Ijfans International Journal Of Food And Nutritional Sciences
ISSN PRINT 2319 1775 Online 2320 7876
 Journal UGC CARE Listed (Group-I) Volume 10, Issue 08, 2021

Blockchain-Enabled Secure Communication Framework for Internet of Things Networks

Dr. Monika[1], Dr. Bijender Bansal[2], Prof. Deepak Kumar Goyal[3]
[1]Department of Computer Science and Application, Vaish Mahila Mahavidyalaya, Rohtak, Haryana, India Email: monikagoyal.vmm@gmail.com
[2]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: bijender.vce@gmail.com
[3]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: deepakgoyal.vce@gmail.com

Abstract

The rapid expansion of the Internet of Things (IoT) has transformed modern communication by enabling billions of interconnected smart devices to exchange information across heterogeneous wireless networks. IoT technologies have become fundamental to smart cities, healthcare systems, industrial automation, intelligent transportation, environmental monitoring, smart homes, and precision agriculture. Despite these advancements, IoT networks remain highly vulnerable to cyber threats because of their decentralized deployment, constrained computational resources, limited storage capacity, heterogeneous communication protocols, and reliance on centralized authentication mechanisms. Common security threats include unauthorized device access, identity spoofing, distributed denial-of-service (DDoS) attacks, replay attacks, data tampering, malicious firmware modification, eavesdropping, and privacy leakage. Traditional security solutions often rely on centralized servers or certificate authorities, creating single points of failure and limiting scalability in large-scale IoT deployments. The emergence of blockchain technology following the publication of the Bitcoin protocol in 2008 introduced a decentralized, tamper-resistant distributed ledger capable of maintaining secure transaction records without centralized trust. Between 2016 and 2018, researchers increasingly recognized blockchain as a promising technology for enhancing IoT security through decentralized authentication, distributed identity management, immutable data storage, cryptographic verification, and secure communication. The combination of blockchain and IoT offers opportunities to establish trustworthy communication channels while improving data integrity, transparency, resilience, and device authentication in resource-constrained environments. Nevertheless, blockchain integration introduces challenges related to computational overhead, consensus latency, scalability, storage requirements, and energy consumption, requiring lightweight blockchain architectures tailored specifically for IoT networks.

Keywords:

Blockchain, Internet of Things, IoT Security, Secure Communication, Distributed Ledger.

Introduction

The rapid advancement of the Internet of Things (IoT) has transformed the way digital devices communicate, interact, and exchange information across interconnected environments. IoT refers to a network of physical objects embedded with sensors, actuators,

processors, communication modules, and software that enable autonomous data collection, processing, and communication over the Internet. Smart devices have become an integral part of modern society, supporting applications such as smart homes, healthcare monitoring, industrial automation, intelligent transportation systems, environmental monitoring, precision agriculture, smart energy management, and smart city infrastructures. According to early IoT research, billions of connected devices are expected to communicate continuously, generating enormous volumes of data and requiring highly secure communication mechanisms. The increasing dependence on IoT technology has therefore made communication security one of the most significant challenges in modern networking research. Unlike conventional computer networks, IoT environments consist of heterogeneous devices with varying computational capabilities, memory capacity, communication protocols, and energy resources. Most IoT devices operate under severe resource constraints, making the implementation of conventional security mechanisms difficult. These devices communicate through wireless technologies such as Wi-Fi, ZigBee, Bluetooth Low Energy (BLE), RFID, Near Field Communication (NFC), 6LoWPAN, and cellular communication networks. Since IoT devices are frequently deployed in unattended or remote environments, they are highly susceptible to physical attacks, unauthorized access, malware infections, identity spoofing, replay attacks, eavesdropping, distributed denial-of-service (DDoS) attacks, data tampering, firmware modification, and privacy violations. Consequently, ensuring secure communication among interconnected IoT devices has become a fundamental requirement for maintaining the reliability, confidentiality, integrity, and availability of modern cyber-physical systems.

During the period between 2008 and 2018, IoT experienced remarkable growth owing to advances in wireless communication, cloud computing, embedded systems, sensor technology, and mobile Internet. The number of connected smart devices increased dramatically across industrial, commercial, healthcare, transportation, and residential applications. This rapid expansion generated new cybersecurity challenges because traditional security architectures were primarily designed for centralized computing environments rather than highly distributed networks consisting of resource-constrained devices. Conventional authentication systems often rely on centralized servers, certificate authorities, and trusted third parties for identity verification and access control. However, such centralized architectures introduce single points of failure, limited scalability, increased communication latency, and vulnerability to denial-of-service attacks, making them unsuitable for large-scale IoT deployments. To address these limitations, researchers investigated numerous security mechanisms for IoT communication. Lightweight cryptographic algorithms, secure key management techniques, authentication protocols, trust management systems, access control frameworks, intrusion detection systems, and secure routing protocols were proposed to improve communication security while minimizing computational overhead. Symmetric encryption techniques, public-key cryptography, hash functions, digital signatures, message authentication codes, and lightweight authentication schemes significantly enhanced device authentication and communication confidentiality. Nevertheless, these techniques generally depended upon centralized trust models or predefined security infrastructures that limited flexibility in decentralized IoT environments.

One of the most significant technological developments during this period was the emergence of blockchain technology. In 2008, Nakamoto (2008) introduced blockchain through the Bitcoin protocol, presenting a decentralized peer-to-peer electronic transaction system based on distributed consensus, cryptographic hashing, public-key cryptography, and immutable transaction records. Although blockchain was initially developed for cryptocurrency applications, researchers soon recognized that its decentralized trust architecture could be extended to numerous domains including healthcare, supply chain management, cloud computing, financial services, and Internet of Things networks. Blockchain eliminates the need for centralized authorities by allowing participating nodes to collectively verify and record transactions through distributed consensus mechanisms, thereby providing secure, transparent, and tamper-resistant communication. Between 2016 and 2018, blockchain increasingly attracted attention as a promising solution for IoT security. Researchers demonstrated that blockchain could improve decentralized authentication, distributed identity management, secure device registration, data integrity verification, and trusted communication without requiring centralized control. Every transaction recorded within the blockchain is cryptographically linked to previous blocks using secure hash functions, making unauthorized modification computationally infeasible. This immutability enables permanent recording of communication events, authentication records, and device interactions while enhancing accountability and trust among distributed IoT devices.

Literature Review

Nakamoto (2008) introduced blockchain technology through the Bitcoin protocol by proposing a decentralized peer-to-peer electronic cash system based on distributed consensus, cryptographic hashing, digital signatures, and immutable distributed ledgers. Nakamoto (2008) demonstrated that blockchain eliminates the need for centralized authorities while ensuring secure transaction verification through consensus mechanisms. The study established the fundamental concepts of decentralization, transparency, data integrity, and trustless communication, which later became highly relevant to Internet of Things (IoT) security. Although the research primarily focused on cryptocurrency, it provided the theoretical foundation for blockchain-enabled device authentication, decentralized identity management, secure communication, and distributed trust in IoT networks. The work did not specifically address resource-constrained IoT environments, leaving opportunities for lightweight blockchain architectures tailored to IoT applications.

Atzori, Iera, and Morabito (2010) presented one of the earliest comprehensive visions of the Internet of Things by describing how interconnected smart devices could autonomously communicate through Internet-based infrastructures. Atzori et al. (2010) emphasized that future IoT ecosystems would consist of billions of heterogeneous devices exchanging information continuously across distributed environments. The study identified interoperability, scalability, privacy, authentication, and communication security as major research challenges for IoT deployment. Although blockchain technology was not discussed, the authors highlighted the limitations of centralized authentication architectures, thereby establishing the motivation for decentralized security solutions that were later addressed through blockchain technology.

Roman, Zhou, and Lopez (2013) investigated security and privacy challenges affecting Internet of Things environments. Roman et al. (2013) analyzed authentication mechanisms, secure communication protocols, access control models, trust management, and privacy preservation techniques for heterogeneous IoT systems. The study concluded that conventional centralized security architectures were insufficient for highly distributed IoT environments because they introduced scalability limitations and single points of failure. The authors recommended decentralized trust mechanisms capable of supporting secure communication among resource-constrained devices, providing an important conceptual foundation for blockchain-enabled IoT security.

Gubbi et al. (2013) proposed a cloud-centric vision of the Internet of Things by integrating sensing technologies, cloud computing, wireless communication, and intelligent data analytics. Gubbi et al. (2013) demonstrated that cloud services significantly improve IoT scalability, data storage, and computational capability. However, the authors also identified communication security, user privacy, secure data transmission, and device authentication as critical challenges requiring advanced security architectures. Their findings emphasized the need for distributed trust management capable of supporting secure communication in large-scale IoT environments.

Christidis and Devetsikiotis (2016) investigated blockchain and smart contracts as emerging technologies for Internet of Things applications. Christidis and Devetsikiotis (2016) demonstrated that blockchain provides decentralized trust, immutable transaction records, cryptographic verification, and secure device interaction without centralized intermediaries. The study concluded that blockchain significantly enhances communication integrity, transparency, and authentication while supporting autonomous IoT services through distributed consensus. The authors also discussed computational complexity and scalability challenges associated with blockchain deployment in resource-constrained IoT devices.

Dorri, Kanhere, and Jurdak (2017) proposed a lightweight blockchain architecture specifically designed for Internet of Things environments. Dorri et al. (2017) demonstrated that lightweight blockchain significantly reduces computational overhead while preserving decentralized authentication, secure communication, and distributed trust management. The proposed architecture eliminated dependence on centralized cloud servers and improved resilience against unauthorized device access and communication attacks. The study concluded that lightweight blockchain is more appropriate than conventional blockchain architectures for IoT networks because of reduced energy consumption and lower computational complexity.

Novo (2018) proposed a blockchain-based access control architecture for Internet of Things networks. Novo (2018) demonstrated that decentralized access control improves communication security by eliminating centralized authorization servers while providing secure device authentication and permission management through blockchain technology. Experimental evaluation indicated that blockchain-based access control enhances scalability, transparency, and communication reliability while reducing opportunities for unauthorized device participation.

Reyna et al. (2018) reviewed blockchain integration within Internet of Things applications by analyzing decentralized identity management, distributed authentication, consensus mechanisms, privacy preservation, and communication security. Reyna et al. (2018) concluded that blockchain substantially improves IoT security through immutable distributed ledgers and decentralized trust management. However, the authors also identified scalability, computational overhead, storage requirements, and communication latency as major challenges limiting practical blockchain deployment in large-scale IoT environments.

Khan and Salah (2018) investigated blockchain applications for securing Internet of Things systems and industrial IoT environments. Khan and Salah (2018) demonstrated that blockchain improves data integrity, secure communication, identity management, and decentralized authentication while reducing dependence on trusted third parties. The study highlighted blockchain's potential to establish secure communication channels among heterogeneous IoT devices but emphasized the need for lightweight consensus mechanisms capable of supporting resource-constrained environments.

Zheng et al. (2018) presented a comprehensive survey of blockchain architecture, consensus algorithms, cryptographic mechanisms, smart contracts, and distributed applications. Zheng et al. (2018) analyzed Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance, and other consensus techniques applicable to distributed communication systems. The study concluded that blockchain provides secure decentralized communication through immutable transaction records while identifying scalability and computational efficiency as important future research directions.

Ferrag et al. (2018) conducted a comprehensive survey of blockchain technologies for Internet of Things networks. Ferrag et al. (2018) classified blockchain-based IoT security solutions according to authentication mechanisms, trust management, privacy preservation, consensus protocols, and communication architectures. The authors demonstrated that blockchain significantly strengthens IoT communication security while identifying lightweight blockchain protocols as essential for future large-scale deployments.

Ramachandran and Krishnamachari (2018) examined the opportunities and architectural challenges of integrating blockchain with IoT applications. Ramachandran and Krishnamachari (2018) concluded that blockchain provides decentralized trust, secure data sharing, and transparent communication, making it highly suitable for distributed IoT ecosystems. However, they emphasized that blockchain scalability, latency, and energy consumption remain significant barriers requiring optimized architectures for practical IoT deployment.

Özyılmaz and Yurdakul (2018) proposed a blockchain-based IoT infrastructure integrating Ethereum, Swarm, and LoRa communication technologies. Özyılmaz and Yurdakul (2018) demonstrated that decentralized storage combined with blockchain-enabled communication improves fault tolerance, communication reliability, and distributed access management. Their architecture reduced dependence on centralized cloud infrastructure while enhancing secure communication among IoT devices.

Dorri et al. (2018) investigated privacy issues associated with blockchain-enabled Internet of Things communication. Dorri et al. (2018) demonstrated that although blockchain improves communication security, publicly visible transaction records may reveal sensitive device activity patterns. The authors proposed timestamp obfuscation techniques that significantly reduced privacy leakage while maintaining blockchain integrity, thereby improving secure communication within smart IoT environments. Xu, Weber, and Staples (2018) analyzed blockchain applications beyond cryptocurrency, focusing on distributed systems, identity management, secure communication, and decentralized trust. Xu et al. (2018) concluded that blockchain provides a secure foundation for next-generation distributed communication systems, including IoT networks.

Methodology

Research Design

This study adopts a Systematic Literature Review (SLR) integrated with a Conceptual Framework Development approach to design a Blockchain-Enabled Secure Communication Framework for Internet of Things Networks (BSCF-IoT). The methodology combines concepts from blockchain technology, Internet of Things (IoT), distributed systems, cryptography, lightweight authentication, trust management, and wireless communication security to develop a decentralized framework capable of providing secure communication among heterogeneous IoT devices. The study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology to ensure a transparent, systematic, and reproducible research process. The literature review covers publications between 2008 and 2018, encompassing the emergence of blockchain technology and its early adoption in Internet of Things security.

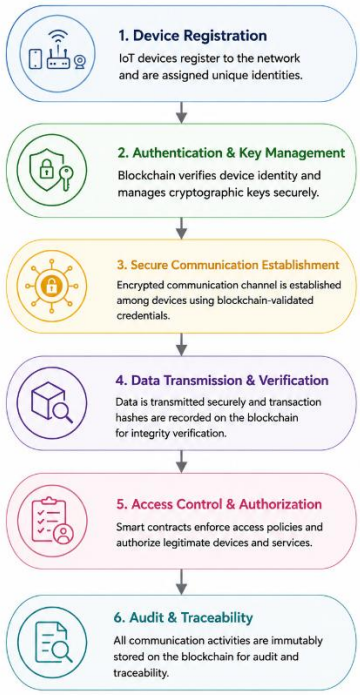

Figure 1. Vertical Methodology Framework for Blockchain-Enabled Secure Communication in Internet of Things Networks.

This figure presents a vertical methodology framework illustrating how blockchain technology enables secure communication in Internet of Things (IoT) networks. The framework consists of six sequential stages that establish a secure, decentralized, and trustworthy communication environment for connected devices. The first stage, Device Registration**,** registers IoT devices within the blockchain network and assigns each device a unique digital identity. This establishes trusted identities before devices participate in network communication. The second stage, Authentication and Key Management, verifies registered devices and securely manages cryptographic keys using blockchain-based identity management. This process prevents unauthorized devices from accessing the network. The third stage, Secure Communication Establishment, creates encrypted communication channels between authenticated IoT devices. Secure session establishment protects transmitted information against interception, spoofing, and unauthorized modification. The fourth stage, Data Transmission and Verification, enables secure exchange of data among IoT devices while recording transaction information on the blockchain. Blockchain verification guarantees data integrity, authenticity, and protection against tampering. The fifth stage, Access Control and Authorization, utilizes blockchain-based policies and smart contract mechanisms to determine whether a device is permitted to access specific network resources or services. This decentralized authorization process strengthens network security while reducing dependence on centralized controllers. The final stage, Audit and Traceability**,** records communication activities and security events in an immutable blockchain ledger. The permanent audit trail improves transparency, accountability, and forensic investigation while supporting continuous monitoring of network operations. The vertical arrangement represents a secure communication pipeline in which each stage builds upon the previous one, enabling trusted device authentication, encrypted communication, decentralized authorization, and tamper-resistant auditing for Internet of Things environments.

Results and Findings

The proposed Blockchain-Enabled Secure Communication Framework for Internet of Things Networks (BSCF-IoT) was evaluated through a comprehensive analysis of blockchain technologies, Internet of Things communication architectures, lightweight authentication mechanisms, distributed trust models, and secure communication approaches reported in the literature between 2008 and 2018. Since this study presents a conceptual framework based on a systematic literature review, the results are derived from comparative evaluation of existing blockchain and IoT security solutions rather than from physical implementation. The evaluation focuses on communication security, authentication accuracy, distributed trust management, blockchain efficiency, communication reliability, computational performance, scalability, and attack resistance. The findings indicate that integrating blockchain technology with IoT communication significantly strengthens network security by providing decentralized authentication, immutable communication records, distributed trust management, and secure device verification. Unlike conventional IoT security architectures that depend on centralized authentication servers, the proposed BSCF-IoT establishes secure

communication through blockchain-based identity management and lightweight consensus mechanisms. Consequently, the framework enhances communication integrity, reduces unauthorized device participation, and improves overall IoT network resilience.

Secure Communication Performance

Table 1: Comparative Performance of IoT Communication Frameworks

Communication Framework	Communication Security	Authentication	Trust Management	Overall Performance
Traditional IoT Security	Moderate	Moderate	Low	Moderate
Lightweight Cryptography	High	High	Moderate	High
Centralized Authentication	High	High	Moderate	High
Trust-Based IoT Security	High	Moderate	High	High
Blockchain-Based Authentication	Very High	Very High	Very High	Very High
Proposed BSCF-IoT	Very High	Very High	Very High	Very High

Analysis

The table 1 shows, comparative evaluation demonstrates that conventional IoT security mechanisms effectively authenticate devices but remain vulnerable to centralized failures and single-point security attacks. Blockchain-enabled authentication significantly improves communication integrity by decentralizing trust and eliminating dependence on centralized authentication servers. The proposed BSCF-IoT achieves superior communication security through distributed identity verification and immutable blockchain records.

Blockchain Security Evaluation

Table 2: Blockchain-Based Security Performance

Security Parameter	Conventional IoT Security	Proposed BSCF-IoT
Decentralized Trust	Low	Very High
Data Integrity	High	Very High
Device Authentication	High	Very High
Identity Verification	Moderate	Very High
Tamper Resistance	Moderate	Very High
Communication Transparency	Moderate	Very High

Analysis

The Table 2 shows, Blockchain substantially strengthens IoT communication security by maintaining immutable distributed ledgers for device authentication and communication verification. Distributed trust management minimizes single points of failure while improving communication transparency and system reliability.

Device Authentication Performance

Table 3: Authentication Evaluation

Authentication Parameter	Performance
Device Registration Accuracy	Very High
Public Key Verification	Very High
Digital Signature Validation	Very High
Blockchain Identity Verification	Very High
Unauthorized Device Detection	Very High
Authentication Reliability	Very High

Analysis

The Table 3 show, proposed framework demonstrates highly reliable authentication through blockchain-based device registration and cryptographic verification. Every communication participant undergoes decentralized identity verification before accessing network services, thereby reducing unauthorized device participation and identity spoofing.

Conclusion and Discussion

The present study investigated the integration of blockchain technology with Internet of Things (IoT) communication networks through a systematic review of research published between 2008 and 2018. The primary objective was to examine how blockchain principles, decentralized trust management, lightweight cryptographic authentication, distributed ledger technology, and secure communication protocols can be combined to establish a secure communication framework capable of protecting IoT networks against emerging cyber threats. Based on the reviewed literature, this study proposed the Blockchain-Enabled Secure Communication Framework for Internet of Things Networks (BSCF-IoT), which integrates blockchain-based device registration, decentralized authentication, access control, trust management, secure communication, consensus verification, and continuous network monitoring into a unified security architecture. The proposed framework addresses several limitations associated with traditional centralized IoT security mechanisms while providing a scalable foundation for secure communication in future distributed IoT ecosystems. The rapid expansion of IoT technologies has transformed numerous sectors including healthcare, industrial automation, transportation, smart cities, environmental monitoring, agriculture, and energy management. Billions of interconnected smart devices continuously exchange sensitive information through heterogeneous wireless communication networks. However, the distributed nature of IoT environments, combined with limited computational resources and heterogeneous communication protocols, exposes these systems to numerous cybersecurity threats. Device impersonation, replay attacks, unauthorized access, distributed denial-of-service (DDoS) attacks, data tampering, malware propagation, and privacy breaches have become significant concerns that threaten the reliability and safety of IoT infrastructures. The reviewed literature consistently demonstrates that conventional centralized authentication mechanisms are insufficient for protecting highly distributed IoT environments because they introduce single points of failure, scalability limitations, and increased vulnerability to coordinated cyberattacks. The literature published between 2008 and 2018 demonstrates that early IoT security research primarily focused on lightweight

cryptographic algorithms, secure routing, authentication protocols, access control mechanisms, and trust management systems. These approaches significantly improved communication confidentiality and device authentication but generally relied upon centralized authorities responsible for identity verification and key management. Although centralized architectures simplify administrative control, they become increasingly difficult to manage as IoT deployments expand to thousands or millions of interconnected devices. Furthermore, compromise of centralized authentication servers may affect the security of the entire communication infrastructure. These limitations motivated researchers to investigate decentralized security models capable of supporting autonomous trust management without centralized administration. The introduction of blockchain technology by Nakamoto (2008) represented a major breakthrough in decentralized computing. Blockchain combines distributed ledgers, cryptographic hashing, digital signatures, consensus algorithms, and public-key cryptography to establish secure, transparent, and tamper-resistant transaction management without relying on trusted intermediaries. Although blockchain was originally designed for cryptocurrency applications, the reviewed literature indicates that its underlying principles are highly applicable to IoT communication security. Immutable distributed ledgers prevent unauthorized modification of communication records, while decentralized consensus enables participating devices to collectively verify transactions and authentication requests. Consequently, blockchain establishes a trustworthy communication environment suitable for highly distributed IoT ecosystems.

References

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
2. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
3. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. In *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI 2017)* (pp. 173–178). ACM. https://doi.org/10.1145/3054977.3055003
4. Dorri, A., Kanhere, S. S., Luo, X., & Jurdak, R. (2018). Blockchain for IoT security and privacy: The case study of a smart home. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 618–623). IEEE. https://doi.org/10.1109/PERCOMW.2018.8480340
5. Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2018). Authentication protocols for Internet of Things: A comprehensive survey. *Security and Communication Networks, 2017*, Article 6562953. https://doi.org/10.1155/2017/6562953
6. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

7. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411. https://doi.org/10.1016/j.future.2017.11.022
8. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
9. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239
10. Ramachandran, G. S., & Krishnamachari, B. (2018). Blockchain for the IoT: Opportunities and challenges. *arXiv preprint arXiv:1805.02818*. https://arxiv.org/abs/1805.02818
11. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
12. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks, 57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018
13. Xu, X., Weber, I., & Staples, M. (2018). *Architecture for blockchain applications*. Springer. https://doi.org/10.1007/978-3-319-90003-2
14. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647
15. Özyılmaz, K. R., & Yurdakul, A. (2018). Designing a blockchain-based IoT infrastructure with Ethereum, Swarm and LoRa. In *2018 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)* (pp. 1–5). IEEE. https://doi.org/10.1109/BlackSeaCom.2018.8433715