Комарець
Катерина Антонівна,
студентка групи КБІКС-19-2 кафедри БІТ
Харківського національного університету радіоелектроніки.
Данилов
Андрій Дмитрович
старший викладач кафедри БІТ
Харківського національного університету радіоелектроніки.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ КРИПТОВАЛЮТИ ВІД ЗЛОВМИСНИКІВ

Впродовж останніх років популярність криптовалюти постійно збільшується. Зі збільшенням попиту на використання криптовалюти збільшується кількість злочинів пов'язаних з криптовалютою. Саме тому, важливо захистити ці цифрові активи від зловмисників. У роботі наводяться результати аналізу методів захисту криптовалюти від зловмисників, зосереджені на використанні шифрування, аутентифікації та інших заходів безпеки.

Під час аналізу предметної галузі було виявлено багато різних методів захисту криптовалюти від зловмисників. Одним з найпоширеніших методів є використання криптографічних протоколів, які забезпечують захист від перехоплення та підробки транзакцій. Також існують методи захисту, що ґрунтуються на використанні технологій блокчейн та "розумних контрактів". Однак, незважаючи на наявність таких методів захисту, зловмисники все ще знаходять способи, щоб отримати доступ до криптовалют.

Криптовалюта − це форма цифрових або віртуальних грошей, що базується на криптографічних принципах та технологіях, які забезпечують безпеку транзакцій та контроль над створенням нових одиниць валюти. Криптовалюти працюють на основі децентралізованої системи, яка дозволяє користувачам проводити транзакції без посередництва банків чи інших посередників [4].

Шифрування є ключовим компонентом захисту криптовалюти від зловмисників. Шифрування – це процес перетворення даних у нечитабельну форму, що ускладнює доступ до даних. Криптовалютні гаманці використовують шифрування для захисту закритих ключів, які використовуються для доступу до гаманця. Крім того, багато бірж використовують шифрування для захисту даних, які вони зберігають, і запобігання доступу зловмисників до конфіденційної інформації [5].

Автентифікація є ще одним важливим заходом безпеки, який використовується для захисту криптовалюти від зловмисників. Автентифікація − це процес перевірки особи користувача перед тим, як дозволити йому отримати доступ до системи. Це часто робиться за допомогою паролів, двофакторної автентифікації, біометричної автентифікації або інших методів. Автентифікація гарантує, що лише авторизовані користувачі можуть отримати доступ до системи, таким чином запобігаючи зловмисникам отримати доступ.

Для захисту криптовалюти від зловмисників також можна використовувати інші заходи безпеки. Холодне зберігання − це спосіб зберігання криптовалюти в автономному режимі, який запобігає доступу зловмисників до коштів. Крім того, гаманці з кількома підписами вимагають кількох підписів від авторизованих користувачів, перш ніж транзакція може бути завершена, що може допомогти захистити від зловмисників.

Отже, найнадійніший спосіб захисту криптовалюти від зловмисників − використання комбінаціъ методів. Розглянемо більш детально кілька методів захисту криптовалюти від зловмисників(окрім тих, що згадано вище):

1. Мультипідписні гаманці: Мультипідписні гаманці вимагають, щоб кілька людей підписали транзакцію перед її виконанням. Це значно ускладнює крадіжку коштів зловмисникам, оскільки їм потрібно буде отримати доступ до кількох гаманців, щоб здійснити транзакцію.
2. Двофакторна автентифікація: двофакторна автентифікація додає додатковий рівень безпеки вашому гаманцю. Щоб отримати доступ до гаманця, потрібно ввести код, надісланий на ваш телефон або електронну адресу. Це значно ускладнює зловмисникам доступ до ваших коштів.
3. Апаратні гаманці: апаратні гаманці – це фізичні пристрої, які зберігають ваші закриті ключі в автономному режимі. Це робить їх набагато безпечнішими, ніж програмні гаманці, оскільки зловмисникам потрібно буде отримати фізичний доступ до пристрою, щоб викрасти ваші кошти.
4. Диверсифікація. Диверсифікація ваших криптовалютних активів – ще один спосіб захистити свої кошти від зловмисників. Розподіляючи свої кошти між кількома гаманцями та біржами, ви значно ускладнюєте зловмисникам доступ до всіх ваших коштів.
5. Регулярне резервне копіювання: регулярне резервне копіювання вашого гаманця – ще один спосіб захистити свої кошти від зловмисників. Зберігаючи копію свого гаманця в безпечному місці, ви можете відновити свої кошти, якщо ваш гаманець буде втрачено або викрадено.

Також, важливо мати ефективну систему моніторингу та виявлення несподіваних транзакцій, які можуть свідчити про порушення безпеки та намагання зловмисників отримати доступ до криптовалюти. Для цього можна використовувати алгоритми машинного навчання, які допоможуть виявляти небезпечні транзакції та зупиняти їх здійснення.

Додатково, можна розглянути методи захисту на рівні протоколу, такі як використання підписів Schnorr, які забезпечують більшу ефективність та безпеку при здійсненні транзакцій. Також можна використовувати методи затвердження транзакцій на основі кворуму, що дозволяє зменшити ризик зламу системи за допомогою атаки "51% атака".

Забезпечення безпеки криптовалюти − важливе завдання, яке потребує постійного аналізу та удосконалення методів захисту. Застосування комбінації різних методів, таких як біометрична аутентифікація, мультипідпис та системи моніторингу транзакцій, може значно підвищити рівень безпеки криптовалюти та зменшити ризик її крадіжки. Також важливо продовжувати дослідження та

розробку нових методів захисту, щоб забезпечити безпеку використання криптовалюти в майбутньому.

Найкращим методом захисту криптовалюти від зловмисників є використання комбінації заходів, таких як двофакторна автентифікація, надійні паролі та апаратні гаманці. Двофакторна автентифікація дає додатковий рівень безпеки вашому обліковому запису, вимагаючи додаткової форми автентифікації, наприклад коду, надісланого на ваш мобільний телефон, перш ніж дозволити доступ. Для захисту облікових записів слід використовувати надійні паролі, а для кожного облікового запису слід використовувати унікальні паролі. Нарешті, апаратні гаманці – це фізичні пристрої, які зберігають ваші закриті ключі в автономному режимі та вважаються одним із найбезпечніших методів зберігання криптовалюти.

Перелік використаних джерел

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.
2. Bennett, S. (2018). Cryptocurrency Security: Threats and Solutions. Wiley.
3. Drescher, D. (2018). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress.
4. Що таке криптовалюта: пояснюємо простими словами. https://forklog.com.ua/exclusive/shho-take-kryptovalyuta-poyasnyuyemo-prostymy-slovamy : веб сайт URL https://forklog.com.ua/exclusive/shho-take-kryptovalyuta-poyasnyuyemo-prostymy-slovamy (дата звернення: 5.03.2023).
5. П. Кравченко, Б. Скрябін, О. Дубініна (2019) “Блокчейн і децентралізовані системи” 1 частина.