MEST Journal
DOI 10.12709/mest.13.13.02.05

PROTECTING BLOCKCHAIN FROM IOT DEVICE ATTACKS: CHALLENGES AND SOLUTIONS

Zoran Cekerevac
Independent Researcher, Belgrade, Serbia
http://orcid.org/0000-0003-2972-2472

Serghei Ohrimenco
Academy of Economic Studies of Moldova, Chisinau, Moldova
https://orcid.org/0000-0002-6734-4321

Petar Cekerevac
Independent Researcher, Belgrade, Serbia
https://orcid.org/0000-0001-6100-5938

JEL Category: **C88, D85, K24, L86, O33**

Abstract

This paper focuses on the challenges and solutions in protecting blockchain technology from attacks through IoT devices, emphasizing the importance of integrating these technologies into modern systems. The study is based on the null hypothesis that there is no significant correlation between security challenges posed by IoT devices and the compromise of integrity, availability, or immutability of blockchain technology. While IoT devices enhance operational efficiency, they simultaneously represent vulnerabilities for potential cyberattacks that may jeopardize the security of blockchain systems. Identified security challenges, including DDoS attacks, data manipulation, ransomware, and protocol compromise, are analyzed through real-world cases and technological solutions. The analysis reveals that Zero Trust architecture, smart contracts, cryptographic algorithms, and artificial intelligence significantly enhance the security and resilience of integrated systems. User education, standardization of IoT security protocols, energy-efficient solutions, and collaboration between industries and regulatory bodies are key to mitigating risks. Based on the analysis, a significant correlation between IoT-related security challenges and blockchain compromise was established, rejecting the null hypothesis. The paper offers recommendations for improving the security of these technologies, highlighting the need for continuous monitoring and innovation in IoT and blockchain environments. It is intended to be useful for cybersecurity professionals, researchers working on IoT and blockchain integration, and companies implementing IoT devices in industrial and commercial contexts.

Address of the corresponding author:
Zoran Cekerevac
zoran@cekerevac.eu

Keywords: *Blockchain, IoT Security, DDoS, Smart Contracts, Zero Trust.*

1 INTRODUCTION

1.1 Blockchain and the Internet of Things (IoT)

Thanks to Bitcoin, distributed ledger technology (DLT) has become widely recognized. Nowadays, this innovative system and the Internet of Things (IoT) are among the most researched technologies. Many are attempting to apply this ledger system in various fields. We believe it is meaningful in areas requiring permanent record-keeping and/or monetization. In specific cases, it can serve as the optimal solution, but frequently, its implementation may not justify the costs or complexity.

Blockchain is highly effective in situations requiring immutability, transparency, and data verification and when tokenization and monetization are necessary:

- Due to its structure based on immutable blocks, it ensures that entered data remains permanent and unchangeable. This feature is crucial for transaction records, contracts, documentation, and supply chain tracking. (Valencia-Payan, Griol, & Corrales, 2024)
- It is frequently associated with economic models involving tokenization. For instance, systems like cryptocurrencies or decentralized finance (DeFi) enable direct exchange and monetization without centralized intermediaries. (Zetzsche, Arner, & Buckley, 2020)
- Much has been written about blockchain technology; here, we will only mention the basic principles necessary for understanding this work. Blockchain functions as a distributed ledger facilitating the tracking of transactions and assets. For easier comprehension, blockchain can be considered an operating system, while Bitcoin is one of the applications running on it (Cekerevac, Prigoda, & Maletic, Blockchain Technology and Industrial Internet of Things in the Supply Chains, 2018).

A distributed ledger represents a database accessible at multiple locations, with data entered through participant consensus (Belin, 2018). Blockchain links records via encrypted blocks relying on previous entries, ensuring immutability and security. Depending on the application, blockchain may be:

- Private, e.g., Hyperledger Fabric, suitable for corporate systems (2023),
- Consortium, e.g., R3 Corda, enabling collaboration among a limited number of participants (R3, 2025), or
- Public, e.g., Ethereum, provides open access and benefits like smart contracts (Ethereum, 2025).

Among these, public blockchains are the most demanding and complex to maintain.

Interoperability and scalability challenges have inspired the idea of “blockchain within blockchain.” This approach represents a step toward the development of 'Internet 2.0.' Internet 2.0 integrates decentralized technologies such as blockchain, cryptocurrencies, and smart contracts to enhance security and transparency. Projects like Polkadot and Cosmos facilitate network communication and scalability, addressing critical interoperability issues (Palkadot, 2024; Cosmos Network, n.d.).

The Internet of Things (IoT) refers to a system of connected devices, machines, objects, and even people and animals with unique identifiers that transmit data over a network without direct user interaction (Wigmore, 2016). Within IoT, the Industrial Internet of Things (IIoT) subcategory has emerged for industrial applications. IIoT devices communicate with each other, improving processes (M2M - Machine-to-Machine). IIoT technologies require higher reliability, precision, security, and interoperability to ensure the efficient operation of facilities. A comparison between a smartphone and a high-end digital camera illustrates the difference between IoT and IIoT—IIoT is better suited for demanding conditions. IIoT technology is heterogeneous, involving various platforms and equipment, and its implementation follows phases such as device connection, data monitoring and analysis, activity automation, and Edge Computing. Each phase includes specific steps, from data collection to automated analytics and device-level management. Examples of IoT devices include smart thermostats that optimize energy consumption and agricultural sensors that enhance irrigation efficiency.

1.2 Security in the Context of Blockchain and IoT Integration

With the rapid development of IIoT and IoT, a growth in cyberattacks on networked devices is expected, highlighting the need for enhanced protection. Integrating blockchain technology and IoT devices can play a key role in improving security, transparency, and operational efficiency in interconnected systems:

- *Data Security:* Blockchain secures data using advanced cryptographic methods, preventing manipulation and reducing the risk of cyberattacks (Bobde, et al., 2024). IoT devices frequently send and receive sensitive information, and blockchain enhances the system's resilience against security threats.
- *Transparency:* Blockchain provides a clear record of interactions and transactions between IoT devices, enabling tracking and problem resolution in industrial and logistical applications (Douaioui & Benmoussa, 2024).
- *Interoperability:* IoT systems are often heterogeneous, comprising devices from different manufacturers. Blockchain facilitates communication and information exchange among these devices, establishing consistent standards.
- *Automation:* Smart contracts within blockchain automate processes based on IoT data, reducing human intervention and increasing efficiency (Zafar, Bhatti, Shabbir, Hashmat, & Akbar, 2021)
- *Monitoring and Management:* Blockchain enables continuous tracking of IoT devices and the data from origin to end-use. For example, in supply chains, blockchain helps identify the origin of products and track their journey (Douaioui & Benmoussa, 2024)

This integration is significant as it unlocks the potential of IoT technology to enhance security and efficiency in industrial processes and daily applications.

1.3 About the Paper

1.3.1 Aim of the Paper

This paper aims to identify the key security challenges that blockchain technology may face due to attacks via IoT devices, alongside analyzing potential solutions and strategies to mitigate these risks. The focus is on understanding how IoT devices can compromise blockchain systems' integrity, availability, and immutability while proposing specific technical, procedural, and organizational approaches to enhance security.

1.3.2 Research Question and Hypotheses

In their study, the authors defined the research question and corresponding hypotheses. This approach provided a structured framework for academic analysis, focusing on identifying security threats, analyzing case studies, and proposing future recommendations.

Research Question: What are the primary security challenges that arise from IoT-driven attacks on blockchain systems, and which solutions are most effective in addressing them?

Null Hypothesis (H_0): There is no significant correlation between security challenges posed by IoT devices and the compromise of key aspects of blockchain technology, regardless of the implementation of advanced cryptographic algorithms, access control mechanisms, or Zero Trust architecture.

Alternative Hypothesis (H_a): There is a significant correlation between security challenges posed by IoT devices and the compromise of key aspects of blockchain technology, whereby advanced cryptographic algorithms, access control mechanisms, and Zero Trust architecture can reduce these risks.

1.3.3 Methodology

This review paper is based on an analysis of available literature and the structural synthesis of data, aiming to identify challenges and solutions for protecting blockchain technology from attacks via IoT devices. The methodological approach encompasses:

1. *Research Framework*. The framework stems from the research question and key areas, including IoT device challenges, blockchain vulnerabilities, and protection strategies.
2. *Literature Review*. The research involved a review of scientific databases, including Google Scholar, Kobson, IEEE Xplore, and

Scopus. Keywords for source identification included terms such as *IoT security blockchain*, *IoT attacks blockchain vulnerabilities*, and *Blockchain cybersecurity IoT*. The focus was on papers published in the last five years, with a few relevant exceptions.

3. *Categorization of Challenges and Solutions*. Security challenges, such as DDoS attacks, MITM attacks, and data manipulation, were identified, while mitigation strategies encompassed advanced cryptographic mechanisms, Zero Trust architecture, and IoT security protocols.
4. *Analysis and Data Synthesis.* All collected data were systematized into thematic areas:
   - Overview of Security Threats identifies the main types of attacks via IoT devices and their impact on blockchain technology.
   - Technological Solutions for Protection include research on existing security mechanisms and their effectiveness.
   - Methods to Protect Blockchain from IoT Attacks and
   - Recommendations for the Future provide suggestions for improving blockchain security within IoT contexts.

   The discussion links challenges to corresponding solutions with case study examples from literature.
5. *Quality Assurance*. This included analyzing consistency, source relevance, and linguistic clarity using relevant tools.

2 SECURITY THREATS

Blockchain technology in IoT systems opens numerous opportunities across various sectors. It also introduces significant risks (Shah, Ullah, Li, Levula, & Khurshid, 2022). While blockchain is inherently well-protected, integrating with IoT devices demands additional security measures to preserve the system's overall safety. This integration can compromise system security in several ways. For instance, compromised IoT devices may introduce malicious data into the blockchain. Attacks such as Man-in-the-Middle (MITM) may disrupt communication between devices and the network (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017). Furthermore, IoT botnet attacks like DDoS can overwhelm blockchain networks and reduce their functionality (Ibrahim, Al-Haija, & Ahmad, 2022).

2.1 IoT Vulnerabilities

IoT devices represent critical points in systems for several reasons. First, the physical accessibility of IoT devices, often located in remote or unprotected areas, may allow sabotage or unauthorized access. Additionally, weak user authentication systems can make it easier for attackers to gain control over devices. Insecure communication channels further increase the risk of data interception, while limited IoT device resources hinder the implementation of encryption, authentication, and constant monitoring, making them vulnerable to attacks.

2.2 Attacks on Blockchain via IoT Devices

Attacks using IoT devices to compromise blockchain technology are diverse and include:

- Trojanization of devices (SC, 2023) through malicious software that sends manipulated data,
- Ransomware attacks that block operations until a ransom is paid, and
- Firmware attacks result in unauthorized control over data.

Additionally, Sybil's attacks enable the creation of numerous fake identities to manipulate consensus processes within blockchain networks. IoT devices are often used as bots in DDoS attacks, which can overwhelm the network and compromise functionality. Compromised IoT devices may manipulate data required for transaction validation or attack network protocols, jeopardizing communication between devices and the blockchain network. (Humayun, Jhanjhi, Alsayat, & Ponnusamy, 2021; Balogh, Gallo, Ploszek, Špaček, & Zajac, 2021)

2.3 General Security Threats

Beyond specific risks, blockchain can be exposed to general threats, including the lack of universal security standards for IoT devices and their integration with blockchain technology. Additional challenges include the limited capacities of IoT devices for energy-intensive security functions such as encryption and data verification, which can reduce the entire system's efficiency (Zaheer, et al., 2024).

3 TECHNOLOGICAL SOLUTIONS FOR PROTECTION

Technological solutions for protecting blockchain from attacks via IoT devices involve a combination of security mechanisms, protocols, and strategies tailored to both systems. One key approach is network segmentation (Sengupta, 2020), which separates IoT devices from the core network using VLANs or dedicated Wi-Fi networks. When IoT devices exhibit suspicious behavior, blockchain networks can quickly isolate compromised devices, preventing the spread of threats.

Communication security is another critical aspect, achieved through robust authentication methods and end-to-end encryption for communication between IoT devices and blockchain networks. Digital signatures provide additional protection by authenticating and verifying data, preventing information manipulation. Furthermore, Zero Trust architecture ensures that network access is granted only after verifying the identity and context of each device and user. TLS/SSL protocols further secure encrypted communication, reducing the risk of data interception. (Liu, et al., 2024)

Data validation automation via smart contracts enables automatic validation of information sent by IoT devices to blockchain networks, speeding up processes and reducing human error. Artificial intelligence (AI) use plays a pivotal role in anomaly detection by analyzing IoT device behavior to identify suspicious activities (Demertzis, Iliadis, Tziritas, & Kikiras, 2020). Additionally, AI can be employed for potential threats predictive analysis based on historical data and behavioral patterns.

Alongside these technical approaches, collaboration between IoT device manufacturers and blockchain networks remains essential. Standardizing security practices contributes to establishing universal standards for integrating IoT devices with blockchain technology, while information sharing on threats enhances protection through collective efforts.

4 METHODS TO PROTECT BLOCKCHAIN FROM IOT ATTACKS

Blockchain technology with its inherent characteristics such as decentralization, cryptographic protection, and data immutability, already possesses a high level of resilience against attacks. Key elements, such as consensus mechanisms (e.g., Proof-of-Work or Proof-of-Stake), encrypted transactions, and distributed ledgers, further contribute to the security and stability of blockchain networks (Becher & Urwin, 2025). However, as the number of IoT devices continues to grow, the complexity of systems demands a comprehensive approach to protection.

Protecting blockchain from threats originating through IoT devices involves preventive actions that prevent data manipulation, strengthen communication protocols, enable advanced analytics, and isolate compromised devices. Data authentication mechanisms, such as algorithms for stricter validation of IoT device information, are crucial for maintaining transaction integrity and preventing the entry of compromised information into the system. Security layers, such as encrypted channels based on TLS (Transport Layer Security) protocols, ensure secure communication between IoT devices and blockchain networks, reducing the risk of data interception or manipulation during transmission. (SSL, 2021)

Artificial intelligence (AI) plays a significant role in enhancing anomaly detection in transactions involving IoT devices. Analytical tools enable the identification of compromised devices, allowing preventive measures to be taken before the network is endangered. Additionally, blockchain networks can isolate suspicious devices, preventing the spread of potential threats and ensuring the security of the core system.

Beyond technical solutions, IoT device manufacturers play a crucial role in implementing security measures. Certification of devices by recognized certification organizations ensures product quality and safety. Regular firmware and software updates, the implementation of robust authentication and encryption methods, and internal security audits further increase device resilience against threats. On the other hand, blockchain networks can conduct detailed device authentication checks during connection, implement continuous certificate and security setting verification, utilize smart contracts for automated data validation, and isolate compromised devices. (Tsaur, Chang, & Chen, 2022)

For the successful integration of IoT devices with blockchain technology collaboration between manufacturers and blockchain networks is required. Joint efforts in defining and implementing security standards, and sharing information about threats and security incidents, enhance protection and achieve long-term security in connectivity. This collaboration ensures that all devices on the network meet the required security standards before being granted access.

The following papers analyzed in detail the topic of IoT security: (Cekerevac, Dvorak, Prigoda, & Cekerevac, 2017; Maletic & Cekerevac, 2019; Cekerevac, Prigoda, & Čekerevac, 2025; Čekerevac, Prigoda, & Čekerevac, 2025A)

5 CASE STUDIES

The technological advancements on the Internet of Things (IoT) have led to the integration of blockchain technology, significantly improving security, scalability, and interoperability in connected systems. The Internet of Things (IoT) has reached a level of integration into everyday objects, from smart toasters to mirrors displaying fitness exercises and statistics (Velazquez, 2022). A novelty in these devices' development is their connection to blockchain technology, which enhances functionality and security. The following examples illustrate successful cases of blockchain solutions implemented in IoT ecosystems.

5.1 Examples of Successful Implementations of Security Solutions for Blockchain and IoT

5.1.1 Helium

Helium is a decentralized network that utilizes blockchain to connect IoT devices through so-called "Hotspots." These devices combine a wireless gateway with a blockchain mining system, enabling users to provide network coverage and earn Helium's token, HNT. The network's key functionality is the Proof-of-Coverage algorithm, which uses radio signals to validate network coverage, even with variable connection quality. Migration to the Solana blockchain allowed faster transactions and support for smart contracts, while the LoRaWAN protocol ensured long-range and low energy consumption. Practical applications of Helium include connecting sensors in smart cities for air quality monitoring, controlling agricultural parameters such as soil moisture and temperature, and tracking shipments in logistics. Helium, known as "The People's Network," further promotes a participatory governance and development model. (Helium, 2025)

5.1.2 Xage Security

Xage Security provides pioneering solutions for protecting IoT devices using blockchain and applying the principles of zero-trust architecture. Their platform, called Xage Fabric, employs distributed architecture to eliminate central points of vulnerability. It ensures granular access control and privileged account management, while network segmentation prevents lateral attacker movement. Additionally, resistance to threats posed by quantum computers ensures long-term system security. Xage Security is relevant in industries such as:

- Energy, where it protects infrastructure like power plants.
- Manufacturing, by securely connecting industrial IoT devices.
- Transportation, by securing smart transportation systems; and
- Government agencies, by safeguarding data and operational infrastructures.

Its scalable solutions improve security and productivity in digital environments. (Xage, 2025)

5.1.3 Atonomi

Atonomi offers a decentralized security layer specifically designed for IoT. Utilizing blockchain to register device identities and manage reputations, Atonomi enables secure connections for validated devices. Each IoT device receives a unique identity recorded on the blockchain, ensuring immutability and authenticity. The system monitors device behavior over time, assigning reputation scores to detect anomalies. Communication between devices is protected via end-to-end encryption, while real-time analytics enable automated detection of potential threats. Atonomi is designed for heterogeneous IoT environments, facilitating easy connections between diverse devices. Practical applications include smart homes, where Atonomi secures communication between devices like smart thermostats and security cameras and healthcare,

industrial IoT, and transportation, providing comprehensive protection for IoT ecosystems. (Atonomi, 2018)

5.1.4 IOTA

Based on the innovative Tangle network, IOTA differs from traditional blockchain technologies. By utilizing Directed Acyclic Graphs (DAG), IOTA enables fee-free transactions, scalability, and energy efficiency, making it particularly suitable for IoT ecosystems. Each transaction in the Tangle network confirms the previous two, decentralizing the validation process and eliminating the need for energy-intensive nodes or miners. IOTA allows secure storage and data exchange between IoT devices, increasing trust within the network. Its applications include resource management in smart cities, supporting mobility and transportation through microtransactions, industrial IoT, and healthcare, and providing secure medical data storage. Scalability and energy efficiency make it an ideal solution for a wide range of IoT applications. (Alsboui, Qin, Hill, & Al-Aqrabi, 2020; Alshaikhli, Al-Maadeed, & Saleh, 2025)

5.1.5 RIZON

RIZON is a blockchain platform focused on interoperability and support for digital currencies and business applications. Leveraging the Tendermint engine and Cosmos SDK infrastructure, RIZON facilitates fast and secure transactions and seamless integration with other blockchain networks via the Inter-Blockchain Communication (IBC) protocol. The platform supports issuing stable digital currencies pegged to fiat, making them suitable for everyday transactions. RIZON is particularly applicable in financial services, e-commerce, supply chain tracking, and decentralized applications. Its high scalability and flexibility allow adaptation to various applications and user needs, making it an attractive choice for companies looking to integrate blockchain technology. (Tendermint, 2025; Rizon, 2022)

5.2 Analysis of Real-World Attacks and Their Solutions

The analysis of real-world attacks on IoT devices reveals significant security challenges that can compromise connected blockchain systems. Examples of documented attacks on IoT devices with implications for blockchain systems and the solutions implemented include:

1. ***Deauthentication Attacks on IoT Devices***

Deauthentication attacks became widely known around 2014 when security researchers uncovered vulnerabilities in Wi-Fi devices used in IoT systems. Victims of these attacks often included users of smart home devices, automation systems, and industrial IoT (IIoT) systems. Attackers used deauthentication techniques to disrupt communication between IoT devices and the network, compromising data integrity and operational reliability. As a result, systems became non-functional, leading to service interruptions and potential data loss. (Kristiyanto & Ernastuti, 2020; Gebresilassie, Rafferty, Chen, Cui, & Abu-Tair, 2023)

- *Attack:* Deauthentication attacks exploit vulnerabilities in Wi-Fi standards by sending specific packets that force devices to disconnect from the network. These attacks often target security cameras and control systems, jeopardizing user privacy and security.
- *Solution:* Using blockchain technology for device authentication, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), helps prevent such attacks by ensuring that only authorized devices can access the network. Additionally, implementing new Wi-Fi standards like WPA3 reduces vulnerabilities to deauthentication attacks. The WPA3 standard introduces improvements such as Simultaneous Authentication of Equals (SAE), further mitigating vulnerabilities.

2. ***Jeep Cherokee Hacking Incident***

One of the most serious incidents, the Jeep Cherokee hacking case of 2015, highlighted vulnerabilities in IoT-connected vehicles. The demonstration showed how attackers could take control of a car, compromising functions such as braking and steering.

- *Attack:* Security researchers demonstrated how they managed to gain control over the Jeep Cherokee vehicle by exploiting vulnerabilities in its infotainment system. Attackers could manipulate functions like braking, acceleration, and steering, raising significant concerns about the safety of connected cars (Blane, 2021)

- *Solution:* In response, manufacturers implemented software security patches for vehicles. Additionally, they introduced stricter measures to secure communication channels between cars and servers, including enhanced encryption and authentication. (McCracken, 2019)

3. **Attacks on Smart Homes**

Attacks on smart homes gained attention in 2016 when researchers uncovered vulnerabilities in devices such as smart thermostats and security cameras. One notable case involved the hacking of smart cameras, enabling attackers to access user networks and sensitive private data. These attacks often target devices with weak security settings, such as default passwords or unencrypted communication. As a result, compromised networks could also jeopardize blockchain systems connected to IoT devices, undermining data integrity and user privacy.

- *Attack:* Attackers exploited vulnerabilities in smart devices to gain control of networks. Hacking smart thermostats allowed attackers to manipulate heating settings, while compromised security cameras provided access to video footage and network data. (Hunter & Moody, 2017; Alam & Tomai, 2023)
- *Solution:* Implementing Zero Trust principles, where each device is verified before being granted network access, is key to preventing such attacks. Regular firmware updates, strong password use, and encrypted communication further enhance the security of smart devices. (Hunter & Moody, 2017)

4. Mirai Botnet Attack

The Mirai botnet attack of 2016 infected millions of IoT devices using default or weak passwords. Infected devices were turned into bots **that** carried out massive DDoS attacks, causing global disruptions to services like Twitter and Spotify. The attack highlighted IoT devices' vulnerabilities due to inadequate security practices, while IoT networks connected to blockchain could potentially also face risks.

- *Attack:* Mirai malware scanned the internet to identify devices with weak passwords, using a predefined list for rapid identification of vulnerable devices. The infected devices became part of a botnet that executed attacks. (Fruhlinger, 2018; Bursztein, 2017)
- *Solution:* Changing default passwords to more complex ones, regularly updating firmware, and implementing systems to detect and block suspicious traffic (IDS/IPS) are essential steps to prevent similar attacks. (Joodat, n.d)

5. Ransomware Attacks on IoT Devices

One of the more recent incidents, the ransomware attack on Colonial Pipeline in 2021, highlighted **vulnerabilities** in IoT devices within critical infrastructure. Although not directly related to blockchain, this attack underscored the vulnerabilities of IoT devices and operational technologies (OT) used in industrial systems. The attack caused significant consequences, including fuel shortages and financial losses.

- *Attack:* Attackers exploited network vulnerabilities within the company to install **ransomware**, resulting in the shutdown of key systems for fuel distribution (Mittal, 2024). Attackers locked IoT devices and demanded ransom, potentially impacting blockchain systems that rely on those devices. (AgilePQ, 2021)
- *Solution:* The company enhanced network segmentation to restrict access to critical systems, reducing potential security risks. It also established policies for regular **software** and firmware updates on IoT devices to minimize vulnerabilities. Although not directly applied in this instance, blockchain is gaining traction as a reliable method for ensuring data integrity in industrial IoT systems. (Lubin, 2023)

These examples emphasize how IoT and blockchain technology integration can be vulnerable and how effectively implemented innovative solutions can improve security.

6 THE FUTURE OF BLOCKCHAIN SECURITY IN THE IOT ERA

The future of protecting blockchain from attacks via IoT devices requires the implementation of Zero Trust architecture, where every device and user is verified before gaining network access. Artificial intelligence can play a pivotal role in anomaly detection and threat prediction, while the development of quantum-resistant cryptographic algorithms becomes essential due to potential threats from quantum computing. Standardizing

security protocols for IoT devices, including encryption and regular updates, is crucial for enhancing security, combined with decentralized authentication via blockchain to eliminate central points of vulnerability.

User education on the importance of strong passwords and recognizing threats is a significant factor, while interoperable solutions enable easier integration of IoT devices with different blockchain networks. The focus should also be on developing energy-efficient technologies, establishing standards for cybersecurity resilience testing, and automating security processes through smart contracts. Finally, collaboration between industries, academic institutions, regulatory bodies, and international organizations is necessary to ensure an integrated approach to addressing challenges.

7 CONCLUSIONS

Protecting blockchain technology from attacks via IoT devices is becoming increasingly significant with the growing adoption of IoT and its integration with decentralized systems. The key security challenges stem from vulnerabilities in IoT devices, such as weak passwords, insecure communication, and limited resources for implementing advanced protective measures. These challenges can compromise the integrity, availability, and immutability of blockchain systems, requiring a proactive and multi-layered approach to risk mitigation.

- The analysis of technological solutions showed that implementing Zero Trust architecture, advanced cryptographic algorithms, and smart contracts significantly enhances security. AI technology used for anomaly detection and threat prediction further ensures the resilience of IoT and blockchain networks. Establishing security standards and fostering collaboration between manufacturers, industry, regulatory bodies, and academic institutions are crucial steps toward improving protection. Based on the analysis, conditions have been met to reject the null hypothesis (H_0), confirming a significant correlation between IoT-related security challenges and blockchain technology compromise.

Recommended protective measures have extensive applicability across key industries, including healthcare, transportation, energy, and manufacturing. For example, blockchain technology can ensure the confidentiality and integrity of medical data in healthcare systems. Smart contracts automate logistical processes in transportation. Energy-efficient IoT devices connected to blockchain networks can improve operational reliability in industrial production, while Zero Trust architecture secures critical infrastructure like power plants and distribution networks. These approaches increase security but also promote productivity and sustainability within digital ecosystems.

Recommendations for the Future Work

Research on quantum-resistant cryptographic algorithms represents a vital step in preparing blockchain systems for emerging threats from quantum computing. Future studies on the effects of user education in reducing IoT device vulnerabilities could provide valuable insights for shaping security policies. Interdisciplinary research that connects technology, economics, and regulations can contribute to a better understanding of how security standards impact the global adoption of blockchain in IoT ecosystems.

The paper provides recommendations for future work and analyzes real-world cases. It highlights the importance of continuous monitoring and improvement of protective measures. These efforts aim to preserve confidentiality, integrity, and the functionality of blockchain systems within IoT environments.

WORKS CITED

AgilePQ. (2021). *Colonial Pipeline Co. Ransomware Attack.* AgilePQ. Retrieved from https://agilepq.com/wp-content/uploads/2021/07/APQ_WP_Colonial_Pipeline_5.14.21.pdf

Alam, H., & Tomai, E. (2023). Security Attacks and Countermeasures in Smart Homes. *International Journal on Cybernetics & Informatics, 12*(2). doi:10.5121/ijci.2023.120209

Alsboui, T., Qin, Y., Hill, R., & Al-Aqrabi, H. (2020). Towards a Scalable IOTA Tangle-Based Distributed Intelligence Approach for the Internet of Things. *Intelligent Computing. SAI 2020. Advances in Intelligent Systems and Computing.* London, UK: Springer, Cham. doi:10.1007/978-3-030-52246-9_35

Alshaikhli, M., Al-Maadeed, S., & Saleh, M. (2025). Enhancing Scalability and Network Efficiency in IOTA Tangle Networks: A POMDP-Based Tip Selection Algorithm. *Computers, 14*(4), 117. doi:10.3390/computers14040117

Atonomi. (2018, 05 17). *Atonomi Launches Identity Registry Network Beta to Enable Secure Interoperability for the Internet of Things.* Retrieved from PR Newswire: https://www.prnewswire.com/news-releases/atonomi-launches-identity-registry-network-beta-to-enable-secure-interoperability-for-the-internet-of-things-300647697.html

Balogh, S., Gallo, O., Ploszek, R., Špaček, P., & Zajac, P. (2021). IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques. *Electronics, 10*(21), 2647. doi:10.3390/electronics10212647

Becher, B., & Urwin, M. (2025, 01 23). *Blockchain: What It Is, How It Works, Why It Matters.* Retrieved from BuiltIn: https://builtin.com/blockchain

Belin, O. (2018, Jan 30). *The Difference Between Blockchain & Distributed Ledger Technology*. Retrieved from TRADEIX: https://tradeix.com/distributed-ledger-technology/

Blane, E. (2021, 02 25). *The Groundbreaking 2015 Jeep Hack Changed Automotive Cybersecurity*. Retrieved from Fractional CISCO: https://fractionalciso.com/the-groundbreaking-2015-jeep-hack-changed-automotive-cybersecurity/

Bobde, Y., Narayanan, G., Jati, M., Raj, R. S., Cvitić, I., & Peraković, D. (2024). Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics, 13*(4). doi:10.3390/electronics13040687

Bursztein, E. (2017, 12 14). *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*. Retrieved from CloudFlare: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Internet of Things and the Man-In-the-Middle Attacks – Security and Economic Risks. *MEST Journal, 5*(2), 15-25. doi:10.12709/mest.05.05.02.03

Cekerevac, Z., Prigoda, L., & Čekerevac, P. (2025). Enhancing Digital Security in the Financial Sector With AI, IoT, and Blockchain. *Sustainability and Economic Resilience in the Context of Global Systemic Transformations.* Chisinau, Moldova.

Cekerevac, Z., Prigoda, L., & Maletic, J. (2018, July 15). Blockchain Technology and Industrial Internet of Things in the Supply Chains. (Z. Cekerevac, Ed.) *MEST Journal, 6*(2), 39-47. doi:10.12709/mest.06.06.02.05

Cosmos Network. (n.d.). *Build on the Interchain.* Retrieved 04 08, 2025, from Cosmos Network: https://cosmos.network/

Čekerevac, Z., Prigoda, L., & Čekerevac, P. (2025). Leading Technological Innovations in Digital Security (TIDS-2025). *Technological Innovations in Digital Security*, (p. 15). Chisinau, Moldova.

Demertzis, K., Iliadis, L., Tziritas, N., & Kikiras, P. (2020). Anomaly detection via blockchained deep learning smart contracts in industry 4.0. *Neural Computing and Applications, 32*, 17361–17378. doi:10.1007/s00521-020-05189-8

Douaioui, K., & Benmoussa, O. (2024). Insights into Industrial Efficiency: An Empirical Study of Blockchain Technology. *Big Data Cogn. Comput, 8*(6), 62. doi:10.3390/bdcc8060062

Ethereum. (2025, 03 03). *Introduction to Smart Contracts*. Retrieved from Ethereum: https://ethereum.org/en/smart-contracts/

Fruhlinger, J. (2018, 03 09). *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet*. Retrieved from CSO: https://www.csoonline.com/article/564711/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Gebresilassie, S. K., Rafferty, J., Chen, L., Cui, Z., & Abu-Tair, M. (2023). Transfer and CNN-Based De-Authentication (Disassociation) DoS Attack Detection in IoT Wi-Fi Networks. *Electronics, 12*(17), 3731. doi:10.3390/electronics12173731

Helium. (2025). *Proof-of-Coverage*. Retrieved from Helium Foundation: https://docs.helium.com/iot/proof-of-coverage/

Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal, 22*(1), 105-117. doi:10.1016/j.eij.2020.05.003

Hunter, A., & Moody, M. (2017). Exploiting known vulnerabilities of a smart thermostat. *Proceedings Of 2016 14Th Annual Conference On Privacy, Security And Trust (Pst)*, (pp. 1-4). doi:10.1109/PST.2016.7906936

Hyperledger Fabric. (2023). *A Blockchain Platform for the Enterprise*. Retrieved from Hyperledger Fabric: https://hyperledger-fabric.readthedocs.io/en/release-2.5/

Ibrahim, R. F., Al-Haija, Q. A., & Ahmad, A. (2022). DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors, 22*(18), 6806. doi:10.3390/s22186806

Joodat, R. (n.d). *Distributed Denial of Service (DDOS) attacks and IoT Security. (Mirai Botnet)*. Retrieved from Academia: https://www.academia.edu/33385809/Distributed_Denial_of_Service_DDOS_attacks_and_IoT_Security_Mirai_Botnet_Cloudflare_Orbit_Robert_Joodat

Kristiyanto, Y., & Ernastuti. (2020). Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test. *CommIT Journal, 14*(1), 45-51.

Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., . . . Liu, Q. (2024). Dissecting zero trust: research landscape and its implementation in IoT. *Cybersecurity, 7*(20). doi:10.1186/s42400-024-00212-0

Lubin, A. (2023). Cyber Plungers: Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation. *Georgia Law Review, 57*, 1607-1634. Retrieved from https://ssrn.com/abstract=4483228

Maletic, J., & Cekerevac, Z. (2019). IIoT Security in Supply Chain. *Proceedings of the V International Scientific and Practical Conference "Scientific and Technical Aspects of Innovative Development of the Transport Complex"*, (pp. 44-48). Doneck. Retrieved from https://cekerevac.eu/biblioteka/K74.pdf

McCracken, S. (2019, 01 19). *The uConnect Infotainment System Was Hacked. Now What?* Retrieved from Jeepproblems.com: https://www.jeepproblems.com/uconnect-hack/

Mittal, M. (2024). Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience. *International Journal of Oil, Gas and Coal Engineering, 12*(6), 106-119. doi:10.11648/j.ogce.20241205.11

Palkadot. (2024, 07 29). *Defy what's possible*. Retrieved from Palkadot: https://polkadot.com/

R3. (2025, 02 12). *Corda*. Retrieved from R3: https://r3.com/corda/

Rizon. (2022, 01 12). *RIZON Blockchain Digital Currency & Asset Hub.* Retrieved from RIZON: http://rizon.world/

SC. (2023, 06 23). *Trojanized OpenSSH used in Linux, IoT device compromise*. Retrieved from SC Media: https://www.scworld.com/brief/trojanized-openssh-used-in-linux-iot-device-compromise

Sengupta, J. (2020). A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 20. doi:10.1016/j.jnca.2019.102481

Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors, 22*(3), 1094. doi:10.3390/s22031094

SSL. (2021, 11 23). *Securing the Internet of Things (IoT) with SSL/TLS.* Retrieved from SSL.com: https://www.ssl.com/article/securing-the-internet-of-things-iot-with-ssl-tls/

Tendermint. (2025). *The standard for interchain communication*. Retrieved from Tendermint: https://tendermint.com/ibc/

Tsaur, W.-J., Chang, J.-C., & Chen, C.-L. (2022). A Highly Secure IoT Firmware Update Mechanism Using Blockchain. *Sensors, 22*(2), 530. doi:10.3390/s22020530

Valencia-Payan, C., Griol, D., & Corrales, J. C. (2024). Blockchain self-update smart contract for supply chain traceability with data validation. *Logic Journal of the IGPL*, jzae047. doi:10.1093/jigpal/jzae047

Velazquez, R. (2022, 10 19). *Blockchain and IoT: 10 Examples Making Our Future Smarter.* Retrieved from Builtin: https://builtin.com/blockchain/blockchain-iot-examples

Wigmore, I. (July 2016 г.). *Internet of Things (IoT)*. Получено из TechTarget - IoT Agenda: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Xage. (2025). *Xage Fabric Platform*. Retrieved from Xage: https://xage.com/products/xage-fabric-platform/

Zafar, S., Bhatti, K. M., Shabbir, M., Hashmat, F., & Akbar, A. H. (2021). Integration of blockchain and Internet of Things: challenges and solutions. *Annals of Telecommunications, 77*, 13-32.

Zaheer, H., Shoaib, M., Iqbal, F., Arshad, S., Altaf, A., Villena, E. G., . . . Ashraf, I. (2024). An Energy-Efficient Technique to Secure Internet of Things Devices Using Blockchain. *Journal of Network and System Management, 32*. doi:10.1007/s10922-024-09870-4

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation, 6*(2), 172-203. doi:10.1093/jfr/fjaa010

Received for publication: 06.04.2025
Revision received: 03.05.2025
Accepted for publication: 08.07.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Cekerevac, Z., Ohrimenco, S., & Cekerevac, P. (2025, 07 15). Protecting Blockchain From IoT Device Attacks: Challenges and Solutions. (Z. Cekerevac, Ed.) *MEST Journal, 13*(2), 81-93. doi:10.12709/mest.13.13.02.05

Style – **Chicago** *Sixteenth Edition:*

Cekerevac, Zoran, Serghei Ohrimenco, and Petar Cekerevac. "Protecting Blockchain From IoT Device Attacks: Challenges and Solutions." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 2 (07 2025): 81-93.

Style – **GOST** *Name Sort:*

Cekerevac Zoran, Ohrimenco Serghei and Cekerevac Petar Protecting Blockchain From IoT Device Attacks: Challenges and Solutions [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 07 15, 2025. - 2 : Vol. 13. - pp. 81-93.

Style – **Harvard** *Anglia:*

Cekerevac, Z., Ohrimenco, S. & Cekerevac, P., 2025. Protecting Blockchain From IoT Device Attacks: Challenges and Solutions. *MEST Journal,* 15 07, 13(2), pp. 81-93.

Style – **ISO 690** *Numerical Reference:*

Protecting Blockchain From IoT Device Attacks: Challenges and Solutions. **Cekerevac, Zoran, Ohrimenco, Serghei and Cekerevac, Petar.** [ed.] Zoran Cekerevac. 2, Belgrade – Toronto : MESTE, 07 15, 2025, MEST Journal, Vol. 13, pp. 81-93.