernize and integrate a complex supply chain. Walmart's Canadian division implemented a blockchain within their operations. The platform integrates blockchain to sensors and GPS within carriers' trucks to track freight shipments and allows for

---

[39] Brig. Gen. Mark T. Simerly and Deaniel J. Keenaghan, " Blockchain for military logistics," *Army Sustainment,* Oct-Dec 2019: 49. https://alu.army.mil/alog/ARCHIVE/PB700201904FULL.pdf

[40] Canada, Office of the Auditor General of, "Supplying the Canadian Armed Forces – National Defence," 5-6, https://opencanada.blob.core.windows.net/opengovprod/resources/.

[41] Ibid., 6.

automatic payment settlement. The data is transmitted on a blockchain network to both Walmart and their freight carriers' ERP systems and allows for real-time visibility as well as analysis of transport costs and confirmation of contracts being fulfilled and triggers final payments.[42]

Conclusion

The vulnerabilities in Canada's defence supply chain (DSC) must be acknowledged. Given the increased threats of cyber enabled economic warfare, counterfeit disruption of supplies, and the lack of trust in data and material integrity, the modernization and integration of the DSC while enhancing security is crucial. Here lies the opportunity to modernize and integrate a disjointed, linear supply chain into a secure trusted digital supply network. Blockchain as an emerging technology can be the enabler to reform the DSC. Blockchain's inherent transparency, traceability, and automation can be used to distribute valuable data and capabilities across multiple domains while protecting against attacks throughout the DSC. There are always risks in adopting new technologies, but the benefits outway the growing vulnerabilities to not modernizing the DSC. Other defence organizations are leveraging blockchain as a promising enabler within their supply chains and other procedures. Blockchain technology will help shift the defence supply chain into the future by integrating the physical and digital, and forming a sustainment environment enabled by collaboration and trust.

---

[42] Lucas, Mearian, "Walmart launches 'world's largest' blockchain-based freight-and-payment network," *ComputerWorld*, Nov 19, 2019, Last accessed 14 March 2021. https://www.computerworld.com/article/3454336/walmart-launches-world-s-largest-blockchain-based-freight-and-payment-network.html

BIBLIOGRAPHY

"Accenture Technology Vision 2018: Intelligent Enterprise Unleashed," Accenture, 2018: 55, Last accessed 03 February 2021, https://www.accenture.com/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

Adams, Victoria. "Why Military Blockchain is Critical in the Age of Cyber Warfare," *ConsenSys Media*, (2019). Last accessed Feb 2021. https://media.consensys.net/why-military-blockchain-is-critical-in-the-age-of-cyber-warfare-93bea0be7619

"Aerospace, Defense Companies Jumping on Blockchain Train." *Material Handling & Logistics* (Jun 21, 2018). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/aerospace-defense-companies-jumping-on-blockchain/docview/2076910124/se-2?accountid=9867

Canada. Department of National Defence, A-LM-007-100/AG-001, *The Supply Administration Manual*. Ottawa: DND Canada, 31 August 2020.

Canada. Department of National Defence, *Strong, Secure, Engaged: Defence Policy,* Ottawa: DND Canada, 2017. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf

Canada, Office of the Auditor General of, "Supplying the Canadian Armed Forces – National Defence," Spring 2020 - Reports of the Auditor General of Canada to the Parliament of Canada – Report 3, 2020. https://www.oag-bvg.gc.ca/internet/English/parl_oag_202007_03_e_43574.html#ex2

Christidis, Konstantinos and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." *IEEE Access* 4, (2016): 2292-2303, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408

CJOC Tasking Order – Deployed Additive Manufacturing, 3350-1 (A/J4) (RDIMS# 522660), Canadian Joint Operations Command, 18 Dec 2020

Ellacott, Jes. "DRMIS: Resource Management at DND," *Frontline Defence*, Vol 9, No 4, 2012. Last accessed 22 February 2021. https://defence.frontline.online/article/2012/4/1235-DRMIS%3A-Resource-Management-at-DND

Flegel, Andreas, M. Stulle, A. Brox, M. Papert. "How blockchain technology boosts Operations Excellence 4.0 of chemical companies: Building trusted supply chains in the chemical industry," *Deloitte,* (2018). https://www2.deloitte.com/content/dam/Deloitte/de/Documents/energy-resources/Chemical-Blockchain-SCM-Whitepaper.pdf

Gupta, Amit. "Introduction to Blockchain," *Chemical Engineering Progress* 116, no. 9 (09, 2020): 37-44. https://search-proquest-com.cfc.idm.oclc.org/docview/2462455245?pq-origsite=summon

Gupta, Nikhil, Akash Tiwari, Satish T. S. Bukkapatnam, and Ramesh Karri. "Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks." *IEEE Access* 8, (2020): 47322-47333, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9026901

Kehoe, Lory, N. O'connell, D. Andrzejewski, K. Gindner, and D. Dalal. "When two chains combine: Supply chain meets blockchain," *Deloitte*, (2017). https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/blockchainsupplychain/IE_C_TL_Supplychain_meets_blockchain_.pdf

Kilmeyer, Jason and Jonathan Holdowsky. "From siloed to distributed: Blockchain enables the digital supply network," *Deloitte Insights*, February 2019. https://www2.deloitte.com/global/en/insights/topics/understanding-blockchain-potential/digital-supply-network-blockchain-adoption.html

McCarter, Jon LCDR. "DON Innovator Embraces a New Disruptive Technology: Bitcoin." *Department of Navy.* 22 Jun 2017. Last accessed 14 Mar 2021. DON Innovation: Block Chain (navy.mil)

Mussomeli, Adam, Doug Gish, and Stephen Laaper. "The rise of the digital supply network: Industry 4.0 enables the digital transformation of supply chains," Deloitte University Press, (2016). https://www2.deloitte.com/content/dam/insights/us/articles/3465_Digital-supply-network/DUP_Digital-supply-network.pdf

"National Defense Authorization Act For Fiscal Year 2020," *U.S. Government Publishing Office*, Washington D.C. December 2019. https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf

Piscini, Eric, Mark Cotteleer, and Jonathan Holdowsky. "Blockchain: A technical primer." *Deloitte Insights*, 06 February 2018. Last accessed 3 March 2021. https://www2.deloitte.com/global/en/insights/topics/emerging-technologies/blockchain-technical-primer.html

"Potential Uses of Blockchain by the U.S. Department of Defense," *Value Technology Foundation*, March 2020. https://www.crowell.com/files/Potential-Uses-of-Blockchain-Technology-In-DoD.pdf

Pournader, Mehrdokht, Yangyan Shi, Stefan Seuring, and S. C. Lenny Koh. "Blockchain Applications in Supply Chains, Transport and Logistics: A Systematic Review of the Literature." *International Journal of Production Research* 58, no. 7 (2020): 2063-2081. https://www-tandfonline-com.cfc.idm.oclc.org/doi/pdf/10.1080/00207543.2019.1650976

Ravich, Samantha, "Cyber Enabled Economic Warfare: An Evolving Challenge (Vol. 2)," The Hudson Institute, November 2015. https://s3.amazonaws.com/media.hudson.org/files/publications/20151117RavichCyberEnabledEconomicWarfareAnEvolvingChallengeVol2.pdf

Ravich, Samantha, and Michael Hsieh. “Leveraging Blockchain Technology to Protect the National Security Industrial Base,” *Foundation for Defense of Democracies*, July 10, 2017. https://www.fdd.org/analysis/memos/2017/07/10/leveraging-blockchain-technology-to-protect-the-national-security-industrial-base/

“SAP Galvanizes the Enterprise with Intelligent New Products and Choice,” *SAP News Center*, June 6, 2018, https://news.sap.com/2018/06/sapphire-now-sap-intelligent-enterprise-products-choice/

SAP Insights. “What Is Blockchain Technology?” (last accessed 03 March 2021) https://insights.sap.com/what-is-blockchain/

Simerly, Mark T. Brig. Gen. and Deaniel J. Keenaghan, “ Blockchain for military logistics,” *Army Sustainment,* Oct-Dec 2019. https://alu.army.mil/alog/ARCHIVE/PB700201904FULL.pdf

Sudhan, Amool, and Manisha J. Nene, “Employability of Blockchain Technology in Defence Applications” *International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, 2017, pp. 630-637. https://ieeexplore-ieee-org.cfc.idm.oclc.org/document/8389247

Underwood, Sarah. "Blockchain Beyond Bitcoin." *Communications of the ACM* 59, no. 11 (2016): 15-17. http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/pdfviewer/pdfviewer?vid=1&sid=9b5f8017-ecb8-4df9-8942-b754439094fc%40pdc-v-sessmgr06

“U.S. Air Force extends blockchain supply chain project,” *Ledger Insights*, June 2020. Last accessed 14 March 2021, U.S. Air Force extends blockchain supply chain project - Ledger Insights - enterprise blockchain

U.S. Senate Committee on Armed Services. “Senate Armed Services Committee Releases Report on Counterfeit Electronic Parts,” May 21, 2012. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

Vice Chief of Defence Staff, *VCDS/DMA Planning Guidance Data and Digitization*: VCD2020-0015391, 02 Nov 2020.

Weston, Greg. “Fake parts in Hercules aircraft called a genuine risk.” *CBC News*, 09 Jan 2013. Last accessed 03 Feb 2021. https://www.cbc.ca/news/politics/fake-parts-in-hercules-aircraft-called-a-genuine-risk-1.1345862

Willink, T.J. “On blockchain technology and its potential application in tactical networks,” Defence Research and Development Canada Scientific Report – DRDC-RDDC-2018-R033, April 2018, Last accessed 03 March 2021. https://www-deslibris-ca.cfc.idm.oclc.org/ID/10101201

Wood, Miranda. “South Korea reveals blockchain plans for defense and arms procurement,” *Ledger Insights*. Last accessed 04 March 2021. https://www.ledgerinsights.com/south-korea-blockchain-defense-arms-procurement/

Wouters, Gilles, A. Quintin, R. Vanholme, and G. Clementz. “Blockchain in defence: a breakthrough?” *FINABEL European Army Interoperability Center*, September 2020. Last accessed 12 Feb 2021. https://finabel.org/blockchain-in-defence-a-breakthrough/