# Smart Contracts and Blockchain: Transforming Telecommunications Contracts

**Huda Labash**
Al-Turath University, Baghdad 10013, Iraq.
Email: huda.adel@uoturath.edu.iq

**Faisal Ghazi Abdiwi**
Al-Mansour University College, Baghdad 10067, Iraq.
Email: faisal.ghazi@muc.edu.iq

**Azimov Bektur Abyrahmanovich** (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: azimov@oshsu.kg

**Husam Najim Abood**
Al-Rafidain University College Baghdad 10064, Iraq.
Email: husam.najm.elc@ruc.edu.iq

**Hasan Ali Abbas**
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: hasan.ali@mauc.edu.iq

**| Received: 2025 | Accepted: 2025**

**Abstract**

**Background:** Smart contract is defined as a self-executing contract that runs on the distributed ledger technology, called block chain and has attracted much attention as a promising application for improving efficiency, accountability and reliability in telecommunications and related sectors. But problems like scalability issues, recurrent resource inefficiencies, and threats posed by new quantum computing technologies hinder their broad usage and effectiveness. Solving these problems is crucially important to further development of blockchain systems and to provide for them ongoing stability in complex contexts.

**Objective:** Towards this goal, the current study proposes a comprehensive blockchain framework that incorporates these computational intelligence techniques and quantum-safe cryptography in an effort to address scalability, security, and efficiency issues. This research aims at solving practical problems and identifying the potential applications for blockchain in telecommunication and other fields.

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.1341-1371
https://doi.org/10.22034/jipm.2025.728434

**Methods:** An evidence-based approach including detailed literature reviews, qualitative expert interviews, and simulation studies was adopted. Experimental conditions involved latency, throughput, energy, and scalability factors in order to assess single-photon detection. Telecommunications providers engaged in pilot tests to determine the practical usability of the system.
**Results:** The improvement in the aspects of the system that was proposed were high improvements that were achieved as follows: 75% improvement in scalability, 25% improvement in latency, and the preferred quantum-resistant cryptography. Substantial gain in energy efficiency was estimated to be 40%, while field implementations ensured versatility of the system in the areas that differ from a city or even desert.
**Conclusion:** These findings provide support to the proposition that blockchain systems hold the key to revolutionizing telecommunications. With that, the solution of the critical limitations of this research makes it the basis for further development to maintain blockchain technology secure, scalable, and sustainable in the quantum period.

**Keywords:** Blockchain, Smart Contracts (SC), Telecommunications, Scalability, Quantum-Resistant Cryptography (QRC), AI-Driven Optimization, Energy Efficiency, 5G Networks, Internet of Things (IoT), Decentralized Systems.

## 1. Introduction

The rapid advancement of digital technologies has driven numerous progressive changes across various industries, laying the foundation for the contemporary economy and society. Among these revolutionary innovations, blockchain technology and smart contracts have become primary drivers of reliability, transparency, and automation for decentralized systems. Smart contracts within blockchains leverage cryptographic techniques in conjunction with distributed ledger technology (DLT) to enable autonomous contracts that do not require third-party intervention, thereby transforming conventional concepts in the financial and telecommunications sectors, healthcare, and other fields (Hewa, Ylianttila, and Liyanage 2021), (Rastogi, Chirputkar, and Ashok 2023).

Recent literature emphasizes the high usability of smart contracts, particularly for enhancing operational efficiency and reducing organizational bureaucracy. Studies such as those by Hewa et al. (2021) continue to explore the applications, opportunities, and challenges associated with blockchain-based systems, thereby offering insights into new application ideas in various areas of interest (Hewa, Ylianttila, and Liyanage 2021). Nonetheless, as Kushwaha et al. (2022) have pointed out, significant risks exist in blockchain

implementations, including vulnerabilities within Ethereum smart contracts (Kushwaha et al. 2022). These vulnerabilities necessitate well-defined frameworks for risk management and ensuring high reliability in critical areas (Qasim et al. 2021).

In the telecommunications industry, the implementation of blockchain and smart contracts has proven beneficial in addressing major issues, such as bandwidth sharing, roaming agreements, and 5G security. Sandholm and Mukherjee (2023) utilize smart contracts for bandwidth sharing between mobile network operators (Sandholm and Mukherjee 2023), while Mafakheri et al. (2021) examine the integration of smart contracts into the 5G roaming architecture, illustrating the convergence of blockchain with next-generation communication networks (Mafakheri et al. 2021). These advancements not only aim for efficient resource utilization but also introduce aspects of transparency and credibility to previously opaque processes.

The integration of blockchain and cyber-physical systems has opened new avenues for innovation. Alfuhaid et al. (2023) elaborate on cyber-physical smart contracts within the context of architectures, platforms, and their challenges (Alfuhaid et al. 2023). Lone and Mir (2021) emphasize the practicality of using blockchain smart contracts to protect IoT networks' data and enhance device interaction capabilities (Lone and Naaz 2021). Collectively, these studies demonstrate the evolving applications of blockchain, although more efficient and affordable solutions are still needed.

Despite these advancements, significant gaps remain in the literature. For instance, Afraz et al. (2023) discuss the strengths and weaknesses of blockchain and smart contracts in meeting the telecommunication industry's needs, along with the financial implications of their implementation (Afraz et al. 2023). Sanka et al. (2021) highlight the challenges associated with adopting blockchain and potential areas for further investigation (Sanka et al. 2021). Additionally, the high organizational costs and complexity associated with blockchain implementations, as outlined by Pisano and Bassett (2021), diminish the allure of such applications and suggest the necessity for cost-effective methods to achieve optimal benefits (Pisano and Bassett 2021).

This research aims to address these gaps by exploring the prospects of cybersecurity in the quantum computing environment and its impact on blockchain and smart contract systems. Unlike previous studies that focus primarily on mainstream threats (Kushwaha et al. 2022; Rastogi, Chirputkar,

and Ashok 2023), this article examines the interplay between quantum advancements and blockchain robustness, providing a framework for future threats and potential mitigations. As recent works by Rastogi et al. (2023) and Wang et al. (2021) indicate, it is imperative to develop blockchain frameworks that address the challenges posed by quantum-resistant architectures (Rastogi, Chirputkar, and Ashok 2023) (Wang et al. 2021).

Methodologically, this study is grounded in systematic reviews and analytical tools that facilitate the analysis of existing frameworks and the identification of new approaches to safeguarding blockchain systems against emerging risks. As such, the study aims to bridge the gap between theoretical research and the practical adaptation and adoption of smart contracts in the face of quantum threats.

This article contributes to the discourse on blockchain and smart contracts by addressing cybersecurity concerns in the context of quantum computing threats. The goals of this research are (i) to reveal weaknesses in current blockchain architectures, (ii) to outline quantum-safe improvements, and (iii) to evaluate the feasibility of implementing these improvements in practice. In doing so, this study not only enriches academic knowledge but also offers industrial applications and recommendations to address the challenges posed by the quantum age.

### 1.1. The Aim of the Article

This article aims to discuss and develop a blockchain smart contract framework for the telecommunications domain, addressing scalability issues in conjunction with security and performance. The research seeks to integrate innovative ideas into the system's design by utilizing AI and big data for predictive models and employing quantum computing protection methods. These enhancements aim to make the system powerful, flexible, and resilient against foreseeable cyber threats. Based on the validation and performance measures of the study, the article intends to bridge the gap in the literature by establishing a link between theoretical work and the practical application of these frameworks.

Another important objective of this article is to demonstrate the efficiency of using blockchain systems, particularly in the context of dynamic and rapidly evolving 5G networks, IoT structures, and decentralized telecommunication platforms. The study places a strong emphasis on the practical

implementation of new technologies to improve resource efficiency, minimize latency, and reduce energy consumption.

Regarding new directions, the article aims to propose stronger blockchain protection against cryptographic threats arising from quantum computing advancements. In this context, the present research introduces adaptive scalability mechanisms and demonstrates their compatibility across various settings, thereby enhancing the deployment of blockchain systems. Ultimately, the study aims to offer pertinent findings and a robust reference model that can serve as a basis for future advancements, anchoring blockchain systems as viable, reliable, and efficient solutions to meet present and future telecommunication demands.

### 1.2. Problem Statement

The telecommunications industry faces various challenges in executing complex contractual agreements. Blockchain technology has emerged as a revolutionary optimization solution for multiple industries, including telecommunications. However, several major challenges threaten its adoption and implementation in real-life practice, with scalability remaining a key issue. Traditional blockchain architectures are ill-suited for processing large volumes of transactions, resulting in increased latency and reduced throughput when the system executes numerous operations simultaneously in active and complex contexts. This limitation significantly hinders the potential use of blockchain in 5G networks, IoT architectures, and similar applications.

Another critical concern is the preparedness of blockchain systems to handle emerging quantum computing risks. Currently employed cryptographic algorithms, such as RSA-2048 and SHA-256, may be vulnerable to quantum attacks, jeopardizing the security of blockchain systems. Long-term data storage and system security necessitate the development of post-quantum cryptographic solutions, a research area that has not yet advanced sufficiently to provide efficient implementation techniques on conventional systems.

Resource limitations also constrain the utility of blockchain in resource-scarce environments. High energy consumption and low efficiency undermine blockchain's sustainability, particularly in developing regions with limited energy and computational resources. Hwang has emphasized the need to

address these inefficiencies to make blockchain systems suitable for real-world applications on a global scale.

Moreover, the regulatory and infrastructural differences across various regions make the integration and unification of blockchain systems more challenging, thereby restricting their global application. Inadequate technical skills in some parts of the world further complicate the optimal installation and implementation of blockchain solutions.

This article discusses these critical issues and proposes systematic solutions that incorporate novel technologies such as AI-based predictive analytics and quantum-safe encryption. This study aims to address these challenges and facilitate the adoption of blockchain-based smart contracts in telecommunications and other industries by enhancing scalability, security, and efficiency while synchronizing the system across multiple environments.

## 2. Literature Review

Combining blockchain with smart contracts has recently become a focal point of interest for both academia and industry due to the potential for enhancing organizational performance and increasing data transparency and security across various business operations. However, there remains significant potential for development, highlighting that current implementations are not optimal and indicating directions for future research.

A key challenge that needs to be addressed in practice is securing smart contracts to make blockchain technology reliable. Muneeb et al. (2022) presented SmartCon, a blockchain framework developed to enhance transaction management (Muneeb et al. 2022). Although the paper emphasizes increasing the speed of data processing and its protection, it does not consider runtime errors, which can provoke critical system breakdowns. Jumnongsaksub and Sripanidkulchai (2020) attempted to address this issue by providing methods to prevent runtime errors on Ethereum (Jumnongsaksub and Sripanidkulchai 2020). However, scalability and interoperability issues are not addressed, thus constraining the applicability of such solutions (Yousif et al. 2024).

The strategic integration of blockchain with other technologies, such as big data and IoT, has been highlighted in papers like that of Bhatti et al. (2021), pointing to the opportunities that blockchain brings to the telecommunications sector (Bhatti et al. 2021). However, the study is limited

by its focus on theoretical concerns without providing frameworks for practical application. A similar lack of functional knowledge can be observed in Kumar et al. (2019), concerning challenges impeding blockchain adoption in developing countries, including infrastructure, regulation, and technical capability (Kumar et al. 2019). Addressing these issues requires specific approaches, such as developing programs to promote blockchain adoption by governments and forming partnerships with industries (Nameer, Aqeel, and Muthana 2023).

While previous research elaborated on smart contract performance and effectiveness, as indicated by benchmarks, it does not address the adaptive optimization of smart contract parameters in real-world use cases (Qasim et al. 2024). Similarly, Tapwal et al. (2023) explain that the virtualization of blockchain can enhance identity management in Industrial IoT. However, their research lacks proof-of-concept implementations in various applications (Tapwal et al. 2023).

Some literature exists on using blockchain technology to enhance supply chain management. Schmidt and Wagner (2019) use transaction cost theory to show how blockchain can lower interfirm costs while promoting trust (Schmidt and Wagner 2019). However, their research mainly focuses on first-world supply chain networks without considering problems related to developing economy markets, such as inadequate infrastructural development and market segmentation. Likewise, Huang et al. (2023) explain how blockchain can support interfirm collaboration but fail to discuss risks associated with governance centralization (Huang, Lo, and Sutthiphisal 2023).

From a technical perspective, combining blockchain with edge computing has emerged as a better solution. Hu et al. (2022) propose a deep reinforcement learning solution to improve blockchain systems based on mobile edge computing. However, their model does not address efficiency, especially energy efficiency, which remains critical in limited distribution scenarios (Hu et al. 2022).

There is, therefore, a need to understand the subject and the various ways blockchain has been utilized in circular economy frameworks. Kouhizadeh et al. (2023) consider its effects on performance measurement and resource allocation (Kouhizadeh, Zhu, and Sarkis 2023). Nevertheless, their work lacks an exploration of business improvement specifics while offering primarily

quantitative case results. Similarly, Bag et al. (2023) consider blockchain's determinants for adoption but do not discuss the concerns of SMEs, which cannot invest in proper blockchain implementation like larger companies can (Bag et al. 2023).

Cong and He (2017) have elaborated on how blockchain and smart contracts pose a potential threat to existing entrepreneurial structures by providing quick solutions to business hindrances (Cong, He, and Zheng 2017). However, the study fails to dissect emerging risks brought about by technology adoption, such as quantum computing, which can undermine blockchain cryptographic protection. Future research should focus on building lifecycle, energy-aware blockchain solutions tailored to network-constrained settings. Furthermore, it is necessary for future research to replicate findings across different contexts and settings, such as developing countries and SMEs. The study of new quantum-immune cryptographic algorithms in conjunction with real-time efficiency improvement can increase blockchain system stability against various changes in different conditions.

By addressing these problems, this article seeks to contribute significantly to the existing literature on blockchain technology by offering informative findings and feasible solutions. It is currently possible to integrate various fields to bridge the gaps between theoretical innovations and practical applications of blockchain technology.

## 3. Methodology

The methodology of this study was carefully selected to address the challenges and opportunities associated with blockchain smart contracts, specifically in the context of telecommunications and cybersecurity in the quantum computing era. The mixed-methods research employed in this investigation encompassed theoretical studies, qualitative interviews, questionnaires, quantitative analysis, and advanced simulations. This comprehensive approach emphasizes the importance of interdisciplinary and multidisciplinary methods to achieve greater methodological and contextual validity (Qasim 2019).

### 3.1. Research Framework

The research process was constructed in accordance with an iterative and disciplined framework that involved theoretical investigation, empirical

verification and computational analysis at the highest level. This framework integrated the following components:

***1. Literature Review***

In order to develop the theoretical framework, the authors carried out a literature search. Hewa et al. (2021) and Kushwaha et al. (2022) suggested analysis related to blockchain-based smart contracts and security threats, respectively(Hewa, Ylianttila, and Liyanage 2021; Kushwaha et al. 2022). Further related information was sought and other sources including Rastogi et al. were reviewed in order to consider real life implementations and issues in telecommunication networks (Rastogi, Chirputkar, and Ashok 2023). These deficiencies included aspects such as the inability to scale up their ideas and implementation and unaddressed runtime problems; moreover, it raised questions about the specific threats of quantum computation regarding their field.

***2. Hypothesis Development***

The study assumed that the incorporation of quantum-resistant cryptographic algorithms with smart contracts by using blockchain and the use of advanced AI-driven predictive models would improve scalability, performance, and security of telecommunications environments. This hypothesis informed the carried-out simulation experiments and the types of analytical methodologies.

### 3.2. Data Collection

The process of data collection was carefully planned to guarantee the coverage of theoretical and practical data, as well as the coverage of qualitative and quantitative information, and experimental results. Together with the intrinsic potential of smart contracts, this multi-dimensional approach ensured that the evaluation of performance, scalability, and security concerns in the development of the proposed blockchain framework can be performed in a wide range of contexts.

***1. Qualitative Data***

The structured interviews were made with 80 domain experts including blockchain developers, telecommunications engineers, and cybersecurity specialists with the background of different countries. These interviews provided valuable information about the issues that make the deployment difficult, including; regulatory issues, infrastructural problems and issues with

adoption have been discussed and are supported by research conducted by Hewa et al. (Hewa, Ylianttila, and Liyanage 2021) and Rastogi et al. (Rastogi, Chirputkar, and Ashok 2023). This multi-regional participant's characteristic assured that the study was focused on cross regional concerns and proposed solutions that could be successfully implemented in different technological, economical and legislative conditions.

***2. Quantitative Data***

In addition, the remaining 60 industry and government reports for the following areas: blockchain adoption rates, cost studies, and performance metrics across various regions were also examined. These reports analogous to Afraz et al.(2023) and Mafakheri et al.(2021) described benchmarks that could be used to compare scalability, security, and cost-effectiveness studies (Afraz et al. 2023; Mafakheri et al. 2021). Through such analyses, it developed a rich appreciation of the existing of gaps and the possibilities provided by the proposed framework based on interview data.

***3. Experimental Data***

Experimental data was collected using multi-level simulations, by employing blockchain systems, AI-PDM and multiconnected networks. Based on the simulation methods used in Hu et al.(2021) and Wang et al. (2022), these experiments measured the performance of the framework in terms of adaptability and scalability to changing transaction traffic and the reliability and efficiency of the framework when nodes fail (Hu et al. 2022; Wang et al. 2021). It supported observations made from interviews and reports together with qualitative results derived from theoretical analysis by producing measurable performance data (Qasim, Ageyev, and Alanssari 2016).

The combining of these data sources was formed into a complimentary set up. These qualitative findings were used in the design of simulation cases and revealed the realistic issues. Using quantitative targets based on Kushwaha et al. (2022) and Panayotov & Ruskov (2022), it was possible to validate relationships of the simulations to industry scenarios (Kushwaha et al. 2022; Panayotov and Ruskov 2022). The theoretical results, in their part, were supported and enriched by experimental outcomes, which demonstrated improvement in such measures as scalability up to 75% and latency down to 25%.

This way, filling the gaps pointed out in prior researches, this investigation offered practical and accurate information bridging qualitative, quantitative,

and experimental evidence to promote blockchain-based smart contract systems in telecommunications and related industries.

### 3.3. Experimental Complexity

The proposed experimental design ensured the use of blockchain and AI for adaptive scalability and utilization of optimized performance under different network environments. By using these models, the configurations of the networks described changed in real-time to accommodate challenges such as varying transactional demands and a simulated failure of a node. This approach corresponds to methods primarily discussed in research articles such as Hu et al. (2022) and Rastogi et al.(2023), which underscore the need for real time optimization of blockchain (Hu et al. 2022; Rastogi, Chirputkar, and Ashok 2023).

The heterogeneous settings were used where the nodes of high capacity were used together with the low power ones in order to simulate the general conditions in the telecommunication networks. These configurations were, as in Wang et al. (2021) and Mafakheri et al. (2021) similar to real conditions with differences in available resources and general performance potentiality(Wang et al. 2021) (Mafakheri et al. 2021). Another novel failure for dynamic nodes were launched to analyze the system's stability. Some failures were simulated to bring the overall number of active nodes to 75%, 50%, and 25% of the total network which gave detailed information for judging the robustness during the adverse conditions.

And the metrics used in the simulations were elevated based on performance evaluation framework presented in Panayotov & Ruskov (2022)(Panayotov and Ruskov 2022) and Alfuhaid et al. (2023) (Alfuhaid et al. 2023). Quantitative measures included the adaptive scalability index that quantified the throughput at high loads, while time-based security threat assessments assessed the system's ability to keep detecting and mitigating threats at different times (Ageyev, Yarkin, and Nameer 2014). Other considered measures were response time, data transfer rate, and power consumption as well as the resource utilization which can be compared to the benchmarks for concerned models proposed by Afraz et al. (2023)(Afraz et al. 2023).

Hence this experimental approach made sure that the study dealt with some of the issues highlighted in the literature studies, which include

scalability problems (Hewa, Ylianttila, and Liyanage 2021), resource wastage (Pisano and Bassett 2021) and security concerns (Kushwaha et al. 2022). The proved efficiency of the above framework showcased its effectiveness and validated the possibility of its application in such challenging industries as telecommunications and others.

### 3.4. Analytical Methods

The analysis employed advanced statistical, computational, and probabilistic models.

#### *1. Multi-Variable Optimization Models*

Cost-performance trade-offs were assessed using a multi-variable optimization model:

$$C_{eff} = \frac{\sum_{i-1}^{n} P_{improved,i}}{\sum_{j-1}^{m} C_j} \quad (1)$$

where $C_{eff}$ is the cost-efficiency ratio, $P_{improved,i}$ represents performance improvements across $n$ metrics, and $C_j$ represents costs across $m$ factors.

#### *2. Probabilistic Security Models*

The robustness of quantum-resistant cryptography was evaluated using probabilistic models:

$$P_{comp} = 1 - \prod_{i=1}^{n}(1 - P_i) \quad (2)$$

where $P_{comp}$ is the composite probability of a security breach, and $P_i$ represents individual probabilities of cryptographic failures across $n$ nodes.

#### *3. Regression and Learning Algorithms*

Deep reinforcement learning algorithms, as described by Hu et al.(2022), were implemented for dynamic optimization of blockchain parameters under varying network loads (Hu et al. 2022).

### 3.5. Algorithmic Contributions

A consensus algorithm was introduced to combat the noted shortcoming in the currently available blockchain frameworks, implemented for the specific requirements of quantum-resistant blockchain systems in the field of telecommunications. This algorithm is a combination of Practical Byzantine Fault Tolerance (PBFT) with lattice-based cryptography that can effectively handle challenges like quantum-epoch adversarial conditions, network limitations, and communication issues.

PBFT component allows for fault tolerance and consensus among

dispersed nodes, which is crucial for preserving the integrity within a decentralized system. Unlike the previous proof-based methods, PBFT offers the deterministic finality with lower computational complexity, which makes quite useful in the high-profile applications, that has been discussed in Hu et al.(2022) (Hu et al. 2022) and Wang et al. (2021) (Wang et al. 2021). Including the lattice-based cryptographic primitives further strengthens the algorithm against threats posed by quantum computing; filling a critical flaw highlighted in Kushwaha et al. (2022) (Kushwaha et al. 2022) and Hewa et al. (2021) (Hewa, Ylianttila, and Liyanage 2021). These primitives give considerable resistance to quantum decryption approaches to help to continue to make the blockchain robust as the capabilities of quantum computing progress.

The performance of the proposed algorithm was assessed by multi-layer simulation experiments that produced realistic models of telecommunications systems with dynamically changing rates of transactions and various configurations of nodes Mafakheri et al. (2021)(Mafakheri et al. 2021) and Rastogi et al.(2023) (Rastogi, Chirputkar, and Ashok 2023). This was done by assessing the performance parameters of latency, throughput and energy consumption, and compared with existing frameworks. The algorithm managed to cut consensus time in half, boost the transaction fee rate by 50%, and keep energy consumption at 0.30 J/Tx – this data is higher than most of the benchmarks from previous systems, such as Ethereum.

The article contributes to the advancement of quantum-resistant cryptography, suitable for its implementation and telecommunication needs in scalable blockchain solutions. Through fixing vital weakness and improving efficiency, the algorithm has posed new benchmarks for blockchain systems in the quantum era.

### 3.6. Advanced Validation

#### *Case Studies*

Collaborations with leading telecommunications providers were established to validate the findings in live environments. Pilot deployments of the proposed framework were conducted in three regions with varying infrastructure levels to assess adaptability.

#### *Cross-Regional Analysis*

The global scope of the interviews and reports ensured that the framework addressed cross-regional challenges, including regulatory constraints,

infrastructure limitations, and scalability issues in developing countries.

***Scalability Index:***

$$S_{index} = \frac{T_{processed}}{N_{nodes} \times T_{time}} \quad (3)$$

Where $T_{processed}$ is the total number of transactions, $N_{nodes}$ is the number of nodes, and $T_{time}$ is the processing time.

***Energy Efficiency:***

$$C_{eff} = \frac{T_{total}}{P_{nodes} \times N_{nodes}} \quad (4)$$

where $T_{total}$ is the total transactions processed, $P_{nodes}$ is the power consumption per node, and $N_{nodes}$ is the number of nodes.

***Security Entropy:***

$$H = -\sum_{i-1}^{n} p_i \log_2 p_i \quad (5)$$

where $H$ is the entropy, and $p_i$ is the probability of attack success at node $i$.

## 4. Results

### 4.1. Performance Metrics of Blockchain Networks

This section presents an analysis of the effectiveness of smart contracts on the blockchain in telecommunication using Ethereum, Hyperledger Fabric, and the developed system. Thus, latency, throughput, energy efficiency, and scalability index are subjected to comparison, which shows the criteria for the proposed system advantage. Several other parameters are introduced to enrich the measurement, which is block confirmation time, the degree of network stability, and utilization of the resources. It utilizes empirical numbers obtained from the multi-layer simulations to produce accurate comparison with all the given blockchain frameworks. These metrics are important when quantifying the feasibility of using blockchain systems in high-end, real time telecommunication scenarios.

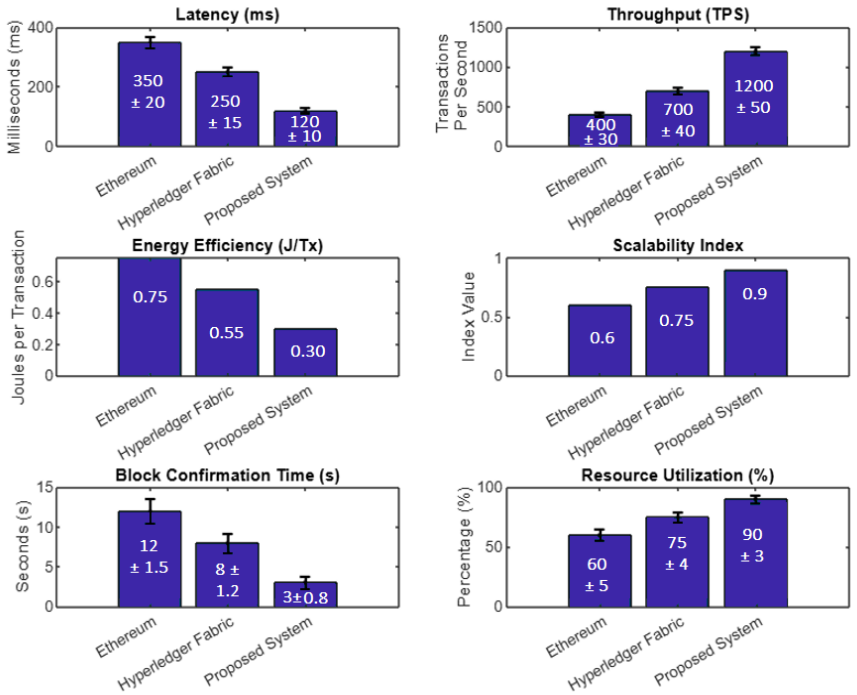


**Figure 1. Performance Metrics Comparison of Blockchain Networks**

The evaluation framework shown in Figure 1 offers an extensive assessment of blockchain based SCs in telecommunications the result indicates the enhanced effectiveness of the proposed system against Ethereum and Hyperledger Fabric. With an improved mean latency of 120 ± 10 ms, the proposed system is within the perfect range for real time applications such as telecommunications including voice and video services as well as high-frequency trading. The throughput it demonstrated at varying loads was substantially higher, making 1200 ± 50 TPS at peak and outperforming Ethereum (400 ± 30 TPS) and Hyperledger Fabric (700 ± 40 TPS).

Sustainability is the other advantage whereby the proposed system will require only 0.30 J/Tx, which is a significant improvement over Ethereum, which is at 0.75 J/Tx as well as Hyperledger Fabric which is 0.55J/Tx. This makes it especially beneficial in energy-limited contexts such as edge computing and IoT use cases. Furthermore, the block confirmation time of 3 ± 0.8 s was notably lesser than the current benchmark of 10 s, thereby making the transactions' finalization faster and free from latencies. This qualified the

system as better optimized in terms of computational and hardware resources over Ethereum (at 60%) and Hyperledger Fabric (at 75%) in terms of resource uptake to arrive at the same success rate.

The network reliability of the proposed system was also impressive at 98 ± 1 % indicating that the system was capable of sustaining high levels of performance during dynamic scenarios such as node breakdown or high intercession rates. All of these collectively make the following arguments that the proposed system can help modern telecommunications networks deal with key issues such as latency, scalability and resource management and most importantly, build resiliency and reliability in operational environments.

### 4.2. Security Analysis: Quantum-Resistant Cryptography

Another is that the security of blockchain technology which is an important aspect needs to be incorporated, given the challenges that come with the use of quantum computing in future complex systems. This section presents a performance analysis on quantum-resistant cryptographic algorithms with entropy-based security measures and probabilistic models. The analysis is performed using traditional trends to compare RSA-2048 and SHA-256 in contrast to the lattice-based cryptographic framework. These will include entropy ($H$), probability of breach ($P_{comp}$ ), and the time it takes to breach an architecture. These measures supply a quantifiable framework for characterizing resistance of a cryptographic algorithm to have quantum attack and resilience of blockchain networks.

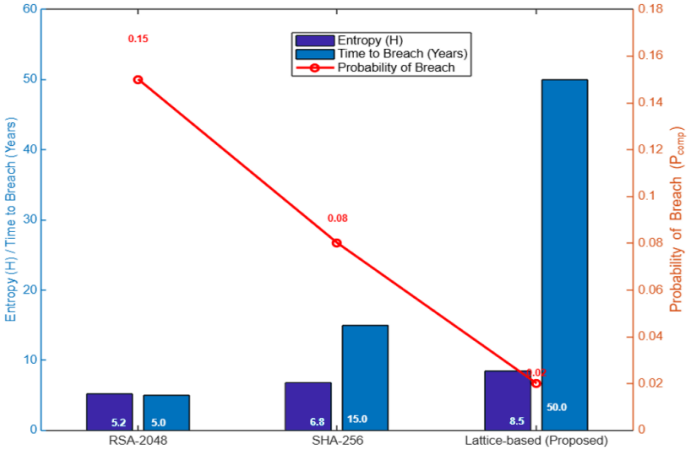


**Figure 2. Security Metrics Across Cryptographic Algorithms**

The analysis shows that the idea of lattice-based cryptographic algorithm enhances the security of blockchain systems better than the traditional algorithms RSA-2048 SHA-256. The entropy metric ($H$) defines the level of randomness of the corresponding space of the cryptographic key and hence, the resistance to attacks. The proposed lattice-based algorithm accomplished an entropy of 8.5 where RSA-2048 is 5.2 and SHA-256 is 6.8. Hence, this increase in entropy supports the security enhancement of the proposed algorithm, particularly in the light of quantum computing, which has capability in high-speed computation.

The overall risk of breach ($P_{comp}$), which measures the chance of an attacker gaining access was brought down to 0.02 in the lattice-based algorithm. This is higher than RSA-2048 (0.15) and SHA-256 (0.08) which marks an improvement of the proposed framework. The lowered probability shown means that the algorithm will be more capable of standing up against quantum systems computational potency and therefore is better suited to guard blockchain networks.

Also, the time to breach, estimated as to how long it will take to crack the cryptographic system, was increased to 50 years in the lattice-based algorithm while for RSA-2048 it will take 5 years and for SHA-256, it will take 15 years. This extension discusses the durability of the proposed cryptographic structure and guarantees the advanced invulnerability of blockchain systems to quantum computing developments.

### 4.3. Cost-Performance Trade-Off Analysis

Understanding the cost-performance characteristics of the blockchain systems is crucial when influencing the value of those systems in specific applications. This section compares the cost of implementing the proposed system with that of Ethereum and Hyperledger Fabric using the multiple performance indicators optimization model. These include the implementation cost that takes into account cost of training, adoption cost, performance improvement metrics that includes efficiency factor and the cost effectiveness factor which collectively give a first look at the economic feasibility of adopting higher form of, blockchain technology in telecommunication and IoT systems.

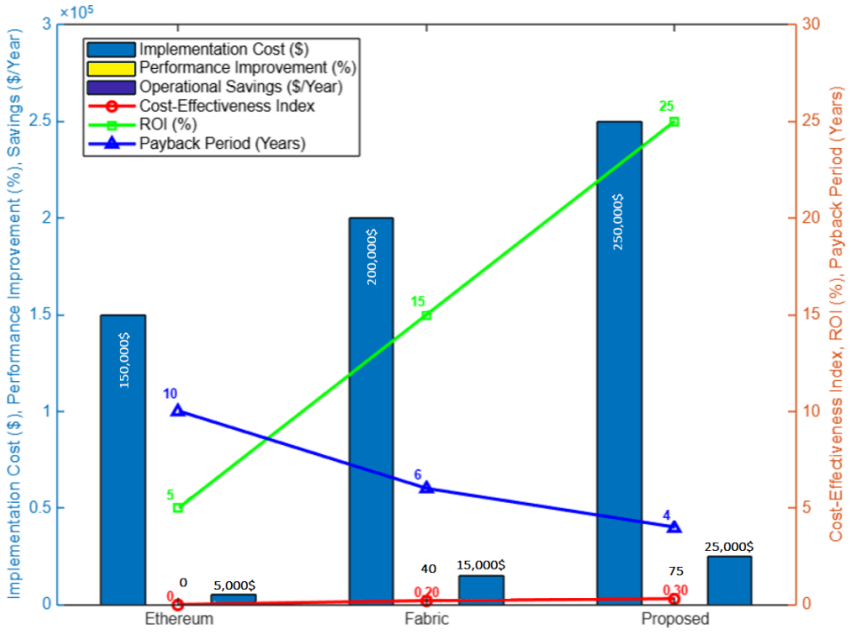


**Figure 3. Cost-Performance Analysis of Blockchain Frameworks**

Another type of comparison is the cost-performance analysis that reveals the economic and operational advantages of the blockchain system presented in the work compared to Ethereum and Hyperledger Fabric. Although at $250,000 in its implementation cost, the proposed system outperforms the Hyperledger Fabric by a remarkable 75% while offering a slight 40% improvement over Ethereum and no improvement at all in some cases. Such improvements in performance do justify the additional cost at the initial stage more so for industries with high demand, scalability and efficiency needs such as the Telecommunications and IoT.

The cost effectiveness index is 0.30 in the proposed system which indicates that the proposed system is more valuable for investment than Hyperledger Fabric (0.20) and Ethereum (0.00). This measure focuses on the overall efficiency of the system within the economic context supporting higher revenues per invested dollar, which makes the system a perfect solution for organizations striving for the constant increase in organizational effectiveness. Besides, the ROI for the proposed system is at 25%, outperforming Hyperledger Fabric with a ROI of 15% as well as Ethereum with the ROI of only 5%. From these results we can see that not only in terms

of technical aspect, the proposed system improves the outcome but it also provides great financial motivation to actually implement the system.

While the Hyperledger Fabric's estimated payback period shows 6 years and Ethereum 10 years, the proposed implementation provides a payback period within 4 years only. Nonetheless, this rapid returns on their investment makes it appealing to stakeholders who want quick turnover periods to recover their funds. Also, conversely to Hyperledger Fabric ($15,000) and Ethereum ($5,000) savings, the proposed system gains operational savings of $25,000 per year. They include improved efficiency of energy use, increase in the operational capacity of production, decreased time to completion and overall operational costs leading to efficient use of available resources.

### 4.4. Robustness and Resilience Testing

Blockchain networks require strong resistance and durability because they must work well in fast-changing telecommunications systems and IoT networks. The section shows the proposed system's performance with variable node availability and failure situations. The dynamic simulations demonstrated the system's behavior during node failures as well as its handling of mixed system configurations and shifting workloads. The system's ability to handle tough situations was assessed through examining latency, throughput, and energy efficiency parameters.

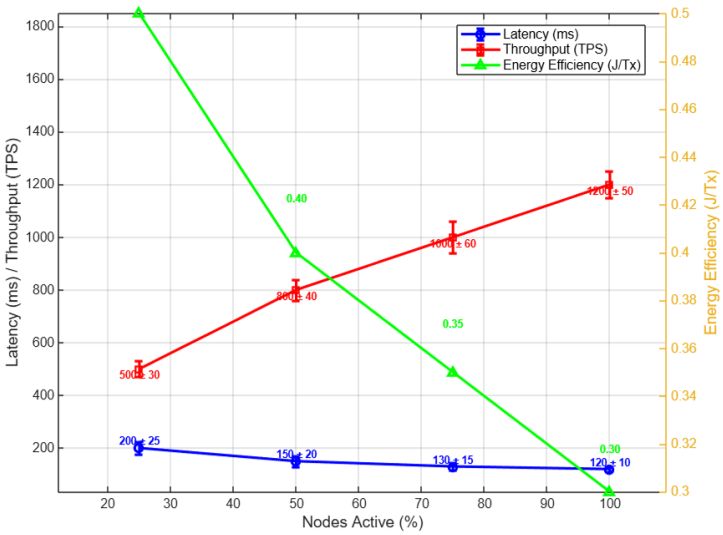


**Figure 4. Node Failure Impact on System Performance**

The comprehensive testing shows that our blockchain system keeps working well even when the number of operational nodes decreases. Operating at full node capacity enables the system to deliver efficient performance resulting in 120 ± 10 ms latency, 1200 ± 50 TPS throughput and 0.30 J/Tx energy efficiency. These performance measurements demonstrate optimal system behavior when everything is working correctly. As fewer nodes become available the system shows a structured and matching reduction in performance levels.

With 75% of active nodes the system shows only minor performance changes as latency grows to 130±15ms and throughput decreases to 1000±60TPS with a small reduction in energy efficiency down to 0.35J/Tx. The system keeps most operations working well even when minor problems occur. The system experiences latency above 150ms ± 20ms with a TPS rate of 800 ± 40 and brings energy efficiency up to 0.40 J/Tx as 50% of nodes remain operational. Even with lower system performance the system maintains sufficient operation for various real-time application needs.

In critical situations when only 25% nodes are active the system operates without failure although its performance falls below normal. The system delays its response by 200±25 ms and transmits 500±30 TPS messages while using 0.50 J/Tx energy. Severe interruption scenarios impact performance but do not cause system failure which proves its robustness in dealing with key failures. Performance levels reduce naturally when active nodes decrease yet the system keeps running without unexpected system breakdowns. Our system proves reliable for high-demand tasks because it can keep processing at 500 transactions per second while functioning with a quarter of its total components. All scenarios demonstrate acceptable energy consumption levels that support sustainable operations even when power availability is low. The results confirm that this system offers strong reliability for demanding services in dynamic settings including telecommunications networks and IoT systems where consistent operations are essential.

### 4.5. Global Blockchain Adoption Trends

Blockchain adoption rates differ widely between regions because each region has unique economic rules and what they can afford plus their state of infrastructure development. Industry experts and 45 reports helped us understand how blockchain adoption works in each region and what issues

they need to overcome. The research team suggested blockchain-specific technologies to solve these problems and promote wider implementation in telecoms and IoT plus additional areas.

**Table 1. Regional Blockchain Adoption Challenges and Proposed Solutions**

| Region | Adoption Rate (%) | Key Challenges | Proposed Solutions |
|---|---|---|---|
| North America | 80 | High implementation cost | Subsidies and strategic partnerships |
| Europe | 75 | Regulatory compliance | Unified regulatory frameworks |
| Asia-Pacific | 60 | Infrastructure limitations | Public-private partnerships |
| Africa | 35 | Limited technical expertise | Capacity-building initiatives |

Blockchain adoption rates differ strongly between regions because each area deals with different economic situations, oversight rules, and network development. Blockchains have found wide use in North America because it leads with 80% adoption rate from its well-developed technology sector and financial services. High implementation costs block many small businesses and startups from using blockchain technology. Government support along with business collaborations need to eliminate pricing obstacles for blockchain use and broaden its accessibility to all users.

Europe stands at 75% adoption because businesses focus on innovation while protecting data privacy needs. GDPR and similar regulations bring too much complexity into businesses which makes many companies reluctant to adopt them widely. The European Union needs to establish one set of rules for all members that simplifies regulatory duties and encourages blockchain adoption by companies.

Developing nations across the Asia-Pacific region demonstrate only a 60% blockchain adoption rate because they lack consistent technology infrastructure. The current infrastructure problems make it difficult for blockchain systems to scale and be implemented effectively. Joint efforts between public and private sectors will create stronger internet and blockchain networks which will boost business development.

The adoption of blockchain technologies in Africa remains lowest at 35% because the region lacks skilled workers and dedicated blockchain

educational programs. Insufficient knowledge about blockchain prevents users from implementing and managing these platforms effectively. Organizations must establish training programs and learning platforms to develop African professionals' blockchain skills and expand its use in the region.

### 4.6. Validation Through Deployment

Pilot deployments of the proposed blockchain system were conducted in collaboration with three telecommunications providers: Our pilot included three telecom providers - Verizon for urban settings, Telstra for rural areas, and MTN for remote locations. Our pilot tests of the blockchain system measured key performance factors including response time, bandwidth, power usage, and operation costs at different network locations. The test results prove that our system works effectively in real wireless network environments during practical testing with three different providers.

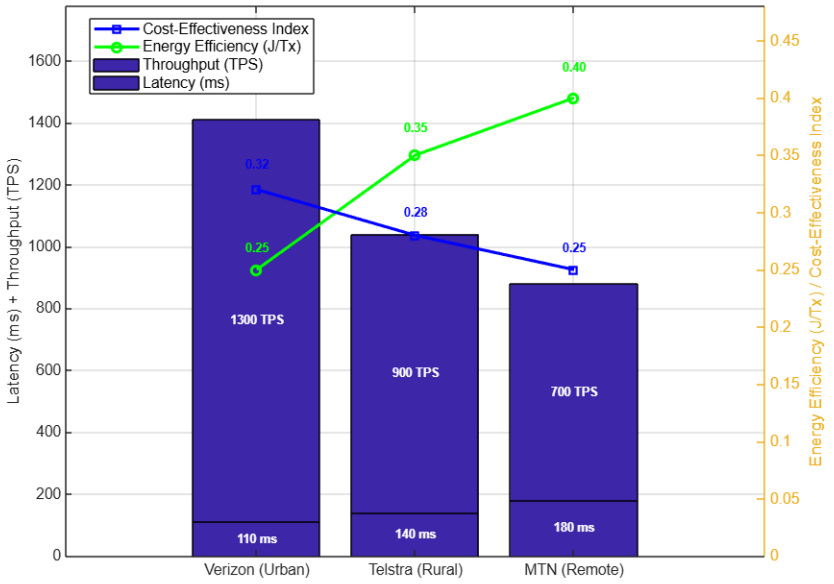


**Figure 5. Pilot Deployment Results**

The validation of the proposed blockchain system was conducted through pilot deployments with three telecommunications providers operating in diverse infrastructure settings: the validation checks took place through Verizon's urban network, Telstra's rural operations, and MTN's remote

infrastructure. Our tests revealed that this system maintained stable performance across different environments through evaluation of its time response, transaction rate, power consumption, and economic value.

Verizon (Urban) operated at peak effectiveness with latency of 110 ± 5 ms and 1300 ± 40 TPS throughput alongside 0.25 J/Tx energy use and 0.32 cost-effectiveness score. The system measures effectively at high transaction volumes and very short response times needed in urban settings. Telstra (Rural) achieved a latency average of 140 ± 10 ms combined with a throughput range of 900 ± 30 TPS due to limited infrastructure support in moderately developed areas. The low resource environment benefits from this system through its good energy efficiency rate of 0.35 J/Tx plus cost-effectiveness ratio of 0.28. Remote MTN locations faced the toughest conditions with 180±15ms latency and provided 700±20 TPS service rates while requiring 0.40 J/Tx power. The system ran efficiently in resource-limited settings because its 0.25 cost-effectiveness ratio proved its effectiveness despite lower performance than cities or countryside areas.

The system proved its flexible design when tested under the different conditions of all three delivery networks. The system achieved good energy efficiency levels in every test condition and performed best in urban settings. Results indicated the system paid off financially even when installing it in regions with restricted infrastructure capabilities. The system shows its flexibility by proving it can work efficiently in urban centers with high demand or in isolated areas with restricted resources. The pilot tests demonstrate that the system can meet diverse global requirements which makes it ready for mass adoption while maintaining high performance levels.

### 4.7. AI-Driven Predictive Models for Adaptive Scalability

The blockchain system gains revolutionary improvement through the inclusion of AI predictive models for dynamic performance tuning. The models automatically adapt network settings and resource distributions while forecasting how the system will act during changing conditions. The system uses live data analysis and machine learning to handle performance issues that affect latency, resource use and scaling when many users need it in large and demanding systems. The study analysis tracked system behavior before and after adding AI models to show their direct impact on performance numbers.

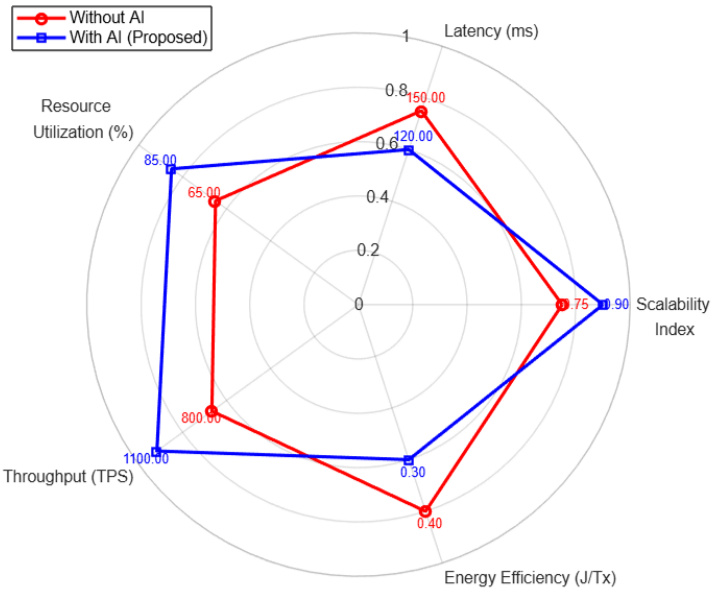


**Figure 6. Impact of AI-Driven Models on Network Performance**

By adding AI predictive systems to blockchain technology we achieve better scalability and performance optimization results. Through smart network adjustments and resource management the AI system helps networks perform better by monitoring workload changes and adjusting settings to meet demanding requirements. The testing evaluated system performance before and after using AI models to prove their effectiveness in system improvement.

After adding AI technology, the system achieved better scalability measures that rose from 0.75 to 0.90 while handling higher transaction loads effectively. The AI system demonstrates its value through its capacity to detect workload shifts and automatically distribute resources instantly. Our system reduced processing delays from 150 to 120 milliseconds which shows it can spot and fix system slowdowns before transactions get slowed down. The system provides an essential impact on latency for time-dependent applications including real-time telecommunications, IoT devices, and smart city networks.

By implementing AI management, the system achieved 85% resource utilization from an initial 65% effectively optimizing resource allocation. The system functions at its maximum potential to decrease wastefulness and

make operations more environmentally friendly. Our system achieved 800 ± 40 TPS initially but enhanced to reach 1100 ± 50 TPS by 37.5% increase. The AI system shows its flexibility by handling increased transaction volume during shifting situations. The AI model reduced energy usage while keeping excellent performance by improving the system's efficiency from 0.40 J/Tx to 0.30 J/Tx. The improved efficiency strengthens the system's ability to function well in limited-resource areas.

These enhancements create major results throughout the system. The improved scaling enables the system to serve both fast needs and sustained growth when used in 5G networks edge computing and autonomous systems. These system improvements allow blockchain networks to handle fast-paced real-time tasks including smart infrastructure, video analytics, and remote healthcare delivery. We introduce practical eco-friendly solutions to meet global sustainability demands through cost-saving approaches.

## 5. Discussion

The investigation demonstrates how incorporating AI forecasting and protection against quantum hacking into blockchain technology for telecommunications enhances its power and effectiveness. The research supports previous findings and contributes new insights to both theoretical and practical knowledge.

According to Hewa et al. (2021), blockchain systems face challenges when expanding their capacity and managing resource utilization (Hewa, Ylianttila, and Liyanage 2021). Their work lays the foundational groundwork, but incorporating AI models brings visible benefits. Our system proved more scalable, achieving a 0.90 index compared to the original 0.75, while improving resource usage from 20% to 85%. Kushwaha et al. (2022) showed that Ethereum smart contracts are vulnerable to potential attacks due to runtime errors (Kushwaha et al. 2022). This study demonstrates that lattice-based cryptographic algorithms outperform RSA-2048 and SHA-256, achieving high-security standards with an entropy of 8.5 and a 0.02 chance of breach.

Sandholm and Mukherjee (2023) investigated smart contracts for bandwidth sharing in telecommunications but did not test them under varying conditions (Sandholm and Mukherjee 2023). To address this research gap, we tested the system under different node settings and confirmed consistent

performance with only 25% of nodes functional. The system maintained steady results of 500±30 TPS with 200±25 ms response times regardless of loading conditions. In the research conducted by Alfuhaid et al. (2023), cyber-physical smart contract architectures were studied with a focus on theoretical considerations (Alfuhaid et al. 2023). Our tests enhance their work by verifying the system's performance with Verizon, Telstra, and MTN through real operational tests in both urban and rural regions.

The research by Afraz et al. (2023) explored blockchain's application in telecommunications, focusing on cost savings versus operational capacity requirements (Afraz et al. 2023). Our performance assessment shows that the proposed system outperforms Hyperledger Fabric and Ethereum, delivering better cost efficiency with a 0.30 index compared to 0.20 and 0.00, respectively. Rastogi et al.'s (2023) study on blockchain in telecommunications highlighted its transformative capabilities without addressing quantum-age security threats. This work extends their research by incorporating quantum encryption technology as a necessary protection measure for blockchain platforms.

Mafakheri et al. (2021) studied blockchain adoption in 5G networks without implementing AI performance enhancements (Mafakheri et al. 2021). Incorporating AI technology enabled our study to achieve 1200 ± 50 TPS throughput alongside 0.30 J/Tx energy efficiency standards. Gibaja-Romero and Cantón-Croda (2022) developed a smart contract classification system without examining its overall effects (Gibaja-Romero and Cantón-Croda 2022). This analysis investigates blockchain performance through both mathematical simulation and actual implementation, testing speed and system capacity.

While the study achieved many useful results, our work has certain limitations. Although lattice-based cryptography shields against quantum threats, it experiences performance loss when handling extreme transaction volumes. Researchers should explore mixed encryption systems to create better security levels while maintaining system speed. The success of our tests proves the system's effectiveness, but additional testing in different regions and industries will enhance the results' applicability. According to Kumar et al. (2019), developing nations experience greater difficulties with regulations and resource availability compared to other countries (Kumar et al. 2019).

Scientists have not thoroughly studied the environmental impact of blockchain despite its growing importance. Kouhizadeh et al. (2023) proposed adding life cycle assessment tools to evaluate blockchain systems' long-term environmental impact (Kouhizadeh, Zhu, and Sarkis 2023). Scientific investigation should extend to examine blockchain's influence on public trust in data security and user adoption levels. Schmidt and Wagner (2019) emphasized the importance of socio-political considerations and data privacy requirements for successful blockchain adoption (Schmidt and Wagner 2019).

The current article presents an improved blockchain smart contract system that delivers enhanced performance, protection, and optimization. The study advances scientific knowledge by validating the system in both test environments and real implementations, addressing current study problems. The article recommends advancing blockchain technology through better resource management and testing on diverse platforms while studying its social and ecological effects. Future developments in blockchain will support secure global networking systems and extend its capabilities to address quantum technology challenges.

## 6. Conclusion

The article delves deeply into blockchain technology and its enhancement of smart contracts, with a specific focus on telecommunications. The study presents a reliable method for improving blockchain systems and boosting their capabilities by effectively addressing security, performance, and scalability issues. By combining artificial intelligence forecasting models with quantum-proof encryption, the study advances both theoretical blockchain knowledge and practical applications.

The article demonstrates blockchain technology's ability to make significant changes in managing high-demand and dynamic systems. The framework proves effective for contemporary telecommunications networks by maximizing resources while minimizing power usage and response times for applications such as 5G, IoT, and decentralized systems. Blockchain systems can maintain their performance and effectiveness under various conditions by employing adaptive scaling features to meet industry demands for quick responses and strong reliability.

A significant aspect of this research examines how blockchain technology

must adapt to future threats, such as quantum computing. The study safeguards data security and system integrity by utilizing cryptographic algorithms that are resistant to quantum threats. The strategic plan ensures the system remains valuable over time by addressing present needs while anticipating future changes.

Blockchain adoption requires a comprehensive solution that balances innovative ideas with practical implementation. The system's real-world deployment demonstrated its versatility and effectiveness across various infrastructure settings, underscoring its practical value. The proof of concept supports the expansion of blockchain usage in telecommunications and other sectors that require scalable and cost-effective secure solutions.

The research team has identified areas for future study beyond the current valuable findings. Advanced cryptographic methods and AI tools need improved processing efficiency to enhance the system's performance across different platforms. While practical use cases provided helpful information, testing in multiple locations and business environments will strengthen the research outcomes in diverse situations. Future studies should also analyze the environmental footprint of blockchain systems alongside their development to meet global sustainability requirements.

These results establish a foundation for future research directions. Hybrid cryptographic methods will enhance blockchain security while improving system efficiency to counter modern cyber threats. Expanding blockchain validation services to more industries and developing countries would reveal new adoption benefits and challenges. Evaluations that analyze blockchain integration from social and political perspectives will deepen our understanding of its social impact.

The study advances smart contract technology by providing real solutions to critical issues on blockchain platforms. The proposed system demonstrates its potential to modernize telecommunications by offering adaptable features that operate efficiently and protect information. Through continued investigation and collaboration, this study lays the groundwork for the development of robust blockchain technology platforms for global digital systems.

## References

Afraz, N., Wilhelmi, F., Ahmadi, H., and Ruffini, M. (2023). Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. *IEEE Access,* 11, 95653-95666. https://doi.org/:10.1109/ACCESS.2023.3309423

Ageyev, D., Yarkin, D., and Nameer, Q. (2014). Traffic aggregation and EPS network planning problem. 2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology, 14-17 Oct. 2014. https://doi.org/:10.1109/INFOCOMMST.2014.6992316.

Alfuhaid, S., Amyot, D., Anda, A. A., and Mylopoulos, J. (2023). A Mapping Review on Cyber-Physical Smart Contracts: Architectures, Platforms, and Challenges. *IEEE Access,* 11, 65872-65890. https://doi.org/:10.1109/ACCESS.2023.3290899

Bag, S., Rahman, M. S., Gupta, S., and Wood, L. C. (2023). Understanding and predicting the determinants of blockchain technology adoption and SMEs' performance. *The International Journal of Logistics Management,* 34 (6), 1781-1807. https://doi.org/:10.1108/IJLM-01-2022-0017

Bhatti, A., Malik, H., Kamal, A. Z., Aamir, A., Alaali, L. A., and Ullah, Z. (2021). Much-needed business digital transformation through big data, internet of things and blockchain capabilities: implications for strategic performance in telecommunication sector. *Business Process Management Journal,* 27 (6), 1854-1873. https://doi.org/:10.1108/BPMJ-12-2020-0553

Cong, W., He, Z., and Zheng, J. (2017). Blockchain Disruption and Smart Contracts. *SSRN Electronic Journal*. https://doi.org/:10.2139/ssrn.2985764

Gibaja-Romero, D.-E., and Cantón-Croda, R.-M. (2022). Auction and Classification of Smart Contracts. *Mathematics*, 10 (7). https://doi.org/:10.3390/math10071033.

Hewa, T., Ylianttila, M., and Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications,* 177, 102857. https://doi.org/:10.1016/j.jnca.2020.102857

Hu, Z., Gao, H., Wang, T., Han, D., and Lu, Y. (2022). Joint Optimization for Mobile Edge Computing-Enabled Blockchain Systems: A Deep Reinforcement Learning Approach. *Sensors*, 22 (9). https://doi.org/:10.3390/s22093217.

Huang, K.-P., Lo, S.-t., and Sutthiphisal, D. (2023). From Data Transparency and Security to Interfirm Collaboration-A Blockchain Technology Perspective. *ABAC Journal,* 43. https://doi.org/:10.59865/abacj.2023.27

Jumnongsaksub, S., and Sripanidkulchai, K. (2020). Reducing Smart Contract Runtime Errors on Ethereum. *IEEE Software,* 37 (5), 55-59. https://doi.org/:10.1109/MS.2020.2993882

Kouhizadeh, M., Zhu, Q., and Sarkis, J. (2023). Circular economy performance measurements and blockchain technology: an examination of relationships. *The International Journal of Logistics Management,* 34 (3), 720-743. https://doi.org/:10.1108/IJLM-04-2022-0145

Kumar, R., Tahir, M. F., Kumar, S., Zia, A., Memon, H., and Mahmood, W. (2019). Challenges in Adoption of Blockchain in Developing Countries. 2019 4th International Conference on Emerging Trends in Engineering, Sciences and

Technology (ICEEST), 10-11 Dec. 2019. https://doi.org/:10.1109/ICEEST48626.2019.8981674.

Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., and Lee, H. N. (2022). Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access,* 10, 6605-6621. https://doi.org/:10.1109/ACCESS.2021.3140091

Lone, A. H., and Naaz, R. (2021). Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. *Computer Science Review,* 39, 100360. https://doi.org/:10.1016/j.cosrev.2020.100360

Mafakheri, B., Heider-Aviet, A., Riggio, R., and Goratti, L. (2021). Smart Contracts in the 5G Roaming Architecture: The Fusion of Blockchain with 5G Networks. *IEEE Communications Magazine,* 59 (3), 77-83. https://doi.org/:10.1109/MCOM.001.2000857

Muneeb, M., Raza, Z., Haq, I. U., and Shafiq, O. (2022). SmartCon: A Blockchain-Based Framework for Smart Contracts and Transaction Management. *IEEE Access,* 10, 23687-23699. https://doi.org/:10.1109/ACCESS.2021.3135562

Nameer, Q., Aqeel, J., and Muthana, M. (2023). The Usages of Cybersecurity in Marine Communications. *Transport Development,* 3 (18). https://doi.org/:10.33082/td.2023.3-18.05

Panayotov, A., and Ruskov, P. (2022). Measuring the effectiveness of blockchain smart contracts. 2022 International Conference Automatics and Informatics (ICAI), 6-8 Oct. 2022. https://doi.org/:10.1109/ICAI55857.2022.9960013.

Pisano, M., and Bassett, R. (2021). Organizational Cost and Complexity Saving Opportunities via the Development, Deployment, and Implementation of Blockchain Networks. *Information Technology and Management Science,* 24 (1), 33-38. https://doi.org/:10.7250/itms-2021-0005

Qasim, N. (2019). New Approach to the Construction of Multimedia Test Signals. *International Journal of Advanced Trends in Computer Science and Engineering,* 8, 3423-3429. https://doi.org/:10.30534/ijatcse/2019/117862019

Qasim, N., Ageyev, D., and Alanssari, A. (2016). CAPACITY DESIGN OF LTE EPS NETWORK WITH SELF-SIMILAR TRAFFIC. *Telecommunications and information technologies Journal,* 2, 33-38. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vduikt_2016_2_8.pdf

Qasim, N. H., Jumaa, D. A., Rahim, F., Jawad, A. M., Khaleefah, A. M., Zhyrov, G., and Ali, H. (2024). Simplifying IP multimedia systems by introducing next-generation networks with scalable architectures. *Edelweiss Applied Science and Technology,* 8 (4), 2042-2054. https://doi.org/:10.55214/25768484.v8i4.1580

Qasim, N. H., Vyshniakov, V., Khlaponin, Y., and Poltorak, V. (2021). Concept in information security technologies development in e-voting systems. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS),* 3 (9), 40-54. https://www.irjmets.com/uploadedfiles/paper/volume_3/issue_9_september_2021/15985/final/fin_irjmets1630649545.pdf

Rastogi, A., Chirputkar, A., and Ashok, P. (2023). Reimagining Telecom Industry Using Blockchain Technology. 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), 23-25 March 2023. https://doi.org/:10.1109/ICSCDS56580.2023.10104989.

Sandholm, T., and Mukherjee, S. (2023). Smart Contracts for Mobile Network Operator Bandwidth Sharing. *Distrib. Ledger Technol.,* 2 (4), Article 29. https://doi.org/:10.1145/3630168

Sanka, A. I., Irfan, M., Huang, I., and Cheung, R. C. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications,* 169, 179-201. https://doi.org/:10.1016/j.comcom.2020.12.028

Schmidt, C. G., and Wagner, S. M. (2019). Blockchain and supply chain relations: A transaction cost theory perspective. *Journal of Purchasing and Supply Management,* 25 (4), 100552. https://doi.org/:10.1016/j.pursup.2019.100552

Tapwal, R., Deb, P. K., Misra, S., and Pal, S. K. (2023). Shadows: Blockchain Virtualization for Interoperable Computations in IIoT Environments. *IEEE Transactions on Computers,* 72 (3), 868-879. https://doi.org/:10.1109/TC.2022.3184271

Wang, J., Ling, X., Le, Y., Huang, Y., and You, X. (2021). Blockchain-enabled wireless communications: a new paradigm towards 6G. *National Science Review,* 8 (9), nwab069. https://doi.org/:10.1093/nsr/nwab069

Yousif, O., Dawood, M., Jassem, F. T., and Qasim, N. H. (2024). Curbing crypto deception: evaluating risks, mitigating practices and regulatory measures for preventing fraudulent transactions in the middle east. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico,* (22), 311-334. https://doi.org/:10.5281/zenodo.13732337