УДК 004.056:004.6

БЛОКЧЕЙН ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ЦИФРОВОМУ СВІТІ

Поліщук В.Г.
Науковий керівник – к.т.н., доцент Куля Ю. Е.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +38(093) 648-49-05

This work is focused on the importance of security in blockchain technology, highlighting its decentralized nature and resistance to cyberattacks. The text explains the key concepts of consensus and immutability, which play crucial roles in ensuring data integrity and transaction reliability. Additionally, the role of cryptography, specifically hashing, is discussed as an essential element in maintaining the security of data within blockchain technology. The combination of these features contributes to the overall security and dependability of blockchain systems.

Безпека є одним з ключових аспектів технології блокчейн, оскільки вона забезпечує надійність системи і захист від можливих атак. Оскільки блокчейн мережа є розподіленою і децентралізованою, вона має покращену стійкість до кібератак та має високу надійність.

Блокчейни використовують різні механізми безпеки, такі як передові криптографічні методи, математичні моделі поведінки та прийняття рішень. Найважливішими функціями для забезпечення безпеки блокчейну є концепції консенсусу та незмінності. Консенсус забезпечує здатність вузлів у мережі узгоджувати справжній стан мережі та достовірність транзакцій, і його досягнення залежить від алгоритмів консенсусу. Незмінність дозволяє блокчейну уникнути змін у підтверджених транзакціях, що забезпечує цілісність даних та записаних транзакцій. Поєднання цих функцій є основою безпеки даних у блокчейні, яке забезпечує дотримання системних правил та узгодження всіх сторін з поточним станом мережі. Кожен новий блок перевіряється перед його додаванням до блокчейну, що забезпечує цілісність та безпеку даних у блокчейн технології [1].

Блокчейни в значній мірі покладаються на криптографію для забезпечення безпеки даних. Однією з надзвичайно важливих криптографічних функцій у цьому контексті є хешування. Хешування – це процес, при якому алгоритм, відомий як хеш-функція, отримує вхідні дані будь-якого розміру і повертає певний висновок, що містить значення фіксованої довжини.

Незалежно від розміру вхідних даних, вихід завжди має однакову довжину. Якщо вхід зміниться, результат буде зовсім іншим. Однак, якщо вхідні дані не змінюються, отриманий хеш завжди однаковий, незалежно від

того, як часто виконувалася хеш-функція. Наприклад, якшо алгоритмом SHA-256, який використовується у біткойні, захешувати дві майже однакові фрази змінивши тільки регістр першої літери, то в результаті буде отримано зовсім різні результати [2].

У блокчейнах хеші використовуються як унікальний ідентифікатор кожного блоку даних. Кожен блок містить хеш попереднього блоку, тому їх можна зв'язати в один ланцюжок. Крім того, хеш кожного блоку залежить від даних, що містяться в цьому блоку, що означає, що будь-яка зміна даних у блоку призведе до зміни його хешу. Таким чином, хеш-ідентифікатори кожного блоку базуються на даних, які він містить, та хеші попередніх блоків, що дозволяє забезпечити надійність та незмінність всього блокчейну [3].

Окрім захисту та запису транзакцій у регістри, криптографія також відіграє роль у захисті гаманців, що використовуються для зберігання криптовалют. Відкритий та приватний парні ключі, що дозволяють користувачам отримувати та надсилати платежі, створюються за допомогою асиметричного шифрування. Відкриті ключі використовуються для генерації цифрових підписів транзакцій, що дозволяє аутентифікувати право власності. Природа асиметричної криптографії не дозволяє нікому, крім власника приватного ключа, отримати доступ до коштів, що зберігаються в гаманці, тому ці кошти зберігаються в безпеці, доки власник не вирішить їх витратити.

Отже, блокчейн технології мають потенціал вирішувати проблеми безпеки в цифрових транзакціях та забезпечувати високий рівень захисту даних. Завдяки своїй децентралізованій структурі та криптографічним методам захисту, блокчейн може захистити транзакції від змін та фальсифікації даних.

Список використаних джерел:

1. Ensuring data security in the blockchain: principles and techniques https://medium.com/coinmonks/data-security-in-blockchain-principles-and-techniques-dc51e5b5c5a5
2. Cryptography in blockchain technology: how it works https://www.coindesk.com/learn/what-is-cryptography
3. Hashing in Blockchain: Basics and Application Examples https://www.toptal.com/bitcoin/what-is-hash-function