AJBAR Vol 1(5), 2022: 52-61, ISSN: 2811-2881

Arid Zone Journal of Basic and Applied Research

Faculty of Science, Borno State University
Maiduguri, Nigeria

Journal homepage: https://www.azjournalbar.com

Research Article

Throughput Analysis and Data Sharing Technique to Assess the Impact of Blockchain Technology using Cryptographic Algorithm

Muhammed Zaharadeen Ahmed[1], Abdulkadir Hamidu Alkali[1], Muhammad Ahmed Aminu[2], Fatima Zakari Abacha[1] and Dauda Yusuf[1]

[1]Department of Computer Engineering, University of Maiduguri, Borno State, Nigeria
[2]Department of Computer Science, Kaduna State University, Kaduna, Kaduna State, Nigeria
*Corresponding author: zaharadeen22@unimaid.edu.ng, doi.org/10.55639/607vpjd

ARTICLE INFO:

Keyword:
Blockchain,
Block rate,
Cryptographic,
Ethereum

ABSTRACT

Blockchain is a data structure made up of chronologically ordered data blocks. Research revealed that traditional blockchains have constrained throughput. It is ideal for blockchain technology to achieve higher throughput by increasing the block size and lessening the block interval. The methodology used in this paper is of two parts. The first approach uses the cryptographic protocol to ensure the authenticity and integrity of the information using an Ethereum blockchain type. This means that transactions are recorded in write-only mode and contributes to transaction trust and transparency. Our methodology automates smart and secure evaluations and provides credentials using an Improved Elliptic Curve Cryptography Algorithm (IECCA). It is implemented using encryption and decryption algorithms and is demonstrated using analytical and content neutrality. We also demonstrate operation from back-end to end-users application including student and faculty members. The Level of security performance of the proposed scheme is compared with another scheme for a 20MB file size. The proposed schemes achieve 83% IECCA, 78 percent DES, 76% RSA, and 70% AES respectively. The second approach identifies the boundary for conventional block sizes and block intervals. Security of blockchain using stale block rate is identified in the network by conducting a realistic experiment. This enables the realization of optimal block parameters like size and interval. Results presents achieve a rate of transmission for a blockchain platform to be deployed in other activities beyond cryptocurrency, like electronic voting.

Corresponding author: Muhammed Zaharadeen Ahmed, Email: zaharadeen22@unimaid.edu.ng
Department of Computer Engineering, University of Maiduguri, Borno State, Nigeria

INTRODUCTION

Blockchain Technology has emanated because of the need to offer communication security for various IoT systems and mechanisms to efficiently audit and control access in a smart environment Tanwar (2020). This means that methods to secure transmission to solve real-world problems of Privacy, Data Integrity, Authentication and Non-repudiation, must be met Alshahrani (2021). In addition, blockchain technology solves the issues of interoperability and large data integration Roehrs (2019). The study of methods for sending messages in a secret, namely encoded information form, so that only the intended recipient can isolate the disguise and read the message is known as cryptography; derived from the Greek words kryptos and graphein, meaning "hidden" and "writing" Egerton & Emmah (2018).

Blockchain Parameters

The rate at which stale blocks are generated is referred to as the stale block rate. They also refer to blocks that are not included in the longest chain for various reasons, such as inconsistency or cache coherency. Stale blocks are harmful to the blockchain's security and performance because they cause unwanted chain forks in the system. Chain forks have a negative impact on the growth of the ledger's main chain and can cause network bandwidth issues. Above all, the presence of many stale blocks increases the ability of dishonest nodes to engage in fraudulent activities such as selfish mining Xu *et al.* (2022).

The delay at which data is appended to the ledger determines the block interval, which is one of the most important parameters of blockchain systems. A smaller block interval would naturally result in higher throughput, but at the cost of an increased likelihood of generating "stale blocks." Changing the block interval implies altering the Proof-of-Work (PoW) puzzle's difficulty level. The PoW puzzle's difficulty is inversely proportional to the rate at which stale blocks can be generated. This implies that changing the difficulty of the puzzle has a direct impact on the ability of dishonest nodes to attack the network by tampering with the longest chain of the ledger Zhai *et al.* (2019).

The amount of revenue that can be collected within each block is determined by the block size. As a result, the maximum block size governs the blockchain system's throughput. The larger the block size, the slower the propagation speed and the higher the slate block rate. As a result, if one wishes to increase system throughput, lowering system security is unavoidable Chen *et al.* (2019).

Related Work

Boosting the block size is one method of increasing the blockchain system's throughput. For example, Bitcoin Cash, a fork of Bitcoin, has an 8MB limit. Although the actual block sizes are typically much smaller than this limit. Shortening the block interval, on the other hand, may increase system throughput, as demonstrated by Ethereum, which has a block interval of about 15 seconds. Some Bitcoin forks, such as Litecoin, use a 2.5-minute block interval, while Dogecoin uses a 1-minute block interval. A theoretical study on the trade-offs between blockchain system security and the block generation rate was carried out by Tanwar *et al.* (2020). They are referred to as block intervals by unveiling a novel security feature known as chain growth. This property defines the chain's minimum growth rate as seen by honest miners. They hypothesize that it is in an adversary's best interest to reduce system throughput (or to enlarge the block interval). They examined the proposed chain growth as well as two previously proposed measures, common prefix, and chain quality, as a function of block intervals. The common

prefix is used to determine whether two miners have the same understanding of the blockchain. The chain quality describes the length of the chain as accepted by honest miners, which contains adversarial block sequences. The most intriguing result is that contrary to an earlier model's prediction - that the system will break down even in the presence of a very small fraction of adversaries - if the block interval is equal to the block propagation time, the system can tolerate the presence of up to 1/3 Byzantine faulty miners under the same condition. It is worth noting that Ethereum's block interval is quite close to the average block propagation time (12.6 seconds).

In Huang *et al.* (2020), an empirical model analysis with a simulator was conducted by simulating the operation environment of Bitcoin. The simulation employed different standards for Bitcoin that is easier-to-understand in addition to security measures as well as looking at the block size, rather than the block interval. However, the paper omits the capacity of the block size in their computation. The interval between the blocks is presented as 0.5sec. Based on simulation results, the parameters used were approximated but precise values are used in the benchmark (Huang *et al.*, 2020).

Lv *et al.* (2021) assumed that the block propagation time is proportional to the block size. Srinivasu *et al.* (2021) assertion are false because the Internet backbone has very high bandwidth and the global block propagation time may be dominated by queuing time at the router. This is not proportional to the block size but rather influenced by the Internet's congestion degree. And transmission time which is proportional to block size.

Yang *et al.* (2021) proposed a hierarchical blockchain architecture to facilitate electronic voting. The hierarchy would correspond to the voting scale, with the smallest unit as its area. County, state, and national levels are all possibilities. Each area would have its blockchain, which would be linked together according to the hierarchy. Tanwar (2020) provides the same level of security for off-chain transactions as the blockchain does. Huang *et al.* (2020) proposed establishing a strong link between off-chain transactions and those placed on the blockchain, allowing off-chain transactions to have the same level of security as those placed on the blockchain.

METHODOLOGY

Using the first approach, the proposed work uses an ethereal blockchain to analyze the cryptographic security. Ethereum is a blockchain platform with a currency called Ether (ETH) and a programming language called Solidity. As a blockchain network, Ethereum is a decentralized public ledger for validating and recording transactions

Alshahrani (2021). This study used a dataset of 1000 students from 20 courses. A computer expert with a decade of experience at the e-learning center determined the courses to be included in the study using same criteria. As a result, a collaborative analysis of the dataset across multiple subjects is feasible.

The schematic representation of the proposed work is shown below (as in Figure 1).

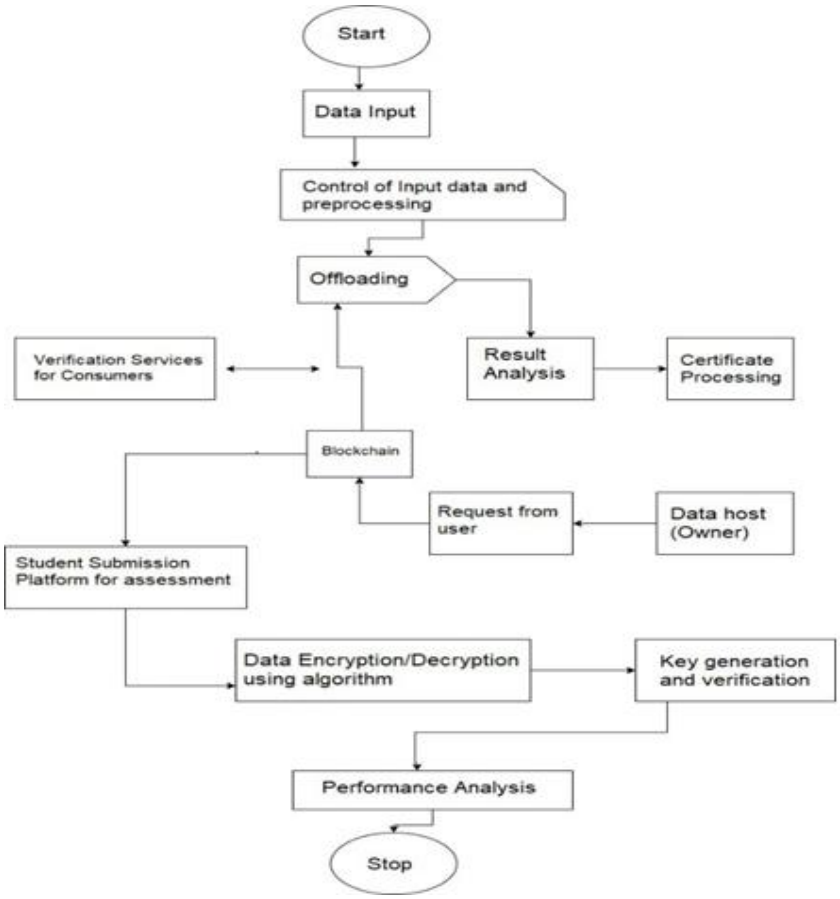

Figure 1: Schematic Representation of the Proposed Work

The proposed design enables the creation of three types of players that interact with one another via smart contracts.

i. Lecturers, teaching assistants, instructors, and other educators.
ii. Learners, which include on-campus students, online students, and others.
iii. Readers, and members of the public who access or validate data, such as employers and higher education institutions.

Controlled Preprocessing

At a point, the input data has not been processed and may contain missing or repetitive packets. It has been preprocessed to remove redundant and duplicated occurrences as well as to clean up missing data. Because the dataset for the education system is large, sample size minimization techniques must be used. Because this dataset contains many attributes, feature extraction tools are required to eliminate those that aren't significant. During the pre-processing stage, the dataset can be normalized. The z-score, which is expressed by Equation, is obtained in the first step of the normalization process as follows.

$$Z = \left[Y - \frac{\alpha}{\omega}\right] \qquad (1)$$

Whereas α represents the mean of the dataset and ω denotes the standard deviation. Therefore, Z is given as follows.

$$Z = \frac{Y - Y'}{D} \qquad (2)$$

Whereas Y represents the sample mean, and D represents the model's standard deviation. The random sample should follow the pattern shown below as follows.

$$Z = \beta 0 + \beta 1 Yj + \xi j \qquad (3)$$

Whereas εj denotes the errors. It is relied on the ω2. Following that, the errors must not depend on one another. Therefore, yj ~ √ ω

$$y_j \sim \frac{\sqrt{\omega} y}{y^2} + \omega - 1 \qquad (4)$$

In equation 4, y represents a random variable. The standard deviation is then used to standardize the movement of the variables. The moment scale deviation is calculated using the expression below.

$$M = \frac{\lambda^m}{\theta^m} \qquad (5)$$

Whereas m denotes the moment scale.

$$\lambda^m = E\ (Y - \alpha)^M \qquad (6)$$

Whereas Y represents a random variable, and E denotes the expected value.

$$\theta^m = \left(\sqrt{E(Y - \alpha^M}\right)^2 \quad y_\omega = \frac{m}{y'} \qquad (7)$$

whereas yω denotes the coefficient of the variance.

After that, the feature scaling procedure will be terminated by setting all of the values to 0 or 1. This procedure is known as the unison-based normalizing approach. The normalized equation will be written as follows:

$$Y' = \frac{y - y_{min}}{y_{msx} - y_{min}} \qquad (8)$$

The data set can be managed once the data has been normalized, and the extent and variability of the data can be constant. This stage is primarily concerned with reducing or eliminating data latency. The normalized data can then be fed into the subsequent stages.

The second approach for this framework is conducted using simulation under predetermined conditions. The first condition states that a dishonest node cannot use more than 30% of the total mining power in its potential state. Block size simulation ranges between 1 - 25 MB, with block interval range between 1 - 30 minutes. In all simulations, the number of generated blocks and the total number of nodes in the network are assumed to be 100. Based on this combination, each simulation runs for 70 seconds to complete, and the order of magnitude is faster than an actual implementation in the real world. Some basic

terminologies used in the simulation is presented (as in table 1) below.

Table 1: Terminologies used in the Simulation

S/No.	Network Parameter	Definition
1.	Stale Block Rate	Percentage of the stale blocks with the total blocks
2.	Block Interval	Average block generation time in seconds
3.	Block size	Fixed size of block in bytes
4.	Number of blocks	Quantity of generated blocks
5.	Number of nodes	Total quantity of nodes in the network
6.	Block RMS	Request management System is the protocol used in managing block request
7.	Number of connections	Connections between nodes on a network

Performance Analysis

For blockchain performance, smart contracts are fully exploited on public permission blockchain. The use of smart contracts presents a state-of-the-art technology to enhance enormous learning experiences, such as assessments, curriculum quality assurance, and learner privacy. It also enhances educational trust procedures and certifications by improving transparency and authenticity while maintaining fine-grained security controls on student data. Some significant simulation parameters are presented (as in table 2) below.

Table 2: Simulation Parameter

S/No.	Parameters	Values
1.	Simulation time	300s, 900s
2.	Size	1000 x 1000m^2
3.	Velocity	12, 45 m/s
4.	Number of Packets	Random number between 10-15
5.	Energy Aggregate	5kWh
6.	Amplitude	0.0123m
8.	Sampling energy	30
9.	Transmission energy	80m
10.	Primary & Secondary User	150, 150
11.	Number of blocks	500, 250,100, 50
12.	Number of nodes	50, 100, 250, 500
13.	Block rate	100/100
14.	Simulation iterations	50 iterations

Improved Elliptic Curve Cryptography Algorithm (IECCA*)*

This algorithm focuses on assessing the security level to compute the strength of a cryptographic primitive. This includes a cipher or hash function. Efficacy is also computed by the comparison approach of the proposed work and other existing strategies. The comparison is the result of three approaches with the proposed approach presented (as in figure 2) below.

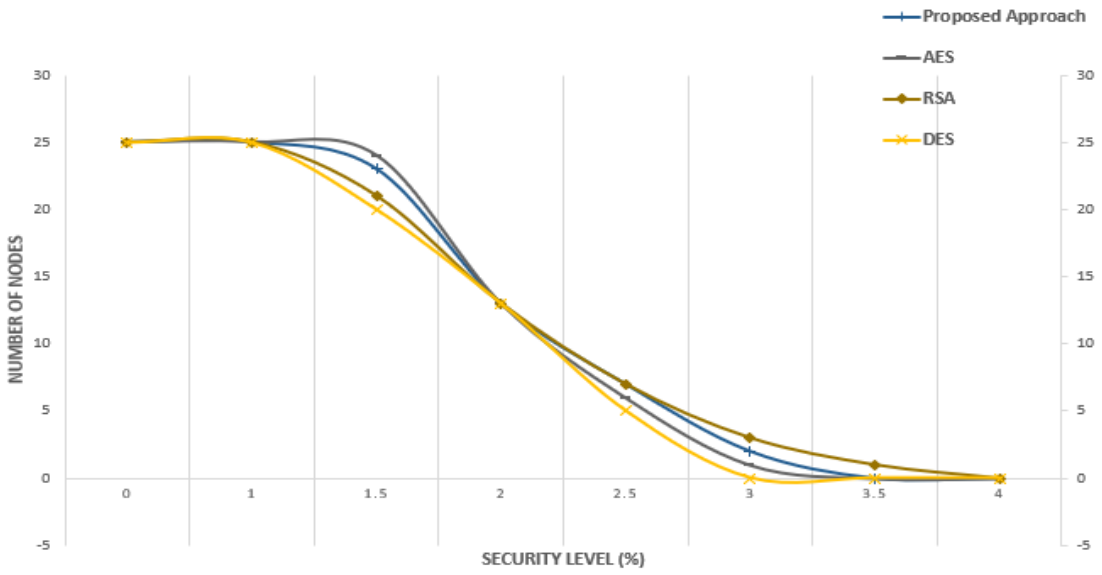

Figure 2: Proposed approach Comparison for security level (%) using different file sizes

In figure 2 above, the IECCA algorithm is used to compare three schemes as Advance Encryption Algorithm (AES), Data Encryption Algorithm (DES), and Rivest Shamir Alderman (RSA), with the proposed scheme. The security level of the 20MB file size has been 83% using the IECCA algorithm, 78 percent DES, 76% RSA, and 70% AES respectively. An assessment of security level is computed for various file sizes such as 40, 60, 80, and 100 MB. The result presents that the proposed approach outperforms other schemes with efficient security levels during network runtime.

Execution Time

The proposed approach is compared with other approaches (DES, RSA, and AES) to determine the Execution time during runtime. This is for different file sizes of 20 MB, 40 MB, 60 MB, and 80 MB. The output is presented graphically (as in figure 3) below.

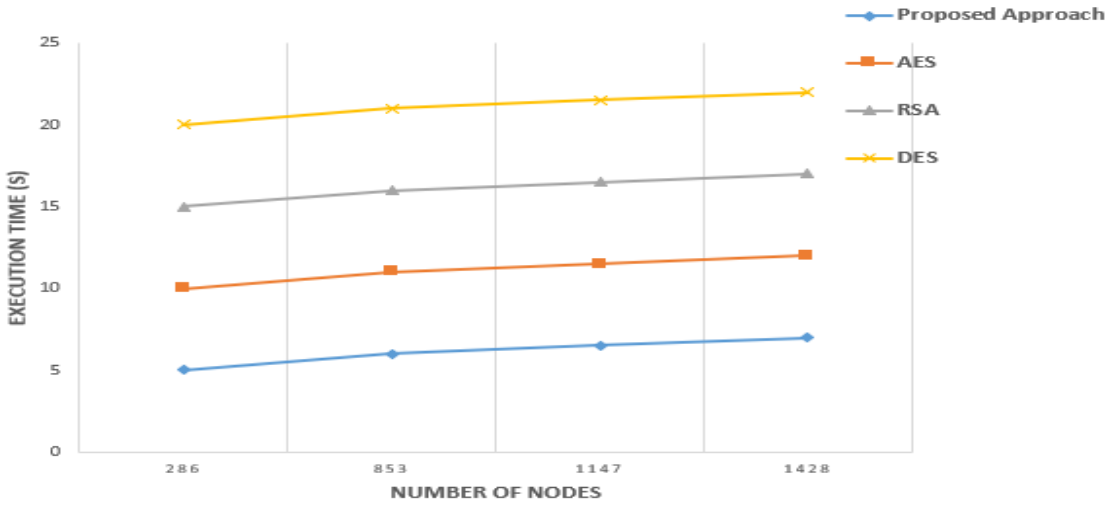

Figure 3: Proposed approach Comparison for execution time (s) for various file sizes

The number of nodes is estimated based on the instruction execution of each scheme. The proposed approach's total execution time is less than 10sec as compared to other approaches higher than 20sec during runtime. This means that the proposed approach outperforms AES, RSA and DES schemes in terms of efficiency.

This research also conducted an assessment using modelling. The goal of these simulations is to investigate the effect of block interval and block size on the stale block rate. A stale block rate is critical in determining blockchain network security. A lower stale block rate is preferable and usually indicates a more secure system (as in figure 4) below.

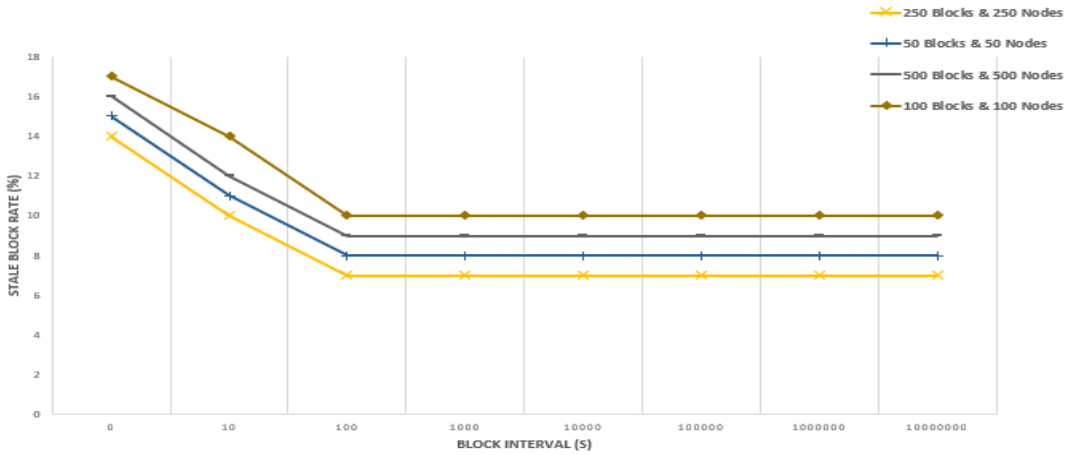

Figure 4: Rate of transmission for Stale block rate Vs block interval using 10 KB block size

Based on the output, This Simulation approach is run for six different block sizes (1 KB, 10 KB, 100 KB, 1 MB, 10 MB, and 25 MB). This is to determine the best security mechanism for our blockchain network. The stale block rate was measured for each of the following block intervals (1, 10, 30, 60, 300, 600, 1200, and 1800 seconds). This covers 48 different scenarios. The stale block rate for each simulation is low as the block interval increases. This ensures a smaller stale block rate is more desired and typically represents a more secure system.

Node rate of transmission is also assessed in the proposed scheme for blockchain voting system using different data (MB) combinations. This is presented (in figure 5) below.

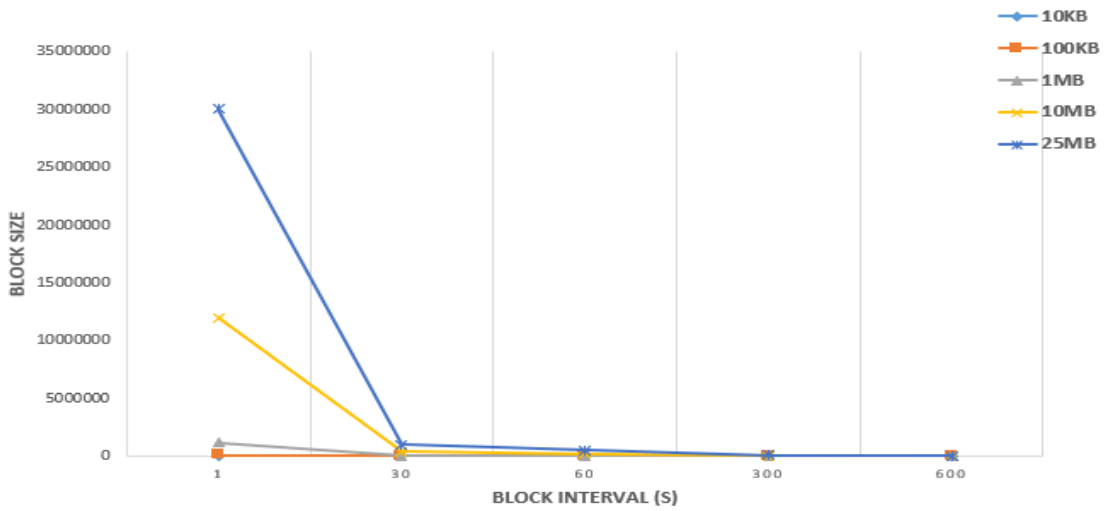

Figure 5: Rate of Transmission

The block interval and size are estimated based on the data unit and the number of blockchain transactions. In addition, it is also determined based on each intersecting point per 10 minutes. This means the maximum throughput can be estimated to achieve a valid block size and interval combinations of the typical transaction size of 500 bytes used. Also, by assuming that there is a tolerance of up to 10% stale block rate. The Green cells indicate valid combinations and orange cells present a stale block rate of more than 10%. The result of the 1KB block size is not presented due to its lack of precision. Also in figure 5, the smallest block interval for the 25MB block size is 600 seconds (i.e., 10 minutes). This is very identical to what has been used by Bitcoin. With a block size of 25MB and a block interval of 600 seconds, the maximum possible throughput is 50,000 transactions per 600 seconds (i.e., 83 transactions per second). All other block size combinations would result in lower maximum throughput.

CONCLUSION

Blockchain technology is a novel solution for decentralized transactions and data management. It does not require the involvement of a trusted third party. The proposed work implements an e-learning platform using, a trust-based blockchain system to assess students' performance. This involves the use of smart contracts to complete evaluations and courses by collating students' feedback. The proposed work also presents how blockchain technology can enhance transparency and trust for evaluation processes and educational activities. An efficient algorithm known as the improved elliptic curve cryptography algorithm (IECCA) is introduced to enhance encryption and decryption. This ensures security level (%) improvement as compared to another approach DES, RSA, and AES in the result.

The Bitcoin operating environment can be simulated using various simulators. The proposed research uses boundary block parameter combinations that keep stale block rates under 10%. Among the parameters we tested, a block size of 25MB with a block interval of 600 seconds appears to provide the best throughput (83 transactions per second). A block size of less than 1MB appears to be impractical, despite the possibility of using smaller block intervals.

REFERENCES

Alshahrani, M. Y. (2021). Implementation of a blockchain system using improved elliptic curve cryptography algorithm for the performance assessment of the students in the e-learning platform. *Applied Sciences*, *12*(1), 74.

Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future generation computer systems*, *95*, 420-429.

Egerton, T., & Emmah, V. (2018). Comparative Analysis of Cryptographic Algorithms in Securing Data. *International Journal of Engineering Trends and Technology (IJETT)*, *58*(3), 118-122.

Gaba, P., Raw, R. S., Mohammed, M. A., Nedoma, J., & Martinek, R. (2022). Impact of Block Data Components on the Performance of Blockchain-based VANET Implemented on Hyperledger Fabric. IEEE Access.

Huang, S., Wang, G., Yan, Y., & Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, *54*, 361-371.

Lv, Z., Qiao, L., Hossain, M. S., & Choi, B. J. (2021). Analysis of using blockchain to protect the privacy of drone big data. *IEEE Network*, *35*(1), 44-49.

Okegbile, S. D., Cai, J., & Alfa, A. S. (2022). Performance analysis of blockchain-enabled data sharing scheme in cloud-edge computing-based IoT networks. IEEE Internet of Things Journal.

Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. Electronics, 10(12), 1437.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407.

Xu, G., Xu, S., Cao, Y., Yun, F., Cui, Y., Yu, Y., & Xiao, K. (2022). PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios. *Security and Communication Networks*, *2022*.

Yang, J., Ma, X., Crespo, R. G., & Martínez, O. S. (2021). Blockchain for supply chain performance and logistics management. Applied stochastic models in business and industry, 37(3), 429-441.

Yadav, K., Kachout, M., Alharbi, Y., Alreshidi, A., Jain, A., Alreshidi, E. J., ... & Alotaibi, S. D. (2022). Securing Diagnosed Parkinson's Disease Data by Blockchain Technology using 2E2C Algorithm. IETE Journal of Research, 1-16.

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In *Journal of Physics: Conference Series* (Vol. 1168, No. 3, p. 032077). IOP Publishing.