Decentralized Payment Framework for Low-Connectivity Areas using Ethereum Blockchains

Burhan Ul Islam Khan
Department of CST, Faculty of CS and IT, University of Malaya, Kuala Lumpur, Malaysia | Fakultas Teknik, Universitas Negeri Padang, Padang, Sumatera Barat, Indonesia
burhankhan@um.edu.my (corresponding author)

Asadullah Shah
Department of IS, Kulliyyah of ICT, International Islamic University Malaysia, Kuala Lumpur, Malaysia
asadullah@iium.edu.my (corresponding author)

Khang Wen Goh
Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia
khangwen.goh@newinti.edu.my

Rusnardi Rahmat Putra
Department of CE, Fakultas Teknik, Universitas Negeri Padang, Padang, Sumatera Barat, Indonesia
rusnardi.rahmat@ft.unp.ac.id

Abdul Raouf Khan
Department of Computer Sciences, King Faisal University, Al-Ahsa, Saudi Arabia
raoufkhan@kfu.edu.sa

Mesith Chaimanee
School of Engineering, Metharath University, Pathum Thani, Thailand
mesith.c@mru.ac.th

Received: 1 August 2024 | Revised: 17 August 2024 | Accepted: 22 August 2024

 DOI: https://doi.org/10.48084/etasr.8582

ABSTRACT

This paper presents a pioneering analytical framework for a secure payment system leveraging blockchain technology tailored to regions with suboptimal network connectivity. Contemporary payment mechanisms utilizing Ethereum are predominantly optimized for areas with robust network infrastructure, neglecting regions with less connectivity. To address this gap, the proposed model integrates novel security attributes and employs an analytical method to design a decentralized payment system. The framework facilitates communication between low-connectivity zones and Internet service providers through auxiliary nodes, creating a local blockchain network for residents, merchants, and auditors. A mathematical model quantifies operational costs, transaction processing, and synchronization of auxiliary nodes, ensuring a resilient and secure payment architecture. A unique aspect of the proposed approach is its robustness against auditor outages and network variability, coupled with an empirical analysis of incentive structures for auditors' block validation activities. Moreover, it delineates the minimum requirements for secure transaction completion. Empirical findings showed a significant improvement in system efficiency, including a 79% reduction in block time, a 28% increase in transaction throughput, a 30% decrease in energy consumption, a 68% shorter confirmation time, a 63% reduction in execution time, a 46% increase in block production rate, and 82% reduced network variability. This study's significant contribution lies in introducing a sustainable, cost-effective, and secure payment system for regions with inadequate network services.

Keywords-blockchain-based payment systems; inferior network connectivity; Ethereum blockchains; secure payment infrastructure; transactional efficiency

I. INTRODUCTION

Blockchain represents a paradigm shift in distributed and decentralized ledger technology, known to secure transactions with enhanced transparency across a network of computer systems. As a cornerstone of various cryptocurrencies, blockchain operates on a peer-to-peer network that contrasts sharply with traditional centralized systems, offering high resilience and security [1]. It also provides a distributed ledger system where each node or participant can access its copy of the complete ledger and updates using a consensus mechanism [2]. The immutable property of blockchain offers a significant ability to either delete or alter any transactional block added to the network, accomplished through the consensus method and the cryptographic hash function [3]. The consensus mechanism allows nodes to agree on the state of the blockchain, including proof-of-state and proof-of-work, which is essential for validating transactions [4]. Another inherent characteristic is its smart contracts, self-executing contracts programmed to execute terms when predefined conditions are met. Ethereum is a popular blockchain platform that supports smart contracts. The adoption of blockchain offers a significant level of transparency because all blockchain transactions are visible to all nodes in the network system. This also improves trust among participants and is essential for blockchain-based payment systems.

The architecture of a blockchain-based payment system typically focuses on adopting fundamental characteristics such as cryptographic security, transparency, immutability, and decentralization. The primary objective is to build a highly resilient and potentially secure payment system that uses blockchain technology. However, there are additional perspectives on blockchain-based payment systems that are indirectly linked to security considerations. Incorporating blockchain into payment systems, regardless of the commercial application domain, has been reported to enhance resilience in the event of specific points of failure. This means that the failures experienced by the blockchain network nodes maintain the overall functionality of the technology [5]. Blockchain is characterized by its unchangeable and permanent nature, which facilitates the creation of an immutable validation trial for each payment transaction. This feature is precious for managing transaction records, auditing, and compliance [6].

Smart contracts within the blockchain play a pivotal role in automating all transactions by enforcing specific agreements without relying on third-party intermediaries. The functionality of smart contracts strikes a balance between payment system efficiency and resistance to security threats [7]. Blockchain-based payment systems are also distinguished by their high accountability and transparency, enabling all participants to access information related to accountability, trust, and transaction history [8]. Moreover, it has been observed that blockchain-based transactions offer faster processing times compared to conventional financial systems, a feature of utmost importance for international transactions [9].

Despite these advantages, blockchain technology still has significant vulnerabilities. The existing blockchain technology adopted in payment systems is yet to be sufficiently resistant to malware, phishing, Sybil attacks, attacks on private keys, and smart contract vulnerabilities. This study aims to contribute to the development of a novel, simplified, and highly sustainable secure payment system using the Ethereum blockchain. The key contributions of this study are summarized below.

- Innovative Smart Contract System: Develop a distinct and novel smart contract system to manage all essential transactions and control incentives for auditors.
- Deployment Scenario in Rural Areas: Consider a new use-case deployment scenario in rural areas with intermittent network connections to implement the proposed blockchain model for secure payment systems.

II. LITERATURE REVIEW

The adoption of blockchain technology has seen significant growth in the past five years, driving advancements in cryptocurrency-based applications with a focus on enhancing security in blockchain-based payment systems. Researchers aim to harness blockchain's capabilities to develop secure payment mechanisms. In [10], mobile payment security and data privacy concerns were addressed by integrating blockchain with an Interplanetary File System (IPFS) on a mobile cloud platform. This approach enhances security and data confidentiality but relies on IPFS network nodes and faces challenges in securely disseminating Electronic Payment Records (EPRs). Although aligned with blockchain principles, it lacks network connectivity considerations, emphasizing low-cost online payment services. In [11], a blockchain-based e-commerce payment model was introduced to reduce the costs and complexities of online payments. Despite the potential for cost savings, this study did not discuss network connectivity or direct alignment with Ethereum blockchains, focusing on reducing operational costs. However, complex encryption operations and key management increase the node operational costs. In [12], a payment system was proposed, which directly attached policies to money using blockchain technology, enhancing flexibility and security. This approach did not explicitly discuss network connectivity or align with Ethereum blockchains, lacked cost details, and did not provide a practical deployment benchmark. In [13], a decentralized architecture was introduced for Electronic Toll Collection (ETC) systems to enhance security and efficiency while mitigating risks. However, network connectivity considerations and detailed cost implications needed to be included. Although this architecture used blockchain technology, it did not explicitly align with Ethereum blockchains. In [14], a blockchain-based architecture was proposed for IoT information exchange, focusing on security and efficiency but neglecting network connectivity or Ethereum alignment. While focusing on reliability and stability, this architecture lacked specific cost considerations.

In [15], secure, covert communication was introduced by embedding messages in a blockchain and leveraging data integrity for security. This study did not discuss network connectivity or Ethereum alignment, lacked cost details, and had high bandwidth requirements. In [16], a random walk-based link prediction model was used to track Ethereum transactions, enhancing user protection and supervision. However, this model did not consider link quality when assessing dynamically vulnerable networks or discussing network connectivity or detailed costs. In [17], Etherless Ethereum Tokens (EETs) were introduced for closed-economy transactions, simplifying the user experience. While highlighting cost-effective deployment, it lacked large-scale information and contract vulnerability assessment. In [18], the Code and Transaction Random Forest (CTRF) model was proposed to identify vulnerable Ethereum contracts by addressing Ponzi schemes. Specific to Ethereum, this study did not discuss network connectivity or implementation costs. In [19], inefficiencies were addressed in crowdfunding markets with a decentralized application (DApp) on Ethereum. However, this approach lacked network connectivity and cost details but emphasized trust and efficiency. In [20], a fixed-price transaction fee structure was proposed using a Monte Carlo approach but did not interpret the impact of trust vulnerability or provide cost details. Using structural equation modeling, a trust model for Ethereum payments was introduced in [21]. However, this model needs to address network connectivity or Ethereum payment costs and faces computational inefficiencies in more extensive networks. In [22], RZcoin enhanced Ethereum transaction privacy and security but lacked a cost analysis.

Table I summarizes the state-of-the-art models studied. A closer look at the findings reveals concerns associated with smart contract management, centralized-decentralized structure ambiguity, intermittent connections, and vulnerable key management. Various methods for blockchain-based payment systems, including fueling, electricity, financial computer systems, supply chains, energy trading, and the hospitality industry, emphasize Ethereum modeling. The studies in [14, 15, 21] stand out because they represent unique architectures that improve secure payment systems and are suitable benchmarks.

Ethereum-based schemes dominate blockchain payment system designs but exhibit open-ended vulnerabilities:

- Less emphasis on smart contract management: Existing studies have overlooked vulnerabilities such as fund manipulation, unchecked external calls, arithmetic flaws, and reentry bugs within smart contracts [11].
- Ambiguity between centralized and decentralized structures: Despite Ethereum's decentralized nature, approaches must support essential services by bridging centralized and decentralized structures [13, 16].
- Non-inclusion of intermittent connections: Studies assuming seamless network connections are impractical in remote areas with limited connectivity [15, 17, 19-21].
- Vulnerable key management: Protecting private keys, crucial for Ethereum transactions, still needs to be addressed [13-21]. Encryption-based approaches have yet to be sufficient for this purpose.

Most state-of-the-art models require extensive analysis and benchmarking to demonstrate their robustness. Although some issues have been partially addressed in previous studies [1, 23], intermittent connections and vulnerable key management gaps represent significant research opportunities. These gaps form the foundation for the proposed research, leveraging Ethereum's characteristics under intermittent network conditions to facilitate secure payment systems.

III. PROBLEM DESCRIPTION

The rapid evolution of blockchain technology, particularly Ethereum, has revolutionized various sectors, including payment systems. Despite these advances, Ethereum-based payment systems are optimized primarily for environments with stable network connectivity and overlook areas with intermittent or limited connectivity. This oversight presents a significant barrier to blockchains' universal adoption and practical utility in diverse geographical and infrastructural contexts. The literature indicates concerted efforts to bolster security and data confidentiality in blockchain-based payment systems using various integrative approaches. However, these studies focused mainly on contexts with robust network infrastructures and did not adequately address the challenges in areas with inferior network connectivity. Moreover, although crucial, the emphasis on cost-effectiveness and versatility needs to address the specific needs of low-connectivity regions directly.

Existing research also highlights the challenges of transaction delays, low throughput in blockchain systems, and inefficiencies of current e-commerce and healthcare payment systems. Although innovative, these studies should consider the unique challenges of limited network environments sufficiently. This gap is particularly critical given the increasing reliance on blockchain for secure transactions in various sectors. Another critical aspect is the management of smart contracts within the Ethereum blockchain. As indicated in the literature, current methods should pay more attention to smart contract management, which leads to vulnerabilities such as unchecked external calls and arithmetic flaws. This issue is exacerbated in low-connectivity settings, in which the reliability of smart contract execution is even more crucial. The ambiguity between centralized and decentralized structures in existing models further complicates this issue as it affects the supportability of essential services such as currency exchange or wallet systems in areas with intermittent connections.

The lack of intermittent connections in existing blockchain-based payment systems is a significant oversight. As observed in most current implementations, the assumption of seamless network connectivity could be more practical in remote areas with limited cellular connectivity. This research gap highlights the need for a blockchain-based payment system that operates effectively under intermittent network conditions to ensure transaction security and system robustness.

TABLE I. SUMMARY OF STATE-OF-THE-ART MODELS

Ref.	Issues addressed	Techniques employed	Benefits	Constraints	Network connectivity consideration	Sustainability and cost
[10]	Security and data privacy in mobile payment systems	Integration of blockchain with decentralized IPFS on a mobile cloud platform	Enhanced security and data confidentiality, minimal network latency, and decreased energy usage	Dependency on IPFS network nodes, challenges in disseminating EPRs securely	Not explicitly stated	Focuses on low-cost online payment services with high versatility
[11]	Cost and complexity of e-commerce payment systems	E-commerce payment model based on blockchain	Reduction in transaction costs, elimination of payment intermediaries	Requires integration with existing e-commerce platforms, potential scalability issues	Not explicitly stated	Focuses on cost reduction in e-commerce operations
[12]	Efficiency and flexibility in payment systems	Blockchain-based programmable money system with dynamic policy attachment to money	Enhanced flexibility, security, and efficiency in payments	Complex implementation and management, scalability	Not explicitly stated	Focus on efficiency and security; specific costs not detailed
[13]	Security threats in centralized ETC systems	Decentralized ETC architecture using blockchain technology	Improved security, prevention of data loss and DDoS attacks, enhanced efficiency in ETC operations	Potential complexity in large-scale implementation, reliance on blockchain stability	Not explicitly stated	Focus on security and efficiency, with no detailed cost analysis
[14]	Security in IoT information exchange	A BCT-based lightweight IoT information exchange security architecture utilizing a dual chain method and practical Byzantine fault-tolerant mechanism	Enhanced data exchange security and privacy, efficient data registering and transactions	Complexity in implementation, potential scalability issues, lack of benchmarking	Not explicitly stated	Emphasizes efficiency and reliability but does not detail specific costs
[15]	Secure communication using blockchain	Method for embedding covert messages into blockchain	Enhanced data integrity, covert communication capabilities	Reliance on blockchain's integrity and security features, complexity of protocol implementation, lack of benchmarking	Not explicitly stated	Focuses on secure communication, specific cost not detailed
[16]	Fraud and money laundering in cryptocurrency transactions	Random-walk-based link prediction model on Ethereum transaction data	Enhanced ability to track and detect suspicious accounts, explainable results from transaction data analysis	Complexity in data collection and model application, reliance on transaction data accuracy	Not explicitly stated	Focuses on tracking and security; specific cost not detailed
[17]	Cumbersome user experience in Ethereum token transactions	EETs for transacting with tokens only, without needing ether for gas	Simplifies user experience allows transactions in a closed-economy manner	Complexity in deployment and operation of EETs, comparison with Gas Station Networks (GSN), security resiliency is not presented	Not explicitly stated	Demonstrated to be less gas intensive than GSN, but detailed cost analysis not provided
[18]	Detection of Ponzi schemes in Ethereum	CTRF model, extracting word and sequence features of smart contract code and transaction features	Improved recall in Ponzi contract detection, effective identification of fraudulent contracts	Complexity of feature extraction and model training; focus on Ethereum-specific contracts; model not applicable for large and streamed numbers of transactions	Not explicitly stated	Focuses on effective detection, specific cost not detailed
[19]	Inefficiencies in the current crowdfunding market	Development of a decentralized application (DApp) for crowdfunding on Ethereum	Improved trust and efficiency, reduction of market inefficiencies by bypassing third parties	Complexity in integrating blockchain technology with crowdfunding platforms, no benchmarked findings	Not explicitly stated	Focuses on lowering market inefficiencies; no detailed cost analysis provided
[20]	Optimization of transaction fees in Ethereum	Monte Carlo approach to predict transaction mining probability	Efficient optimization, effective prediction of transaction fees and processing times, enhancing user experience	Less practical parameters of miners, less flexible smart contracts, rely on historical data, may not account for sudden changes in network conditions	Not explicitly stated	Focuses on optimization, specific cost impact not detailed
[21]	Trust issues in Ethereum payments	Structural equation modeling to develop a trust model in Ethereum payments	Provides a comprehensive model to understand trust factors in cryptocurrency payments, low fees for transactions	Model complexity, may not account for all user behaviors and preferences, lacks benchmarking	Not explicitly stated	No specific focus on cost, emphasizes understanding user trust
[22]	Privacy and security in Ethereum transactions	Improvement of RZcash to RZcoin, implementing new signature schemes and bulletproofs for asset information privacy in Ethereum	Enhanced security and privacy, reduced communication costs, and proof sizes	Higher resource consumption; addresses key redundancy issues but may still face challenges in complex transactions	Not explicitly stated	Focuses on security with lower communication costs, specific costs not detailed

Furthermore, vulnerable key management in Ethereum-based systems still needs to be addressed. Protecting private keys is crucial to secure transactions. However, current models need comprehensive solutions for secure key storage, particularly in low-connectivity environments. This vulnerability poses a significant risk to the integrity and security of blockchain-based payment systems. In summary, there is a clear need for a comprehensive, secure, and efficient blockchain-based payment system specifically designed for areas with limited network connectivity. This study aimed to fill this gap by proposing an Ethereum-based framework tailored to such environments. This framework integrates novel security attributes and employs an analytical method to design a decentralized payment system that is resilient to network variability and auditor outages, ensuring secure and efficient transactions in low-connectivity settings.

IV. RESEARCH METHOD

The aim is to facilitate a non-conventional mechanism to implement a secure online payment system in the most cost-effective way within an area with intermittent and uncertain network connectivity. To implement a secure payment framework, the proposed scheme assumes that it is possible to construct a communication network using wireless networks in such regions using available wireless standards (multiple hotspots, access points, etc.). This study also assumes that such a rural region has only one base station connected to the Internet, with a deficient channel capacity. To assess the robustness and sustainability of the proposed model, the study assumed the availability of a smaller number of conventional infrastructure (e.g., base stations) in remote rural areas. The core idea is to implement a payment scheme in rural areas with less scope for many connectivity establishments. Thus, the model assumes that the network connection to a base station and other Internet service providers is inferior with degraded quality of service performance. Such challenging network conditions are considered to justify the fact associated with the problem solution and to facilitate a highly secure payment system built in a highly vulnerable and troubleshooting network. Figure 1 illustrates the proposed architecture.

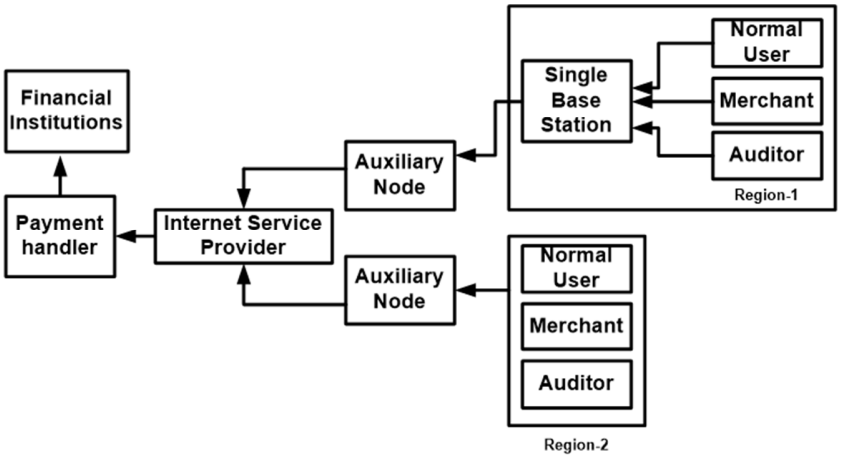

Fig. 1. Proposed architecture.

Figure 1 shows the presence of various inhabitants within the rural region consisting of three types of actors: customers, merchants, and auditors. The base station within that region acquires transaction information. In addition, it communicates with its connected Internet service provider, linking it to nearby rural areas and other available service providers. It also shows that the second rural area does not have a base station and will need to depend only on the base station in the first area. In addition, a digital payment system handler is considered, linking all financial institutions that hold each actor's accounts in the system model. The model considers multiple payment handlers, one of which is assigned to control an auxiliary node. The auxiliary nodes act as a communication bridge between rural regions and service providers. The blockchain can process payment-based transactions that an inhabitant can control. Therefore, the scheme does not offer any form of dependence on centralized authority. Furthermore, note that none of the blockchains in rural areas depend on each other and use payment keys to perform their operations. Figure 2 elaborates on this scheme.

As shown in Figure 2, regular users with merchants within the defined rural region initiate a digital payment system while connected to the auxiliary nodes. The proposed scheme also allows any resident to voluntarily play the role of an auditor in a distributed and decentralized manner to validate ongoing transactions. For this purpose, a mobile phone application can be designed that can be used by regular users to use this digital payment service, where blockchain is running on its underlying network. Normal users can use this service on their handheld mobile devices. Simultaneously, merchants and auditors must have slightly high-processing computing devices to perform auditing operations. The study also assumes that the auxiliary nodes continue to operate under intermittent connections with the service providers, while any number of regular users can join or leave the system. The additional node also performs operations related to the distribution of auditing incentives and the management of accounts. Another novelty of this scheme is that it does not deploy an Ethereum blockchain as it is. However, it uses a payment-key-based distinct currency for local transactions, offering more accountability and security.

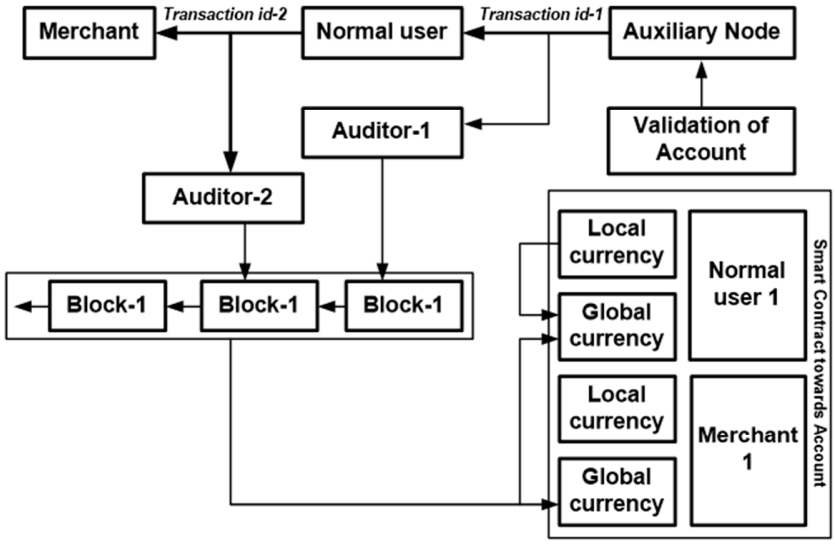

Fig. 2. Elaboration of blockchain operation in the proposed scheme.

The proposed scheme implements a unique integration of the payment-key-based management of payment services with the smart contract in the blockchain, as it can restrict any user attempting to access the system, offering better access control. Furthermore, it provides more flexibility for payment handlers to perform their tasks in the event of link breakage with auxiliary nodes. As shown in Figure 2, two forms of transactions are facilitated: (i) regular transactions between merchants and everyday users, and (ii) transactions related to the exchange of local currency to obtain the actual money conversion in the form of payment keys. To perform a typical transaction, all regular users must initiate the connection of their local digital financial transactional application via a mobile application with the payment keys. After the financial institution approves this connection, a specific form of transactional identity is assigned to the first auditor and incorporated into a particular block. After confirmation of the transactional identity, the scheme triggers a smart contract, followed by updating the regular user's payment key.

A typical user pushes and forwards a new transactional identity to the merchant to acquire payment services obtained by the second auditor and validated in consecutive blocks. Irrespective of the availability of an auxiliary node, the scheme offers fair treatment towards processing and authorizing all types of routine transactions. After the system connects to an auxiliary node, it synchronizes them and executes the smart contract and the payment key locally for merchants and regular users. Like a blockchain node, the system also constructs dual-account identities for auxiliary nodes. If a new node attempts to join the network, it will first be required to request an auxiliary node, as it will not have any valid payment key to facilitate transactions in a new network. After the auxiliary node authenticates the new node, it acquires the payment-key-based current obtained by converting its payment key locally. It forwards it to the new requestor node's destination node (who will receive the payment). Therefore, the auxiliary node acts as a gateway when one node in a rural area attempts to communicate with another node in a different rural area.

To construct a distinct form of network connection for a secured digital payment system, the proposed scheme allows the payment handler to extensively use high-processing nodes as auxiliary nodes. Payment handlers construct a smart contract to keep track of all accounts and balances of regular users in both currency forms (local and actual). A smart contract also performs audit operations in a distributed manner. At the same time, it also informs the auxiliary node of the event when auditors explore a new block or when a new user attempts to participate in the network for recent transactions. To keep the system up-to-date, the smart contract accesses the upgraded form of the ledger module in the linked state of the network. The smart contract also updates its states between the rural region and an auxiliary node, irrespective of the linked or non-linked network state. All blockchain nodes sync with the auxiliary node in the linked state to either process the request related to currency exchange or update the regular users' financial balance.

The proposed scheme offers a highly interconnected local network with fewer dependencies on utilizing any sophisticated internal operation for decentralized blockchain operation. It is secure and provides a highly accountable payment system that maintains the two forms of currency. It is also cost-effective due to the selection and internal operation of the auxiliary nodes and smart contract systems.

V. SYSTEM IMPLEMENTATION

Before implementation, it is essential to highlight some significant design considerations. It is assumed that auditors possess adequate processing capabilities and resources to carry out their operations. The scheme also assumes that the assigned block size can accommodate all the necessary transactions. To facilitate a higher technical adoption of the proposed model, the system does not levy any reward or processing charges to audit any unchanged blocks. This is because the scheme uses a payment key to manage blockchain-based payment system operations. The channel capacity assigned to the environment is also considered adequate.

A. Configuring Blockchain Transaction

The proposed scheme considers all of its operations from the viewpoint of regular incoming new transactions $N_{s_i,}$ where s_i represents the transaction's start time. The mean rate of adding new blocks is represented by α_t (number of transactions per time unit). Therefore, the probability attribute f toward the generation of a block is mathematically expressed as:

$$f(\beta) = \alpha.a \quad (1)$$

where β represents the time of generation of the unit block, α is computed as $[E(\beta)]^{-1}$, and variable a represents $e^{-\alpha\beta}$. According to [24], the approximated timing of a block in Ethereum is nearly 12 s, which was also considered here. It should be noted that the proposed scheme does not keep any new blocks under the queue, as, according to the assumption, all the newly arriving blocks are added to subsequent blocks. This is also because the scheme assumes an adequate block size is maintained for all transactions in the case study. Hence, the processing time of the transaction is computed as

$$s_p = \beta - s_i \quad (2)$$

where the transaction start time s_i and the processing time of the transaction s_p range between 0 and β. In addition, the throughput score of all transactions is computed as the summation of all the start times, an s_i is divided by the time of generation of unit block β. This part of the implementation also estimates the size of the block that must be accommodated for both regular and multiple transactions as follows:

$$m_b = m_t.A \quad (3)$$

This equation computes the size of the newly added block m_b with respect to two variables, where m_t denotes the size of the blockchain transaction and A denotes the summation of all standard incoming new transactions N_{s_i} considering the start time of the transaction s_i. However, it should be noted that the variable m_b is only associated with regular transactions. However, from the perspective of multiple sessions, the variable m_b was upgraded to m_{b1}, which was empirically calculated as follows:

$$m_{b1} = A1.E(\beta) \quad (4)$$

where m_{b1} represents the blocks that must be added during multiple transactions considering $A1$ and $E(\beta)$, where $A1$ represents $\alpha_t.m_t$ and the anticipated blocking time. A similar mechanism is used to exchange the currency involved in each transaction with the auxiliary node η. This completes the essential configuration involved in the proposed blockchain transaction.

B. Cost Management Center

This is the next operational block, which is responsible for all transactions involving cost attributes. This module is primarily responsible for tracking and evaluating the payment system, auditing the rewards, and applying operations toward the blockchain. This module carries out the cost of the system operation, performing three types of cost computation:

1) Cost Toward Block Incentive

This entity is responsible for computing the cost associated with the block operation in Ethereum toward the payment system. Notably, the block incentive is an additional cost incurred by the payment system of service providers, although it is considered one of the potential benefits for the auditors. The cost computation for the block incentive is performed by

$$\theta_I = \lambda.I \quad (5)$$

where θ_I represents the cost of the block incentive, where the suffix I denotes the incentive and variable λ denotes the number of blocks involved in the transaction. It should be noted that incentive I is deployed by the payment operator toward its usage for expending I number of payment tokens.

2) Cost Toward Resource Management

This module is responsible for computing the costs associated with the network resources. This can be mathematically represented as follows:

$$\theta_\lambda = A2.C_{cap} \quad (6)$$

The cost computation toward resource management attribute θ_λ considers variables $A2$ and channel capacity C_{cap}. $A2$, represents the product of the cost of the channel capacity demanded in a specific blockchain network $\theta_{C_{cap}}$ and the duration of linking with the blockchain network D_l. The proposed model defines a particular period for relaying one transactional service D_s as the summation duration of linking with the blockchain network D_l and non-linking with the blockchain network D_{ul}. It should be noted that the proposed cost computation is modeled considering only the utilization of network resources associated with the bridge network. During full-fledged network coverage (linking state D_l), the auxiliary node acquires historical blockchain transactions, followed by synchronization. Furthermore, the auxiliary nodes also proceed toward processing the request for money exchanges during the transaction.

3) Cost Toward System Operation

This module θ_{tot} sums the cost toward the block incentive θ_I and the cost of resource management θ_λ.

$$\theta_{tot} = \theta_I + \theta_\lambda \quad (7)$$

C. Auxiliary Node Management

The internal operation, illustrated in prior subsections, shows that the proposed scheme supports the incoming of all regular transactions only when the auxiliary nodes are confirmed to be linked (D_l) by the bridge network. However, during non-linking (D_{ul}) with the bridge network from the auxiliary nodes, the system only facilitates transactions toward currency exchange operations. A severely challenging situation is considered in the proposed scheme, where the duration of linking and non-linking D_l/D_{ul} between the auxiliary nodes and bridge network is much longer than the duration required for blocking operations in blockchain networks.

Let λ_l and λ_{ul} represent the number of blocks constructed during the linking and non-linking states D_l and D_{ul},

respectively. m_{ul} is the size of the blocks permissible to be added during a non-linked duration (D_{ul}), given by

$$m_{ul} = \sum_{i=1}^{\lambda_l} m_t . U \quad (8)$$

The evaluation of m_{ul} is carried out considering m_t and U, which represent the size of the transaction and the summation of all regular incoming new transactions N_{s_i}, respectively. For the simplified computation of the proposed scheme, the modeling does not consider network-based artifacts (interference, overhead, and delay in the communication channel). The proposed system computes the synchronous block size as follows:

$$m_p = m_{ul} + A3 \quad (9)$$

where $A3 = g(m_t, N_{s_i}, m_{ex}, \gamma_{si}) - C_{cap_d}$. Here, the calculation of the synchronous block size m_p is carried out considering the summation of the size of blocks permissible in non-linked transaction m_{ul} and a unique transaction operator $A3$. Operator $A3$ is responsible for obtaining residual information toward synchronized transactions by applying a discrete function $g(x)$ to its assigned input arguments, and the result is subtracted from the instantaneous channel capacity parameter C_{cap_d}.

The function $g(x)$ is responsible for adding two entities, where the first entity is a product of the size of transaction m_t and normal incoming new transaction N_{s_i}, and the second entity is a product of the size of exchanged data m_{ex} and incoming transaction during currency exchange γ_{si}. It should be noted that the system could positively complete the synchronization task once the links are closed after the incoming new blocks of transactions. Channel capacity also affects the synchronization process. In the availability of maximized channel capacity, the scheme considers an instantaneous time, where no more data must be synchronized. This can be expressed as follows:

$$d_o = \frac{m_{ul}}{A4} \quad (10)$$

The instantaneous time variable d_o is computed by considering the size of blocks permissible in non-linked transactions m_{ul} and $A4$. The computation of $A4$ is further carried out as $A4 = C_{cap} - (\alpha_t . m_t + \alpha_{ar} . m_{ex})$, where the variables $\alpha_t, m_t, \alpha_{ar}, m_{ex}$ represent the mean rate of adding a new block, transaction size, arrival rate of exchanged data, and size of exchanged data, respectively. Hence, the synchronization of auxiliary nodes is rendered in both linked/non-linked states.

D. Auditor Network Management

The next set of implementations is associated with auditing the blockchain network, in which the core agenda is to confirm a higher degree of optimal security and trustworthiness. The first task in this process is to evaluate the possibilities of streaming services during service outages (owing to non-linked network events). Notably, all auditor modules are assigned specific incentives while performing their assigned tasks. However, it is feasible for them to leave the current network while joining a different network simultaneously. Ad_t and Ad_l are total and linked auditors, respectively, where Ad_t is always greater than Ad_l. The generalized expression for all auditors to attain a non-linked state of the network (offline) is

$$\begin{aligned} Anticipated[Ad_l] &= Ad_t - Anticipated[\chi] \\ &= Ad_t - Ad_t . \mu_d \\ Ad_t &= Anticipated[Ad_l]/(1 - \mu_d) \end{aligned} \quad (11)$$

Here, it can be noted that the proposed system initially computes the anticipated value of the linked auditor (online) by finding the difference between the total number of auditors Ad_t and the expected number of auditors found to be in a non-linked state χ and considering when all the auditors are non-linked, then $\mu_1 = \mu_2 = \cdots = \mu_d$. Hence, (11) facilitates computing the total number of auditors to confirm its state of outages (or not linked with the blockchain network connectivity for any eventual reason).

The next part of implementation is associated with assigning incentives to auditors. Based on the budget related to blockchain operational services, the service operators (responsible for facilitating all payment-based operations) allocate incentives to auditors. The empirical expression for the anticipated gain is mathematically represented as follows:

$$\tau = A5 - \psi_h \beta \quad (12)$$

Here, the computation of the anticipated gain for each block being audited τ is carried out considering $A5 (= I/Ad_t)$, ψ_h denotes the cost of blockchain operation for auditors, and β is the time of generation of the unit block. It should be noted that every auditor encounters a challenge while attempting to audit the blocks (to obtain a legitimate block) in the presence of many competitors. This process significantly minimizes auditors' expected incentives. The research challenge was mitigated by computing the lowest auditing incentive score. It should be noted that $A5$ is obtained from the anticipated cost for each round of auditing, $I' = I/Ad_t$. At the same time, the system does not perform any form of auditing operation for any nonoperational block with unchanged information. Furthermore, the value of τ can be expected to be higher than 0 for a better gain score in auditing operations.

The final part of this implementation caters to the minimal demands of linking blockchain networks. All nodes must acquire a ledger copy for optimal linking to facilitate better-synchronized communication. Furthermore, optimal payment security can be ensured only when many linked nodes exist. However, specific nodes want to delink from the network to reduce resource utilization costs. This study considers that all auditors should be linked with Ad_l (mean linked auditors) so that the range of Ad_l is $[0. Ad_t]$. The connected adjoining nodes acquire information about the blocks or transactions the specific auditor nodes receive. This phenomenon can be functional until all the residual nodes in the blockchain network acquire complete information. The study further limits the highest number of hops to δ to acquire the state of the directly connected nodes as:

$$\vartheta \geq A6(\delta) \quad (13)$$

where ϑ denotes the proportion of directly connected nodes in the blockchain network, which should be slightly higher than

$A6(= arg_{max}(Ad_l)/Ad_t)$. To balance the computational demands and optimal blockchain security, the scheme does not consider linked auditors Ad_0, as all auditors will eventually possess the blockchain information stored within them.

Thus, (13) assists the proposed system in providing a minimal number of auditors with balanced incentives, high security, and minimal computational burden. From a practical point of view, all auditors in rural areas must be encouraged to improve their linking capabilities. This can consistently increase the optimal syncing operations. However, this is only sometimes recommended, as it further increases resource utilization. It is also essential to acquire information on the churn rate from practical location-based information to precisely define auditors' incentives. From the above discussion, it is observed that operators belonging to the local network are utilized to offer a secure payment system to rural areas that are characterized by inferior connections. Therefore, the proposed scheme generates a novel form of a local network that is usually isolated from each other and resides in various regions within the rural area where blockchains are deployed. This allows individuals to process blockchain transactions without relying on any centralized module in the proposed payment system. The proposed scheme can be used as a local blockchain deployment using Ethereum, due to its assurance of verification, faster processing, and decentralized consensus. Apart from this, all auditors work on an incentive-based approach governed by the cost management center and its budget. To fulfill this claim, this study assumes that every auditor is required to maintain a minimal number of connections with nodes.

VI. RESULTS AND DISCUSSION

A typical test environment is considered to assess the performance of the proposed scheme. For this purpose, multiple virtual machines were employed to run using Ethereum on Linux.

A. Assessment Environment

The virtual machine configuration employed had 10 GB of storage and 2 GB of internal memory on an NVIDIA GPU and Core i5 processor. This study uses a specific form of analytical engine with a distributed search constructed on Apache Lucene to trace the operational intelligence of the proposed use cases. This search engine deployed Python libraries to monitor the behavior of the network. All nodes were arranged in a star topology, and their interconnections were facilitated by an ethernet switch capable of transmitting GB of data.

TABLE II. SIMULATION PARAMETERS

Parameters	Values
Transmission rate	1 GB/s
Sessions of sequential services	150
D_l	40 minutes
D_{ul}	480 minutes
Channel Capacity	5-130 KB/s

Table II lists the simulation parameters used to assess the proposed model. It should be noted that all of the above-initialized values are considered based on frequent observations from different related works. The results analysis of the model was performed based on the assigned values. Furthermore, the variation in such values reasonably affects the study model to demonstrate the practicality of its deployment.

To validate the proposed scheme, an environment to process the transaction was simulated by applying a transmission rate of 1 GB/s to a set of arbitrary addresses from multiple clients. During the experiment, the transaction rate was studied to benchmark the performance of the local blockchain. The assessment environment consisted of 150 sequential service sessions in linked and non-linked modes, where $D_l =$ 40 minutes and $D_{ul} =$ 480 minutes. These values were chosen hypothetically and can be altered based on detailed events linking the states of rural areas. The transactions consider 5-130 KB/s channel capacity. The scenario also chooses to fluctuate the availability of channel capacity to artificially create an environment with an intermittent link state between the base station and the Internet service provider.

A higher channel capacity is seen to witness a faster task completion time, while depreciation of channel capacity leads to the accumulation of new incoming transactions. During this process, the assessment also computes the block generation time by differentiating the two corresponding timestamps of the transactions. Additionally, processing time is obtained from the point of transaction initiation to the extraction of the transaction receipt. Furthermore, multiple performance parameters were chosen to evaluate the efficiency of the proposed scheme, which is benchmarked with state-of-the-art models on blockchain-based secured payment systems. Table III presents the numerical evaluation results using five performance metrics.

TABLE III. NUMERICAL OUTCOMES OF THE ASSESSMENT

Approach	P_{m1}	P_{m2}	P_{m3}	P_{m4}	P_{m5}
[14]	3.729	4144	5.95	9.1092	7.9983
[15]	3.779	3100	4.31	5.0887	6.4021
[21]	5.187	5305	4.76	7.1882	12.173
[22]	0.981	5928	5.85	2.1875	6.1992
Proposed	0.371	7500	2.51	0.8218	2.03

B. Analysis of Block Time

This primary performance parameter signifies the mean duration required to add a new block to the blockchain. The primary reason for choosing this parameter is that it helps to evaluate the actual speed of processing a transaction in a blockchain network. Although various methods exist to calculate this parameter (e.g., consensus-based, proof-of-work-based, difficulty adjustment-based), the proposed scheme mechanizes a simplified mean block time calculation, the duration involved in auditing a block for a given period. Figure 3 shows the block time results for various blockchain-based payment schemes. The results show that the proposed system (Prop) offers approximately 79% reduced block time compared to existing systems. The study in [21] includes extensive information on the user account, which requires significant computation time. This trust-based model offers a longer block time with increasing traffic. In [14, 15], a blockchain

architecture was implemented using game theory and a symmetric encryption scheme, which was lightweight compared to the model in [21] and led to reduced block time. The proposed scheme outperformed all other schemes due to its strategy for block management using payment keys and smart contract management without any encryption scheme. Furthermore, the smart contract involved ensures faster management of payment handlers, irrespective of the linking state of the blockchain network.

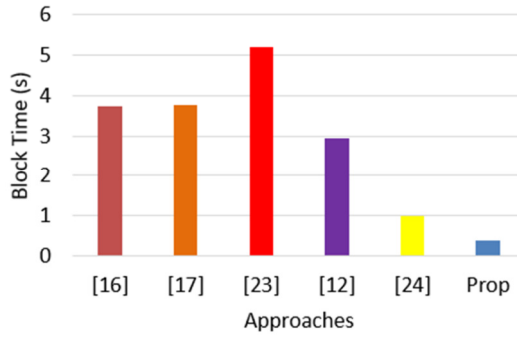

Fig. 3. Comparative analysis of block time.

C. Analysis of Transaction Throughput

This essential performance metric computes the number of transactions that the blockchain handles in one second. The primary reason for adopting this metric is to acquire the true notion of system processing capacity. Figure 4 shows that the proposed system offers an approximately 28% increase in transaction throughput compared to existing schemes. The model in [15] deployed a random oracle model with extensive utilization of hashing. Although it offered better security, hashes management significantly affected transactional throughput. The model in [21] employed a simplified validation scheme for blockchain transactions using signatures from all parties, increasing the validation time during each set of transactions and reducing its throughput. Furthermore, in [14], a complex strategy formulation was employed using dynamic game theory, which involved iterative assessment of trust, leading to an extensive reduction in throughput.

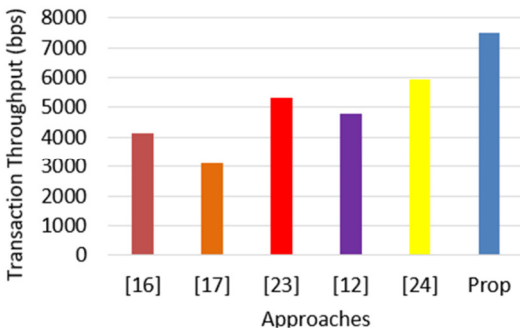

Fig. 4. Comparative analysis of transaction throughput (bps).

In contrast, the proposed scheme deploys a smart contract system in which a distributed module is designed for all transactional monitoring for users and merchants. At the same time, the auditors perform sequential blocking operations with the help of the auxiliary node. This means that most of the operational tasks are highly decentralized and distributed and data transmission is least affected by the block management of the proposed scheme. This results in better throughput.

D. Analysis of Energy

This is another essential performance metric for determining the hash rate (computational power) harnessed during an auditor's validation process. To compute this parameter, the proposed scheme initially assigned 10 J of initialized energy to be used by various nodes to perform a single hash operation. The mean energy depleted was multiplied by the cumulative hash rate of the blockchain network to obtain the results shown in Figure 5.

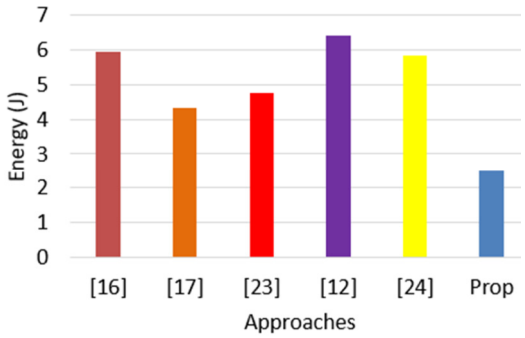

Fig. 5. Comparative analysis of energy.

Figure 5 shows that the proposed scheme ensures approximately 30% reduced energy consumption, in contrast to existing state-of-the-art models of secure payment systems using blockchain. This result is justified by those mentioned in the analysis of the throughput and block time.

E. Analysis of Confirmation Time

This performance parameter computes the duration for a transaction to be validated and appended to the blockchain. A better model is expected to reduce the confirmation time. From a practical implementation perspective, the proposed blockchain method offered a reduced confirmation time with an increasing traffic load, which is essential.

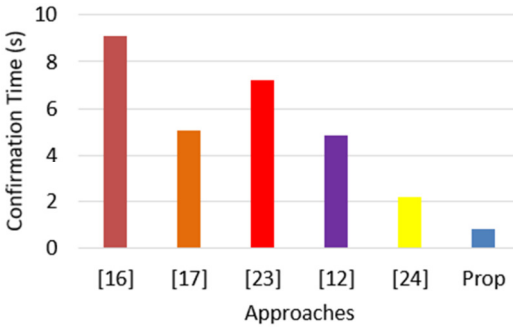

Fig. 6. Comparative analysis of confirmation time.

Figure 6 shows that the proposed scheme offers an approximately 68% reduced confirmation time compared to existing models. The adoption of the Byzantine fault-tolerant system in [14] used a consensus scheme in which a higher number of validations for each transaction was implemented in a complex form. This increases the security level but costs a higher confirmation time. The model in [21] deployed extensive trust-based computational parameters that involved personal and contextual information analyses. Evaluating such variables takes time and increases the confirmation time during block generation. It is also noted that the model in [17] offered shorter confirmation times compared to [14, 21], which is mainly due to its emphasis on channel-based validation models using a smaller number of security parameters. However, the embedding and extraction processes required extensive time during each transaction. Such problems are witnessed in [22], due to a completely decentralized environment in which the proof size was substantially reduced using the signature scheme and addressing the problem of key redundancy. However, the proposed system still excelled better in terms of reduced confirmation time, mainly due to its transaction flow mechanism. The presence of an auxiliary node is one of the significant novelties introduced in the proposed scheme, differentiating it from the other systems, as it acts as a bridge between all actors and services. This reduces the extensive effort of validating a block by each node, whereas smart contract management allows a better sync between blockchain nodes and auxiliaries. Therefore, the proposed system has a reduced confirmation time due to its faster block generation and validation processes.

F. Analysis of Block Production Time

This evaluation targets the evaluation of auditors' outages, which is accomplished using block production time. For this purpose, the observation focused on the rate at which novel blocks are generated, directly indicating either a slowdown or a halt in generating new blocks. Hence, the auditor's outage can be evaluated by finding either cessation or a sudden drop in the production of blocks. The obtained values were averaged for each individual to show the comparative results with existing schemes.

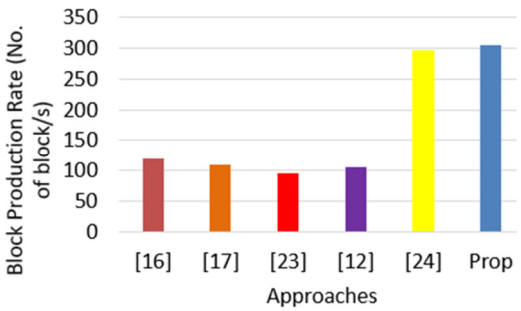

Fig. 7. Comparative analysis of block production rate.

The proposed scheme offers significant benefits, mainly due to the management of the auxiliary and auditor nodes presented in a decentralized environment. The proposed system shows an increase in the block production rate of approximately 46 % compared to existing systems. It should be noted that the proposed scheme does not consider any form of incentive allocation toward the stale block. Thus, its results are mainly related to the active blocking operations for all incoming transactions. This also results in faster transactions and an increased rate of block generation. Apart from this, as resource utilization is carried out in the backhaul network under ideal conditions of the network, the proposed scheme always offers synchronized operation for every new transaction, keeping the operational cost as low as possible, which leads to the availability of more incentive scores ready to be allocated to auditor nodes. However, this is different from any existing approach.

G. Analysis of Network Variability

This assessment investigates network variability, which is calculated by estimating the latency standard deviation. A higher score for these performance parameters will result in a higher fluctuation score, indicating degraded network performance. Stable network performance can be represented by a lower value of the network variability score, especially when it is in a decentralized form. Figure 8 shows that the proposed system offers approximately 82% reduced network variability compared to existing state-of-the-art mechanisms. The primary factor contributing to this result is directly related to the network design of the auditor. It should be noted that complete auditor operations are based on assigned incentives, where they are permitted to leave the current or join a new network. The system computes the probability of auditors' both active and passive modes and acts accordingly to ensure no downtime in case of any transactions. Furthermore, consistent network performance of auditors is ensured by maintaining a minimum incentive computed to ensure seamless operation of auditors around the clock. This results in higher consistency of processing block transactions, potentially keeping the network variability as low as possible, which is not witnessed in existing approaches.

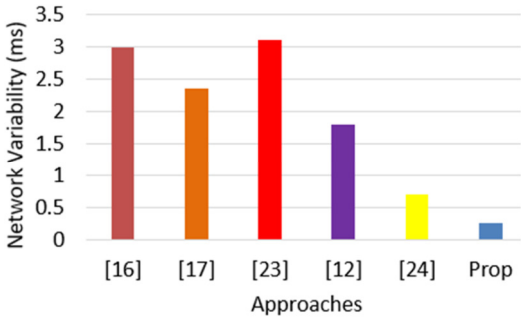

Fig. 8. Comparative analysis of network variability.

H. Analysis of Execution Time

This performance parameter evaluates the overall execution time of the proposed model. The idea was to assess the possible computational complexity associated with the duration of complete execution. Figure 9 shows that the proposed scheme offered an approximately 63% reduced execution time. One of the main reasons for the increased execution time is the inclusion of extensive variables involved in modeling as well

as the involvement of a higher number of iterative processes towards a secure payment system, as noted in [14, 15, 21, 22].

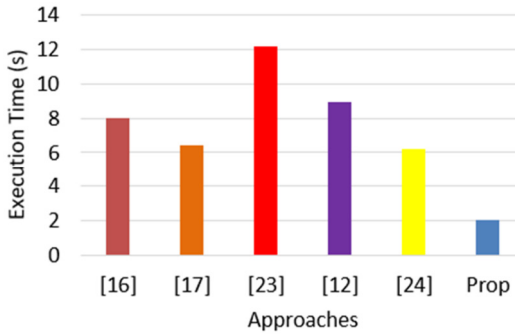

Fig. 9. Comparative analysis of execution time.

VII. CONCLUSION

This study introduced an innovative approach to the transformation of payment systems, particularly in regions affected by poor network connectivity. While Ethereum has become a prevalent choice for payment schemes, it is apparent that the prevailing state-of-the-art methods have primarily focused on deployment scenarios characterized by robust network connectivity in metropolitan areas, neglecting the pressing needs of regions beset by network limitations. The proposed scheme leveraged an analytical research method to address these challenges. It introduces a novel payment model embedded with fresh security attributes accompanied by the strategic deployment of multiple auxiliary nodes. These nodes serve as vital communication conduits, bridging the connectivity gap between areas struggling with substandard network links and Internet service providers. Users and residents of these underserved areas participate in a local blockchain network comprising ordinary users, merchants, and auditors. The method employs a streamlined mathematical approach to model auxiliary nodes' operational costs, transaction processing, and synchronization. A distinguishing feature of this model is its ability to manage auditor outages under varying network link conditions. Furthermore, an empirical evaluation of incentives for auditors has been undertaken to ensure the validation of each block while delineating minimal prerequisites for secure transactions. The core findings underscore its effectiveness, yielding an impressive array of results: an approximately 79% reduction in block processing time, a 28% increase in transaction throughput, a 30% reduction in energy consumption, a 68% decrease in confirmation time, and a 63% reduction in execution time.

This study significantly mitigates vulnerabilities in existing blockchain payment systems. It focuses on developing a novel, simplified, highly sustainable, and secure payment system using the Ethereum blockchain. The central contributions of this study include an innovative smart contract system designed to supervise crucial transactions and proficiently manage auditor incentives. Moreover, it introduces a fresh use-case deployment scenario that targets rural areas characterized by intermittent network connections, extending the reach of secure payment systems to these underserved regions. Looking ahead, the research trajectory builds on this model, as optimization-based algorithms can be explored across a diverse range of heterogeneous test cases along with exclusive entities to harness its full potential. The overarching objective is to facilitate a more secure, cost-effective, and efficient payment system, thereby profoundly impacting non-metropolitan areas grappling with inferior network coverage.

ACKNOWLEDGMENT

This research was partially supported by the INTI IU Research Seeding Grant Phase 1/2023 initiative under Project Number: INTI-FDSIT-02-01-2023.

REFERENCES

[1] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[2] B. U. I. Khan, K. W. Goh, M. S. Mir, N. F. L. Mohd Rosely, A. A. Mir, and M. Chaimanee, "Blockchain-Enhanced Sensor-as-a-Service (SEaaS) in IoT: Leveraging Blockchain for Efficient and Secure Sensing Data Transactions," *Information*, vol. 15, no. 4, Apr. 2024, Art. no. 212, https://doi.org/10.3390/info15040212.

[3] I. P. Suyatna, Y. H. Mohamed, M. S. Abbas, A. F. Ismail, M. M. Magiman, and Y. Yunus, "The Emergence and Challenges of Blockchain Technology in Business and IoT Applications," in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Greater Noida, India, May 2023, pp. 1136–1140, https://doi.org/10.1109/ICACITE57410.2023.10182600.

[4] D. Xu, Y. Gao, and X. Xiao, "Precision Poverty Alleviation Methods in the Agricultural Field Based upon Wireless Communication Networks and Blockchain," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022, Art. no. 2687445, https://doi.org/10.1155/2022/2687445.

[5] R. Weerawarna, S. J. Miah, and X. Shao, "Emerging advances of blockchain technology in finance: a content analysis," *Personal and Ubiquitous Computing*, vol. 27, no. 4, pp. 1495–1508, Aug. 2023, https://doi.org/10.1007/s00779-023-01712-5.

[6] P. Garg, B. Gupta, K. N. Kapil, U. Sivarajah, and S. Gupta, "Examining the relationship between blockchain capabilities and organizational performance in the Indian banking sector," *Annals of Operations Research*, Mar. 2023, https://doi.org/10.1007/s10479-023-05254-0.

[7] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021, https://doi.org/10.1007/s12083-021-01127-0.

[8] T. M. Tan and S. Saraniemi, "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," *Journal of the Academy of Marketing Science*, vol. 51, no. 4, pp. 914–939, Jul. 2023, https://doi.org/10.1007/s11747-022-00889-0.

[9] D. Costa, M. Teixeira, A. N. Pinto, and J. Santos, "High-performance blockchain system for fast certification of manufacturing data," *SN Applied Sciences*, vol. 4, no. 1, Dec. 2021, Art. no. 25, https://doi.org/10.1007/s42452-021-04909-6.

[10] X. Li and X. Shen, "Blockchain Technology-Based Electronic Payment Strategy for City Mobile Pass Cards," *Mobile Information Systems*, vol. 2022, no. 1, 2022, Art. no. 4085036, https://doi.org/10.1155/2022/4085036.

[11] S. I. Kim and S. H. Kim, "E-commerce payment model using blockchain," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 3, pp. 1673–1685, Mar. 2022, https://doi.org/10.1007/s12652-020-02519-5.

[12] I. Weber and M. Staples, "Programmable money: next-generation blockchain-based conditional payments," *Digital Finance*, vol. 4, no. 2, pp. 109–125, Sep. 2022, https://doi.org/10.1007/s42521-022-00059-5.

[13] S. Huang, L. Yang, X. Yang, X. Li, and F. Gao, "A Decentralized ETC Architecture Based on Blockchain Technology," *Journal of Advanced Transportation*, vol. 2021, no. 1, 2021, Art. no. 8848697, https://doi.org/10.1155/2021/8848697.

[14] A. Aljumah and T. A. Ahanger, "Blockchain-Based Information Sharing Security for the Internet of Things," *Mathematics*, vol. 11, no. 9, Jan. 2023, Art. no. 2157, https://doi.org/10.3390/math11092157.

[15] J. Partala, "Provably Secure Covert Communication on Blockchain," *Cryptography*, vol. 2, no. 3, Sep. 2018, Art. no. 18, https://doi.org/10.3390/cryptography2030018.

[16] D. Lin, J. Wu, Q. Xuan, and C. K. Tse, "Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction," *Physica A: Statistical Mechanics and its Applications*, vol. 600, Aug. 2022, Art. no. 127504, https://doi.org/10.1016/j.physa.2022.127504.

[17] J. Andrews, M. Ciampi, and V. Zikas, "Etherless Ethereum tokens: Simulating native tokens in Ethereum," *Journal of Computer and System Sciences*, vol. 135, pp. 55–72, Aug. 2023, https://doi.org/10.1016/j.jcss.2023.02.001.

[18] X. He, T. Yang, and L. Chen, "CTRF: Ethereum-Based Ponzi Contract Identification," *Security and Communication Networks*, vol. 2022, no. 1, 2022, Art. no. 1554752, https://doi.org/10.1155/2022/1554752.

[19] S. S. Bamber, "CrowdFund: CrowdFunding Decentralized Implementation on Ethereum Blockchain," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 3s, pp. 235–240, Feb. 2023.

[20] A. Laurent, L. Brotcorne, and B. Fortz, "Transaction fees optimization in the Ethereum blockchain," *Blockchain: Research and Applications*, vol. 3, no. 3, Sep. 2022, Art. no. 100074, https://doi.org/10.1016/j.bcra.2022.100074.

[21] A. Zarifis, "A Model of Trust in Ethereum Token 'Ether' Payments, TRUSTEP," *Businesses*, vol. 3, no. 4, pp. 534–547, Dec. 2023, https://doi.org/10.3390/businesses3040033.

[22] H. Zhao, X. Bai, S. Zheng, and L. Wang, "RZcoin: Ethereum-Based Decentralized Payment with Optional Privacy Service," *Entropy*, vol. 22, no. 7, Jul. 2020, Art. no. 712, https://doi.org/10.3390/e22070712.

[23] R. F. Olanrewaju, B. U. I. Khan, M. L. M. Kiah, N. A. Abdullah, and K. W. Goh, "Decentralized Blockchain Network for Resisting Side-Channel Attacks in Mobility-Based IoT," *Electronics*, vol. 11, no. 23, Jan. 2022, Art. no. 3982, https://doi.org/10.3390/electronics11233982.

[24] E. Kapengut and B. Mizrach, "An Event Study of the Ethereum Transition to Proof-of-Stake," *Commodities*, vol. 2, no. 2, pp. 96–110, Jun. 2023, https://doi.org/10.3390/commodities2020006.