НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп’ютерного практикуму “Реалізація смарт-контракту або анонімної криптовалюти”

Виконав:
студент групи ФБ-31мп
Варгіч Дмитро

Перевірила:
Селюх П.В.

Київ — 2024

Мета роботи: «Отримання навичок роботи із смарт-контрактами або анонімними криптовалютами»

Завдання: дослідження методів анонімізації/деанонімізації запропонованої криптовалюти із аналізом складності проведення атак деанонімізації і втрат ефективності анонімних криптовалют у порівнянні із Bitcoin/Litecoin;
оцінка та обґрунтування необхідних ресурсів (гасу і ефіру), потрібних для функціонування смарт-контракту.

Природа і особливості криптовалют

Головною особливістю криптовалют є їхня відкритість: кожен учасник мережі може переглянути історію всіх транзакцій. Це називається громадським реєстром. «Адреси» у блокчейні можна порівняти з публічними іменами, які використовуються для ідентифікації людей. Але вони створюються із особливих секретних імен, які знають лише самі власники. Таким чином, блокчейн-адреси не містять жодної особистої інформації про власників, наприклад, їх справжні імена або місця проживання. Це допомагає зберігати приватність та безпеку власників криптовалютних адрес.

Однак, незважаючи на те, що адреси не містять відкритої інформації про власника, вони можуть бути атрибутовані конкретним людям або організаціям через точки взаємодії з традиційною фінансовою системою: обмінники, біржі, гаманці з підтримкою KYC (Know Your Customer) та інші послуги, що потребують ідентифікації користувача.

Деанонімізація криптовалютних платежів

1. Зв'язок із криптовалютними біржами

У багатьох країнах криптовалютні біржі повинні проводити процедуру KYC. Це означає, що під час реєстрації на біржі ви повинні розкрити свою особисту інформацію. У випадку, якщо біржа приймає рішення про співпрацю з державними структурами або стає жертвою атаки хакерів, ця інформація може бути використана для деанонімізації.

2. Аналіз блокчейну

За допомогою спеціалізованих інструментів можна простежити історію транзакцій від певної адреси. Якщо ця адреса була прямо пов'язана з людиною або організацією (наприклад, через біржу або обмінник), це дозволяє розкрити історію його транзакцій.

Якщо розглянути це докладніше, можна переконатися, що в найпростішому випадку аналіз блокчейна дозволяє переглянути всі транзакції окремим гаманцем. Можна взяти адресу біткойн-гаманця, ввести його на сайті blockchain.com і побачити, що така адреса здійснила стільки-то транзакцій на Bitcoin-блокчейні, всього було отримано стільки-то коштів, відправлено стільки-то, а поточне значення цієї адреси таке (скільки зараз на рахунку).

3. Мережевий аналіз

Якщо криптовалютні транзакції здійснюються через інтернет без використання анонімних технологій (наприклад, VPN або Tor), IP-адреси можуть бути використані для визначення розташування користувача та відстеження транзакцій.

Варто враховувати: біткоін-транзакції відправляються в незашифрованих пакетах через інтернет, що дозволяє відстежити IP-адресу відправника і потім за необхідності атрибутувати власнику цієї адреси.

4. Комбінований підхід

Інтеграція даних із різних джерел може підвищити ймовірність деанонімізації. Наприклад, суміщення інформації від криптовалютних бірж, даних про транзакції в блокчейні та мережевих даних може призвести до значно більш точної деанонімізації. Наприклад, США регулярно накладає арешт на криптовалюту, і це призвело до того, що у власності уряду Штатів більше біткоїнів, ніж у будь-якої іншої країни. Влада комбінує всі підходи, щоб знайти або ідентифікувати криптовалюту та конфіскувати її.

Способи підтримки анонімності

- Конфіденційні криптовалюти

Є криптовалюти, наприклад Monero та Zcash, які були розроблені з акцентом на покращену конфіденційність. Monero застосовує обфускацію даних транзакцій лише на рівні свого протоколу, що робить їх

непрозорими для публічного блокчейну. Zcash пропонує опцію "захищених транзакцій", які також приховують інформацію про транзакції.

- Мікшер монет (Coin Mixing)

"Мікшер монет" - це як машинка, яка перемішує монети. Цей підхід передбачає змішування транзакцій різних користувачів з метою ускладнення їхнього відстеження. У випадку з біткоїнами такі сервіси часто називають Bitcoin tumblers. Але варто бути пильними, оскільки деякі сервіси можуть виявитися шахрайськими чи скомпрометованими. Також США розпочали боротьбу з такими сервісами у рамках боротьби з відмиванням грошей.

- Використання одноразових гаманців

Цей спосіб підходить як організаціям, які збирають пожертвування, так і відправникам. Організації можуть створювати одноразовий гаманець під кожну пожертву і потім уже брати на себе турботи щодо анонімізації. Це технічно складно реалізувати, але дозволяє убезпечити тих донорів, хто не перейнявся своєю анонімністю. Також одноразовий гаманець чи просто окремий гаманець під перекази можуть зробити самі жертводавці.

- Анонімність

Застосування VPN або мережі Tor для здійснення транзакцій може допомогти приховати IP-адресу та підвищити рівень анонімності.

- Децентралізовані обмінні пункти (DEX)

На відміну від традиційних бірж, DEX не вимагають процедури ідентифікації користувача, що знижує можливість деанонімізації. По суті, це біржі, де відбуваються лише транзакції peer-to-peer – від користувача до користувача. Цей спосіб дозволяє обійти централізовані біржі з прив'язкою гаманця до паспорта, але для максимальної анонімності він все одно вимагає приховувати свою IP-адресу та проводити монети через мікшер.

Висновки

Кожен із вищеперелічених методів має свої переваги та недоліки. Їхня ефективність у конкретній ситуації залежатиме від безлічі факторів, включаючи технічну грамотність користувача та особливості правового режиму.

Порівняння Zdash та Bitcoin

Методи анонімізації Zcash:

zk-SNARKs – це основний метод, що дозволяє перевірку транзакцій без розкриття додаткової інформації про відправника, отримувача або суму транзакції. Це досягається через математичні докази, які доводять правдивість інформації без її розголошення. Використання zk-SNARKs вимагає додаткових обчислювальних ресурсів, що може впливати на швидкість і вартість транзакцій. Однак, з покращенням технологій, ці витрати зменшуються, роблячи анонімні транзакції все більш доступними. Цей метод значно ускладнює деанонімізацію завдяки сильній криптографії. Для успішної атаки потрібні величезні обчислювальні ресурси та доступ до значної кількості даних про транзакції.

Крім того, Zcash пропонує два типи адрес - прозорі (t-addr) і захищені (z-addr). Транзакції між z-addr повністю анонімні і не розкривають деталей транзакції. Транзакції між z-addr практично неможливо відслідковувати без компрометації приватних ключів, що робить атаку надзвичайно складним завдання.

Методи анонімізації Bitcoin:

CoinJoin - це метод, при якому користувачі відправляють свої монети в одну транзакцію, яка потім розподіляє монети новим адресатам. Це створює багато входів і виходів, які ускладнюють аналіз. Складність деанонімізації зростає з кількістю учасників у CoinJoin транзакціях. Однак, при використанні неякісних CoinJoin сервісів можливі атаки, що дозволяють часткове відстеження.

CoinSwap дозволяє двом або більше користувачам обмінюватися монетами безпосередньо, але через посередників або кілька транзакцій, щоб розірвати зв'язок між відправником і отримувачем. Дуже високий рівень анонімності, оскільки транзакції не мають прямого зв'язку між відправником і отримувачем. Складність деанонімізації значно зростає, якщо використовуються надійні посередники.

Stealth Addresses дозволяють відправнику генерувати нову унікальну адресу для кожної транзакції, яка потім прив'язується до отримувача. Відправник використовує публічний ключ отримувача для створення унікальної одноразової адреси для кожної транзакції, що ускладнює відстеження отримувача. Цей метод значно ускладнює відстеження

транзакцій, але потребує додаткової обчислювальної потужності та ресурсів.

Методи деанонімізації Zcash:

Аналізуючи зв'язки між різними адресами, можна виявити потенційні шаблони або зв'язки, навіть якщо використовується zk-SNARKs. Однак, для Zcash з повністю захищеними транзакціями цей метод значно ускладнюється.

Кореляційні атаки: Спостерігаючи за вхідними і вихідними транзакціями з обмінниками, можна спробувати зіставити певні транзакції. Наприклад, якщо відомо, що користувач купив певну кількість Zcash, а потім спробував їх витратити.

Методи деанонімізації Bitcoin:

- Аналіз графу транзакцій: аналіз структури та зв'язків між адресами у блокчейні.
- Аналіз сполучень (clustering): якщо адреси використовуються в одній транзакції як входи, можна припустити, що вони контролюються однією особою.
- Blockchain Forensics: компанії, такі як Chainalysis або Elliptic, надають послуги з аналізу блокчейну для виявлення зв'язків між адресами та реальними особами.
- IP-адреси та мережевий трафік: мережеві вузли можуть логувати IP-адреси користувачів, що надсилають транзакції, і зіставляти їх з транзакціями в блокчейні.