Триснюк В.М., д.т.н., с.н.с.,
Інститут телекомунікацій і глобального інформаційного простору,
Сметанін К.В., к.т.н., ст. викладач
Житомирський військовий інститут ім. С.П. Корольова

ВЕКТОРИ АТАК НА БЛОКЧЕЙН: ВРАЗЛИВОСТІ НАЙБЕЗПЕЧНІШИХ ТЕХНОЛОГІЙ

Блокчейн насправді не такий безпечний, як ми думаємо. Хоча безпека інтегрована в усі блокчейн-технології, навіть найнадійніші блокчейни піддаються атакам сучасних кіберзлочинців. Експерти Apriorit вже проаналізували атаки на Coincheck, Verge і біржу Bancor, які сильно підірвали репутацію самого блокчейна.

Блокчейни можуть досить добре протистояти традиційним кібератакам, але кіберзлочинці винаходять нові підходи спеціально для злому технології блокчейнів. У цій статті ми описуємо основні вектори атак на технологію блокчейн і розглянемо найбільш значні атаки на блокчейн на сьогоднішній день.

Блокчейн – це розподілена база даних, яка забезпечує безпеку та надійність шляхом зберігання та передачі інформації між користувачами за допомогою криптографії [1]. Однак, як і будь-яка інша технологія, блокчейн також має свої вразливості.

Одна з найбільш поширених атак на блокчейн – це атака 51%. Ця атака полягає в тому, що хакер (або група хакерів) здійснює контроль над більшістю обчислювальної потужності мережі блокчейн, що дає можливість їм змінювати блоки та транзакції в мережі [2]. Якщо хакер здобуде контроль над більшістю обчислювальної потужності мережі, то він зможе здійснювати такі дії, як перевід коштів з одного рахунку на інший, змінювати кількість коштів у транзакціях та навіть виконувати подвійні витрати.

Іншою поширеною атакою є атака Sybil. У цій атаці хакер створює велику кількість вузлів (або ідентичних копій) в мережі блокчейн, що дає йому контроль над мережею. Ця атака дуже небезпечна, оскільки вона дозволяє хакеру впливати на процес прийняття рішень в мережі, змінювати дані та транзакції, впливати на кількість голосів при прийнятті рішень у голосуванні та т.д.

Ще одна уразливість блокчейн – це smart contract (розумні контракти). Ці контракти – це програми, що автоматизують процес виконання договору та виконуються на блокчейн [3]. Однак, ці контракти можуть бути уразливі до атак, якщо вони не написані належним чином. Якщо хакер знайде уразливість у розумному контракті, то він може використати цю уразливість для виконання зловживань, таких як витрати коштів зі смарт-контракту, зміна його поведінки або навіть знищення контракту.

Також існує ризик використання блокчейн для злочинних цілей, таких як відмивання грошей, фінансування тероризму та інші види фінансової злочинності. Блокчейн може допомогти у протидії таким злочинам, але він не може повністю запобігти їм.

Нарешті, існує ризик людської помилки та необережності при використанні блокчейн, таких як неправильне збереження приватного ключа, який забезпечує доступ до гаманця з крипто валютою. Якщо приватний ключ буде втрачений або скомпрометований, то хакер може отримати доступ до коштів, збережених на гаманці.

Отже, блокчейн має свої уразливості, які можуть бути використані для злочинних цілей. Щоб уникнути таких ризиків, важливо забезпечити належну безпеку та криптографію, використовувати належні практики управління ризиками та надійність смарт-контрактів, а також дотримуватись належних стандартів безпеки використання блокчейн.

Список використаних джерел

1. Кравченко П. Блокчейн і децентралізовані системи : навч. Посібник для студ. закладів вищ. освіти : в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. — Харків : ПРОМАРТ, 2019. — 452 с.
2. Cost of a 51% Attack for Different Cryptocurrencies. – URL: https://www.crypto51.app.
3. CrosbyM. Blockchain Technology/ Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. // Berkeley Education, Sutardja Center for Entrepreneurship & Technology Technical