International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Analyze Compatibility Issues in Integrating Heterogeneous Devices with Blockchain Systems

**Maradani Pavani Devi[1], Dr. Shrija Madhu[2], Navya Padma Priya[3], M Subrahmanyeswara Rao[4]**

**Submitted:** 07/09/2024 **Revised:** 20/10/2024 **Accepted:** 29/10/2024

**ABSTRACT:** The Internet of Things (IoT) is a network of physical objects interconnected over the internet to gather data and facilitate intelligent decision-making. It is a swiftly expanding domain globally, accompanied by accelerated advancements in research sectors. It facilitates worldwide access, monitoring, and control of these devices. The absence of internal security controls jeopardizes IoT, and its rampant use has led to several security and privacy issues. The deficiencies of IoT may be addressed with the integration of blockchain technology. Blockchain technology is a secure, decentralized database management solution that organizes data into blocks. This paper presents a concise overview of the integration of blockchain and IoT. This article's primary contributions are: (i) the benefits of combining both technologies, (ii) the obstacles to their integration, (iii) the use of blockchain and IoT in the education sector, and (iv) prospective advancements of IoT with blockchain.

***KEYWORDS****: Internet of things (IoT), Blockchain (BC), Blockchain with IoT.*

## INTRODUCTION

The use of IoT has significantly increased in the domain of research and technology. This technique creates an automated system requiring minimum human involvement. It simultaneously links millions of devices for communication and information sharing.

Let us get a concise overview of the IoT landscape by examining the below points:

The Internet of Things (IoT) pertains to physical objects that link to a network of technologies, including software and sensors, to exchange data or information.

Software is a program including instructions and mechanisms that function according to these directives.

A sensor is an electrical component that identifies physical activities and transmits data or commands to other systems. The International Telecommunication Union (ITU) research [1] indicates that the Internet of Things (IoT) is gaining prominence, with projections of over twenty billion physical items connecting to the internet via IoT technology by the conclusion of 2021. The Internet of Things has a wide array of applications, including face recognition systems and autonomous cars, among others. [2], [3]. Various types of sensors enable the acquisition of environmental data. IoT gadgets are enhancing our lives. Billions of gadgets are interconnected via the internet, producing substantial amounts of data. The Internet of Things (IoT) is now transforming the globe by offering sophisticated services that link environmental entities for information acquisition; yet, concomitantly, security and privacy issues are increasing. Your sensitive data may be exploited outside your private network via fraudulent authentications. Thilakarathne delineated IoT security concerns concerning the fundamental information security principles of confidentiality, integrity, and availability [4]. Algarni et al. examined a distributed capability-based access control system using public-key cryptography to address some difficulties [5]. Centralized models of IoT devices authenticate users via the server. A centralized authentication system is unnecessary with blockchain technology. A concise overview of blockchain technology is shown here.

1. Blockchain employs networks, routers, and decentralized chains of blocks (referred to as nodes) rather than centralized servers. Every node has a distributed ledger (DL). DL is a distributed database that records each category of transaction and associated information inside this ledger.

A distributed ledger is an open-source digital database accessible to various users. The data is synced and accessible to the user over the network.

[1,2,3,4]*International School Of Technology And Sciences For Women, A.P, India.*

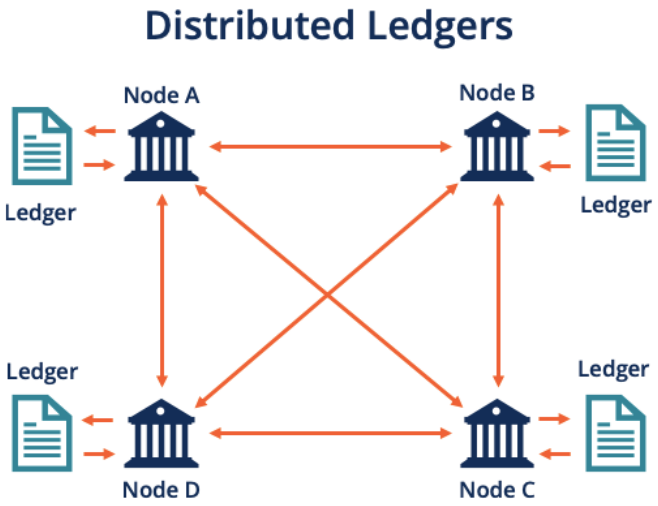


**Figure 1: Shows high level work flow of distributed ledgers at each node**

## LITERATURE REVIEW

A considerable body of research has developed around the incorporation of blockchain technology inside IoT ecosystems. This section concisely encapsulates pertinent surveys on the subject matter.
The following papers provide profound analyses:

Md Ashraf Uddin et al. [61] investigate the integration of blockchain inside IoT systems to address challenges like privacy difficulties, single points of failure, and data bottlenecks. The authors examine current developments in blockchain applications within several IoT domains, such as eHealth and smart cities, while addressing the associated difficulties and possible solutions.

Elhama Shammar et al. [62] examine the integration of blockchain with IoT via a security lens, analyzing studies conducted from 2017 to 2021. Their research classifies articles according to security domains and offers a thorough analysis of contemporary initiatives and obstacles in safeguarding IoT ecosystems with blockchain technology.
Alia Al Sadawi et al. [63] examine the potential of blockchain to improve IoT systems regarding security, authenticity, dependability, and scalability. They investigate the function of blockchain in enhancing data storage, processing, security, and authentication inside IoT, and provide an architectural framework for the integration of these technologies.
Abdelzahir Abdelmaboud et al. [64] provide a comprehensive analysis of how blockchain might address challenges with scalability, interoperability, security, privacy, and trust in IoT applications. They provide a classification of blockchain applications in IoT, examine prominent platforms, and delineate recent advancements and obstacles for future study.

Ahmed Alkhateeb et al. [65] examine the use of hybrid blockchain systems for the Internet of Things (IoT). They examine the motives for using hybrid platforms, the associated technology, and the issues encountered, emphasizing both the benefits and impediments of deploying hybrid blockchain solutions.
Rajesh Kumar and Rewa Sharma [66] investigate the function of blockchain in augmenting trust inside IoT networks. They provide an overview of IoT and blockchain, examine trust-related difficulties, and contrast conventional and blockchain-based trust management methodologies.
Haider Dhia Zubaydi et al. [67] do a thorough literature study on the amalgamation of blockchain and IoT to tackle security and privacy concerns. Their analysis addresses the advantages of enhanced security and anonymity, obstacles including storage capacity and legal concerns, and prospective research trajectories in this field.
Sarvesh Tanwar et al. [68] investigate the potential of blockchain to enhance security and privacy in IoT. The authors examine contemporary research, underscore challenges, and analyze how blockchain's security attributes can mitigate vulnerabilities in IoT systems.
Vinay Gugueoth et al. [69] examine the security and privacy difficulties in the Internet of Things (IoT) and the potential of decentralized blockchain technologies to mitigate these issues. Their research encompasses security risks, blockchain solutions, consensus protocols, and the problems of integrating

blockchain with IoT, providing insights into prospective research avenues.

**Characteristics**

The following are the main qualities of blockchain that enhance its robust applications [63], [64]:
Decentralization: Blockchain functions inside a decentralized structure, whereby various nodes are accountable for administering and sustaining the network. In contrast to centralized systems like conventional banks, which are governed by a single authority, every node in a blockchain network has an identical copy of the digital ledger. This decentralization markedly elevates the expense of hacking, rendering it a crucial attribute for bolstering the security of blockchain-enabled ecosystems.

Immutability: Blockchain constitutes a permanent and unchangeable network of connecting nodes. Each node maintains a replica of the ledger, and every transaction must be authenticated and verified prior to its inclusion in the chain.
This renders the data exceptionally resilient to manipulation owing to the robust safeguards provided by the network. Consequently, blockchain guarantees a transparent and secure framework in which transactions are accessible to everyone but remain immutable and irretrievable.
Automation: Blockchain employs smart contracts to accelerate transaction processing. Smart contracts are digital agreements that autonomously execute upon the fulfillment of specified circumstances. This automation facilitates expedited and more efficient transactions by removing the need for middlemen and human supervision.
Transparency: Blockchain offers unparalleled transparency, essential for sophisticated data security solutions. In the decentralized network, transactions are confirmed by the majority of nodes, enabling users to get real-time updates while ensuring complete transparency across the network. This transparency guarantees the integrity of the data.
Security: Blockchain assures security by encryption of chain addresses and a consensus mechanism that maintains data integrity. Blockchain records of transactions and contracts are secure, hence streamlining IoT protocols. Unlike centralized systems, blockchain offers enhanced safeguards against piracy. The distributed architecture, together with cryptographic hash algorithms, makes data forgery almost difficult, hence safeguarding the integrity of transaction histories and protecting against hostile attacks.
Trust: Blockchain fosters trust by establishing a decentralized, tamper-proof ledger of transactions, eliminating the need for centralized authority. Smart contracts automate the implementation of agreements, hence enhancing confidence among parties. Within the IoT framework, blockchain facilitates dependable transactions, secure data governance, and device identity verification, hence enhancing confidence in IoT networks.
Privacy is a significant barrier in IoT applications, especially when managing sensitive data, as in the healthcare sector.
Although blockchain is regarded as an optimal method for identity management, instances such as Bitcoin underscore the need of anonymity. Some IoT devices, like wearables and smart automobiles, may need the protection of private information. Safeguarding these devices necessitates the use of encryption technologies, which must take into account the devices' restricted resources and financial limitations.
Traceability: The traceability of blockchain is defined by its capacity to preserve a comprehensive and immutable record of data from its inception. Each transaction is documented publicly and chronologically in successive blocks, enabling stakeholders to follow the events that resulted in the development of the data. This guarantees comprehensive visibility of the data's lifespan, enhancing confidence by ensuring the transparency, validity, and verifiability of any information documented on the blockchain.
The dependability of blockchain is derived from its resilient architecture, based on decentralization and consensus techniques like Proof-of-Work (PoW) or Proof-of-Stake (PoS). Decentralization reduces the danger of singular points of failure, since each node retains a copy of the ledger, so assuring resilience. Consensus techniques provide uniformity on the ledger's condition, enhancing trust in the data's precision.
This design, along with the immutability afforded by encryption, provides a dependable basis for diverse applications by protecting the blockchain's integrity from manipulation or failure.

3) Consensus Mechanisms

The consensus algorithm is fundamental to blockchain technology, guaranteeing the integrity and security of the network. It is a technique by which the nodes of the blockchain network achieve

consensus on the current state of ledger entries. Diverse blockchain systems use various algorithms to achieve consensus, with each algorithm functioning and executing distinctly.

The principles of these algorithms may be articulated as follows.:

Proof of Work (PoW): Proof of Work (PoW) is a fundamental consensus method in blockchain technology. It ascertains which miner will possess the authority to generate the subsequent block in the chain. This procedure necessitates miners to resolve a sophisticated cryptographic conundrum, which acts as a security assurance. The first node to resolve this mathematical problem is granted the privilege to create the subsequent block. Proof of Work requires substantial processing power, making the process very competitive and enhancing the network's security and resilience.

Proof of Work (PoW) sprang to popularity via Bitcoin, where it guarantees the blockchain's security and integrity by motivating miners to allocate substantial resources towards block production. Nonetheless, despite its shown efficacy, Proof of Work (PoW) encounters criticism due to its significant energy usage, which raises environmental issues.

## INTEGRATING BLOCKCHAIN TECHNOLOGY IN IOT

The decentralized nature of blockchain makes it an effective solution for the challenges of security and privacy in IoT systems. This objective has not yet been achieved in the conventional IoT's regulated yet scalable architecture [1] [2]. Devices may securely transmit data to blockchain ledgers for inclusion in distributed transactions when blockchain technology is incorporated into IoT upon transaction approval; each peer executes the same smart contract and has a copy of the ledger with immutable entries. Each data change is documented as a tamper-proof block. Consequently, the data cannot be accessed by unauthorized individuals. Owing to their diverse and extensive applications, IoT devices need safe and collaborative data exchange among the device, cloud, user, and other devices.

Incorporating blockchain technology into an Internet of Things (IoT) environment is a hard endeavor, although it is attainable with meticulous design and execution. Consider many methods by which blockchain technology might enhance the functionality of your IoT devices. Examples include verifying the authenticity of devices, ensuring the accuracy of sent information, monitoring the whereabouts of items across a supply chain, and distributing control among several individuals rather than a single entity. Comprehending the many applications of blockchain will enable you to determine its utilization with your equipment.

Select the most suitable computer system for your requirements. Consider factors such as its capacity, decision-making processes, safety, compatibility with other systems, and the availability of personnel to enhance its performance [16]. Notable computer systems for establishing connections include Ethereum, Hyperledger Fabric, IOTA, and Corda. Figure [3] illustrates the many advantages of using blockchain technology inside the Internet of Things (IoT).

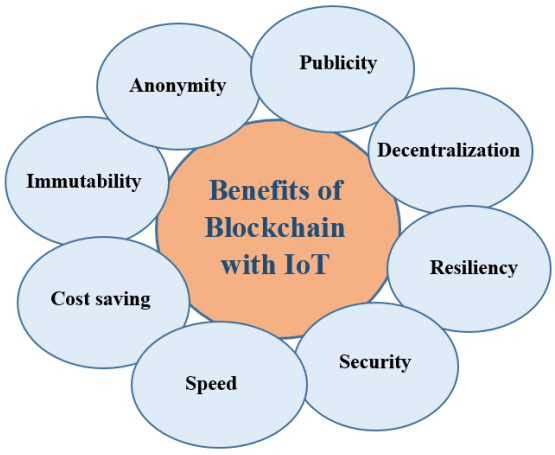


**Fig 2. Benefits of Blockchain with IoT**

Device Integration: Ensure compatibility of smart devices with the blockchain network. Certain devices may need additional software or components to interface with the blockchain.

Depending on the device, it may need a specialized wallet, advanced mathematical proficiency, or the capability to interact with the blockchain system. Establish a secure method for IoT devices to communicate with the blockchain network. This indicates that we will use specialized codes to maintain the confidentiality of the information sent and received. We shall use distinct "signatures" to ensure the material remains unaltered by unauthorized parties.

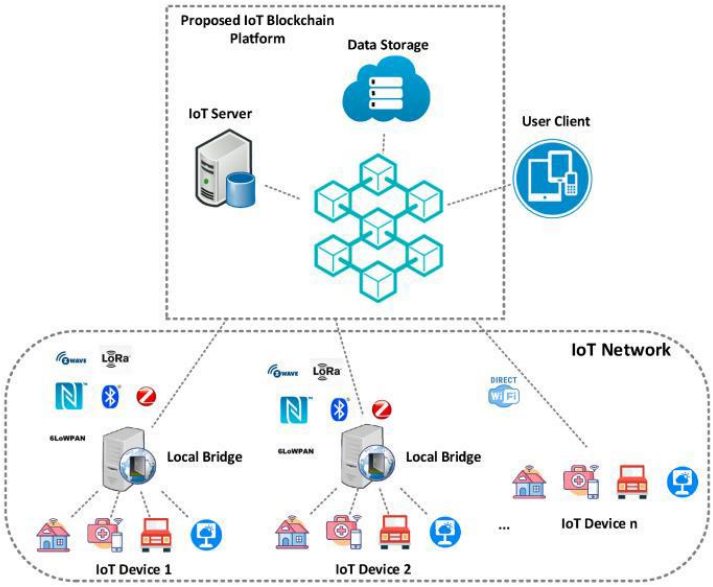


**Fig 3. Blockchain integration**

We may use specialized protocols such as TLS or secure MQTT to ensure the safety of this connection. Data collection and orchestration are crucial in this context. Envision a system that aggregates data from many devices, such as intelligent appliances, smart lighting, and automated thermostats. This method ensures that the information is prepared for use utilizing a specialized technology known as blockchain. To do this, it aggregates data from the devices, organizes it, and modifies it somewhat to ensure compatibility with blockchain technology. Certain gadgets, referred to as gateway devices or edge computing devices, facilitate this process.

**Application Area**

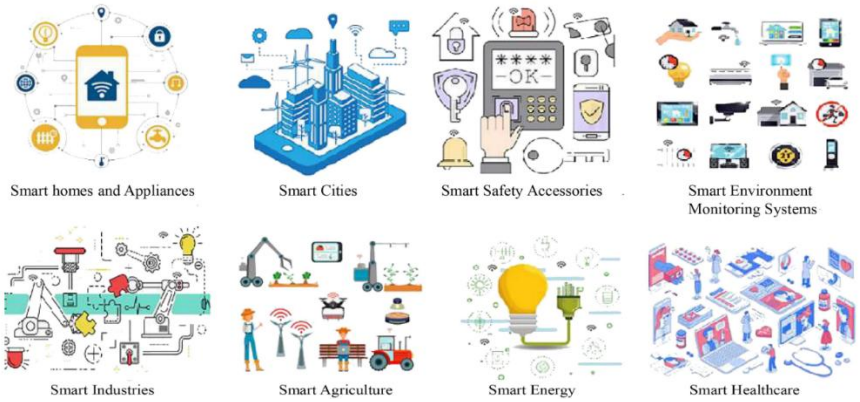


**Fig 5: applications areas of blockchain technology**

The incorporation of blockchain technology into IoT applications signifies a pivotal advancement in the industry (see Figure 4). The proliferation of IoT applications is increasingly using the distinctive advantages of blockchain technology. The Internet of Things (IoT) has become a pivotal element in the pursuit of a more intelligent and linked society, impacting both ordinary consumers and large

businesses. As we gaze into the future, it is evident that the integration of blockchain inside the IoT ecosystem represents a significant advancement rather than a mere fad. The integration of these two technologies is very promising, using blockchain's core principles of decentralization, security, and transparency to strengthen the foundations of the IoT. Smart home systems, smart grids, smart healthcare solutions, and several creative smart accessories are adopting this paradigm change. Figure 4 illustrates many application domains of blockchain technology inside IoT environments: This section examines how blockchain integration is transforming IoT applications across several domains, enhancing security, trust, and efficiency in IoT ecosystems.

Intelligent Urban Areas [61], [64], [67]: The incorporation of blockchain technology into smart cities is transforming urban development via the deployment of intelligent infrastructure, including smart lighting, water management, and parking systems.

This connection enhances data security and transparency, safeguarding information integrity and preventing illegal access, while also facilitating transparent urban administration via secure digital identity verification and transactions. Blockchain technology in smart cities fosters sustainable urban growth, improves citizen services, and bolsters urban resilience, therefore defining the future of networked urban environments.

Intelligent Home and Devices In the domain of consumer IoT devices, blockchain improves the security and functionality of smart homes and appliances. Blockchain guarantees data privacy and integrity, safeguarding against unwanted access and manipulation, in conjunction with utilities such as smart voice assistants (Siri, Alexa, and Google Assistant) and a variety of gadgets (smart fans, TVs, lighting systems, refrigerators, and wearables). It facilitates safe and transparent transactions, promoting confidence and enhancing user experiences. This integration represents a substantial advancement towards safer, more interconnected, and efficient smart homes, enabling users to oversee their everyday activities with enhanced control and security.

Smart Healthcare: In smart healthcare systems, blockchain is essential for improving data security and automating procedures such as insurance claims and invoicing using smart contracts. This invention empowers individuals by providing them control over their health data and facilitating more active involvement in healthcare choices. Blockchain enhances healthcare accessible in distant regions devoid of physical infrastructure.

The amalgamation of IoT and blockchain reconciles healthcare inequities, fosters patient-centric treatment, and provides secure, efficient healthcare services.

Smart Industries [65], [67]: The use of blockchain technology in smart industries significantly enhances industrial operations. The Internet of Things has already progressed several areas via breakthroughs such as intelligent sensors, sophisticated control systems, and autonomous robotics. Blockchain provides an essential layer of security and transparency, safeguarding data integrity and preventing illegal access. This integration facilitates transparent supply chain management, improving dependability, efficiency, and cooperation among industries, so propelling them toward more intelligent and productive futures.

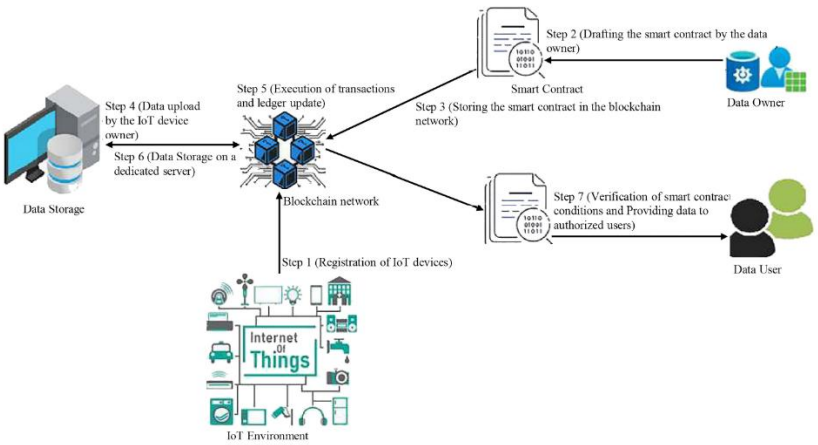


**Fig 6: Integration of blockchain and IoT based system**

## CONCLUSION

Blockchain technology is set to transform the next generation of the Internet of Things (IoT). This paper offers a comprehensive examination of the integration of blockchain technology with the IoT paradigm in several contexts, while also evaluating current initiatives in this field. It meticulously analyzes the intricacies of both IoT and blockchain technologies, including security features, privacy issues, consensus methods, and their comparative evaluations. The paper examines the incorporation of blockchain into the IoT framework, highlighting the relevant methodologies, advantages, and constraints. The results demonstrate that blockchain technology has considerable potential to improve the security and privacy of data in IoT systems, therefore promoting the expansion of IoT applications. Nevertheless, it is crucial to recognize that the application and execution of blockchain for IoT remain nascent, requiring further study to address the constraints and complexity inherent in this integration. This study delineates critical unanswered inquiries and prospective research trajectories that may help scholars focused on the intersection of blockchain and IoT.

## References


[1] Union Report Telecommunication, *Measuring the Information Society Report*, **[**online]. https://www.itu.int/pub/D-IND-ICTOI-2015 (2015).

[2] Alnefaie, S., Alshehri, S., and Cherif, A., *A survey on access control in IoT: models, architectures and research opportunities*, International Journal of Security and Networks, **16**(1)(2021), 60-76.

[3] Shen, Y., *Distributed storage system model design in internet of things based on hash distribution*, International Journal of Security and Networks, **12**(3)(2017), 141-151.

[4] Thilakarathne, N. N., *Security and privacy issues in IOT environment*, International Journal of Engi- neering and Management Research, **10**(1)(2020),26–29.

[5] Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., and Yamin, M., *Blockchain-based secured access control in an IoT system*, Applied Sciences, **11**(4)(2021), p. 1772.

[6] Wang, H., and Zhang, J., *Blockchain based data integrity verification for largescale IoT data*, IEEE Access, **7** (2019), 164996-165006.

[7] Singh, S., Hosen, A. S., and Yoon, B., *Blockchain security attacks, challenges, and solutions for the future distributed IOT network*, IEEE Access, **9**(2021), 13938-13959.

[8] Kitchenham, B., and Charters, S., *Guidelines for performing systematic literature reviews in SE Kitchen- ham et al guidelines for performing systematic literature reviews in software engineering source*, Guide- lines for performing Systematic Literature Reviews **i**(2007), 1-44.

[9] Petersen, K., Feldt, R., Mujtaba, S., and Mattsson, M., *Systematic mapping studies in software engineer- ing*, In 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), **12**(2008), 1-10.18

[10] Zhang, Y., and Wen, J., *An IoT electric business model based on the protocol of bitcoin*, In 2015 18th international conference on intelligence in next generation networks, IEEE, (2015), 184-191.

[11] Roth, N., *An architectural assessment of bitcoin: using the systems modelling language*, Procedia Com- puter Science, **44**(2015), 527-536.

[12] Samaniego, M., Jamsrandorj, U., and Deters, R., *Blockchain as a service for IoT*, In 2016 IEEE in- ternational conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (Smart- Data), (2016), 433-436.

[13] Dorri, A., Kanhere, S. S., and Jurdak, R., *Blockchain in internet of things:challenges and solutions*, (2016), arXiv preprint arXiv:1608.05187.

[14] Christidis, K., and Devetsikiotis, M., *Blockchains and smart contracts for the internet of things*, IEEE Access, **4** (2016), 2292-2303.

[15] Kshetri, N., *Can blockchain strengthen the internet of things?*, IT professional, **19**(4) (2017), 68-72.

[16] Khan, M. A. , and Salah, K., *IoT security: Review, blockchain solutions, and open*

*challenges*, Future generation computer systems,**82** (2018), 395-411.

[17] Huh, S., Cho, S., and Kim, S., *Managing IoT devices using blockchain platform*, In 2017 19th interna- tional conference on advanced communication technology (ICACT), IEEE, (2017), 464-467.

[18] Zhang, Y., and Wen, J., *The IoT electric business model: Using blockchain technology for the internet of things*, Peer-to-Peer Networking and Applications,**10**(4)(2017), 983-994.

[19] Fernandez-Carames, T. M., and Fraga-Lamas, P., *A review on the use of blockchain for the internet of things*, IEEE Access, **6**(2018), 32979-33001.

[20] Panarello, A., Tapas, N., Merlino, G., Longo, F., and Puliafito, A., *Blockchain and iot integration: A systematic survey*, Sensors, **18**(8)(2018), 2575. 19

[21] Banerjee, M., Lee, J., and Choo, K. K. R., *A blockchain future for internet of things security: a position paper*, Digital Communications and Networks, **4**(3)(2018), 149-160.

[22] Novo, O., *Blockchain meets IoT: An architecture for scalable access management in IoT*, IEEE Internet of Things Journal, **5**(2) (2018), 1184-1195.

[23] Kumar, N. M., and Mallick, P. K., *Blockchain technology for security issues and challenges in IoT*, Elsevier, Procedia Computer Science, **132** (2018), 1815-1823.

[24] Atlam, H. F., Alenezi, A., Alassafi, M. O., and Wills, G., *Blockchain with internet of things: benefits, challenges, and future directions*, International Journal of Intelligent Systems and Applications, **10** (6) (2018), 40-48.

[25] Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., and Pustisek, M., *Towards decentralized IoT security enhancement: A blockchain approach*, Computers & Electrical Engineering, **72**(2018), 266-273.

[26] Dittmann, G., and Jelitto, J., *A blockchain proxy for lightweight iot devices*, In 2019 Crypto Valley Conference on Blockchain Technology (CVCBT), IEEE, (2019), 82-85.

[27] Ding, S., Cao, J., Li, C., Fan, K., and Li, H., *A novel attribute-based access control scheme using blockchain for IoT*, IEEE Access, **7** (2019), 38431-38441.

[28] Watanabe, H., and Fan, H., *A novel chip-level blockchain security solution for the internet of things networks*, Technologies,**7** (1) (2019), 28.

[29] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B., *A survey on IoT security: application areas, security threats, and solution architectures*, IEEE Access, **7** (2019), 82721-82743.

[30] Casino, F., Dasaklis, T. K., and Patsakis, C., *A systematic literature review of blockchain-based appli- cations: current status, classification and open issues*, Telematics and informatics, **36** (2019), 55-81.