Лабораторна робота №2

«Реалізація смарт-контракту або анонімної криптовалюти»

Абдуллаєва Есміра, Товстенко Артем, Пашинський Максим ФБ-31мп

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.

Хід роботи

Ethereum, друга за популярністю криптовалюта, використовує модель публічного блокчейну, де всі транзакції відкриті для перегляду. Це забезпечує прозорість, але також ставить під загрозу конфіденційність користувачів.

1. Дослідження методів анонімізації та деанонімізації Ethereum

У цьому дослідженні буде розглянуто методи анонімізації та деанонімізації транзакцій Ethereum, проаналізовано складність атак деанонімізації та порівняємо рівень анонімності Ethereum з Bitcoin та Litecoin.

1.1.Методи анонімізації

Змішування монет: Цей метод ґрунтується на багаторазовому надсиланні коштів через різні адреси та пули змішування, щоб ускладнити відстеження походження та власника монет. Популярні сервіси для змішування Ethereum включають Tornado Cash та Aztec Protocol.

Zk-SNARKs (докази з нульовим розглашенням): Ця криптографічна технологія дозволяє користувачам підтверджувати транзакції без розкриття їхніх деталей, таких як суми та адреси. Zk-SNARKs використовуються в проектах, таких як Zcash та zkSync.

Анонімні криптовалюти, орієнтовані на конфіденційність: Monero та Dash - це приклади криптовалют, які вбудовують анонімність у свій протокол, використовуючи такі методи, як криптографічні маски та кільцеві підписи.

1.1.1. Плюси та мінути методів анонімізації

Плюси:

- Підвищена конфіденційність: Анонімні транзакції складніше відстежити та пов'язати з конкретними користувачами.
- Захист від цензури: Уряди або інші органи не можуть легко блокувати транзакції або заморожувати кошти.
- Захист від злочинців: Анонімність може допомогти захистити користувачів від крадіжки коштів або інших злочинів.
- Більший контроль над даними: Користувачі мають більший контроль над тим, які дані про себе вони розкривають.

Мінуси:

- Складність використання: Деякі методи анонімізації можуть бути складними у використанні або мати певні компроміси, наприклад, зменшення швидкості транзакцій або збільшення комісій.
- Зниження швидкості транзакцій: Анонімні транзакції можуть бути повільнішими, ніж звичайні транзакції Ethereum.
- Збільшення комісій: Анонімні транзакції можуть бути пов'язані з більш високими комісіями, ніж звичайні транзакції Ethereum.
- Ризик використання для незаконних цілей: Анонімність може використовуватися злочинцями для відмивання грошей або інших незаконних цілей.
- Можливість деанонімізації: Деякі методи анонімізації не є абсолютно стійкими до атак деанонімізації.

Важливо зазначити, що ефективність та безпека методів анонімізації може варіюватися. Деякі з цих методів можуть бути складними у використанні або мати певні компроміси, наприклад, зменшення швидкості транзакцій або збільшення комісій.

1.2. Методи деанонімізації

Атаки деанонімізації націлені на розкриття особистостей користувачів або деталей їхніх транзакцій. Складність проведення таких атак залежить від обраного методу анонімізації та загального рівня безпеки мережі. Деякі можливі методи атак включають:

Аналіз ланцюжка блоків: Цей метод включає відстеження транзакцій між адресами та пошук зв'язків, які можуть розкрити інформацію про власників цих адрес.

Кластерний аналіз: Цей метод використовується для групування адрес, які, ймовірно, належать одному власнику, на основі їхньої історії транзакцій.

Атаки з використанням сайд-каналів: Ці атаки використовують інформацію, яка не записується в блокчейн, наприклад, час транзакції або розмір комісії, щоб деанонімізувати користувачів.

Атака Sybil: Цей тип атаки використовує створення множини псевдонімних адрес гаманців для приховування особистості користувача та його транзакцій.

Кореляція IP-адрес: Цей метод використовує поєднання аналізу ланцюжка блоків та відстеження IP-адрес для зв'язку транзакцій з конкретними користувачами.

Соціальний інженеринг: Цей метод використовує психологічні маніпуляції для того, щоб змусити користувачів розкрити свою особисту інформацію, пов'язану з їхніми адресами Ethereum.

Складність атак деанонімізації залежить від використовуваних методів анонімізації та деанонімізації. Змішування та сервіси збереження конфіденційності роблять анонімізацію більш стійкою до деанонімізації, але й їх використання може бути пов'язано з певними компромісами, наприклад, зменшенням швидкості транзакцій або збільшенням комісій.

1.2.1. Заходи протидії методам деанонімізації

Використання міксерів Ethereum: Міксери Ethereum - це децентралізовані служби, які дозволяють користувачам змішувати свої криптовалюти з іншими користувачами, щоб приховати походження та призначення транзакцій.

Використання Zcash: Zcash - це криптовалюта, що використовує zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) для забезпечення конфіденційності транзакцій.

Використання децентралізованих VPN (dVPN): dVPN - це децентралізовані мережі VPN, які не мають централізованого контролю, що робить їх більш стійкими до цензури та відстеження.

Уважне ставлення до онлайн-активності: Користувачі повинні бути обережні з тим, яку інформацію вони розкривають в Інтернеті, та уникати зв'язку своїх адрес Ethereum з особистою інформацією.

Важливо зазначити, що жоден метод деанонімізації або протидії їй не є абсолютно надійним. Зловмисники постійно розробляють нові методи відстеження та деанонімізації користувачів Ethereum, тому важливо

використовувати комбінацію різних методів захисту для забезпечення максимального рівня конфіденційності.

1.2.2. Складність атак деанонімізації

Атаки деанонімізації на Ethereum можуть відрізнятися за складністю залежно від використовуваного методу. Основні підходи:

Аналіз транзакцій (висока складність):

- Цей підхід передбачає аналіз публічної книги транзакцій у блокчейні Ethereum.
- Вивчаючи закономірності в історії транзакцій, взаємодії гаманців і використанні смарт-контрактів, зловмисники можуть спробувати зв'язати різні адреси Ethereum разом, потенційно розкриваючи особу користувача.
- Цей метод часто вимагає значної обчислювальної потужності та передових методів машинного навчання для ефективного виявлення кореляцій, що робить його більш складним.

Аналіз однорангової мережі (помірної складності):

- Цей підхід зосереджений на аналізі основної однорангової (P2P) мережі, яка підтримує Ethereum.
- Відстежуючи IP-адреси або інші мережеві дані, якими обмінюються вузли, зловмисники можуть спробувати з'єднати адресу Ethereum користувача з його реальною IP-адресою.
- Цей метод може бути помірно складним, оскільки вимагає використання вразливостей у протоколі P2P або зламу певних вузлів у мережі.

Загалом, деанонімізація в Ethereum є активною сферою досліджень, і складність атак може змінюватися. Ось деякі додаткові фактори, які слід враховувати:

- Поведінка користувача: користувачі, які практикують гарну опсеку (оперативну безпеку), використовуючи різні адреси для транзакцій і уникаючи їх повторного використання, можуть ускладнити аналіз.
- Методи мережевої обфускації: такі сервіси, як міксери або орієнтовані на конфіденційність гаманці, можуть додатково анонімізувати транзакції, приховуючи походження та призначення коштів.
- Розвиток блокчейну: сам блокчейн Ethereum постійно розробляється, і майбутні оновлення можуть запроваджувати функції, які покращують конфіденційність користувачів.

Важливо пам’ятати, що Ethereum пропонує псевдонім, а не повну анонімність. Розуміючи різні методи атак і вживаючи запобіжних заходів, користувачі можуть підвищити рівень конфіденційності в мережі Ethereum.

1.3. Втрата ефективності анонімних криптовалют у порівнянні з Bitcoin і Litecoin

Анонімні криптовалюти, або "приватні криптовалюти", — це цифрові валюти, що спеціально розроблені для забезпечення високого рівня конфіденційності та анонімності фінансових транзакцій. На відміну від традиційних криптовалют, таких як Bitcoin, де транзакції публічно доступні і можуть бути відстежені, анонімні криптовалюти використовують різні технології для приховування інформації про відправників, отримувачів і суми транзакцій.

Анонімізація криптовалют спрямована на забезпечення конфіденційності користувачів, але ці заходи можуть впливати на ефективність мережі. Порівняння анонімних криптовалют із такими, як Bitcoin і Litecoin, допомагає зрозуміти, які компроміси доводиться робити для досягнення високого рівня анонімності.

1.3.1. Види втрат ефективності

1. Швидкість транзакцій

Bitcoin: Середній час підтвердження транзакції становить близько 10 хвилин. Швидкість транзакцій обмежена приблизно 7 транзакціями в секунду (TPS).

Litecoin: Середній час підтвердження транзакції становить близько 2,5 хвилин, з пропускною здатністю близько 28 TPS.

Анонімні криптовалюти: Використання складних криптографічних методів, таких як кільцеві підписи (ring signatures) в Monero або zk-SNARKs в Zcash, значно збільшує час обробки транзакцій. Це може призвести до повільнішого підтвердження транзакцій у порівнянні з Bitcoin і Litecoin.

2. Комісії за транзакції

Bitcoin: Комісії варіюються залежно від завантаженості мережі. У пікові періоди комісії можуть бути високими, але зазвичай залишаються прийнятними для більшості користувачів.

Litecoin: Комісії зазвичай нижчі через швидший час підтвердження і вищу пропускну здатність.

Анонімні криптовалюти: Використання методів анонімізації збільшує обчислювальні ресурси, необхідні для підтвердження транзакцій. Це може призвести до вищих комісій за транзакції у порівнянні з Bitcoin і Litecoin.

3. Розмір блоків та обсяг даних

Bitcoin: Розмір блоку обмежений до 1 МБ, що дозволяє включати обмежену кількість транзакцій у кожен блок.

Litecoin: Має більший розмір блоку (4 МБ), що дозволяє включати більше транзакцій у кожен блок.

Анонімні криптовалюти: Додаткові дані, необхідні для забезпечення анонімності (наприклад, zk-SNARKs в Zcash або кільцеві підписи в Monero), збільшують розмір транзакцій. Це призводить до того, що кожен блок може включати меншу кількість транзакцій, що знижує загальну пропускну здатність мережі.

4. Обчислювальна складність

Bitcoin: Використовує алгоритм PoW, який потребує значних обчислювальних ресурсів, але не включає складних криптографічних методів для забезпечення анонімності.

Litecoin: Використовує алгоритм Scrypt, який є більш ресурсозатратним щодо пам'яті, але також не включає складних методів анонімізації.

Анонімні криптовалюти: Використання передових криптографічних методів (zk-SNARKs, кільцеві підписи) значно збільшує обчислювальну складність і, відповідно, вимоги до апаратного забезпечення для майнінгу та верифікації транзакцій.

5. Масштабованість

Bitcoin: Працює над рішеннями другого рівня (Lightning Network) для підвищення масштабованості.

Litecoin: Також розглядає впровадження рішень другого рівня для підвищення масштабованості.

Анонімні криптовалюти: Складні методи анонімізації ускладнюють впровадження рішень для підвищення масштабованості, що може обмежити їх здатність обробляти великий обсяг транзакцій.

Висновок. Забезпечення високого рівня анонімності в криптовалютах часто супроводжується компромісами у вигляді втрат ефективності. Це включає збільшення часу підтвердження транзакцій, вищі комісії, збільшення розміру блоків та підвищення вимог до обчислювальних ресурсів. Порівняння з Bitcoin і Litecoin показує, що менш анонімні криптовалюти

мають переваги у швидкості та вартості транзакцій, але втрачають в аспекті конфіденційності.

2. Оцінка та обґрунтування необхідних ресурсів (гасу і ефіру), потрібних для функціонування смарт-контракту.

Смарт-контракти в Ethereum виконуються на віртуальній машині Ethereum (EVM) і потребують обчислювальних ресурсів, які вимірюються в одиницях гасу (gas). Гас є внутрішньою валютою для оплати обчислень, а ефір (ETH) використовується для оплати гасу. Розуміння того, скільки гасу і ефіру потрібно для функціонування смарт-контракту, є важливим для розробників і користувачів, оскільки це впливає на вартість та ефективність використання контракту.

Кількість газу, необхідного для смарт-контракту, залежить від різних факторів, включаючи:

- **Складність коду:** Більш складні контракти з більшою кількістю операцій та циклів потребуватимуть більше газу.
- **Обсяг даних:** Операції з великими обсягами даних, такі як читання та запис даних в блокчейн, потребуватимуть більше газу.
- **Поточний стан мережі:** Комісії за газ можуть динамічно змінюватися залежно від завантаженості мережі Ethereum.

Існує кілька методів оцінки використання газу для смарт-контракту:

- **Аналіз коду:** Досвідчені розробники можуть оцінити використання газу, аналізуючи код контракту.
- **Інструменти симуляції:** Існують онлайн-інструменти та бібліотеки, які дозволяють симулювати виконання контракту та оцінювати його використання газу.
- **Розгортання тестового контракту:** Розгортання тестового контракту в тестовій мережі Ethereum може дати більш точну оцінку використання газу в реальних умовах.

Вартість виконання смарт-контракту в ефірі визначається його використанням газу та поточною ціною газу. Ціна газу динамічно змінюється залежно від завантаженості мережі.

2.1. Оцінка ефіру

Базові операції

Прості операції: Додавання, віднімання, множення та ділення мають фіксовану вартість гасу. Наприклад, додавання та віднімання коштують 3 гасу, множення – 5 гасу, а ділення – 8 гасу.

Зберігання даних: Запис даних у сховище є однією з найдорожчих операцій. Зберігання одного 256-бітного слова в сховищі коштує 20,000 гасу, тоді як оновлення існуючого запису коштує 5,000 гасу.

Читання даних: Читання даних із сховища коштує 200 гасу за кожне 256-бітне слово.

Складні операції

Виклик функцій: Вартість виклику функції залежить від кількості та типів параметрів, а також від обчислень, які вона виконує. Виклик зовнішньої функції коштує 700 гасу плюс вартість виконання коду функції.

Створення контракту: Створення нового смарт-контракту коштує 32,000 гасу плюс вартість виконання коду контракту.

Логічні операції та контролюючі структури

IF/ELSE: Виконання умовного оператора має незначну вартість гасу, яка включає базову вартість виконання коду.

Цикли: Вартість циклу залежить від кількості ітерацій і складності операцій усередині циклу. Кожна ітерація додає вартість гасу відповідно до обчислювальних операцій у ній.

2.2. Оцінка ефіру

Ціна гасу (Gas Price)

Встановлення ціни гасу: Користувачі можуть встановлювати ціну гасу (в gwei), яку вони готові заплатити за виконання своїх транзакцій. Висока ціна гасу збільшує шанси на швидке включення транзакції в блок.

Динаміка ринку: Ціна гасу змінюється в залежності від завантаженості мережі. У пікові періоди ціни можуть бути значно вищими.

Загальна вартість (Gas Limit x Gas Price)

Gas Limit: Це максимальна кількість гасу, яку користувач готовий витратити на транзакцію. Якщо транзакція використовує менше гасу, ніж встановлено в ліміті, залишок повертається користувачеві.

Обчислення вартості: Загальна вартість транзакції в ефірі розраховується як добуток Gas Limit та Gas Price. Наприклад, якщо Gas Limit становить 100,000 гасу, а Gas Price – 20 gwei, загальна вартість буде 100,000 * 20 = 2,000,000 gwei або 0.002 ETH (при 1 ETH = 1,000,000,000 gwei).

2.3. Приклад розрахунку вартості смарт-контракту

Простий смарт-контракт, що включає функцію додавання чисел і зберігання результату в сховищі:

```
pragma solidity ^0.8.0;

contract SimpleContract {
    uint256 public result;

    function add(uint256 a, uint256 b) public {
        result = a + b;
    }
}
```

a. **Вартість зберігання даних**

   Зберігання змінної result: 20,000 гасу.

b. **Вартість додавання чисел**

   Додавання a і b: 3 гасу.

c. **Загальна вартість виконання функції add.**

   Вартість зберігання результату: 20,000 гасу.

   Вартість додавання: 3 гасу.

   Виклик функції: 700 гасу.

   Загальна вартість: 20,000 + 3 + 700 = 20,703 гасу.

d. **Розрахунок вартості в ефірі**

   Припустимо, Gas Price = 20 gwei.

   Загальна вартість в ефірі: 20,703 * 20 = 414,060 gwei або 0.00041406 ETH.

Оцінка та обґрунтування необхідних ресурсів для функціонування смарт-контракту є важливими для розробників та користувачів. Розуміння вартості гасу для різних операцій і обчислення загальної вартості в ефірі дозволяє оптимізувати код контракту та знижувати витрати на його виконання. Це також допомагає уникнути перевитрат і забезпечує ефективне використання ресурсів в мережі Ethereum.