

MILITARY SUPPLY CHAIN MANAGEMENT AND BLOCKCHAIN DEVELOPMENT

Syarifah Bahiyah Rahayu^{1,2}, Sharmelen A/L Vasanthan³,
Afiqah M. Azahari^{1,2}, Joe Chai⁴

¹Cyber Security and Digital Revolution Industry Centre,
National Defence University of Malaysia, 57000 Kuala Lumpur, Malaysia

²Fac. of Defence Science & Technology National Defence University of
Malaysia 57000 Kuala Lumpur, Malaysia

³Campus SophiaTech, 450 Route des Chappes, 06410 Biot, France

⁴Joe Chai, ProximaX Malaysia Sdn. Bhd, Lot 3A.09, Level 3A, GLO
Damansara, Jalan Damansara, 60000 Kuala Lumpur, Malaysia

ABSTRACT

Blockchain has become a powerful technology and when it comes to supply chain management, blockchain has a lot to offer which could contribute to its development and make the supply chain more effective. The same benefit could be also gained when blockchain is incorporated in the Military Supply Chain Management (MSCM). The aim of this paper is to develop and integrate blockchain in the MSCM. The developed MSCM is focusing on three (3) main blockchain components, which are transparency, integrity and secure communication. The methodology to develop the MSCM blockchain similar to UnicalCoin. The findings show that incorporating blockchain into the MSCM enables transparency, integrity and secure communication. Thus, blockchain may reduce fraud, improve communication between parties and made end-to-end tracking transparency in MSCM. Future work is to embed a smart contract feature to automate some processes in MSCM.

KEYWORDS

Blockchain, distributed ledger technology, smart contract, supply chain, nodes.

1. INTRODUCTION

Supply chain management (SCM) has been widely used in various industry sectors. SCM is a complex distribution process involving cross functional approaches in managing the product chain from the starting point (i.e., raw material) until the ending point (i.e., consumer) [1]. The ultimate supply chain management components comprise of manufacturers, suppliers, distributors, and consumers as well as other service providers such as finance, logistics, and market research firms.

Security and defence sectors are also adopting SCM. For instance, military supply chain management (MSCM) is focused on manufacturing, distributing and shipping military materials, parts or applications. In order to maximize its effectiveness and efficiency, these processes must be transparent, highly integrity and good communication between SCM components. However, the current conventional SCM methods failed to meet these three key aspects [2].

The first key, transparency, allows all the parties that are involved including the consumer to know the status of the product [3]. This problem is related to traceability and auditing. Without transparency and traceability, any product which encounters problems during manufacturing, distribution and shipping will result in delay or late product delivery [4]. While the second key, integrity, ensures every transaction record that has been made should not be tampered with or counterfeited [5]. Currently, every transaction record between military and other components in the MSCM is saved in a database. The database is vulnerable to data tampering either from an insider or a malicious party. For instance, changing (i.e., modify, delete, and add) transaction records for bad intentions. This caused inconsistency of the transaction records. Another problem arises with counterfeit products. Delivering counterfeit products affect a wide range of industries. For example, distribution of counterfeit COVID-19 vaccines has potential for health risks globally. Thus, MCSM must eliminate distribution of military counterfeit parts to avoid failure in battlefield missions and compromise the security of a nation [6].

The last key is communication where every party should communicate with each other on updating the status of the product and record it [7]. Communication is important to ensure a smooth product distribution at all levels. Another contribution to product shipment delay is miscommunication [8]. These MSCM problems could be overcome by integrating blockchain technology.

Blockchain is a digitized public ledger of all transactions. This public ledger has been conducted and shared within the blockchain community. Blockchain is designed to work in a decentralized manner. Each transaction conducted within the public ledger is confirmed by the community who owns a node in the blockchain [9]. Once a transaction is recorded in the public ledger, the information is immutable which means it cannot be changed. Figure 1 shows the transaction process of Blockchain. Blockchain always records every confirmed transaction that has been made in the community and the record is kept across the nodes.

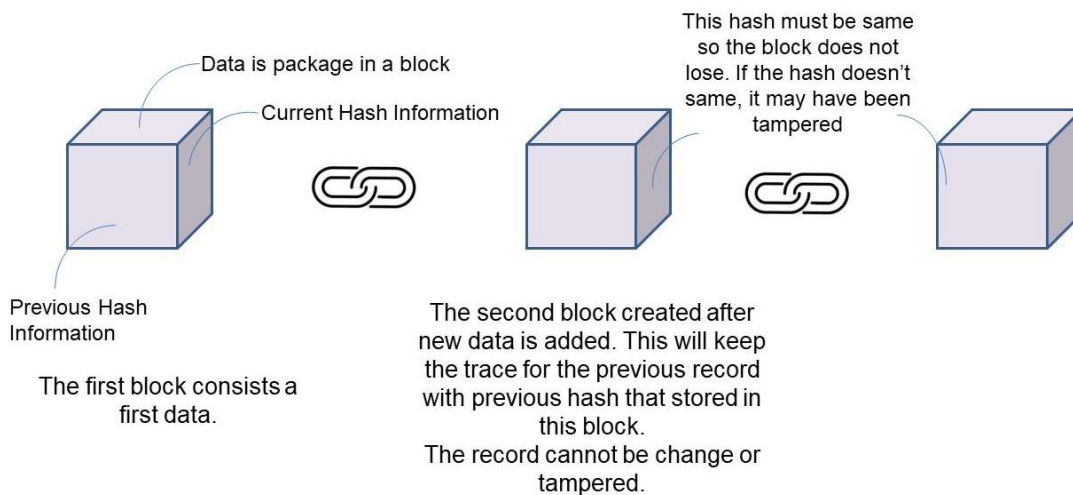


Figure 1. Transaction process in Blockchain

There are two types of blockchain that are private and public blockchain [10]. A blockchain is considered to be public if any individual can access it and use it to conduct transactions as well as when there is a consensus mechanism involved in verifying the transaction made. As an incentive for the community to use their resources to verify a transaction, a token or cryptocurrency will be earned. On the other hand, blockchain is considered to be private when only a certain individual

or organization owns the nodes and verifies the transaction. The permission to perform a transaction is given by an authority of an organization who owns the blockchain. In blockchain there are three main components of cryptography that plays an important role which are (i) the hashing mechanism where the hash of the predecessor block is stored in header of the new block, (ii) Merkle tree where all the transaction hashes are combined to form on hash and kept in the block, and (iii) digital signature is used for non-repudiation [10], [11].

Table 1. Differences between private and public blockchain

Characteristic	Public Blockchain	Private Blockchain
Level of access to the Blockchain	Anyone can be a part of the community and make transactions. Nodes owned by multiple parties can verify the transaction via consensus mechanism applied in a blockchain network.	Only authorised individuals can access the community and make transactions. Nodes only owned by a certain party can verify a transaction and usually consensus mechanism is not needed.
Authority	Decentralized	Centralized
Consensus	Permissionless	Permissioned
Number of transactions per second	High	Low
Immutability	Full	Partial
Transparency	Yes	Yes

In 2019, a group of researchers did an experiment by incorporating blockchain into the supply chain to reduce false information that spread over the networks of a supply chain and also to prevent companies from any moral misconduct such as counterfeiting or changing any data in the database [12]. The findings of this experiment show incorporating blockchain into the supply chain is worth the cost for a supply chain that requires trustworthy data and counterfeit data can be prevented. However, in a real time SCM it is unavoidable. Therefore, it is advisable only authorized agents are allowed to access the blockchain. A recent survey [13] shows that incorporating blockchain in the manufacturing domain and logistic domain can be very useful. The findings of the manufacturing domain reveal the cost is economical and it could fight counterfeiting too. This is due to the blockchain feature in providing history to consumers. Similarly, the results in the logistic domain are showing blockchain integration is useful.

Some of the benefits that can be achieved by applying blockchain includes reducing delivery delay time and avoiding any human errors thus enhancing the efficiency of agreements between manufacture and consumers [13]. Considering the benefits of blockchain technology, thus the current issues of MSCM could be eliminated. Therefore, this paper presents MSCM development using blockchain technology.

2. METHODOLOGY

This study is applying a similar methodology of (UnicalCoin). Instead of using UnicalCoin, this study is using ProximaX blockchain platform, Sirius Chain to integrate with MSCM. There are three main stages in this development as shown in Figure 2.



Figure 2. System Methodology

Sirius Chain is blockchain technology that is developed by ProximaX's company. The Sirius Chain generate a new block that records transaction data for every 15 seconds, by default. Once the Sirius Chain algorithm has been implemented in the nodes some modifications are done as it is operating in a private network, own by Military. Among the modifications is no crypto currency used in the MSCM blockchain environment. Due to MSCM private blockchain environment, there is no incentive mechanism to reward the node that validate the blocks. Another modification is the addition of a message authentication mechanism, external parties cannot access the nodes without permission. Thus, any transaction receipt that comes from the node needs some form of authentication.

Then, the second step is to create a supply chain simulation model that recreates a model company with networks. For the supply chain model, several different computers/ machines are selected and used to test out the supply chain management. Some machines represent the external parties, i.e., product manufacturer, and the machines have been installed with the client application. The client application establishes interaction between externals' machine the with the server. Furthermore, the client application acts as a mediator and sends the information to the nodes that are operated by Sirius Chain. The snippet of pseudocode for the client application as follows:

```

import modules

generate panels with different service for selection
process the service selected by the clients

if client app connected to server:
  show panels related to specific service

if information is given:
  send information to the server
  receive response from the server
  show the information received to client
else:
  show error message from the server

else:
  tell client that server is not running
  
```

The last step is to generate a connector. Generating a connector to connect the blockchain network to the simulated model, i.e UnicalCoin to the connector software that was written in Java [12]. In this study, server is the connector between the blockchain and MSCM. Every information that is sent via client application to the Sirius Chain go through the server, first. The server is the gateway between the nodes and client application. The server checks the validity of the message that it has received. If the message is valid, the message is sent to the Sirius Chain, otherwise the message will be discarded. The pseudocode for the server is as follows:

```

import modules

connect to client database
receive message from client app

check service selected by client

select the service selected by client
check message validity in database

if message = valid
    Send the transaction to Sirius Chain
else :
    Send an error message

```

For security and confidentiality of sensitive military data, MSCM is a private blockchain as suggested by [14]. The following flowchart (Figure 3) shows a detailed overview on how MSCM has incorporated the ProximaX Sirius Chain. In the MSCM environment, all the parties that are involved will be given a client application. Once each party has received the client application they can start to interact with the server. The client app will send this information that is given by the client to the server where the server acts as a gateway and checks the validity of the information that is given by the client, if the information is valid, it will send the information to the nodes and will be recorded in the Sirius Chain. Clients can use this client app to update the status of the assets and for the military staff they have the option to see their entire transaction history with other companies as for parties that are not military affiliated can only see their personal transaction history to prevent any information leakage.

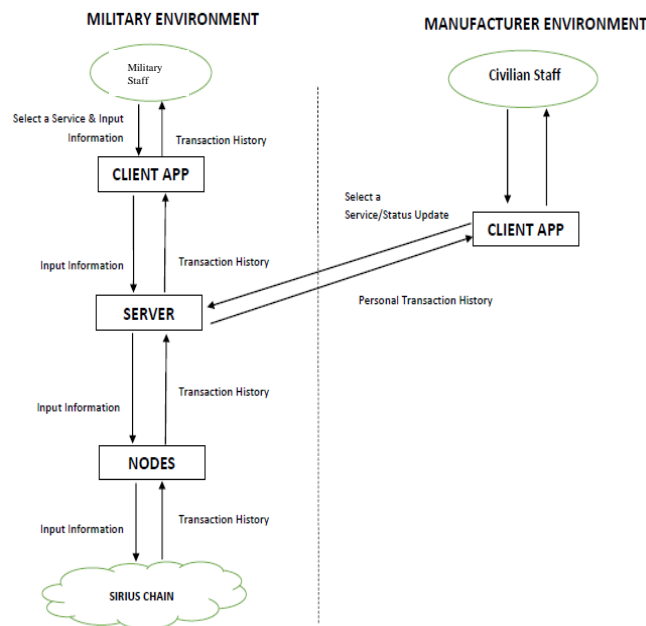


Figure 3. MSCM System Overview

The owner of the MSCM is the military department. They must prepare the nodes to store every transaction on the blockchain. The preparation of the nodes, especially its location is very crucial as setting all the nodes into one specific location can lead to single point failure. Therefore, the nodes are advisable to be installed at different locations in the military compound. Once the nodes have been set up, then MSCM blockchain is embedded into the installed nodes and perform a test run. Then, the military department creates a server that processes all the

information and requests to check its credentials and validity before sending the transaction to the ProximaX Sirius Chain. Once a server has been built, a simple client application should be created. As mentioned previously the client application is the communication medium for all the involved parties to connect to the server.

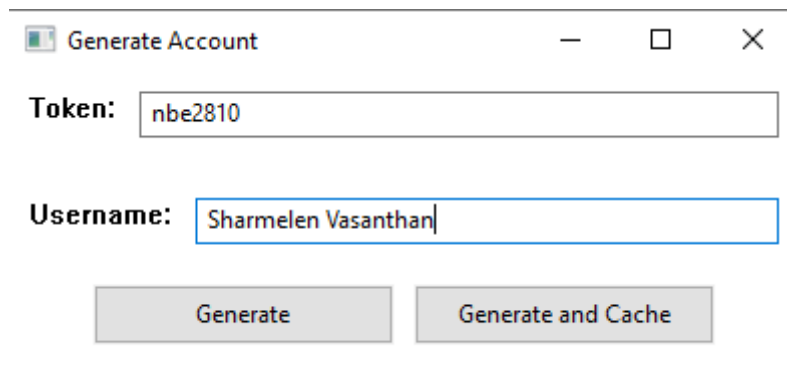
MSCM is using the default time duration to generate blocks. Each block in Sirius Chain is linked by the hash of the predecessor block in its header. When the required criteria are met and the Sirius Chain has been installed in the nodes of the Military department, other parties that are required to be in the chain such as manufacturer can be integrated in the chain as well. All the parties that are involved in the chain can create a transaction and record it in the chain across the nodes. Due to the confidentiality, only military personnel that are involved in the supply chain are allowed to see all the transactions that happen with the manufacturer during the manufacturing, distribution and shipping of the military material, parts or application. Specific manufacturers can only access their own transaction record.

3. RESULTS AND DISCUSSIONS

3.1. Result Analysis

MSCM has been tested to find out its capability in terms of traceability, integrity and secured communication. Several test runs have been done using Sirius Chain and the results have been recorded and explained as follows.

The first test was when a client tries to generate an account for MSCM (Figure 4).



The screenshot shows a window titled "Generate Account" with standard window controls (minimize, maximize, close). It contains two text input fields: "Token:" with the value "nbe2810" and "Username:" with the value "Sharmelen Vasanthan". Below the fields are two buttons: "Generate" and "Generate and Cache".

Figure 4. Generate User Account

First for account generation, there two textboxes that require a token and a username. The token is used like a SWIFT code where only an individual that has received this token can actually create an account to prevent an unwanted party from generating an account and username is used to identify the individual who generated this account. Then, there are two buttons, "Generate" and "Generate and Cache". The "Generate" button is used for only generating the account, While the latter is used to cache the generated information into the machine. Every time a user makes a transaction, they do not have to enter the private key, but this is not a safe practice.

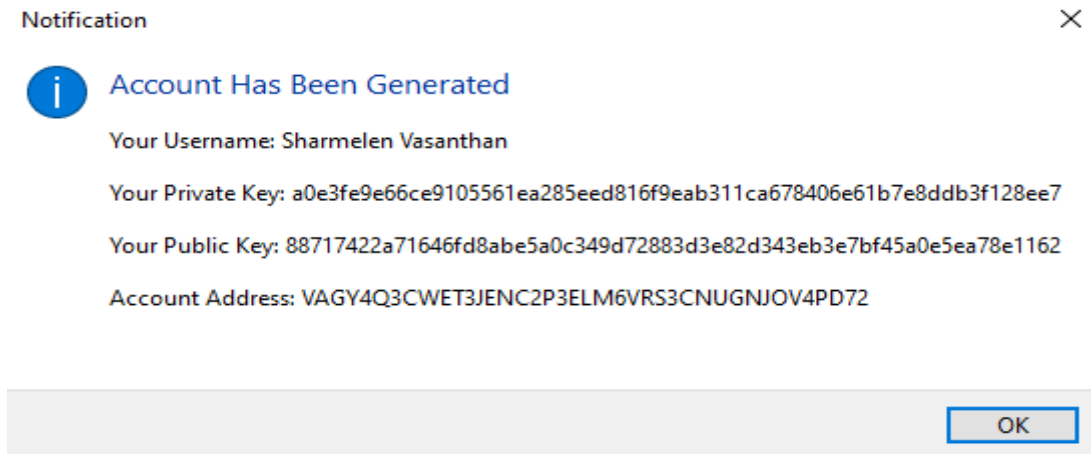


Figure 5. Account Information Generated

The user will receive a notification (Figure 5) saying the account has been generated along with their credentials. This information is crucial, especially the private key. The private key must be entered every time the user makes a transaction.

Next is client application. The user can use the client application to get information about their account (Figure 6).

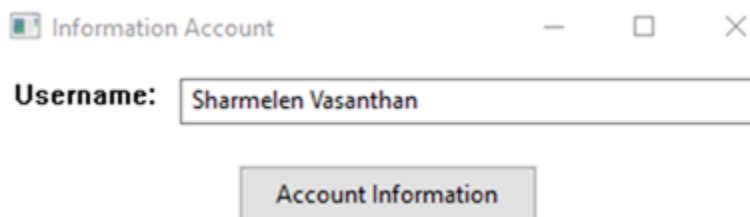


Figure 6. Login to Account Information

By entering the username, user can obtain the information about their account (Figure 7).

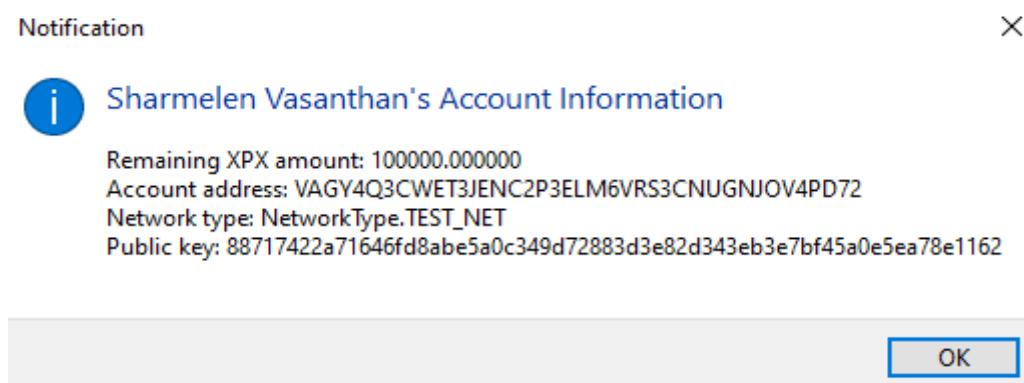
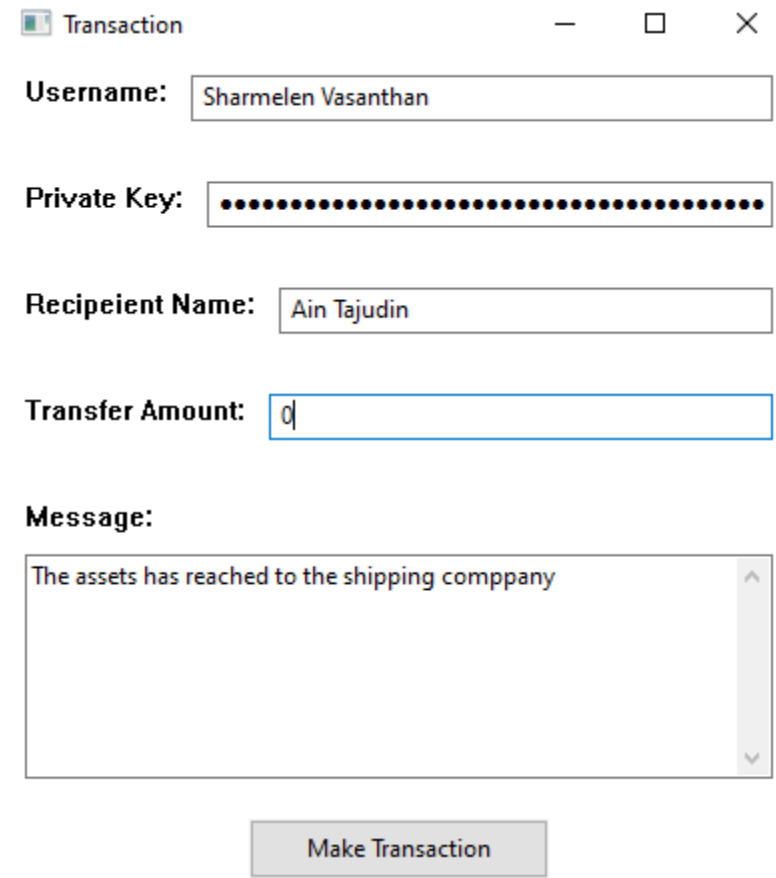


Figure 7. Account Information

The notification shows the information of the account that is associated with this account.

On top of that, users can also send messages to update the status of the assets in the MSCM environment.



The screenshot shows a window titled "Transaction" with a standard Windows title bar (minimize, maximize, close buttons). The form contains the following fields:

- Username:** A text input field containing "Sharmelen Vasanthan".
- Private Key:** A text input field filled with 25 black dots, representing a masked private key.
- Recipient Name:** A text input field containing "Ain Tajudin".
- Transfer Amount:** A text input field containing "0".
- Message:** A text area containing the message "The assets has reached to the shipping comppany".

At the bottom of the form is a grey button labeled "Make Transaction".

Figure 8. Make Transaction

Once the required information has been added the user can press the “Make Transaction” (Figure 8) button to send the status update to the related party and the message will be recorded in the Sirius Chain. As for the amount the user can set it to 0 transaction fee since the main objective of this private blockchain is to ensure the integrity and transparency of the data among the MSCM community.

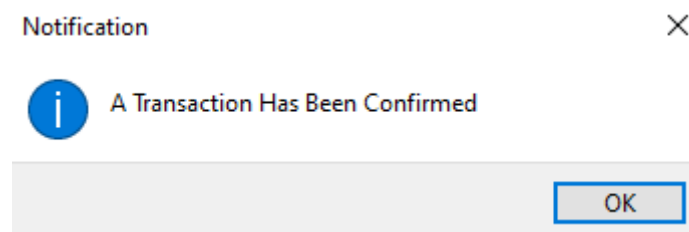


Figure 9. Transaction Notification

Once the transaction has been confirmed the server will send a notification saying that transfer was successful (Figure 9).

Finally, the party who is involved in the MSCM can also get their personal transaction via client application.

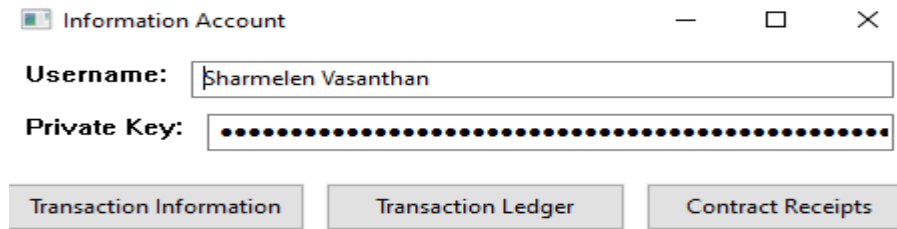


Figure 10. Information Account

Figure 10 shows Information Account has three buttons. The first button, “Transaction Information” button is to get a personal transaction that has been done between one-to-one transactions i.e. from sender to receiver. Then, “Transaction Ledger” button is used to get transactions that have been recorded from the beginning to the current validated block which has many to many transactions and is only available to ATM staff. The last button is the “Contract Receipts” for getting the contract that has been generated so far.

Here is the example of a normal transaction receipt (Figure 11).

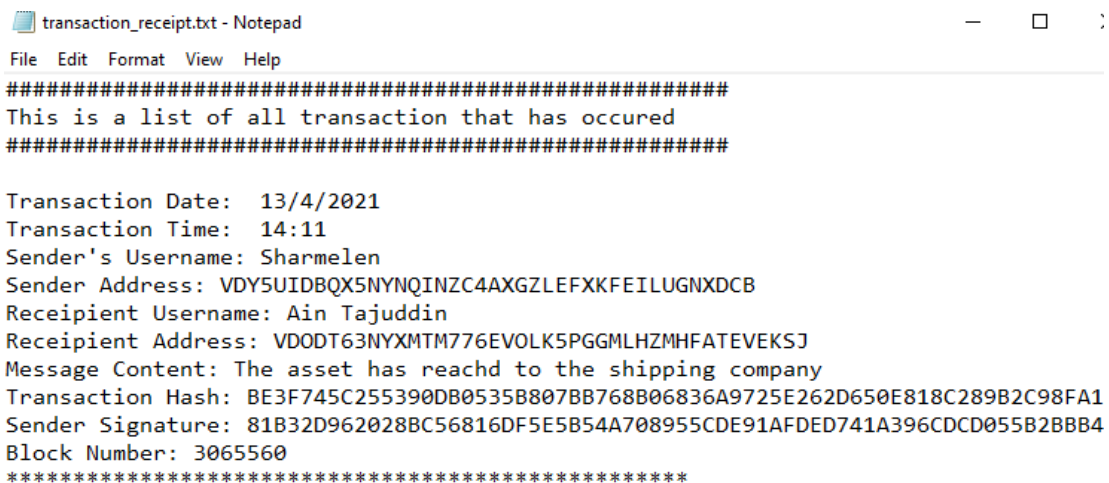
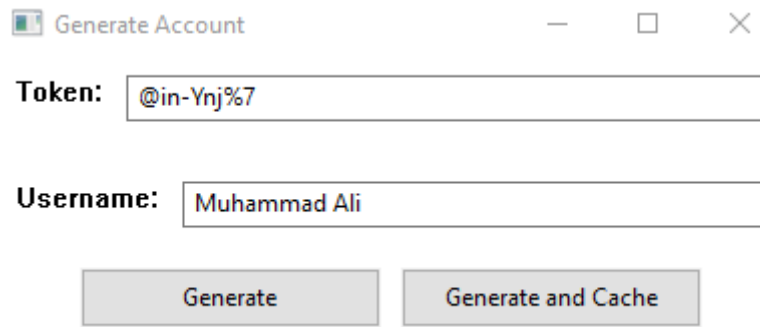


Figure 11. Transaction Receipt

Further system evaluations are using incorrect information into the client application. The objective to reveal that the server can check the data validity with the database and discard the information.

During the account generating process in the client application, invalid token have been inserted in the token textbox (Figure 12).



Generate Account

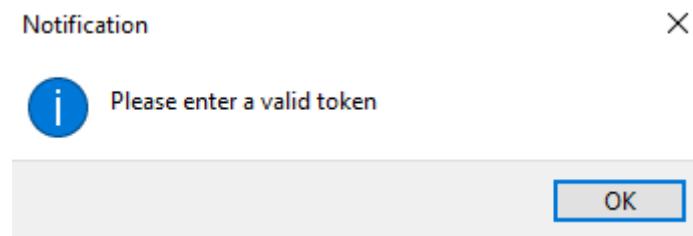
Token: @in-Ynj%7

Username: Muhammad Ali

Generate Generate and Cache

Figure 12. Inserting Invalid Token

Figure 13 shows the notification that token inserted was invalid. Because the server checks the validity of the token, and the token does not correspond as the one in the database.



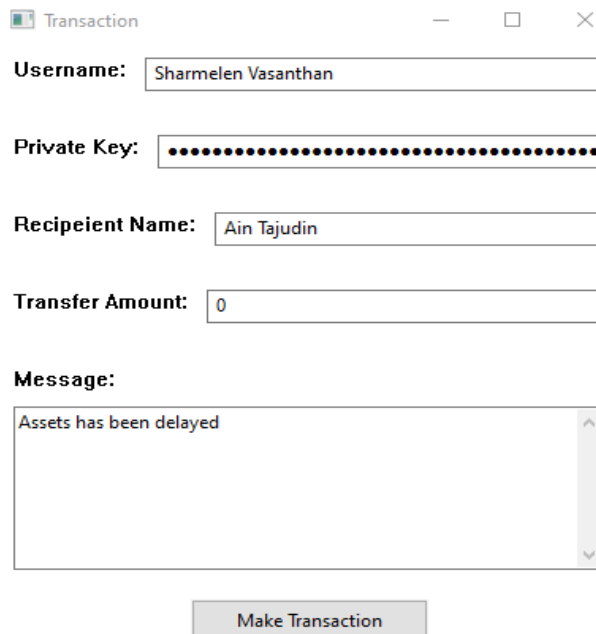
Notification

Please enter a valid token

OK

Figure 13. Invalid Token Notification

Next, insertion of the wrong private key in the panel during the transaction and the response was as follows (Figure 14).



Transaction

Username: Sharmelen Vasanthan

Private Key:

Recipeient Name: Ain Tajudin

Transfer Amount: 0

Message: Assets has been delayed

Make Transaction

Figure 14. Entering a Wrong Private Key

The server sends a notification saying that the private key that was entered is invalid (Figure 15).

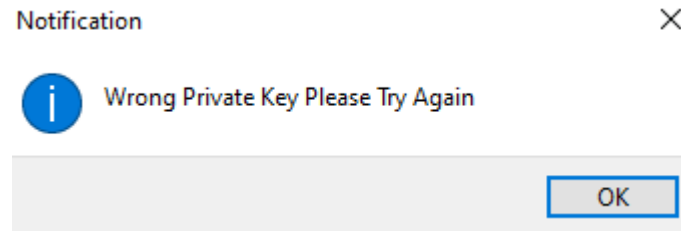


Figure 15. Wrong Private Key Notification

In conclusion, this experiment (testing and evaluation) shows the server is quite resilient in filtering invalid data and runs smoothly even if the data that was entered is invalid.

4. FINDINGS

This study reveals the integration of MSCM with blockchain technology is beneficial to all SCM components. Every single transaction recorded in the blocks is immutable. Furthermore, this transaction is transparent and anyone who got access to the blockchain is able to see it. The transaction record that happens between the parties who are involved in the MSCM can be accessed by those in the chain and can stay updated about the ongoing business transaction. Communication or error in data transfer is avoided as the party involved in the supply chain can send messages in the chain instead of sending the message personally between any party. Moreover, digital signatures are offered in the blockchain technology making sure that the message to be sent is non-repudiation. Incorporating blockchain in MSCM also allows parties involved in the supply chain to trace back the source of the problem if the asset that is bought had issues in receiving or delivery. Adaptation of blockchain in supply chain management system assuredly can improve supply chain traceability [18], [19]. Lastly, integrity issues can be resolved since every single transaction that has occurred is recorded across the nodes and it is impossible to tamper them.

5. FUTURE RESEARCH

MSCM will be expanded using Smart contract in the future. Smart contract is a self-executing term of agreement between buyer and seller. Without any intermediary's involvement and time loss, the agreement is directly written into a line of code and stored on a blockchain. The codes of agreements exist across a distributed, decentralized blockchain. There are many benefits that can be obtained from smart contracts. As no single entity owns the record, all relevant parties can access the information and investigate how the transaction was made or how value is processed. The distributed and decentralized structure ends the requirement of middleman therefore making transactions less vulnerable to corruption. Smart contract allows two parties which are in this case the military and suppliers to record their business agreement on a blockchain. Both parties will hold the encryption key and anytime can give authorized users to review the contract or agreement. [15], [16]. Contract written in blockchain is immutable which means they could not be tampered with thus the integrity of the contract can be maintained. Another benefit that is offered by smart contracts is transparency, where the parties that are involved in the MSCM environment can see the transactions that have been done so far and get access to the contract [17]. Smart contract can be fit in along with the proposed incorporated MSCM environment which is an ongoing future research.

6. CONCLUSION

As a conclusion, implementing blockchain in the MSCM environment is promoting transparency within the parties that are involved in the chain. Moreover, the communication between parties can be also more efficient since the communications that happened are considered as a transaction and recorded in the ledgers of the blockchain. Lastly, integrity in the MSCM can be tremendously improved by applying blockchain since data that is recorded is immutable. Future work is to expand this blockchain technology to other domains in the military environment such as logistics and finance.

7. AUTHOR CONTRIBUTIONS

Syarifah Bahiyah Rahayu led the research; Sharmelen has developed the blockchain system software using SDK provided by ProximaX; Joe is the expert of Sirius Chain and assists in blockchain platform; Sharmelen, Syarifah Bahiyah Rahayu and Afiqah M. Azahari wrote the paper, all the authors had agreed and approved the final version of the paper.

ACKNOWLEDGEMENTS

The authors would like to thank National Defense University of Malaysia for financially supporting the conference paper under grant UPNM/2020/GPJP/ICT/8.

REFERENCES

- [1] M. Felea and I. Albăstroi, "Defining the concept of supply chain management and its relevance to romanian academics and practitioners," *Amfiteatru Econ. J.*, vol. 15, no. 33, pp. 74–88, 2013.
- [2] S. B. Rahayu, M. H. M. Halip, A. M. Azahari, N. D. Kamarudin, and H. Mohamed, "New Traceability Approach Using Swarm Intelligence for Military Blockchain," *Zulfaqr J. Def. Sci. Eng. Technol.*, vol. 4, no. 1, pp. 51–59, 2021.
- [3] Ramanathan Venkataraman, "Supply chain transparency: creating stakeholder value," *KPMG Nederland*. 2020, Accessed: Jun. 01, 2021. [Online]. Available: <https://home.kpmg/nl/nl/home/insights/2020/01/supply-chain-transparency-creating-stakeholder-value.html>.
- [4] T. Sermpinis and C. Sermpinis, "Traceability decentralization in supply chain management using blockchain technologies," *arXiv Prepr. arXiv1810.09203*, 2018.
- [5] J. Picard and C. Alvarenga, "Illicit Trade, Supply Chain Integrity, and Technology," 2012, pp. 57–63.
- [6] S. B. Rahayu, N. D. Kamarudin, A. M. Azahari, and N. Jusoh, "Integrating Military Blockchain in A Supply Chain Management," 2019.
- [7] G. Fulantelli, M. Allegra, and A. Z. P. Vitrano, "The Lack of Communication and the Need of IT for Supply-Chain Management Strategies in SMEs," in *Informing Science & IT Education Conference*, 2002, pp. 19–21.
- [8] C.-D. AF, Y. RI, K. Case, S. Rahimifard, and B. NM, "Building supply chain communication systems: a review of methods and techniques," *Data Sci. J.*, vol. 5, pp. 29–51, 2006.
- [9] M. Crosby, "Integration von Big Data-Komponenten in die Business Intelligence," *Appl. Innov. Rev.*, vol. 27, no. 4–5, pp. 222–228, 2015, doi: 10.15358/0935-0381-2015-4-5-222.
- [10] D. Guegan, "Public Blockchain versus Private blockchain," Université Panthéon-Sorbonne (Paris 1), Centre d'Economie de la Sorbonne, Apr. 2017. [Online]. Available: <https://econpapers.repec.org/RePEc:mse:cesdoc:17020>.
- [11] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," *EURASIP J. Wirel. Commun. Netw.*, vol. 2020, no. 1, pp. 1–15, 2020.
- [12] F. Longo, L. Nicoletti, A. Padovano, G. D'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Comput. Ind. Eng.*, vol. 136, pp. 57–69, 2019.

- [13] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.
- [14] S. B. Rahayu, N. D. Kamarudin, and A. M. Azahari, "Military blockchain for supply chain management," *J. Educ. Soc. Sci.*, vol. 13, no. 1, pp. 353–361, 2019.
- [15] I. Karamitsos, M. Papadaki, and N. B. Al Barghuthi, "Design of the Blockchain Smart Contract: A Use Case for Real Estate," *J. Inf. Secur.*, vol. 09, no. 03, pp. 177–190, 2018, doi: 10.4236/jis.2018.93013.
- [16] J. Maupin *et al.*, "Blockchain: A World - Without Middlemen? Promise and Practice of Distributed Governance Contributors:," *Giz*, p. 92, 2019, [Online]. Available: <https://www.giz.de/en/downloads/giz2019-EN-Blockchain-A-World-Without-Middlemen.pdf>.
- [17] Smart Contracts Alliance, "Smart Contracts: 12 Use Cases for Business & Beyond," *SSRN Electron. J.*, vol. 41, no. 2, pp. 125–140, 2018, [Online]. Available: http://www.ibtimes.co.uk/how-are-banks-actually-going-use-blockchains-smart-contracts-1539789%0Ahttp://blockchainapac.fintecnet.com/uploads/2/4/3/8/24384857/smart_contracts.pdf%0Ahttps://medium.com/@jeroen.hesp/chainlink-how-smart-contracts-can-be-used-in.
- [18] J. M. Song, J. Sung, and T. Park, "Applications of blockchain to improve supply chain traceability," *Procedia Comput. Sci.*, vol. 162, pp. 119–122, 2019.
- [19] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *2016 13th international conference on service systems and service management (ICSSSM)*, 2016, pp. 1–6.

AUTHORS

Syarifah Bahiyah Rahayu, Ph.D. is a fellow researcher, Cyber Security Centre, and a senior lecturer, Defense Science Department, Faculty of Science and Technology in National Defence University of Malaysia. She has vast experience in IT industry and academia. Her research interests (not limited to) blockchain, artificial intelligence, cyber security and big data.



Sharmelen Vasanthan was born in Teluk Intan, Perak. He received his Bachelor of Science in Information System Security from National Defence University of Malaysia in 2019. His main research interests are data mining and blockchain based applications in various domains. He also has a military training under the Reserve Officer Training Unit at NDUM and was commissioned as a Lieutenant in 2019. Currently, he is pursuing his Masters of Digital Security in Eurecom, France.



Afiqah M. Azahari is a fellow researcher of Cyber Security Centre and a lecturer in the Faculty of Science and Technology in National Defence University of Malaysia (NDUM). She holds a Master's Degree in Security and Management from University of Warwick, UK. Her area of research includes Cyber Security Development, Digital Forensic and Internet of Things (IoT).



Joe Chai is a Solutions Architect with more than 10 years of system integration experience. His research interests include blockchain, fintech, IoT, cloud, security, software applications and infrastructure. His work with multinational companies includes ProximaX, NEC, Dataprep, MCSB and YTL. Joe holds a Bachelor's Degree of Engineering (Honours) in Electrical & Electronic Engineering from Universiti Teknikal Malaysia.

