APPLICATION OF HYBRID ENCRYPTION METHODS IN BLOCKCHAIN NETWORKS

Artem LAKTIONOV, master student
ORCID ID: 0009-0008-8161-6355
Semen Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine

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. 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of information in blockchain environments often takes place without additional layers of encryption or using outdated algorithms.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. 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 purpose of the study is to substantiate and develop a hybrid cryptographic scheme adapted for secure data transfer in blockchain networks. The research methods include such methods as theoretical analysis of cryptographic protocols, simulation of encryption processes, design of secure circuits, and experimental performance assessment. The practical significance of the study lies in combining modern cryptographic approaches into one effective hybrid model that takes into account the peculiarities of the functioning of blockchain networks.

In today's information space, blockchain technologies are being actively implemented in various industries, from the financial sector and logistics to education, healthcare, and public administration. The main advantage of blockchain is to ensure the integrity, transparency, and immutability of information stored on a distributed ledger. At the same time, contrary to the popular 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 classical computer networks remain relevant: Man-in-the-Middle (MITM) attacks, which allow interfering with the transmission of data between nodes; substitution of transactions or manipulation of content until they are included in the block; interception of private information in the process of creating, signing or transferring transactions; Exploitation of weak or outdated cryptography algorithms that do not meet modern standards. Additionally, blockchain networks often use public keys to identify users, while the corresponding private keys are stored locally. Loss or compromise of a private key results in an irreversible loss of access or full control of the account, confirming the need for additional layers of protection. The problem of privacy in blockchain environments requires special attention. A number of studies show that some blockchain applications (especially in the field of healthcare, digital identity, corporate document management) need not only to preserve the integrity of data, but also to ensure their confidentiality. However, the standard mechanisms of most public blockchain platforms do not provide for this. While TLS or HTTPS protocols provide channel protection in classic networks, in the blockchain such protection must be implemented independently, at the application level, or using specialized cryptographic schemes. One of the possible solutions to increase the security of information transmission in such networks is the use of hybrid encryption. It allows you to encrypt the content of the message itself using symmetric algorithms (AES), as well as secure key exchange using asymmetric algorithms (for example, ECC or RSA).

This approach not only ensures privacy 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 related to the confidentiality and security of data transmission channels remain relevant. This creates the need to introduce additional cryptographic tools, in particular, hybrid encryption methods, which make it possible to comprehensively increase the level of information security in blockchain networks. In the context of the rapid development of decentralized technologies, there is a growing need to assess not only the functional, but also the applied effectiveness of information security tools. For blockchain systems, where every transaction is public, and the structure of the network does not provide for centralized security elements, the ability of the chosen cryptographic model to provide reliable protection of the 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 studied in the previous sections, and 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 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).

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. 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. Encryption. Types and algorithms. – URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.