ZULFAQAR Journal of
Defence Science, Engineering & Technology

Journal homepage: https://zulfaqar.upnm.edu.my/

NEW TRACEABILITY APPROACH USING SWARM INTELLIGENCE FOR MILITARY BLOCKCHAIN

Syarifah Bahiyah Rahayu, Mohd Hazali Mohamed Halip, Afiqah M. Azahari, Nur Diyana Kamarudin, Hassan Mohamed

Cyber Security Centre, National Defence University of Malaysia, Kuala Lumpur, Malaysia

Faculty of Defence Science and Technology, National Defence University of Malaysia, Kuala Lumpur, Malaysia

*Corresponding author: *syarifahbahiyah@upnm.edu.my*

ARTICLE INFO

Article history:
Received
09-06-2020
Received in revised
22-10-2020
Accepted
20-02-2021
Available online
30-06-2021

Keywords:
Consensus Protocol,
Defense Shipment,
Supply Chain

e-ISSN: 2773-5281
Type: Article

ABSTRACT

Current military supply chain management is complex and complicated. Activities such as information, and knowledge sharing among involved parties are prone to cybercriminal. Protection of such private and confidential documents are very important. Therefore, a military supply chain derives a critical need for decentralized and digitize transactions in the ledger. This study is proposing a new traceability chain algorithm for military shipment using blockchain. The development of this traceability chain algorithm is based on algorithm development methodology. The new traceability chain algorithm is expected to trace product movement along with the blockchain network. In addition, it is also believed that this study will provide positive results for defense shipment. Future work is to broaden the scope to other military areas such as threat intelligence.

Introduction

Blockchain is a decentralized digital ledger of transactions (Schrepel, 2018) without using a central point of authority (Nakamoto, 2008) to facilitate transaction recording and tracking assets within the business network (Britchenko et al., 2018). Blockchain starts where users are sharing a copy of the ledger containing their valid transactions and predecessor's hash value in sequential order. Once a transaction occurs, it is time-stamped and transmitted to all the nodes in the system. These transactions are immutable and can be seen by all users. Then, the nodes approve and validate the transaction based on a consensus protocol. The nodes show their acceptance of the transaction by beginning to build the next block in the chain based upon the hash of the accepted block. The subsequent nodes simultaneously updated (Asharaf & Adarsh, 2017; Tosh et l., 2017; Zhang et al., 2014). The hash value keeps the nodes secured from cyber threat. Figure 1 shows the blockchain process (Lewis, 2015)

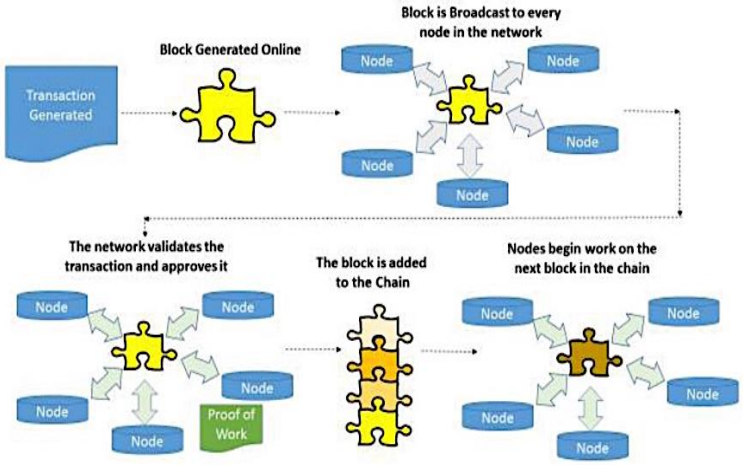

Fig. 1: Blockchain process (Lewis, 2015)

The blockchain first appeared in the 2008 article "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008.). To create digital record keeping and consensus between both parties, he proposed an electronic currency: Bitcoin, based on the de-centralized P2P system design structure which is one of the application of the blockchain (Cao et al., 2017). Currently, few military defenses are exploring the needs of blockchain in defense and security in maximizing its capacity and capability in terms of assets, actions, and operations. For instance, US Department of Defense is applying blockchain technology in its defense and security fields (Simkin, 2018). They are designing non-traditional cyber security systems into business transactions through a concept known as cyber-aware systems engineering to enhance data integrity, speed problem discovery and mitigation, and reduce the volume of regression testing. Incorporating blockchains within the military supply chain will streamline the system by allowing agencies to order only the components they need to enhance front-end operations, rather than expending funds and wait-time on full assemblies. Known as additive manufacturing, 3D printing with blockchain ledgers also can harness 3D printing capabilities to produce military standard parts on site and could resolve issues surrounding intellectual property rights when producing military-standard parts in the field. Beyond supply chain risk management and additive manufacturing, blockchain technologies have been proposed to be implemented on military installations to establish more resilient renewable energy production and consumption, in the event base facilities are connected through a blockchain network (Linkov et al., 2018). Lebanese Army Forces show an interest in blockchain technology to maintain the centralized army (Chedrawi & Howayeck, 2018). Despite the significant growth in blockchain technology, Malaysia regulators have relatively favorable and positive attitude towards the advent of cryptocurrencies, hence several regulations have been proposed to supervise the use of cryptocurrencies in virtual transactions. In Malaysia, blockchain technology involves an essential activity such as retail transaction, secure money transfers and swift authentication particularly in retail market industry (Miraz et al., 2019).

However, the Malaysia Ministry of Defense is still behind this new technology. The current military supply chain management is complex and complicated (Rahayu et al., 2019). Therefore, a military supply chain derives a critical need for decentralized and digitize transactions in the ledger. This study is focusing on the traceability approach for military supply chain blockchain using swarm intelligence. The main motivation of this study is to ensure the defense shipments meet the requirement, assurance and not tempered with (Rahayu et al., 2019). Thus, traceability approach is extremely important in maintaining supply chain shipment of weapons, gear, and spare parts due to the exponential growth of counterfeit military products.

Blockchain Consensus Protocols

To date, there are some popular blockchain consensus protocols such as PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance) and Ripple (Zhang & Lee, 2019). Each of them has their strengths and weaknesses. The existing consensus protocol is designed as a validating mechanism and offering incentives (rewards) to the successful validator (miner). However, this protocol prone to system vulnerabilities such as malicious behavior, potential cyber-attacks, and collusion. For instance, PoW (Back, 2002) algorithm is using intensive energy to validate transactions

but finality may not be suitable for certain use cases (Pilkington, 2015). While, PoS (Castor, 2017) algorithm allows validators to simultaneously create blocks in multiple chains and automatically deducting coins owned or deposited. Furthermore, PBFT (Lamport et al., 1982) may contain a small number of unreliable or potentially malicious nodes to validate a bad block/set of transactions. Furthermore, these algorithms main pitfall is the inability to track and trace nodes along the network. Thus, the new design of the good consensus and traceability protocol would be based on the existing protocol should consider good fault tolerance and how to make the best use of it in the appropriate application scenario. The new traceability chain algorithm is expected to trace product movement along with the blockchain network.

The only blockchain traceability chain algorithm is Takagi-Sugeno (T-S) Fuzzy Cognitive Maps Artificial Neural Network (ANN) (Chen, 2018). This traceability chain algorithm is a mining mechanism to execute the applicability of the digital process in the blockchain. It explores the non-linear transformation that could be expressed as a set of linear subsystems from a nonlinear system using representations to explore inference (Green & Foster, 2005). Unlike consensus protocol, this algorithm needs to be trained until it can reach traceability decision. Up to now, this traceability chain algorithm has not been implemented in any blockchain platform system.

Traceability approach is an effective solution to this problem (Barg et al., 2003; Chor et al., 2000; Safavi-Naini & Wang, 2003; Silverberg et al., 2003). The secured traceability approach at the product and information level and illustrates its configuration through an example military blockchain using three consecutive supply chain partners coded A (manufacturer), B (third party), and C (military depot) as shown in Figure 2 below.

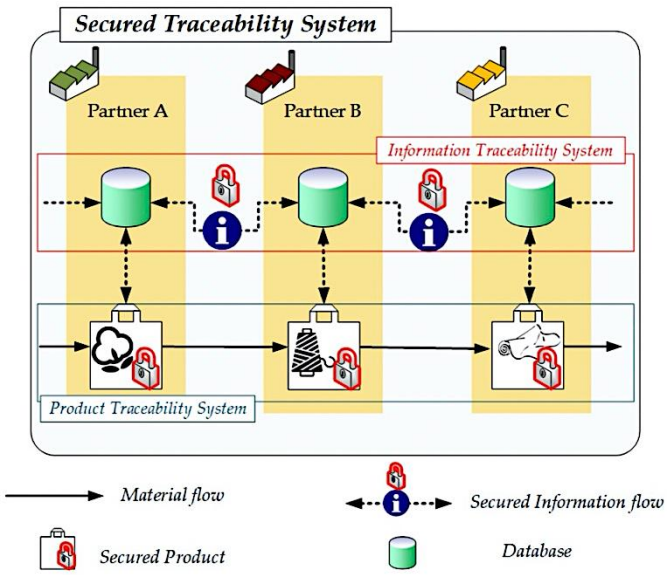

Fig. 2: Secured traceability system (Agrawal, 2019)

Partner B functions as an upstream supplier to Partner C and, at the same time, Partner B has a supplier, Partner A, from whom Partner B receives or purchases inbound materials. To implement a secured traceability system, it is vital that, while exchanging the physical products, the supply chain partners also share related traceability information and simultaneously ensure the security of the information and product. This would require two-component systems; one for information capturing and secure sharing (information traceability system) and the other for physical product exchange while securing it from being copied or lost (product traceability system). These subsystems are connected to form an aggregate system that serves the greater goal of secured traceability in the military blockchain.

Among benefits of using blockchain technology include assurance of supply chain integrity, improve transaction speed, and asset traceability in supply chain. Therefore, military blockchain has the potential to create a smarter and more secure supply chain because the products can be tracked through a clear and solid audit trail with near real-time visibility. All the involved partners in all industries could track materials, determine where they arrived, who received and handled them, and how and when they were transported to the next stage. Military blockchain systems could enable every party involved to track the

product's journey from the manufacturing floor to the military depot. Thus, the records are traceable, validated and secured where it will prevent from being lost or tampered with.

Recently, studies have shown that military has utilize blockchain technology in their defense applications and services. Blockchain technology has been integrated into military operation by providing a shared and distributed database for military intelligence. While, (Wrona & Jarosz, 2019) discuss how blockchain can be used to store metadata describing information received from military application of the Internet of Things (IoT) devices. Moreover, blockchain is also used in military supply chain management applications (Neil Barnas & Foster Maxwell Air Force Base, 2016) to track military service spare parts throughout their life cycles. Blockchain will ensures the spare parts are correctly processed, thus, it provides means for a complete spare parts traceability. In addition, the U.S Navy is turning to blockchain technology to track and manage aviation parts (ITAMCO, 2018). The primary goal of the project is to keep track of aircraft parts for the F-18 Hornet. Blockchain technology can resolve the intellectual property right issues for military standard parts by implementing a secured log for every print, and to support small utility grid for establishing more resilient renewable energy production and consumption.

Thus, a new traceability chain algorithm is expected to trace product movement along with the blockchain network. The new design of the good consensus and traceability protocol should consider good fault tolerance and optimize the usage in the appropriate application scenario. For this research, a consensus and traceability protocol will be designed and deployed on the military blockchain. This algorithm will ensure the authenticity of data and the transactions in the decentralized network. The design will be based on the use of algorithms in artificial intelligence.

Swarm Intelligence

The application of swarm intelligence is proposed to assist the traceability of defense shipment transactions. Swarm intelligence is relatively a new branch of Artificial Intelligence (AI). It models the collective behavior of social swarms in nature, such as ant colonies, honeybees and bird flocks (Ahmed & Glasgow, 2012). Among various swarm intelligence algorithms are Ant Colony Optimization (ACO) (Dorigo & Stützle, 2004), Particle Swarm Optimization (PSO) (Kennedy & Eberhart, 1995) and Artificial Bee Colony Algorithm (Karaboga, 2005). These algorithms have been applied in many areas such as healthcare, bioinformatics, machine learning and industrial related applications. These agents (just like the insects or swarm individuals) would interact each other collectively without main control i.e centralized system. They are self-organizing in coordinating and performing task to achieve their goals. This behavior is much related to blockchain as blockchain are composed of many individual nodes which are relatively homogeneous and with no central control i.e. decentralized system. Thus, this research will mainly focus on two of the most popular swarm intelligences algorithms: ACO and PSO. Based on these two algorithms, a study will propose a new traceability chain algorithm for military blockchain.

ACO in particular inspired by foraging behavior of some ant species. Observing the behavior of ants searching for food, which at first the ants will wander randomly. When an ant finds a source of food, it walks back to the colony, leaving markers or known as pheromones that show the path that have food. When more ants find the paths, there will be a couple of streams to the source of food. Shorter path become stronger as more pheromones dropped by ants every time they bring the food, hence optimizing the 'solution' (Dorigo et al., 2006). Example of solutions that work very well with this algorithm include in solving telecommunication networks routing problems (Di Caro & Dorigo, 1998), solving scheduling problem (Gravel et al., 2002) and finding solution of vehicle routing problems (Bautista-Valhondo & Pereira, 2002).

Invented by Eberhart and Kennedy in 1995, PSO algorithm is a population-based evolutionary algorithm which simulated a cooperative way of animal such as insects, herds, birds and fishes finding food. A bird that closest to the food chirps louder and the other bird swing around it direction (Wang et al., 2017). If there are any other bird become closest to the food compared to the first bird, it will chirp louder. Then, the other birds will veer towards the second bird. This act will be continued until the birds happen upon the food. Over a number of iterations, value in nodes adjusted closer to the node which its value closest to the target. Presently, PSO has been widely implemented in application category such as automation control system (Kechagiopoulos & Beligiannis, 2014; Zhang et al., 2014), communication theory (Das et al., 2014;

Scott-Hayward & Garcia-Palacios, 2014; Yazgan & Cavdar, 2014), operations research (Liu & Wang, 2012) and other applications. Table 1 shows the comparison between ACO and PSO.

Table 1: Comparison Between ACO and PSO

	Ant Colony Optimization (ACO)	Particle Swarm Optimization (PSO)
Definition	Multi-agents to search the cheapest path in a discrete optimization problem.	Multi-agent to find the shortest path in a robust stochastic optimization problem.
Procedure	• Local rule: the best individual iteration pheromone • Global rule: the best pheromone based on collective iteration	• Local/particle best: the individual's best solution achieved by i) own experience, and ii) nearest neighbor experience • Global Best Particle: the best solution in the neighborhood.

Several researchers mentioned the advantages and disadvantage of ACO (Abreu et al, 2011; Selvi & Umarani, 2010) and PSO (Ab Wahab et al., 2015; Bai, 2010; Gong et al., 2009) run an experiment to evaluate performance of swarm intelligence algorithms on benchmark function. The result reveals a Selection PSO performed better after Differential Evolution (Angeline, 1998).

Proposed Traceability Chain Algorithm

The proposed traceability chain algorithm is using ACO due to the nature of military blockchain. Below is the pseudocode for the proposed algorithm:

Procedure of ACO for traceability algorithm

BEGIN
Transaction proposal
Repeat
    Begin Iteration process of local pheromone
If blocks propose a transaction;
    (blocks are using a gas for updating transaction)
        (block is using a pheromone value to leave the trails)

Update of pheromone value
Repeat
Begin Iteration process for global pheromone
    ind_pheromone_value += pheromone value
    (blockchain network will gather all the pheromone values)
    *Trails = len(trails)*pheromone edge and compare with the gas*
    (calculate the cheapest trails)
Until
All blocks have built a complete solution;

Final Solution
    Until
    (transaction delivery to all blocks)
    (verify the policy)
END

The algorithm starts after the creations of blocks (nodes) such as genesis, sealers, and others. When the transaction *i* is proposed by a block, the first iteration process will start. The block will use a gas to update its transaction, and it will use a pheromone value to leave the trails on the blockchain network. The process will repeatedly apply a discrete optimization to build a trail. While building a trail, the process will update its trail using a pheromone parameter. Then the process will update its pheromone value using another iteration process for global value. After all the global is gathered, then the cheapest trail will be calculated. The calculation is based on the pheromone parameter (i.e edge) and the gas. Lastly, the transaction will be delivered to all blocks using the cheapest trail. Other blocks may verify the transaction

according to the military blockchain policy for defense shipment. The traceability will be used at the backend system to support military authorities to trace the movement of product securely. The above pseudocode will be converted into a computer algorithm using the Solidity Programming in Remix IDE. The simulation of the blockchain's transactions will be using Go Ethereum (Geth).

Research Methodology

General development of this traceability chain algorithm is started after a thorough analysis process of previous works, and defining the traceability chain components such as Data attributes, Product Routing, Time-Stamped, Bill of Lading and etc. Then the traceability chain algorithm will be developed. This study is following the method of algorithm development (Levitin, 2000) as shown in Figure 3.

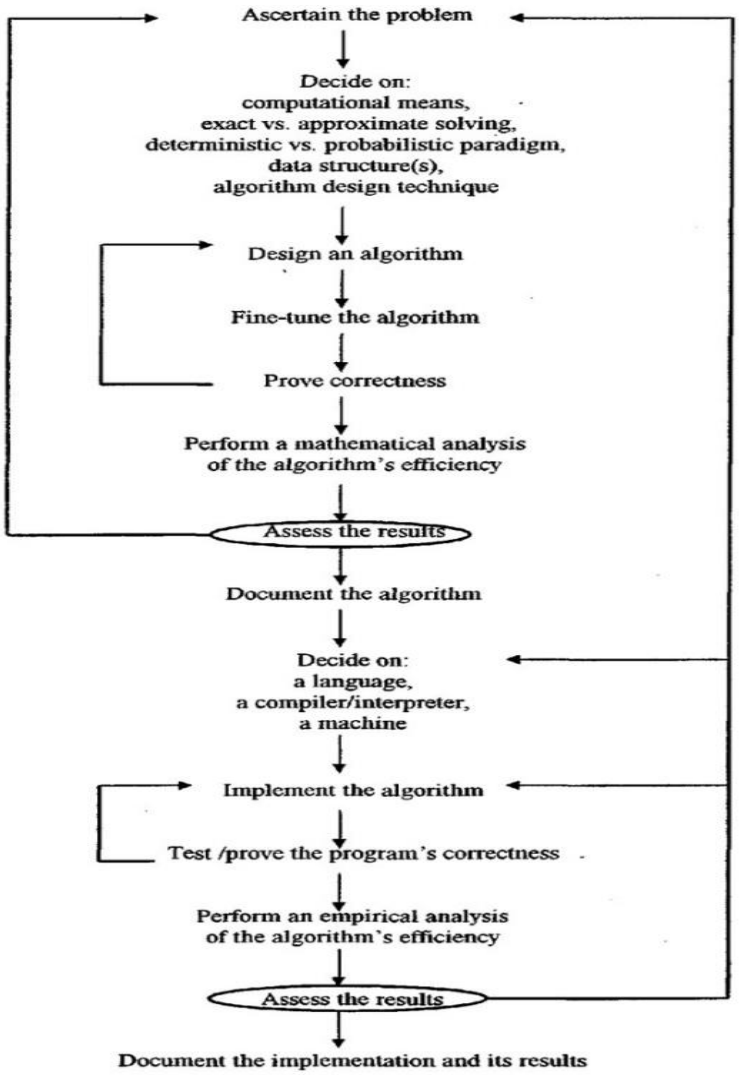

Fig. 3: Details Activities for Algorithm Development (Levitin, 2000)

In this study, after finding the research gap, the next step is to decide on computational means, data structures and algorithm design technique. Next, a new traceability chain algorithm will be designed and made changes (fine-tune) to prove correctness. Later, formulate a new algorithm that defines product traceability from starting node to the latest updated node. Then, the result will be accessed, and the Solidity Programming Language is selected to convert it into coding.

Next step is to implement and test the algorithm in a blockchain simulation, Go Ethereum. The performance will be analyzed using a statistical analysis. The statistical analysis method comprises two

parts. In the first part, this article presents statistical analysis method such as the usage of Analytical Hierarchy Process (AHP) method based on multi- criteria evaluation. In the second part, the proposed statistical analysis method presents further interpretation on the most preferred priority selection after by using AHP method. It incorporates both quantitative and qualitative criteria ranking by comparing and analyzing the powerful indices such as correctness, efficiency, and conciseness between consensus chain alternative and traceability chain alternative in a hierarchical manner. Then, the implementation and its results will be documented.

Conclusions

Blockchain technology and cryptocurrency have already had a significant impact on blockchain communities, government and private organizations in Malaysia. In recent years, military supply chain network securely manages, traces and verifies transactions along the network at near real time. However, these activities are using information, and knowledge sharing among involved parties that are prone to cybercriminal. In this study, Swarm Intelligence Blockchain Model using traceability chain algorithm has been introduced to assist the traceability of defense shipment transactions. By having this model, a new traceability chain algorithm can be implemented to reduce the issues and challenges in tracing product, service and information. Besides, this new model is expected to trace every product movement using proper blockchain orders and secured blockchain network via proposed algorithm. Furthermore, it is also believed that this study will provide positive results for tracing defense shipment. Future research is to apply military blockchain in different areas, such as inventory stock, battlefield communication, and threat intelligence.

Acknowledgement
The authors would like to acknowledge Centre of Research Management and Innovation, NDUM for their dedication, critical and moral support in pursuing this research.

References

Abreu, N., Ajmal, M., Kokkinogenis, Z., & Bozorg, B. (2011). *Ant colony optimization*. Technical Report, University of Porto, Portugal.

Agrawal, T. K. (2019). Contribution to development of a secured traceability system for textile and clothing supply chain (Doctoral dissertation, Högskolan i Borås).

Ahmed, H., & Glasgow, J. (2012). Swarm intelligence: concepts, models and applications. School Of Computing, Queens University Technical Report.

Angeline, P. J. (1998, May). Using selection to improve particle swarm optimization. In 1998 IEEE International Conference on Evolutionary Computation Proceedings. IEEE World Congress on Computational Intelligence (Cat. No. 98TH8360) (pp. 84-89). IEEE.

Asharaf, S., & Adarsh, S. (Eds.). (2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities: Emerging Research and Opportunities*. IGI Global.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Bai, Q. (2010). Analysis of Particle Swarm Optimization Algorithm. *Computer and Information Science*, *3*(1). https://doi.org/10.5539/cis.v3n1p180

Barnas, N. B. (2016). Blockchains in national defense: Trustworthy systems in a trustless world. *Blue Horizons Fellowship, Air University, Maxwell Air Force Base, Alabama.*

Barg, A., Blakley, G. R., & Kabatiansky, G. A. (2003). Digital fingerprinting codes: Problem statements, constructions, identification of traitors. *IEEE Transactions on Information Theory*, *49*(4), 852–865. https://doi.org/10.1109/TIT.2003.809570

Bautista Valhondo, J., & Pereira Gude, J. (2003). Ant algorithms for a line balancing problem. In *actas* (pp. 1-8).

Britchenko, I., Cherniavska, T., & Cherniavskyi, B. (2018). Blockchain technology into the logistics supply

Cao, S., Cao, Y., Wang, X., & Lu, Y. (2017). A review of researches on blockchain. In *Wuhan International Conference on e-Business*. Association For Information Systems. Retrieved from http://aisel.aisnet.org/whiceb2017/57

Castor, A. A. (2017). A (Short) Guide to Blockchain Consensus Protocols - CoinDesk. Retrieved May 15, 2020, from https://www.coindesk.com/short-guide-blockchain-consensus-protocols

Chedrawi, C., & Howayeck, P. (2018). The role of Blockchain Technology in Military Strategy formulation, a resourcebased view on capabilities. In *Cognitive Analytics Management Conference 2018 At: American University of Beirut Lebanon*.

Chen, R. Y. (2018). A traceability chain algorithm for artificial neural networks using T–S fuzzy cognitive maps in blockchain. *Future Generation Computer Systems*, *80*, 198-210. https://doi.org/10.1016/j.future.2017.09.077

Chor, B., Fiat, A., Naor, M., & Pinkas, B. (2000). Tracing traitors. *IEEE Transactions on Information Theory*, *46*(3), 893–910. https://doi.org/10.1109/18.841169

Das, G., Pattnaik, P., & Padhy, S. (2014). Artificial Neural Network trained by Particle Swarm Optimization for non-linear channel equalization. *Expert Systems with Applications*, *41*, 3491–3496. https://doi.org/10.1016/j.eswa.2013.10.053

Di Caro, G., & Dorigo, M. (1998). AntNet: Distributed stigmergetic control for communications networks. *Journal of Artificial Intelligence Research*, *9*, 317-365.

Dorigo, M., Birattari, M., & Stützle, T. (2006). Ant Colony Optimization. *IEEE computational intelligence magazine, 1*(4), 28–39. https://doi.org/10.1109/MCI.2006.329691

Dorigo, M., & Stützle, T. (2004). *Ant Colony Optimization*. Cambridge: MIT Press. Retrieved from https://mitpress.mit.edu/books/ant-colony-optimization

Gong, D., Lu, L., & Li, M. (2009, May). Robot path planning in uncertain environments based on particle swarm optimization. In *2009 IEEE Congress on Evolutionary Computation* (pp. 2127-2134). IEEE.

Gravel, M., Price, W. L., & Gagne, C. (2002). Scheduling continuous casting of aluminum using a multiple objective ant colony optimization metaheuristic. *European Journal of Operational Research*, *143*(1), 218-229.

Green, K., & Foster, C. (2005). Give peas a chance: transformations in food consumption and production systems. *Technological forecasting and social change*, *72*(6), 663-679. https://doi.org/10.1016/j.techfore.2004.12.005

ITAMCO. (2018). Naval Aviation Enterprise Exploring Blockchain With Indiana-Based Company ITAMCO. Retrieved May 22, 2020, from https://www.prnewswire.com/news-releases/naval-aviation-enterprise-exploring-blockchain-with-indiana-based-company-itamco-300716633.html

Karaboga, D. (2005). *An idea based on honey bee swarm for numerical optimization* (Vol. 200, pp. 1-10). Technical report-tr06, Erciyes university, engineering faculty, computer engineering department.

Kechagiopoulos, P. N., & Beligiannis, G. N. (2014). Solving the urban transit routing problem using a particle swarm optimization based algorithm. *Applied Soft Computing*, *21*, 654-676.

Kennedy, J., & Eberhart, R. (1995, November). Particle swarm optimization. In *Proceedings of ICNN'95-International Conference on Neural Networks* (Vol. 4, pp. 1942-1948). IEEE

Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In *Concurrency: the Works of Leslie Lamport* (pp. 203-226). https://doi.org/10.1145/357172.357176

Levitin, A. (2000, March). Design and analysis of algorithms reconsidered. In *Proceedings of the thirty-first SIGCSE technical symposium on Computer science education* (pp. 16-20). https://doi.org/10.1145/330908.331802

Lewis, A. (2016). A gentle introduction to immutability of blockchains. *Bits on Blocks*, *29*.

Linkov, I., Fox-Lent, C., Read, L., Allen, C. R., Arnott, J. C., Bellini, E., ... & Hynes, W. (2018). Tiered approach to resilience assessment. *Risk Analysis*, *38*(9), 1772-1780. https://doi.org/10.1111/risa.12991

Liu, Z., & Wang, X. (2012, June). A PSO-based algorithm for load balancing in virtual machines of cloud

computing environment. In *International conference in swarm intelligence* (pp. 142-147). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-30976-2_17

Miraz, M. H., Hasan, M. G., & Sharif, K. I. (2019). Blockchain technology implementation in Malaysian retail market. *Journal of Advanced Research in Dynamical and Control Systems*, *11*(5), 991–994.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from Bitcoin.

Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing.

Rahayu, S. B., Jusoh, N., Kamarudin, N. D., & Azahari, A. M. (2019). 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

Rahayu, S. B., Jusoh, N., Kamarudin, N. D., & Azahari, A. M. (2019). Military Blockchain For Supply Chain Management. *Journal of Education and Social Sciences (JESOC), 13*(1).

Safavi-Naini, R., & Wang, Y. (2003). Sequential traitor tracing. *IEEE Transactions on Information Theory*, *49*(5), 1319-1326. https://doi.org/10.1109/TIT.2003.810629

Schrepel, T. (2018). Is blockchain, the death of antitrust law. *The blockchain anitrust paradox*, *3*.. https://doi.org/10.2139/ssrn.3193576

Scott-Hayward, S., & Garcia-Palacios, E. (2014). Channel time allocation PSO for gigabit multimedia wireless networks. *IEEE Transactions on multimedia*, *16*(3), 828-836. https://doi.org/10.1109/TMM.2014.2298211

Selvi, V., & Umarani, R. (2010). Comparative analysis of ant colony and particle swarm optimization techniques. *International Journal of Computer Applications*, *5*(4), 1-6.

Silverberg, A., Staddon, J., & Walker, J. L. (2003). Applications of list decoding to tracing traitors. *IEEE Transactions on Information Theory*, *49*(5), 1312-1318. https://doi.org/10.1109/TIT.2003.810630

SImkin, H. (2018). *SMA White Paper: What Do Others Think and How Do We Know What They Are Thinking?* A Strategic Multilayer Assessment (SMA) Periodic Publication.

Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C., & Njilla, L. (2017, October). Consensus protocols for blockchain-based data provenance: Challenges and opportunities. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)* (pp. 469-474). IEEE. https://doi.org/10.1109/UEMCON.2017.8249088

Wahab, M. N. A., Nefti-Meziani, S., & Atyabi, A. (2015). A comprehensive review of swarm optimization algorithms. *PloS one*, *10*(5), 1-36.

Wang, D., Tan, D., & Liu, L. (2018). Particle swarm optimization algorithm: an overview. *Soft Computing*, *22*(2), 387-408. https://doi.org/10.1007/s00500-016-2474-6

Wrona, K., & Jarosz, M. (2019, April). Use of blockchains for secure binding of metadata in military applications of IoT. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 213-218). IEEE. https://doi.org/10.1109/WF-IoT.2019.8767315

Yazgan, A., & Cavdar, I. H. (2014). A comparative study between LMS and PSO algorithms on the optical channel estimation for radio over fiber systems. *Optik*, *125*(11), 2582-2586. . https://doi.org/10.1016/j.ijleo.2013.11.015

Zhang, S., & Lee, J. H. (2019). Analysis of the main consensus protocols of blockchain. ICT Express (2019). *Online: https://doi. org/10.1016/j. icte*, *1*.

Zhang, W., Xie, H., Cao, B., & Cheng, A. M. K. (2014). Energy-Aware Real-Time Task Scheduling for Heterogeneous Multiprocessors with Particle Swarm Optimization Algorithm. *Mathematical Problems in Engineering 2014*. https://doi.org/10.1155/2014/287475