РЕФЕРАТ

Актуальність теми. В умовах стрімкого розвитку блокчейн-технологій та цифрових активів питання захищеного зберігання приватних ключів набуває особливої важливості. Приватний ключ – критичний елемент криптографічних механізмів автентифікації та цифрового підпису, а його компрометація може призвести до значних фінансових і репутаційних втрат. Традиційні методи зберігання, такі як апаратні гаманці чи централізовані сервіси, мають суттєві недоліки, включаючи ризики злому, втрати фізичних носіїв або компрометації серверів. У зв'язку з цим необхідні нові підходи, що забезпечать високий рівень безпеки та ефективності зберігання ключів, що є предметом даного дослідження.

Мета роботи. Основною метою дослідження є підвищення безпеки зберігання приватних ключів у блокчейн-мережах завдяки використанню способів, що поєднують криптографічні алгоритми, фрагментацію ключа, розподілене зберігання та паралельну обробку фрагментів для підвищення безпеки, продуктивності та стійкості до атак.

Об'єкт дослідження. Процеси зберігання, захисту та управління приватними ключами в блокчейн-системах.

Предмет дослідження. Способи підвищення безпеки та продуктивності при зберіганні приватних ключів на основі криптографічних алгоритмів, фрагментації та паралельної обробки.

Методи дослідження. У роботі використано математичні методи криптографії, алгоритми симетричного та асиметричного шифрування (AES та RSA), методи розподілених обчислень, моделювання ефективності алгоритмів, а також програмну реалізацію та тестування запропонованих методів.

Наукова новизна. У межах дослідження запропоновано три нові методи захищеного зберігання приватних ключів: метод фрагментації ключа, комбінований підхід AES + RSA та метод паралельної обробки шифрування. Запропоновані способи забезпечують підвищену безпеку за рахунок зменшення

ризиків компрометації ключів, а також підвищують продуктивність шляхом оптимізації процесів шифрування та дешифрування. Вперше проведено комплексний аналіз ефективності таких методів у контексті блокчейн-мереж.

Практична цінність. Запропоновані методи можуть бути застосовані у фінансових установах, криптовалютних біржах, децентралізованих додатках (DApps) та інших сферах, що потребують високого рівня безпеки при зберіганні криптографічних ключів. Метод фрагментації AES-256 скорочує час шифрування до 22 мс і розшифрування до 21 мс, комбінований AES+RSA забезпечує високу безпеку при 75 мс шифрування і 130 мс дешифрування, а паралельна обробка зменшує час до 31 мс і 56 мс відповідно, вона дозволяє зменшити затримки шифрування в реальних високонавантажених системах. Наведені показники роблять дані методи придатними для широкомасштабного впровадження.

Особистий внесок магістранта. Мною було проведено глибокий аналіз існуючих методів зберігання приватних ключів, розроблено та програмно реалізовано три нові методи підвищеної безпеки, виконано тестування на реальних даних та проведено порівняльний аналіз запропонованих рішень.

Апробація результатів дисертації. Основні результати дослідження були представлені на наукових конференціях та у статті, а також застосовані в експериментальних системах зберігання криптографічних ключів у блокчейн-інфраструктурі. Розроблені алгоритми пройшли тестування на ефективність та безпеку у різних умовах експлуатації.

Публікації. За результатами дослідження опубліковано наукові статті у фахових виданнях та матеріалах міжнародних конференцій.

Структура та обсяг роботи. Магістерська дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Основні розділи включають аналіз проблеми, опис розроблених методів, оцінку їх ефективності та перспективи подальших досліджень. Загальний обсяг роботи становить 102 сторінки, 51 рисунок, 8 таблиць і додатки.

Ключові слова: приватний ключ, блокчейн, криптографія, шифрування, фрагментація, AES, RSA, паралельна обробка, безпека даних, оптимізація.

ABSTRACT

Relevance of the topic. In the context of the rapid development of blockchain technologies and digital assets, the issue of secure private key storage has become particularly important. The private key is a critical component of cryptographic authentication and digital signature mechanisms, and its compromise can lead to significant financial and reputational losses. Traditional storage methods, such as hardware wallets or centralized services, have substantial drawbacks, including the risk of hacking, loss of physical devices, or server breaches. Therefore, new approaches are needed to ensure a high level of security and efficiency in key storage, which is the subject of this research.

Purpose of the study. The main goal of the study is to enhance the security of private key storage in blockchain networks by employing methods that combine cryptographic algorithms, key fragmentation, distributed storage, and parallel fragment processing to improve security, performance, and resilience to attacks.

Object of the study. The processes of storing, protecting, and managing private keys in blockchain systems.

Subject of the study. Methods for improving the security and performance of private key storage based on cryptographic algorithms, fragmentation, and parallel processing.

Research methods. The study utilizes mathematical methods of cryptography, symmetric and asymmetric encryption algorithms (AES and RSA), distributed computing techniques, algorithm efficiency modeling, and the software implementation and testing of the proposed methods.

Scientific novelty. This research proposes three new methods for securely storing private keys: the key fragmentation method, the combined AES + RSA approach, and the parallel encryption processing method. These methods enhance security by reducing the risk of key compromise and improve performance through optimized encryption and decryption processes. A comprehensive analysis of the

effectiveness of these methods in the context of blockchain networks has been conducted for the first time.

Practical value. The proposed methods can be applied in financial institutions, cryptocurrency exchanges, decentralized applications (DApps), and other areas that require a high level of cryptographic key security. The AES-256 fragmentation method reduces encryption time to 22 ms and decryption to 21 ms. The combined AES+RSA method ensures high security with 75 ms encryption and 130 ms decryption. Parallel processing reduces the time to 31 ms and 56 ms, respectively, which helps minimize encryption delays in real high-load systems. These results make the methods suitable for large-scale deployment.

Personal contribution of the master's student. I conducted a comprehensive analysis of existing private key storage methods, developed and implemented three new high-security methods, performed testing on real data, and carried out a comparative analysis of the proposed solutions.

Approval of dissertation results. The main results of the research were presented at scientific conferences and in a published article. They were also applied in experimental cryptographic key storage systems within blockchain infrastructure. The developed algorithms were tested for efficiency and security under various operating conditions.

Publications. The research results have been published in scientific professional journals and in the proceedings of international conferences.

Structure and volume of the work. The master's thesis consists of an introduction, four chapters, conclusions, a list of references, and appendices. The main chapters include a problem analysis, a description of the developed methods, their performance evaluation, and future research prospects. The total volume of the work is 102 pages, including 51 figures, 8 tables, and applications.

Keywords: private key, blockchain, cryptography, encryption, fragmentation, AES, RSA, parallel processing, data security, optimization.