УДК 004.056.55

І. О. Бондаренко
Є. В. Котелянець
А. С. Камінська

АСИМЕТРИЧНЕ ШИФРУВАННЯ В ТЕХНОЛОГІЯХ БЛОКЧЕЙНУ ТА КРИПТОВАЛЮТАХ ДЛЯ ЗАХИСТУ ТРАНЗАКЦІЙ І ГАМАНЦІВ

Вінницький національний технічний університет

Анотація

У роботі розглянуто застосування асиметричного шифрування в блокчейн-технологіях і криптовалютах як одного з ключових інструментів забезпечення безпеки транзакцій та захисту криптогаманців. Проаналізовано принцип дії асиметричної криптографії, зокрема, використання пар ключів (публічного та приватного), та їх роль у процесі цифрового підпису, верифікації транзакцій і захисту доступу до криптовалютних активів. Особливу увагу приділено алгоритмам RSA та ECDSA, що широко використовуються у сучасних криптовалютних системах. Визначено переваги та потенційні вразливості такого підходу в контексті децентралізованих мереж.

Ключові слова: блокчейн, криптовалюта, асиметричне шифрування, приватний ключ, публічний ключ, цифровий підпис, безпека транзакцій, криптогаманець.

Abstract

The paper examines the application of asymmetric encryption in blockchain technologies and cryptocurrencies as one of the key tools for ensuring transaction security and protecting cryptocurrency wallets. It analyzes the operating principles of asymmetric cryptography, particularly the use of key pairs (public and private), and their role in the process of digital signing, transaction verification, and safeguarding access to cryptocurrency assets. Special attention is given to the RSA and ECDSA algorithms, which are widely used in modern cryptocurrency systems. The advantages and potential vulnerabilities of this approach are identified in the context of decentralized networks.

Keywords: blockchain, cryptocurrency, asymmetric encryption, private key, public key, digital signature, transaction security, crypto wallet.

Вступ

Швидкий розвиток цифрових технологій та зростаюча популярність криптовалют спричинили підвищений інтерес до питань кібербезпеки та захисту даних у децентралізованих системах. Одним із базових елементів безпеки у блокчейні є асиметричне шифрування – метод криптографії, що забезпечує захист транзакцій і доступ до криптогаманців за допомогою пари ключів: публічного та приватного. Завдяки цьому механізму користувачі можуть підписувати транзакції, підтверджувати право власності на цифрові активи та запобігати несанкціонованому доступу до своїх коштів. У рамках даного дослідження розглядаються основні принципи функціонування асиметричної криптографії, її застосування в контексті блокчейн-технологій та криптовалют, а також потенційні ризики, що можуть виникати при неправильному зберіганні або компрометації ключів.

Результати дослідження

Сучасні блокчейн-системи базуються на децентралізованій архітектурі, де особливу увагу приділено безпеці обміну даними та автентифікації транзакцій. Асиметричне шифрування є ключовою технологією, що забезпечує безпеку децентралізованих систем, зокрема, блокчейну та криптовалют. На відміну від симетричних методів, воно дозволяє здійснювати захищений обмін даними без необхідності попереднього спільного секрету, що робить його ідеальним рішенням для цифрових транзакцій та управління криптогаманцями. Асиметрична криптографія в блокчейні базується на парі ключів: приватному та публічному. Приватний ключ використовується для створення цифрового

підпису транзакції та має бути відомий лише власнику. Публічний ключ, у свою чергу, відкрито поширюється і служить для перевірки справжності підпису. Наприклад, у Bitcoin для генерації ключів застосовується алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) на основі еліптичної кривої secp256k1, що забезпечує високу швидкість обробки транзакцій при мінімальному розмірі ключів (256 біт) [1]. Асиметричне шифрування в блокчейні реалізується через спеціалізовані криптографічні алгоритми, кожен з яких має унікальні властивості та сфери застосування. Алгоритм RSA (Rivest-Shamir-Adleman) базується на складності факторизації великих простих чисел: відкритий ключ є добутком двох простих чисел, а закритий обчислюється через функцію Ейлера [2]. Незважаючи на широке застосування в минулому, RSA рідко використовується в сучасних блокчейнах через великі розміри ключів (2048+ біт) та низьку швидкість роботи. Натомість він частіше використовується в корпоративних рішеннях, де важлива сумісність зі старими системами [3]. Серед недоліків варто виділити вразливість до квантових атак, зокрема, через алгоритм Шора [4]. Алгоритм ECDSA використовує математику еліптичних кривих, де публічний ключ – це точка на кривій, отримана множенням приватного ключа на базову точку G (secp256k1) [5]. До переваг ECDSA належать короткі ключі, що забезпечують безпеку, еквівалентну 3072-бітному RSA, та висока швидкість, яка робить цей алгоритм оптимальним для транзакцій у Bitcoin та Ethereum [5]. Водночас існують недоліки, пов'язані з безпекою: слабкі генератори випадкових чисел (RNG) можуть призвести до повторення nonce, що у свою чергу дозволяє зловмиснику вирахувати приватний ключ – прикладом є інцидент з Sony PS3 у 2010 році [6]. Крім того, ECDSA має обмежену стійкість до квантових обчислень [7]. Удосконаленням цього алгоритму є EdDSA (Edwards-curve Digital Signature Algorithm), який базується на кривих Едвардса, наприклад Curve25519, і використовується в криптовалютах Monero та Zcash [6]. EdDSA забезпечує вищу швидкість підпису, стійкість до timing-атак, а також не потребує випадкових nonce, що усуває відповідні ризики [7]. Крім того, підписи EdDSA компактніші: 64 байти проти 70–72 у ECDSA. У Monero цей алгоритм використовується для захисту анонімності транзакцій через механізм RingCT. Приватний ключ у Bitcoin – це випадкове 256-бітне число, що зберігається в гаманці користувача. Публічний ключ обчислюється за формулою [8]:

$$Q = k \cdot G \tag{1}$$

де Q – публічний ключ,

k – приватний ключ,

G – базова точка еліптичної кривої secp256k1.

Для створення адреси застосовується хешування публічного ключа: спочатку алгоритм SHA-256, потім RIPEMD-160. Отриманий хеш перетворюється у формат Base58Check для формування адреси – наприклад, 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa [8].

Повний процес виглядає так [9]:

приватний ключ → ECDSA → публічний ключ → SHA-256 → RIPEMD-160 → Base58Check → адреса

Цифровий підпис транзакцій здійснюється шляхом хешування даних транзакції (h = SHA-256(tx_data)), після чого генерується підпис (r, s) з використанням приватного ключа та випадкового nonce [8]. Мережеві вузли потім перевіряють підпис за допомогою публічного ключа відправника [9]. Якщо nonce повторюється, виникає загроза витоку приватного ключа, як це трапилось із Sony PS3 [8]. Для уникнення цієї проблеми EdDSA використовує детерміновані nonce. Захист криптогаманців забезпечується через кілька механізмів. HD-гаманці (Hierarchical Deterministic Wallets) згідно BIP-32/BIP-44 дозволяють генерувати ієрархію ключів з однієї seed-фрази (наприклад, 12 слів). Формула для генерації ключів [9]:

$$\mathrm{child}_{\mathrm{key}} = \mathrm{parent}_{\mathrm{key}} + \mathrm{index} \cdot \mathrm{G} \tag{2}$$

Інший підхід – мультипідпис (Multisig), коли для підтвердження транзакції потрібні підписи кількох приватних ключів (наприклад, 2 з 3). Це створює додатковий рівень захисту в разі компрометації одного з ключів.

Висновки

Асиметричне шифрування є невід'ємною складовою безпечного функціонування блокчейн-систем, забезпечуючи автентичність, цілісність і захист транзакцій. Застосування алгоритмів ECDSA та EdDSA дозволяє ефективно поєднувати високу швидкодію з компактністю ключів і підписів, що є критично важливим для масштабованості децентралізованих мереж.

Незважаючи на існуючі вразливості, зокрема, пов'язані з генерацією nonce та потенційними загрозами квантових обчислень розробка вдосконалених алгоритмів, зокрема, постквантових, а також механізмів мультипідпису та HD-гаманців відкриває перспективи подальшого підвищення рівня кіберстійкості блокчейну. Таким чином, розвиток асиметричної криптографії залишається ключовим чинником у забезпеченні безпеки цифрових фінансових екосистем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Алгоритми шифрування та захисту приватності в криптовалютах URL: https://itc.ua/ua/blogs/algorytmy-shyfruvannya-ta-zahystu-pryvatnosti-v-kryptovalyutah/ (дата звернення: 02.04.2025)
2. Асиметричне шифрування URL: https://shorturl.at/qmy3O (дата звернення: 05.04.2025)
3. What is asymmetric encryption? URL: https://www.ibm.com/think/topics/asymmetric-encryption (дата звернення: 05.04.2025)
4. Asymmetric cryptography URL: https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography (дата звернення 07.04.2025)
5. What Is Encryption? A Brief Overview URL: https://www.gemini.com/cryptopedia/what-is-encryption-blockchain-symmetric-asymmetric (дата звернення 07.04.2025)
6. Асиметричні алгоритми шифрування URL: https://shorturl.at/TydL3 (дата звернення 09.04.2025)
7. Symmetric VS Asymmetric Encryption in Cryptography URL: https://shorturl.at/ZfddB (дата звернення 11.04.2025)
8. Asymmetric Cryptography In Blockchains URL: https://hackernoon.com/asymmetric-cryptography-in-blockchains-d1a4c1654a71 (дата звернення 15.04.2025)
9. Applications of blockchain in ensuring the security and privacy of electronic health record systems URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7362828/ (дата звернення 15.04.2025)

Котелянець Євгеній В'ячеславович **–** студент групи 2КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: evgen.kotelyanecz@gmail.com

Камінська Анна Сергіївна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: akaanyaa@gmail.com

Науковий керівник: ***Бондаренко Ірина Олексіївна*** **–** асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: bondarenko.i@vntu.edu.ua

Kotelyanets Evgeniy V. – student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: evgen.kotelyanecz@gmail.com.

Kaminska Anna S. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: akaanyaa@gmail.com

Supervisor*:* ***Bondarenko Iryna O.*** **–** assistant of the Department of Management and Security of Information Systems Vinnytsia National Technical University, Vinnytsia, e-mail: bondarenko.i@vntu.edu.ua