Обмеження. Метод не порушує незалежність подій, проте якість оцінок залежить від вхідних ймовірностей станів. Для надто великих графів з багатостановими вузлами кількість «ймовірнісних пакетів» зростає — у таких випадках варто агрегувати малозначущі вузли, застосовувати кешування підмаршрутів і аналізувати «складні» ділянки окремо.

Висновки. Живучість клієнт-серверних ігрових та мультимедійних систем є критичною властивістю, що забезпечує безперервність роботи попри збої мережі чи часткові відмови компонентів. Для її кількісної оцінки доцільно застосовувати метод ЛІТМ, який дозволяє одночасно виявляти чинники ризику в ієрархії сервісів і оцінювати наслідки їх деградації для користувацького досвіду. На основі ЛІТМ можна створити інструменти для автоматизованого розрахунку показників живучості в різних топологічних і архітектурних сценаріях (mono vs micro, один CDN проти multi-CDN, фолбек-політики). Підхід забезпечує швидке отримання практичних метрик — частки часу в «зеленій» зоні QoE, ймовірності утримання сесії, очікуваного впливу на FPS/RTT — і напряму пов’язує надійність з’єднання та стани компонентів із продуктивністю гри. Загалом, використання ЛІТМ підвищує точність і оперативність аналізу живучості та сприяє підтриманню високих SLA у мережевих ігрових застосунках.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sanap, Prof. (2025). Design and Implementation of Real Time Clock using RTC DS3231 and Arduino Uno. International Journal for Research in Applied Science and Engineering Technology. 13. 1545-1551. 10.22214/ijraset.2025.67162.
2. Guarnieri, Thiago & Almeida, Jussara & Borges, Alex. (2025). Revisiting the Relation between QoS and QoE to improve predictive Models in Adaptive Streaming. 10.21203/rs.3.rs-7455416/v1.
3. Adegoke, Olasupo. (2025). Efficiency and QOS in Cloud Data Centers: An Analysis of DyVoFesLoReMu'S SLA Violations. 9. 1-9. 10.70382/mejaimr.v9i2.056.

UDC 004.93'1:336.74

APPLICATION OF HYBRID ENCRYPTION METHODS IN BLOCKCHAIN NETWORKS

SKORIN YURI (yuriy.skorin@hneu.net)
ARTEM LAKTIONOV (artem.laktionov@hneu.net)
Kharkiv National Economic University named after Semen Kuznets

The purpose of the research is to implement hybrid encryption methods to ensure the confidentiality, integrity and authenticity of transmitted data in blockchain networks. Modern cryptographic algorithms were analyzed, their advantages and disadvantages were identified, and a hybrid scheme was proposed that combines symmetric and asymmetric encryption. The object of the research is the process of data exchange between participants in the blockchain network. The subject of the research is cryptographic methods aimed at increasing the security of information transmission. An analysis of cryptographic risks was conducted, and typical vulnerabilities of data transmission in public blockchains were identified, in particular when exchanging keys and transmitting confidential information to or beyond the network consensus. The result of the research is the development of a solution for a secure data transmission channel using hybrid encryption, adapted to the characteristics of the blockchain environment.

Statement of the problem.

In modern information systems, issues related to ensuring cybersecurity are becoming key. With the growth of digital transactions, the popularity of decentralized applications, and the use of blockchain technologies in various areas (logistics, finance, healthcare, identification, etc.), the need for reliable methods of protecting transmitted information is also growing. Although the blockchain itself ensures the integrity and immutability of records in a distributed registry, it does not guarantee complete confidentiality and authenticity of transmitted data, especially in interaction channels between users or network nodes. Information transmission in blockchain environments often occurs without additional layers of encryption or using outdated algorithms. This creates 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 level. One of the promising directions for solving these problems is the implementation of hybrid encryption methods that combine the advantages of symmetric (high speed) and asymmetric (secure key exchange) cryptographic systems. This approach allows for both fast information encoding and secure exchange of key parameters, which is especially relevant in open or partially open blockchain networks.

The purpose of the research is to substantiate and develop a hybrid cryptographic scheme adapted for secure data transmission in blockchain networks. The object of the research is the process of transmitting digital data in decentralized computing systems. The subject of the research is symmetric and asymmetric encryption methods, their combined application in a distributed environment. The research methods used include theoretical analysis of cryptographic protocols, modeling of encryption processes, design of secure schemes, and experimental performance evaluation. The practical significance of the research is the combination of modern cryptographic approaches into one effective hybrid model that takes into account the peculiarities of the functioning of blockchain networks.

Presentation of the main material.

In the modern information space, blockchain technologies are actively implemented in various industries - from the financial sector and logistics to education, healthcare and public administration. The main advantage of blockchain is ensuring the integrity, transparency and immutability of information stored in a distributed registry. At the same time, despite the widespread opinion about the high level of security of decentralized systems, blockchain itself does not provide full protection of transmitted information, especially at the level of communication between network participants.

Threats inherent in classic computer networks remain relevant: Man-in-the-Middle (MITM) attacks, which allow for interference in data transmission between nodes; substitution of transactions or manipulation of content before they are included in a block; interception of private information during the process of creating, signing, or transmitting transactions; exploitation of weak or outdated cryptographic algorithms that do not meet modern standards.

In addition, blockchain networks often use public keys to identify users, while the corresponding private keys are stored locally. The loss or compromise of a private key leads to an irreversible loss of access or full control over the account, which confirms the need for additional layers of protection. The issue of confidentiality in blockchain environments requires special attention. For example, in financial applications or decentralized exchanges, transactions contain data on amounts, addresses of parties, hashes of contracts, etc. If such information is accessible to third parties, this can lead to a leak of commercial or personal information. A number of studies show that some blockchain applications (especially in the field of healthcare, digital identification, corporate document management) require not only preserving data integrity, but also ensuring their confidentiality. However, the standard mechanisms of most public blockchain platforms do not provide for this. While TLS or HTTPS level protocols provide channel protection in classical networks, in blockchain such protection must be implemented independently, at the application level or through specialized cryptographic schemes. One possible solution to increase the security of information transmission in such networks is the use of hybrid encryption. It allows you to encrypt the message content itself using symmetric algorithms (for example, AES), as well as perform secure key exchange using asymmetric algorithms (for example, ECC or RSA). This approach provides not only confidentiality and authenticity, but also increases efficiency in decentralized networks with a large number of participants.

Thus, despite the strengths of the blockchain architecture in ensuring the immutability and verifiability of information, vulnerabilities associated with the confidentiality and security of data transmission channels remain relevant. This creates the need to implement additional cryptographic tools - in particular, hybrid encryption methods, which allow for a comprehensive increase in the level of information security in blockchain networks. In the context of the rapid development of decentralized technologies, the need to assess not only the functional, but also the applied effectiveness of information protection tools is growing. For blockchain systems, where each transaction is public, and the network structure does not provide for centralized security elements, the ability of the selected cryptographic model to provide reliable protection of transmitted information without compromising performance, availability, and compatibility with existing protocols is extremely important.

In this regard, it is advisable to conduct a comprehensive analysis of the effectiveness of the hybrid encryption model, which was investigated in the previous sections, and to determine its advantages, limitations, and prospects for use in modern blockchain infrastructures.

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 the acceptable range even for interactive DApps or mobile applications. The hybrid model was compared with other methods used in cryptography (only symmetric or only asymmetric encryption), according to key parameters. These results confirm that the hybrid model provides the best balance between security and performance, especially in conditions where it is necessary to ensure secure key exchange and message integrity 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 (in particular, quantum threats).

Conclusions.

During the course work, a comprehensive study of hybrid encryption methods and their application to ensure information protection in blockchain environments was conducted. The aim of the work was to investigate the principles of construction and operation of hybrid cryptographic systems, analyze their advantages in comparison with traditional encryption methods, and also assess the feasibility and effectiveness of their integration into the blockchain technology infrastructure. 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, which is provided by asymmetric algorithms (for example, ECC). Such a combination allows you to achieve an optimal balance between performance and security in decentralized networks.

In the practical part, tools for implementing hybrid encryption were analyzed, in particular the PyCryptodome library, which demonstrated high functionality and compliance with modern information security requirements. Encryption, key exchange, message integrity verification scenarios were simulated, and algorithm performance analysis was conducted.

The results of the study demonstrated the high efficiency of the chosen cryptographic model: low latency during 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 transmission in Web3 systems, decentralized applications, and new generation digital ecosystems.

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.
4. Encryption. Types and algorithms [Electronic resource]. – Access mode: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.
5. Encryption: types and algorithms. What is it, how do they differ and where are they used [Electronic resource]. – Availability mode: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.
6. Comparison of symmetric and asymmetric encryption [Electronic resource]. – Access mode: https://exbase.io/uk/wiki/simetrichne-i-asimetrichne-shifruvannya.