GRADIVA

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

Fraud Incidence Response in Power Sector Using Optimized Consensus Blockchain Technique

Lois Onyejere Nwobodo[1], Udeh Chukwuma Callistus[2]*, Eze Marcel Nduka[3], Ozoani Uchechukwu Isaac[4], Mbamalu Ikenna Chuddy[5], Nwamuo Chibuzo Udochukwu[6] & Ebere Uzoka Chidi[7]

1.Department of Computer Engineering, Faculty of Engineering, Enugu State University of Science and Technology, Enugu, Nigeria.
2.Department of Computer Science, Enugu State University of Science and Technology.
*Corresponding Author Email: chukwuma.udeh@esut.edu.ng
3,4.Department of Electrical Electronics Engineering, Enugu State University of Science and Technology, Enugu, Nigeria.
5.Department of Electrical Electronics Engineering, Caritas University, Amorji, Nike, Enugu State, Enugu, Nigeria.
6.African Center of Excellence for Sustainable Power and Energy Development, Department of Renewable Energy, University of Nigeria Nsukka, Enugu, Nigeria.
6.Watling Academy, Milton Keynes, United Kingdom.
7.African Center of Excellence for Sustainable Power and Energy Development, Department of Control and Instrumentation Engineering, University of Nigeria Nsukka, Enugu, Nigeria.

Abstract

Every year, the global power sector losses $80 billion globally due to non-technical losses, and one major contributor to this problem is fraud across the Energy Supply Chain Management System (ESCMS). Related works reviewed has positioned blockchain as a reliable solution to help combat fraud across global ESCMS; however the research gap is that traditional consensus algorithms like Proof of Authority (PoA) fall short of reliability, flexibility and delay in fraud incidence response. To solve this problem, the aim of this paper is fraud incidence response in power sector using optimized consensus blockchain technique. The methodology is experimental. The method of design began with modeling of the ESCMS framework, modeling of improved blockchain using novel dynamic validator algorithms, integration of the with the ESCMS, implementation as software, validation with real-world grid import report data collected from the Enugu State Electricity Distribution Company (EEDC). The results when tested showed that when fraud is carried at the recorded transaction, there is real-time incidence response at the node where is fraud was perpetrated. Comparism of the improved PoA with existing algorithms considering key attributes such as trust, multi validator and real-time incidence response showed that our system competes among the best, nut the most reliable due to its ability for real-time fraud detection.

Keywords: *Fraud, Power Sector, Blockchain, Incidence Response, Multi Validator.*

1. INTRODUCTION

Fraud is an intentional act of deception initiated to achieve unlawful or unfair gain. The International Standards for the Professional Practice of Internal Auditing (ISPPIA, 2026) Define it as "irregularities and unlawful act which is characterized by intentional misrepresentation". In law, fraud is a crime which involves misrepresentation of facts to create deception. Gresoi et al. (2025) opined that this intentional deception not only undermine trust but also violates ethical standards, resulting to financial loses, reputational damages and legal consequences. Despite several efforts to combat fraud, its persistence has continued to affect individual, companies and national economy (Ali et al., 2023). While no sector is exempted for potential fraud, the power sector has continued to suffer massive losses due to fraud. The power

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

sector is an umbrella which encompasses several entities involved for the generation, transmission and distribution of electricity. This sector according to (Nguyen et al., 2025; Osama et al., 2025) is a critical part of every economy and must be sustainable to facilitate rapid growth and development of a nation; however persistent fraud related incidence has continued to undermine the reliability of power system in developing and under developed nations particularly. No doubt there are losses in the power sector, which are inevitable and are grouped into Technical Losses (TL) and Non Technical Losses (NTL). TL are losses are inevitable dissipation of energy from the power lines during transmission and distribution, while the NTL comprises fraud, non-payment, theft and billing irregularities (Carr and Thomson, 2022). The NTL has continued to dominate reason for financial losses in the power sector and has remained a major challenge, with fraud a major contributor (Carr and Thomson, 2022; Smith, 2004). The impact of NTL accounts for over $80 billion per annum globally and affects quality of service (Louw, 2025).

Several approaches have been proposed to help combat NTL. These include temper proof meters (Lampietti et al., 2020), law enforcement (Birseno et al., 2020), privatization, energy theft investigation, forensic auditing (Kumar et al., 2020). However these approaches lack transparency subjected to corruption (Nneka and Chidubem, 2025) and overall has not been able to address fraud particularly.

Recently Blockchain Technology (BCT) has continued to make wave particularly in the financial and other related industry through the utilization cryptographic technology and decentralization (Zarrin et al., 2021). BCT has several benefits such as transparency, privacy, scalability, cost effectiveness, accountability, privacy and integrity (Zarin et al., 2021). While there are several works in literature which have applied BCT to diverse industrial applications, there is considerable lack of research which proposes to address financial related fraud in the power sector using BTC.

BTC is a decentralized technology which contains several block validated through hash cryptographic keys (Hameed et al., 2022). Each of the blocks are transformed into records of hash values which help in fraud detection. For BTC to operate successfully, a good consensus algorithm is required. Popular BTC consensus algorithm include Proof of Work (PoW), proof of authority, proof of elapsed time, proof of search, Proof of Activity (PoA), proof of capacity, and proof of authentication (Hameed et al., 2022). Among these algorithms PoA is a popular algorithm developed as an improved version of PoW (Miglani et al., 2020). It is suitable for an enclosed system which requires an administrator (Zarrin et al., 2021).

However Hameed et al. (2022) revealed that PoA suffers some drawbacks which include centralized risk, high transactional overload, fixed validator and lack adaptivity. In addition, the integration of PoA for fraud detection suffers delay in fraud detection, which is a problem as the culprit must have escaped before fraud is detected. The reason is due to its dependence on the analysis of hash key considering different peers or previous blocks to detect fraud which can be time consuming; hence there is need for an improved PoA which is flexible, optimized validator, real time fraud detection capability and incidence response capability. This when integrated in the power sector will drastically reduce NTL and also provide instant alert and response when fraud is carried out. To this end, the contributions of this paper are as follows;

i. Novel dynamic validator algorithm for optimized trust in PoA.
ii. Real-time fraud alert algorithm to facilitate rapid incidence response during fraud.
iii. Apply improved blockchain solution for fraud management in Nigerian power sector.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

iv. Practically test the improved blockchain with real data from the Nigerian Power Distribution Company, and qualitatively compare performance with existing consensus algorithms

2. LITERATURE REVIEW

Related works on the application of BTC for fraud detection were discussed in this section. Ashfaq et al. (2022) Combine BTC and machine learning algorithms for fraud detection. Extreme gradient boasted algorithm and random forest were trained with bitcoin dataset for the classification of transactions, while the BTC was integrated to detect fraud, however it was not clear the consensus algorithm used for the study. Badis et al. (2022) applied BTC for fake check detection. PoW was used as the consensus algorithm which validated transaction and help detect fake check in banks. However PoW suffers high computation delay, huge power consumption and lack flexibility. David et al. (2018) Revealed several areas which include grid transmission, peer to peer transactions, and energy financing as for the application of BTC in power sector. Chris (2023) applied BTC for fraud detection in cloud environment. This was achieved using smart contracts developed with rule based approach and Ethereum, while Dong et al. (2025) applied BTC for peer to peer energy trading system. Game theory was proposed for dynamic pricing and then simulation examples were applied to validate the model. While these works have successfully applied BTC in different application for fraud detection, there is gap such as limited practical test of BTC in these applications; secondly there is limited focus on the consensus algorithms used for the BTC, which is key to facilitate real-time fraud detection, incidence response and transparency. PoA for instance despite low cost, low energy consumption suffers has fixed validator, lack incidence response and also dependent hash key analysis for fraud detection. There is need for a model which provides real-time fraud alert, dynamic validator which is based on reputation and reliability. The study focus is the power distribution company in Nigeria.

Rizal and Kim (2025) developed a thorough survey of the aspects of AI and ML implementation in blockchain consensus mechanisms and how the novel technologies are able to optimise the performance and safety of blockchain as well as create new issues. A broad spectrum of ML methods such as deep learning, reinforcement learning, and clustering as applied to consensus processes in the study was reviewed and noted to contribute to enhancing effectiveness, reliability, and adaptability in blockchain systems. Some of the key findings were that AI can optimise transaction validation, decrease the latency, and enhance scalability, yet there were risks, like centralization of data, the excessive computational load and the susceptibility to adversarial attacks. To address these problems, the authors mentioned such strategies as federated learning to maintain privacy, Secure Multi-Party Computation (SMPC) to safeguard sensitive information, and decentralised AI marketplaces to maintain equitable distribution of resources. The findings highlighted the dualism of AI in blockchain: on the one hand, it has the potential to become an incredibly efficient and versatile solution and enhancement, but on the other hand, it has to be balanced cautiously to preserve decentralisation and trust.

To ascertain the appropriateness of various blockchain consensus mechanisms to various blockchain applications, Fahim et al., (2023) did a comparative study of four mainstream blockchain consensus algorithms, including PoW, PoS, PoA and PoV. The study design was composed of a literature based comparative analysis, in terms of metrics of security, energy efficiency, scalability and IoT compatibility. The findings revealed that PoW provides very

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

high security through its HashCash and micro-mint methods but suffers from poor energy efficiency and scalability, though improvements like Green-PoW could reduce energy consumption by 50%. PoS was also more energy efficient and scalable than PoW, but it has lower security against pool mining, yet is more resistant to double-spending attacks. PoA was discovered to be secure and stable than PoS, with greater throughput and efficiency, whereas its reputation based model, which is centralised, restricts decentralisation. PoV was more scalable and created blocks faster than PoW and used less energy, although with mediocre security integrity. Altogether, the paper has highlighted that every consensus algorithm possesses specific advantages and disadvantages, and their suitability varies in terms of the needs of blockchain networks, particularly in the randomly used scenario such as the IoT, where energy-efficiency and scalability are the key factors.

Ankarberg and Juvencius (2021) conducted a bachelor thesis at KTH, which was dedicated to the implementation and comparison of two PoA consensus algorithms on IIoT equipment. The necessity to decentralise the operations of IoT data management that is traditionally based on centralised bodies and forms a single point of failure inspired the study. The two algorithms have been experimented on a CloudRail IIoT device, though there were severe hardware constraints which impacted on the performance. The algorithm 1 was much faster and more feasible in IIoT networks, and its execution time became seconds, although its security was compromised because of small encryption keys because of the limitations of the device. However, Algorithm 2 was too slow in practise with a maximum of 56 minutes needed to execute simple tasks, and thus was not suitable in real-time IIoT applications. Such risks as compromised trusted nodes, false data injection, and ElGamal encryption (Algorithm 1) or storage of keys (Algorithm 2) vulnerability were mentioned by the authors. They also highlighted the ecological and ethical significance of lightweight consensus mechanisms in order to lower the energy usage. Conclusively, the research found that Algorithm 1 could be the possible candidate of IIoT consensus, and the responsiveness of Algorithm 2 was not good enough, which did not make it a candidate in the current application environment. It was advised that future work would be to test the two algorithms on more capable IIoT devices with secure key lengths and updated programming environments.

Wang et al., (2020) provided a comparative analysis of blockchain consensus algorithms, in the case of PoW, PoS, DPoS, and PBFT. It was found in the paper that they are examined in terms of their inner mechanisms, benefits, and shortcomings in different dimensions, including resource consumption, decentralisation, throughput and time of transaction confirmation. PoW has been noted to be extremely decentralised and secure but lacked in scalability, high confirmation times and high levels of hardware and energy waste. PoS enhanced efficiency and decentralisation of energy but it had problems such as intricate implementation, vulnerabilities to security, and prone to nothing-at-stake attacks.

DPoS was also highly performing, scalable, and efficient since the number of validating nodes was minimised at the expense of centralization risks and the chances of collusion, as observed in EOS bribery scandals. High throughput, finality and security in permissioned environments were touted as well but PBFT was hamstrained by lack of scalability, fixed node requirements and low fault tolerance (tolerance to a third of malicious nodes only).

It was concluded by the study that hybrid consensus mechanisms like PoW + PoS or PoW + PCFT are new promising methods as they bring together the advantages of other protocols in order to achieve a balance between efficiency, scale and security.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

Darwish et al., (2020) reviewed the blockchain consensus algorithms in a Shariah perspective with a focus to consider the value of analysing the applications of cryptocurrencies, and the underlying blockchain platforms through evaluation. The paper compared PoW, PoS, DPoS, PBFT, Stellar Consensus Protocol (SCP), and Ripple consensus mechanisms with the Shariah regulations against interest (riba), uncertainty (gharar), and gambling (maisir).

The findings indicated that PoW and SCP are not Shariah compliant: PoW has uncertainty and gambling in its rewarding mechanism whereas SCP has uncertainty in its vote-based rewarding mechanisms. PoS, DPoS, PBFT, and Ripple, on the contrary, were considered compiant, since they do not facilitate these forbidden financial practises.

The result indicated that permissionless algorithms such as PoW are scalable, but they tend to contradict the Shariah principles, unlike permissioned algorithms, including PBFT, which are much more throughput and compliant but adversely affect decentralisation. The authors made a conclusion that to design Shariah-compliant blockchain platforms, it is necessary to have consensus mechanisms that provide the balance between efficiency, scalability, and Islamic financial ethics.

The methodology used by Zhebka et al., (2024) to select the most suitable consensus algorithm in blockchain technology has four very important criteria such as energy consumption, decentralisation, security, and bandwidth. Their research pointed out that blockchain systems unlike the traditional databases are dependent on distributed nodes in order to achieve immutability and trust, and therefore the decision on the consensus mechanism is core to efficiency and resilience.

The methodology involved analysing how each algorithm balances resource efficiency with decentralization, how well it resists attacks (including Sybil and 51% attacks), and its ability to scale transaction throughput without compromising security. Notably, these criteria were modelled by the authors as Python-based programme that can be used in the decision-making process and enables developers and organisations to choose consensus algorithms specific to particular uses, be it financial transactions, digital identity, logistics, or asset tokenization. What was emphasised was that blockchain systems are secure, efficient, and adaptable since combining a variety of criteria instead of using one factor results in more accurate and context-sensitive consensus selection.

The map of blockchain consensus algorithm development and sustainability is conducted with the help of systematic literature review by Pineda et al., (2024) as well. Their study included a tedious process of searching and filtering thousands of articles published in the 2020-2024 period, the consensus mechanisms were PoW, PoS, DPoS, PoA and hybrid PoW/PoS. The paper highlighted the environmental cost of these algorithms, especially the huge power usage and carbon emissions of PoW which were up to 707.6kWh and 380,000g of CO2 per transaction. By contrast, PoS, DPoS and PoA were much more sustainable with under 0.002 kWh per transaction in consumption and with a non-negligible amount of emissions.

The results have revealed that PoW is securest but least sustainable and PoS and its variations have a compromise of scalability, efficiency, and environmental friendliness. Hybrid models offered compromises in-between losing energy use than PoW and still less efficient than PoS. Generally, the review determined that sustainable consensus algorithms are the key to the future of blockchain, and scalability, decentralisation, and sustainability must be optimised to make blockchain popular and climate-friendly. Table 2.2 summarized the literatures.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

3. METHODOLOGY

The methodology of this study began with the modeling of the existing Energy Supply Chain Management System (ESCMS), followed by the integration of the BTC model to form the benchmark ESCMS.

An improved PoA was proposed and the algorithm developed; in addition, incidence response algorithm was also developed and integrated with the proposed PoA and then applies to the benchmark ESCMS as an improved system.

Data was collected from Enugu Electricity Distribution Company (EEDC), audit department and then apply to test both models and their performance compared and findings discussed as shown in the flow chart of figure 1.

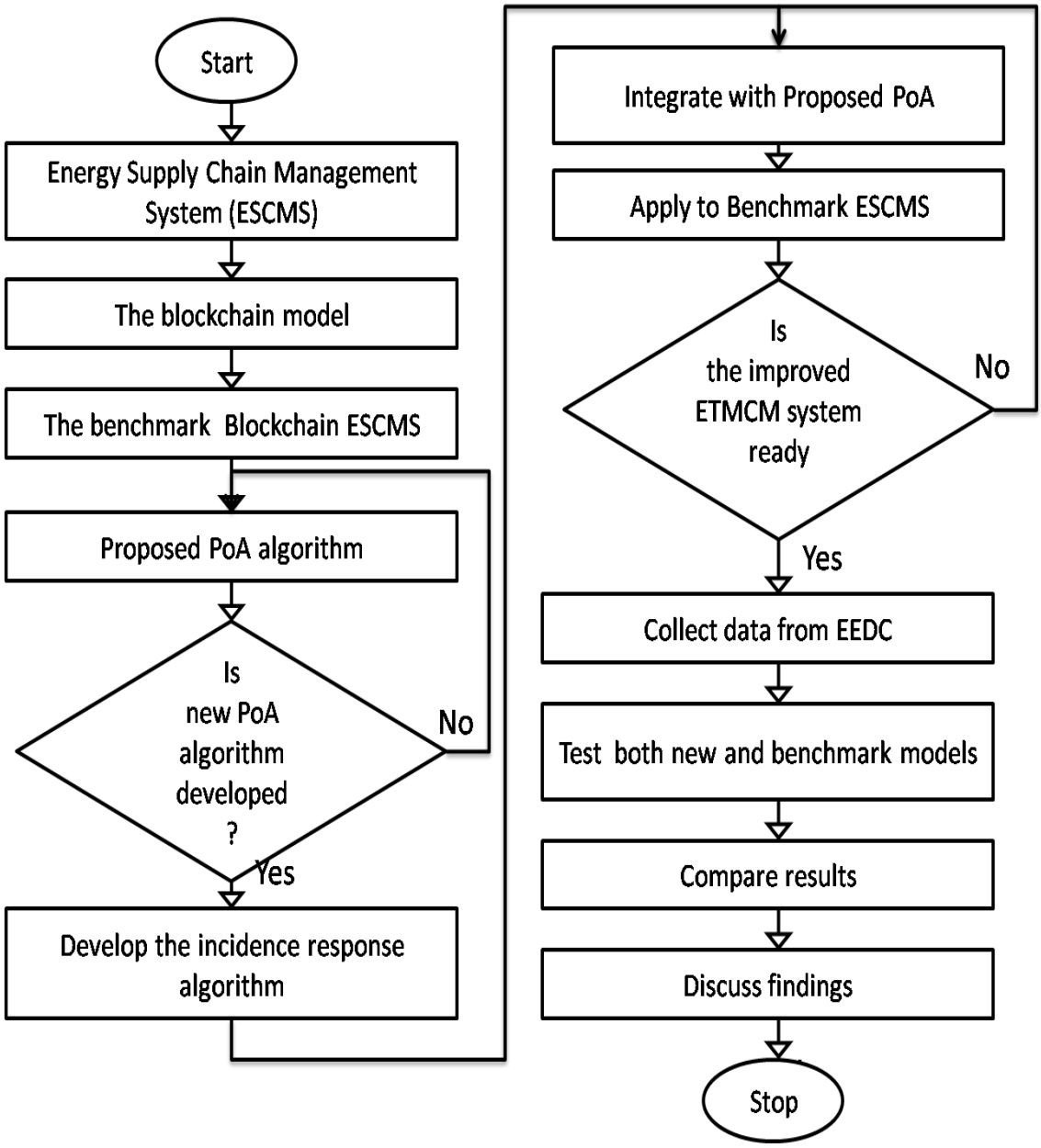

Figure 1: Flow chart of the research methodology

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

3.1 Energy Supply Chain Management System (ESCMS) for Distribution Company

The ESCMS for Distribution Company is made of several components which are the distribution company branch, injection station, monitoring section, marketing, billing and revenue as shown in the block diagram of figure 2.

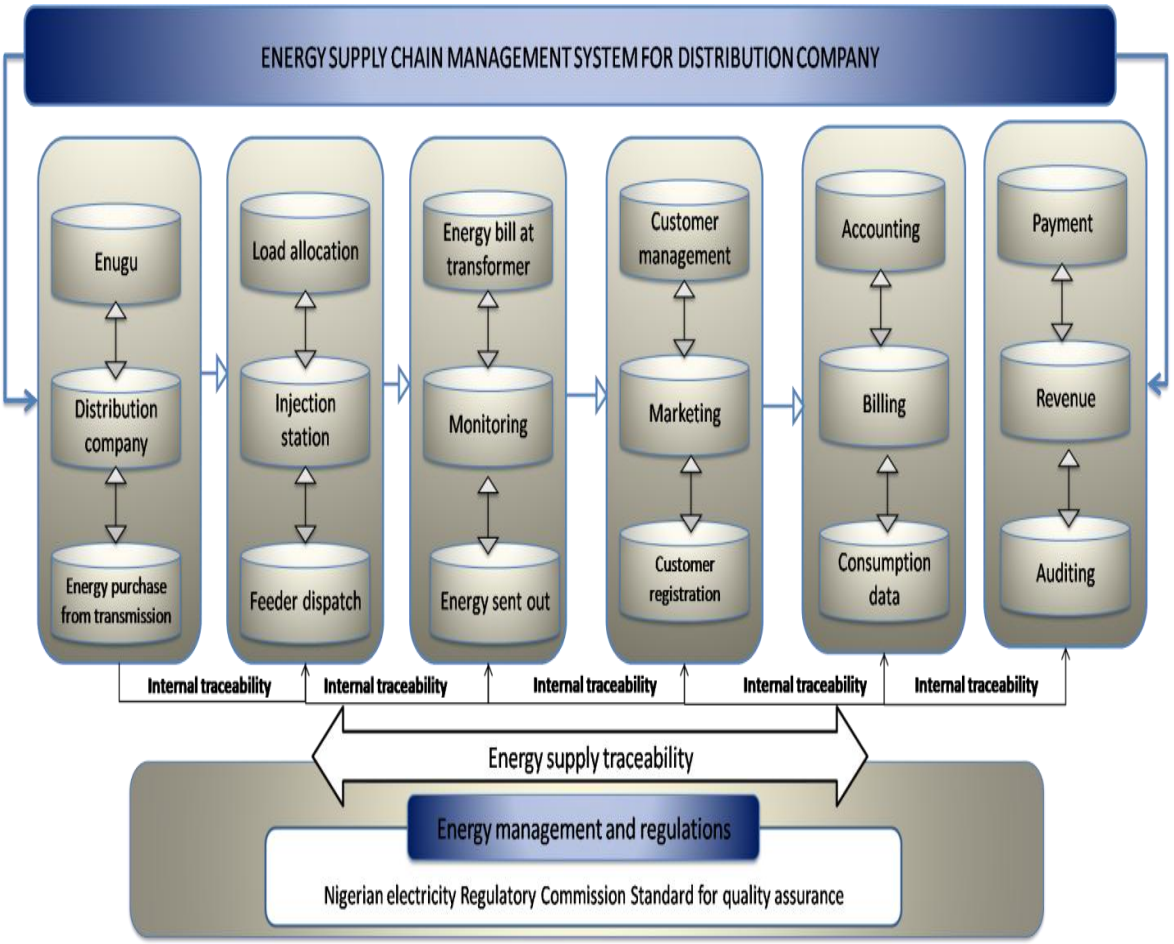

Figure 2: Block diagram of the ESCMS

Figure 2 presents the ESCMS block diagram staring with the distribution company located at Enugu Nigeria, who purchased the energy from the transmission company of Nigeria. The energy purchased are allocated to an injected sub-station through the feeder dispatch. The monitoring section supervises the energy sent out to different distribution transformers and the cost in Naira.

Marketing section takes care of customer management such as user registration, request for metering and fault recording and overall customer service. The account section calculates customer data (energy used) and then bill the user.

Finally is the revenue generation section which collected and supervises payment from customers and then record at the auditing department. Each step of this process over the years has experienced several fraud related cases which has resulted to huge financial loss to the distribution company. This paper proposes an improved blockchain solution to address the problem.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

3.2 The Benchmark blockchain model with traditional PoA consensus

Blockchain is a decentralized ledger technology made of n blocks and timestamp as shown in figure 3. Each block is connected to a previous block through hash keys (Al-Rakhami and Al-Mashari, 2021). The nonce is a unique transaction block number. Different entities can create smart contracts without intervention and the data is difficult to alter after it has been validated.

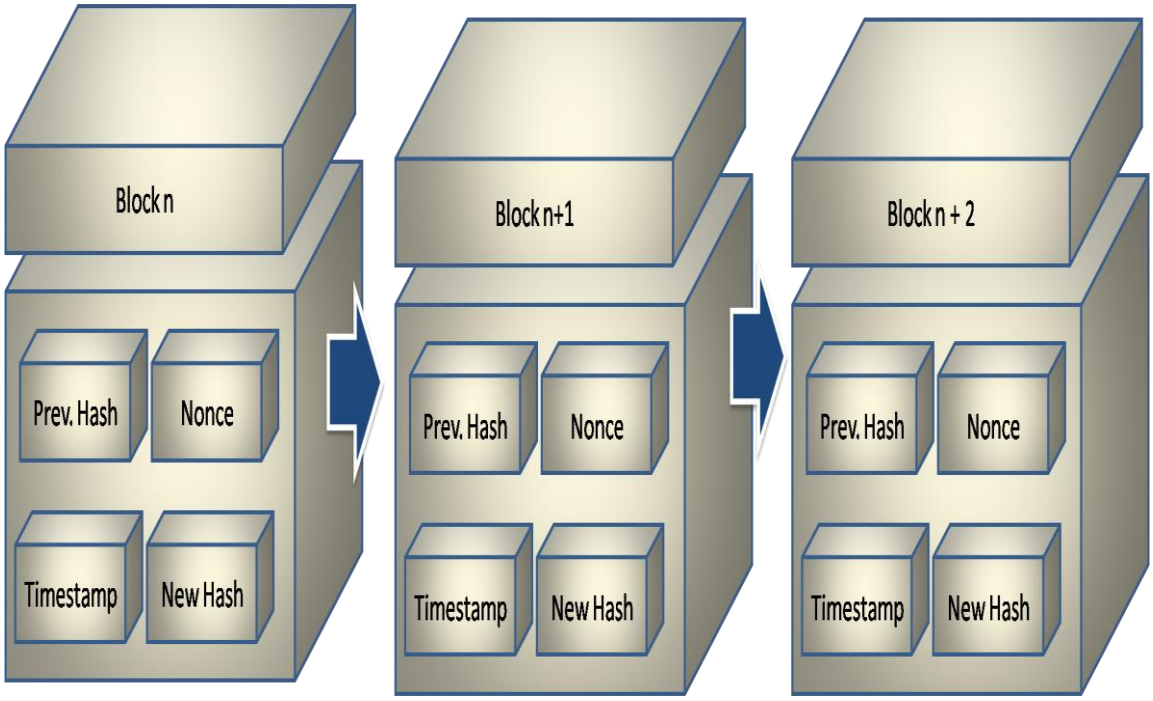

Figure 3: Blockchain diagram

The block in figure 3 operated with PoA as the consensus algorithm. This PoA ensures the transactions are validated while the smart contacts are rules of codes which executes with the activities of users. When data are stored, the hash values are automatically generated and have a link to the next block.

Altering the data changes the hash values while the smart contract detects and then triggers action for fraud detection. While this blockchain can secure data of power distribution system transaction, some weakness such as fixed validator, low scalability, and difficulty in fraud detection are some of the weakness which need addressing to make the system very reliable. In addition, this PoA is not suitable for application in an institution characterized with insider threat, since validators are pre-defined.

Pooja and Ashok (2020) added that validators can collaborate and manipulate the system, which is the case for power sectors, particularly in under developing and developing nations, which has left the sector very unproductive, despite huge investment pumped into the sector.

To solve this problem, this paper proposed a dynamic PoA system where validators are dynamically assigned based on reputation and also a real time incidence response to facilitate real-time fraud detection and management. Figure 4 presents the flowchart of the traditional PoA.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

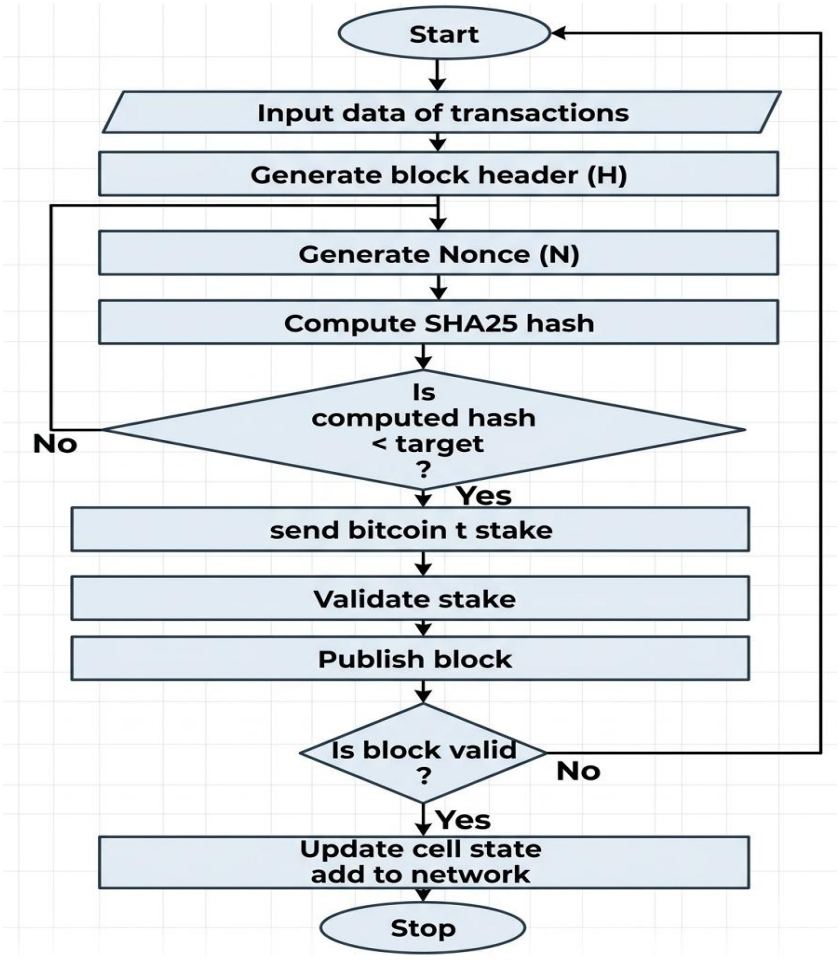

Figure 4: Flowchart of traditional PoA

Figure 4 presents the flow chart of the traditional POA which showed the operational workflow of the blockchain transaction validation and block generation process for secured data within the distributed network. The flow chart began with input of records to be protected. This header bock of the records are generated containing information like hash functions, timestamps and transaction ID. The nonce which is a random number to guide the mining process is generated. Encryption has function is then generated with the SHA-256 cryptographic technique using the nonce and block header. This hash is then compared with predefined target values for validation and then sends to bitcoin state. This stake is then verified to confirm legitimacy before the block is published to the distributed blockchain network. Upon publication, validation is performed on the block and then updated to the new ledger.

3.3 The Dynamic PoA Consensus Model

This paper introduced new PoA with dynamic validator and real-time alert for fraud.

3.3.1 The dynamic validator model

The validators are intelligently selected based on trusts, integrity, accountability and reliability. These criteria are measured using reputation score. The PoA operated with K number of validators, which is very good unlike the traditional system which has fixed validators and not flexible. Among the validators, the top 5 are selected to validate transactions. In every epoch, a reputation engine computes individual reputation score for v_i candidate

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

considering availability (A) as a measure for reliability score, quality index of block (Q), downtime (D) which is the penalty for misbehavior and trust index score (T). The Global Reputation Score (GRS) is at time (t) is computed as equation 3.1;

$$GRS_i(t) = a_i A_i(t) + a_2 Q_i(t) + a_3 D_i(t) - a_4 T_i(t) \quad 3.1$$

Where $A \in [0,1]; Q \in [0,1]; D \in [0,1]; and\ T \in [0,1]$; a is the weight such that $\sum_{j=1}^{4} a_j = 1$. In this work we assumed 0.4 as the threshold for validator disqualification (θ) and 0.5 as the initial validator score for all candidates. The set $V(t)$where validators are selected t epoch t, and K as the number of validator is defined as equation 3.2 which represents the selected validator and then equation 3.3 the rejected validators.

$$V_{select}(t) = TopK\ (\{GRS_i(t) | i \in V\ (t)\}) \quad 3.2$$

$$V_{reject}(t) = \{i \in V(t) | GRS_i(t) < \theta\} \quad 3.3$$

For validator involved with events such as misbehaver, downtime received penalty. The severity misbehavior weight is indicated as β_k for k validator, while $m_k \in \{0, 1\}$ indicates presence of type k-misbehavior. Following this action, the equation 3.1 updated at epoch (t) as equation 3.4;

$$GRS_i(t+1) = \varphi . GRS_i(t) + (1 - \varphi) . New\ GRS_i(t) \quad 3.4$$

Where $\varphi \in [0,1]$ is the memory coefficient to smooth change and the updated validator score is the $New\ GRS_i(t)$

3.3.2 Real-time for fraud detection

The real-time alert is introduced to combat issues of delay in fraud detection observed in the traditional PoA. The system upon fraud detection, immediately notify every subsequent block of the fraud event. The process began with the identification of the block information such as the peer, reputation score, block name and keys. The validator of the block are recorded and internally stored, upon changes in the block, which is detected through variation of hash keys after, a real-time flag on the block from the local storage is enables and then alert is broadcasted for all subsequent block. The combination of the dynamic validator algorithm and real-time alert fraud algorithm depicts the dynamic PoA flow chart in figure 5, while the use case diagram is presented in figure 6 with four actors which are the users, validator, fraudster and peer nodes. Figure 6 presents the use case diagram of the improved blockchain based ESCMS. The user actor loads the data of ESCMS information at different blocks, the improved PoA computer the validator with algorithm 2. Keys are generated and the data stored. When fraudster attempt to manipulate the data, subsequent block in peer nodes are alerted using algorithm 1.

Algorithm 1: The real-time alert system	
1.	Start
2.	Initialize block information [block ID, peer, reputation, blockchain]
3.	Validate block integrity
4.	If not is valid block
5.	Print “Alert sign”
6.	Record incidence information

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

7.	Identify block information
8.	Broadcast alert response to peers
9.	Flag block for local storage
10.	Update chain [block]
11.	Else
12.	Return True
13.	End

Algorithm 2: The dynamic validator system

1.	Start
2.	Parameter initialization $(a_i, a_2, a_3 = 0.3)$
3.	$\theta = 0.4, K = 10$ [Number of validators]
4.	Set epoch transition [validator, epoch_logs]
5.	Compute reputation scores with equation 3.1
6.	Select top validator with equation 3.2
7.	Reject poor validator with equation 3.3
8.	Update reputation log with equation 3.4
9.	Def-consensus round [validator, current block)
10.	Vote block [choose best K]
11.	If top 5 k are selected
12.	Finalize block
13.	Else
14.	Penalize
15.	End

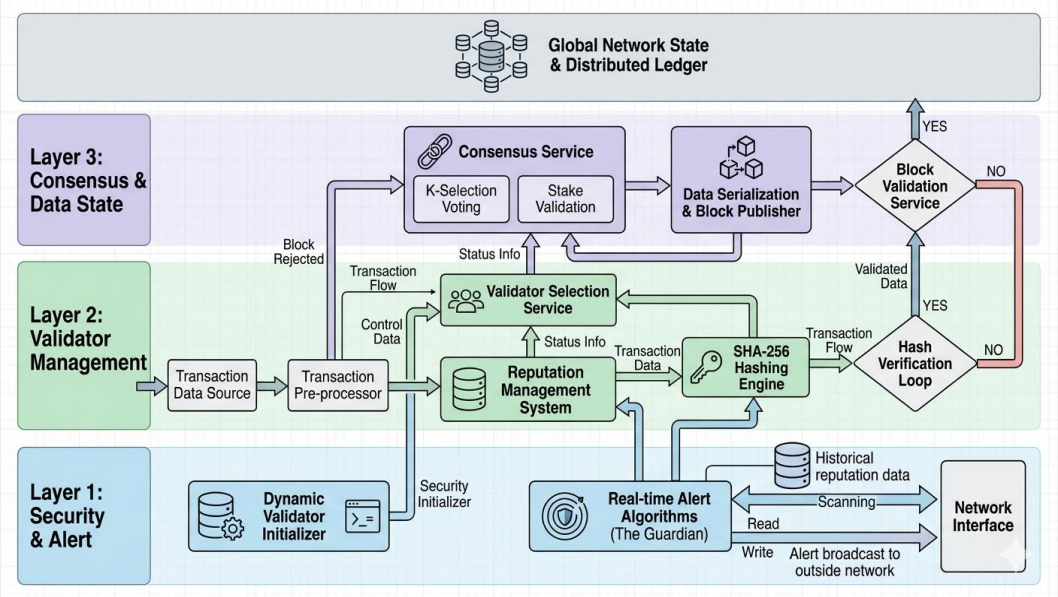

Figure 5: Flowchart of the dynamic PoA

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

The figure 5 presents the multi layered dynamic PoA to secure the decentralized transactions through validator section and data management. The flow chart began with the initialization of the dynamic validator in algorithm 1. This setup the network also continues monitoring function with the real-time alert module in algorithm 2. The two algorithms make up the security and alert layer. When the transactions records are enter in the validator management layer, they are pre-processed into the reputation management system which computed the score to guide validator selection service in selecting the trust worthy network participants. Simultaneously, the transactions are passed through the SHA-256 Hash engine for cryptographic encryption before decision point with hash verification loop to reproduces transaction not validated. At the consensus and data state layer, this combines the k-selection voting mechanism with stake validation among chosen validators to reach agreement, in serialization with the data bock publisher. Prio to final acceptance, the new block must clear a final block validation service decision, while those not validated are rejected and looped back into the validator system to select new network actors and pass the final check before officially added to update the immutable distributed layer.

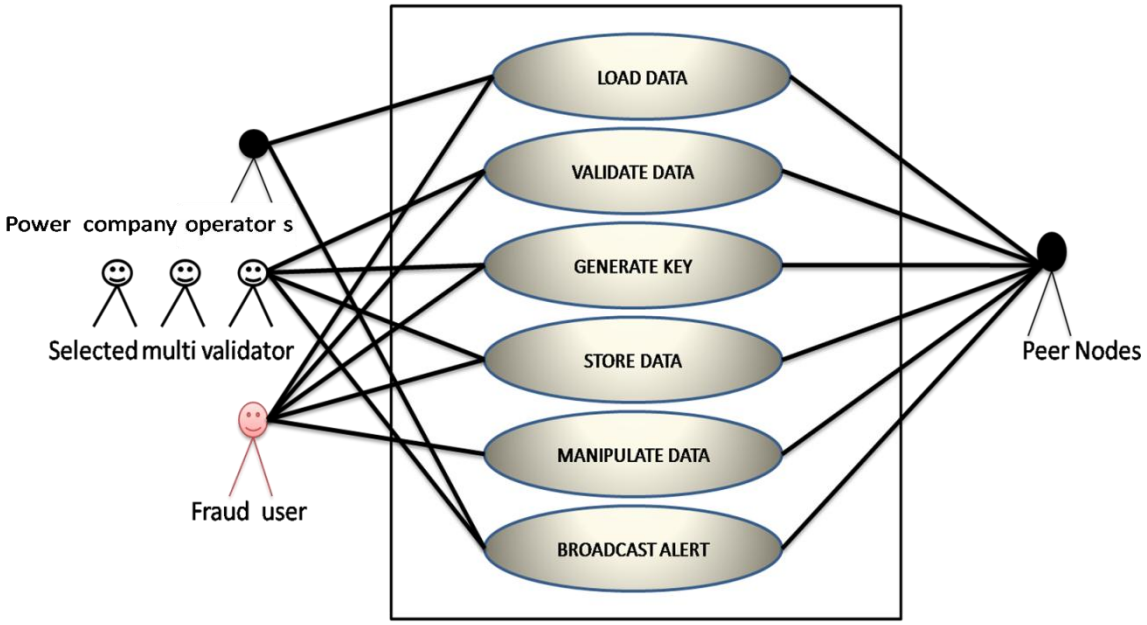

Figure 6: Use case diagram of the system for fraud detection

The use case diagram in figure 6 has the normal users, fraud users and selected multi-validator as the main actor while the peer nodes are the supporting actor. The normal users which are the operators of power transaction load data which contains records of power. The data are validated by the multi validators, and then encrypted with the SHA-256 algorithm. The information are stored and broadcasted to the peer nodes. When manipulated by the fraud users, the real-time incidence response alert at the particular nodes where the fraud is committed for immediate control.

3.2.3 System Implementation

The system implementation of the benchmark block chain model was done with demo blockchain software, while the new blockchain in ESCMS was done with react programming language. The reason for the two choice of programming was because demo blockchain lack features to test the dynamic PoA presented for improved ESCMS management.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

3.2.4 Data collection to test the implemented system

The data used for this work was collected from the Enugu Electricity Distribution Company (EEDC), of Nigeria. The data used is the EEDC monthly grid energy meter reading import report for the month of March, 2025. The total energy purchased by EEDC in the month of March is 245,978.12MWH, feed across18 districts 33/11kV injection feeders all around south east Nigeria. This work considered the Ogui district import data to test the softwares. In the month of March, a total of 23,672.26MWH of energy was imported to the Ogui injection substation. The readings considering the different supply chain such as during importation, size and capacity, 33/11KV injection feeder, monitoring section, marketing section, billion unit and revenue department information were all extracted and used to test the model.

4. RESULTS AND DISCUSSIONS

This section presents the results of the new and traditional blockchain model with ESCMS. The results were reported considering transaction validation, integrity test and fraud detection capabilities. Figure 7 present the results of single block creation in ledger of peer A and peer B.

The Figure 7 presents the result of ledger which are decentralized nodes which continued the created block. The result showed the creation of the distribution company block. From the observation, it was noticed that the hash key from the two blocks are similar, which is an indication that the validated data from each node has not been manipulated. This process results to the desired transparency, and confidentiality which is a good attribute of the traditional PoA. Figure 8 presents the blockchain creation of the ESCMS with traditional blockchain in peer A and Peer B, considering the first three blocks which are Distribution Company, Ogui injection station and monitoring unit.

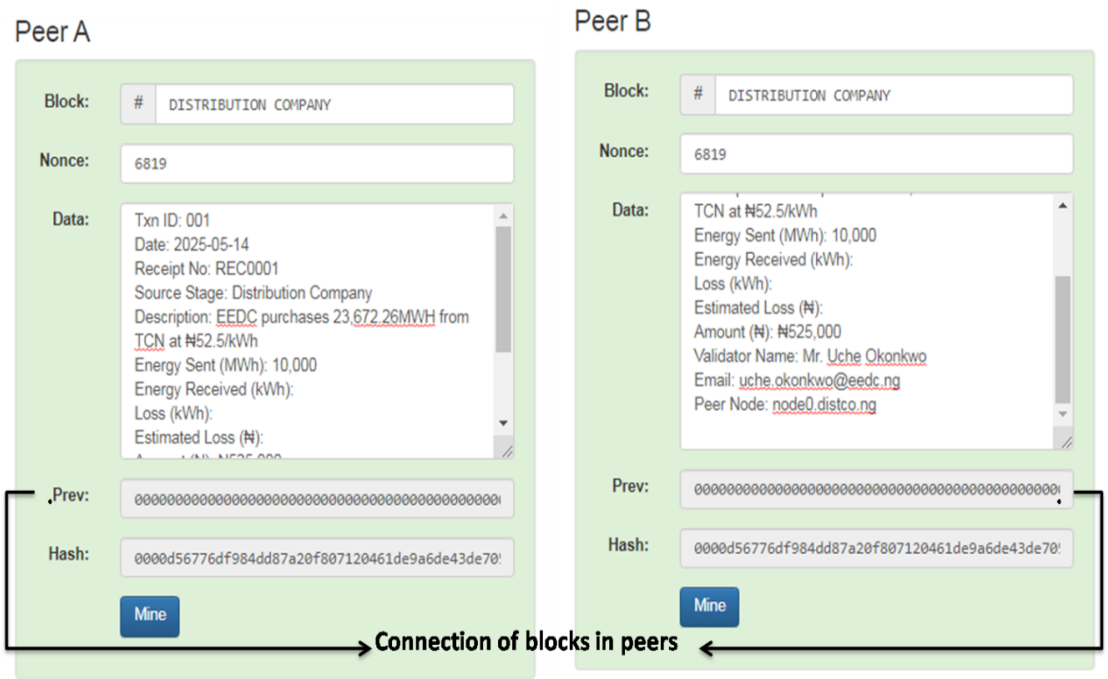

Figure 7: Result of block creation in ledger of Peer A and Peer B

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

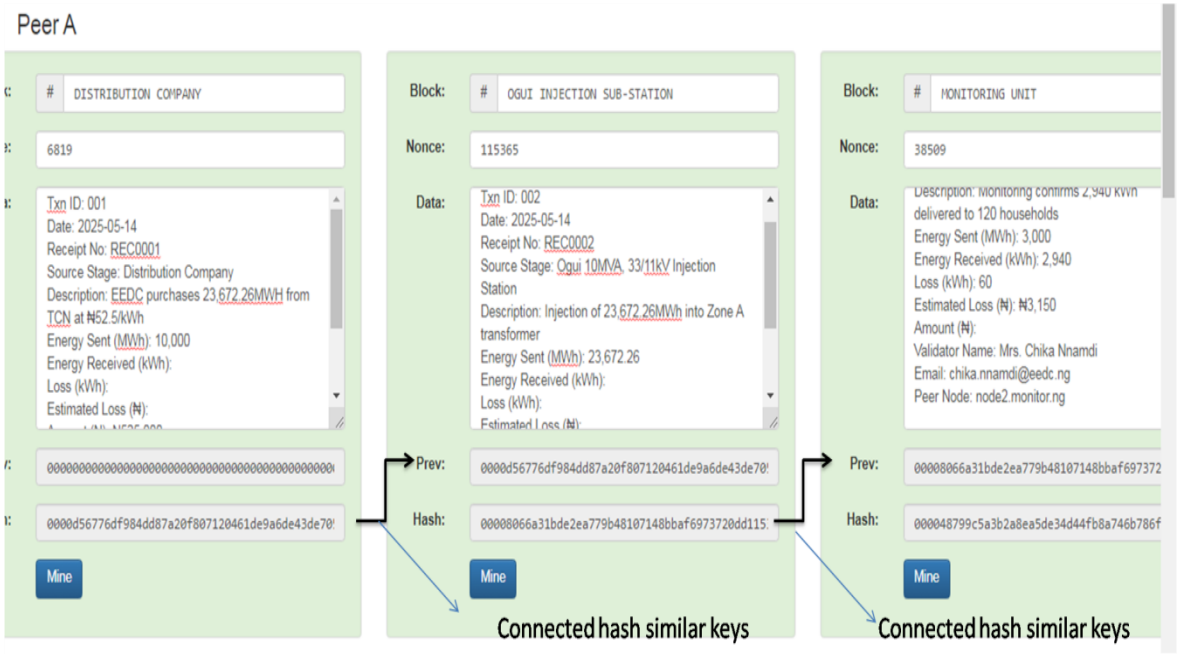

Figure 8: ESCMS with traditional blockchain model

Figure 8 showed that the hash key was used to connected the blockchain. i.e new hash keys in distribution company block forms the previous has key in the injection substation block, and the new hash key in the injection substation block forms the previous hash key in the monitoring unit block and vice versa. What this mean is that each of the block are connected as a chain when validated. This connection is necessary and ensures that once fraud is committed by manipulating the data subsequent block are alerted as shown in figure 9, where the Ogui injection substation block is manipulated by changing the capacity of energy sent from 23,672.26MWH to 20,672.26MWH.

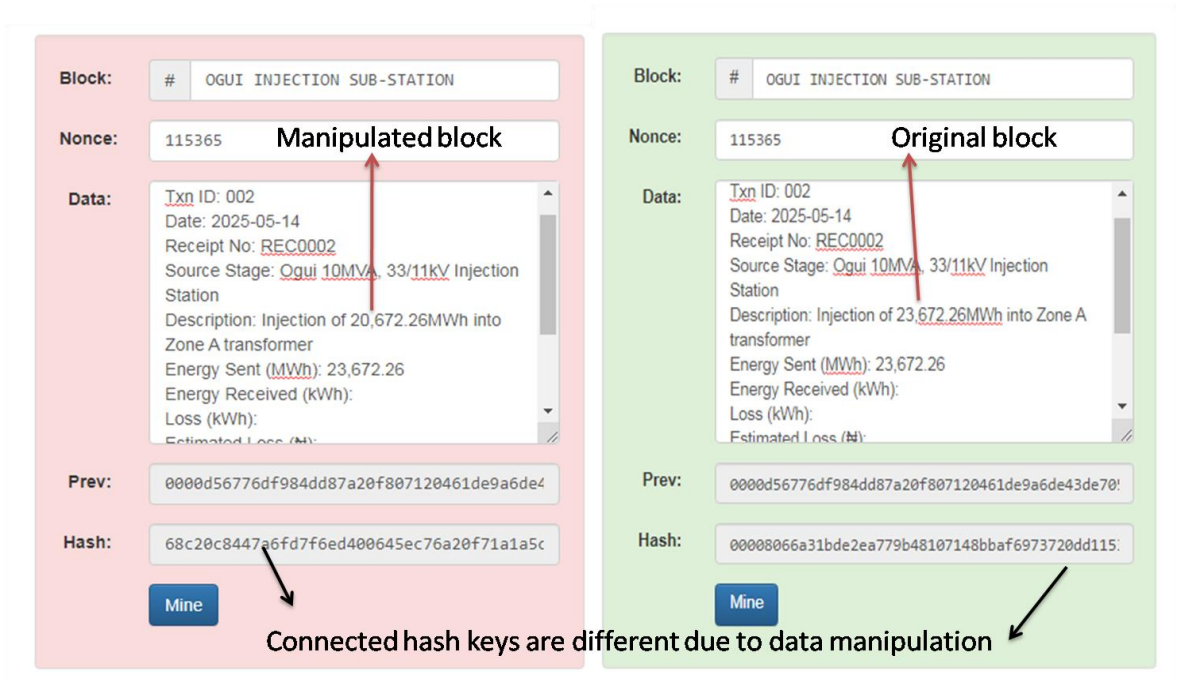

Figure 9: Integrity test of the traditional blockchain for ESCMS

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

Figure 9 presents the integrity test of the model with the Ogui injection substation block manipulated. It was observed that the block immediately changed to red background color which implied data manipulation. This is very good as it enhances trust; sustain transparency and immediate fraud alert. However, the weakness of the traditional block chain is that because the validators are fixed, they can collaborate and hide the fraud. The collaboration results to the re-mining of subsequent block as shown in the figure 10, which produced the normal ESCMS background, even though size of energy sent has been manipulated.

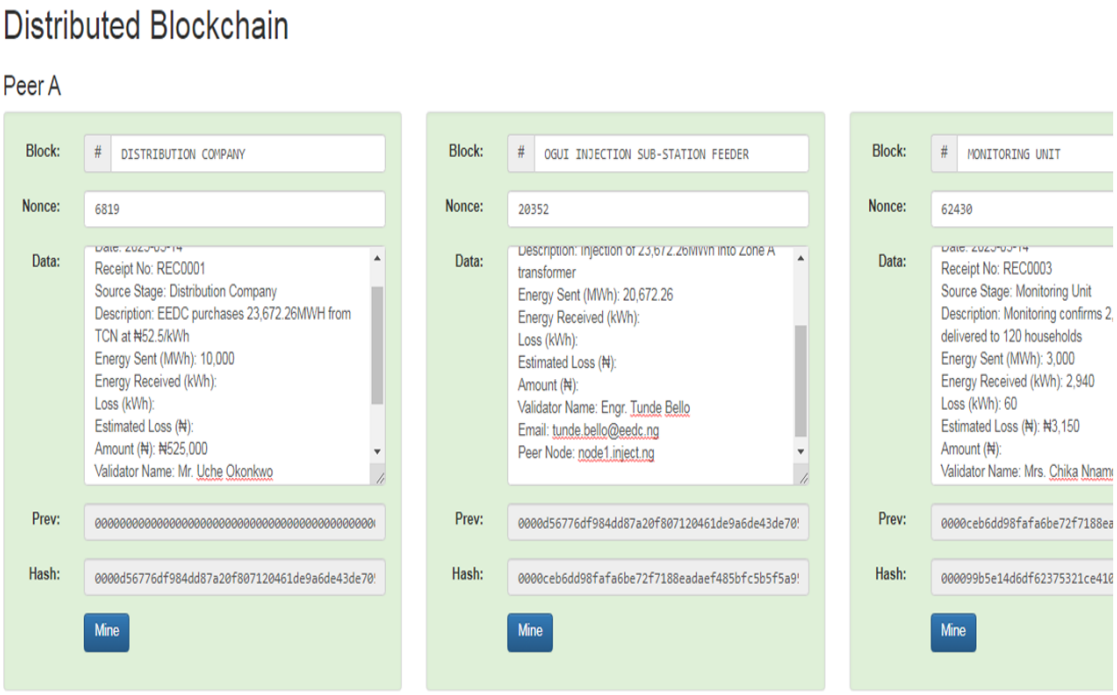

Figure 10: Result of the ESCMS with traditional blockchain when data is manipulated and hidden

Figure 10 results is a proof that fraud can be hidden in the traditional blockchain model. This is possible because validators collaborated and hide the fraud in each block. The reason was because validators are fixed and pre-defined, which a very big risk is. Secondly, it was observed that detection no fraud is dependent on critical analysis and comparism of hash keys, which can e time consuming and delay in fraud detection. These problem motivated the new blockchain where dynamic PoA in algorithm 2 and the real-time alert response in algorithm 1 combined to upgrade the PoA as shown in the figure 5 was used to improve security, transparency and real-time fraud detection in the ESCMS.

Figure 11 presents the result of the ESCMS blockchain creations with the six different block as originally modelled in figure 2. From the result of figure 10, it was observed that the size blocks were created with several validators. Unlike the traditional blockchain with PoA, which has fixed blocks, the new blockchain used equation 3.1 to compute the reputation score of all K validators and then apply equation 3.2 to select those with high reputation score while applying equation 3.3 to reject those which are not trusted during the transaction process. The top validators with best scores are selected to approve transactions. From the new ESCMS blockchain created, it was observed that each block were connected with a previous has key, which is very good and indicated interconnectivity between blocks. Figure 12 presents integrity test of the ESCMS. This was done by manipulating the size of energy sent to the Ogui Injection

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

sub-station, while figure 12 also tested the model integrity by manipulating data at the monitoring unit section.

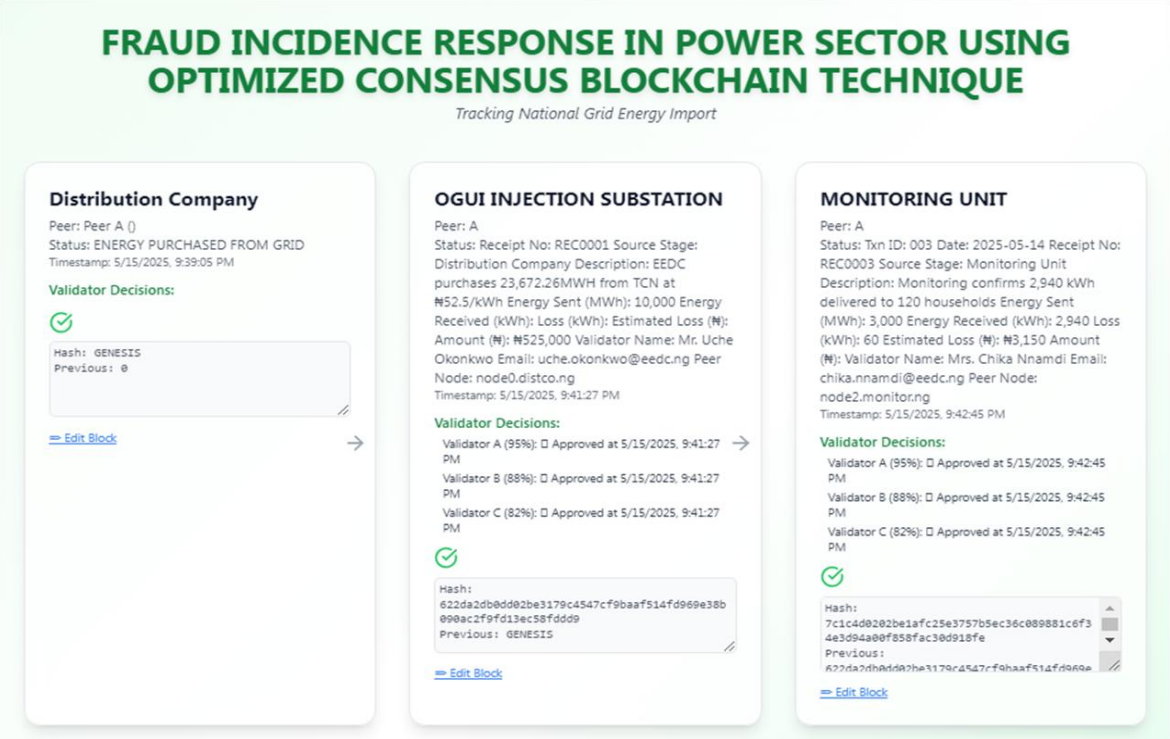

Figure 11: Blockchain creation of the ESCMS with the dynamic PoA integrated as new Blockchain

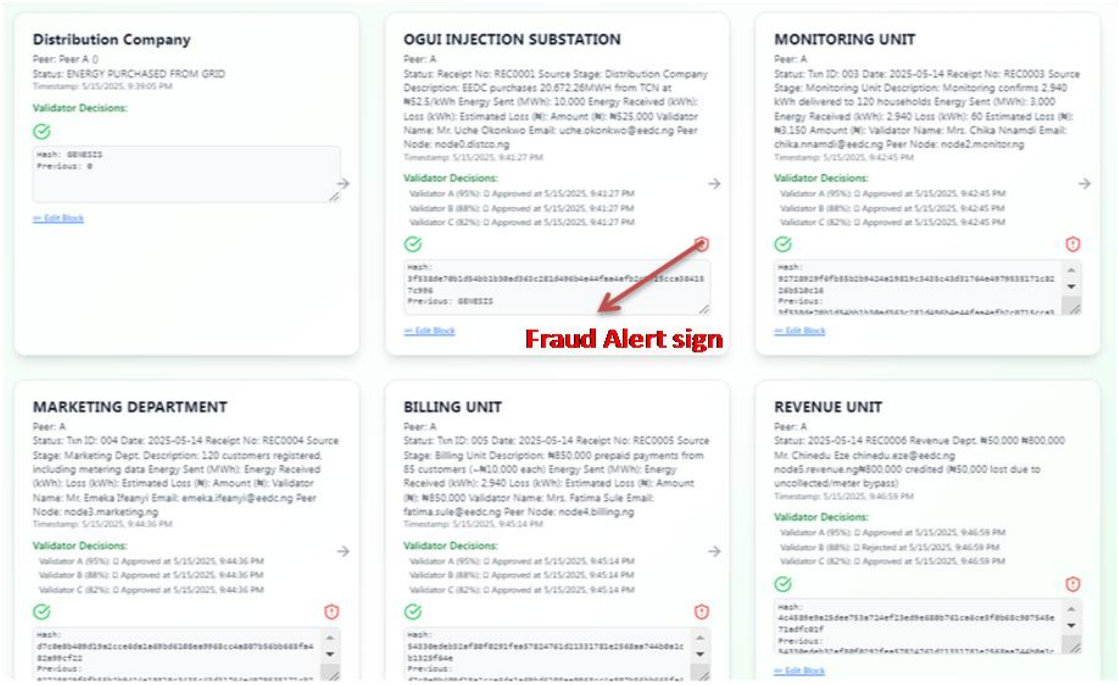

Figure 12: Integrity test of the new Blockchain for ESCMS

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

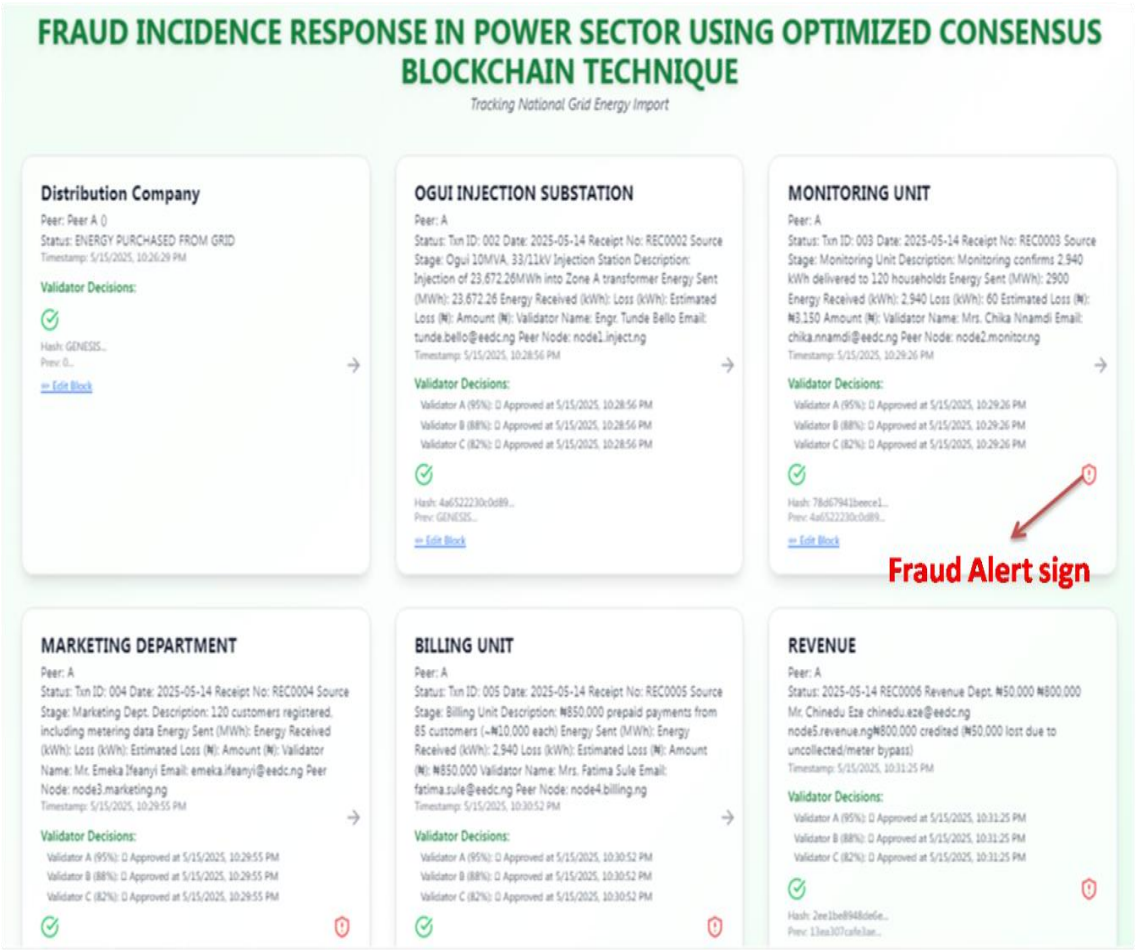

Figure 13: Integrity test by manipulating the Monitoring unit of the ESCMS

In figure 12, the Ogui injection sub-station block was manipulated and it was observed that that all the sub-sequent block were immediately alerted of the fraud. The results also showed that after fraud was committed and re-mined to hide the fraud, all affected block were signaled with permanent fraud alert sign, which facilitates instant incidence response. The advantage of this model against the traditional blockchain is that fraud cannot be hidden; validators are reliable which limits potential fraud. In figure 13, another test was carried out by manipulating the monitoring unit section, through data alteration. The results showed that all subsequent block were alert of the fraud. This alert sign facilitated incident response which will lead to immediate investigation and apprehension of the culprit. Subsequently, the dynamic PoA was compared with other consensus algorithm as reported in table 1.

Table 1: Comparative analysis of consensus algorithms

Source	(Bhuvana et al., 2020; Wang et al., 2021; Thulya, 2020)							Our work
Consensus algorithms	PoA	PoW	PoS	DPoS	PBFT	PoET	Ripple	Dynamic PoA
Blockchain permission	X	X	X	✓	✓	✓	✓	X
Transaction finality	✓	X	✓	✓	✓	✓	✓	✓
Rate of transaction	X	X	✓	✓	✓	✓	✓	✓
Participant cost	✓	✓	✓	✓	X	X	✓	✓
Scalability	✓	✓	✓	✓	X	✓	✓	✓
Trust	X	X	X	X	X	X	X	✓
Short transaction delay time	✓	✓	X	✓	✓	✓	X	✓
Decentralization	✓	✓	✓	✓	✓	✓	✓	✓

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

Security	✓	✓	✓	✓	✓	✓	✓	✓
Multi validator	X	X	X	X	X	X	X	✓
Real-time incidence response	X	X	X	X	X	X	X	✓
Throughput	X	X	✓	✓	✓	✓	✓	✓
Reliability	✓	✓	✓	✓	✓	✓	✓	✓
Fraud can be hidden	✓	✓	✓	✓	✓	✓	✓	X

Table 1 compared the dynamic PoA with other consensus algorithms. The results revealed that while the dynamic PoA competes with the rest in satisfying other quality of service requirements, it stands out in performance considering key attributes such as trust, multi validator and real-time incidence response. The reason was because validators are determined based on trust, performance and integrity. Secondly only our model does not depend on hash key analysis as the only mechanism for fraud detection, which is very good.

5. CONCLUSION

In this paper, a new PoA which approves grid energy import transactions with multiple validators selected based on reputation metric such as availability, trust quality index, and reliability was presented. In addition, a real-time incidence response alert notification algorithms was integrated for fraud detection, making it impossible to hide fraud, even if validators collaborate to manipulate data like in the case of traditional PoA. These multi-validator and real-time features were then applied for ESCMS at the EEDC, Nigeria, using energy import data for March, 2025. From the comparative analysis carried out, it was observed that while our model competed with other consensus algorithms, it standout in terms of trust, inability to hide fraud and real-time incidence response capabilities. Therefore this work is recommended to Distribution Company all over the world, to help manage non technical losses which have remain unsolved in the power sector.

6. CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

7. DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, Ebere U.C., upon request and are used confidentially.

References

1) Ali, S., Yongzhi, M., & Ali, W. (2023). Prevention and Detection of Electricity Theft of Distribution Network. *Sustainability*, *15*(6), 4868. https://doi.org/10.3390/su15064868.

2) Al-Rakhami, M. S., & Al-Mashari, M. (2021). A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management. *Sensors*, *21*(5), 1759. https://doi.org/10.3390/s21051759

3) Ankarberg, T., & Juvencius, K. (2021). Consensus algorithms for adding blocks to private blockchains in IIoT networks: Comparison of two Proof-of-Authentication implementations on IIoT hardware [Bachelor's thesis, KTH Royal Institute of Technology, School of Engineering Sciences in Chemistry, Biotechnology and Health]. TRITA-CBH-GRU-2021:34.

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

4) Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*, *22*(19), 7162. https://doi.org/10.3390/s22197162

5) Badis Hammi, Sherali Zeadally, Yves Christian Elloh Adja, Manlio Del Giudice, Jamel Nebhen. Blockchain-Based Solution for Detecting and Preventing Fake Check Scams. IEEE Transactions on Engineering Management, 2022, 69 (6), pp.3710-3725. https://hal.science/hal-04400815/file/Blockchain%20Based%20Solution%20For%20Detecting_and_Preventing_Fake_Check_Scams.pdf

6) Briseño, H.; Rojas, O. Factors associated with electricity theft in Mexico. *Int. J. Energy Econ. Policy* **2020**, *10*, 250–25

7) Carr, D., & Thomson, M. (2022). Non-Technical Electricity Losses. *Energies*, *15*(6), 2218. https://doi.org/10.3390/en15062218

8) Chris E. (2023)" Integration of blockchain for fraud prevention"; https://www.researchgate.net/publication/387958719_Integration_of_Blockchain_for_Fraud_Prevention

9) Darwish, T., Abu Bakar, K., Matsuda, G., Aliyu, A., Abdullah, A. H., Ismail, A. S., Zahilah, R., Yusof, A. F., Mohamad, M., Idris, M. Y., Ismail, Z., Che Yaacob, A., & Hermans. (2020). A comparative analysis of blockchain consensus algorithms from Shariah perspective. Journal of Contemporary Islamic Studies.

10) David Livingston, Varun Sivaram, Madison Freeman, and Maximilian Fiege (2018)" Applying Blockchain Technology to Electric Power Systems"; https://www.ourenergypolicy.org/wp-content/uploads/2018/07/Discussion_Paper_Livingston_et_al_Blockchain_OR_0.pdf

11) Dong, J., Ning, P., Zhao, H. *et al.* Decentralized peer-to-peer energy trading: A blockchain-enabled pricing paradigm. *J. King Saud Univ. Comput. Inf. Sci.* **37**, 10 (2025). https://doi.org/10.1007/s44443-025-00025-2

12) Fahim, S., Rahman, S. K., & Mahmood, S. (2023). Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV. International Journal of Mathematical Sciences and Computing, 3(3), 46–57. https://doi.org/10.5815/ijmsc.2023.03.04

13) Gresoi, S., Stamatescu, G., & Făgărășan, I. (2025). Advanced Methodology for Fraud Detection in Energy Using Machine Learning Algorithms. *Applied Sciences*, *15*(6), 3361. https://doi.org/10.3390/app15063361

14) Hameed, H., Zafar, N.A., Alkhammash, E.H. & Hadjouni, M. (2022) Blockchain-based formal model for food supply chain management system using VDM-SL. Sustainability, 14, 14202. DOI: 10.3390/su142114202.

15) International Standards for the Professional Practice of Internal Auditing. Global Practice Guide: Internal Auditing and Fraud. The IIA. Available online: **https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/global-practice-guide-internal-auditing-and-fraud/** (accessed on 10May 2026).

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

16) Kumar, J.C.R.; Majid, M.A. Renewable energy for sustainable development in India: Current status, future prospects, challenges, employment, and investment opportunities. *Energy Sustain. Soc.* **2020**, *10*, 2.

17) Lampietti, J.A.; Banerjee, S.G.; Branczik, A. *People and Power: Electricity Sector Reforms and the Poor in Europe and Central Asia*; The International Bank for Reconstruction and Development/The World Bank: Washington, DC, USA, 2007

18) Louw, Q.E. The Impact of Non-Technical Losses: A South African Perspective Compared to Global Trends. Available online: **https://www.sarpa.co.za/SARPA_Paper_Quentin_Louw-1.pdf** (accessed on 22 April 2025)

19) Miglani A., Kumar N., Chamola V., (2020)" Blockchain for Internet of Energy management: Review, solutions, and challenges"; Computer Communications 151 pp.395–418

20) Nguyen The Vinh, Nguyen Van Dung (2025)" Bidirectional AC/AC converter linking two microgrids in a flexible microgrid" International Journal of Power Electronics and Drive Systems(IJPEDS) Vol. 16, No. 1, March2025, pp. 389~406 ISSN: 2088-8694, DOI: 10.11591/ijpeds.v16.i1.pp389-406ρ389

21) Nneka J., Chidubem V. (2025)" Privatisation, prepaid metering and electricity billing scam of Enugu electricity distribution company (EEDC) in Enugu metropolis of Nigeria"; journal of public affairs; volume 22; Issue 4; e2644; https://doi.org/10.1002/pa.2644

22) Osama M. Arafa, Mona M. Mamdouh, Ahmed Mansour, Zeinab Elkady (2025)" Harmonics elimination and reactive power compensation based on novel SDFT-PLL shunt active power filter control approach" International Journal of Power Electronics and Drive Systems (IJPEDS)Vol. 16, No. 1, pp. 298~310ISSN: 2088-8694, DOI: 10.11591/ijpeds.v16.i1.pp298-310□29

23) Pineda, M., Jabba, D., Nieto-Bernal, W., & Pérez, A. (2024). Sustainable consensus algorithms applied to blockchain: A systematic literature review. Sustainability, 16, Article 10552. https://doi.org/10.3390/su162310552

24) Pooja Khobragade and Ashok Kumar Turuk (2020)" Blockchain Consensus Algorithms: A Survey"; http://dspace.nitrkl.ac.in:8080/dspace/bitstream/2080/3720/1/2022_ICBA_PKhobragade_Blockchain.pdf

25) Rizal, S., & Kim, D.-S. (2025). Enhancing blockchain consensus mechanisms: A comprehensive survey on machine learning applications and optimizations. Blockchain: Research and Applications, 6, Article 100302. https://doi.org/10.1016/j.bcra.2025.100302

26) Smith, T.B. Electricity theft: A comparative analysis. *Energy Policy* **2004**, *32*, 2067–2076.

27) Wang, Q., Huang, J., Wang, S., Chen, Y., Zhang, P., & He, L. (2020). A comparative study of blockchain consensus algorithms. Journal of Physics: Conference Series, 1437(1), Article 012007. https://doi.org/10.1088/1742-6596/1437/1/012007

Volume 65 | Issue 05 | May 2026
DOI: 10.5281/zenodo.20229269

28) Zarrin, J., Wen Phang, H., Babu Saheer, L. *et al.* Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Comput* **24**, 2841–2866 (2021). https://doi.org/10.1007/s10586-021-03301-8

29) Zhebka, V., Zhebka, S., Bazhan, T., Skladannyi, P., & Sokolov, V. (2024). Methodology for choosing a consensus algorithm for blockchain technology. In Proceedings of DECaT'2024: Digital Economy Concepts and Technologies (pp. 1–10). CEUR Workshop Proceedings. https://ceur-ws.org