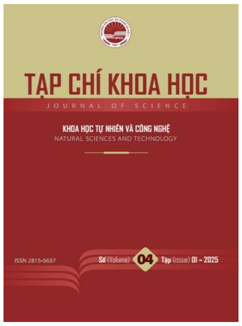
HPU2 Journal of Sciences:
Natural Sciences and Technology

Journal homepage: https://sj.hpu2.edu.vn


TẠP CHÍ KHOA HỌC
JOURNAL OF SCIENCE
KHOA HỌC TỰ NHIÊN VÀ CÔNG NGHỆ
NATURAL SCIENCES AND TECHNOLOGY
ISSN 2815-5637
Số (Volume) 04 Tập (issue) 01 – 2025

Article type: Research article

Blockchain with IoT to enhance security, data integrity, and automation

Thi-Nhung Nguyen*

Thai Nguyen University of Information and Communication Technology, Thai Nguyen, Vietnam

Abstract

The integration of Blockchain technology with the Internet of Things (IoT) presents a transformative approach to addressing critical challenges in security, data integrity, and automation. This paper explores the synergies between these technologies, proposing a framework that leverages the decentralized and immutable nature of Blockchain to enhance IoT ecosystems. By eliminating single points of failure, Blockchain ensures robust security for IoT devices and networks. Furthermore, its transparent and tamper-resistant data structure guarantees the integrity of data exchanged across IoT systems. The study also examines how smart contracts can automate processes within IoT environments, enabling real-time decision-making and reducing human intervention. Practical use cases, such as secure supply chain management, automated healthcare systems, and industrial IoT applications, are discussed to illustrate the effectiveness of the proposed framework. The results demonstrate significant improvements in system resilience, trustworthiness, and operational efficiency, highlighting the potential of Blockchain-enabled IoT to revolutionize diverse industries.

Keywords: Blockchain, IOT, system, industrial, technology, security

1. Introduction

1.1. Background on Blockchain Technology

Blockchain technology, originally conceptualized in 2008 by an anonymous person or group of people under the pseudonym Satoshi Nakamoto, was first implemented in 2009 as the foundational technology behind Bitcoin, the first cryptocurrency. The core idea of blockchain is a decentralized and distributed digital ledger that records transactions across multiple computers in such a way that the recorded transactions cannot be altered retroactively [1], [2].

[*] Corresponding author, E-mail: ntnhung@ictu.edu.vn

https://doi.org/10.56764/hpu2.jos.2024.4.1.84-94

Received date: 09-01-2025; Revised date: 03-3-2025; Accepted date: 27-3-2025

A blockchain is composed of a series of blocks, each containing a list of transactions. These blocks are linked together in a chronological order, forming a chain. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. This structure ensures that once a block is added to the blockchain, it becomes immutable and any attempt to alter the data in a block would require altering all subsequent blocks, which is computationally impractical [1], [2].

One of the primary features of blockchain is decentralization. Unlike traditional centralized databases, a blockchain does not rely on a single central authority. Instead, it is maintained by a network of nodes (computers) that follow a consensus protocol to agree on the validity of transactions. This decentralization enhances the security and transparency of the system, as there is no single point of failure and all participants can verify the data independently [2], [3].

Blockchain technology can be classified into three main types: public, private, and consortium. Public blockchains, like Bitcoin and Ethereum, are open to anyone and are fully decentralized. Private blockchains are restricted to specific participants and are often used within organizations to enhance security and efficiency. Consortium blockchains are semi-decentralized, controlled by a group of organizations, and are typically used in industries requiring collaboration between multiple entities [2], [4].

The key components of blockchain technology include blocks, chains, nodes, and consensus mechanisms. Blocks contain the transaction data and a hash of the previous block. The chain is a sequence of these blocks. Nodes are the network participants that maintain the blockchain and validate transactions. Consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), ensure that all nodes agree on the state of the blockchain [1].

Blockchain offers several advantages, including enhanced security through cryptographic techniques, transparency due to its public ledger, and immutability which ensures that data, once written, cannot be altered. These characteristics make blockchain an appealing technology for various applications beyond cryptocurrencies, such as supply chain management, healthcare, finance, and more [2].

1.2. Overview of Internet of Things (IoT)

The Internet of Things (IoT) is a transformative paradigm that envisions a world where everyday physical objects are connected to the internet, allowing them to collect, exchange, and process data autonomously. This interconnected network of devices ranges from simple household items like refrigerators and thermostats to complex industrial machines and smart city infrastructures. By integrating sensors, software, and connectivity, IoT enables objects to communicate and interact with each other and with humans in real-time [2], [5].

The IoT ecosystem comprises various components, including sensors and actuators, which gather and respond to data, connectivity protocols that enable communication between devices, and data processing units that analyze and interpret the collected information. Sensors are embedded in devices to capture data such as temperature, humidity, light, and motion. Actuators, on the other hand, can initiate actions based on processed data, like adjusting the thermostat or turning on lights [1], [5].

IoT applications are diverse and span across numerous sectors. In healthcare, IoT devices such as wearable health monitors track patients' vital signs and send alerts to healthcare providers in case of anomalies, enhancing patient care and remote monitoring capabilities. In agriculture, IoT-based smart farming techniques use sensors to monitor soil moisture, weather conditions, and crop health, optimizing resource use and improving yield. Smart cities leverage IoT to manage infrastructure efficiently, from traffic lights and parking systems to waste management and energy grids, promoting sustainability and improving the quality of urban life. In manufacturing, IoT enables predictive maintenance by monitoring machinery conditions in real-time, reducing downtime and operational costs [1], [2], [5].

Despite its vast potential, IoT faces several challenges. Security is a significant concern, as interconnected devices are susceptible to cyberattacks that can compromise sensitive data and disrupt services. Ensuring data integrity and privacy in an environment where vast amounts of information are collected and transmitted is another critical issue. Scalability is also a challenge, as the number of connected devices grows exponentially, requiring robust infrastructure and efficient management systems. Additionally, the lack of standardization across different IoT platforms can hinder interoperability and seamless integration of devices from various manufacturers [6].

We give an example of implementing blockchain in IoT system by the following figure (Figure 1).

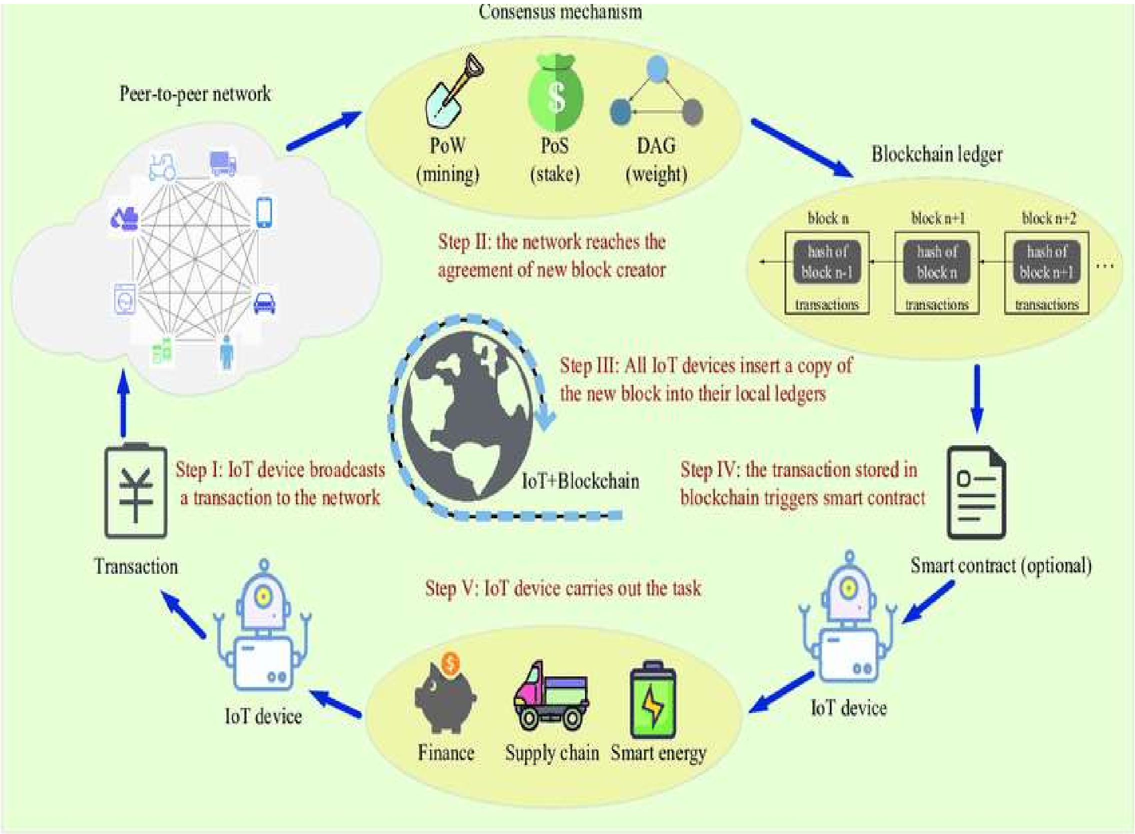

Consensus mechanism
Peer-to-peer network
PoW (mining)
PoS (stake)
DAG (weight)
Blockchain ledger
block n
block n+1
block n+2
hash of block n-1
hash of block n
hash of block n+1
transactions
transactions
transactions
Step II: the network reaches the agreement of new block creator
Step III: All IoT devices insert a copy of the new block into their local ledgers
IoT+Blockchain
Step I: IoT device broadcasts a transaction to the network
Step IV: the transaction stored in blockchain triggers smart contract
Transaction
Smart contract (optional)
Step V: IoT device carries out the task
IoT device
IoT device
Finance
Supply chain
Smart energy

Figure 1. An example of implementing blockchain in IoT system Source : Scientific Diagram [3]

1.3. Importance of Integrating Blockchain with IoT

Integrating blockchain with the Internet of Things (IoT) holds significant potential for enhancing security, data integrity, and automation across various applications. IoT systems, which consist of interconnected devices that collect, exchange, and process data, are increasingly prevalent in industries such as healthcare, agriculture, smart cities, and manufacturing. However, these systems face substantial challenges related to security, data integrity, and the efficient management of vast amounts of data [1], [6].

One of the primary reasons for integrating blockchain with IoT is to address security concerns. IoT devices are often vulnerable to cyberattacks due to their interconnected nature and the varying levels of security implemented across different devices. Blockchain’s decentralized and immutable ledger can enhance the security of IoT networks by providing a secure method for recording and verifying transactions. Each transaction or data exchange recorded on the blockchain is time-stamped and cannot be altered without the consensus of the network, thus significantly reducing the risk of tampering and unauthorized access. Additionally, the decentralized nature of blockchain eliminates the single point of failure, making IoT systems more resilient to attacks [2], [4], [6].

Data integrity is another critical area where blockchain integration can provide substantial benefits. IoT systems generate vast amounts of data that need to be accurate, consistent, and reliable. Blockchain ensures data integrity by creating a tamper-proof record of all transactions and data exchanges. This immutable record allows for the verification of data authenticity, which is crucial in applications where data accuracy is paramount, such as in healthcare monitoring systems or supply chain management. By using blockchain, organizations can ensure that the data collected from IoT devices is trustworthy and has not been altered, thereby improving decision-making and operational efficiency [6],[7].

Moreover, the integration of blockchain with IoT can significantly enhance automation. Blockchain’s smart contracts, which are self-executing contracts with the terms of the agreement directly written into code, can automate processes within IoT systems. Smart contracts can trigger actions automatically based on predefined conditions, reducing the need for human intervention and minimizing errors. For example, in a smart energy grid, a smart contract could automatically adjust energy distribution based on real-time data from IoT sensors, optimizing energy usage and reducing costs. This level of automation can streamline operations, increase efficiency, and enable more responsive and adaptive systems.

Furthermore, blockchain can improve the scalability and interoperability of IoT networks. As the number of IoT devices continues to grow, managing and processing the data they generate becomes increasingly complex. Blockchain can provide a scalable solution for handling this data by distributing the workload across a decentralized network. Additionally, blockchain’s standardized protocols can facilitate interoperability between different IoT devices and systems, enabling seamless communication and integration across various platforms and applications.

2. Materials and Methods

Blockchain technology, at its core, is a decentralized and distributed digital ledger system designed to record transactions across many computers in such a way that the recorded transactions cannot be altered retroactively. This ensures a high level of security and trust without the need for a central authority. The key characteristics of blockchain include decentralization, where the control of the ledger is distributed among all participants; transparency, where all transactions are visible to all participants; immutability, which prevents any modification of transaction data once it is recorded; and security, ensured through cryptographic methods and consensus mechanisms that validate transactions [1], [7], [8].

Blockchain can be broadly categorized into three types: public, private, and consortium blockchains. Public blockchains, like Bitcoin and Ethereum, are open to anyone and fully decentralized, allowing anyone to participate in the network, validate transactions, and maintain the ledger. Private blockchains, on the other hand, are restricted and controlled by a single organization. These are used primarily for internal purposes where the organization needs to control access and permissions. Consortium blockchains fall somewhere in between, being controlled by a group of organizations rather than a single entity. These are often used in industries where multiple organizations need to collaborate and share information securely, such as banking or supply chain management.

The fundamental components of blockchain technology include blocks, chains, nodes, and consensus mechanisms. A block is a container that holds a list of transactions. Each block contains a unique code called a hash, which is generated from the transaction data within the block, and a hash of the previous block, linking the blocks together in a chronological chain. This linkage forms the blockchain. Nodes are individual computers that participate in the blockchain network, each maintaining a copy of the entire blockchain and working to validate new transactions and blocks. Consensus mechanisms are protocols used by the nodes to agree on the validity of transactions and the order in which they are added to the blockchain. Common consensus mechanisms include Proof of Work (PoW), which requires nodes to solve complex mathematical problems to validate transactions, and Proof of Stake (PoS), which relies on validators who hold and lock up a certain amount of cryptocurrency to secure the network [7], [8].

The advantages of blockchain technology are manifold. Decentralization eliminates the need for a central authority, reducing the risk of centralized control and single points of failure. Security is enhanced through cryptographic techniques that protect transaction data and prevent unauthorized changes. Transparency is achieved by making the transaction history visible to all network participants, which fosters trust and accountability. Immutability ensures that once data is recorded on the blockchain, it cannot be altered or deleted, providing a permanent and tamper-proof record of all transactions. These characteristics make blockchain a powerful tool for creating secure, transparent, and efficient systems across various industries, from finance and healthcare to supply chain management and beyond [8], [9].

The Internet of Things (IoT) refers to the network of interconnected devices embedded with sensors, software, and other technologies that enable them to collect and exchange data with other devices and systems over the internet. IoT devices can range from everyday objects like household appliances and wearable devices to industrial machinery and infrastructure components. The key characteristics of IoT include connectivity, interoperability, autonomy, and the ability to generate and process data in real-time.

IoT systems consist of several key components working together to collect, transmit, and process data. These components include sensors, which gather data from the physical environment, actuators, which control physical processes or devices based on the data received, connectivity technologies such as Wi-Fi, Bluetooth, or cellular networks, and data processing systems that analyze and derive insights from the collected data. Together, these components form a networked ecosystem that enables the seamless exchange of information between devices and systems [9].

IoT technology has numerous applications across various industries, revolutionizing processes and enabling new capabilities. In healthcare, IoT devices such as wearable fitness trackers and remote patient monitoring systems help monitor patients' health status and track vital signs in real-time, leading to improved diagnosis and treatment outcomes. In agriculture, IoT sensors deployed in fields and livestock facilities monitor environmental conditions, soil moisture levels, and animal health, optimizing crop yields and livestock productivity. Smart city initiatives leverage IoT technology to improve urban infrastructure and services, including traffic management, waste management, and energy efficiency. In manufacturing, IoT-enabled smart factories utilize sensors and data analytics to optimize production processes, reduce downtime, and enhance product quality.

Despite its potential benefits, IoT technology also presents several challenges that need to be addressed for widespread adoption and implementation. Security is a major concern, as IoT devices are often vulnerable to cyberattacks due to their interconnected nature and the proliferation of devices with inadequate security measures. Ensuring data integrity and privacy is another challenge, as the massive amounts of data generated by IoT devices raise concerns about unauthorized access and misuse of personal information. Scalability is also a challenge, as the sheer number of IoT devices and the volume of data they generate can overwhelm existing network infrastructure and data processing capabilities. Additionally, interoperability issues between different IoT platforms and devices can hinder seamless communication and integration, limiting the potential benefits of IoT technology.

3. Results and Discussion

IoT devices are susceptible to various security threats due to their interconnected nature and often limited security features. Common security issues in IoT include device vulnerabilities, inadequate authentication mechanisms, lack of encryption for data transmission, susceptibility to malware and botnet attacks, and the risk of unauthorized access to sensitive information. These vulnerabilities can lead to data breaches, privacy violations, and disruptions to critical services.

Blockchain technology offers several security benefits that can address many of the vulnerabilities present in IoT systems. By leveraging its decentralized and immutable ledger, blockchain enhances the security of IoT data by providing tamper-proof and transparent records of device interactions and data transactions. Additionally, blockchain's consensus mechanisms and cryptographic techniques ensure data integrity and authenticity, reducing the risk of unauthorized modifications or tampering. Moreover, blockchain enables secure peer-to-peer communication and device authentication without relying on centralized authorities, enhancing the resilience of IoT networks against cyberattacks [10], [11].

Blockchain-IoT integration employs cryptographic techniques such as public-key cryptography, digital signatures, and hash functions to secure IoT data and communications. Public-key cryptography enables secure device authentication and data encryption, ensuring that only authorized devices can access and transmit data. Digital signatures provide a means of verifying the authenticity and integrity of data exchanged between IoT devices, while hash functions generate unique identifiers for data blocks, enabling tamper-proof data storage and verification. Decentralized security mechanisms inherent in blockchain networks eliminate single points of failure and reduce the risk of malicious attacks, enhancing the overall security posture of IoT systems [11], [12].

Blockchain-IoT integration offers various use cases for enhancing security in IoT applications. Secure device authentication ensures that only authorized devices can access IoT networks and services, preventing unauthorized access and malicious activities. Blockchain-based identity management systems enable secure and decentralized authentication of IoT devices, enhancing trust and transparency in device interactions. Additionally, blockchain enables secure peer-to-peer communication channels between IoT devices, ensuring confidentiality and integrity of data exchanged over the network. Use cases such as secure supply chain management, smart energy grids, and decentralized asset tracking demonstrate the potential of blockchain-IoT integration to address security challenges and unlock new opportunities for secure and resilient IoT deployments.

We give some examples to study as follows.

3.1. Secure supply chain management.

In the food and pharmaceutical industries, blockchain-IoT integration can ensure the integrity and safety of products throughout the supply chain. IoT sensors attached to shipments can monitor temperature, humidity, and other environmental conditions, while blockchain records these data in an immutable ledger. If any discrepancies or deviations occur, smart contracts can trigger alerts or automate actions, such as rerouting shipments or initiating quality control measures. This transparent and tamper-proof system helps prevent counterfeit goods, reduce spoilage, and ensure compliance with regulatory standards [5], [6], [13].

In the pharmaceutical industry, ensuring the integrity and safety of drugs throughout the supply chain is crucial to safeguarding public health. Counterfeit medications, temperature fluctuations, and improper handling during transportation can compromise the efficacy and safety of pharmaceutical products. Blockchain-IoT integration offers a secure and transparent solution to address these challenges [14], [15].

Pharmaceutical companies integrate IoT sensors and devices into packaging and transportation containers to monitor various parameters such as temperature, humidity, light exposure, and location in real-time. These sensors continuously collect data throughout the journey of the drugs from manufacturing facilities to distribution centers to pharmacies. IoT devices securely transmit the collected data to a blockchain network. Each data point is time-stamped, encrypted, and recorded on the blockchain, creating an immutable and tamper-proof ledger of the drug's journey [16], [17]. This ensures transparency and traceability of the entire supply chain process. The blockchain ledger serves as a decentralized database that records all transactions and data exchanges related to the pharmaceutical supply chain. Each participant in the supply chain, including manufacturers, distributors, logistics providers, and regulatory agencies, has access to the blockchain network and can verify the authenticity and integrity of the data.

Smart contracts embedded in the blockchain network automate various supply chain processes based on predefined conditions and rules. For example, if the temperature of a shipment exceeds the specified range, a smart contract can trigger alerts, initiate quality control measures, or even reroute the shipment to prevent spoilage or contamination. Pharmacies and healthcare providers can verify the authenticity and provenance of pharmaceutical products by accessing the blockchain ledger. They can scan a QR code or use a mobile app to access detailed information about the drug's manufacturing history, transportation conditions, and regulatory compliance. This enhances trust and confidence in the quality and safety of the medication [18], [19].

Blockchain-IoT integration enables real-time tracking and authentication of pharmaceutical products, reducing the risk of counterfeit medications entering the supply chain. By verifying the legitimacy of drugs at every stage of the supply chain, stakeholders can ensure that patients receive genuine and safe medications. Continuous monitoring of environmental conditions during transportation and storage using IoT sensors helps maintain the quality and efficacy of pharmaceutical products. Any deviations from the optimal conditions can be detected and addressed promptly, minimizing the risk of product degradation and ensuring compliance with regulatory standards. Blockchain provides a transparent and auditable record of regulatory com

pliance throughout the supply chain. Regulatory agencies can access real-time data on drug shipments and storage conditions, streamline inspection processes, and enforce regulatory requirements more effectively [19], [20].

By enhancing the security and integrity of the pharmaceutical supply chain, blockchain-IoT integration ultimately protects patient safety. Patients can have confidence that the medications they receive are genuine, safe, and effective, leading to better health outcomes and reduced risks of adverse reactions or treatment failures.

3.2. Smart Energy Grids

Blockchain-IoT integration enhances the security and efficiency of energy distribution and management systems. IoT devices installed in smart meters and grid infrastructure can monitor energy consumption, detect anomalies, and optimize energy distribution in real-time. Blockchain technology records energy transactions and ensures transparent billing and settlement processes. Smart contracts can automate energy trading between consumers and producers, enabling peer-to-peer energy transactions while maintaining data privacy and security. This decentralized and secure energy ecosystem promotes renewable energy adoption, reduces operational costs, and enhances grid resilience against cyberattacks and power outages [2], [16].

In logistics and asset management, blockchain-IoT integration enables secure and transparent tracking of assets throughout their lifecycle. IoT devices equipped with GPS, RFID, or sensors can monitor the location, condition, and status of assets in real-time. Blockchain records and verifies asset movements and transactions, providing a tamper-proof audit trail for stakeholders. Smart contracts automate asset management processes, such as inventory tracking, maintenance scheduling, and supply chain logistics, while ensuring data integrity and security. This decentralized and trustless system eliminates manual record-keeping errors, reduces fraud and theft risks, and streamlines asset management operations across industries [16].

Smart energy grids leverage IoT sensors and devices installed in utility infrastructure, power plants, renewable energy sources (such as solar panels and wind turbines), and consumer premises (smart meters, smart appliances) to monitor energy consumption, production, and distribution in real-time. These sensors collect data on energy usage patterns, grid stability, renewable energy generation, and equipment performance [17].

IoT devices securely transmit the collected data to a blockchain network. Each data point, including energy production, consumption, and distribution, is time-stamped, encrypted, and recorded on the blockchain ledger. This creates a transparent and tamper-proof record of energy transactions and grid operations. The blockchain ledger serves as a decentralized database that records all energy-related transactions and data exchanges within the smart energy grid. Each participant in the grid, including energy producers, consumers, grid operators, and regulatory agencies, has access to the blockchain network and can verify the authenticity and integrity of the data.

Smart contracts embedded in the blockchain network automate various energy management processes based on predefined conditions and rules. For example, smart contracts can automatically execute energy trading agreements between prosumers (consumers who also produce energy) and utility companies, optimize energy distribution based on real-time demand and supply dynamics, and incentivize energy conservation and efficiency measures [19], [20].

Blockchain-IoT integration enables peer-to-peer energy trading among consumers and prosumers within the smart energy grid. Prosumers can sell excess energy generated from renewable sources (such as solar panels) to nearby consumers directly, bypassing traditional utility companies. Smart contracts facilitate secure and transparent energy transactions, ensuring fair pricing, settlement, and billing. By integrating IoT sensors and renewable energy sources into the grid, blockchain-IoT integration enables efficient and reliable integration of renewable energy into the energy mix. Real-time monitoring of renewable energy generation and grid stability allows for optimal utilization of clean energy resources and reduces reliance on fossil fuels

IoT sensors provide granular insights into energy consumption patterns and grid operations, enabling grid operators to optimize energy distribution, balance supply and demand, and manage peak loads more effectively. Smart contracts automated demand response programs, incentivizing consumers to adjust their energy usage during periods of high demand or supply constraints. Blockchain-IoT integration facilitates peer-to-peer energy trading, empowering consumers to buy, sell, and exchange energy directly with each other. This decentralized energy marketplace promotes energy democratization, fosters energy independence, and encourages the adoption of renewable energy technologies at the local level. The decentralized and immutable nature of blockchain ensures the security and resilience of the smart energy grid against cyberattacks, data manipulation, and single points of failure. By eliminating intermediaries and central authorities, blockchain-IoT integration enhances trust, transparency, and reliability in energy transactions and grid operations.

3.3. Future Prospects

In this part, We give some future works which can be studied in the near future.

The convergence of blockchain and IoT is expected to lead to several emerging trends in the coming years. These include the widespread adoption of blockchain-based IoT platforms and protocols, the integration of artificial intelligence (AI) and machine learning (ML) with blockchain-IoT systems to enable predictive analytics and autonomous decision-making, and the development of decentralized IoT marketplaces and ecosystems. Additionally, innovations in edge computing, 5G networks, and quantum computing are likely to further enhance the capabilities and scalability of blockchain-IoT solutions.

Future research in blockchain and IoT is expected to focus on addressing key challenges and exploring new opportunities for innovation. Potential innovations include the development of scalable and energy-efficient consensus mechanisms for blockchain networks, the integration of privacy-preserving techniques such as zero-knowledge proofs (ZKPs) and homomorphic encryption with blockchain-IoT systems, and the exploration of novel applications such as blockchain-based autonomous agents and self-sovereign identity management. Moreover, research in areas such as interoperability, sustainability, and governance models for blockchain-IoT ecosystems will play a crucial role in shaping the future of the technology.

Standardization and collaboration will be essential for the widespread adoption and interoperability of blockchain and IoT solutions. Industry consortia, standards bodies, and regulatory authorities will need to work together to establish common protocols, interoperability standards, and regulatory frameworks that facilitate seamless integration and deployment of blockchain-IoT systems across industries and jurisdictions. Collaborative efforts to address security, privacy, and scalability challenges will also be crucial for building trust and confidence in blockchain-IoT technologies among stakeholders.

The long-term impact of blockchain and IoT integration on industries and society is expected to be transformative. In industries such as healthcare, supply chain management, and energy, blockchain-IoT solutions will enable greater efficiency, transparency, and trust, leading to improved quality of services, reduced costs, and enhanced customer experiences. Moreover, the decentralization and democratization of data enabled by blockchain-IoT technologies have the potential to empower individuals, promote data sovereignty, and create new economic opportunities. However, challenges such as digital divide, data privacy, and ethical considerations will need to be addressed to ensure that the benefits of blockchain-IoT integration are equitably distributed and socially responsible.

4. Conclusion

The implications of blockchain-IoT integration are profound for both industry and academia. Industry stakeholders can leverage blockchain-IoT solutions to streamline operations, enhance security, and create new business models. Academia plays a crucial role in advancing research and development in blockchain-IoT technologies, addressing technical challenges, and educating the workforce of the future. As blockchain and IoT continue to evolve, their integration holds the potential to revolutionize various aspects of our lives, from healthcare and supply chain management to energy distribution and smart cities. The future of blockchain-IoT integration is bright, but challenges such as scalability, interoperability, and regulatory compliance must be addressed to realize its full potential. With continued innovation, collaboration, and investment, blockchain-IoT integration will play a pivotal role in shaping the digital economy of tomorrow.

References

[1] E. Ezema, A. Abdullah, and N. F. B. Mohd, “Open Issues and Security Challenges of Data Communication Channels in Distributed Internet of Things (IoT): A Survey,” *Circulation in Computer Science*, vol. 3, no. 1, pp. 22–32, Jan. 2018, doi: 10.22632/ccs-2017-252-63.

[2] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT Security:Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology,” *Internet of Things*, vol. 11, p. 100227, May 2020, doi: 10.1016/j.iot.2020.100227.

[3] C. Li and J. V. de Oliveira, “Advances in intelligent computing for diagnostics, prognostics, and system health management,” *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 6, pp. 3397–3401, Jun. 2018, doi: 10.3233/jifs-169520.

[4] S. Mihai et al., “Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2255–2291, 2022, doi: 10.1109/comst.2022.3208773.

[5] M. H. Miraz and M. Ali, “Integration of Blockchain and IoT: An Enhanced Security Perspective,” *Annals of Emerging Technologies in Computing*, vol. 4, no. 4, pp. 52–63, Oct. 2020, doi: 10.33166/aetic.2020.04.006.

[6] C. Butpheng, K.-H. Yeh, and H. Xiong, “Security and Privacy in IoT-Cloud-Based e-Health Systems–A Comprehensive Review,” *Symmetry*, vol. 12, no. 7, p. 1191, Jul. 2020, doi: 10.3390/sym12071191.

[7] Y. Qu et al., “Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020, doi: 10.1109/jiot.2020.2977383.

[8] Z. Iftikhar et al., “Privacy Preservation in Resource-Constrained IoT Devices Using Blockchain–A Survey,” *Electronics*, vol. 10, no. 14, p. 1732, Jul. 2021, doi: 10.3390/electronics10141732.

[9] S. Sun, R. Du, S. Chen, and W. Li, “Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain,” *IEEE Access*, pp. 1–1, 2021, doi: 10.1109/access.2021.3059863.

[10] S. Algarni et al., “Blockchain-Based Secured Access Control in an IoT System,” *Applied Sciences*, vol. 11, no. 4, p. 1772, Feb. 2021, doi: 10.3390/app11041772.

[11] Y. L. Zhao, “Research on Data Security Technology in Internet of Things,” *Applied Mechanics and Materials*, vol. 433–435, pp. 1752–1755, Oct. 2013, doi: 10.4028/www.scientific.net/amm.433-435.1752.

[12] A. Prashanth Joshi, M. Han, and Y. Wang, “A survey on security and privacy issues of blockchain technology,” *Mathematical Foundations of Computing*, vol. 1, no. 2, pp. 121–147, 2018, doi: 10.3934/mfc.2018007.

[13] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, “Management and Monitoring of IoT Devices Using Blockchain,” Sensors, vol. 19, no. 4, p. 856, Feb. 2019, doi: 10.3390/s19040856.

[14] A. Al-Hasnawi, S. M. Carr, and A. Gupta, “Fog-based local and remote policy enforcement for preserving data privacy in the Internet of Things,” Internet of Things, vol. 7, p. 100069, Sep. 2019, doi: 10.1016/j.iot.2019.100069.

[15] A. Goap, D. Sharma, A. K. Shukla, and C. Rama Krishna, “An IoT based smart irrigation management system using Machine learning and open source technologies,” Computers and Electronics in Agriculture, vol. 155, pp. 41–49, Dec. 2018, doi: 10.1016/j.compag.2018.09.040.

[16]H.Nandanwar and R. Katarya, "Deep learning enabled intrusion detection system for Industrial IOT environment," Expert systems with applications, vol. 249, pp. 123808–123808, Sep. 2024, doi: 10.1016/j.eswa.2024.123808.

[17]M. Andoni et al., "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renewable and Sustainable Energy Reviews, vol. 100, no. 1, pp. 143–174, Feb. 2019, doi: 10.1016/j.rser.2018.10.014.

[18] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, Nov. 2017, doi: 10.1016/j.telpol.2017.09.003.

[19] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[20] E. F. Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," Security and Communication Networks, vol. 2018, pp. 1–27, Apr. 2018, doi:10.1155/2018/9675050.