ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ “ІННОВАЦІЙНІ ПІДХОДИ ДО РОЗВИТКУ ТЕХНОЛОГІЙ ТА ЕКОНОМІКИ”

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Innovation and science

ЗАКАРПАТСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗУНУ

Свалява - 2025

ЗМІСТ

БЕЗПЕКА БЛОКЧЕЙНУ: ПОТЕНЦІАЛ І РИЗИКИ

Хома Надія Григорівна,
кандидат фізико-математичних наук, доцент, доцент кафедри економічної кібернетики та інформатики,
Західноукраїнський національний університет,
khoma.nadiya@gmail.com,
Цинайко Софія Петрівна,
ФБСт-21,
ВСП «ФКЕПІТ» Західноукраїнського національного університету,
stsynaiko@gmail.com

Безпека блокчейну є одним із ключових факторів його популярності у сучасному цифровому світі. Завдяки своїм технічним особливостям, ця технологія може значно покращити захист даних і систем. Як саме блокчейн може забезпечити безпеку?

Передусім, блокчейн дозволяє ефективно запобігати шахрайству завдяки процесу верифікації та підтвердження транзакцій перед їх додаванням до мережі. Це гарантує, що в систему потрапляють лише законні операції. Ще однією важливою перевагою є шифрування особистих даних та їх зберігання в децентралізованій формі, що суттєво ускладнює доступ до цієї інформації стороннім особам.

Технологія блокчейн [1] також забезпечує високий рівень прозорості, адже всі транзакції зберігаються в незмінному вигляді, відкритому для перегляду всім учасникам мережі. Додатковим елементом безпеки є захист від кібератак за допомогою сучасних методів шифрування, що ускладнює несанкціонований доступ або зміну даних.

Ще одна важлива сфера використання блокчейну – це забезпечення надійних і захищених транзакцій [2]. Завдяки обов'язковому процесу верифікацій перед кожною операцією, виключається можливість фальсифікації або підробки. Аналогічним чином підвищується безпека у логістиці – зберігання детального ланцюга постачань у блокчейн дозволяє всім учасникам мати однакову інформацію, що сприяє відповідальності та відкритості.

Попри високий рівень безпеки, блокчейн не є абсолютно захищеним від ризиків. Як і будь-яка новітня технологія, він створює нові виклики. Одним із таких викликів є атака 51%, за якої одна особа чи група отримує контроль над більш ніж половиною обчислювальної потужності мережі. Це відкриває можливість маніпулювати транзакціями, дублювати витрати та блокувати участь інших користувачів. Особливо небезпечно це в публічних блокчейнах, відкритих для широкого загалу.

Ще одним уразливим аспектом залишаються смарт-контракти. Хоча вони й дозволяють автоматизувати багато бізнес процесів, неправильно написаний код може мати серйозні наслідки. Зловмисники здатні використовувати

вразливості для викрадення коштів або роботи мережі. Додаткові загрози походять від соціальної інженерії [3,4] – методів, спрямованих на обман користувачів із метою отримання доступу до їхніх даних. Найпоширенішими сере них є фішингові атаки [3,4], під час яких створюються підроблені сайти, що імітують офіційні, з метою викрасти облікові дані.

Значну небезпеку становлять також атаки на криптовалютні біржі. Вони стають мішенню для хакерів, що прагнуть отримати доступ до користувацьких коштів, завдаючи не лише фінансових втрат, а й шкоди репутації таких платформ. Окрема загроза – це майнинг-ботнети: мережі заражених комп'ютерів, що використовуються для незаконного майнінгу без відома їхніх власників. До цього додається ще й проблема подвійних витрат, коли одна й та сама сума криптовалюти використовується двічі, що підриває стабільність усієї системи.

Попри це. Існують ефективні підходи до зменшення ризиків. Захист від атаки 51% передбачає підтримку децентралізації та впровадження таких механізмів консенсусу, як Proof-of-Work або Proof-of-Stake, що сприяють рівномірному розподілу потужностей. Для безпеки смарт-контрактів важливими є правильне програмування, ретельний аудит та використання автоматизованих інструментів для виявлення вразливостей.

Щодо соціальної інженерії, то ключову роль відіграє навчання користувачів: як розпізнати фішинг, захищати свої гаманці, використовувати двофактурну автентифікацію та апаратні рішення. Біржам варто інвестувати в системи моніторингу та зберігати більшість коштів у холодних гаманцях. Аби уникнути захоплення ботнетами, потрібно регулярно оновлювати захисне програмне забезпечення та слідкувати за аномальною активністю на пристроях. Щодо подвійних витрат, то ефективним методом впровадження надійних консенсусних механізмів і постіqне відстеження транзакцій у мережі.

Блокчейн уже давно вийшов за межі криптовалют і дедалі частіше використовується як інструмент для підвищення безпеки в різних сферах. Ось кілька прикладів із реального світу, які демонструють, як блокчейн-технології застосовуються:

1. У фінансовому секторі платформа Ripple використовує блокчейн для забезпечення миттєвих міжнародних переказів із підтвердженням транзакцій у режимі реального часу. Це не лише підвищує швидкість обробки, а й запобігає спробам подвійної витрати коштів.

2. Великий гігант Walmart застосовує блокчейн для відстеження походження продуктів харчування в ланцюзі постачань. Завдяки цьому вдається оперативно виявити джерело зараження у разі харчових інцидентів.

3. У сфері охорони здоров'я компанія Medicalchain впровадила блокчейн для захисту медичних даних пацієнтів. Дані зберігаються децентралізовано та доступні лише за згодою пацієнта, що виключає несанкціонований доступ і знижує ризик витоку конфіденційної інформації.

4.У 2020 році біржа KuCoin зазнала атаки, в результаті якої було вкрадено понад $280 млн у криптовалютах. Хоча частину коштів вдалося повернути, цей інцидент показав вразливість централізованих платформ і важливість холодного зберігання активів.

5. Ethereum став класичним прикладом використання смарт-контрактів у реальному світі. Однак у 2016 році через помилку в коді The DAO (децентралізованої автономної організації) було втрачено близько $60 млн. Цей випадок підкреслює важливість аудитів та якісної розробки контрактів.

6. Зловмисники також активно створюють фішингові сайти, які імітують популярні криптогаманці, як-от MetaMask. Користувачі, які неуважно вводять свої приватні ключі, втрачають доступ до активів. Це ілюструє, наскільки критичним є навчання користувачів основам безпеки.

7. У деяких випадках хакери створювали майнінг-ботнети, як-от відомий Smominru, який у 2017 році заразив сотні тисяч комп'ютерів по всьому світі для прихованого майнінгу Monero. Це підкреслює необхідність постійного оновлення захисного програмного забезпечення.

Список використаних джерел:

1. Що таке блокчейн і як він працює? URL: https://academy.binance.com/uk-UA/articles/what-is-blockchain-and-how-does-it-work

2. Volodymyr Muravskyi, Nadiia Khoma, Larysa Khokhlova, Liu Chengyu. Open document flow based on blockchane technology for cyber security of the accounting system. *Вісник економіки*. 2021. № 4. С. 156-170. DOI: 10.35774/visnyk2021.04.156

3. Хома Н. Г., Цинайко В. П. Безпека в інформаційному просторі. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення* (випуск 94): *матеріали Міжнародної наукової інтернет-конференції,* (м. Тернопіль, Україна, м. Ополе, Польща, 11-12 грудня 2024 р.). С. 84-86. URL:http://www.konferenciaonline.org.ua/ua/article/id-1999 http://dspace.wunu.edu.ua/handle/316497/54492

4. Хома Н. Г., Цинайко В. П. Безпека в інформаційному просторі. *Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи: матеріали XV Міжнародної науково-практичної інтернет-конференції, м. Тернопіль, 10 квітня, 2025 р.* Тернопіль: ТНПУ ім. В. Гнатюка, 2025. С.239-242. http://dspace.wunu.edu.ua/handle/316497/54495