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 ФІ-32мн
Мельник Ілля,
Міснік Аліна

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 прозорістю та децентралізацією. Хоча ці функції мають багато переваг, вони також означають, що транзакції в системі Ethereum є загальнодоступними, і будь-хто може переглянути деталі транзакції, включаючи суму переказу та адресу відправника та одержувача. Така відсутність конфіденційності може становити значний ризик для безпеки мережі та ідентифікації користувачів.

Є кілька способів зберегти конфіденційність у мережі Ethereum, наприклад:

1) Використання приватного гаманця: одним із найефективніших способів збереження конфіденційності в системі Ethereum є використання приватного гаманця. Приватні гаманці, також відомі як некастодіальні гаманці, дозволяють користувачам повністю контролювати свої кошти та особисті дані. Вони генерують закритий ключ, який зберігається на пристрої користувача, який використовується для підписання транзакцій. Це означає, що приватний ключ ніколи нікому не надається, а користувач є єдиним, хто може отримати доступ до своїх коштів.

2) Використання міксерів: міксер — це служба, яка дозволяє користувачам змішувати свої кошти з коштами інших користувачів, що ускладнює відстеження джерела коштів. Змішувачі працюють, об'єднуючи кошти, а потім перерозподіляють їх на різні адреси, що ускладнює відстеження походження транзакцій. Міксери не є надійними, і були випадки, коли користувачі втрачали свої кошти. Тому вкрай важливо користуватися послугами міксерів з хорошою репутацією.

3) Використання dApp (децентралізовані програми), орієнтованих на конфіденційність: у системі Ethereum є кілька dApp, які зосереджені на збереженні конфіденційності. Ці програми використовують передові

криптографічні методи, щоб забезпечити приватність і безпеку транзакцій. Наприклад, Tornado.cash — це dApp, орієнтований на конфіденційність, який дозволяє користувачам надсилати та отримувати приватні транзакції в системі Ethereum. dApp використовує докази з нульовим знанням, щоб гарантувати, що транзакції є приватними та непростежуваними.

Крім цього, Ethereum запровадила різні заходи, щоб транзакції користувачів не були загальнодоступними, особливо якщо вони проводять конфіденційні транзакції. Серед цих заходів можна виділити такі основні методи:

1) **Докази з нульовим знанням (ZKPs):** ZKPs — це криптографічні докази, які дозволяють сторонам довести, що вони мають певну інформацію, не розкриваючи цю інформацію. Ця технологія дозволяє користувачам підтвердити право власності на закритий ключ, не розкриваючи сам ключ. Це особливо корисно для конфіденційних операцій.

2) **Кільцеві підписи:** кільцеві підписи дозволяють користувачам підписувати транзакцію, не розкриваючи свою особу. Це робиться шляхом створення групи можливих підписантів, а потім підписання транзакції комбінацією підписів учасників групи. Через це будь-кому важко визначити, хто насправді підписав транзакцію.

3) **Транзакції поза ланцюгом:** транзакції поза ланцюгом дозволяють користувачам проводити транзакції, не транслюючи їх у загальнодоступну мережу Ethereum. Натомість транзакції проводяться поза мережею, а потім розраховуються в мережі Ethereum. Це забезпечує додатковий рівень конфіденційності та безпеки.

4) **Зашифровані транзакції:** зашифровані транзакції – це транзакції, які шифруються перед трансляцією в мережу. Це гарантує, що лише призначений одержувач зможе прочитати транзакцію.

Загалом система Ethereum вживає значних заходів для збереження конфіденційності своїх користувачів, однак існують також і деякі труднощі, зокрема:

– Ethereum використовує публічні адреси, які можна пов'язати з

особистістю користувача.

– Смарт-контракти є публічними та можуть розкривати деталі транзакції, включаючи суму та залучених сторін.

– Система Ethereum підлягає нормативній відповідності, що може поставити під загрозу конфіденційність користувачів. Наприклад, якщо користувача підозрюють у використанні Ethereum для незаконної діяльності, його особисту інформацію можуть вимагати правоохоронні органи.

Одним із найпопулярніших рішень для підвищення конфіденційності транзакцій на Ethereum є Tornado.cash. Це рішення з відкритим вихідним кодом, яке не вимагає зберігання, і використовує докази з нульовим знанням, щоб допомогти користувачам здійснювати приватні транзакції в 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 будь-якої конкретної транзакції. Після того, як кошти змішані, користувачі можуть вивести їх на нову адресу, що допомагає ще більше заплутати транзакцію.

Іншим рішенням для збереження конфіденційності на Ethereum є Aztec Protocol. Цей протокол забезпечує конфіденційність для виконання смарт-контракту, використовуючи докази з нульовим знанням для шифрування вхідних і вихідних даних смарт-контракту. Це означає, що деталі транзакції, включаючи відправника, одержувача та суму переказу, зберігаються прихованими від публічної книги. Aztec Protocol також підтримує конфіденційні токени, що дозволяє створювати та передавати активи без розкриття будь-якої інформації про них.

Серед інших можливих способів забезпечення анонімності є також наступні:

1) **Zether:** протокол із відкритим вихідним кодом, який використовує докази з нульовим знанням для забезпечення приватних транзакцій у системі Ethereum. Zether дозволяє користувачам вносити Ether у смарт-контракт, який вони потім можуть вивести на нову адресу,

зберігаючи деталі транзакції конфіденційними.

2) **Nightfall:** протокол, розробленний Ernst & Young, який використовує докази з нульовим знанням для забезпечення приватних транзакцій у мережі Ethereum. Nightfall розроблено для роботи з додатками корпоративного рівня, він забезпечує конфіденційність як для транзакцій, так і для виконання смарт-контрактів.

3) **Enigma:** протокол, який 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.

4) **zk-SNARKs:** використовуючи цю технологію, користувачі можуть надсилати повністю приватні транзакції, які бачать лише одержувачі.

1.2 Анонімність біткоїну

Однією з основних проблем фіату, для вирішення яких створювався Bitcoin, є відсутність конфіденційності інформації про користувачів. Розробник криптовалютної платіжної системи прагнув зробити Біткоїн анонімним. Для цього автор використовував технологію децентралізованого зберігання інформації та інші методи підвищення конфіденційності. Проте абсолютної анонімності біткоїну досягти не вдалося.

Що робить біткоїн анонімним

Блокчейн зберігає конфіденційність даних користувачів. Анонімність Bitcoin обумовлюють такі особливості мережі:

– **Відсутність прив'язки криптовалютних адрес (номерів) до користувачів.** Для створення нового сховища учасникам системи Біткоїн не потрібно вказувати особисту інформацію. Також вони можуть створювати гаманці у будь-якій кількості, коли потрібно.

– **Відсутність прив'язки біткоін-транзакцій до їх ініціаторів.** Для здійснення криптовалютного перекладу власникам BTC також не

потрібно вказувати персональну інформацію.

– **Випадковість вибірки вузлів (нід) для обробки операцій.** Дані про біткоін-транзакції ретранслюються майнерами всередині мережі. Хоча видобувні вузли зв'язуються між собою через IP-адреси, вони не можуть бути впевнені, що одержують на обробку перекази від їхніх ініціаторів.

Як розкривається анонімність

Конфіденційність користувачів мережі Біткоїн може бути порушена. Через це криптовалютне ком'юніті вважає систему Bitcoin псевдоанонімною монетою. Існує 5 способів ідентифікувати особистість відправника або одержувача BTC:

– Час.

– Джерело коштів.

– Граф транзакцій.

– Кластеризація.

– Евристика.

Час

Bitcoin – прозорий цифровий ланцюжок. Користувачі можуть вільно брати публічну інформацію з блокчейна, якщо потрібно. Робити це простіше через послуги моніторингу криптомереж.

Використовуючи публічну інформацію, методом аналізу можна визначити територію, де проживає власник обраного гаманця. Для цього потрібно:

1) Вибрати біткоін-транзакцію.

2) Копіювати хеш перекладу.

3) Знайти гаманець відправника або одержувача (залежно від мети) по ідентифікатору біткоін-транзакції через сервіс моніторингу криптовалютної мережі.

4) Використовувати отриману адресу гаманця в просунутому браузері блокчейна на кшталт oxt.me.

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

Після п'ятого кроку потрібно додати деякий час до знайденого проміжку. Наприклад, якщо в середньому період найменшої активності був з 17:00 до 22:00 за UTC, варто відсунути його на 8 годин у більшу сторону. Тоді вийде проміжок з 01:00 до 06:00 за GMT+8. На території цього часового поясу, найімовірніше, і проживає власник вибраного гаманця.

Джерело коштів

У цифрових мережах є поняття «входи транзакцій». Вони є своєрідною історією, звідки криптовалюта приходить на нову адресу, — UTXO (джерелом коштів). Входи транзакцій дозволяють оминати анонімність BTC.

Оскільки біткоін-перекладі складаються в послідовний ланцюжок, UTXO не є адресою гаманця відправника або хешем самої транзакції. Технічно джерело коштів – це невитрачений вихід (одержувач) попереднього переказу.

Визначити UTXO можна, використовуючи просунуті моніторинг-сервіси криптомереж. Вони показують весь список входів та виходів Bitcoin-транзакцій та те, як насправді виробляються перекладі. З цією інформацією легко дізнатися кількість біткоїнів на гаманці відстежуваного користувача.

Граф транзакцій

Завдяки UTXO біткоін-перекладі збираються в ланцюжок. У спільноті користувачів цифрових активів вона називається графом транзакцій BTC. Через нього можна відстежити передачу криптовалюти з Bitcoin-гаманця A до сховища B. При цьому глибина використання графа не обмежена. Учасники блокчейну Bitcoin можуть відстежити повну історію передачі криптовалюти до і після конкретної угоди.

Власники деяких адрес відомі громадськості. Здебільшого це номери сховищ популярних особистостей чи великих компаній. Коли біткоїни надійдуть на відому адресу, можна буде точно сказати, кому належить криптовалюта.

Кластеризація

Bitcoin-перекладі можуть мати кілька джерел. До них часто входять

адреси здачі. Такі номери автоматично генеруються сервісом, де користувач створив гаманець. Вони потрібні для переведення здачі на рахунок ініціатора BTC-операції.

У блокчейні Bitcoin цей процес відбувається автоматично та часто непомітний його учасникам. З технічного погляду загальна кількість монет у сховищі є однією «купюрою». Не можна відправити лише її частину. Для проведення біткоін-транзакції потрібно надіслати цілу купюру. Залишок суми повертається як здавання. Цей принцип аналогічний до оплати товарів у магазині.

Біткоїн-адреси здачі та інші UTXO можна збирати до груп. Цей процес називається кластеризацією. Аналітик збирає інформацію про різні джерела коштів, щоб визначити їхню причетність до фінансування конкретного гаманця. Зібравши такий кластер, можна припустити, що вони належать до спільного господаря. У цьому розкриття власника однієї адреси призведе до деанонімізації всієї групи.

Евристичні дані

Час, UTXO, граф Bitcoin-транзакцій та кластери разом дозволяють пов'язати одного власника з групою адрес. Вся ця інформація називається «евристичними даними». Вони здатні знизити анонімність біткоїну. Однак конфіденційну інформацію можна захистити.

Як зберегти анонімність біткоїну

Існує 3 популярні методи збільшення конфіденційності:

1) **TOR.** Браузери на основі технології The Onion Router використовують для підключення до інтернету багаторівневе шифрування з'єднання 3 ключами. Вони генеруються випадково при проходженні сигналу через проксі-сервери (проміжні ланки між користувачем та мережею). Tor дозволяє приховувати IP-адресу та будь-яку іншу інформацію.

2) **Міксери.** За допомогою такого ПЗ можна анонімізувати ініціатора наступних біткоін-транзакцій. Міксери збирають криптовалюту користувачів і ретельно перемішують її, переганяючи цифрові активи за різними адресами.

В результаті учасники мережі отримують вкладену суму назад, але від різних відправників та частинами.

3) **Спеціальні гаманці.** Існують непрозорі сховища, якими можна анонімно відправляти криптовалюту. Вони закривають доступ до інформації про адреси та біткоін-транзакції клієнтів. В цьому випадку у власників сервісу є кілька криптогаманців. Отримавши монети однією, вони відправляють аналогічну суму з інших. Внаслідок цього практично неможливо пов'язати ці транзакції.

Як купити BTC анонімно

Зловмисники можуть встановити особу власника гаманця кількома методами. З цієї причини багато інвесторів і трейдерів намагаються купувати біткоїни анонімно. Є 3 основних способи:

– Lightning Network (LN).

– Пряме придбання.

– Даркнет.

Lightning Network

LN — протокол другого рівня або технологія створення платіжних каналів поверх головного блокчейна монети BTC. Lightning Network створено у 2015 році командою розробників криптовалютної організації Bitcoin Core.

Технологія LN здатна зберегти анонімність біткоїну з трьох причин:

– BTC-транзакції з платіжних каналів не обов'язково включати до блоків публічного реєстру Bitcoin.

– Використовується технологія TOR для анонімізації.

– Немає можливості провести кластеризацію Lightning-транзакцій.

Інші способи

Щоб зберегти конфіденційність персональних даних, можна придбати монети BTC безпосередньо. Спочатку потрібно знайти продавця та домовитися про умови здійснення операції. Рекомендується наполягати на угоді під час особистої зустрічі. Такий підхід дозволить знизити ризик шахрайства.

За прямої угоди користувач отримує монети звичайним переказом від відправника. Сам факт покупки не фіксується в Інтернеті.

Ще один спосіб зберегти конфіденційність – використання послуг сервісів у даркнеті. Проте такі ресурси працюють напівлегально чи незаконно. Також послуги з тіньового інтернету беруть велику плату за свої послуги. Наприклад, місячна підписка на використання напівлегального ресурсу Helix коштує 0,01 BTC, а також потрібно віддавати комісію 2,5% з кожної операції.

Політика бірж щодо анонімності Bitcoin

Більшість популярних криптовалютних торгових платформ зобов'язують клієнтів верифікувати особу за паспортом або іншим документом. Це вібдувається через тиск фінансових регуляторів країн, в яких біржі ведуть свою діяльність. Тому торгові майданчики негативно ставляться до віртуальних активів, що зберігають повну конфіденційність користувачів.

1.3 Роль газу і етеру у функціонуванні смарт-контракту

Газ – це витрати, пов'язані з виконанням транзакцій і смарт-контрактів в мережі Ethereum. Вони слугують механізмом запобігання зловживанню мережею, стимулюють майнерів включати транзакції в блоки і забезпечують загальну стабільність мережі.

Плата за газ виражається в «гвеях», одиницях етеру (ETH), який є рідною криптовалютою Ethereum. Gwei – це скорочення від "giga" і "wei", що означає 0.000000001 ETH. Ініціюючи транзакцію або смарт-контракт, користувачі встановлюють ціну газу в gwei, яку вони готові заплатити 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 плату за газ, щоб збільшити пріоритет своїх транзакцій.

Плата за газ також виступає як механізм забезпечення безпеки мережі. Вона запобігає перевантаженням, які викликають зловмисники або спам-транзакції в мережі. Тобто плата також потрібна для підтримки якості транзакцій у мережі.

Ціни на газ Ethereum постійно коливаються в залежності завантаженості мережі. Існує багато факторів, які впливають на вартість газу, наприклад:

– **Складність функції:** Складність функції, представленої в мережі Ethereum, впливає на час валідації. Кількість зусиль, докладених валідаторами для виконання завдання в мережі, визначає початковий розмір комісії. Багатофункціональність збільшує складність, вимагаючи більше обчислювальних потужностей і вищу плату за газ.

– **Терміновість транзакцій:** Зростаюча корисність додатків на основі Ethereum створила підвищену потребу у валідації. Рішення Layer – 2 в мережі допомагають вирішити цю проблему. Тим не менш, блокчейн Ethereum все ще виконує розрахунки за транзакцією.

– **Стан мережі:** Мережа Ethereum має обмежену кількість валідаторів, а низький показник TPS (транзакцій в секунду) робить її схильною до перевантажень в періоди високої завантаженості. Система підтримується за рахунок газових платежів, які в першу чергу задовольняють термінові транзакції з більш високим пріоритетом. Стан мережі визначає ціни на газ, оскільки перевантажена мережа неодноразово задовольняє заявки з вищими комісіями, перш ніж приймати транзакції з базовими комісіями або без комісій.

Плата за газ складається з двох компонентів: ціни газу та ліміту газу. Ліміт плати за газ – це її жорстке обмеження, що поширюється на такі дії в мережі Ethereum, як надсилання етеру з одного гаманця в інший і виконання смарт-контрактів. Ліміт – це максимальна межа в гаманці, що дозволяє стягувати плату в мережі. Ліміт забезпечує безпеку і запобігає завищенню плати за транзакції через перевантаженість або аномалії.

Коли користувач ініціює транзакцію в мережі Ethereum, він вказує

кількість газу, яку готовий заплатити за її виконання. Базова ставка комісії – це вартість одиниці газу.

Загальний розмір плати за газ можна розрахувати за такою формулою:

$$\text{Плата за газ} = \text{Ліміт газу} \times (\text{Базова комісія} + \text{плата за пріоритет})$$

Загальну комісію за газ для транзакції можна розрахувати, помноживши ліміт газу на суму базової комісії та комісії за чайові (якщо вони застосовуються). При цьому враховується мінімальна вартість комісії, тобто базова комісія та комісія за пріоритет або чайові, які додаються до транзакції для прискорення її виконання.

Навіть за умови правильних розрахунків, остаточний розмір плати за газ може змінюватися. Базова плата коливається, і ціна може змінюватися в залежності від попиту в мережі. Якщо мережа перевантажена, транзакції з вищою платою за газ матимуть пріоритет. Для виконання термінових транзакцій користувачі підвищують ціну на газ, щоб зробити свою транзакцію пріоритетною.

Навігація зменшенню трати на газ в Ethereum вимагає стратегічного підходу. Можливі методи оптимізації транзакцій:

Калькулятори вартості газу

Різні онлайн-інструменти та гаманці надають калькулятори вартості газу (як приклад etherscan.io), які рекомендують відповідну ціну на газ, виходячи з умов мережі. Ці калькулятори можуть допомогти знайти баланс між швидким виконанням транзакції та економічною ефективністю.

Використання в непікові періоди

Ініціюйте транзакції в періоди меншої активності мережі. Плата за газ, як правило, нижча в непікові періоди – для України це ніч, вихідні.

Рішення другого рівня

Рішення для масштабування другого рівня, такі як Optimistic Rollups і zk-Rollups, спрямовані на вирішення проблем масштабування Ethereum шляхом обробки транзакцій поза мережею і проведення розрахунків у

мережі. Ці рішення можуть значно зменшити комісію за газ і час транзакцій. Якщо є вибір, в якій мережі виконувати транзакції, то краще в дешевших L2.

Пакетні транзакції

Деякі гаманці та платформи дозволяють користувачам об'єднувати декілька транзакцій в одну. Такий підхід дозволяє заощадити на витратах на газ, оскільки кілька транзакцій обробляються в одному блоці.

Газові токени

Газові токени – це токени, які можна карбувати, коли ціни на газ низькі, і спалювати (знищувати), коли ціни на газ високі. Цей механізм дозволяє користувачам хеджувати майбутні підвищення цін на газ.

Ефективність смарт-контрактів

Розробники можуть оптимізувати смарт-контракти для мінімізації споживання газу. Це включає в себе такі методи, як скорочення непотрібних операцій зберігання та використання більш ефективних алгоритмів. Цей варіант не стосуєтья звичайних користувачів, а тільки розробників.

ВИСНОВКИ

Ethereum забезпечує певний ступінь анонімності, однак прозорість блокчейну також означає, що всі транзакції видимі будь-кому в Інтернеті. Останніми роками розробники працювали над різними рішеннями для збереження конфіденційності в мережі Ethereum, але все ще є багато проблем, які потрібно вирішити.

Одним із запропонованих рішень є використання доказів з нульовим знанням. Ця технологія дозволяє користувачеві довести, що він володіє певною інформацією, фактично не розкриваючи цю інформацію, що дає можливість здійснювати приватні транзакції в системі.

Однак виникає проблема масштабованості, оскільки впровадження нових протоколів вимагає значних обчислювальних ресурсів, які можуть уповільнити роботу системи, якщо їх запровадити у великому масштабі. Крім того, існує проблема балансу між конфіденційністю та дотриманням нормативних вимог.

Оскільки мережа продовжує рости та розвиватися, ймовірно, що питання конфіденційності ставатиме дедалі важливішим. Працюючи разом, розробники та користувачі можуть гарантувати, що система Ethereum залишається безпечним і захищеним місцем.

Незважаючи на відсутність прив'язок даних транзакцій та гаманців до користувачів, мережа Bitcoin також псевдоанонімна. Конфіденційність інформації можна порушити, використовуючи методи евристики. Головну роль цьому відіграють джерела коштів — невитрачені виходи попередніх транзакцій — UTXO.

Зберегти анонімність біткоїну допоможуть:

– **The Onion Router.** Технологія багаторівневого шифрування інтернет-з'єднання.

– **Міксери.** Програмне забезпечення для перемішування UTXO.

– **Непрозорі гаманці.** Сховища, які закривають доступом до

персональної інформації користувачів.

– **Технологія Lightning Network.** Протокол другого рівня системи Біткоїн.

Плата за газ Ethereum є невід'ємним аспектом функціонування мережі. Хоча це може створювати певні труднощі, вона також є свідченням популярності та корисності Ethereum. Розуміючи фактори, які впливають на газові комісії, та впроваджуючи стратегії оптимізації, користувачі можуть ефективніше орієнтуватися в екосистемі Ethereum та отримувати максимальну віддачу від її інноваційних додатків.