УДК 621.382

МЕТОДИ ЗАХИСТУ ВІД АТАК НА ОДНОРАНГОВІ БЛОКЧЕЙН МЕРЕЖІ БІТКОІНА

Валуйський С.В., Кравчук І.В.
Навчально-науковий інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: ilyukha.kravchuk@gmail.com

METHODS OF PROTECTION AGAINST ATTACKS ON PEER-TO-PEER BLOCKCHAIN NETWORKS OF BITCOIN

This work is focused on researching and developing methods to protect against attacks on the peer-to-peer blockchain network of Bitcoin. This will involve analyzing various types of attacks and developing and implementing new security methods, such as multisignatures, confidential transactions, enhanced authentication, and smart contracts.

Біткоїн був запропонований у 2008 році під псевдонімом Сатоші Накамото через документ, опублікований на криптографічному форумі. У січні 2009 року відбулася перша транзакція біткоїну між Накамото та розробником Галеном Філдсом. Біткоїн став першою криптовалютою, яка використовує технологію блокчейн для забезпечення децентралізованого обміну валюти. З 2010 року біткоїн став предметом значного інтересу як серед технологічно орієнтованих груп, так і серед інвесторів.

Біткоїн має однорангову блокчейн мережу, де кожен вузол має однакові права та можливості. Кожен вузол може виступати як клієнт, що ініціює транзакції, так і сервер, що обробляє та передає їх. Мережа функціонує без централізованого органу контролю чи управління, кожен вузол має копію блокчейну, що містить історію всіх транзакцій.

Ключовим елементом мережі є процес майнінгу, де спеціалізовані комп'ютери (майнери) розв'язують складні математичні завдання для підтвердження та обробки транзакцій. Цей процес забезпечує безпеку та надійність мережі, додаючи нові блоки з транзакціями до блокчейну. Однорангова структура мережі дозволяє біткоїну працювати без централізованої влади чи контролю, забезпечуючи при цьому високий рівень безпеки та анонімності. Кожен учасник мережі може бачити та перевіряти всі транзакції, забезпечуючи прозорість та відкритість системи.

Мета роботи. Основна мета роботи полягає в дослідженні методів захисту від атак на однорангові блокчейн мережі біткоїна. Для цього використовуються аналіз різних видів атак, таких як повторна витрата, атака 51%, форкінг та селфіш-майнінг, а також розробка та аналіз ефективних методів захисту від них.

Огляд методів захисту від атак на однорангові блокчейні мереж [1-4].

Multisig. Використання мультипідписів дозволяє створювати адреси, які потребують авторизації від кількох підписників для здійснення транзакції. Це

підвищує безпеку та зменшує ризик втрати коштів внаслідок несанкціонованих транзакцій.

Confidential Transactions. Використання криптографічних протоколів, які дозволяють захистити конфіденційність суми транзакцій, забезпечуючи при цьому можливість перевірки їх валідності (рис.1).

Рис.1. Приклад роботи Confidential Transactions.

Enhanced Authentication Schemes. Розробка та впровадження методів аутентифікації, які базуються на більш складних криптографічних протоколах, що ускладнюють спроби підробки транзакцій (рис.2).

Рис.2. Приклад Enhanced Authentication Schemes (біометричної аутентифікації).

Smart Contracts. Розробка смарт-контрактів для автоматизації та забезпечення безпеки операцій, що відбуваються в мережі біткоїна, таких як умовні операції або розподіл коштів в залежності від виконання певних умов.

Взаємодія між відправником та отримувачем полягає в обміні зашифрованими даними та доказами через спеціальний протокол обміну. Цей протокол дозволяє їм здійснювати конфіденційну транзакцію, зберігаючи приватність сум, які не розкриваються сторонами під час процесу обміну.

Біометрична аутентифікація для користувача біткоїна включає сканування відбитка пальця, його аналіз для визначення унікальних характеристик, порівняння з зразком у системі і, в разі підтвердження відповідності, надання доступу до біткоїн-гаманця або функціоналу.

Smart Contracts спочатку створюються, після чого визначаються їх умови, включаючи параметри та обмеження (рис.3). Умови зберігаються, і потім виконуються, перевіряючи їх на виконання та виконуючи відповідні дії в залежності від результатів.

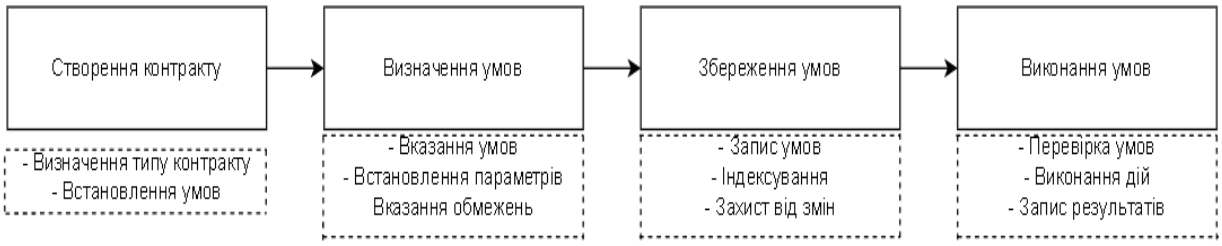

Рис.3. Smart Contracts

Висновок. Робота спрямована на розробку та аналіз ефективних методів захисту від цих атак. Досліджуючи методи захисту, розглянуто такі методи, як Multisig, Confidential Transactions, Enhanced Authentication Schemes та Smart Contracts. Multisig дозволяє створювати адреси, які потребують авторизації від кількох підписників для здійснення транзакцій, підвищуючи при цьому безпеку. Confidential Transactions забезпечують захист конфіденційності сум транзакцій, а Enhanced Authentication Schemes ускладнюють спроби підробки транзакцій за допомогою складних криптографічних протоколів. Smart Contracts автоматизують та забезпечують безпеку операцій, що відбуваються в мережі біткоїна, виконуючи умовні операції згідно з певними параметрами.

Література

1. Bitcoin’s Blockchain Peer-to-Peer Network Security Attacks and Countermeasures / Mahmoud Mostafa. INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY, february 2020, Vol 13(07), 767 – 786. URL: https://doi.org/10.17485/ijst/2020/v13i07/149691.
2. Refund Attacks on Bitcoin’s Payment Protocol / McCorry Patrick, Shahandashti Siamak F. Financial Cryptography and Data Security, 22-26 Feb 2016. URL: https://doi.org/10.1007/978-3-662-54970-4_34.
3. Formal Modelling and Security Analysis of Bitcoin's Payment Protocol / Paolo Modesti, Siamak F. Shahandashti, Patrick McCorry, Feng Hao. Computers & Security, Volume 107, 2021, 102279, ISSN 0167-4048, URL: https://doi.org/10.1016/j.cose.2021.102279.
4. An enhanced authentication scheme for Internet of Things and cloud based on elliptic curve cryptography / Pallavi Bhuarya, Preeti Chandrakar, Rifaqat Ali, Aakanksha Sharaff. Communication systems, Volume 34, Issue 10, 10 July 2021. URL: https://doi.org/10.1002/dac.4834.