Безпека технології блокчейн для децентралізованих систем

Данило Скічко[1], Тетяна Гріненко[2], Олексій Нарєжній[3]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: meksvinz@gmail.com

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: tetiana.grinenko@nure.ua

3. Кафедра безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. *Каразіна*, УКРАЇНА, м. Харків, майдан Свободи, 4, E-mail: o.nariezhnii@karazin.ua

The analysis of blockchain technology security and analysis of existing systems to identify existing vulnerabilities and possible attacks on decentralized systems are given. The work provides examples of technologies built on the blockchain and evaluates their software features.

Атака, безпека, блокчейн, вразливість, криптовалюта, технологія, bitcoin, monero.

I. Вступ

Сьогодні дуже популярною є помилкова думка, що технології, які побудовані на блокчейні майже не мають вразливостей, а клієнти, які користуються такими технологіями, не можуть понести матеріальних або будь-яких інших видів збитків. Але це не так. Блокчейн сам по собі – це всього лише підхід до зберігання даних, а безпека технологій, побудованих на ньому, в більшості випадків залежить тільки від програмної реалізації останніх.

Блокчейн має на увазі децентралізацію, а децентралізація, в свою чергу, безліч вузлів і клієнтів в мережі, які постійно взаємодіють один з одним [1]. Найчастіше, до такої мережі може приєднається кожен охочий (запустивши попередньо на своєму вузлі відповідне програмне забезпечення).

До технології, що побудована на блокчейні, висуваються високі вимоги безпеки. Такі технології повинні мати якомога менше програмних вразливостей, що можуть бути використані зловмисником, яким потенційно може бути будь-який новий член мережі. Варто зауважити, що проблема високих вимог до мережі частково вирішується формуванням довіреного кола вузлів, які будуть підтримувати блокчейн, тим самим не даючи зловмисникам використовувати уразливості навіть за їх наявності.

II. Вразливості блокчейн

Переважна більшість технологій, що побудовані на блокчейні – це криптовалюти [1]. Одна з найвідоміших вразливостей криптовалют – це атака 51%. Суть її полягає в тому, що зловмисники отримують контроль над мережею, шляхом володіння обчислювальною потужністю, яка складає 51% від потужності всієї мережі.

При успішному використанні цієї вразливості, зловмисники можуть фактично диктувати дані, які будуть додані в блокчейн в майбутньому. За допомогою цієї уразливості, в контексті криптовалют, можна провести так звану атаку подвійної витрати. Варто зауважити, що на сьогодні досить багато проектів закрилися на самому старті саме через те, що зловмисники досить легко використовували цю вразливість (на старті проекту у мережі мало вузлів і сумарна потужність не надто велика).

У блокчейн рішеннях користувач є відповідальним за доступність своїх даних, а атрибутом доступу до системи зазвичай виступає ключова пара. Ще одна вразливість – крадіжка або втрата ключової пари. Фактично факт володіння активами в блокчейні підтверджується особистим ключем користувача. При крадіжці ключа зловмисник зможе безперешкодно використовувати активи користувача. Ще одним недоліком є те, що користувач, маючи на руках всі докази втрати або крадіжки ключів, ніяк не зможе їх відновити (так буває при втраті або компрометації пароля якогось сервісу). Тому користувачі децентралізованих систем, побудованих на блокчейні, повинні розуміти відповідальність за збереження своїх даних і враховувати не тільки особливості безпеки технології, а й уразливості своїх локальних машин або сховищ даних.

Недоліки, пов'язані з втратою особистих ключів, вирішуються за допомогою використання сторонніх сервісів, які виступають в ролі посередника між користувачем і кінцевою системою. Тим самим вони беруть на себе відповідальність за збереження особистих даних користувачів. З одного боку, це полегшує життя кінцевим користувачам, а з іншого, подібні сервіси вже не раз піддавалися атакам з наступною крадіжкою ключових даних (що відповідно є великою шкодою для клієнтів). Тому для здійснення транзакції в системі оптимальним рішенням буде використання мультипідпису або смартконтрактів.

Крім вразливостей, пов'язаних з аспектом децентралізації та ключових пар, у криптовалют є програмні уразливості або особливості, які, наприклад, дозволяють сторонньому спостерігачеві провести аналіз дій користувача і дізнатися конфіденційну інформацію про нього. Наприклад, в Bitcoin всі транзакції і адреси відкриті всім користувачам мережі і стороннім спостерігачам. При належних зусиллях можна зіставити адреси, з яких проводилися транзакції і події в реальному світі (наприклад, покупка автомобіля), та спробувати дізнатися особистість клієнта системи або інформацію, яка в кінцевому підсумку призведе до клієнта. Крім простого аналізу до Bitcoin застосовні й інші алгоритми, які дозволяють деанонімізувати користувача.

III. Децентралізована облікова система Monero

Однак не всі криптовалюти працюють так як Bitcoin. Адже криптовалюта – це всього лише програмна реалізація протоколу, який працює на блокчейні. В одних протоколах приділяється увага відкритості та прозорості операцій, тоді як в інших, приділяється увага безпеці користувачів системи (що найчастіше ускладнює їм життя на благо збереження їх особистих даних). Прикладом такої криптовалюти є проект Monero. Децентралізована облікова система Monero – це система, в якій упор зроблений в першу чергу на забезпечення анонімності користувача [2].

В системі Monero така інформація як: суми транзакцій, ідентифікаційні дані відправника та ідентифікаційні дані одержувача приховані в ланцюжку блоків, тому дії по зберіганню і витраті монет не можна відстежити. Monero також включає в себе модуль wallet (гаманець). Гаманець зберігає ключі і здійснює складні криптографічні операції з управління активами. Для доступу до гаманця необов'язково контролювати приватні ключі, досить зберегти seed фразу, яка була використана при генерації гаманця. Seed – це секретне число, яке гаманець використовує, щоб згенерувати ключі та отримати доступ до монет, хоча для зручності і сприйняття людиною це число перетворюється в серію з 12-25 слів [2]. Seed фраза (або основний секрет) повинен бути доступний тільки користувачеві гаманця, так як знання seed-фрази гаманця визначає володіння активами, які гаманець зберігає.

В Monero забезпечуються розширені функціональні можливості, анонімність і конфіденційність завдяки використанню декількох унікальних криптографічних технологій, які захищають користувачів і їх діяльність від публічного доступу, таких як:

– RingCT (ring confidential transactions) – приховує суму транзакції;

– Ring signatures – дозволяє захистити користувача від розкриття виходу, який був витрачений;

– Stealth address – гарантує, що адреса отримувача не буде записана в ланцюжку блоків;

– Kovri – це реалізація I2P, написана на C++, яка дозволяє розірвати зв'язок між транзакціями і фізичним місцем розташування, приховуючи мережеві ознаки активності вузла Monero.

RingCT – це криптографічна технологія, яка приховує кількість грошей, що надійшли в будь-якій транзакції. У більшості криптовалют суми транзакцій відправляються у вигляді відкритого тексту, який є видимим будь-якому спостерігачеві. RingCT зберігає цю конфіденційну інформацію в секреті, дозволяючи відправнику довести, що у нього достатньо грошей для транзакції, не розкриваючи значення цієї суми. Це можливо завдяки криптографічним зобов'язаннями і range proofs. Range proofs – ще один важливий механізм в RingCT, як метод, який гарантує, що відправляєма кількість монет більше нуля і менше певного числа. Це необхідно для запобігання відправки користувачем від'ємних або неймовірно великих сум.

Ring signatures (кільцеві підписи) – це функція Monero, яка використовується для захисту відправника транзакції шляхом маскування джерела витрачених монет (не витраченого виходу). Маскування забезпечується шляхом перемішування ключів кількох виходів в ланцюжку блоків. У результаті можна перевірити, що один з виходів був витрачений, але який саме визначити практично неможливо. Кільцеві підписи за замовчуванням застосовуються до кожної транзакції.

Всі транзакції в Monero використовують stealth addresses для захисту конфіденційності одержувача, тобто для запобігання запису адреси одержувача в ланцюжок блоків. Кожна транзакція в Monero відправляється на унікальну одноразову адресу, доступ до якої має тільки той, кому призначалася транзакція.

Kovri – це функція протоколу Monero, яка призначена для захисту від розкриття IP адреси вузла. Трафік, що виходить від вузла мережі Monero, проходить через інтернет-провайдера, який може виділити активність вузла і ідентифікувати його як вузол мережі Monero.

Висновок

Відкритість транзакцій в децентралізованих системах, з одного боку, є плюсом для спільноти, а з іншого – з'являються ризики розкриття адреси суб'єкта. Аналіз існуючих децентралізованих систем (наприклад, Bitcoin, Ethereum) дозволяє зробити висновок, що на основі ланцюжка блоків можна ідентифікувати приналежність деяких адрес конкретним суб'єктам. Тому для здійснення транзакції в системі оптимальним є використання мультипідпису або смартконтрактів.

Література

[1] Кравченко П. Блокчейн и децентрализованные системы: учебное пособие для студ. заведений высш. Образования : в 3 частях. Ч. 1 / П. Кравченко, Б. Скрябин, О. Дубинина. – Харьков : ПРОМАРТ, 2018. – 400 с. – ISBN 978-617-7634-26-2.

[2] Mastering Monero [Электронный ресурс] – https://github.com/monerobook/monerobook