Загрози в мережі Blockchain

Дмитро Фесенко[1], Володимир Караваєв[2]

1. Кафедра безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки,
УКРАЇНА, г. Харків, пр. Науки, 14,
E-mail: dmytro.fesenko@nure.ua

2. Кафедра безпеки інформаційних технологій,
Харківський національний університет радіоелектроніки,
УКРАЇНА, г. Харків, пр. Науки, 14,
E-mail: volodymyr.karavaiev@nure.ua

Коротка анотація – Blockchain is a digital system that is based on model without a central storage. To design the system according to the requirements of blockchain, developers must take to attention rules on using such kind of system. The only system's thread itself that will be implemented on the blockchain during development, will make your system much less robust, so to create a really good-secured system developers should understand all threads in blockchain and to be possible to persist them.

Ключові слова – Blockchain, Атака, Вразливість, Децентралізація, Підміна.

I. Вступ

Ідеологія проектів, що застосовують технологію блокчейн - це можливість розмежованого використання доступу до інформації з унеможливленням зміни даних в реєстрі, що доступний усім користувачам мережі. Ця технологія стала відома коли вона була застосована для забезпечення появи електронних грошей, де здійснюються цифрові перекази грошей у розподілених системах. Через це блокчейн часто розглядається як пов'язаний з біткоїном або рішеннями в сфері електронної валюти в цілому. Незважаючи на це, технологія може бути використана більш широко для різних сфер застосування.

II.Побудова систем з використанням blockchain

Кожен компонент блокчейн можна просто описати та використовувати як структурний елемент, щоб зрозуміти більш складну систему.

В системі до старих даних додаються нові блоки, попередні блоки стає все важче модифікувати. Нові блоки додаються до всіх копій учасників реєстру в мережі та будь-які конфлікти вирішуються автоматично за допомогою встановлених правил.

Системи блокчейн можуть здаватися складними, але їх можна легко зрозуміти вивчаючи кожну компонентну технологію індивідуально.

Важливим компонентом технології блокчейн є використання криптографічних геш-функцій для гешування вмісту блоку, наприклад, в багатьох технологіях пов'язаних з блокчейн використовується алгоритм гешування Secure Hash Algorithm (SHA) з вихідним розміром 256 біт. Багато комп'ютерів підтримують цей алгоритм в апаратному забезпеченні, що робить його швидким для обчислення.

Використаний алгоритм гешування (SHA-256) є стійким до колізій (пошуку двох однакових дайджестів для різних початкових значень), тому що для виявлення такої ситуації в SHA-256 потрібно було б виконати алгоритм в середньому близько 2128 разів. Технології блокчейн беруть список транзакцій та створюють геш для списку. Кожен, хто має такий же список транзакцій, може генерувати точно такий самий відбиток. Якщо змінюється одне значення транзакції в списку, дайджест для цього блоку змінюється, що дозволяє легко виявити навіть незначні зміни в одному біті [1].

Важливо визначити дійсність транзакції тому, що те, що хтось стверджує, що транзакція відбулася, не означає, що це дійсно відбулося. Транзакції підписані, та їх можна будь-коли перевірити за допомогою пари публічних / приватних ключів.

Для передачі цінності в мережах блокчейн використовуються адреси.

Адреса користувача – це короткий буквено-цифровий рядок, що походить від відкритого (публічного) ключа користувача, використовуючи функцію гешування. Адреси використовуються для надсилання та отримання цифрових активів. Адреси коротші за відкриті ключі та не таємні. Для створення адреси необхідно взяти відкритий ключ, його геш-значення та перетворення гешу в текст.

Користувачі можуть генерувати так багато пар приватних / публічних ключів, а значить, адрес, як того хочуть, дозволяючи змінювати ступінь псевдоанонімності. Адреси виступають як ідентифікація блокчейну для користувача та часто за допомогою простого користування адреса перетворюється на QR-код. Підписавши цифрову транзакцію за допомогою приватного ключа, транзакцію можна перевірити за допомогою публічного ключа.

В блокчейні використовується асиметрична ключова криптографія, що використовує пару ключів: публічний та приватний ключ, які математично пов'язані один з одним. Публічний ключ може бути оприлюднений без зниження безпеки процесу, але приватний ключ повинен залишатись секретом, якщо інформація має зберігати свій криптографічний захист. Попри те, що існує взаємозв'язок між двома ключами, приватний ключ не може ефективно визначатися на підставі знання публічного ключа.

Під час роботи кожного вузла мережі блокчейн використовується та зберігається реєстр обліку, що є сукупністю транзакцій, які передавалися між усіма вузлами за весь час роботи [1].

Учасники мережі можуть подавати кандидати транзакцій в реєстр обліку, відправивши ці транзакції до деяких вузлів, що беруть участь у блокчейні. Подані транзакції поширюються на інші вузли мережі

(але це само по собі не включає транзакцію в блокчейн). Розподілені транзакції очікують у черзі або пулі транзакцій, доки вони не будуть додані до блокчейну вузлом видобування (процес майнінгу).

Після створення кожний блок гешується, створюючи таким чином дайджест, що представляє блок. Зміна навіть одного біта в блоці повністю змінить геш-значення. Дайджест блоку використовується для захисту блоку від змін, після того, як всі вузли матимуть копію геш-значення блоку, можна перевірити, чи не було змінено блок.

III.Атаки на мережу блокчейн

Стосовно мережі блокчейн, порушники можуть бути зовнішніми або внутрішніми [2]. Внутрішній порушник – це, здебільшого, розробник певного проекту або додаткового компоненту (модуля) проекту, що хоче порушити безпеку системи ще на етапі розробки або експлуатації, реалізує внутрішнє проникнення або віддалене, де використовується вже відома помилка у безпеці. Зовнішній – атакує мережу, як звичайний користувач або учасник мережі (вузол або нод мережі), реалізує віддалені атаки.

Мета порушника:

1) одержання можливості вносити зміни в мережу блокчейн згідно зі своїми намірами;

2) перешкоджати нормальній роботі мережі (перевантажувати вузли, блокувати доступ, отримати контроль над мережею тощо);

3) отримання матеріальної або іншої вигоди, шляхом крадіжки даних / грошових ресурсів.

Для того, щоб здійснити атаку, внутрішній порушник повинен:

1) мати доступ до редагування програмної частини мережі або створення та додавання до неї власних частин (бекдорів), що дадуть змогу використати мережу у своїх цілях;

2) володіти достатніми знаннями про роботу мережі та про її вразливі місця.

Зовнішній порушник повинен:

1) володіти достатньою кількістю обчислювальних та матеріальних ресурсів для здійснення своєї атаки;

2) володіти достатніми знаннями про роботу мережі та про її вразливі місця.

У ситуації для внутрішнього порушника, технічна оснащеність не є важливою тому, що використання бекдорів або заздалегідь створених каналів для несанкціонованого доступу є простою здачею для одного звичайного комп'ютера.

У ситуації для зовнішнього порушника, ресурси для атаки є вкрай важливими через те, що безпека багатьох сучасних блокчейн систем опирається на складність вирішення певних криптографічних задач. Успішність атаки залежить від кількості обчислювальних ресурсів / потужностей зловмисника, якщо мова не йде про використання знайденої помилки у мережі безпеки [3].

Кількість людей, що здійснюють атаку, може бути різною і залежить лише від плану самої атаки. Для внутрішнього зловмисника достатньо і однієї людини. Атаку із необхідністю великої кількості ресурсів, одній людині буде виконати вже важче. Загалом, сучасні атаки на блокчейн або на користувачів мереж блокчейн, здійснюються підготовленою командою із продуманим планом дій на кожному етапі атаки.

В нашому випадку при розгляді безпеки ФГ, необхідно брати до уваги як внутрішніх, та і зовнішніх зловмисників. Щодо функцій гешування може бути застосована загроза «зламування криптоалгоритмів», в основі якої лежить необхідність в великій обчислювальній потужності.

Висновки

Кожен учасник мережі повинен використовувати шифрування (здебільшого асиметричне). Заходи безпеки вбудовані в мережу і закладені у загальному протоколі, що забезпечує конфіденційність і автентичність для користувачів.

Користувачі повинні контролювати свої дані. У кожного має бути право вирішувати, які відомості, коли, як і в якому обсязі повідомляти про себе – тобто ти сам володієш своїми конфіденційними даними і без твого відома їх ніхто не може отримати.

Права учасників системи – рівні, прозорі і закріплені та підтверджуються в мережі усіма і всі з ним погоджуються.

При виконанні всіх рекомендацій з безпеки, використання перевірених та надійних криптографічних засобів можна легко побудувати гарно захищену систему на основі технології блокчейн.

Література

[1] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. NISTIR 8202 Blockchain Technology Overview.

[2] Halpin H., Piekarska M. Introduction to Security and Privacy on the Blockchain //2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2017. – С. 1-3.

[3] Tosh D. K. et al. Security implications of blockchain cloud with analysis of block withholding attack //Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. – IEEE Press, 2017. – С. 458-467.