ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

UDC 004.75:004.738.5:004.056

O. Streltsov, PhD, Assoc. Prof.,
M. Katrichenko,
Yu. Ornovetsky,
M. Hrynyov
Odessa Polytechnic National University, Shevchenko Ave. 1, Odesa, Ukraine, 65044, e-mail: streltsov.o.v@op.edu.ua

USING BLOCKCHAIN TECHNOLOGY TO IMPROVE SECURITY IN THE DISTRIBUTED INTERNET OF THINGS

О. Стрельцов, М. Катріченко, Ю. Орновецький, М. Гриньов. **Використання технології blockchain для покращення безпеки у розподіленому інтернеті речей.** Сучасний розвиток інформаційних технологій дедалі більше орієнтується на побудову розподілених систем, зокрема Інтернету речей (IoT), який об'єднує мільярди пристроїв у єдину глобальну інфраструктуру. Проте масштабне поширення IoT супроводжується зростанням ризиків у сфері кібербезпеки, оскільки централізовані підходи до зберігання та обробки даних часто виявляються вразливими до атак, маніпуляцій або відмов обладнання. У цьому контексті все більшої уваги набуває використання технології блокчейн, яка завдяки своїм ключовим характеристикам – децентралізації, прозорості та незмінності даних – відкриває нові можливості для підвищення рівня безпеки в розподіленому Інтернеті речей. У статті розглянуто проблематику забезпечення захисту інформації в IoT-системах, проаналізовано основні загрози, такі як несанкціонований доступ, підробка даних, витоки конфіденційної інформації та DDoS-атаки. Особлива увага приділяється аналізу того, як інтеграція blockchain здатна мінімізувати ці ризики шляхом децентралізованого управління доступом, автентифікації пристроїв, захищеного зберігання та передачі даних. Розглянуто можливості застосування смарт-контрактів для автоматизації процесів взаємодії між вузлами IoT-мережі, що підвищує довіру між учасниками та знижує потребу у посередниках. У результаті дослідження визначено, що поєднання IoT та blockchain створює передумови для побудови надійних, стійких до зловмисних впливів розподілених систем. Це може мати практичне застосування у таких сферах, як «розумні» міста, промисловий Інтернет речей, охорона здоров'я та енергетика. Водночас відзначено виклики, пов'язані з масштабованістю, затримками при обробці транзакцій та енергоспоживанням. Перспективними напрямами подальших досліджень є оптимізація протоколів консенсусу, використання гібридних архітектур та розробка спеціалізованих рішень для IoT-середовища.
Ключові слова: інтернет речей, блокчейн, однорангова мережа, доказ автентифікації, децентралізована мережа

O. Streltsov, M. Katrichenko, Yu. Ornovetsky, M. Hrynyov. **Using blockchain technology to improve security in the distributed internet of things**. The rapid development of information technologies increasingly focuses on building distributed systems, in particular the Internet of Things (IoT), which integrates billions of devices into a single global infrastructure. However, the large-scale adoption of IoT is accompanied by growing cybersecurity risks, since traditional centralized approaches to data storage and processing often prove to be vulnerable to attacks, manipulations, or equipment failures. In this context, the use of blockchain technology is gaining increasing attention. Owing to its key features – decentralization, transparency, and immutability of data – blockchain provides new opportunities to enhance security in distributed IoT environments. The article addresses the problem of information protection in IoT systems and analyzes major threats such as unauthorized access, data tampering, leakage of sensitive information, and DDoS attacks. Particular attention is given to how the integration of blockchain can minimize these risks through decentralized access management, device authentication, and secure storage and transmission of data. The use of smart contracts for automating interaction processes between IoT nodes is also examined, highlighting how they foster trust among participants and reduce the need for intermediaries. The findings suggest that combining IoT with blockchain technology creates the foundation for secure and resilient distributed systems that are resistant to malicious activities. Practical applications include smart cities, industrial IoT, healthcare, and energy management. At the same time, the paper outlines key challenges related to scalability, transaction latency, and energy consumption. Future research directions include optimizing consensus protocols, exploring hybrid architectures, and designing specialized blockchain solutions tailored to IoT environments.
Keywords: Internet of Things, blockchain, peer-to-peer network, proof of authentication, decentralized network

1. Introduction

In today's era of digital transformation, the Internet of Things (IoT) plays a key role in the development of information and communication technologies, allowing physical objects with built-in sensors, software and communication devices to be connected into a single network. The rollout of fifth-generation (5G) networks, which provide high bandwidth and reduced data transmission latency, has significantly accelerated the adoption of IoT in various areas, from smart home systems to critical infrastructure: smart cities, e-Health systems, industrial IoT (IIoT), automated agriculture, distributed control systems and intelligent transport [1, 2].

Although the introduction of IoT technologies contributes to process automation, resource optimisation and increased efficiency, it is accompanied by significant challenges in the field of cybersecurity. In particular, the scale of IoT infrastructure deployment, its heterogeneity, limited hardware resources of devices, and frequent disregard for proper protection mechanisms create numerous attack vectors [3].

DOI: 10.15276/opu.2.72.2025.14

One of the key threats is the possibility of remote takeover of IoT devices for use in botnets – networks of compromised devices controlled by an attacker. A typical scenario involves hacking poorly protected remote administration interfaces, in particular using default passwords or unpatched vulnerabilities in the firmware. Such botnets can be used to carry out distributed denial-of-service (DDoS) attacks, intercept or modify traffic, substitute data, attack the integrity of services, or interfere with the operation of critical facilities [4].

In centralised IoT architectures, there is an increased risk of compromising key nodes, such as central servers or microcontrollers that coordinate data exchange between devices. A successful attack on such an infrastructure element can lead to large-scale interference in the operation of the entire network, which highlights the need to develop mechanisms for redundancy, decentralisation, and protection of communication channels.

Thus, the security problem in the distributed Internet of Things is complex and requires an interdisciplinary approach, including the development of adaptive security protocols, authentication and authorisation mechanisms, software update strategies, and the application of artificial intelligence methods to detect anomalous behavior in network traffic. A blockchain-oriented Internet of Things architecture with smart contract-based data transfer can significantly improve integrity and trust in distributed Internet of Things systems [5].

2. Analysis of literature and statement of the problem

One of the main architectural models traditionally used to organise Internet of Things (IoT) systems is a centralised management model, in which the main processing, control and data storage are concentrated on a central server or in a cloud environment. This approach is relatively simple to implement, but has significant limitations in terms of attack resistance, scalability, and fault tolerance. The central point of control creates a critical vulnerability: if the server infrastructure is compromised, an attacker could potentially gain access to the entire network of IoT devices [6].

In contrast, decentralised architecture provides for distributed management, where each device in the network acts as an independent node capable of communicating without the need for a centralised intermediary. This means that compromising one device does not allow the attacker to control the entire network. To completely take over control of the system, an attacker would have to compromise a large number of nodes, which significantly complicates the attack [7].

An additional advantage of the decentralised model is provided by the implementation of blockchain technologies, which allow the creation of a secure communication environment between nodes by transmitting signed transactions stored in a distributed ledger. Such a ledger guarantees data immutability and message authenticity, and also provides the ability to verify each transaction by other nodes in the network [8]. Blockchain also eliminates the need for centralised trust, allowing the creation of trustless systems based on peer-to-peer (P2P) interaction. Smart contracts on blockchain create both opportunities and challenges in automation [9].

The key advantages of decentralised IoT include:

– decentralised management, which minimises the risks associated with centralised points of failure;

– high security through digital signatures, encryption and transaction verification mechanisms;

– device identification provided by public key authentication;

– network flexibility and scalability, allowing new nodes to be connected without rebuilding the infrastructure;

– autonomous operation, independent of the stability or performance of the central server;

– data reliability, as data is only recorded on the blockchain after verification, which prevents the creation or substitution of information.

Compared to centralised systems, decentralised IoT networks demonstrate a higher level of fault tolerance, which is particularly important for critical applications, such as in healthcare, energy, or transport infrastructure.

Therefore, a decentralised approach to building IoT systems is a promising direction that combines modern cryptographic methods, distributed computing and the concept of autonomous interaction, providing a new level of security, trust and stability in the context of a rapidly growing number of connected devices.

3. Purpose and objectives of the study

The purpose of this study is to analyse architectural approaches to building Internet of Things systems, with an emphasis on the advantages of a decentralised model compared to a centralised one. The paper examines the impact of decentralisation on the level of information security, resistance to

ISSN 2076-2429 (print)
ISSN 2223-3814 (online)

attacks, scalability and network autonomy. It also identifies the potential for integrating blockchain technologies to build trusted, secure and fault-tolerant distributed IoT systems.

4. Materials and methods

Based on a comparative analysis of centralised and decentralised IoT architectures in terms of key parameters of security, flexibility and resistance to attacks, scientific sources covering current approaches to ensuring security in IoT (in particular, using blockchain technologies), a logical communication diagram for a distributed IoT network with blockchain support is proposed (Fig. 1).

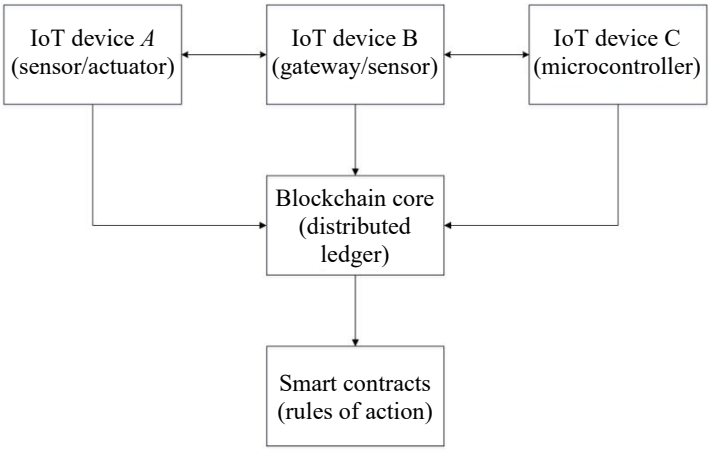

Fig. 1. Communication model in a distributed IoT network with blockchain support

The proposed model illustrates how nodes interact in a decentralised IoT network, where blockchain technology is used for data protection and access control.

Each IoT device (sensor, gateway, actuator, etc.) is a full-fledged network node with the following functions:

– data collection (temperature, pressure, movement, etc.);

– signing transactions with your own private key;

– sending messages to other nodes;

– validating transactions from a distributed ledger (partially or completely).

In some cases, nodes can be full nodes or light nodes, depending on resources.

The central element of decentralised logic is the blockchain core (distributed ledger).

Each node has a copy of the registry (complete or partial). Data sent by devices is recorded as transactions (in JSON format). Validation occurs through consensus (e.g., Proof-of-Authority, Delegated Proof-of-Stake, or IBFT for IoT). Recent advances in lightweight consensus and sharding techniques for IoT data exchange have demonstrated significant performance improvements under high transaction loads [10].

Smart contracts are software rules that automate actions in response to events:

– when a certain threshold value is reached or exceeded, the sensor activates the corresponding executive element;

– control access to data;

– process microtransactions between devices.

The communication process in the network occurs in the following sequence:

1. Data collection: The IoT device measures a parameter (e.g., temperature).

2. Transaction formation: The data is packaged into a transaction, which is signed with the device's private key.

3. Network transmission: the transaction is distributed via a P2P network to other nodes.

4. Validation: neighboring nodes check the signature, time, format and presence of conflicts.

5. Recording to the blockchain: once consensus is reached, the transaction is added to the next block.

6. Smart contract execution: if there is a corresponding trigger, an action is performed (e.g., a command to a relay).

7. Status update: all nodes synchronise their copies of the ledger.

5. Research results

This approach ensures data security – all transactions are signed and verified, and the data is immutable. The scheme has the advantage of autonomy: nodes operate without a central coordinator.

The proposed model is resistant to attacks because the failure of a single node does not affect the operation of the entire network. It has transparent access to data in an open registry that cannot be changed in an unauthorised manner. The network has good dynamic scalability and does not require additional configuration.

For the practical implementation of the logical model of a decentralised IoT network, the Ethereum platform was used – one of the most widespread blockchain ecosystems with built-in support for smart contracts.

When using this platform, each IoT device (or its gateway) interacts with the Ethereum network via an Ethereum light client node (e.g., via Geth, Infura, or Alchemy), which allows transactions to be transmitted without the need to store the entire blockchain on the device.

The implementation of the logical model consists of three main components:

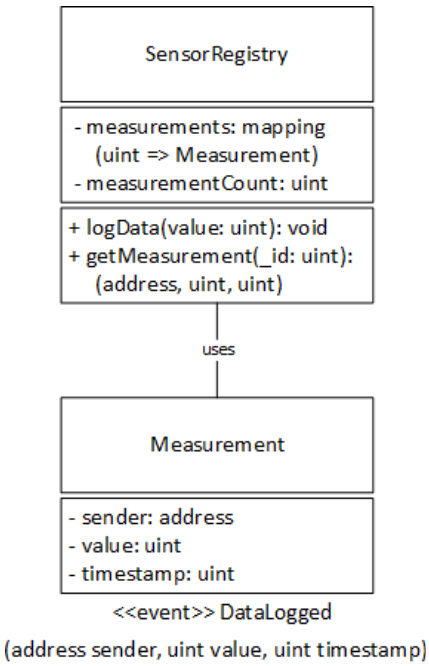

Fig. 2. Diagram of a smart contract fragment

1. An IoT device that generates key pairs (private/public), signs measured values (e.g., temperature) and transmits the transaction to the Ethereum gateway.

2. An Ethereum gateway connected to the Ethereum main net or test network (e.g., Sepolia, Goerli) that accepts transactions from multiple devices and forms calls to smart contracts.

3. The smart contract, which accepts parameters (sender, value, timestamp), stores the transaction history in event logs or arrays, and implements the logic for notification or triggering automated actions (Fig. 2).

Each IoT device (via a gateway) calls the logData() method, passing the measured value. The information is stored in a mapping with the possibility of further reading. The DataLogged event allows the system to respond to new measurements in real time (for example, in an external infrastructure via a Web3 connection).

Implementation on Ethereum determines storage reliability: all transactions are recorded in the blockchain and cannot be changed. Smart contracts enable the implementation of complex response logic, which provides certain opportunities for automation.

Integration with other systems is possible, for example, payment systems for micropayments for device services.

6. Conclusions

The proposed implementation of the model has certain limitations on the amount of storage in the smart contract. Transaction costs (gas fees) can complicate mass data recording.

For optimisation, only data hashes can be transferred to the blockchain, while the data itself is stored in external storage (IPFS, Filecoin).

To reduce transaction costs, Ethereum *L2* solutions (e.g., Arbitrum, Optimism) can be used.

As a result, this implementation allows for the creation of a reliable, distributed, scalable IoT system capable of autonomous operation, in which all transactions are confirmed by the Ethereum network consensus, and data is protected from unauthorised modification or falsification.

Література

1. Гриневич О. М., Ткачук А. В. Забезпечення кібербезпеки в системах Інтернету речей. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2021. № 3(41). С. 54–60.
2. Шаров Ю. М., Бондар С. І. Проблеми інформаційної безпеки у розподілених IoT-системах. *Збірник наукових праць Харківського університету Повітряних Сил*. 2022. № 4(74). С. 112–117.

3. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*. 2015. Vol. 76. P. 146–164. DOI: https://doi.org/10.1016/j.comnet.2014.11.008.
4. Kolias C., Kambourakis G., Stavrou A., Voas J. DDoS in the IoT: Mirai and other botnets. *Computer*. 2017. Vol. 50, No. 7. P. 80–84. DOI: https://doi.org/10.1109/MC.2017.201.
5. Albulayhi A. S., Alsukayti I. S. A Blockchain-Centric IoT Architecture for Effective Smart Contract-Based Management of IoT Data Communications. *Electronics*. 2023. Vol. 12, No. 12. Art. 2564. DOI: https://doi.org/10.3390/electronics12122564.
6. Пономаренко В. С., Кравченко О. О., Станіславенко В. А. Застосування блокчейн-технологій для підвищення захищеності IoT-мереж. *Інформаційні технології в освіті, науці та техніці*. 2021. № 1(20). С. 45–51.
7. Reyna A., Martín C., Chen J., Soler E., Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*. 2018. Vol. 88. P. 173–190. DOI: https://doi.org/10.1016/j.future.2018.05.046.
8. Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*. 2018. Vol. 5, No. 2. P. 1184–1195. DOI: https://doi.org/10.1109/JIOT.2018.2812239.
9. Khan S. N. et al. Blockchain smart contracts: Applications, challenges, and future directions. *Peer-to-Peer Networking and Applications*. 2021. Vol. 14. P. 2151–2163. DOI: doi.org.
10. Haque E. U. et al. Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. *Scientific Reports*. 2024. Vol. 14. Art. 26561. DOI: https://doi.org/10.1038/s41598-024-77706-x.

References

1. Hrynevych, O. M., & Tkachuk, A. V. (2021). Ensuring cybersecurity in Internet of Things systems. *Naukovi zapysky Ukrainskoho naukovo-doslidnoho instytutu zv'iazku*, *3*(41), 54–60.
2. Sharov, Yu. M., & Bondar, S. I. (2022). Problems of information security in distributed IoT systems. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh Syl*, *4*(74), 112–117.
3. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008.
4. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201.
5. Albulayhi, A. S., & Alsukayti, I. S. (2023). A blockchain-centric IoT architecture for effective smart contract-based management of IoT data communications. *Electronics*, *12*(12), Article 2564. https://doi.org/10.3390/electronics12122564.
6. Ponomarenko, V. S., Kravchenko, O. O., & Stanislavenko, V. A. (2021). Application of blockchain technologies to increase the security of IoT networks. *Informatsiini tekhnolohii v osviti, nautsi ta tekhnitsi*, *1*(20), 45–51.
7. 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.
8. 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.
9. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., & Bennani, E. (2021). Blockchain smart contracts: Applications, challenges, and future directions. *Peer-to-Peer Networking and Applications*, *14*, 2151–2163.
10. Haque, E. U., Abbasi, W., Almogren, A., Choi, J., Altameem, A., Ur Rehman, A., & Zaidi, S. A. R. (2024). Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. *Scientific Reports*, *14*, Article 26561. https://doi.org/10.1038/s41598-024-77706-x.

Стрельцов Олег Васильович; Oleh Streltsov, ORCID: https://orcid.org/0000-0002-4691-5703
Катріченко Михайло Олегович; Mykhailo Katrichenko, ORCID: https://orcid.org/0009-0004-2251-5600
Орновецький Юрій Васильович; Yuriy Ornovetsky, ORCID: https://orcid.org/0009-0006-2470-1559
Гриньов Максим Андрійович; Maksym Hrynyov, ORCID: https://orcid.org/0009-0007-7189-4485

Received September 29, 2025
Accepted November 01, 2025