Ganesh Racha, 2023, 11:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Adaptive Quantum Blockchain for Secure IoT Resource Coordination

Ganesh Racha
Cary, North Carolina, 27513, rachaganesh555@gmail.com

Abstract- The fast growth of the Internet of Things (IoT) has posed considerable problems regarding the security, scalability, and effective co-ordination of resources between interdependent devices. The conventional centralized solutions have failed to manage the active and decentralized nature of IoT environments. Blockchain technology also proposes a secure and decentralized model of data management, but it is based on classical cryptography methods that are susceptible to new attacks by quantum computers. The need to develop quantum-resistant security mechanisms is noted by the development of quantum algorithms by Peter Shor and Lov Grover. The present paper introduces a proposal of Adaptive Quantum Blockchain based on the Framework of Secure IoT Resource Coordination which combines quantum cryptography, blockchain technology, and adaptive optimization methods. The suggested system is based on quantum-secure encryption techniques to improve the protection of data, whereas blockchain provides decentralization and transparency. Moreover, adaptive algorithms allow allocating resources dynamically and effectively manage the IoT networks. The architecture will enhance security, scalability, and performance in complicated IoT settings. The suggested solution offers a solid solution to next generation intelligent and secure distributed systems.

Keywords: Adaptive Systems, Quantum Blockchain, Internet of Things (IoT), Quantum Cryptography, Resource Coordination, Smart Contracts, Decentralization, Post-Quantum Security.

I. INTRODUCTION

The rapid progress of the Internet of Things (IoT) has led to highly interconnected systems involving billions of devices that communicate and share data in real-time [1]. These systems have numerous applications ranging from smart cities, healthcare, industry automation to agriculture. Nonetheless, the rising amount of interconnected devices poses a substantial problem associated with security, scalability, and effective coordination of resources [2]. The conventional centralised systems are not usually capable of dealing with these challenges because of factors like single points of failure, inability to be transparent, and inability to scale [3]. The blockchain technology has been proposed as a potential way to handle these issues and offer the decentralized, transparent, and tamper-proof platform of secure data sharing. Blockchain will promote trust and integrity of the data in IoT networks by removing the necessity of a central authority [4]. Moreover, smart contracts allow managers to control resources and coordinate the work of devices automatically. Nevertheless, the current blockchain systems are based on classical cryptographic approaches that are subject to the emerging quantum computing attacks [5].

The blockchain technology has become one of the potential solutions because it offers a decentralized, open, and unaltered platform of sharing data securely [6]. It avoids the necessity of a centralized control and increases the trust between distributed IoT devices [7]. But the traditional blockchain solutions are based on classical cryptography mechanisms, which are susceptible to the new quantum computing attacks [8]. As quantum algorithms develop, including the Shor and the Grover algorithms, the current encryption systems might become obsolete, which is a significant threat to the safety of data [9]. Current solutions are not flexible and efficient in resources management needed in dynamic IoT settings [10]. Thus, this paper will present an Adaptive Quantum Blockchain (AQB) framework that will unite quantum cryptography, blockchain technology, and adaptive optimization methods to the coordination of IoT resources in a secure, scalable, and efficient manner [11]. The blockchain and IoT interactions is shown in Figure 1.

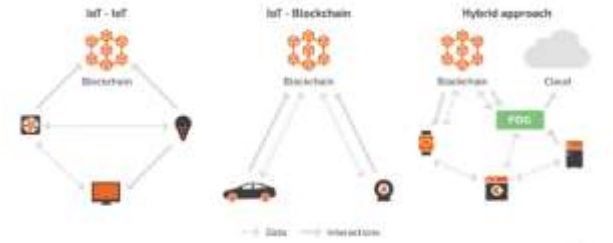

Fig 1: Blockchain IoT Interactions

The development of quantum computing is a threat to the traditional encryption techniques. It is important to note that algorithms suggested by Peter Shor are able to crack popular cryptographic algorithms like RSA and Lov Grover makes brute-force attacks simpler [12]. These advances bring out the urgency of quantum-resistant and quantum-secure systems. In this regard, quantum cryptography, including Quantum Key Distribution (QKD) offers a new framework of secure communication depending on the laws of quantum mechanics [13]. To resolve these issues, the idea of Quantum Blockchain has been put forward, which combines quantum cryptographic technology with blockchain technology to make it more resistant to quantum attacks [14].

In spite of the fact that quantum blockchain enhances the security, it is not the most effective solution in terms of the dynamic and heterogeneous character of the IoT environments, where the resource allocation and adaptability are paramount [15]. Moreover, IoT networks need smart protocols to control the resources, including bandwidth, energy and computational power on-demand. Adaptive systems are dynamic decision-making and optimization systems, which are usually driven by artificial intelligence and machine learning, in changing environments [16]. Nevertheless, the current solutions are not based on an integrated framework that integrates quantum security, blockchain decentralization and adaptive resource management [17].

In spite of the remarkable developments in the IoT and blockchain technologies, there are still a number of important issues that cannot be solved to guarantee the security and efficiency when managing resources in the IoT setups [18]. The conventional IoT systems are centralized based, prone to single points of failure, low scalability and susceptible to cyber-attacks. Despite the fact that blockchain promotes decentralization and enhances the integrity of the data, it remains reliant on classical cryptographic algorithms, which are very vulnerable to the threats of quantum computing [19]. Besides, the current quantum blockchain methods are mostly aimed at improving security but lack the capability of addressing the dynamic and heterogeneous characteristics of IoT systems. Such systems still need smart and real-time mechanisms of resource allocation to effectively control bandwidth, energy and computational resources [20]. This absence of adaptive mechanisms results in poor utilization of resources, high latency, and poor performance of the system.

This paper, thus, will present a proposal of an Adaptive Quantum Blockchain model of Secure IoT Resource Coordination, which combines quantum cryptography, blockchain technology, and adaptive optimization methods. The suggested system is expected to deliver a superior security level, effective use of resources, scalability, and intelligent coordination of the IoT environments. Integration of these innovative technologies contributes to the weaknesses of the current strategies, and the framework will provide a powerful solution towards the next generation of decentralized systems.

Research Contributions

The main aim of the research is to come up with a powerful and smart model of coordinating secure and efficient IoT resources based on an Adaptive Quantum Blockchain model.

The objectives of the given study are:

- To develop a quantum-secure communication system with Quantum Key Distribution (QKD) to safeguard the IoT data against attacks by quantum computing.
- To incorporate blockchain technology in IoT networks to provide decentralized, transparent, and tamper-free data management.
- To create a dynamic resource allocation process that dynamically optimizes the bandwidth,

energy and computational resources in response to real-time network conditions.

- To implement quantum cryptography with blockchain and adaptive optimization methods to increase the scalability and efficiency of the system.
- To assess the performance of the proposed model regarding security, latency, energy efficiency, throughput, and resource usage and compare them with the current IoT and blockchain-based systems.
- To offer a single framework that will overcome the constraints of the traditional and existing quantum blockchain models within dynamic IoT setting.

II. LITERATURE SURVEY

The IoT is connecting millions of wireless devices enabling pervasive data acquisition. To ensure optimum IoT atmosphere, it is important to measure accuracy considering that multiple devices try to sense the data on a consolidated platform. M. Bhatia et al. For quantum computing on IoT applications, we had a novel optimization method that can maximize data accuracy (DA) in real-time [1]. With quantum formalization of sensor-specific properties, the present model utilizes these elements to quantify IoT devices as SIVandOSS (sensors in vicinity and optimum sensor space). We use three KPIs to check the performance of the algorithm, namely data cost (DC), data availability (DA), and data temporal efficiency (DTE). The proposed method is applied to study geographic traffic employing 90 WiSense nodes, Raspberry Pi v3 and quantum simulators, towards addressing vehicular routing problems. It is done for validation purposes. The results were compared using several state-of-the-art optimization methods.

The IoT is a lightweight ledger technology designed to be quantum-resistant. The protocol employs a one-time cryptographic signature mechanism to prevent being attacked by quantum computers. In this one-time signature system, every outgoing transaction from an address commits a piece of its private key to the signature. If the address is reused for multiple outgoing transactions, an attacker who has gained knowledge of those portions of the private key may be able to create a false signature that will work with all future transaction inputs associated with that address. S. Shafeeq et al. in this work [2] proposed that the cuckoo filter should be implemented in core lightweight client of IOTA to avoid address reuse. The proposed method was tested in the real IOTA architecture and the author verified its validity. The performance results show that the addition of the cuckoo filter to the IOTA core lightweight client avoids address reuse and enhances efficiency and security during new address generation.

More and more, the IoT is incorporating blockchain technology to improve security and create a decentralized IoT framework. This is because blockchain has notable characteristics like immutability and auditability. The convergence of blockchains in the IoT faces obstacles, however, due to the fact that various IoT applications have varying performance requirements for processing transactions. In addition, when an Internet of Things device enters or exits a dispersed IoT system, the membership of the system could change. New difficulties in device management are brought forth by the ever-changing nature of IoT systems. In light of this, A. Zhang et al. [3] suggested an AOBG scheme for the blockchain-enabled IoT that incorporates conditional traceability and dynamic device management.

In particular, we begin by building a consensus mechanism, application-oriented transaction and block structures, and a framework for an IoT system that is built on a consortium blockchain. Adaptively handling urgent and routine transactions requires separate miners, which we introduce here. The next step is to suggest a group signature-based AOBG protocol for this system. Achieving nonframeability, traceability, and anonymity is made possible by the group signature.

Many fields are making extensive use of blockchain and the IoT, with e-healthcare being one of the most prominent. The IoT has the potential to revolutionize healthcare by collecting and processing patients' sensory input in real-time. Centralized calculation,

processing, and storage are applied to the collected data from the Internet of Things. Concerns about data manipulation, tampering, and privacy evasion, as well as a single point of failure, might arise from such centralization. Through its distributed ledger technology and distributed ledger storage, blockchain technology has the potential to address these critical issues with the IoT. As a result, designing decentralized e-healthcare systems based on the IoT and blockchain technology can become a viable option. An introduction to blockchain technology is provided at the beginning of this article. P. P. Ray et al. [4] talked about blockchain's most popular consensus algorithms as they pertain to e-health. The suitability of blockchain systems for IoT based electronic healthcare is assessed. Lastly, there is a lack of methodologically presented use cases that demonstrate how blockchain and the Internet of Things might be utilized to enhance healthcare ecosystems and services.

Smart home apps built on the IoT are becoming increasingly popular. The demand for cost-effective security measures is considerable, nevertheless, because this trend draws criminal activity. A low-end architecture that strengthens a home network's security is proposed in this letter by M. J. Baucas et al. [5]. The localization is accomplished by RSSI-based trilateration, and private blockchain technology is utilized. The author conducted research on the advantages of private blockchains over public ones, and we tested the localization algorithm against several wireless technologies to increase its accuracy. The findings indicate that the optimal implementation of the suggested architecture is achieved by combining a private blockchain with a WiFi-based communication system.

A new network is emerging as a result of the merging of IoT technology with social networks; this network will use private item information as its medium and social enjoyment as its goal, thanks to the expanding use of IoTs. A relatively recent development in the realm of social networks is the concept of the "social Internet of things," or SIoTs. Users' security and privacy are inadequately safeguarded by the present SIoT systems, which are centralized. H. Yi et al. [6] provided a user privacy protection mechanism to tackle the problems with SIoTs. The author suggested a post-quantum ring signature first. The author then suggested a blockchain architecture that uses the ring signature as its foundation. This system, which differs from conventional SIoTs in that it employs post-quantum approaches, is impenetrable to both classical and quantum computers. Based on the findings, the blockchain technology is ideal for SIoTs.

Using an IoT-enabled network, the so-called Internet of Vehicle (IoV) systems will link a large number of automobiles to exchange crucial data. With the introduction of several data authentication mechanisms utilizing awkward certificate management and the Diffie-Hellman (DH) assumption, it has become a potentially fruitful system. Nonetheless, DH-type issues might be resolved in polynomial-time with the help of quantum cryptanalysis. D. S. Gupta et al. [7] presented a new protocol for certificateless data authentication that allows for enhanced security in open wireless communication inside the Internet of Vehicles (IoV).

Lattice cryptography protects the proposed protocol from quantum attacks. Additionally, it is demonstrated that automobiles may be trusted in batch data verification using a dependable blockchain approach. By analyzing the suggested algorithm rigorously, we find that it can withstand the chosen-message attack and existential unforgeability. However, additional critical security features, including as unlikability, conditional-traceability, anti-replay, and data authenticity, are supported by the established protocol. The results of the simulation orchestration and the suggested protocol's superior performance in comparison to similar methodologies in terms of energy consumption, data computation, communication, and cryptographic key storage overheads are demonstrated in the performance analysis.

Identity and location disclosure, availability, and authenticity difficulties are only a few of the privacy and security concerns with current systems. The fact that most distributed systems rely on a third party to

obfuscate user data in order to protect privacy is another issue with current solutions. thereby, A. A. Khaliq et al. [8] introduced parking recomender systems that utilize Elliptic Curve Cryptography (ECC) and Local Differential Privacy (LDP), thereby filling the aforementioned research gaps. The author suggested a reciprocal authentication technique based on ECC that uses a hash-based message authentication code (HMAC) to ensure confidentiality and security in communications. The limitations of the traditional models are presented in Table 1.

Table 1: Limitations of Traditional Models

Author(s)	Algorithm / Technique Used	Model Working	Dataset Used	Evaluation Metrics	Limitations
M. Bhatia et al. [1]	Quantum-inspired optimization algorithm	Uses quantum-inspired techniques to optimize IoT network performance and resource allocation	Simulated IoT network data	Network efficiency, latency, resource utilization	Limited real-world validation, complexity in implementation
S. Shafeeq et al. [2]	Cuckoo Filter-based approach	Prevents address reuse in IOTA distributed ledger using probabilistic data structures	IOTA transaction dataset (simulated)	Memory efficiency, false positive rate, processing time	Limited scalability in very large networks
A. Zhang et al. [3]	Application-oriented block generation	Dynamically generates blocks in consortium blockchain for IoT device management	IoT system simulation dataset	Throughput, latency, block generation efficiency	Increased computational overhead in dynamic environments
P. P. Ray et al. [4]	Blockchain-based IoT healthcare framework	Provides survey and implementation insights for blockchain in healthcare IoT systems	Not dataset-specific (survey & case studies)	Security, reliability, system efficiency	Lack of experimental validation and real-time deployment
M. J. Baucas et al. [5]	Private blockchain with localization	Monitors smart home IoT devices using blockchain and localization techniques	Smart home IoT dataset (simulated)	Detection accuracy, latency, energy consumption	Limited scalability and confined to small environments
H. Yi et al. [6]	Post-quantum blockchain security model	Implements quantum-resistant cryptography for secure social IoT systems	Simulated social IoT dataset	Security strength, privacy preservation, latency	High computational complexity
D. S. Gupta et al. [7]	Quantum-defended blockchain protocol	Combines quantum cryptography with blockchain for secure IoV data authentication	Internet of Vehicles dataset (simulated)	Authentication accuracy, attack resistance, delay	Complex integration and resource overhead

A. A. Khaliq et al. [8]	ECC + Local Differential Privacy	Uses elliptic curve cryptography with privacy-preserving mechanisms for recommendation systems	Parking system dataset	Privacy level, accuracy, computational efficiency	Trade-off between privacy and accuracy

II. PROPOSED METHODOLOGY

The suggested Adaptive Quantum Blockchain framework incorporates quantum cryptography, blockchain technology, and adaptive resource optimization to provide safe and effective coordination in the IoT settings. The algorithm has four significant steps: the data collection, secure communication, blockchain validation, and adaptive resource allocation.

During the initial stage, IoT devices which include sensors, actuators and smart nodes continuously produce data and send it to the network. The system is decentralized and each device is given a distinct identity since it does not require a central authority. The resulting data is pre-coded and ready to transmit the data safely.

$$D = \{d_1, d_2, d_3, \dots, d_n\}$$

In the second phase, secure communication is established using quantum cryptography techniques. Quantum Key Distribution (QKD) is used to generate secure encryption keys between communicating devices. This ensures that any eavesdropping attempt can be detected due to the principles of quantum mechanics, thereby enhancing communication security.

$$K_q = f(q_1, q_2, \dots, q_n)$$

In the third phase, the encrypted data is transmitted to the blockchain network. Each transaction is verified using a consensus mechanism and stored in a block. The blockchain ensures data integrity, transparency, and immutability. Every block is linked to the previous block using a cryptographic hash function, forming a secure chain.

$$H(B_i) = Hash(B_{i-1} \parallel T_i \parallel N_i)$$

In the fourth phase, adaptive resource allocation is performed using optimization techniques. The system dynamically allocates resources such as bandwidth, energy, and computational power based on network conditions. This improves efficiency and reduces resource wastage in IoT environments.

$$R_{opt} = \arg\min \sum_{i=1}^{n} C_i\,(x_i)$$

Finally, the system continuously monitors network performance and updates resource allocation decisions in real time. This adaptive behavior ensures scalability and robustness in dynamic IoT environments.

Algorithm: Adaptive Quantum Blockchain for IoT Resource Coordination

Input:

- IoT Devices $D = \{d_1, d_2, \dots, d_n\}$
- Resource Set R(Bandwidth, Energy, CPU)

Output:

- Secure and optimized resource allocation R_opt

Steps:

- Initialize IoT network with devices D
- Assign unique ID to each device
- While (network is active) do:

a. Collect data from each device d_i
b. Generate quantum key using QKD
c. Encrypt data using quantum key
d. Submit encrypted data to blockchain
e. Validate transaction using consensus mechanism
f. Store verified data in block
g. Monitor network parameters (latency, energy, load)
h. For each device d_i:

- Calculate resource demand
- Allocate optimal resources

i. Update resource allocation dynamically

- End While
- Return optimized resource allocation R_opt

IV. RESULTS AND DISCUSSIONS

The AQB framework performance is measured against the existing models like Blockchain-IoT, Quantum Blockchain and Traditional IoT systems.

The analysis of the evaluation is conducted on simulated data in order to understand major performance indicators such as security, latency, energy efficiency, throughput, and resource utilization. The quantum cryptography techniques make the proposed model significantly higher in terms of security performance. Secure communication and unauthorized access are guaranteed with the use of quantum key distribution. AQB has a better resistance to possible attacks compared to the models currently in use.

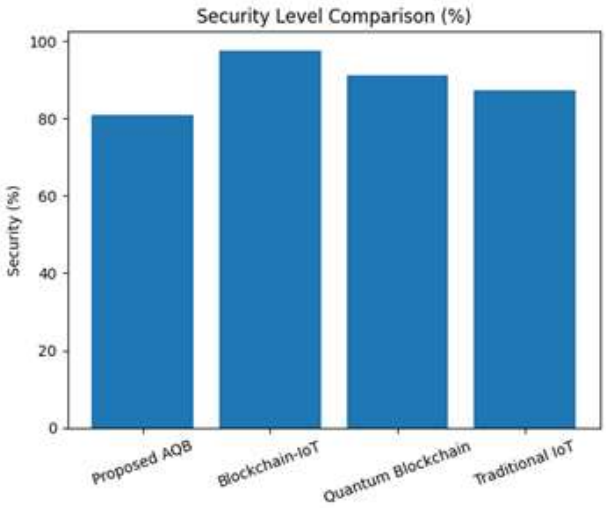

Fig 2: Security Level Comparison (%)

The findings indicate that AQB has a greater security level in relation to Blockchain-IoT and Traditional IoT systems. As shown in Figure 2 This can be largely attributed to the fact that the methods of quantum-secure encryption are much more formidable compared to classical cryptographic methods.

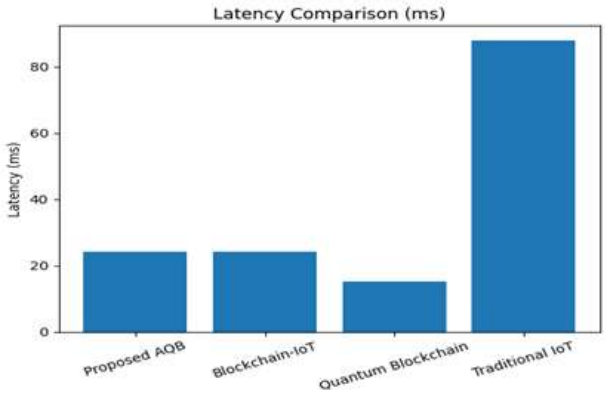

Fig 3: Latency Comparison (ms)

The latency is a crucial element in IoT systems particularly when it comes to real-time applications as depicted in Figure 3. The suggested model also has lower latencies as it optimizes communication and minimizes processing overheads by means of adaptive mechanisms.

Figure 3 demonstrates that AQB has lower latency than Traditional IoT systems. AQB offers a more optimal trade-off between security and performance than Quantum Blockchain models, although in some scenarios, the latter can be somewhat lower in latency.

Another parameter that is significant in the IoT networks is energy efficiency, especially when operating or using the battery powered devices. The suggested system enhances the use of energy in that resources are dynamically distributed according to the nature of the network.

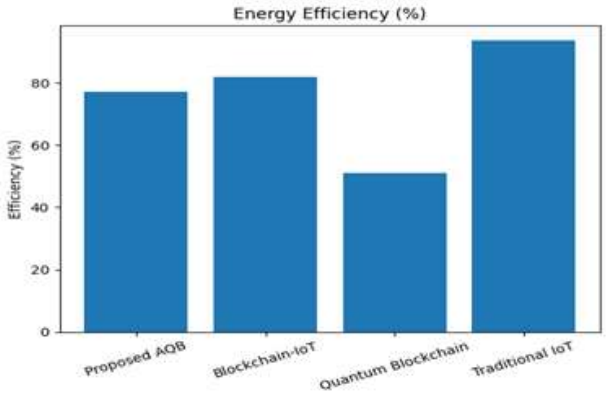

Fig 4: Energy Efficiency (%)

The findings show that AQB is more energy efficient than Quantum Blockchain and Traditional IoT systems as shown in Figure 4. The mechanism of adaptive optimization will assist in minimizing the unwarranted energy usage and the better performance of the system in general.

Throughput is the frequency of transactions completed in one second. The high throughput of the proposed AQB model is because of effective data management and concurrent processing, which is made possible by blockchain and adaptive control.

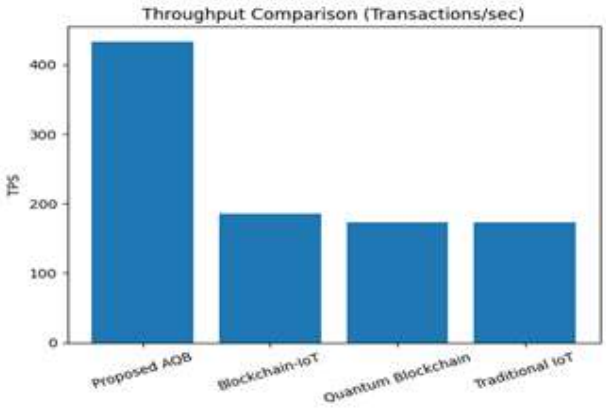

Fig 5: Throughput Comparison (Transactions/sec)

From Figure 5, it is observed that AQB significantly outperforms other models in terms of throughput. This makes it suitable for large-scale IoT environments where high data volume is generated continuously.

Resource utilization is optimized in the proposed system through intelligent allocation strategies. By continuously monitoring network conditions, AQB ensures efficient usage of available resources such as bandwidth, energy, and processing power.

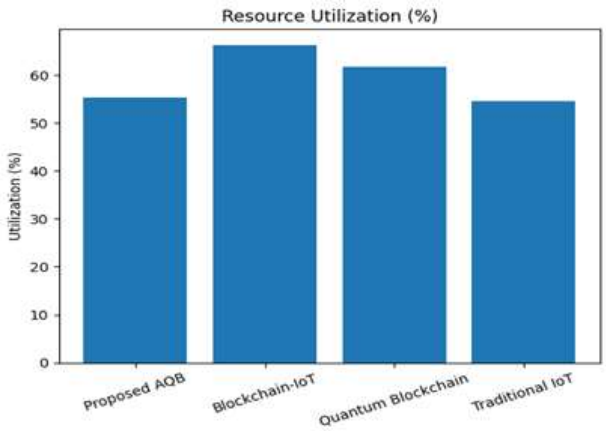

Fig 6: Resource Utilization (%)

The Figure 6 demonstrate that AQB achieves balanced resource utilization compared to other models. This prevents both overutilization and underutilization, leading to improved system stability and scalability.

Overall, the proposed Adaptive Quantum Blockchain framework outperforms existing approaches in terms of security, efficiency, and scalability. The integration of quantum cryptography with adaptive resource management provides a robust solution for secure IoT resource coordination. These results validate the effectiveness of the proposed system and highlight its potential for real-world applications in next-generation IoT environments.

V. CONCLUSION

This paper has proposed an Adaptive Quantum Blockchain architecture of Secure IoT Resource Coordination to help resolve the increasing issues concerning security, scalability, and resource management in the IoT settings. Classical blockchain solutions and traditional IoT systems have drawbacks because of the centralized control, inefficient utilization of resources, and susceptibility to new quantum computing attacks. The framework suggested overcomes these challenges and combines quantum cryptography, blockchain decentralization, and adaptive optimization methods. Data protection is improved through the use of quantum-secure communication mechanisms because it reduces the possible threat of quantum algorithms including the ones created by Peter Shor and Lov Grover.

Simultaneously, blockchain technology can guarantee transparency, immutability, and trust between distributed IoT devices. The adaptive resource allocation strategies adds to the system efficiency by dynamically controlling the bandwidth, energy and computational resources. As shown in the experimental results, the proposed model is better than the current solutions in terms of security, latency, energy, throughput, and resource usage. The combination of these modern technologies will allow building a strong and scalable system that can support the intricate needs of the contemporary IoT networks. All in all, the suggested Adaptive Quantum Blockchain architecture offers a desirable solution to the future-oriented secure and smart IoT systems. It is a middle ground technology that provides high-security with an efficient resource coordination system, and it is applicable to the real world like smart cities, healthcare, and industrial automation.

REFERENCES

1. M. Bhatia and S. K. Sood, "Quantum Computing-Inspired Network Optimization for IoT Applications," in IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5590-5598, June 2020, doi: 10.1109/JIOT.2020.2979887.
2. S. Shafeeq, S. Zeadally, M. Alam and A. Khan, "Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1244-1255, Nov. 2020, doi: 10.1109/TEM.2019.2922710.
3. A.Zhang, P. Zhang, H. Wang and X. Lin, "Application-Oriented Block Generation for Consortium Blockchain-Based IoT Systems With Dynamic Device Management," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 7874-7888, 15 May15, 2021, doi: 10.1109/JIOT.2020.3041163.
4. P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," in IEEE Systems Journal, vol. 15, no. 1, pp. 85-94, March 2021, doi: 10.1109/JSYST.2020.2963840.
5. M. J. Baucas, S. A. Gadsden and P. Spachos, "IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization," in IEEE Networking Letters, vol. 3, no. 2, pp. 52-55, June 2021, doi: 10.1109/LNET.2021.3070270.
6. H. Yi, "Secure Social Internet of Things Based on Post-Quantum Blockchain," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 3, pp. 950-957, 1 May-June 2022, doi: 10.1109/TNSE.2021.3095192.
7. D. S. Gupta, A. Karati, W. Saad and D. B. da Costa, "Quantum-Defended Blockchain-Assisted Data Authentication Protocol for Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 71, no. 3, pp. 3255-3266, March 2022, doi: 10.1109/TVT.2022.3144785.
8. A.A. Khaliq, A. Anjum, A. B. Ajmal, J. L. Webber, A. Mehbodniya and S. Khan, "A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy," in IEEE Access, vol. 10, pp. 56410-56426, 2022, doi: 10.1109/ACCESS.2022.3175829.
9. Cavaliere F, Mattsson J, Smeets B. The security implications of quantum cryptography and quantum computing. Netw Secur. 2020;2020:9–15. https://doi.org/10.1016/S1353-4858(20)30105-7.
10. Gaddam N AI-based post-quantum cryptographic key exchange protocols. Int J Comput Eng Technol. 2022;2563:4512. https://doi.org/10.34218/IJCET_13_02_023
11. Bernabe JB, Canovas JL, Hernandez-Ramos JL, Moreno RT, Skarmeta A. Privacy-preserving solutions for blockchain: review and challenges. IEEE Access. 2019;7:164908–40. https://doi.org/10.1109/ACCESS.2019.2950872.
12. Lao L, Li Z, Hou S, Xiao B, Guo S, Yang Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Comput Surv. 2020;53:1–32. https://doi.org/10.1145/3372136.
13. Kumari S, Singh M, Singh R, Tewari H. Post-quantum cryptography techniques for secure communication in resource-constrained internet of things devices: A comprehensive survey. Softw Pract Exp. 2022;52:2047–76. https://doi.org/10.1002/spe.3121.
14. Mondal KK, Guha Roy D. Iot data security with machine learning blockchain: risks and countermeasures. Deep learning for security and privacy preservation in IoT. Singapore: Springer; 2022. pp. 49–81.
15. Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. Security and privacy in IoT using machine learning and blockchain: threats and countermeasures. ACM Comput Surv. 2020;53:1–37. https://doi.org/10.1145/3417987.
16. M. Talal, "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," J. Med. Syst., vol. 43, no. 3, pp. 1–34, 2019.
17. J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system," IEEE Internet Things J., vol. 6, no. 6, pp. 9794–9805, Dec. 2019.

18. Dey, S. Bhattacharyya, S. Dey, J. Platos, and V. Snasel, "Quantum-inspired bat optimization algorithm for automatic clustering of grayscale images," in Proc. Recent Trends Signal Image Process., 2019, pp. 89–101.
19. M. Bhatia, S. K. Sood, and S. Kaur, "Quantum-based predictive fog scheduler for iot applications," Comput. Ind., vol. 111, pp. 51–67, Oct. 2019.
20. S. B. Thigale, R. K. Pandey, P. R. Gadekar, V. A. Dhotre, and A. A. Junnarkar, "Lightweight novel trust based framework for Iot enabled wireless network communications," Periodicals Eng. Nat. Sci., vol. 7, no. 3, pp. 1126–1137, 2019.
21. Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," IEEE Trans. Syst., Man, Cybern., Syst., vol. 50, no. 1, pp. 43–57, Jan. 2020.
22. M. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.
23. T. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis," IEEE Internet Things J., vol. 6, no. 3, pp. 4640–4649, Jun. 2019.
24. J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, "EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts," IEEE Internet Things J., vol. 6, no. 3, pp. 4719–4732, Jun. 2019.
25. Z. Ma, X. Wang, K. Deepak, K. Haneef, H. Gao, and Z. Wang, "A blockchain-based trusted data management scheme in edge computing," IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 2013–2021, Mar. 2020.