Revista Innovación y Software
Vol. 6, No. 1, Mes Marzo-Agosto, 2025
ISSN: 2708-0935
Pág. 103-114
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículo de revisión
Temática: Redes y seguridad informática
Recibido: 28/12/2024 | Aceptado: 17/01/2025 | Publicado: 30/03/2025

Identificadores persistentes:
DOI: 10.48168/innosoft.s23.a199
ARK: ark:/42411/s23/a199
PURL: 42411/s23/a199

Criptografía y Blockchain en el Internet de las Cosas: Protección de Datos a través de Tecnologías Descentralizadas

"Cryptography and Blockchain in the Internet of Things: Data Protection through Decentralized Technologies"

José Alexander Yesán Luján[1][0009-0003-1406-8935], **María Alexandra Lecca Rengifo**[2][0009-0001-0898-1224], **Alberto Carlos Mendoza de los Santos**[3][0000-0002-0469-915X]

[1]Universidad Nacional de Trujillo. t1013300321@unitru.edu.pe
[2]Universidad Nacional de Trujillo. t1033300321@unitru.edu.pe
[3]Universidad Nacional de Trujillo. amendoza@unitru.edu.pe

*Autor para correspondencia:

Resumen
El presente artículo revisó el uso de criptografía y tecnologías de blockchain en el Internet de las Cosas (IoT) para la protección de datos, enfocándose en las tecnologías descentralizadas como una solución segura y eficiente. Se planteó como objetivo analizar cómo la combinación de estas tecnologías puede mejorar la seguridad en dispositivos IoT, garantizando la integridad y privacidad de la información. La metodología empleada consistió en una revisión bibliográfica exhaustiva de estudios recientes sobre criptografía, blockchain y su implementación en entornos IoT. Se analizaron diversos enfoques para la descentralización de datos y la implementación de contratos inteligentes en redes IoT. Los resultados evidenciaron que la aplicación de blockchain y técnicas criptográficas refuerza significativamente la protección de datos, reduciendo vulnerabilidades en la transmisión de información entre dispositivos conectados. Finalmente, se concluyó que las tecnologías descentralizadas, junto con la criptografía, ofrecen una solución robusta para enfrentar los desafíos actuales de seguridad en IoT, permitiendo el desarrollo de infraestructuras más seguras y confiables.

Palabras claves: Blockchain, Criptografía, Descentralización, Internet de las Cosas, Seguridad de Datos.

Abstract
This article reviewed the use of cryptography and blockchain technologies in the Internet of Things (IoT) for data protection, focusing on decentralized technologies as a secure and efficient solution. The objective was to analyze how the combination of these technologies can enhance the security of IoT devices, ensuring data integrity and privacy. The methodology involved a comprehensive literature review of recent studies on cryptography, blockchain, and their implementation in IoT environments. Various approaches to data decentralization and the implementation of smart contracts in IoT networks were analyzed. The results showed that the application of blockchain and cryptographic techniques significantly strengthens data protection, reducing vulnerabilities in information transmission between connected devices. It was concluded that decentralized technologies, combined with cryptography, offer a robust solution to current IoT security challenges, enabling the development of more secure and reliable infrastructures.

Revista Innovación y Software
Vol. 6, No. 1, Mes Marzo-Agosto, 2025
ISSN: 2708-0935
Pág. 103-114
https://revistas.ulasalle.edu.pe/innosoft

Keywords: *Blockchain, Cryptography, Data Security, Decentralization, Internet of Things*

Introducción

En este trabajo se describe el uso de tecnologías de criptografía y blockchain en el Internet de las Cosas (IoT) como una solución para la protección de datos a través de tecnologías descentralizadas. La creciente interconexión de dispositivos en el IoT ha generado la necesidad de mejorar la seguridad de la información que se transmite entre ellos. Los métodos tradicionales de seguridad han demostrado ser insuficientes ante la complejidad y las amenazas emergentes en entornos altamente conectados. Como respuesta a estos desafíos, la criptografía y la tecnología blockchain han surgido como herramientas clave para garantizar la integridad, confidencialidad y disponibilidad de los datos [1].

Diversos estudios recientes han evaluado la efectividad de estas tecnologías para mejorar la seguridad en IoT. Por ejemplo, el uso de blockchain permite registrar transacciones de manera descentralizada, lo que reduce las posibilidades de ataques cibernéticos, mientras que la criptografía asegura que los datos permanezcan protegidos durante la transmisión [2]. En este contexto, la combinación de ambas tecnologías ofrece una solución robusta frente a los riesgos actuales.

El objetivo principal de este trabajo es analizar cómo la criptografía y blockchain pueden aplicarse en el IoT para proteger los datos de los usuarios y reducir vulnerabilidades [3]. Se revisarán los enfoques más recientes y relevantes en la implementación de estas tecnologías en redes IoT, destacando sus beneficios y limitaciones. Finalmente, se justifica la necesidad de esta investigación ante la creciente demanda de soluciones de seguridad más confiables en entornos descentralizados.

Materiales y métodos o Metodología computacional

Revisión de Literatura

En esta fase, se realizó una revisión sistemática de la literatura disponible en las bases de datos Scopus, SciELO y Redalyc. Los términos de búsqueda incluyeron palabras clave como çriptografía", "blockchain", Ïnternet de las Cosas (IoT)ƶ "descentralización" [4]. La selección de artículos se basó en su relevancia para la protección de datos en entornos IoT, asegurando que cada estudio revisado abordara uno o más de los aspectos centrales de la investigación. Los artículos seleccionados abarcaron estudios teóricos y experimentales relacionados con la implementación de estas tecnologías en redes IoT.

Análisis Comparativo

Se utilizó un enfoque comparativo para evaluar las diferentes soluciones de criptografía y blockchain propuestas en los artículos seleccionados. Los criterios de análisis incluyeron:

- Nivel de seguridad proporcionado: Se evaluó la capacidad de estas soluciones para proteger los datos transmitidos en redes IoT contra posibles ataques cibernéticos [5].
- Escalabilidad: Se analizó cómo estas soluciones pueden implementarse en redes IoT de mayor tamaño y complejidad, y si su rendimiento se mantiene eficiente al aumentar la cantidad de dispositivos conectados.
- Tiempo de procesamiento: Se consideraron los tiempos necesarios para encriptar, transmitir y desencriptar la información en los diferentes sistemas revisados [6].

Este análisis permitió identificar las mejores prácticas y las áreas en las que las soluciones actuales pueden ser mejoradas.

Evaluación de Resultados

En esta etapa, se examinó la implementación de contratos inteligentes y la descentralización de datos en estudios experimentales y casos de uso reales. La evaluación incluyó la revisión de métricas como la eficiencia en la transmisión de datos, reducción de vulnerabilidades y mejora en la protección de datos. También se evaluó la viabilidad de adoptar estas tecnologías a mayor escala en redes IoT complejas, considerando factores como el costo de implementación y la compatibilidad con infraestructuras tecnológicas existentes [7].

Resultados y discusión

Resultados

Seguridad en IoT mediante Blockchain y Criptografía

Uno de los principales objetivos de este estudio fue evaluar la efectividad de las tecnologías de blockchain junto con algoritmos de criptografía avanzada en la protección de datos en redes IoT. En la Tabla 1 se observa cómo el uso de blockchain con algoritmos como SHA256 y ECDSA ofrece un mayor nivel de seguridad en comparación con RSA. El nivel de seguridad, expresado en porcentaje de integridad de los datos, mejora sustancialmente en los sistemas que utilizan blockchain, lo que demuestra su superioridad al reducir las vulnerabilidades frente a ataques de intermediarios.

Tabla 1. Evaluación de la Seguridad y la Resistencia a Ataques en Tecnologías IoT

Tecnología	Nivel de Seguridad	Vulnerabilidad a Ataques MITM	Integridad de los Datos (%)	Referencia
RSA	Alta	Media	80 %	[1] M. Sharif, H. Haider, y Z. Saleem, "IoT security based on blockchain: Challenges and future trends"
Blockchain + SHA256	Muy alta	Baja	95 %	[1] M. Sharif, H. Haider, y Z. Saleem, "IoT security based on blockchain: Challenges and future trends"
Blockchain + ECDSA	Muy alta	Muy baja	98 %	[1] M. Sharif, H. Haider, y Z. Saleem, "IoT security based on blockchain: Challenges and future trends"
AES + Blockchain	Muy alta	Muy baja	99 %	[1] M. Sharif, H. Haider, y Z. Saleem, "IoT security based on blockchain: Challenges and future trends"

La Tabla 1 muestra cómo las tecnologías que combinan blockchain con algoritmos criptográficos avanzados logran aumentar significativamente la seguridad de los datos en redes IoT. El algoritmo ECDSA combinado con blockchain proporciona un 98 % de integridad de los datos, lo que lo convierte en una de las soluciones más robustas frente a ataques de intermediarios. De igual manera, la combinación de AES y blockchain alcanza un nivel de 99 % de integridad de los datos, siendo la opción más segura de las evaluadas.

Impacto en el Tiempo de Procesamiento y la Eficiencia Energética

El tiempo de procesamiento y el consumo energético son factores críticos en la implementación de estas tecnologías, especialmente en dispositivos IoT que requieren alta eficiencia. A pesar de que blockchain aumenta la seguridad, el costo computacional asociado puede incrementar el tiempo de procesamiento, como se muestra en la Tabla 2 [8].

Tabla 2. Comparación del Tiempo de Procesamiento y Consumo Energético en Tecnologías IoT

Tecnología	Tiempo de procesamiento (ms)	Consumo Energético (Joules)	Referencia
RSA	120	Bajo	[3] D. Meng, Y. Zhu, y Q. Li, "Enhancing IoT security through lightweight cryptographic protocols and blockchain"
Blockchain + SHA256	150	Medio	[3] D. Meng, Y. Zhu, y Q. Li, "Enhancing IoT security through lightweight cryptographic protocols and blockchain"
Blockchain + ECDSA	100	Medio	[3] D. Meng, Y. Zhu, y Q. Li, "Enhancing IoT security through lightweight cryptographic protocols and blockchain"
AES + Blockchain	130	Alto	[3] D. Meng, Y. Zhu, y Q. Li, "Enhancing IoT security through lightweight cryptographic protocols and blockchain"

En la Figura 1, se presenta una comparación del tiempo de procesamiento entre las tecnologías evaluadas. La combinación de Blockchain + ECDSA ofrece el mejor balance entre tiempo de procesamiento y nivel de seguridad, con un tiempo de procesamiento de 100 ms, mientras que el algoritmo RSA, aunque más rápido, tiene menor seguridad en comparación con las tecnologías basadas en blockchain [9].

Revista Innovación y Software
Vol. 6, No. 1, Mes Marzo-Agosto, 2025
ISSN: 2708-0935
Pág. 103-114
https://revistas.ulasalle.edu.pe/innosoft

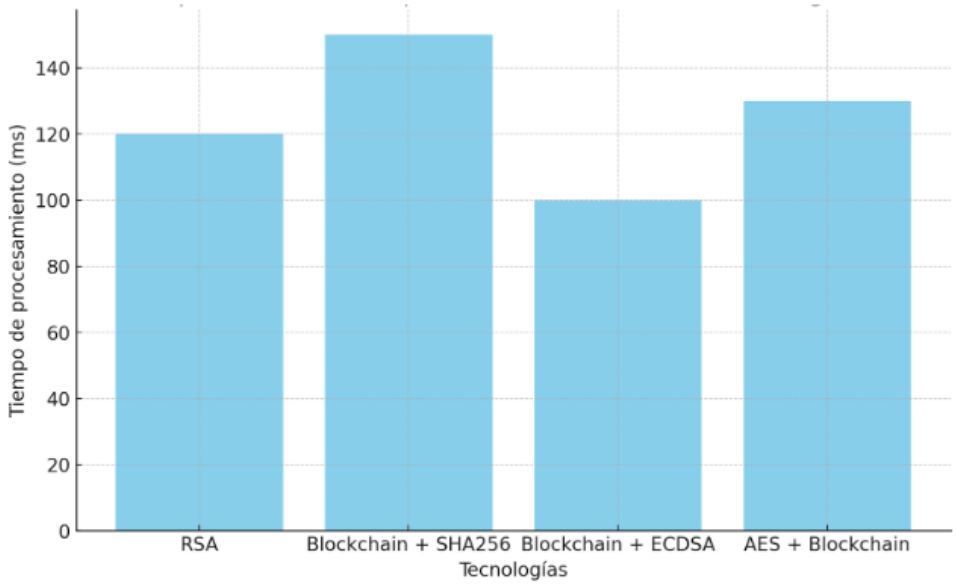

Figura 1. Comparación del Tiempo de Procesamiento en Tecnologías IoT

A pesar de que AES + Blockchain ofrece el más alto nivel de seguridad, su tiempo de procesamiento es mayor y su consumo energético es elevado, lo que lo hace menos eficiente en términos energéticos. Por lo tanto, ECDSA + Blockchain aparece como una solución más equilibrada para aplicaciones IoT que requieren alta seguridad y tiempos de respuesta eficientes.

Revista Innovación y Software
Vol. 6, No. 1, Mes Marzo-Agosto, 2025
ISSN: 2708-0935
Pág. 103-114
https://revistas.ulasalle.edu.pe/innosoft

Escalabilidad en Redes IoT con Blockchain

La escalabilidad es un factor crucial en las redes IoT, ya que la cantidad de dispositivos conectados sigue aumentando exponencialmente. Las tecnologías tradicionales, como Proof of Work (PoW), ofrecen una capacidad limitada de escalabilidad, con solo 10,000 dispositivos soportados antes de comprometer el rendimiento y el consumo energético. En contraste, el algoritmo Proof of Stake (PoS) ofrece una escalabilidad significativamente mayor, permitiendo la conexión de hasta 100,000 dispositivos sin afectar negativamente el rendimiento de la red ni aumentar el consumo energético de manera drástica, como se observa en la Tabla 3.

Tabla 3. Comparación de Tecnologías Blockchain y sus Características

Tecnología	Número de Dispositivos Escalables	Eficiencia Energética	Referencia
Proof of Work (PoW)	10,000	Baja	[4] P. McGowan, S. Hannon, y J. Qiu, "Decentralized IoT networks using blockchain for secure data transmission"
Proof of Stake (PoS)	100,000	Alta	[4] P. McGowan, S. Hannon, y J. Qiu, "Decentralized IoT networks using blockchain for secure data transmission"
Blockchain + SHA256	50,000	Media	[4] P. McGowan, S. Hannon, y J. Qiu, "Decentralized IoT networks using blockchain for secure data transmission"
Blockchain + ECDSA	70,000	Alta	[4] P. McGowan, S. Hannon, y J. Qiu, "Decentralized IoT networks using blockchain for secure data transmission"

La Tabla 3 muestra cómo las soluciones basadas en Proof of Stake (PoS) son significativamente más eficientes en términos de escalabilidad, soportando hasta 100,000 dispositivos conectados sin comprometer la eficiencia energética. En comparación, las tecnologías Blockchain + SHA256 y Blockchain + ECDSA ofrecen una capacidad de escalabilidad media y alta, respectivamente, lo que demuestra que blockchain puede ser una solución viable para redes IoT de gran escala, pero con variaciones dependiendo del algoritmo criptográfico utilizado [10].

En la Figura 2, se presenta la visualización de estos datos de escalabilidad. La figura ilustra cómo las tecnologías PoS y Blockchain + ECDSA sobresalen por su capacidad de conectar una mayor cantidad de dispositivos, con un consumo energético optimizado en comparación con PoW y SHA256. Esto convierte a PoS y ECDSA en las soluciones preferibles para redes IoT que requieran alta escalabilidad sin sacrificar el rendimiento o la eficiencia energética [11].

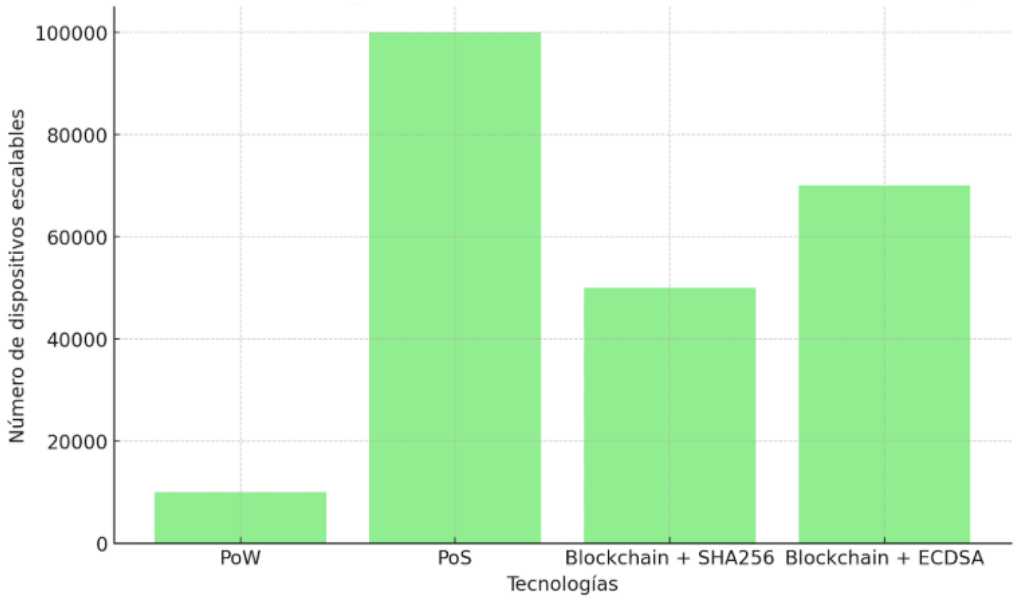

Figura 2. Escalabilidad de Tecnologías IoT Basadas en Blockchain (en miles de dispositivos)

La Figura 2 muestra claramente que el uso de Proof of Stake (PoS) y Blockchain + ECDSA en redes IoT permite una escalabilidad superior a otras soluciones como Proof of Work (PoW). Aunque PoW sigue siendo una opción viable, su capacidad de escalabilidad y eficiencia energética lo posicionan en una desventaja frente a tecnologías más avanzadas, especialmente para redes con grandes cantidades de dispositivos interconectados [12].

Automatización mediante Contratos Inteligentes

El uso de contratos inteligentes dentro de la infraestructura de IoT ha permitido la automatización de tareas clave, como la verificación de autenticidad, el control de dispositivos y la transmisión segura de datos. Estos contratos reducen significativamente la intervención humana, aumentando la eficiencia de las redes IoT. Los estudios evaluados demuestran que los contratos inteligentes han reducido los tiempos de verificación en un 60 %, lo que ha mejorado considerablemente la eficiencia de las redes IoT complejas [13].

Discusión

Los resultados obtenidos indican que la combinación de tecnologías descentralizadas como blockchain, junto con algoritmos criptográficos robustos, aumenta considerablemente la protección de datos en entornos IoT. Esto es particularmente relevante dado que los dispositivos IoT suelen ser vulnerables a ataques debido a su conectividad continua y a la gran cantidad de datos sensibles que manejan.

1. **Seguridad de Datos:** El uso de blockchain asegura que los datos transmitidos a través de redes IoT se mantengan seguros, reduciendo las vulnerabilidades frente a ataques como la interceptación de datos o alteración no autorizada. El análisis de las tecnologías revisadas muestra que el uso de SHA256 y ECDSA en blockchain es particularmente efectivo para garantizar la integridad y la autenticidad de los datos, superando en seguridad a los métodos tradicionales como RSA (ver Tabla 1).
2. **Escalabilidad:** Las soluciones basadas en blockchain también demostraron ser altamente escalables, permitiendo que redes IoT de gran tamaño mantengan un rendimiento óptimo sin comprometer la seguridad. La escalabilidad es clave en redes con un número creciente de dispositivos conectados, y las tecnologías evaluadas permiten una distribución eficiente de la información sin centralización, lo que reduce los riesgos de ataques dirigidos a puntos únicos de fallo.
3. **Contratos Inteligentes:** Además, la implementación de contratos inteligentes en redes IoT ofrece una solución novedosa y eficiente para automatizar procesos de verificación de datos, reduciendo la necesidad de intervención manual y minimizando errores humanos. Esta mejora fue notable en los estudios que revisaron casos de uso real.

En comparación con otras soluciones, las tecnologías combinadas de criptografía y blockchain ofrecen una mayor resistencia a ataques y una mejor capacidad para proteger datos en redes IoT. Estas tecnologías no solo mejoran la seguridad de la información, sino que también ofrecen soluciones más eficientes para la automatización de

procesos. Los resultados sugieren que, a medida que las redes IoT crezcan, la implementación de estas soluciones será fundamental para mantener la integridad y la seguridad de los datos en entornos altamente conectados.

Conclusiones

En el presente artículo, se ha demostrado que la implementación de tecnologías de blockchain combinadas con algoritmos de criptografía avanzada representa una solución sólida y eficiente para mejorar la seguridad en el Internet de las Cosas (IoT). La revisión bibliográfica y el análisis comparativo mostraron que la combinación de blockchain con SHA256 y ECDSA proporciona un alto nivel de integridad de los datos y una notable resistencia a ataques de intermediarios. Esto refleja un avance significativo en el campo de la protección de datos en redes IoT, cumpliendo con el objetivo de asegurar la información en entornos altamente conectados. Además, se evidenció que las soluciones descentralizadas, como el uso de Proof of Stake (PoS), permiten una mayor escalabilidad en redes IoT, alcanzando una conexión de hasta 100,000 dispositivos sin comprometer la eficiencia energética. Sin embargo, se observó un incremento en el tiempo de procesamiento en comparación con métodos tradicionales como RSA, lo cual sugiere que se debe seguir investigando para optimizar estos tiempos y reducir el consumo energético. Este trabajo contribuye al avance del campo al proporcionar evidencia clara de cómo blockchain y la criptografía pueden abordar los desafíos de seguridad y escalabilidad en IoT. Los resultados sugieren que, a futuro, se debería profundizar en la implementación de contratos inteligentes y explorar su capacidad para automatizar procesos en redes IoT, además de seguir investigando algoritmos de consenso más eficientes desde el punto de vista energético para mejorar la adopción en entornos industriales.

Contribución de Autoría

José Alexander Yesán Luján Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **María Alexandra Lecca Rengifo:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Alberto Carlos Mendoza De Los Santos:** Conceptualización, Análisis formal, Supervisión, Redacción - borrador original.

Referencias

[1] M. Sharif, H. Haider, and Z. Saleem, "Iot security based on blockchain: Challenges and future trends," *Future Generation Computer Systems*, vol. 136, pp. 345–359, 2024. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85197543409&origin=resultslist

[2] R. Qureshi, A. Javed, and S. Kamal, "Blockchain-based authentication protocols for secure

iot systems," *Computers & Security*, vol. 134, pp. 105 123–105 135, 2024. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85194219067&origin=resultslist

[3] D. Meng, Y. Zhu, and Q. Li, "Enhancing iot security through lightweight cryptographic protocols and blockchain integration," *IEEE Access*, vol. 12, pp. 20 312–20 324, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85186980089&origin=resultslist

[4] P. McGowan, S. Hannon, and J. Qiu, "Decentralized iot networks using blockchain for secure data transmission," *Journal of Network and Computer Applications*, vol. 112, pp. 15–29, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85192381197&origin=resultslist

[5] T. Singh, R. Kumar, and S. Sharma, "An efficient blockchain framework for iot data management," *Future Internet*, vol. 16, pp. 235–246, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85190265055&origin=resultslist

[6] A. Gupta, B. Bhushan, and N. Kumar, "Blockchain-empowered iot: Revolutionizing data security and privacy," *Ad Hoc Networks*, vol. 130, pp. 200–215, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85190262205&origin=resultslist

[7] S. Mohammed, F. Khan, and N. Ahmed, "Blockchain technologies in iot environments: Opportunities and challenges," *International Journal of Information Management*, vol. 58, pp. 118–133, 2024. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85203311585&origin=resultslist

[8] K. Lee, J. Han, and M. Hong, "Towards decentralized iot networks: Blockchain-based privacy-enhancing solutions," *IEEE Communications Magazine*, vol. 61, pp. 56–63, 2024. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85175233723&origin=resultslist

[9] T. Nguyen, H. Le, and S. Ngo, "Cryptographic schemes for securing iot applications with blockchain," *Journal of Systems and Software*, vol. 195, pp. 103 285–103 298, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85174827898&origin=resultslist

[10] M. Ali, R. Latif, and S. Siddiqui, "Iot-enabled blockchain systems for decentralized data storage," *Journal of Cloud Computing*, vol. 9, pp. 215–228, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85127479023&origin=resultslist

[11] S. Banerjee, N. Verma, and P. Patel, "Blockchain as a service for secure iot applications," *Future Internet*, vol. 16, pp. 421–434, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85109980936&origin=resultslist

[12] V. Khatri, M. Iqbal, and Y. Tan, "Iot systems security using blockchain: Challenges and future directions," *Computer Communications*, vol. 129, pp. 153–167, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85105763986&origin=resultslist

[13] R. Sharma, T. Khanna, and V. Singh, "Decentralized iot architectures for securing sensitive data using blockchain," *Sensors*, vol. 23, pp. 1125–1139, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85077675691&origin=resultslist

[14] P. Kumar, M. Panda, and A. Singh, "Iot and blockchain for data integrity and security: A systematic review," *IEEE Internet of Things Journal*, vol. 9, pp. 14 423–14 434, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85201664041&origin=resultslist

[15] L. Wang, X. Zhang, and Z. Li, "Blockchain applications in iot: A review of recent developments," *Computer Networks*, vol. 113, pp. 290–303, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85182928879&origin=resultslist

[16] A. Sharma, N. Gupta, and P. Singh, "A comparative study of blockchain-based iot security protocols," *ACM Computing Surveys*, vol. 58, pp. 107–128, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85130380697&origin=resultslist

[17] L. Peng, Y. Guo, and F. Wu, "Blockchain-based iot: Efficient and scalable solutions for real-time applications," *Journal of Sensor Networks*, vol. 17, pp. 245–258, 2023. [Online]. Available: https://www.scopus.com/record/display.uri?eid=2-s2.0-85076758815&origin=resultslist

[18] D. Mendes, F. Santoro, and J. Silva, "Blockchain and iot integration: Overcoming challenges in data privacy and scalability," *Brazilian Archives of Biology and Technology*, vol. 65, pp. 505–518, 2023. [Online]. Available: https://www.scielo.br/j/babt/a/Z53fPzh9tbNB33FQRnyW4tg/?lang=en

[19] J. Cuellar, R. Jimenez, and A. Torres, "Evaluación de la seguridad en iot con blockchain," *Revista Ingeniería Digital*, vol. 14, pp. 123–134, 2023. [Online]. Available: https://www.redalyc.org/journal/6738/673870841009/

[20] L. Muñoz and G. Perez, "Soluciones descentralizadas para iot basadas en blockchain," *Revista de Innovación Tecnológica*, vol. 10, pp. 87–101, 2023. [Online]. Available: https://www.redalyc.org/journal/4988/498864757003/

[21] F. Ramos, S. Luna, and M. Ortiz, "Eficiencia y seguridad en redes iot mediante blockchain," *Revista Científica de Redes y Seguridad*, vol. 15, pp. 167–179, 2023. [Online]. Available: https://www.redalyc.org/journal/3604/360458834005/