References

1. Kondratiev, Oleksandr. Development of a web application for managing tasks and projects in order to optimize project management processes / O. Kondratiev // Materials of the International Scientific and Practical Conference of Young Scientists, Postgraduates and Students "Information Technologies in the Modern World: Studies of Young Scientists": abstracts of reports, February 27–28, 2025 – Kh.: Semen Kuznets KhNEU, 2025. – P. 4.2.
2. How to Create a Backend with Supabase / Coding Academy // YouTube. – URL : https://www.youtube.com/watch?v=ae2Eaz_zEqQ
3. Project Management Institute – Learn about project management standards and certifications // PMI. – URL: https://www.pmi.org.
4. Supabase – The open source Firebase alternative. – URL : https://supabase.com.

EXPLORING HYBRID ENCRYPTION METHODS IN BLOCKCHAIN NETWORKS

Laktionov Artem, student
Supervisor - Candidate of Technical Sciences, Associate Professor **Yuriy Skorin**
Semen Kuznets Kharkiv National University of Economics

In modern information systems, issues related to cybersecurity are of key importance. With the growth of digital transactions, the popularity of decentralized applications, and the use of blockchain technologies in various fields (logistics, finance, healthcare, identification, etc.), the need for reliable methods of protecting transmitted information is also growing.

Problem statement

While the blockchain itself ensures the integrity and immutability of records in the distributed ledger, it does not guarantee the complete confidentiality and authenticity of the transmitted data, especially in the channels of interaction between users or network nodes. The transmission of information in blockchain environments often takes place without additional layers of encryption or using outdated algorithms. This poses a threat of interception, unauthorized access, or even modification of critical information. Using only symmetric or only asymmetric algorithms is not always effective due to the trade-off between performance and security.

Purpose of the study

The purpose of the study is to implement hybrid encryption methods to ensure the confidentiality, integrity, and authenticity of transmitted data in blockchain networks.

Research results

One of the promising areas for solving these problems is the introduction of hybrid encryption methods that combine the advantages of symmetric (high performance) and asymmetric (secure key exchange) cryptographic systems. This approach allows for both fast encoding of information and secure exchange of key

parameters, which is especially important in open or partially open blockchain networks.

The analysis showed that the most resource-intensive steps are the generation of asymmetric keys and the calculation of the shared secret, which is expected. However, the overall latency remains within acceptable limits, even for interactive DApps or mobile applications. The hybrid model was compared with other methods used in cryptography (symmetric only or only asymmetric encryption) in terms of key parameters. These results confirm that the hybrid model provides the best balance between security and performance, especially in environments where secure key exchange and message integrity must be ensured in an open, decentralized network.

As a result of testing, comparison, and analytical analysis, it was confirmed that the hybrid cryptographic model has high practical value in the context of increasing the information security of data transmission in blockchain networks. It demonstrates an effective combination of cryptographic reliability, performance, implementation flexibility, and compliance with future challenges (including quantum threats).

Conclusions and prospects

In the course of the work, a comprehensive study of hybrid encryption methods and their application to ensure the protection of information in blockchain environments was carried out. Based on the theoretical analysis, it was found that hybrid cryptography combines the strengths of both symmetric and asymmetric encryption methods: high speed of symmetric algorithms (in particular, AES) and secure key transfer provided by asymmetric algorithms (for example, ECC). This combination allows you to achieve an optimal balance between performance and security in the conditions of decentralized networks.

The results of the study demonstrated the high efficiency of the chosen cryptographic model: low delays in encryption and decryption, support for modern standards, scalability, and protection against major types of attacks (including MITM and traffic analysis). The comparative evaluation also confirmed the advantages of the hybrid model over classical approaches. Thus, the results obtained are the basis for the development of practical solutions in the field of secure data transfer in Web3 systems, decentralized applications and digital ecosystems of the next generation.

References

1. DSTU 3008:2015 Information and documentation. Reports in the field of science and technology. Structure and rules of registration. – Kyiv: State Enterprise UkrNDNC, 2015. – 28 p.

2. DSTU 3582:2013. Information and documentation. Bibliographic description. Abbreviations of words and phrases in Ukrainian. General requirements and regulations (ISO 4:1984, NEQ; ISO 832:1994, NEQ) / Nats. standard of Ukraine. – Kyiv: Ministry of Economic Development of Ukraine, 2014. – 18 p.

3. DSTU 8302:2015. Information and documentation. Bibliographic reference. General provisions and rules of compilation / Nats. standard of Ukraine. – Kyiv: SE "UkrNDNC", 2016. – 18 p.