Laktionov Artem
student of higher education
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine
Supervisor: Candidate of Technical Sciences, Associate Professor
Skorin Yuriy

APPLICATION OF HYBRID ENCRYPTION METHODS IN BLOCKCHAIN NETWORKS OF THE FINANCIAL SECTOR

The purpose of the study 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 that combines symmetric and asymmetric encryption was proposed.

The object of the study is the process of data exchange between participants in the blockchain network.

The subject of the study is cryptographic methods aimed at improving the security of information transmission.

An analysis of cryptographic risks was carried out, typical vulnerabilities of data transmission in public blockchains were identified, in particular when exchanging keys and transferring confidential information to or outside the network consensus.

The result of the study is the development of a solution for a secure data transmission channel using hybrid encryption, which is adapted to the peculiarities of the blockchain environment.

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– exploitation of weak or outdated cryptography algorithms that do not meet modern standards.

In the course of the study, a comprehensive study of hybrid encryption methods and their application to ensure information protection in blockchain environments was conducted.

Based on the theoretical analysis, it was established that hybrid cryptography combines the strengths of both symmetric and asymmetric encryption methods: the high execution speed of symmetric algorithms (in particular, AES) and the secure key exchange ensured by asymmetric algorithms (such as ECC). This combination makes it possible to achieve an optimal balance between performance and security in decentralized network environments.

In the practical part, the implementation tools for hybrid encryption were analyzed, particularly the PyCryptodome library, which demonstrated high functionality and compliance with modern information security requirements. Scenarios involving encryption, key exchange, message integrity verification, and algorithm performance analysis were modeled.

The results of the study demonstrated the high efficiency of the chosen cryptographic model:
– low latency during encryption and decryption, as well as support for modern standards,
– scalability,
– protection against major types of attacks (including MITM and traffic analysis).

The comparative assessment also confirmed the advantages of the hybrid model over classical approaches.

Thus, the obtained results form the basis for developing practical solutions in the field of secure data transmission in Web3 systems, decentralized applications, and next-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/.