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

Звіт з виконання комп'ютерного практикуму

ОТРИМАННЯ НАВИЧОК РОБОТИ ІЗ СМАРТ-КОНТРАКТАМИ АБО АНОНІМНИМИ КРИПТОВАЛЮТАМИ

Виконали студенти
групи
ФЕ-31мн
Альошкін
Володимир,
Межуєв
Максим

Перевірила:
Селюх П.В.

Київ — 2024

Мета роботи: Отримання навичок налаштування платформ виконання смартконтрактів та криптовалют.

Постановка задачі: Дослідити методи анонімізації/деанонімізації запропонованої криптовалюти із аналізом складності проведення атак деанонімізації і втрат ефективності анонімних криптовалют у порівнянні із Bitcoin/Litecoin; оцінити та обґрунтувати необхідні ресурси (газ і етер), потрібні для функціонування смарт-контракту.

1 ХІД РОБОТИ

1.1 Методи анонімізації та деанонімізації в Ethereum

Система Ethereum відома своєю відкритістю та децентралізованою природою. Хоча ці характеристики мають багато переваг, вони також означають, що всі транзакції в мережі Ethereum є публічно доступними, дозволяючи будь-кому переглядати деталі операцій, включаючи суму переказу, а також адреси відправника і одержувача. Такий рівень відкритості може створювати суттєві ризики для конфіденційності та безпеки користувачів мережі.

Є кілька способів зберегти конфіденційність у мережі Ethereum, наприклад:

1) Використання приватного гаманця: Одним із найефективніших способів збереження конфіденційності в мережі Ethereum є застосування приватних гаманців. Ці гаманці, також відомі як некастодіальні, дозволяють користувачам повністю контролювати свої кошти та особисті дані. Вони створюють закритий ключ, який зберігається на пристрої користувача і використовується для підписання транзакцій. Це забезпечує, що приватний ключ ніколи не передається третім особам, а доступ до коштів має тільки сам користувач.
2) Використання міксерів: Міксери — це сервіси, що дозволяють користувачам змішувати свої кошти з коштами інших користувачів, ускладнюючи тим самим відстеження джерела транзакцій. Міксери об’єднують кошти, а потім перерозподіляють їх на різні адреси, що значно ускладнює простежування походження транзакцій. Однак, ці сервіси не завжди є надійними, і були випадки втрати коштів користувачами. Тому важливо використовувати міксери з доброю репутацією.
3) Використання децентралізованих додатків (dApps), орієнтованих на конфіденційність: У мережі Ethereum існує кілька dApps, які акцентують увагу на збереженні конфіденційності. Ці додатки застосовують передові криптографічні методи для забезпечення приватності та безпеки транзакцій.

Наприклад, Tornado.cash — це dApp, що спеціалізується на конфіденційних транзакціях, дозволяючи користувачам надсилати та отримувати приватні транзакції в мережі Ethereum. Цей додаток використовує докази з нульовим розголошенням для забезпечення приватності та непростежуваності транзакцій.

Крім цього, в мережі Ethereum впроваджено різні заходи для забезпечення конфіденційності транзакцій користувачів, особливо для приватних транзакцій. Основні методи включають:

- Докази з нульовим знанням (ZKPs): ZKPs є криптографічними доказами, що дозволяють сторонам підтвердити наявність у них певної інформації без її розкриття. Ця технологія дозволяє користувачам підтвердити володіння закритим ключем, не розкриваючи сам ключ, що особливо корисно для конфіденційних операцій.

- Кільцеві підписи: кільцеві підписи надають користувачам можливість підписувати транзакцію без розкриття своєї особи. Це досягається створенням групи потенційних підписантів, після чого транзакція підписується комбінацією підписів учасників групи, що ускладнює визначення справжнього підписанта.

- Транзакції поза ланцюгом: транзакції поза ланцюгом дають змогу користувачам проводити транзакції, не транслюючи їх у загальнодоступну мережу Ethereum. Натомість ці транзакції виконуються поза мережею, а потім остаточно розраховуються в мережі Ethereum, що забезпечує додатковий рівень конфіденційності та безпеки.

- Зашифровані транзакції: зашифровані транзакції – це такі транзакції, які шифруються перед трансляцією в мережу, забезпечуючи, що лише призначений одержувач зможе прочитати вміст транзакції.

Загалом, Ethereum застосовує різні заходи для збереження конфіденційності своїх користувачів, проте існують певні труднощі, зокрема: –

Використання публічних адрес, які можна пов’язати з особою користувача. – Смарт-контракти є публічними та можуть розкривати деталі транзакцій, включаючи суму та залучених сторін. – Система Ethereum підлягає нормативному регулюванню, що може поставити під загрозу конфіденційність користувачів, наприклад, у випадку підозри у використанні Ethereum для незаконної діяльності, правоохоронні органи можуть вимагати розкриття особистої інформації користувача.

Одним із найбільш популярних рішень для підвищення конфіденційності транзакцій на Ethereum є Tornado.cash. Це відкрите програмне рішення, яке не вимагає зберігання даних і використовує докази з нульовим знанням для забезпечення приватності транзакцій у мережі Ethereum. Tornado.cash дозволяє користувачам вносити Ether та інші токени ERC-20 в пул, де вони змішуються з коштами інших користувачів, що ускладнює відстеження джерела конкретної транзакції. Після змішування коштів користувачі можуть вивести їх на нову адресу, що додатково заплутує транзакцію.

Інший спосіб забезпечення конфіденційності на Ethereum - Aztec Protocol. Цей протокол застосовує докази з нульовим знанням для шифрування вхідних і вихідних даних смарт-контрактів, що гарантує конфіденційність їх виконання. Таким чином, деталі транзакцій, включаючи відправника, одержувача та суму переказу, залишаються прихованими від загального доступу. Aztec Protocol також підтримує конфіденційні токени, що дозволяє створювати і передавати активи без розголошення будь-якої інформації про них. Серед інших можливих способів забезпечення анонімності можна виділити такі:

Zether: протокол з відкритим вихідним кодом, що використовує докази з нульовим знанням для забезпечення приватних транзакцій у системі Ethereum. Zether дозволяє користувачам депонувати Ether у смарт-контракт, з якого вони можуть потім вивести кошти на нову адресу, зберігаючи деталі транзакції в таємниці.

Nightfall: протокол, створений Ernst & Young, який застосовує докази з нульовим знанням для забезпечення приватних транзакцій у мережі Ethereum. Nightfall призначений для корпоративних додатків і забезпечує конфіденційність як транзакцій, так і виконання смарт-контрактів.

Enigma: протокол, що використовує безпечні багатосторонні обчислення для забезпечення приватних обчислень у мережі Ethereum. Enigma дозволяє користувачам створювати ринки даних, де вони можуть купувати та продавати дані, не розкриваючи жодної інформації про самі дані.

zk-SNARKs: технологія, яка дозволяє користувачам здійснювати повністю приватні транзакції, видимі лише для одержувачів.

1.2 Анонімність біткоїну

Однією з головних проблем фіатних валют, яку мав вирішити Bitcoin, є відсутність конфіденційності даних про користувачів. Розробник криптовалютної платіжної системи прагнув зробити Bitcoin анонімним. Для цього автор використав технологію децентралізованого зберігання інформації та інші методи підвищення конфіденційності. Проте, досягти повної анонімності Bitcoin не вдалося.

Що робить біткоїн анонімним

Блокчейн зберігає конфіденційність даних користувачів. Анонімність Bitcoin забезпечується такими особливостями мережі:

- **Відсутність прив'язки криптовалютних адрес до користувачів**: Для створення нового гаманця користувачам системи Bitcoin не потрібно надавати особисту інформацію. Вони також можуть створювати необмежену кількість гаманців за потреби.
- **Відсутність прив'язки транзакцій до ініціаторів**: Для проведення криптовалютних переказів власникам BTC не потрібно розкривати особисті дані.

- **Випадковий вибір вузлів для обробки операцій**: Дані про біткоїн-транзакції ретранслюються майнерами в межах мережі. Хоча видобувні вузли взаємодіють через IP-адреси, вони не можуть точно знати, що отримують транзакції безпосередньо від ініціаторів.

Як розкривається анонімність

Конфіденційність користувачів мережі Bitcoin може бути скомпрометована, через що криптовалютна спільнота вважає Bitcoin псевдоанонімною валютою. Існує п'ять способів ідентифікувати особу відправника або одержувача BTC:

- Час**.**
- Джерело коштів**.**
- Граф транзакцій**.**
- Кластеризація**.**
- Евристика**.**

Час

Bitcoin є прозорим цифровим ланцюжком, що дозволяє користувачам вільно доступатися до публічної інформації з блокчейна. Це стає простішим завдяки сервісам моніторингу криптомереж. Використовуючи доступну інформацію, можна визначити місцезнаходження власника певного гаманця за допомогою аналізу. Для цього слід виконати такі кроки:

1. **Вибрати біткоін-транзакцію**.
2. **Скопіювати хеш транзакції**.
3. **Знайти гаманець відправника або одержувача** (залежно від мети) за ідентифікатором транзакції через сервіс моніторингу криптовалютної мережі.
4. **Використовувати отриману адресу гаманця** в просунутому блокчейн-браузері, наприклад, oxt.me.

5. **Визначити період найменшої активності гаманця** (у сервісі моніторингу вказується час за UTC).

Після виконання п'ятого кроку необхідно додати деякий час до знайденого періоду. Наприклад, якщо період найменшої активності припадає на 17:00-22:00 за UTC, варто змістити його на 8 годин вперед. Отримається проміжок з 01:00 до 06:00 за GMT+8. Власник обраного гаманця, найімовірніше, проживає в цьому часовому поясі.

Джерело коштів

У цифрових мережах існує поняття «входи транзакцій», яке представляє історію, звідки криптовалюта надходить на нову адресу, відоме як UTXO (невитрачені виходи транзакцій). Входи транзакцій дозволяють обійти анонімність BTC.

Оскільки біткоїн-перекази утворюють послідовний ланцюжок, UTXO не є адресою гаманця відправника або хешем самої транзакції. Технічно джерело коштів – це невитрачений вихід (одержувач) попередньої транзакції.

Визначити UTXO можна за допомогою просунутих сервісів моніторингу криптомереж. Вони показують повний список входів та виходів Bitcoin-транзакцій і демонструють, як саме відбуваються перекази. Маючи цю інформацію, можна легко дізнатися кількість біткоїнів на гаманці відстежуваного користувача.

Граф транзакцій

Завдяки UTXO, біткоін-перекази формуються в послідовний ланцюжок, відомий у спільноті користувачів цифрових активів як граф транзакцій BTC. За його допомогою можна простежити передачу криптовалюти від одного Bitcoin-гаманця до іншого. Глибина аналізу графа не обмежена, тому учасники

блокчейну Bitcoin можуть відстежити всю історію передачі криптовалюти як до, так і після конкретної угоди.

Деякі адреси відомі громадськості, зазвичай це гаманці відомих особистостей або великих компаній. Коли біткоїни потрапляють на відому адресу, можна точно визначити, кому належить криптовалюта.

Кластеризація

Bitcoin-транзакції можуть мати кілька джерел, включаючи адреси для здачі. Такі адреси автоматично генеруються сервісом, де користувач створив гаманець, і використовуються для повернення здачі на рахунок ініціатора BTC-операції.

У блокчейні Bitcoin цей процес відбувається автоматично і часто непомітний для користувачів. Технічно, загальна кількість монет у гаманці вважається однією "купюрою", і не можна відправити лише її частину. Для здійснення біткоїн-транзакції потрібно надіслати всю "купюру", а залишок повертається як здача, аналогічно до оплати товарів у магазині.

Адреси для здачі та інші UTXO можна групувати. Цей процес називається кластеризацією. Аналітик збирає інформацію про різні джерела коштів, щоб визначити їхню причетність до конкретного гаманця. Зібравши такий кластер, можна припустити, що всі адреси належать одному власнику. У разі розкриття власника однієї адреси буде деанонімізовано всю групу.

Евристичні дані

Час, UTXO, граф транзакцій Bitcoin і кластери разом дозволяють пов'язати одного власника з групою адрес. Уся ця інформація називається "евристичними даними". Вони можуть зменшити анонімність біткоїна. Проте, конфіденційну інформацію все ж можна захистити.

Збереження анонімності біткоїну

Існують три популярні методи для збільшення конфіденційності:

1. **TOR (The Onion Router):** Цей метод використовує браузери, які базуються на технології The Onion Router, щоб підключатися до Інтернету через мережу з багаторівневим шифруванням з'єднань за допомогою 3 ключів. Ключі генеруються випадково під час проходження сигналу через проксі-сервери, що дозволяє приховувати IP-адресу та іншу інформацію користувача.
2. **Міксери (туманізатори):** Це програмне забезпечення дозволяє анонімізувати ініціатора наступних біткоїн-транзакцій. Міксери збирають криптовалюту користувачів і ретельно перемішують її, перекидуючи цифрові активи між різними адресами. У результаті учасники мережі отримують суму назад, що містить внески від різних відправників у різних частинах.
3. **Спеціальні гаманці:** Існують прозорі сховища, які дозволяють анонімно відправляти криптовалюту. Вони забезпечують захист доступу до інформації про адреси та біткоїн-транзакції клієнтів. В таких сховищах у власників є кілька криптогаманців. Після отримання монет одним, вони відправляють аналогічну суму з інших, що робить практично неможливим зв'язок між цими транзакціями.

Як придбати BTC анонімно

Щоб уникнути можливості виявлення особистості власника гаманця, багато інвесторів та трейдерів прагнуть купувати біткоїни анонімно. Існують три основні способи для цього:

- **Мережа Lightning (LN):**
- **Пряме придбання:**
- **Даркнет:**

Використання Мережі Lightning (LN)

LN представляє собою протокол другого рівня або технологію, яка створює платіжні канали над головним блокчейном Bitcoin. Розроблено у 2015 році командою розробників криптовалютної організації Bitcoin Core.

Технологія LN може зберегти анонімність біткоїну з трьох причин:

- BTC-транзакції з платіжних каналів не обов'язково фіксуються у блоках публічного реєстру Bitcoin.
- Використовується технологія TOR для анонімізації.
- Неможливість проведення кластеризації Lightning-транзакцій.

Інші Методи

Щоб зберегти конфіденційність особистих даних, можна купувати монети BTC безпосередньо. Спочатку потрібно знайти продавця та домовитися про умови операції. Рекомендується укласти угоду особисто, щоб знизити ризик шахрайства.

При прямій угоді користувач отримує монети звичайним переказом від відправника. Сам факт покупки не зафіксовується в Інтернеті.

Ще один спосіб збереження конфіденційності - використання послуг сервісів у даркнеті. Однак такі ресурси функціонують напівлегально або незаконно. Крім того, послуги тіньового Інтернету мають великі витрати. Наприклад, місячна підписка на використання напівлегального ресурсу Helix коштує 0,01 BTC, а також потрібно сплачувати комісію у розмірі 2,5% з кожної операції.

Політика криптовалютних бірж щодо анонімності Bitcoin

Більшість популярних криптовалютних торгових платформ вимагають від клієнтів підтвердження особи за допомогою паспорта або іншого

ідентифікаційного документа. Це відбувається під тиском фінансових регуляторів країн, в яких ці біржі діють. Таким чином, торгові майданчики виявляють негативне ставлення до віртуальних активів, які забезпечують повну конфіденційність користувачів.

Важливість газу та етеру у функціонуванні смарт-контрактів

Газ в мережі Ethereum визначає витрати, пов'язані з виконанням транзакцій та смарт-контрактів. Це служить для запобігання зловживання мережею, стимулює майнерів включати транзакції у блоки та забезпечує загальну стабільність мережі.

Оплата за газ виражається в одиницях етеру (ETH), який є основною криптовалютою Ethereum. Gwei, скорочено від "giga" та "wei", представляє собою дрібну одиницю ETH, еквівалентну 0.000000001 ETH. При ініціюванні транзакції або смарт-контракту користувачі встановлюють ціну газу в gwei, яку вони готові сплатити за обчислювальні ресурси, необхідні для обробки їхнього запиту.

Оскільки кількість учасників обмежена, мережа може схвалити тільки обмежену кількість транзакцій, тому майнери зацікавлені в тому, щоб включати транзакції з більшою винагородою. Користувачі підвищують оплату за газ, щоб збільшити пріоритетність своїх транзакцій.

Вартість газу виступає і як засіб забезпечення безпеки мережі. Вона протидіє перевантаженням, що можуть викликати зловмисники або спам-транзакції в мережі. Таким чином, оплата газу є необхідною для забезпечення якості транзакцій у мережі Ethereum.

Ціни на газ постійно змінюються в залежності від завантаженості мережі. Існує багато факторів, що впливають на вартість газу, такі як:

- Складність функції: Складність завдань, що виконуються в мережі Ethereum, впливає на час їх валідації. Кількість ресурсів, які витрачають

валідатори для виконання завдань у мережі, визначає початковий розмір комісії. Зростання складності завдань призводить до збільшення витрат на газ.

- Терміновість транзакцій: Популярність додатків на базі Ethereum призвела до збільшення потреби у їх валідації. Рішення Layer-2 допомагають вирішити це питання, але блокчейн Ethereum все ще обробляє транзакції.
- Стан мережі: Мережа Ethereum має обмежену кількість валідаторів, а низька пропускна здатність (TPS) робить її вразливою до перевантажень в періоди високої активності. Платежі за газ сприяють забезпеченню терміновості транзакцій з більш високим пріоритетом.

Плата за газ складається з двох складових: ціна газу та ліміт газу. Ліміт газу - це максимальна межа, яка обмежує оплату за газ і забезпечує безпеку та запобігає завищенню платежів за транзакції через перевантаження або аномалії.

Плата за газ розраховується за такою формулою:
Плата за газ = Ліміт газу × (Базова комісія + плата за пріоритет)

Повна вартість газу для транзакції може бути визначена шляхом множення ліміту газу на суму базової комісії та, якщо це застосовується, комісії за пріоритет чи чайові. При цьому враховується мінімальна вартість комісії, що складається з базової комісії та додаткових витрат, які можуть бути додані до транзакції для її прискорення.

Навіть при правильних розрахунках, кінцевий розмір платежу за газ може змінюватися. Базова плата може коливатися, а ціна може змінюватися в залежності від попиту у мережі. У разі перевантаження мережі транзакції з більш високою комісією за газ матимуть пріоритет. Для проведення термінових транзакцій користувачі підвищують ціну на газ, щоб забезпечити пріоритетність своєї транзакції.

Ефективне управління витратами на газ у мережі Ethereum потребує стратегічного підходу. Деякі можливі методи оптимізації транзакцій включають:

Інструменти та програми в мережі, такі як etherscan.io, пропонують **калькулятори вартості газу**, які рекомендують оптимальну ціну за газ, враховуючи поточні умови мережі. Ці калькулятори можуть допомогти знайти баланс між швидкістю виконання транзакції та економічною вигодою.

Щоб зекономити на комісіях за газ, рекомендується ініціювати транзакції у часи меншої активності мережі. Зазвичай, в непікові періоди, наприклад, вночі або вихідні дні, плата за газ є нижчою.

Для зменшення комісій та прискорення транзакцій також можна розглянути використання рішень другого рівня, таких як Optimistic Rollups і zk-Rollups. Ці рішення спрямовані на вирішення проблем масштабування Ethereum, переносячи обробку транзакцій поза основною мережею і проводячи розрахунки в надійній мережі другого рівня. Вони можуть значно знизити комісії за газ та час виконання транзакцій, зокрема в мережі L2, яка є більш доступною варіантом з точки зору витрат.

Пакетні транзакції

Певні гаманці та платформи дають можливість збирати кілька окремих транзакцій в одну групову. Цей метод дозволяє економити на витратах за газ, оскільки кілька транзакцій обробляються у межах одного блоку.

Токени газу

Газові токени - це токени, які можна створити, коли ціни на газ низькі, і знищити (спалити), коли ціни на газ високі. Цей механізм дозволяє користувачам захищатися від можливих подорожчань газу в майбутньому.

Ефективність смарт-контрактів

Розробники мають можливість підвищити ефективність смарт-контрактів, щоб зменшити їхнє споживання газу. Це включає в себе такі стратегії, як видалення зайвих операцій зберігання та використання більш продуктивних алгоритмів. Проте цей аспект стосується виключно розробників, а не звичайних користувачів.

ВИСНОВКИ

Ethereum пропонує певний рівень анонімності, але одночасно транзакції у мережі є відкритими для всіх користувачів Інтернету через прозорість блокчейну. У останні роки розробники активно працюють над різними рішеннями, щоб зберегти конфіденційність в мережі Ethereum, проте залишається багато проблем, які треба вирішити.

Одним із запропонованих рішень є використання доказів з нульовим знанням. Ця технологія дозволяє користувачам підтверджувати свою інформацію, не розкриваючи її, що дозволяє проводити приватні транзакції у системі. Проте виникає проблема масштабування, оскільки впровадження нових протоколів потребує значних обчислювальних ресурсів, що може сповільнити роботу системи при великому масштабі. Крім того, існує проблема балансу між конфіденційністю та відповідністю нормативним вимогам.

З ростом та розвитком мережі ймовірно, що питання конфіденційності стане ще важливішим. Працюючи разом, розробники та користувачі можуть забезпечити, що мережа Ethereum залишається безпечним і захищеним середовищем.

Незважаючи на відсутність прив'язки транзакцій та гаманців до користувачів, мережа Bitcoin також псевдоанонімна. Конфіденційність інформації можна порушити за допомогою методів евристики, де ключову роль відіграють джерела коштів — невитрачені виходи попередніх транзакцій (UTXO).

Щоб зберегти анонімність Bitcoin, можна використовувати:

- The Onion Router для шифрування інтернет-з’єднання.
- Міксери для перемішування UTXO.
- Непрозорі гаманці, що приховують персональну інформацію користувачів.
- Технологія Lightning Network, яка є протоколом другого рівня системи Bitcoin.

Плата за газ Ethereum є необхідною для функціонування мережі. Хоча це може створювати певні труднощі, вона також свідчить про популярність та корисність Ethereum. Розуміючи фактори, які впливають на газові комісії, та впроваджуючи стратегії оптимізації, користувачі можуть ефективніше орієнтуватися в екосистемі Ethereum та отримувати максимальну вигоду від її інноваційних додатків.