АНАЛІЗ МЕТОДІВ ЗАХИЩЕНОСТІ У БЛОКЧЕЙН СИСТЕМАХ

Назаренко Д.М.

Харківський Національний Університет
Радіоелектроніки,
Україна.

E-mail: dmytro.nazarenko1@nure.ua

Abstract

Blockchains are secured using various mechanisms, including advanced cryptographic methods and mathematical models of behavior and decision-making. Blockchain technology is the basic structure of most cryptocurrency systems and prevents the duplication or destruction of such digital money. Security in blockchain systems is a key concern because these systems store a large amount of important information and carry out transactions between users without an intermediary. Various aspects of security are explored, such as cryptographic techniques, decentralized consensus mechanisms, smart contracts, and the latest solutions to protect against attacks and tampering.

Інтернет за останні роки розрісся до небачених масштабів. Напевно на Землі вже майже немає людей, що так чи інакше не взаємодіють з ним. У зв'язку з цим постала проблема правдивості даних, оскільки в інтернеті тепер може бути написано що завгодно. І для того, щоб виправити цю проблему, був вигаданий блокчейн. Ця технологія з'явилась у далекому 2008 році, розроблена Сатоші Накаморою, хоча досі невідомо, був він окремою людиною, чи командою професіоналів[1].

Актуальність блокчейну на цей час є незаперечною, на фоні нинішнього розвитку криптовалют. Звісно, технологія не стоїть на місці, її покращують, на її покращених версій роблять різноманітні криптовалюти, які дорожчають. А сама ціна таких грошей і показує, що технологія є потрібною для звичайного користувача.

Блокчейн (Blockchain) - це розподілена база даних, яка забезпечує безпеку, надійність і невідмінність інформації. Ця технологія виникла як основа для криптовалют, зокрема для Bitcoin, але зараз.

Актуальність захисту блокчейн систем залишається вельми високою через ряд причин:

1. Криптографічна безпека. Блокчейн використовує криптографію для захисту даних. Це включає в себе публічний та приватний ключі, хеш-функції та електронні підписи. Розвиток квантових комп'ютерів вимагає постійного вдосконалення криптографічних методів для захисту від нових загроз.

2. Захист від атак. Через свою децентралізовану природу, блокчейн має менше вразливостей до традиційних видів кібератак, але існують загрози, які можуть бути уникнуті за допомогою вдосконалення технічних засобів безпеки та алгоритмів консенсусу.

3. Соціальна інженерія. Користувачі блокчейн систем можуть стати жертвами соціальної інженерії, яка використовує маніпуляцію та обман для здобуття доступу до конфіденційної інформації.

4. Забезпечення конфіденційності: У багатьох випадках, конфіденційність даних у блокчейні є обмеженою. Технології, такі як нуль-знання докази та обфускація даних, допомагають збільшити рівень конфіденційності в блокчейн системах.

5. Оновлення протоколів: Розвиток технологій і виявлення нових загроз вимагають постійного оновлення протоколів блокчейн систем для забезпечення захисту від сучасних атак.

6. Регулятивні стандарти: Зміни в законодавстві та введення регулятивних стандартів можуть вплинути на вимоги до захисту блокчейн систем та змусити їх вдосконалювати свої методи захисту.

Багаторічний розвиток технології відкрив перед нами нові перспективи. Ця еволюція призвела до різноманітності типів блокчейну. Різні типи блокчейну приведені в табл.1 [2]. Вони різняться за структурою, механізмом консенсусу та доступністю. Ці відмінності зумовлюють унікальні застосування і потенціал для бізнесу та суспільства.

Таблиця 1. Типи блокчейну

Тип блокчейну	Опис	Приклади
Публічний блокчейн	Відкритий для всіх, доступний для будь-кого. Підходить для публічних мереж і криптовалют.	Bitcoin, Ethereum
Приватний блокчейн	Закрита мережа для авторизованих учасників. Забезпечує високий рівень конфіденційності.	Hyperledger Fabric
Консорціумний блокчейн	Гібрид між публічним і приватним блокчейнами, використовується кількома організаціями для консенсусу.	R3 Corda, Quorum
Блокчейн з дозволеним доступом	Обмежений доступ лише для авторизованих учасників. Забезпечує конфіденційність.	Hyperledger Besu
Гібридний блокчейн	Поєднує публічні та приватні характеристики для різних використань.	Dragonchain, QuarkChain

Однією з основних проблем, пов'язаних із безпекою блокчейну, є атака 51%. В атаці 51% одна особа або група осіб контролює понад 50% обчислювальної потужності мережі. Це дає їм можливість маніпулювати транзакціями та контролювати блокчейн. Атакуючий може скасувати транзакції, двічі витратити монети та заважати іншим користувачам брати участь у мережі [3]. Такий тип атаки особливо небезпечний у публічних блокчейнах, куди може приєднатися хто завгодно.

Іншою проблемою, пов'язаною з безпекою блокчейну, є вразливості смарт-контрактів. Смарт-контракти – це самоздійснювані договори, в яких умови угоди між покупцем і продавцем записуються безпосередньо в коді. Смарт-контракти використовуються для автоматизації різних бізнес-процесів, таких як платежі, страхові претензії та управління ланцюгами поставок. Однак, якщо ці контракти не написані правильно, вони можуть бути вразливими для атак. Зловмисники можуть використовувати ці вразливості, щоб вкрасти кошти або порушити роботу мережі.

Крім вищезазначених аспектів, сфера безпеки блокчейну також схильна до низки інших викликів. Тактики соціальної інженерії використовують шахраї для обману користувачів і отримання їхньої особистої інформації або доступу до їхніх криптовалютних гаманців. Ці тактики можуть включати фішингові електронні листи, фальшиві дзвінки служби підтримки та інші методи, спрямовані на обман користувачів і виявлення конфіденційної інформації.

Фішингові атаки – поширені методи шахраїв, спрямовані на отримання доступу до особистої інформації користувачів, включно з обліковими даними та приватними ключами. Такі атаки зазвичай включають у себе створення підроблених веб-сайтів, що імітують офіційні, з метою підлаштувати користувачів до розкриття своїх конфіденційних даних. Після того як шахраї отримують доступ до цієї інформації, вони можуть не тільки вкрасти криптовалюту з гаманців користувачів, а й спричинити серйозні загрози та порушення у сфері блокчейн-безпеки.

Зломи бірж. Криптовалютні біржі – це онлайн-платформи, на яких користувачі можуть купувати, продавати та зберігати криптовалюту. Однак ці біржі часто піддаються атакам хакерів, які

намагаються отримати доступ до коштів користувачів. Атаки на біржі можуть призвести до втрати великих сум криптовалюти та завдати шкоди репутації постраждалої біржі.

Майнінг-ботнети – це мережі комп'ютерів, які були захоплені зловмисниками та використовуються для майнінгу криптовалюти без відома їхніх власників. Ці ботнети можуть використовуватися для видобутку великих обсягів криптовалюти за рахунок користувачів, чиї комп'ютери були скомпрометовані.

Подвійні витрати. Під час цієї атаки, користувач відправляє одні й ті самі кошти двічі, щоб отримати більше криптовалюти, що може призвести до порушення безпеки мережі. Ця атака може бути особливо руйнівною в публічних блокчейнах, де громадськість може вільно приєднатися до мережі та брати участь у консенсусі.

У наш час є методи захисту, які використовуються в блокчейн системах:

1. Криптографія. Блокчейн використовує криптографічні методи, такі як шифрування та цифровий підпис, для захисту даних під час зберігання і передачі.

2. Децентралізація: Блокчейн розподілений між безліччю комп'ютерів (вузлів), що робить його менш вразливим перед атаками, такими як DDoS (розподілений запит на послуги).

3. Контроль доступу: Системи блокчейн можуть використовувати методи контролю доступу, щоб забезпечити, що лише авторизовані користувачі можуть здійснювати транзакції чи вносити зміни до системи.

4. Спрощена верифікація: Деякі блокчейн системи, такі як Bitcoin, використовують консенсус-протоколи, такі як Proof of Work (доказ роботи), для важливих рішень. Ці протоколи вимагають великої обчислювальної потужності для зміни блоків у ланцюгу, що робить атаки 51% менш ймовірними.

5. Смарт-контракти: Смарт-контракти - це програми, які автоматизують виконання угод на основі умов, зазначених у контракті. Вони допомагають уникнути шахрайства та забезпечують автоматизовану виконавчу логіку.

6. Невідомість: В більшості публічних блокчейнів, таких як Bitcoin та Ethereum, користувачі можуть залишати анонімні транзакції, що робить їх важко відстежуваними.

7. Резервне копіювання та відновлення даних: Бекапи та можливість відновлення даних допомагають уникнути втрати інформації в разі втрати доступу до блокчейн системи.

8. Мережева безпека: Забезпечення безпеки мережі та захист від різних видів атак, наприклад, атаки Sybil, дуже важливо для безпеки блокчейн систем.

9. Регулювання та внутрішні політики: Встановлення відповідних нормативів та політик безпеки може допомогти уникнути вразливостей та забезпечити ефективний захист.

Одним із способів підвищення захисту блокчейн систем є постійне навчання та освіта користувачів, а також впровадження нових технічних рішень, щоб протистояти сучасним кіберзагрозам. Важливо також співпрацювати з експертами з кібербезпеки та дотримуватися найкращих практик у галузі безпеки даних. Важливо зазначити, що жоден метод захисту не є абсолютно непроникним, і захищеність блокчейн системи залежить від комбінації різних заходів безпеки та відповідних практик користувачів.

*Л*ітература

1. Huckle S. Internet of Things, Blockchain and Shared Economy Applications / S. Huckle, R. Bhattacharya, M. White, N. Beloff // Procedia Comput. Science. – Oct. 2016. – Vol. 98. – P. 461–466.

2. Baran P. On distributed communications: I. Introduction to distributed communications networks [Електроний ресурс] / Paul Baran. – Aug. 1964. – Режим доступу:https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf

3. Ghassan O.Karame, Elli Androulaki. Double-spending attacks on fast payments in Bitcoin. 2012. [Електроний ресурс] Режим доступу:https://eprint.iacr.ord/2012/248.pdf.