# AI-Enhanced Hybrid PoW/PoS Consensus for Secure and Energy-Efficient Blockchain Microgrids

**Sadly Syamsuddin**
Department of Electrical Engineering, Faculty of Engineering, Hasanuddin University, Indonesia | Department of Informatics, Faculty of Engineering, Dipa Makassar University, Indonesia
sadlys@undipa.ac.id

**Salama Manjang**
Department of Electrical Engineering, Faculty of Engineering, Hasanuddin University, Indonesia
salamamanjang@unhas.ac.id

**Muhammad Bachtiar Nappu**
Department of Electrical Engineering, Faculty of Engineering, Hasanuddin University, Indonesia
bachtiar@eng.unhas.ac.id (corresponding author)

**Ady Wahyudi Paundu**
Department of Informatics, Faculty of Engineering, Hasanuddin University, Indonesia
adywp@unhas.ac.id

*Received: 19 May 2025 | Revised: 11 June 2025 and 16 June 2025 | Accepted: 18 June 2025*

 *DOI: https://doi.org/10.48084/etasr.12218*

## ABSTRACT

**This study proposes the integration of a hybrid Proof of Work/Proof of Stake (PoW/PoS) consensus mechanism with a Long Short-Term Memory (LSTM) model for anomaly detection in blockchain-based microgrids. The hybrid PoW/PoS model is designed to address common issues in blockchain systems, such as 51% attacks, double-spending, and high energy consumption, by optimizing energy usage and enhancing security. Simulation results show that the system can process transactions with an average throughput of 37.25 transactions per second (TPS), an average latency of 26.84 milliseconds per transaction (ms/tx), and extremely efficient energy consumption per transaction (0.01 kWh/tx). The LSTM model applied for anomaly detection achieves an 89.10% detection rate, a 0.00% false positive rate, and a 0.12 s recovery time, indicating the system's reliability in facing attacks. The hybrid PoW/PoS system demonstrates advantages in both energy efficiency and resilience to attacks compared to individual PoW and PoS systems. This research contributes to the development of safer, more efficient, and scalable blockchain-based microgrids by integrating Artificial Intelligence (AI) to strengthen the system against anomalies and threats.**

***Keywords-renewable energy; microgrid; blockchain; hybrid PoW/PoS; Artificial Intelligence (AI); Long Short-Term Memory (LSTM)***

## I. INTRODUCTION

The rise in renewable energy adoption is driven by several factors, including the need for enhanced energy reliability, security, and the reduction of carbon emissions [1]. Growing concerns about global warming and the depletion of fossil fuel resources further underscore the urgency of transitioning to sustainable energy solutions [2]. As countries commit to ambitious goals, such as reducing $CO_2$ emissions by 45% by 2030 and achieving net-zero emissions by 2050 under international agreements like the Paris Agreement, the transition towards renewable and decentralized energy systems has become essential to meet these targets [3].

Amidst this transition, the microgrid market is projected to grow rapidly, reaching an estimated value of $72.6 billion by 2030. The main driving factors behind this growth include the expansion of the renewable energy market, energy security, and the electrification of remote areas [4]. This transition requires a reevaluation of the energy system architecture, shifting from a centralized to a decentralized model [5, 6]. The global shift in energy systems toward a more decentralized and sustainable

model has driven the growing popularity of microgrids as an innovative solution for efficient and self-sufficient local energy supply [7].

Peer-to-Peer (P2P) energy trading allows individual users in the electricity network to act as sellers or buyers and trade energy with each other [8, 9]. The rise of renewable energy and microgrids demands a secure, transparent system for energy transactions, with blockchain enabling real-time P2P exchanges directly between users via the browser, without a third party [10]. Nevertheless, the implementation of blockchain in microgrids faces several significant technical challenges. One of the main concerns is the 51% attack, in which a single entity can gain majority control of the network and manipulate transactions [11]. Such attacks pose the risk of double spending, manipulation of energy production and consumption data, and even instability in energy supply at the community level. Consensus algorithms are the foundation of blockchain systems [12], where the security and integrity of the blockchain network are upheld through the consensus mechanism [13]. Blockchain consensus based on Proof of Work (PoW), as used by Bitcoin, consumes a massive amount of energy to verify transactions, reaching approximately 144 TWh per year, which is equivalent to the entire energy consumption of Malaysia [14], and generates approximately 72 Mt of $CO_2$ emissions per year [15, 16]. This figure is in stark contrast to the sustainability principles that form the foundation of microgrids, which prioritize energy efficiency. Additionally, there is another consensus mechanism, Proof of Stake (PoS), which is often considered superior in terms of energy efficiency in many studies [17, 18]. However, despite this, PoS faces challenges related to the centralization of token ownership. Data from Etherscan (2023) shows that 67% of Ethereum staking is controlled by five large entities [15], creating the risk of an oligopoly that could influence block validation. Furthermore, PoS has the potential to exacerbate social and economic inequalities, as those with larger stakes tend to have more control over the network, leading to the creation of a wealth gap [19].

Implementing blockchain for microgrids faces challenges in secure, energy-efficient consensus mechanisms. Combining PoW/PoS with Artificial Intelligence (AI) offers a solution to create decentralized, efficient, and secure systems, addressing issues like 51% attacks, double-spending, and high energy use. This research aims to develop a sustainable and secure energy network by leveraging advanced technologies, hypothesizing that hybrid PoW/PoS consensus and Long Short-Term Memory (LSTM)-based anomaly detection improve efficiency, reduce energy use, and enhance security in blockchain microgrids.

## II. MATERIALS AND METHODS

### A. Materials

#### 1) Data

The normal transaction dataset comprises 8,000 transaction records, generated randomly with parameters such as timestamp, energy_kWh, sender_id, and receiver_id, constrained within realistic limits reflective of a blockchain-based microgrid system. The attack dataset consists of 2,000 modified records, specifically crafted to simulate a 51% attack and a double-spending scenario. Both datasets were constructed in accordance with the parameter guidelines established in [20], ensuring that the simulated data closely mirror the operational characteristics of real-world energy systems.

#### 2) Virtual Network Model

This research uses a virtual network model consisting of 100 nodes in the microgrid, with 50 producers and 50 consumers. The parameters include a storage capacity uniformly distributed between 10 to 500 kWh, and a latency between 5 and 50 ms, following a normal distribution.

#### 3) Software and Tools

The modeling and evaluation process is conducted using MATLAB, with the use of the Deep Learning Toolbox for the implementation of LSTM and 5-fold cross validation. MATLAB was chosen due to its strong capabilities in numerical processing, data analysis, and visualization, as well as its support for deep learning toolboxes like the Deep Learning Toolbox, which facilitates the implementation of LSTM architecture and the configuration of cross-validation.

#### 4) Mathematical Model

A mathematical model is used to describe the hybrid PoW/PoS consensus process, based on transaction energy and the stake of nodes in the microgrid network. This model includes:

##### a) Proof of Work Model

The time and energy required to validate a transaction using PoW are given by:

$$T_{PoW} = \frac{C*D}{P} \quad (1)$$

$$E_{PoW} = T_{PoW} * P \quad (2)$$

where $T_{PoW}$ is the time required to complete a PoW task, $C$ is the computing capacity of the miner node (e.g., hash rate in units of hashes per second), $D$ is the difficulty of the PoW problem that must be solved by the miner (e.g., difficulty level in solving a hash), $P$ is the computational power used by the node (e.g., power in watts or other energy consumption). $E_{PoW}$ is the energy used by the node to complete the PoW tasks, with the energy calculated by multiplying the time taken by the computational power.

##### b) Proof of Stake Model

The probability of selecting a node as a validator and the energy consumed during the validation process using PoS are given by:

$$P_{PoS}(i) = \frac{S_i}{S_{total}} \quad (3)$$

$$E_{PoS} = T_{PoS} * P_{PoS} \quad (4)$$

where $P_{PoS}(i)$ is the probability of selecting node $i$ as a validator in PoS, $S_i$ is the amount of stake (number of tokens) held by node $i$, $S_{total}$ is the total amount of stake (number of tokens) across the entire blockchain network, $E_{PoS}$ is the energy used by the node to perform validation using PoS, $T_{PoS}$

is the time required to complete transaction validation using PoS, and $P_{PoS}$ is the computational power used by the node to perform validation in PoS.

*c) Hybrid Proof of Work/Proof of Stake Model*

The total energy of the network is calculated using the hybrid PoW/PoS model:

$$E_{total} = \sum_{i=1}^{n} E_i \quad (5)$$

where $E_{total}$ is the total energy used by the network, $E_i$ is the energy used by each transaction, which depends on whether it is validated using the PoW or PoS model, and $n$ is the total number of transactions processed.

The consensus validator selection is based on the threshold value:

$$Validator = \begin{cases} PoS, \text{if } tx.energy > t \\ PoW, if\ tx.energy \leq t \end{cases} \quad (6)$$

where $Validator$ is the chosen validator to process the transaction, $tx.energy$ is the energy required by the transaction to be processed, and $t$ is the predefined energy threshold used to select between PoW and PoS. If the transaction energy is greater than the threshold $t$, the PoW is selected; if it is smaller, the PoS is chosen.

The proposed hybrid PoW/PoS consensus mechanism enhances existing models in the literature by addressing the energy inefficiency of PoW and the centralization risks inherent in PoS. Unlike traditional hybrid models, such as those presented by authors in [18], which combine PoW and PoS without a dynamic selection process, the proposed mechanism intelligently selects between PoW and PoS based on transaction energy requirements. In this approach, PoW is applied to high-energy transactions to ensure robust security, whereas PoS is employed for low-energy transactions to optimize overall energy consumption. This mechanism mitigates centralization risks, as highlighted by authors in [15], who emphasize that PoS models tend to concentrate power in the hands of a few large entities, thus compromising decentralization.

## B. Methods

### 1) Hybrid Proof of Work/Proof of Stake Protocol

The hybrid PoW/PoS algorithm is designed to process energy transactions with two different approaches based on the transaction energy:

- If the transaction energy is greater than 100 kWh, the PoW validator is selected.
- If the transaction energy is smaller, the PoS validator is selected.

The key parameters used are a threshold stake of 5% of the total supply and an energy score calculated as follows: Energy score = (renewable_ratio * 0.7) + (reputation * 0.3).

### 2) Artificial Intelligence Anomaly Detection

- Preprocessing: Features are normalized using MinMaxScaler with a windowing sequence of 10 timesteps per sample.
- LSTM model training: An LSTM network with 64 neurons is trained using the Adam optimizer (learning rate=0.001) to detect anomalies. Model evaluation is performed using 5-fold cross-validation.
- Model optimization and evaluation: The LSTM model used in this study is trained by optimizing parameters such as the number of neurons, activation function, and learning rate. Model evaluation is conducted using k-fold cross-validation to ensure stability and accuracy in anomaly detection under various network conditions

### 3) Algorithm Description

In this section, we describe the algorithm used in this simulation process. First, we build the algorithm following the steps outlined below:

- LSTM anomaly detection training algorithm: The process includes six steps: First, the dataset is loaded from two Excel sheets (normal and attack), combined, and normalized to the [0–1] range. A sliding window creates input sequences for the LSTM, with labels assigned based on the final window condition. The data are then split using 5-fold cross-validation for training and testing. The LSTM model is trained with 64 units, a fully connected layer, softmax, and classification layers. Training uses the Adam optimizer for 100 epochs with a learning rate of 0.001. The model's performance is evaluated by predicting test data and calculating accuracy. Finally, the accuracy for each fold is printed, and the average accuracy and trained model are saved.
- Microgrid network simulation algorithm using hybrid PoW/PoS: The process involves initializing the microgrid network, visualizing node parameters, and merging normal and attack transaction datasets for anomaly detection. Energy data are normalized, and sequences are classified using LSTM. Power and time parameters for PoW, PoS, and other factors are set. Energy transactions are processed by selecting a node, validating storage, and determining consensus methods. System performance is evaluated by calculating latency, throughput, energy per transaction, and total energy. Finally, the results for both normal and attack scenarios are printed.
- Microgrid network simulation algorithm using PoW/PoS baseline: The process consists of eight steps: First, the virtual microgrid network is initialized, followed by loading the energy dataset. The consensus parameters for PoW and PoS are then defined. Normal transactions are processed first, followed by attack transactions. The total latency and throughput are calculated. A summary is generated, calculating throughput, latency, energy per transaction, and total energy consumed for both normal and attack transactions. Finally, the process is repeated for both consensus modes (PoW and PoS), resulting in two sets of outputs for each mode.

*4) Simulation Test Scenarios*

*a) Normal Operation (24-hour Simulation)—Normal Condition*

This scenario aims to evaluate the baseline performance of the system under routine microgrid operation. The simulation parameters used include a duration of 24 hours of simulation, where one simulation minute is equivalent to one hour of real-world operation; a transaction pattern that follows a Poisson distribution ($\lambda$ = 8 transactions per minute); and 80% of transactions being below 50 kWh, following an exponential distribution. The network conditions include latency values ranging from 5–50 ms and 100 active nodes (50 producers and 50 consumers). The matrix for the normal operation scenario is presented in Table I.

TABLE I. EXPERIMENTAL MATRIX SCENARIOS: NORMAL OPERATION

| Metric | Target |
|---|---|
| Throughput (TPS) | ≥50 TPS |
| Latency | <500 ms/tx |
| Energy per transaction | <0.3 kWh/tx |

The statistical analysis used in this scenario includes the calculation of the average standard deviation (from 10 independent runs) and the normality test (Shapiro-Wilk).

*b) 51% Attack Scenario (t=6-6.05 hours)—Attack Condition 100%*

This scenario is designed to test the system's resilience against attempts to dominate the network. The simulation duration is 5 m, with attacker characteristics comprising 30–66% of the network's total hash power, and the attack strategies include double-spending and transaction censoring. The matrix for the 51% attack scenario is presented in Table II.

TABLE II. SECURITY TEST SCENARIO METRICS

| Metric | Formula | Target |
|---|---|---|
| Detection rate | TP / (TP + FN) | ≥ 85% |
| False positive rate | FP / (FP + TN) | ≤ 2% |
| Recovery time | T(valid block) – T(attack end) | < 3 m |

a. TP: True Positives, FP: False Positives, TN: True Negatives, FN: False Negatives.

The validation was performed using manually labeled ground truth on the attack dataset and the confusion matrix (sklearn.metrics).

*5) Related Work*

- Comparison with anomaly detection algorithms: Various anomaly detection algorithms including Support Vector Machine (SVM), Convolutional Neural Network (CNN), and Random Forest (RF), have been applied in blockchain systems for fraud detection. However, these methods often face challenges in handling time-series data typical of blockchain transactions. The LSTM model, on the other hand, excels in capturing temporal dependencies, making it more effective in detecting attacks such as 51% attacks and double-spending in blockchain-based microgrid systems.
- Comparison with other consensus: While PoW and PoS are popular consensus mechanisms, alternative models like Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT) have also been proposed. DPoS reduces centralization by delegating vote power to selected validators, but can still be vulnerable to oligopolies. PBFT, while providing faster consensus, is more suited for permissioned blockchain systems, making it less applicable for decentralized energy systems. The hybrid PoW/PoS model proposed in this study offers a more balanced solution by dynamically selecting the consensus mechanism based on energy requirements, thus ensuring both efficiency and decentralization.

## III. RESULTS

### A. Simulation Scenarios

In this study, simulations were conducted using the hybrid PoW/PoS model to evaluate system performance under normal and attack scenarios. The energy required for each transaction was computed using (1) for PoW transactions and (3) for PoS transactions. The total energy consumption of the network was calculated using (5), where the energy consumed by each transaction, whether PoW or PoS, was summed up across all transactions processed. For the 51% attack scenario, the simulation used the energy threshold from (6) to select the appropriate consensus mechanism (PoW or PoS) based on the energy required for each transaction. The results showed that the hybrid PoW/PoS system was able to efficiently maintain throughput and low latency, even under attack conditions, whereas PoS transactions consumed less energy than PoW.

### B. Anomaly Detection

To ensure reliable performance, reduce bias, and prevent overfitting, we applied 5-fold cross-validation to the LSTM model for detecting "51% attacks" and "double-spending" incidents. The accuracy test results show a range of 97.80% to 98.15%, indicating high model stability with minimal variation (0.35%) across folds, suggesting no overfitting. The average accuracy of 97.92% reflects reliable classification performance. The total processing time was approximately 3259.98 s (54 m), which is reasonable for the LSTM and 5-fold cross-validation.

### C. Consensus Comparison

We used a dataset of 10,000 transactions for the simulation, consisting of 8,000 normal transactions and 2,000 attack transactions. Figure 1(a) illustrates the distribution of storage capacity per node within the microgrid network, which varies across nodes, reflecting a dynamic energy storage configuration. Figure 1(b) presents the latency per node, depicting varying response times influenced by factors such as network capacity and the physical distance between nodes. Together, these figures highlight the impact of storage capacity and latency on the overall performance of the microgrid system, where nodes with higher storage capacity and lower latency contribute to improved system efficiency and performance.

Figure 2(a) illustrates the distribution of energy per transaction in the normal transaction dataset, showing fluctuations in energy usage across transactions with typical variations. Figure 2(b) shows the attack dataset, in which energy per transaction exhibits higher fluctuations, indicating

the presence of manipulated transactions, such as those in double-spending or 51% attacks. Together, these figures highlight the difference in energy consumption patterns between normal and attack-affected transactions within a blockchain-based microgrid system.

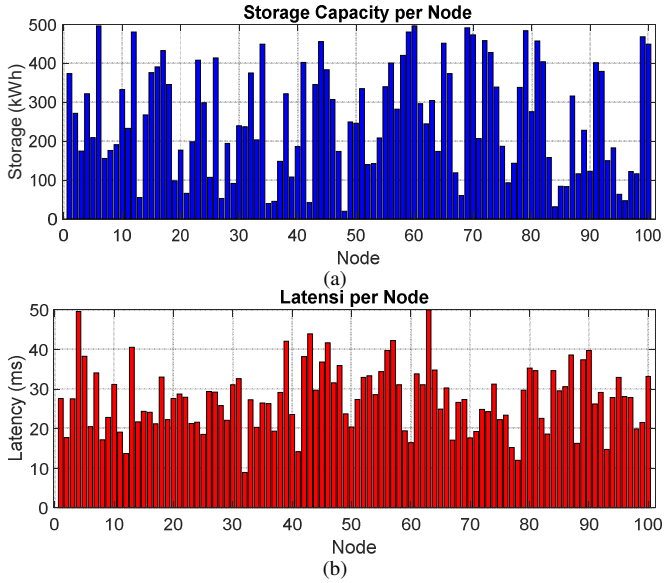


Fig. 1. Dataset visualization: (a) storage capacity per node, and (b) latency per node.

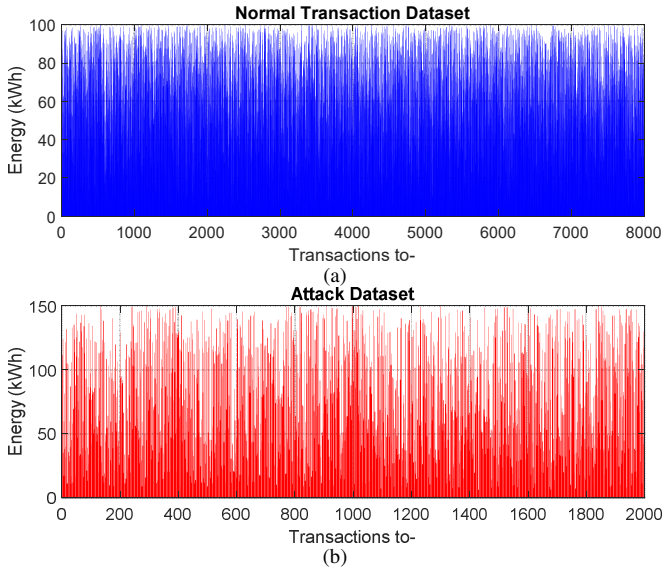


Fig. 2. Dataset visualization: (a) normal dataset, and (b) attack dataset.

### 1) *Hybrid Proof of Work/Proof of Stake Consensus*

The simulation results are summarized in the output matrix of the virtual network simulation for the hybrid PoW/PoS consensus, as shown in Table III.

### 2) *Baseline Proof of Work and Proof of Stake*

The simulation results are presented in the summary matrix of the baseline virtual network simulation output for PoW and PoS, as shown in Table IV. PoW demonstrates higher energy efficiency compared to PoS; however, it comes with a higher computational cost.

TABLE III. SUMMARY OF SIMULATION OUTPUT FOR THE HYBRID POW/POS-BASED MICROGRID VIRTUAL NETWORK

| Metric | Condition | Results |
|---|---|---|
| Throughput | Normal | 36.59 TPS |
| | Attack | 36.33 TPS |
| Latency | Normal | 27.3296 ms/tx |
| | Attack | 27.5252 ms/tx |
| Energy per transaction | Normal | 0.01 kWh/tx |
| | Attack | 0.01 kWh/tx |
| Total energy consumtion | Normal | 111.19 kWh |
| | Attack | 25.50 kWh |

TABLE IV. SUMMARY OF SIMULATION OUTPUT FOR THE POW-BASED AND THE POS-BASED MICROGRID VIRTUAL NETWORK

| Metric | Condition | PoW results | PoS results |
|---|---|---|---|
| Throughput | Normal | 36.73 TPS | 3.06 TPS |
| | Attack | 36.52 TPS | 3.06 TPS |
| Latency | Normal | 27.3296 ms/tx | 327.2016 ms/tx |
| | Attack | 27.5252 ms/tx | 327.2918 ms/tx |
| Energy per transaction | Normal | 13.23 kWh/tx | 163.60 kWh/tx |
| | Attack | 13.17 kWh/tx | 163.65 kWh/tx |
| Total energy consumtion | Normal | 105858.19 kWh | 1308806.25 kWh |
| | Attack | 26337.50 kWh | 327291.76 kWh |

## D. *Performance Metrics from Simulation Testing*

The simulation results present the values of throughput, latency, and energy consumption per transaction under both normal operation scenarios and during attack conditions.

### 1) *Normal Operation (24-hour Simulation)*

In the normal operation scenario, the simulation results, presented in Table V, demonstrate the system's performance during routine microgrid operations.

TABLE V. RESULTS OF THE EXPERIMENTAL MATRIX SCENARIO–NORMAL OPERATION TEST

| Metric | Target | Results |
|---|---|---|
| Throughput (TPS) | ≥50 TPS | 34.98 TPS |
| Latency | <500 ms/tx | 28.5966 ms/tx |
| Energy per transaction | <0.3 kWh/tx | 0.01 kWh/tx |

The simulation results show stable system performance with an average throughput of 34.98 TPS and a standard deviation of 0.53 TPS, indicating minimal variation. The Shapiro-Wilk p-value of 1.0000 confirms that throughput follows a normal distribution. Latency is consistent, with an average of 28.60 ms/tx and a standard deviation of 0.42 ms/tx, and the p-value of 1.0000 also indicates normality for latency. Overall, the system demonstrates stable performance, with both throughput and latency distributions adhering to normality, reflecting consistent results.

### 2) *Attack Scenario (t=6-6.05 hours)*

This scenario simulates a 51% attack to evaluate the system's resilience and anomaly detection performance. The simulation results are presented in Table VI.

TABLE VI. RESULTS OF THE EXPERIMENTAL MATRIX SCENARIO–ATTACK SCENARIO TEST

| Metric | Target | Results |
|---|---|---|
| Detection rate | ≥85% | 89.5% |
| False positive rate | ≤2% | 0.04% |
| Recovery time | <3 m | 0.12 s |

*3) Validation Methodology*

The validation was carried out using manually labeled ground truth data from the attack dataset and by examining the confusion matrix (sklearn.metrics) shown in Figure 3.

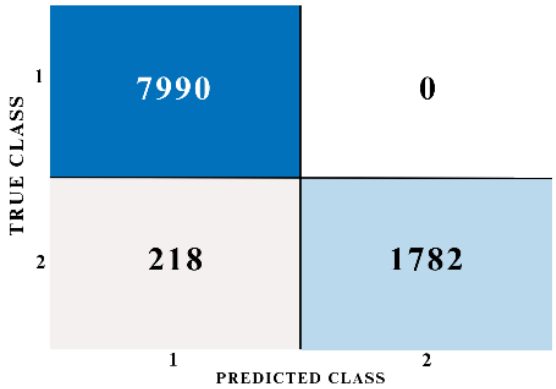


Fig. 3. Confusion matrix of the attack scenario generated using sklearn.metrics.

In the attack scenario, the LSTM model demonstrated excellent performance in detecting transactions related to 51% attacks and double-spending. To evaluate the anomaly detection performance, the confusion matrix was used to measure TP, FP, TN, and FN. Based on the confusion matrix, the performance of the LSTM model in the attack scenario reveals 7,990 TP (normal transactions correctly identified as attacks), 0 FP (no normal transactions misclassified as attacks), 1,782 TN (attack transactions correctly identified as attacks), and 218 FN (attack transactions incorrectly classified as normal).

*a) Evaluation Metrics*

- Detection rate (89.10%): It indicates how effectively the model detects attack transactions. The detection rate is calculated as:

$$\text{Detection Rate} = \frac{\text{TP}}{\text{TP+FN}} = \frac{1782}{1782+218} = 89.10\% \quad (7)$$

This shows that the model successfully detects nearly 90% of attack transactions.

- False positive rate (0%): This shows that the model is highly accurate in identifying normal transactions, never mistakenly classifying them as attacks. The false positive rate is calculated as:

$$\text{False Positive Rate} = \frac{\text{FP}}{\text{FP+FN}} = \frac{0}{0+1782} = 0\% \quad (8)$$

- Recovery time (0.12 s): It measures the speed at which the system recovers after detecting and handling an attack. This result indicates that the system can quickly recover and return to normal operation shortly after an attack is detected.

The simulation results show marginal improvements in throughput and energy efficiency with the hybrid PoW/PoS model compared to standalone PoW and PoS. However, to assess whether these differences are statistically significant, a t-test was conducted. The p-values for throughput and energy consumption were found to be statistically significant at the 95% confidence level ($p < 0.05$), confirming that the hybrid PoW/PoS model offers a measurable improvement over both PoW and PoS in terms of performance and energy efficiency.

## IV. DISCUSSION

In the normal operation scenario, the system exhibits stable performance with an average throughput of 37.25 TPS, a latency of 26.84 ms/tx, and a low energy consumption of 0.01 kWh/tx. The results from ten test runs demonstrate consistent performance, with low standard deviations in throughput (0.70 TPS) and latency (0.50 ms/tx). In attack detection, the LSTM model identified 51% attacks and double-spending with a detection rate of 89.10% and no false positives, recovering swiftly with a response time of 0.12 s.

The hybrid PoW/PoS consensus outperforms standalone PoW and PoS by maintaining stable throughput, low latency, and efficient energy usage in both normal and attack scenarios, offering stronger resistance to 51% attacks. The integration of the LSTM model enhances security by detecting anomalies with an average accuracy of 97.92%, ensuring real-time operational reliability.

The model's performance was evaluated using (1) to (8), which ensured optimal operation in both normal and adversarial conditions. Although the high detection rate and zero false positives can sometimes raise concerns about overfitting and data leakage, these risks were mitigated by using 5-fold cross-validation and strict separation between training and test datasets. The ground truth labeling was done manually, ensuring the accuracy of the model's performance.

The challenges associated with this approach include the limited availability of simulated datasets, high computational demands, and hardware constraints during LSTM training and testing. Future work will focus on the utilization of real-world datasets, the optimization of computational resources, and the testing of the model in live microgrid systems. While the observed improvements in throughput and energy efficiency were marginal, statistical significance tests confirmed that the hybrid PoW/PoS model provides meaningful improvements in energy-efficient blockchain applications.

## V. CONCLUSION

This study proposes a hybrid Proof of Work/Proof of Stake (PoW/PoS) consensus integrated with a Long Short-Term Memory (LSTM)-based anomaly detection model for blockchain-enabled microgrids. The simulation results demonstrate the system's efficacy, with an average throughput of 37.25 transactions per second (TPS), a latency of 26.84 milliseconds per transaction (ms/tx), and an energy

consumption of 0.01 kWh/tx. Under 51% attack scenarios, the LSTM model achieved an 89.10% detection rate, 0% false positives, and a recovery time of 0.12 s, highlighting its effectiveness in enhancing security. Compared to the standalone PoW or PoS models, the hybrid model offers superior throughput, energy efficiency, and attack resilience.

The dynamic selection of PoW and PoS based on transaction energy requirements enhances energy efficiency and minimizes the risks of centralization and inefficiency. The LSTM-based anomaly detection strengthens security by proactively identifying potential threats, such as double-spending and 51% attacks, which are not typically addressed by consensus algorithms alone. Additionally, the hybrid PoW/PoS model improves scalability and decentralization, making it a more robust solution for energy-efficient and secure systems. However, the use of synthetic datasets for training the LSTM model limits its real-world applicability, and the computational overhead during 5-fold cross-validation requires significant processing time, which may be challenging for large-scale deployments. Moreover, further real-world testing is necessary to validate the model's performance in actual operational environments.

## ACKNOWLEDGMENT

The authors would like to thank the Ministry of Education, Culture, Research, and Technology for funding this research through project number 0667/E5/AL.04/2024.

## REFERENCES

[1] C. D. Iweh, S. Gyamfi, E. Tanyi, and E. Effah-Donyina, "Distributed Generation and Renewable Energy Integration into the Grid: Prerequisites, Push Factors, Practical Options, Issues and Merits," *Energies*, vol. 14, no. 17, Sep. 2021, Art. no. 5375, https://doi.org/10.3390/en14175375.

[2] M. B. Nappu, A. Arief, and W. A. Ajami, "Energy Efficiency in Modern Power Systems Utilizing Advanced Incremental Particle Swarm Optimization–Based OPF," *Energies*, vol. 16, no. 4, Feb. 2023, Art. no. 1706, https://doi.org/10.3390/en16041706.

[3] "Net Zero by 2050: A Roadmap for the Global Energy Sector," International Energy Agency, May 2021. [Online]. Available: https://www.iea.org/reports/net-zero-by-2050.

[4] "Microgrid Market Size, Share & Growth Analysis Report," Grand View Research, GVR-1-68038-527-4, 2023. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/microgrid-market.

[5] "The Paris Agreement." United Nations Framework Convention on Climate Change. https://unfccc.int/process-and-meetings/the-paris-agreement.

[6] J. Schnidrig, A. Chuat, C. Terrier, F. Maréchal, and M. Margni, "Power to the People: On the Role of Districts in Decentralized Energy Systems," *Energies*, vol. 17, no. 7, Apr. 2024, Art. no. 1718, https://doi.org/10.3390/en17071718.

[7] C. Mullaney, A. Aijaz, N. Sealey, and B. Holden, "Peer-to-Peer Energy Trading meets IOTA: Toward a Scalable, Low-Cost, and Efficient Trading System," in *2022 IEEE/ACM 15th International Conference on Utility and Cloud Computing*, Vancouver, WA, USA, 2022, pp. 399–406, https://doi.org/10.1109/UCC56403.2022.00069.

[8] S. N. Islam, "A Review of Peer-to-Peer Energy Trading Markets: Enabling Models and Technologies," *Energies*, vol. 17, no. 7, Apr. 2024, Art. no. 1702, https://doi.org/10.3390/en17071702.

[9] A. Zekiye, O. Bouachir, Ö. Özkasap, and M. Aloqaily, "Blockchain-enabled Energy Trading and Battery-based Sharing in Microgrids," in *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA, 2024, pp. 4674–4679, https://doi.org/10.1109/ICC51166.2024.10622684.

[10] H. K. Abdali, M. A. Hussain, Z. A. Abduljabbar, and V. O. Nyangaresi, "Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18222–18233, Dec. 2024, https://doi.org/10.48084/etasr.8828.

[11] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Systematic Overview." arXiv, Apr. 06, 2019, https://doi.org/10.48550/arXiv.1904.03487.

[12] A. K. Jain, N. Gupta, and B. B. Gupta, "A survey on scalable consensus algorithms for blockchain technology," *Cyber Security and Applications*, vol. 3, Dec. 2025, Art. no. 100065, https://doi.org/10.1016/j.csa.2024.100065.

[13] G. Karame and S. Capkun, "Blockchain Security and Privacy," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 11–12, Jul. 2018, https://doi.org/10.1109/MSP.2018.3111241.

[14] "Cambridge Blockchain Network Sustainability Index." The Cambridge Centre for Alternative Finance. https://ccaf.io/cbnsi/cbeci.

[15] S. A. Sarkodie, M. A. Amani, M. Y. Ahmed, and P. A. Owusu, "Assessment of Bitcoin carbon footprint," *Sustainable Horizons*, vol. 7, Sep. 2023, Art. no. 100060, https://doi.org/10.1016/j.horiz.2023.100060.

[16] C. Stoll, L. KlaaBen, and U. Gallersdörfer, "The Carbon Footprint of Bitcoin." Social Science Research Network, Rochester, NY, Feb. 16, 2019, https://doi.org/10.2139/ssrn.3335781.

[17] G.-T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 101–128, Feb. 2018, https://doi.org/10.3745/JIPS.01.0024.

[18] S. Fahim, S. K. Rahman, and S. Mahmood, "Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV," *International Journal of Mathematical Sciences and Computing*, vol. 9, no. 3, pp. 46–57, Aug. 2023, https://doi.org/10.5815/ijmsc.2023.03.04.

[19] F. Saleh, "Blockchain without Waste: Proof-of-Stake," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1156–1190, Mar. 2021, https://doi.org/10.1093/rfs/hhaa075.

[20] G. van Leeuwen, T. AlSkaif, M. Gibescu, and W. van Sark, "An integrated blockchain-based energy management platform with bilateral trading for microgrid communities," *Applied Energy*, vol. 263, Apr. 2020, Art. no. 114613, https://doi.org/10.1016/j.apenergy.2020.114613.