INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 07 (2025)

THE ROLE AND POTENTIAL OF BLOCKCHAIN TECHNOLOGY IN SECURING IOT DEVICES

Rustamjonova Moxinur Jo'rabek kizi

Student of Kokand University, Andijan Branch, Faculty of Social-Humanitarian Sciences and Pedagogy, Part-time Department of Computer Engineering, Group 24-02

Abstract: The exponential growth of the Internet of Things (IoT) has introduced unprecedented convenience and interconnectivity, but also significant security vulnerabilities. Traditional security architectures are increasingly inadequate for the decentralized and resource-constrained nature of IoT networks. This article explores the integration of blockchain technology as a robust solution for enhancing IoT security. We discuss the architecture, potential applications, and current limitations of blockchain-based security frameworks in the IoT ecosystem. Real-world use cases in smart cities, healthcare, and industrial IoT are also presented.

Keywords: IoT security, blockchain, distributed ledger, device authentication, smart contracts, cybersecurity

The Internet of Things (IoT) has become a core driver of digital transformation, enabling a vast network of interconnected devices to collect, exchange, and analyze data in real-time. However, the proliferation of IoT devices also expands the attack surface, making them attractive targets for cyber threats such as spoofing, data tampering, DDoS attacks, and unauthorized access[1]. Conventional centralized security models are often inadequate for IoT ecosystems, where devices typically have limited computing power and operate in decentralized environments. In this context, blockchain technology, with its decentralized, immutable, and transparent nature, offers a promising paradigm for enhancing IoT security[2].

- **Overview of Blockchain Technology**

Blockchain is a distributed ledger technology (DLT) that maintains a continuously growing list of records, called blocks, that are securely linked using cryptographic hashes. The core attributes of blockchain—immutability, consensus, transparency, and decentralization—make it highly suitable for applications requiring integrity, traceability, and trust[3]. In a blockchain network, all transactions are verified through consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), and stored in a decentralized manner, thereby eliminating single points of failure[4].

[1] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

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

[4] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data. https://doi.org/10.1109/BigDataCongress.2017.85

- **Challenges of IoT Security**

IoT devices often operate autonomously and are deployed in untrusted environments. Key security challenges include:

- Weak authentication and authorization protocols
- Insecure data transmission and storage
- Lack of centralized monitoring and response mechanisms
- Firmware vulnerabilities and unpatched software[5]

Furthermore, due to resource limitations, many IoT devices are incapable of implementing robust cryptographic operations.

- **Blockchain as a Solution for IoT Security**

➢ Decentralized Device Authentication

Blockchain enables decentralized authentication, allowing IoT devices to verify their identities using cryptographic keys and digital signatures without relying on centralized certificate authorities[6]. Projects like IBM's ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) have demonstrated the use of blockchain for M2M (machine-to-machine) authentication.

➢ Data Integrity and Tamper Resistance

Blockchain's immutability ensures that data recorded by IoT sensors cannot be altered retroactively, enabling trustworthy logs and audit trails[7]. This is critical in applications like medical monitoring or industrial automation, where data integrity can have life-threatening implications.

➢ Smart Contracts for Autonomous Execution

Smart contracts—self-executing code stored on a blockchain—can automate responses to specific IoT events, such as triggering alarms, initiating firmware updates, or performing routine diagnostics[8]. This adds programmability and intelligence to IoT systems while reducing human error.

---

[5] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[6] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

[7] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[8] Buterin, V. (2013). Ethereum white paper: A next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/

➢ Secure Firmware Updates

Blockchain can be used to distribute verified firmware updates across IoT devices, ensuring authenticity and integrity. Each update can be hashed and stored on-chain, and devices can validate them before installation[9].

- **Use Cases**

Smart Cities: In smart grids and traffic systems, blockchain ensures secure data exchange among sensors, meters, and control units[10].

Healthcare IoT: Patient-monitoring devices can record critical health metrics on blockchain to ensure data accuracy and privacy[11].

Industrial IoT (IIoT): Blockchain secures supply chain devices and ensures the traceability of industrial processes, enhancing quality control[12].

- **Limitations and Future Directions**

Despite its promise, blockchain integration into IoT is not without challenges:

o Scalability Issues: Blockchain consensus mechanisms can be resource-intensive and unsuitable for lightweight IoT devices[13].
o Latency: Real-time applications may face delays due to block confirmation times.
o Storage Overhead: Blockchain's growing size poses difficulties for memory-constrained IoT devices.

To address these issues, hybrid approaches like off-chain storage, sidechains, and lightweight consensus protocols (e.g., DAG, IOTA) are being researched[14].

---

[9] Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

[10] Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650–655. https://doi.org/10.1016/j.future.2018.03.066

[11] Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

[12] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[13] Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. Springer.

[14] Popov, S. (2017). The Tangle. IOTA Foundation. https://iota.org/research/academic-papers

Conclusion

Blockchain technology offers a transformative potential in securing IoT systems by addressing critical issues such as trust, authentication, data integrity, and secure automation. While integration challenges remain, especially in terms of scalability and energy efficiency, ongoing advancements in lightweight cryptography and blockchain optimization are paving the way for secure, decentralized IoT ecosystems.

References:

[1]: Weber, R. H. (2010). Internet of Things–New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

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

[4]: Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data. https://doi.org/10.1109/BigDataCongress.2017.85

[5]: Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[6]: Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

[7]: Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[8]: Buterin, V. (2013). Ethereum white paper: A next-generation smart contract and decentralized application platform. https://ethereum.org/en/whitepaper/

[9]: Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251–279. https://doi.org/10.1016/j.jnca.2018.10.019

[^10]: Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. Future Generation Computer Systems, 86, 650–655. https://doi.org/10.1016/j.future.2018.03.066

[^11]: Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

[^12]: Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

[^13]: Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. Springer.

[^14]: Popov, S. (2017). The Tangle. IOTA Foundation. https://iota.org/research/academic-papers