Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

«Блокчейн та децентралізовані системи»
Лабораторна робота №2

Тема: „Реалізація смарт-контракту або анонімної криптовалюти.”

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

Виконав:
студент групи ФІ-41мн
Намчук Максим

Для першого типу лабораторних:

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.

MONERO

Monero (XMR) — це децентралізована криптовалюта з відкритим кодом, головна мета якої — забезпечити повну анонімність транзакцій. На відміну від Bitcoin, де всі платежі відкриті й відстежувані, Monero приховує:

- Хто кому надсилає гроші
- Яку суму надсилають
- Баланси користувачів

1. Методи анонімізації в Monero

Stealth Addresses (приховані адреси)

Stealth-адреси дозволяють одержувачу приховати свій публічний ключ у блокчейні. Коли відправник ініціює транзакцію, він генерує унікальну адресу, яка базується на публічному ключі отримувача. Це унеможливлює прив'язку транзакції до конкретного одержувача.

Ring Signatures (кільцеві підписи)

Кільцеві підписи дають змогу приховати особу відправника транзакції. Кожна транзакція включає кілька можливих підписів (які називаються "деки"), один з яких є справжнім, але його неможливо визначити. Це забезпечує анонімність відправника серед групи користувачів.

RingCT (Ring Confidential Transactions)

RingCT дозволяє приховувати суму транзакції. Завдяки криптографічному механізму Pedersen Commitments лише учасники транзакції знають точну суму, при цьому вся мережа може перевірити її коректність.

2. Методи деанонімізації Monero

Хоча Monero забезпечує високий рівень конфіденційності, існують теоретичні та практичні методи, що можуть бути використані для деанонімізації користувачів. Вони мають обмежену ефективність і часто є неточними:

Аналіз часових міток

Якщо атакуючий має інформацію про час створення транзакції, є шанс, що він може визначити реального відправника, оскільки деякі транзакції можуть бути старішими за інші.

Аналіз кількості декоїв

Раніше Monero використовував невелику кількість декоїв, що спрощувало ймовірність правильного визначення відправника. Однак, із новими версіями кількість декоїв збільшена до 11 і більше, що значно ускладнює статистичні атаки.

Аналіз мережевого рівня

Якщо зловмисник спостерігає за мережею через вузли, теоретично можна відстежити IP-адресу, яка ініціює транзакцію. Для цього використовуються атаки типу "global passive adversary", але Monero також застосовує технології захисту через Tor або I2P.

1. Ring Signatures (приховують відправника)

Кожна транзакція приховує реального відправника серед кількох фіктивних учасників (декоїв). Зараз для замовлення використовується 16 учасників у кільці, що значно

зменшує ймовірність правильного визначення. Навіть при складному аналізі злочинець не може точно визначити, хто з підписантів є справжнім. Атаки можуть бути здійснені лише при статистичному аналізі великих обсягів транзакцій, часто з використанням сторонніх даних (наприклад, якщо відомо, коли користувач щось купував).

Складність: дуже висока, особливо з актуальною кількістю декоїв.

2. Stealth Addresses (приховують отримувача)

Кожна транзакція створює нову унікальну адресу, навіть якщо відправляються кошти тому самому гаманцю. Це значно ускладнює відстеження балансу будь-якого гаманця через блокчейн. Жодна зовнішня особа не може знати, хто є отримувачем.

Складність деанонімізації: майже неможливо без приватного ключа.

3. RingCT (приховує суму)

Сума в кожній транзакції зашифрована за допомогою механізму Pedersen Commitments. Перевірити її правильність може лише мережа, яка не знає, яка вона насправді. Навіть при аналізі великих транзакцій не вдається точно визначити, скільки було передано.

Складність деанонімізації: дуже висока, існуючими методами — нереально.

4. Атаки на мережевому рівні (мережеве спостереження)

Теоретично можливе спостереження за IP-адресами через вузли (наприклад, якщо вузол контролюється зловмисником). Але користувачі можуть використовувати Tor або I2P для повного приховування маршруту. Крім того, Monero використовує протокол Dandelion++, який ускладнює відстеження початкової точки мережі.

Складність: висока, особливо якщо користувачі використовують базові заходи безпеки.

Параметр	Bitcoin	Monero	Втрата ефективності у Monero
Середній розмір транзакції	~250 байт	~1,500–3,000 байт	У 6–12 разів більший через автоматизацію
Час створення блоку	10 хвилин	2 хвилини	30 сек. - 1 хвилина

Транзакцій в секунду (TPS)	~3–7 TPS	~1–4 TPS	Менша пропускна здатність через великі транзакції
Розмір поточного блокчейну (2024)	~500 GB	~150 GB	Monero зростає шви GB/місяць проти ~1- GB/місяць)
Тип алгоритму майнінгу	SHA-256 (ASIC-дружній)	RandomX	Вищі вимоги до ОЗП та CPU для звичайного користувача
Обчислювальні витрати на валідатори	Низькі/середні	Високі (через кільцеві підписи та RingCT)	Більше часу на ресурси для перевірки транзакцій
Анонімність транзакцій	Відсутня	Повна (адреса, сума і відкриття приховані)	Немає втрат, а навпаки перевірка
Підтримка бірж та сервісів	Майже скрізь	Частково/обмежено	Monero часто не підтримується через регуляторні і правові обмеження