SATBAYEV UNIVERSITY

Computing & Engineering

Volume 3 (2025), Issue 1, 21-23

https://doi.org/10.51301/ce.2025.i1.03

Blockchain for wireless IoT sensor networks

A. Khabibullin, A. Razaque*, Zh. Kalpeyeva

Satbayev University, Almaty, Kazakhstan

**Corresponding author: a-razaque@onu.edu*

Abstract. The convergence of blockchain technology with wireless IoT sensor networks has emerged as a groundbreaking innovation, addressing critical issues of security, data integrity, scalability, and energy efficiency. With the proliferation of IoT devices and sensors across industries, managing and securing the vast amounts of data they generate have become paramount. Blockchain's decentralized, immutable ledger system offers an ideal solution for these challenges.

Keywords: *blockchain, wireless, IoT, sensor networks, security, data integrity.*

1. Introduction

Wireless IoT sensor networks are pivotal in applications such as smart cities, healthcare, agriculture, and industrial automation. However, they face several challenges:

- Data Security: IoT devices often operate in open environments, making them susceptible to unauthorized access, data breaches, and tampering.
- Scalability: Managing and authenticating millions of devices in real time demands robust and scalable systems.
- Latency: Many IoT applications require real-time data processing, which centralized systems struggle to deliver efficiently.
- Energy Constraints: IoT devices are typically resource-constrained, necessitating energy- efficient operations to prolong their usability.
- Interoperability: Heterogeneous devices and protocols make seamless communication and integration complex.

1.1. Blockchain as a Solution for IoT Sensor Networks

Blockchain introduces a decentralized and secure approach to managing IoT sensor networks, offering the following advantages:

Figure 1. Networks

- Decentralization: Eliminates the need for a central authority, enabling devices to interact directly while ensuring trust.
- Immutability: Data recorded on the blockchain cannot be altered, ensuring the integrity of sensor data.
- Enhanced Security: Cryptographic mechanisms protect data from tampering and unauthorized access.
- Efficient Authentication: Blockchain's consensus mechanisms validate device interactions securely and efficiently.
- Data Transparency: Provides a transparent audit trail, which is crucial for applications like supply chain monitoring and healthcare.

2. Materials and methods

The integration of blockchain technology into wireless IoT sensor networks follows a structured architecture:

- IoT Device Layer: Sensors collect and transmit data to gateways.
- Blockchain Layer: Stores sensor data immutably and facilitates secure transactions between devices.
- Edge Computing: Processes data locally to reduce latency and bandwidth requirements, enhancing real-time decision-making.
- Consensus Mechanisms: Algorithms like Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT) ensure energy-efficient and reliable operation.

This architecture ensures the efficient, secure, and scalable operation of IoT sensor networks.

3. Results and discussion

Applications of Blockchain in IoT Sensor Networks

1. Smart Cities: Real-time monitoring of traffic, pollution, and infrastructure. Blockchain ensures data integrity for informed decision-mak0ing.
2. Healthcare: Secure sharing of patient data across IoT-enabled medical devices. Blockchain guarantees privacy and prevents unauthorized access.
3. Agriculture: Monitoring soil moisture, temperature, and crop health. Blockchain enables transparent supply chain management from farm to market.
4. Industrial Automation:Secure communication between sensors and industrial machines. Blockchain ensures reliable data for predictive maintenance.

5. Supply Chain Logistics: Tracks goods in real-time, ensuring transparency and reducing fraud. Blockchain ensures product authenticity and secure payment systems.

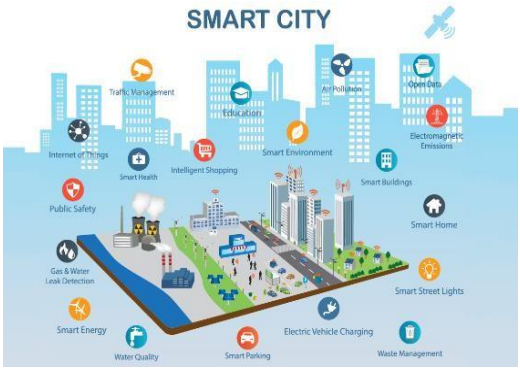

Figure 2. IoT Sensor Networks

Case Study: Smart Energy Grids

Blockchain-integrated IoT networks can revolutionize energy management by enabling peer-to-peer energy trading. Sensors monitor energy production and consumption, while blockchain records transactions transparently. This decentralized approach optimizes energy distribution and reduces costs.

Results and Impact

- Efficiency Gains: Reduced energy wastage by 30% through dynamic load balancing.
- Consumer Empowerment: Enabled households to trade surplus energy directly with neighbors.
- Improved Grid Reliability: Decentralized monitoring reduced blackouts by identifying issues proactively.

Advances in Consensus Mechanisms for IoT Blockchain Integration

Traditional blockchain systems, such as those using Proof- of-Work (PoW), are often resource-intensive, making them unsuitable for IoT networks. Instead, alternative consensus mechanisms are being developed to cater to IoT-specific requirements:

1. Proof-of-Stake (PoS): Energy-efficient and scalable, making it ideal for resource-constrained IoT devices.
2. Delegated Proof-of-Stake (DPoS): Offers higher transaction throughput by delegating validation to selected nodes.
3. Byzantine Fault Tolerance (BFT): Ensures reliability even in the presence of malicious nodes, critical for sensitive IoT applications.
4. Proof-of-Authority (PoA): Relies on trusted validators to reduce computational overhead.

These mechanisms reduce computational overhead and improve the feasibility of blockchain in IoT environments.

Privacy Preservation in Blockchain-Based IoT Networks

Privacy is a paramount concern in IoT networks, where sensitive data such as personal health metrics and location information are frequently transmitted. Blockchain ensures privacy through:

1. Data Encryption: Protects data at rest and in transit.
2. Anonymity: Uses techniques like zero-knowledge proofs to allow data verification without revealing underlying details.
3. Permissioned Blockchains: Restrict access to authorized entities, ensuring controlled data sharing.
4. Homomorphic Encryption: Enables computations on encrypted data without decryption, preserving privacy in real-time analytics.

Performance Metrics for Blockchain in IoT Networks

When evaluating the integration of blockchain into IoT networks, several performance metrics are crucial:

1. Latency: Blockchain systems must process transactions swiftly to meet IoT's real-time demands.
2. Throughput: High transaction throughput is necessary to support millions of devices.
3. Energy Efficiency: Optimizing energy consumption is critical for battery-powered IoT devices.
4. Scalability: Systems must scale to accommodate the exponential growth of IoT devices.
5. Reliability: Networks should ensure uninterrupted operation even in adverse conditions.

Emerging Technologies Complementing Blockchain in IoT

1. Artificial Intelligence (AI): AI algorithms analyze blockchain data to predict device failures and optimize network performance.
2. Edge Computing: Processes IoT data locally, reducing the load on blockchain networks and improving response times.
3. 5G NETWORKS: Provides the high-speed, low-latency backbone necessary for seamless blockchain-IoT integration.
4. Quantum Computing: Potentially enhances encryption techniques and accelerates consensus processes in blockchain networks.

Future Directions and Research Opportunities

1. Scalability Enhancements: Develop hybrid blockchain models to manage the growing number of IoT devices. Implement sharding techniques to partition the blockchain and reduce processing load.
2. Integration with AI: Leverage artificial intelligence to predict network traffic patterns and optimize blockchain operations. AI-driven anomaly detection enhances security in IoT networks.
3. Green Blockchain: Focus on reducing blockchain's energy consumption for sustainable IoT operations. Explore consensus mechanisms that rely on renewable energy sources.
4. Standardization: Establish global standards for integrating blockchain with IoT protocols. Facilitate interoperability between different blockchain platforms and IoT devices.
5. Advanced Security Mechanisms: Develop post-quantum cryptographic techniques to secure IoT data against quantum computing threats. Implement multi-factor authentication for IoT devices accessing blockchain networks.

Dynamic Network Management: Real-time adaptation of blockchain parameters based on network conditions. Incorporation of self-healing mechanisms to ensure uninterrupted operations.

4. Conclusions

Blockchain technology provides a transformative framework for addressing the challenges of wireless IoT sensor networks. By ensuring data security, integrity, and scalability, blockchain enhances the reliability and efficiency of IoT applications across industries. As research and development

continue, the integration of blockchain with IoT sensor networks promises to unlock new possibilities for secure and intelligent systems. Future advancements in consensus mechanisms, energy efficiency, and standardization will further solidify blockchain's role in the IoT ecosystem.

The synergy between blockchain and IoT lays the foundation for next-generation digital ecosystems. By addressing current challenges and leveraging emerging technologies, blockchain-enabled IoT networks can drive innovation, enhance operational efficiency, and ensure a sustainable and secure future for diverse applications.

References

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Retrieved from*: https://bitcoin.org/bitcoin.pdf

[2] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, *2292-2303.* https://doi.org/10.1109/ACCESS.2016.2566339

[3] Dorri, A., Kanhere, S.S. & Jurdak, R. (2017). Blockchain in Internet of Things: Challenges and Solutions. *IEEE IoT Journal*, *4(6), 2252- 2263.* https://doi.org/10.1109/JIOT.2017.2746189

[4] Ali, M., Nelson, J., Shea, R. & Freedman, M. J. (2016). Blockstack: A Global Naming and Storage System Secured by Blockchains. *USENIX Annual Technical Conference*. *Retrieved from*: https://www.usenix.org/conference/atc16/technical-sessions/presentation/ali

[5] Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional*, *19(4), 68-72.* https://doi.org/10.1109/MITP.2017.3051335

[6] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. & Wan, J. (2019). Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of Things Journal*, *6(2), 1594-1605.* https://doi.org/10.1109/JIOT.2018.2879703

[7] Ferrag, M. A., Shu, L., Choo, K.-K. R. & Derradji, F. (2018). Blockchain Technologies for IoT: Research Issues and Challenges. *IEEE Internet of Things Journal*, *6(2), 2188-2204.* https://doi.org/10.1109/JIOT.2018.2882041

[8] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and Its Integration with IoT. *Future Generation Computer Systems*, *(88), 173-190.* https://doi.org/10.1016/j.future.2018.05.046

[9] Wang, H., Chen, Z. & Xu, H. (2019). IoT-Blockchain: A Decentralized Solution for Security and Privacy Challenges in IoT Systems. *Computers & Security*, *(87), 101-116.* https://doi.org/10.1016/j.cose.2019.101586

[10] Esposito, C., De Santis, A., Tortora, G., Chang, H. & Choo, K.-K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5(1), 31-37.* https://doi.org/10.1109/MCC.2018.011791712

IoT сымсыз сенсорлық желілеріне арналған блокчейн

А. Хабибуллин, А. Разак*, Ж. Кальпеева

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: a-razaque@onu.edu*

Аңдатпа. Блокчейн технологиясының IoT сымсыз сенсорлық желілерімен жақындасуы қауіпсіздіктің, деректердің тұтастығының, ауқымдылығының және энергия тиімділігінің маңызды мәселелерін шешетін жаңашыл жаңалық ретінде пайда болды. Заттар Интернеті құрылғылары мен сенсорларының әртүрлі салаларға таралуымен олар жасайтын деректердің үлкен көлемін басқару және олардың қауіпсіздігін қамтамасыз ету өте маңызды болды. Блокчейннің орталықтандырылмаған, өзгермейтін бухгалтерлік жүйесі осы мәселелер үшін тамаша шешім ұсынады.

Негізгі сөздер: *блокчейн, сымсыз, интернет заттары, сенсорлық желілер, қауіпсіздік, деректердің тұтастығы*.

Блокчейн для беспроводных сенсорных сетей IoT

А. Хабибуллин, А. Разак*, Ж. Кальпеева

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: a-razaque@onu.edu*

Аннотация. Конвергенция технологии блокчейн с беспроводными сенсорными сетями Интернета вещей стала новаторской инновацией, решающей важнейшие вопросы безопасности, целостности данных, масштабируемости и энергоэффективности. С распространением устройств и датчиков Интернета вещей в различных отраслях управление и защита огромных объемов данных, которые они генерируют, приобрели первостепенное значение. Децентрализованная, неизменяемая система учета на блокчейне предлагает идеальное решение для этих задач.

Ключевые слова: *блокчейн, беспроводная связь, IoT, сенсорные сети, безопасность, целостность данных.*

Received: 17 October 2024
Accepted: 16 March 2025
Available online: 31 March 2025