УДК 519.7:004.75:336.7

В. В. Задорожний
О. А. Смалько

ПЕРСПЕКТИВНІ МАТЕМАТИЧНІ КОНЦЕПЦІЇ ТА ТЕХНОЛОГІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У КРИПТОБЛОКЧЕЙНАХ

Кам'янець-Подільський національний університет імені Івана Огієнка

Анотація

Описано важливі математичні концепції, що застосовуються у комплексних програмно-апаратних рішенях сучасної блокчейн-технології, проаналізовано їхню користь у задачах підтримки цілісності трансакцій, блоків, вузлів і метаданих.

Ключові слова: криптовалюта, криптоблокчейн, цілісність даних, незмінюваність блоків, автентичність метаданих, цифровий підпис

Abstract

The authors describe important mathematical concepts used in complex hardware and software solutions of modern blockchain technology, and analyze their usefulness in maintaining the integrity of transactions, blocks, nodes, and metadata.

Keywords: cryptocurrency, crypto blockchain, data integrity, immutability of blocks, metadata authenticity, digital signature

Постановка проблеми

За весь час існування криптовалют в їхніх платіжних системах постійно вдосконалюються підходи та відповідні інструменти, спрямовані на захист автентичності, цілісності, конфіденційності, а також на забезпечення їхньої стійкості і захищеності від різних атак. З метою надійного гарантування цілісності даних у криптовалютних блокчейнах втілюються деякі математичні концепції та технології, що витримали перевірку часом і є досить перспективними.

Мета даної публікації

Метою роботи є аналіз ефективних математичних підходів до забезпечення цілісності даних у криптовалютних блокчейнах, зокрема зосереджено увагу за методах захисту цілісності блоків, трансакцій і мережевих вузлів. Описано способи підтримки автентичності та незмінності важливих метаданих, що супроводжують усі трансакції.

Виклад основного матеріалу

Для забезпечення цілісності даних у блокчейні – розподіленому, децентралізованому реєстрі, що складається із сукупності послідовно зв'язаних блоків, дуже важливо дбати про цілісність усіх блоків і трансакцій. Цілісність блоків передбачає їхню незмінюваність. Це забезпечується криптографічними хеш-функціями, якими послуговуються для зв'язування блоків між собою – кожен блок містить хеш попереднього блоку, що забезпечує послідовність і незмінність блоків. Всі трансакції мають бути підтвердженими, вони не можуть дублюватись. Достовірність трансакцій підтверджується вузловими точками і забезпечується цифровими підписами, які свідчать про те, що трансакція походить від власника приватного ключа.

Для забезпечення цілісності трансакцій у блоці використовується хеш-дерево (або дерево Меркла), його листами є хеші кожної криптовалютної трансакції у блоці. Потім листи попарно хешуються, і над ними формується шар внутрішніх вузлів. Зі звуженням дерева догори у наступних шарах вузли розгалуження продовжують хешуватись по двоє. Врешті утворюється результат останнього

хешування, який називається коренем Меркла [1] – хеш всіх трансакцій у блоці. Він, як правило, зберігається у заголовку блоку, і з його допомогою можна швидко перевірити, чи є певна трансакція у блоці.

Довжина і структура блоку може варіюватися залежно від криптовалюти та конкретного блокчейну, але є загальні компоненти, які часто використовуються у блоках. Окрім кореня Меркла, обов'язковими компонентами блоку здебільшого є нонс і часова мітка. Нонс – це число, яке змінюється під час процесу майнінгу для того, щоб знайти підходящий хеш (який відповідає належним критеріям складності). Часова мітка – це час, коли блок було створено, ця компонента допомагає забезпечити хронологічний порядок блоків.

Для обчислення унікальних хеш-кодів фіксованої довжини для повідомлень з довільною довжиною застосовують найефективніші на наш час алгоритми безпечного хешування з сімейства SHA (Secure Hash Algorithm) [2]. Поширений у багатьох блокчейнах (включаючи Bitcoin) алгоритм SHA-256 бере за основу 32-бітні слова і забезпечує фіксований розмір хеша (256-біт) для будь-якого повідомлення У ньому використовується хеш-функція Меркла-Демґард. Більш досконалі хеш-процедури включають в себе варіанти хешування на основі алгоритму SHA-3 (Keccak), який працює за принципом криптографічної губки [3]. Хеш-код SHA може використовуватись для перевірки цілісності повідомлення, а також для створення цифрового підпису повідомлення.

При забезпеченні цілісності даних у криптоблокчейнах слід захищати незмінність та автентичність таких важливих метаданих, що супроводжують всі трансакції, як відомості про відправника і одержувача. Кожен учасник блокчейну має пару криптографічних ключів: приватний і публічний ключі. Приватний ключ відомий лише власнику і використовується для підписання трансакцій. Публічний ключ відомий іншим учасникам мережі і застосовується для перевірки підпису. Процес підписання трансакції виглядає нескладно: відправник створює трансакцію, яка містить інформацію про одержувача, суму переказу та інші необхідні дані. Відправник підписує трансакцію своїм приватним ключем. Цей підпис забезпечує автентичність і не дозволяє змінювати дані трансакції без виявлення. Потім відбувається процес перевірки трансакції: інші вузли мережі використовують публічний ключ відправника для перевірки підпису. Якщо підпис справжній, то трансакція вважається автентичною і додається до блоку.

Для підтвердження того, що трансакція утворюється власником відповідного приватного ключа, наразі використовуються алгоритми цифрових підписів, в основі яких лежить еліптична криптографія. Зокрема, найбільш поширеним у наш час є алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm), але подекуди застосовується й алгоритм EdDSA (Edwards-curve Digital Signature Algorithm), що забезпечує кращу швидкість і безпеку [4].

Фундаментальними елементами блокчейну є мережеві вузли (ноди), які зберігають копію всієї блокчейн-мережі, перевіряють трансакції/блоки та передають ці дані іншим вузловим точкам. Їхня цілісність крім вже згаданої вище криптографії забезпечується регулярними перевірками нових блоків і трансакції на відповідність правилам консенсусу, а також шляхом синхронізації, що забезпечує актуальність даних на всіх вузлах. Перевагою блокчейн-технології є її децентралізована природа, яка гарантує те, що жоден мережевий вузол не може самостійно змінювати дані без схвалення інших вузлових точок. Тому основою технології розподіленого реєстру є протокол консенсусу.

Існує багато різних консенсус-протоколів. Але найбільш поширеними у криптоблокчейнах є механізми підтвердження виконання поставленої роботи, що базуються на складності розв'язання криптографічної задачі, а також методи підтвердження розміру частки (різних модифікацій), які замість майнінгу спираються на розмір наявної у потенційних учасників формування чергових блоків блокчейну частки власності у токенах.

Висновки

Задача забезпечення цілісності даних у криптовалютних блокчейнах є дуже важливою. Але знаходячись на порозі ери квантових комп'ютерів, потрібно активізувати пошуки стійкіших алгоритмів захисту різних цифрових активів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Дерево Меркла та його роль у блокчейні. URL: https://learn.bybit.com/uk/blockchain/what-is-merkle-tree
2. Landman N., Williams C., Ross E. Khim J. Secure Hash Algorithms. URL: https://brilliant.org/wiki/secure-hashing-algorithms
3. Bertoni G., Daemen J., Peeters M., Assche G. Cryptographic sponge functions. URL: https://keccak.team/files/CSF-0.1.pdf
4. FIPS 186-5. Federal Information Processing Standards Publication. Digital Signature Standard (DSS). Gaithersburg: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.186-5

Задорожний Володимир Володимирович **—** здобувач магістерського рівня вищої освіти, фізико-математичний факультет, Кам'янець-Подільський національний університет імені Івана Огієнка, м. Кам'янець-Подільський, e-mail: kn1b18.zadorozhnyi@kpnu.edu.ua

Смалько Олена Аркадіївна **—** кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук, Кам'янець-Подільський національний університет імені Івана Огієнка, м. Кам'янець-Подільський, e-mail: smalko.olena@kpnu.edu.ua

Zadorozhnyi V. — Faculty of Physics and Mathematics, Kamianets-Podilskyi Ivan Ohiienko National University, Kamianets-Podilskyi

Smalko Olena A. — Candidate of Pedagogic Sciences, Docent, Associate Professor at the Department of Computer Science, Kamianets-Podilskyi Ivan Ohiienko National University, Kamianets-Podilskyi