Research Article

Consortium Block chain for Military Supply Chain

Sharifah Saadiah[1], Syarifah Bahiyah Rahayu[2]*

[1,2]Cyber Security Centre, National University Defense of Malaysia, Kuala Lumpur, Malaysia
E-mail: *syarifahbahiyah@upnm.edu.my

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: Few countries are deploying a blockchain technology for their military supply chain management. Blockchain implementation shows a positive impact on a Military Supply Chain Management (MSCM). The existing military blockchain is adopting a private blockchain setting due to sensitivity level of military data. However, the private blockchain allows non-military authorities' involvement. This research is focusing on the secondary data analysis. This paper proposes a new consortium military blockchain for defense shipment. Blockchain layers are introduced to accommodate military authorities and suppliers. Further research in this area may strengthen the traceability and tracking features in the military logistics including military asset shipment and life cycles.

Keywords: Consortium Blockchain, Smart Contract, Military Supply Chain Management

1. Introduction

Blockchain technology is a permanent data storage records in which every transaction information stored in a blockchain cannot be altered, tampered, or deleted once the information is entered into the system (Lashari, 2017; Rejeb & Rejeb, 2020). This technology can also be described as a digital ledger platform and decentralized which its main function is to provide data sharing and transparency of the data within the network systems. Blockchain is using Peer-to-Peer network (P2P) system for data addition, validation, and transactions record in the blockchain platform. Moreover, blockchain data storage is able to contain and records upgraded data and also stored the record's history with a timestamp. Blockchain technology integrates the cryptography approach into the system in order to strengthen data security and privacy. Cryptography is a common ideal approach toward data integrity and confidentiality (Banerjee, Lee, & Choo, 2018).

Blockchain technology provides data sharing platform in the form of the distributed data storage, where all the shared ledgers within the nodes must be identical. The ledger is shared and kept on decentralized networks (Carlan, Coppens, Sys, Vanelslander, & Van Gastel, 2020). The Distributed Ledger Technology (DLT) is a synchronized database system in which an identical digital ledger is shared across multiple participants. DLT has no central data store or administration involvement and the systems function to records the transaction of assets (Rouse, 2017). The blockchain technology system can be either in public, private, or consortium network. A consortium blockchain is also known as a hybrid blockchain. The basic blockchain layer consists of the data layer, network layer, consensus layer, incentive layer, contract layer, and the application layer (Alladi, Chamola, Sahu, & Guizani, 2020). The backbone of the blockchain is the consensus layer in which the data tampering trace-and track performance is depending on the consensus mechanism selections.

Blockchain for Supply Chain Management (SCM) arises the application in food logistics (De Giovanni, 2020; Kamath, 2018; Neil Barnas & Foster Maxwell Air Force Base, 2016; Wagner & Wisnicki, 2019), water supply system (Maouriyan & Krishna, 2019), health system (Clim, Zota, & Constantinescu, 2019; Zubaydi, Chong, Ko, Hanshi, & Karuppayah, 2019), civil industry logistics (Alladi et al., 2020; Krishnapriya & Sarath, 2020) and many more. In general, the adoption of the blockchain technology in SCM offering users a solution related to internal data privacy issues. Blockchain technology for SCM is benefitting users for its useful features in provenance tracking, inventory management, identity verification, shipping logistics, payment efficiency, food supply chain, and automotive supply chain to avoid counterfeits in the shipment process (P. Boobalan et al, 2020).

The purpose of consensus mechanism in the blockchain is to provide verification on the transactions platform. The traceability feature is employed as the element in the blockchain and proven to be suitable for tracing and tracking operation. The traceability element is implemented for these operations of the cryptocurrency transactions to protect the data from being tampered (Gagneja, Goode, Rentos, & Rezk, 2020). Kanwal Gagneja et al. in their study analyze the performance of the blockchain for its traceability of the cryptocurrency transactions. Gavina Baralla et al. proposed a generic agri-food supply chain blockchain-based

traceability integrating a QR code scan to verify the quality and product health using Hyperledger Sawtooth (Baralla, Pinna, & Corrias, 2019).

This paper is proposing a Military Supply Chain Management (MSCM) blockchain for transaction management while integrating the military assets movement tracing system. One of the ways to ensure product authenticity is by having visible accessibility through smart contracts. In this paper, a consortium military blockchain for MSCM is proposed to be integrated with the consensus mechanism that able to control the trace- and track of military asset movement by using the GIS system.

2. Military Block chain

The overall performance of the blockchain implementation is still under research. The early technology adoption shows some promising outcome. Defense Department in countries such as the US, South Korea, Republic of China, and France have deployed the blockchain technology in their military system. Moreover, some of them have implemented the blockchain in their MSCM. The introduction of blockchain technology in managing the procurement for military asset shipment is to improve the conventional SCM system (Rahayu, Jusoh, Kamarudin, & Azahari, 2019b, 2019a). The transparency of the document history and updates can be accessed by all the authorities in the military nodes. The visibility of the product's transaction history is made available and the issues on tampered data could be hindered. Yinjin Lu et al have analyzed and proposed a blockchain model for the military logistics supply chain (Lu, Xu, & Le, 2019). Based on their research, payment risk management, cost management, and entire process management limitation were able to be solved. Thus, the performance of the deployment of blockchain technology may improve military logistics management towards agility logistics.

According to Major Neil B. Barnas, the implementation of the blockchain technology in MSCM could resolve the provenance issues of the circuit board supplied at the depot. In addition, blockchain could deploy track-and-trace mechanisms in the system to allocate the spare part movement (Neil Barnas & Foster Maxwell Air Force Base, 2016). U.S Navy implements the mechanism to track aircraft parts for its fleet of F-18 Hornet multirole fighter jets (Henry S. Kenyon, n.d.). Angus MacGregor-Miller reports that Systems, Applications & Products in Data Processing (SAP) currently deployed the Keyless Signature Insfrastucture (KSI) blockchain technology on the SAP cloud platform to improve the MSCM using Guartime's KSI Technology (MacGregor-Millar, 2017). SAP introduces a KSI Container concept in which the proof of authenticity for every spare part or software component is made available. The digital fingerprint of an asset is utilized, and relevant metadata added to the system such as data on the producer information, serial number, and other relevant data is preserved.

U.S Department of Defense (DoD) is currently still focusing on the research to improve the blockchain architecture for defense logistics to achieve an efficient MSCM operation. The potential of the blockchain establishment in the U.S DoD system in the early stage of implementation shows trustworthy out-turn regarding the data tampering prevention through the validating mechanism in the blockchain (Carrico & Greaves, 2008). Defense Advanced Research Projects Agency (DARPA) in a project for defense logistics proposes the employment of the advanced information technology to control the logistics pipeline called as Advance Logistics Project (ALP). The limitation arises in MSCM is in terms of the visibility of the logistics process, the optimization of scheduling, and the operation flow process between military baseline (Wang, Guan, Jiang, & Yao, 2010). The common problem in defense logistics is the lack of agility and velocity of the logistic process of MSCM. Besides, conventional system is requiring movement control over the military asset requisition and ownership transfer between the supplier and military depot authorities. The system requires a central authority (CA) to control operational procedure of the sales contracts purchased requisition and procurement of purchased order management in the military depot. The process of requesting and transferring of the military assets is lacking in terms of agility because the transactions required only approvals from CA (Akter, Bhardwaj, Lee, & Kim, 2019). This limitation affecting the process at the military base, and directly interrupting operational performance. Moreover, the time and authenticity constraint within the defense logistics processes are also contribution factors which lead to slower operational system. Therefore, MSCM requires a robust and organized information system.

3. Methodology

The research starts with defining the problems in MSCM for defense shipments. The research scope is based on research works done by Tae Hwan Oh et al. and Yinjin Lu et al. After defined the research scope, the research is designed to close the existing problems. Then, the later stage is gathering secondary data. The secondary data consists of academic literatures and relevant case studies related to military blockchains, MSCM operational

routine and in industrial logistics. The gathered data is analyzed using the secondary data analysis (Johnston, 2014). The last stage is to model a new military blockchain for MSCM. The blockchain framework is designed according to the operational procedure of MSCM implemented in Navy Depot. The essential features of military blockchain are outline based on the problem that arises in SCM. The smart contract components are designed based on the requirement of asset provenance documentation. The research methodology process is shown in the Fig. 1 below.

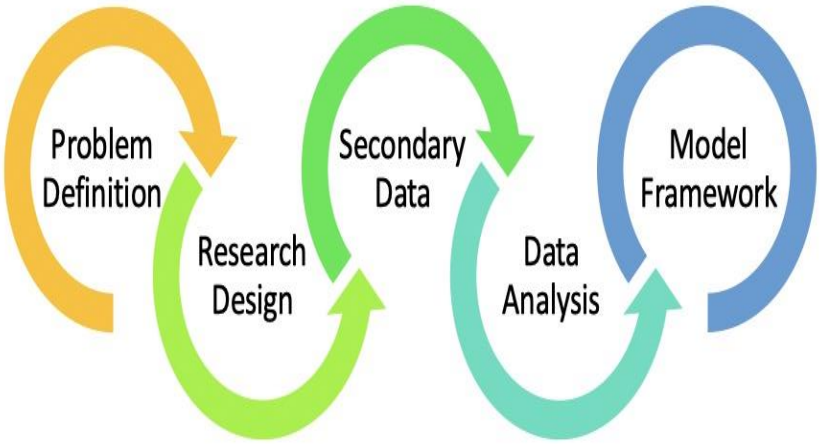

Figure 1. Secondary Data Analysis

4. The Proposed MSCM Block chain

This study is proposing a consortium military blockchain for MSCM. The MSCM blockchain architecture is designed using blockchain technology to manage the supply chain for defense shipment. The consortium blockchain is a semi-decentralized where the system allows multiple organizations to participate together (K R & M, 2020). There are two types of organization involved in the consortium MSCM blockchain, military authority and non-military authority. The military authority are military nodes, while non-military authority are the suppliers and third parties. Due to the involvement of non-military authority (i.e suppliers, third parties), the proposed MSCM blockchain must complies with the MSCM demands in the asset management and the supply order process. They are located in the client network, and military nodes are using P2P network.

The non-military authority nodes are connected to MSCM blockchain via Client mode, Application Programming Interface (API) network system. The Client chain includes a consortium promotor from multiple affiliations to send product quotations to founding members of military depot. Therefore, the quotation shared is genuine and contains related information only. The consortium promotor requires to undergo operating rules for filtering the required information. A superior block is assigned to the block of the founding members. The superior block is the first block of the blockchain to control the first transaction of the purchased order. The roles of this block are to select and distribute the best quotation to subordinate block, to collect purchase requisition, to verify transaction of the purchased product, and to access the information of the ordered product movement. The smart contract connects subordinate blocks in decision making and order placement (Alahmadi & Lin, 2019). Fig. 2 shows a system model of consortium blockchain for MSCM.

The consortium MSCM block chain composes of blockchain layers of Application Layer, Contract Layer, Complementary Layer, Consensus Layer, Network Layer, and Data Layer. The Application Layer is the supply chain (logistic) system. The Contract Layer provides separate smart contract between military authority and suppliers when validating transactions within the subordinate block. In the Complementary Layer, the blockchain development is leveraging RFID application (Oh, Choi, & Chouta, 2012) requires a complementary of Geographical Informational System (GIS) technology (Alahmadi & Lin, 2019). While, the Consensus Layer are using the existing consensus protocols i.e Proof of Stake (PoS) and Proof of Authority (PoA). The block is operating using the P2P Network layer, and this blockchain is implementing the secured integration of blockchain with command information system.

Through separate smart contracts between military authority and non-military authority, the confidential military data in the shared ledger is secured. The proposed smart contract divided into military authorities and non-military authorities, the non-militatry authorities are the participant members who only validate the product certifications document. This is important to ensure the authenticity of the purchased product and to validate the

provenance of the product by the manufacture manager. Participant members are required to provide the validation of product's manufacturing certification, inventory certification and to verify the transfer of ownership and update the validation to the superior block. Fig. 3 shows the protocol addressed for the participant member and the smart contract set for military authorities' contract layer.

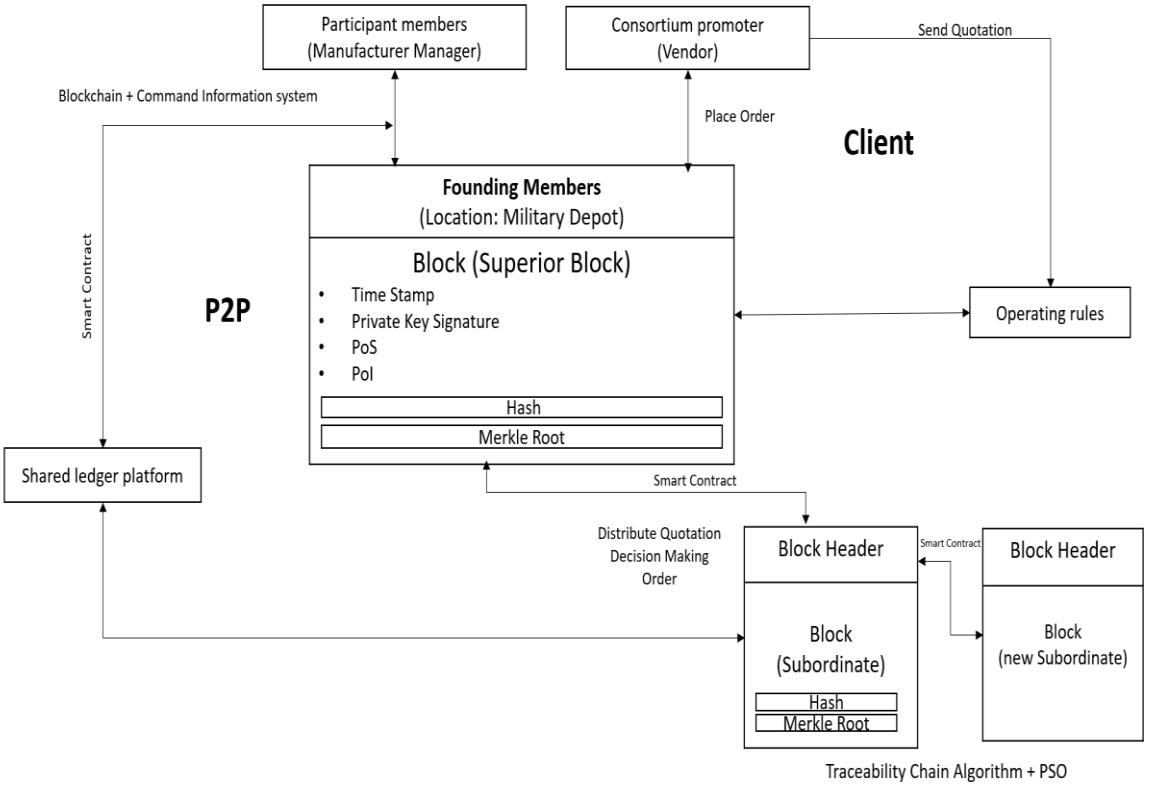

Figure 2. The System Model of Consortium Blockchain for MSCM

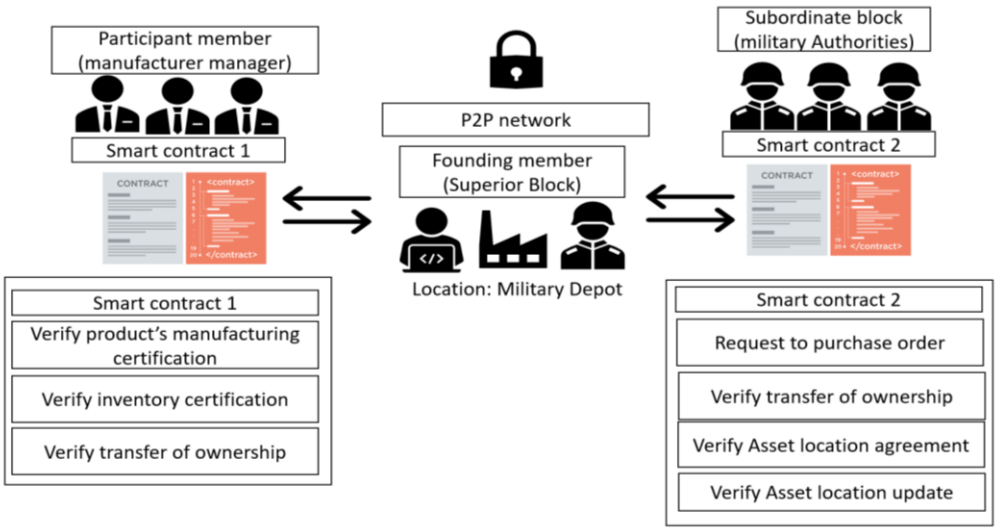

Figure 3. Smart Contract

The shared ledger platform offers the participant to access information from the smart contract. In the proposed system, the shared ledger of the participant members is set with limited data extraction to protect the sensitive data exposure to all participant members. Superior block and the subordinate blocks have an authorization to retrieve a complete version of the shared ledger, while the participant members can only retrieve the information sent through the smart contract. The shared ledger of the superior block and subordinate block is provided with the Uniform Resource Locator (URL) of the GIS link to the Radio Frequency Identification (RFID) tags embedded on the military assets for trace-and track purposes. Through GIS, the real-time movement tracking of the military assets is made visible to the authorized block. The block allows to update information in

the ledger (i.e registering a new location of the asset). Fig. 4 shows the shared ledger information access contents settings in the blockchain systems based on separate smart contracts.

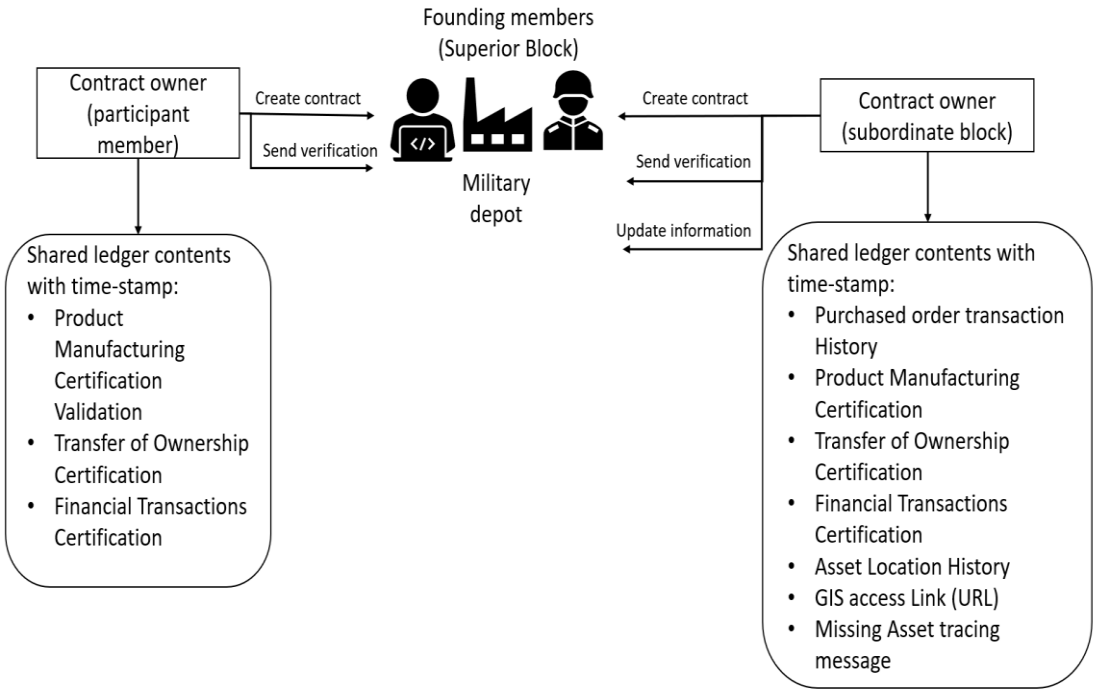

Figure 4. Figure shows the separate smart contract content for participant members and the military authorities

The proposed consortium MSCM blockchain is expected to reduce the fallacy percentage of the military data management risks on the cyber attacker's intrusion from the outsider (i.e suppliers, hackers, cyber criminals). Besides, the consortium MSCM blockchain shall improve the issues on data privacy, where the features in the system can protect the military confidential information from non-military authorities. One of data privacy protection alternatives is using a smart contract in the consortium MSCM block chain.

5. Conclusion

There are several issues in the early stage of blockchain technology deployment such as trustworthiness, security, and data privacy. Based on case studies and academic literatures, blockchain technology for SCM has successfully brought the modernity in a conventional ledger system by alternating it into the electronics digital ledger. The information shared in the digital ledger between the participants in the blocks is expected to be more oriented, secured and organized. The finding shows the consortium blockchain network framework is applicable to be implemented into MSCM. This is due to its effectiveness in securing sensitive data i.e military data. Next step is to develop this consortium MSCM blockchain using blockchain programming language. Moreover, strengthening the contract layer are considered major in this research. Future research is to embed traceability and features in the military logistics including military asset shipment and life cycles.

6. Acknowledgements

The authors would like to acknowledge UPNM for the financial support.

References

1. Akter, R., Bhardwaj, S., Lee, J. M., & Kim, D. S. (2019). Highly Secured C3I Communication Network Based on Blockchain Technology for Military System. In ICTC 2019 - 10th International Conference on ICT Convergence: ICT Convergence Leading the Autonomous Future (pp. 780–783). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICTC46691.2019.8939813
2. Alahmadi, A., & Lin, X. (2019). Towards Secure and Fair IIoT-Enabled Supply Chain Management via Blockchain-Based Smart Contracts. In IEEE International Conference on Communications (Vol. 2019-May). Institute of Electrical and Electronics Engineers Inc.

https://doi.org/10.1109/ICC.2019.8761216
3. Alladi, T., Chamola, V., Sahu, N., & Guizani, M. (2020, June). Applications of blockchain in unmanned aerial vehicles: A review. Vehicular Communications. Elsevier Inc. https://doi.org/10.1016/j.vehcom.2020.100249
4. Banerjee, M., Lee, J., & Choo, K. K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3), 149–160. https://doi.org/10.1016/j.dcan.2017.10.006
5. Baralla, G., Pinna, A., & Corrias, G. (2019). Ensure traceability in european food supply chain by using a blockchain system. In Proceedings - 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain, WETSEB 2019. https://doi.org/10.1109/WETSEB.2019.00012
6. Carlan, V., Coppens, F., Sys, C., Vanelslander, T., & Van Gastel, G. (2020). Blockchain technology as key contributor to the integration of maritime supply chain? In Maritime Supply Chains (pp. 229–259). Elsevier. https://doi.org/10.1016/b978-0-12-818421-9.00012-4
7. Carrico, T., & Greaves, M. (2008). Agent Applications in Defense Logistics (pp. 51–72). https://doi.org/10.1007/978-3-7643-8571-2_4
8. Clim, A., Zota, R. D., & Constantinescu, R. (2019). Data exchanges based on blockchain in m-health applications. In Procedia Computer Science (Vol. 160). https://doi.org/10.1016/j.procs.2019.11.088
9. De Giovanni, P. (2020). Blockchain and smart contracts in supply chain management: A game theoretic model. International Journal of Production Economics, 228. https://doi.org/10.1016/j.ijpe.2020.107855
10. Gagneja, K., Goode, A., Rentos, D., & Rezk, K. (2020). Traceability of cryptocurrency transactions using blockchain analytics. International Journal of Computing and Digital Systems, 9(2), 159–165. https://doi.org/10.12785/IJCDS/090202
11. Henry S. Kenyon. (n.d.). Navy Raises Anchor on Blockchain | SIGNAL Magazine.
12. Johnston, M. P. (2014). Secondary Data Analysis: A Method of which the Time Has Come. Qualitative and Quantitative Methods in Libraries (QQML), 3, 619–626.
13. K R, K., & M, K. (2020). Military Message Passing using Consortium Blockchain Technology. In 2020 5th International Conference on Communication and Electronics Systems (ICCES) (pp. 1273–1278). IEEE. https://doi.org/10.1109/ICCES48766.2020.9138014
14. Kamath, R. (2018). Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. The Journal of the British Blockchain Association, 1(1), 1–12. https://doi.org/10.31585/jbba-1-1-(10)2018
15. Krishnapriya, S., & Sarath, G. (2020). Securing Land Registration using Blockchain. In Procedia Computer Science (Vol. 171). https://doi.org/10.1016/j.procs.2020.04.183
16. Lashari, Z. A. S. I. A. (2017). Blockchain Technology the New Internet. International Journal of Management Sciences and Business Research, April-2017, 6(4), 167–177.
17. Lu, Y., Xu, Z., & Le, X. (2019). Research on the Application of Block Chain Technology in Military Supply Chain: Applications and Techniques in Cyber Security and Intelligence (pp. 915–920). https://doi.org/10.1007/978-3-319-98776-7_109
18. MacGregor-Millar, A. (2017). Combat Cyber Risk in Military Supply Chains with Blockchain.
19. Maouriyan, N., & Krishna, A. G. A. (2019). Aquachain-Water Supply-Chain management using Distributed Ledger Technology. In 2019 Proceedings of the 3rd International Conference on Computing and Communications Technologies, ICCCT 2019. https://doi.org/10.1109/ICCCT2.2019.8824945
20. Neil Barnas, B., & Foster Maxwell Air Force Base, H. (2016). Blue Horizons Fellowship Air University Blockchains In National Defense: Trustworthy Systems In a Trustless World a Research Report Submitted to the Faculty In Partial Fulfillment of the Graduation Requirements.
21. Oh, T. H., Choi, Y. B., & Chouta, R. (2012). Supply Chain Management for Generic and Military Applications using RFID. International Journal of Future Generation Communication and Networking (Vol. 5).
22. P. Boobalan, R. Keerthana, K. Nandhini & P. Vignesh. Multi Feature Detection and Signature Sharing of Android Malware using Blockchain. IIRJET. V-5, I-3, 2020.
23. Rahayu, S. B., Jusoh, N., Kamarudin, N. D., & Azahari, A. M. (2019a). Integrating Military Blockchain In A Supply Chain Management. In The 13th Kuala Lumpur International Communication, Education, Language and Social Science Conference (KLiCELS13). https://doi.org/10.1017/CBO9781107415324.004
24. Rahayu, S. B., Jusoh, N., Kamarudin, N. D., & Azahari, A. M. (2019b). Military Blockchain For Supply Chain Management. Journal of Education and Social Sciences (JESOC), 13(1).

25. Rejeb, A., & Rejeb, K. (2020). Blockchain and supply chain sustainability, 16, 363–372. https://doi.org/10.17270/J.LOG.2020.467
26. Rouse, M. (2017). What is distributed ledger technology (DLT)? - Definition from WhatIs.com.
27. Wagner, N., & Wisnicki, B. (2019). Application of Blockchain Technology In Maritime Logistics, 4, 155–164.
28. Wang, K., Guan, Y., Jiang, D., & Yao, P. (2010). Analysis of information flow control in military supply chain management. In 2010 8th International Conference on Supply Chain Management and Information (pp. 1–4).
29. Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M., & Karuppayah, S. (2019). A review on the role of blockchain technology in the healthcare domain. Electronics (Switzerland). https://doi.org/10.3390/electronics8060679