Encrypting of Digital Banking Transaction Records: An Blockchain Cryptography Security Approach

Nabilah Aziz
Departement Information Technology
Gunadarma University

Rodiah Rodiah
Departement Information Technology
Gunadarma University

Heru Susanto
Research Center for Informatics
Indonesia Institute of Sciences and
School of Business, University of Technology Brunei

ABSTRACT
Increased use of digital banking poses a risk to the security of its transactions. As result the system more vulnerable risks faced by digital banking stemmed of cyber-attacks. This study reveals blockchain technology algorithms that encrypted through RSA cryptography and SHA-256 hashes, to enhance digital banking security and reduce the risk of cyberattacks over the banking transaction. The level of blockchain data accuracy and completeness tested through the mathematics permutation method to find out which data-combination that may lead to vulnerable. However, this study is very promosing. The most significant parameter in influencing the validity of the transaction is Value with an accuracy percentage value of 88%, and then followed by Sender Address with an accuracy percentage value of 70% and the last is the Recipient Address with a percentage value. an accuracy of 62%. In other hand, the study reveals that the use of key pairs improves system reliability by implementing of SHA-256 hash on the blockchain.

General Terms
Security, Algorithm, Banking, Blockchain, Cryptography, Encryption

Keywords
Blockchain, RSA Cryptography, SHA-256, Data Integrity, Security

1. INTRODUCTION
The rise of digital banking technology increases the risk of banking transaction security in the form of cyberattacks. One of the cyber attacks that occur in digital banking is data tampering. Data tampering is one of the acts of cybercrime in which the perpetrator modifies valuable data or documents covertly to obtain purposes. In digital banking, this action causes financial losses and reduces customer trust in the bank[1]. A way to prevent this threat is by fulfilling three cybersecurity principles, confidentiality, integrity, and availability. Blockchain is a technology that fulfills these three principles.

Blockchain is a decentralized distributed system used for online transactions where transactions occurred without a third party acting as an authority or an intermediary in a transaction. Every transaction that occurs within the blockchain will go through the stages of verification and validation by all participants involved in the Blockchain. There is a consensus mechanism to increase transparency between transaction participants on the Blockchain. This consensus mechanism is necessary because there is no central authority on the Blockchain. Each participant has data from transactions on the Blockchain where, if there is an attempt by one party to tamper the data, all participants on the network will be aware of this. Every piece of data on the blockchain has a value to identify the data, which is called a hash value. The hash value on the blockchain serves to detect changes in data because if it is modified even if it's only 1 bit, the hash value will change according to that data. Each block stores the hash value of the previous block, so changing one block affects other blocks. This is what makes the blockchain immutable, which means if a data/transaction has been stored in the blockchain, it cannot be changed anymore.

This research analyzes Blockchain technology on digital banking transaction data using the RSA key generation algorithm and 256-bit SHA cryptographic hashes. The data used in this research is banking transaction data totaling 60 transaction records, where one plaintext line of transactions does not have a maximum character length. The level of accuracy of the data on the blockchain will be tested through the permutation method. This research was conducted to prevent damage to digital banking transaction data so that data integrity is always maintained.

2. LITERATURE REVIEW
Jasvinder Kaur research [2] states that the use of blockchain schemes in cloud services can improve data integrity. He created a system for blockchain-based data integrity management that every transaction in the system will be encrypted using the MD5 method integrated with inverse multiplication so that the integrity of every file stored in the cloud is guaranteed. The existence of these features increases system reliability and reduces security threats as much as 66.7%.

A Study conducted by Zyskind, G., Nathan, O., & Pentland, AS [3] in 2015 using a blockchain with Distributed Hashtable and asymmetric cryptography, which is defined by three tuples, namely Generator, decryption, and encryption using the ECDSA and SHA-256 algorithms. This system ensures that the user has full control over the data, and the decentralized nature of the blockchain, combined with digitally signed transactions, guarantee the security of user data.

Research conducted by Shangping wang [4] using blockchain in the medical field to increase control by data owners and guarantee data privacy and integrity. Each medical record is encrypted and generates a hash value, then stored on the blockchain. Each hash value has an index stored in the smart contract. This scheme, increasing tamper-resistance and the control and privacy of medical record owners.

Lukman et al [5] in 2019 implemented blockchain technology to prevent data tampering in one of the petroleum industry in

Nigeria. This study uses a public permissioned blockchain with the SHA-1 cryptographic hash algorithm to protect and monitor the distribution data of Petroleum products. This crypto-blockchain implementation increases resistance to tampering with transaction data within the petroleum industry

Research conducted by Hsin-Te Wu and Chun-Wei Tsai [6] applies blockchain to an intelligent agricultural system. Data containing factors affecting agricultural cultivation stores on the blockchain, and each entity that will access the data must pass the authentication stage using the appropriate session key. The authentication process on the blockchain in this system uses asymmetric cryptographic keys to verify the data source. This system is proven to ensure data integrity, the confidentiality of information, and prevent cyber attacks.

Based on research conducted by Diego Romano and Giovanni Schmid in 2017 [7], Blockchain is currently used in Financial Institutions and proved to help organizations save resource use by reducing inefficiencies caused by the presence of third parties, reducing network security risks, and several other issues.

3. RESEARCH METHODS

This research begins by collecting banking transaction data, creating nodes, generating keys pairs with the RSA cryptographic algorithm, storing digital banking transactions into the system, generating blocks wherein the process the data will go through a hash process, and then the block validity will be tested through the Proof of Work algorithm before broadcasted to the blockchain network. The final step is to test the accuracy of digital banking transaction data on the blockchain using the permutation test method by grouping transaction data into five parameters, Transaction ID, Sender Address, Recipient Address, Value, Timestamp.

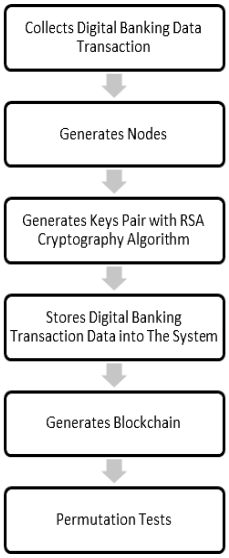

Fig 1: Research Metodology

3.1 Data Collection

This study uses Digital Banking Transaction Data from an anonymous Private Bank containing 60 records of transactions with the following fields:

- Trans id: The identity of the transaction.
- Account id: The account identity of the customer.
- Trans amount: The amount of money to be sent to the receiving customer.
- Balance after trans: The remaining balance after a transaction.
- Trans bank partner: the recipient bank of the transaction.
- Trans account partner: account of the recipient of the transaction. Trans type: type of transaction.
- Trans operation: procedures performed by the bank for a successful transaction.

Table 1. Sample of Digital Bank Transaction Data

Trans Id	Account id	Trans amount	Balance after Trans	Trans bank partner	Trans account Partner	Trans Type	Trans Operation
3625459	2872	44.6	29556.1	NaN	NaN	Credit	Credit_in_cash
843726	2872	113.5	48990.3	NaN	NaN	Credit	Credit_in_Cash
410010	2872	4900.0	12393.6	NaN	NaN	Credit	Credit_in_Cash

3.2 Generate Nodes

Data exchange on the blockchain is carrying out through a peer-to-peer network where the network consists of nodes. Nodes are representations of participants on the blockchain network. Nodes function to validate block transactions, store validated blocks and, broadcast them on the blockchain network so that other nodes can update and synchronize data. The node topology on the blockchain in this study is shown in Figure 2.

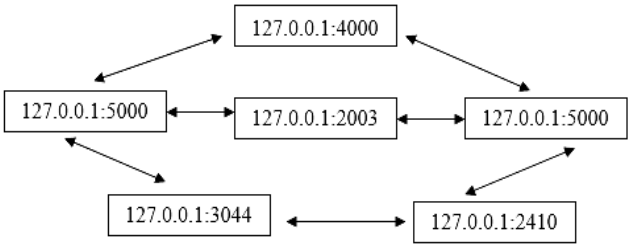

Fig 2: Node Topology

3.3 Generate Keys Pair

Each transaction in this study is protected by an asymmetric cryptographic key consisting of a private key and a public key, and the two keys are mathematically linked. These keys are formed using the RSA Cryptography algorithm with a key length of 1024 bits in hexadecimal form. Public Key is used to encrypting transaction data and generate transaction signatures that are used in the transaction validation process and Private Key is used to identifying entities regarding the ownership of transaction data and the accuracy of the transaction data[8].

At this stage, a Transaction ID is also generated as the identity of the transaction. These keys are useful for verifying and maintaining the integrity of transactions and increasing the confidence of transaction participants in a blockchain. Users are required to have these keys before making digital banking transactions, the keys generate process can be seen in figure 3.

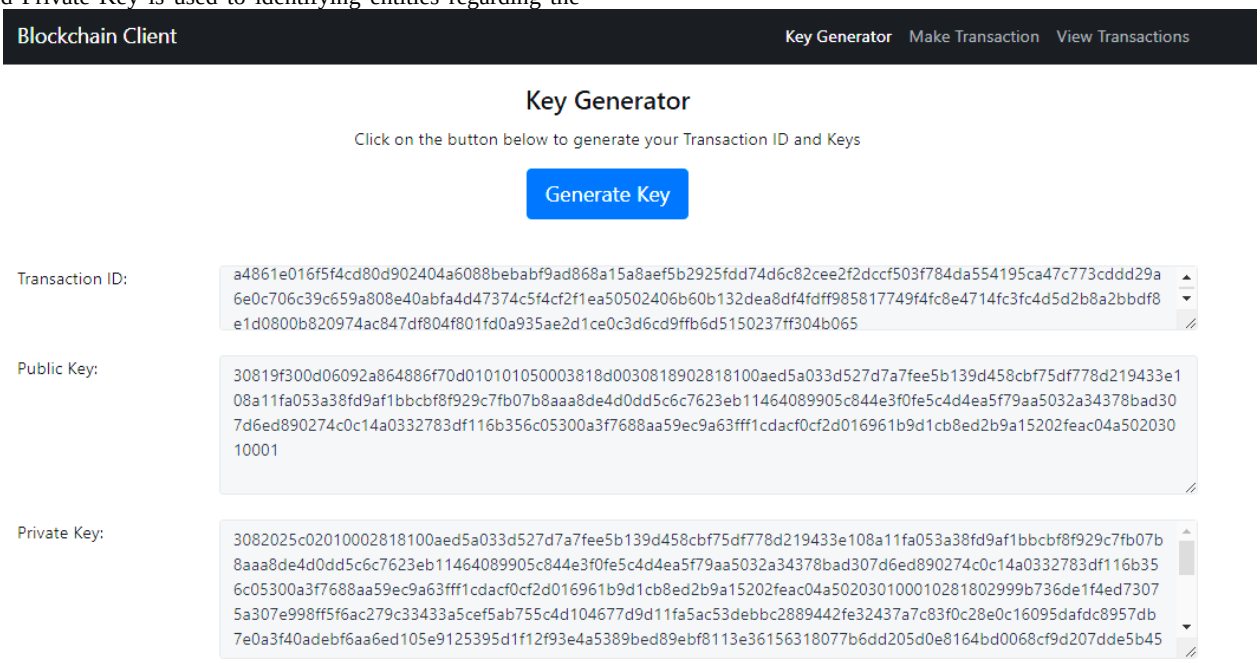

Fig 3: Generate Key Process

3.4 Storing Transaction Data

In this study, digital banking transactions are carried out on a web-based application by filling out transaction information consisting of the Transaction ID, the Sender's address, the Sender's Private key, the Recipient's Address, and the Transaction Amount. The Transaction ID is a random character consisting of letters and numbers generated automatically by the system as the transaction's identity. The Sender's Address is the public key generated at the keys generated stage. The private key of the sender is used to encrypt transactions so that the confidentiality of the transaction is protected. The Recipient's address is filled with the Recipient's Public Key. The Transaction Amount is filled with the amount of money sent to the recipient. The transaction data is first validated before it is sent to the recipient of the transaction and will be stored temporarily in the transaction table before the data is stored in the blockchain. Validation process is shown in figure 4.

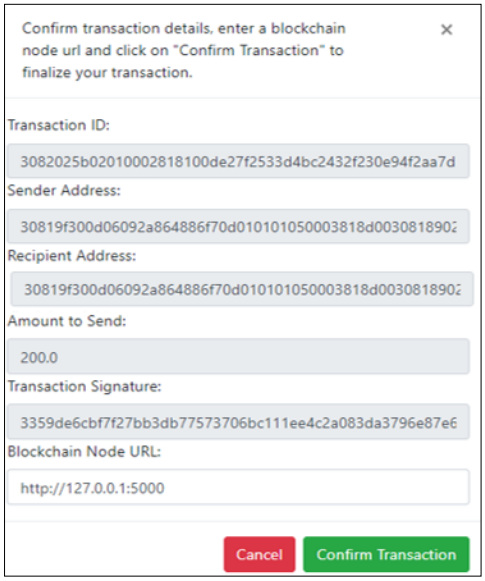

Fig 4: Validation Process

3.5 Generates Blockchain

Banking transactions carried out in the previous stage will be permanently stored on the blockchain. The blockchain will store transactions grouped by the time they occurred. Transactions carried out at the same time by several nodes (participants), will be collected into one block. A block is then linked with other blocks and arranged linearly based on the order of time. Each block stores the hash value of the previous

block, so changing one block affects other blocks. This is what makes the blockchain immutable, namely if a data transaction has been recorded on the blockchain, the data cannot be changed anymore. At this stage, there is also a hashing process to maintain consistency and accuracy of transaction data. Transactions that go through the hashing process will produce a unique output that functions as an identity marker of the transaction data (digest). In this research, the hash algorithm used is SHA-256, so the digest size produced in the hashing process is 256 bits. Sample of Digest Value from digital banking data transaction, is show in table 2.

Table 2. Sample of Digest Value from Digital Banking Data Transactiom

No	Trans id	Account id	Trans amount	Digest Value
1	843716	2872	200.0	cbae66631609dbd30ccd823dff4dc6a92229a2556bdb7f3e62148e726504fcdb
2	843725	2872	12149.0	a934d32bf6a3189d7b619ada5469568ce69edb7ad3cd923e0dbbbf4e693712e7

Digest value generated in the hashing process will be stored on the blockchain and inserted in the header block, each block on the blockchain stores the hash value that the previous block has so that the data in the modified block can be detected immediately. Transaction data stored on the blockchain can be seen in figure 5.

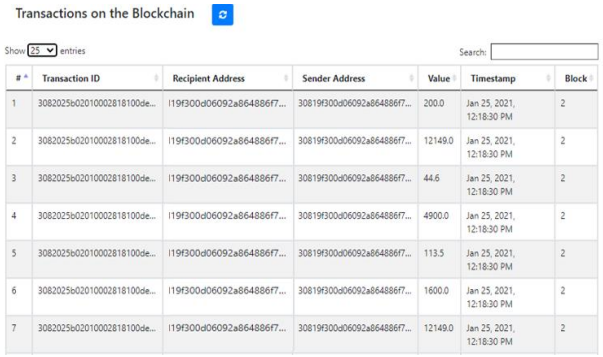

Fig 5: Transaction Data stored on The Blockchain

3.6 Permutation Tests

The permutation test in this study was conducted to test the statistical significance by rearranging it based on several parameters in the data studied. The input test parameters were sourced from the School of Business, Brunei. The test data is transaction simulation data consisting of 8 parameters, namely date, day, month, hour, transaction, debit, credit and, balance. The parameters are then normalized, to eliminate and reduce data redundancies. The normalization process produces 5 parameters consisting of Transaction Id, Recipient Address, Sender Address, Value, Timestamp. The permutations of these parameters will be tested based on the predetermined numbers. The value generated from the permutation test stage is used as a representation of the accuracy of the data provided by the user, as well as the significance of the data in determining the validity of the transaction. Permutations are carried out by forming 5 groups, in which there are values used for the permutation test for each existing parameter.

Table 3. Permutation Group (Source: School of Business, Brunei)

Permutation Group	Parameters				
	Transaction Id	Recipient Address	Sender Address	Value	Timestamp
A11	90	50	40	30	20
A21	80	40	30	20	50
A31	70	30	20	50	40
A41	60	20	50	40	30
A51	55	50	40	30	20
B11	50	90	40	30	20
B21	40	80	30	20	50
B31	30	70	20	50	40
B41	20	60	50	40	30
B51	50	55	40	30	20
C11	50	40	90	30	20
C21	40	30	80	20	50
C31	30	20	70	50	40
C41	20	50	60	40	30
C51	50	40	55	30	20
D11	20	50	40	90	30
D21	50	40	30	80	20
D31	40	30	20	70	50
D41	30	20	50	60	40
D51	20	50	40	55	30
E11	30	20	50	40	90
E21	20	50	40	30	80
E31	50	40	30	20	70
E41	40	30	20	50	60
E51	30	20	50	40	55

4. RESULTS

Permutation tests are performed by forming 5 groups in which values are used for the permutation test for each parameter, namely group A, group B, group C, group D, group E. The value generated at the permutation test stage is a representation of the percentage accuracy of the data provided by the client, as well as the importance of the data in

determining the validity of the transaction. The permutation test was performed ten times in each group to determine the significance of the existing parameters to find the validity of transactions by selecting the three parameters with the highest accuracy value for each experiment.

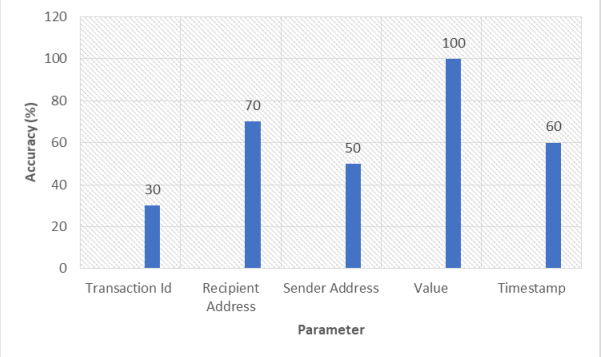

Fig 6: Permutation test results for group A

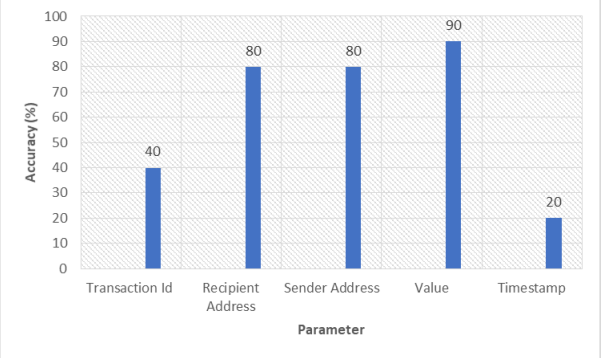

Fig 7: Permutation test results for group B

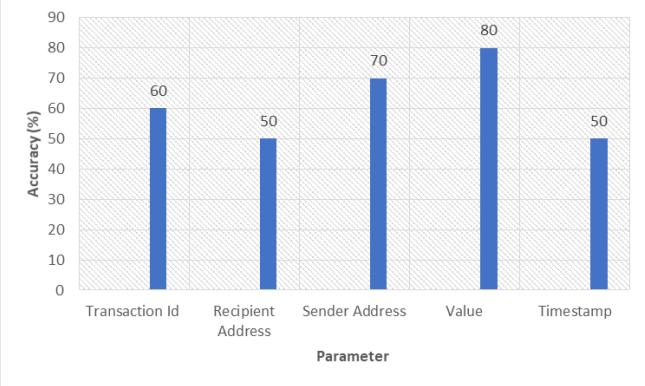

Fig 8: Permutation test results for group C

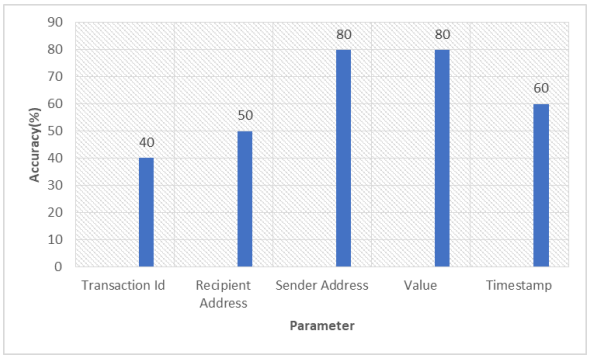

Fig 9: Permutation test results for group D

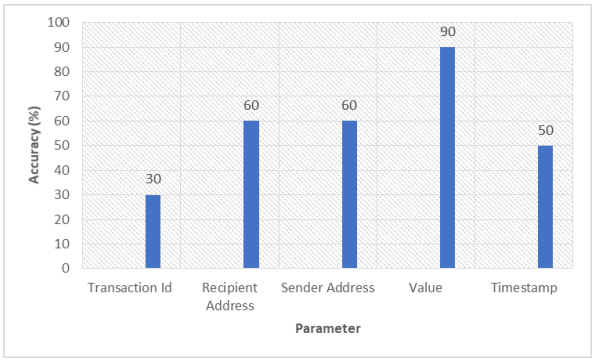

Fig 10: Permutation test results for group E

The permutation test results can be seen in the bar graph as shown in Figure 6 to Figure 10. The results of the five-group permutation test show that the most significant parameters for determining the validity of transactions by clients are the address of the recipient, the address of the sender, and the value with the highest accuracy of the data value, which is as much as 100 % generated by the group A permutation test.

The results from the permutation test of the five groups were then combined to determine the final accuracy of each parameter. The combined value concludes that the most significant parameter affecting the validity of the transaction is the value with an accuracy percentage value of 88 %, followed by the sender address with an accuracy percentage value of 70 % and, the last one is the recipient address with an accuracy percentage value of 62 % as shown in Figure 11.

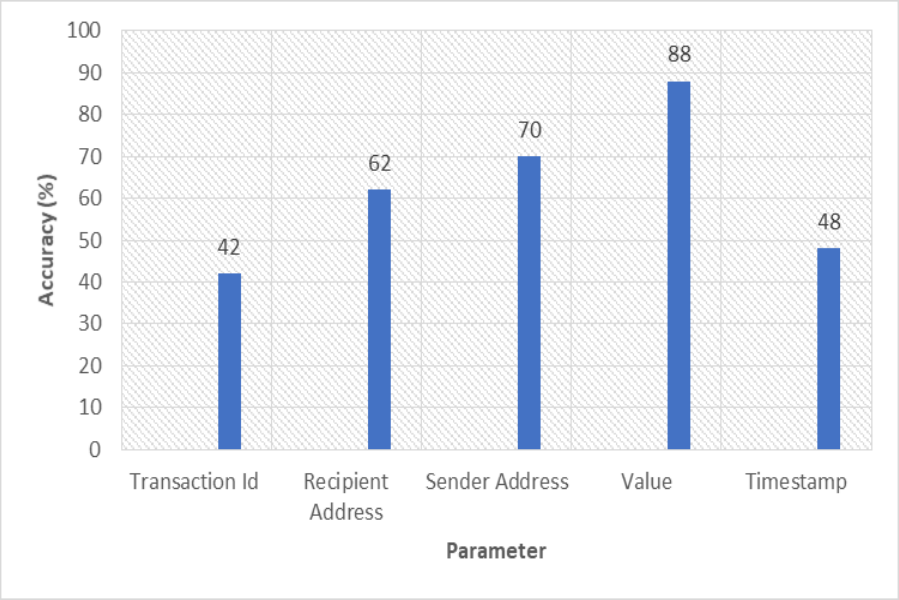

Fig 11: Graph of Parameter Accuracy Test Results

5. CONCLUSION

In this study, based on the results of the permutation test, the most significant parameter in influencing the validity of the transaction is Value with an accuracy percentage value of 88%, and then followed by Sender Address with an accuracy percentage value of 70% and the last is the Recipient Address with a percentage value. an accuracy of 62%.

This research reveals that the use of key pairs generated by the RSA cryptographic algorithm on the blockchain improves system reliability, because only legitimate users, who have the appropriate key pairs, can perform digital banking transactions. The implementation of SHA-256 hash on the blockchain also ensures the integrity of transaction information generated by users.

6. REFERENCES

[1] Abomhara, M. & Køien, G. M., "Cyber security and the internet of things : vulnerabilities , threats , intruders", 2015, Journal of Cyber Security and Mobility, 4(1), pp. 65–88.

[2] Kaur, J., "Improving data integrity using blochain technology", 2018, International Journal of Electronics Engineering, 10(1), 315–320.

[3] Bernardini, M., Pennino, D., Pizzonia, M., Roma, S., & Ingegneria, D., "Blockchains meet distributed hash tables : Decoupling validation from state storage (Extended Abstract)", 2019, DLT Paper, 2334, 1–13.

[4] Wang, S., Zhang, D., Zhang, Y., "Blockchain-based personal health records sharing scheme with data integrity verifiable", IEEE Access, 2015, (4), 1-1.

[5] Lukman, A., Agajo, J., Adedokun, E., & Loveth, K., "Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry", Multidisciplionary Scientific Journal, 2019, 2(3), 300–325.

[6] Wu, H. & Tsai, C., "An intelligent agriculture network security system based on private blockchains", Journal of Communications and Networks, 2019, 21(5), 503–508

[7] J Romano, D. & Schmid, G., "Beyond Bitcoin: A Critical Look at Blockchain-Based Systems",2017,Cryptography, 1-15.

[8] Sobti, R., & Ganesan, G., "Cryptographic hash functions: A review",2012, International Journal of Computer Science Issues, 9, pp. 461 - 479.