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

Звіт з виконання комп'ютерного практикуму №2

РЕАЛІЗАЦІЯ СМАРТ-КОНТРАКТУ АБО АНОНІМНОЇ КРИПТОВАЛЮТИ

Виконали студенти
групи ФІ-32мн
Пелешенко Любов,
Панасюк Єгор,
Маринін Іван Павло

Перевірила:
Селюх П.В.

Київ — 2024

1

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

Постановка задачі: 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.

1.1 Анонімізація та деаномізація

У сучасному світі криптовалюта і, як наслідок, технологія блокчейн набувають все більшого інтересу і широко використовуються. Дуже часто такий інтерес пояснюється тим, що технологію блокчейн, так само як і криптовалюта, часто називають не тільки децентралізованими, але й анонімними.

Тому нам пропонується так званий острів свободи в нашому цифровому світі, що розвивається та контролюється. Необхідно розуміти, наскільки можна забезпечити анонімність, які рішення існують і як вони працюють. Зауважимо, що не всі криптовалюти та блокчейни здатні забезпечити анонімність користувачів. Вивчати питання необхідно з двох сторін, як з позиції можливої реалізації максимальної анонімності, так і можливої деанонімізації користувачів мережі.

Анонімність описує ситуації, коли фігура діючої особи невідома. Анонімність можна розглядати як технологію або спосіб реалізації специфічних інших цінностей, таких як конфіденційність або свобода.

Деанонімізація — це технологія аналізу даних, яка повторно ідентифікує зашифровану або узагальнену інформацію. Деанонімізація

також перехресно посилається на анонімну інформацію з іншою доступною інформацією, щоб ідентифікувати особу, транзакцію чи групу.

Анонімні транзакції, завдяки використанню цього типу протоколів блокчейну, які користувачі можуть безпечно витрачати, знаючи, що інші не можуть стежити за їхніми балансами або відстежувати транзакційну активність.

Це допущення здійснення транскордонних переказів між будь-якими юрисдикціями, визначення напряму переказів та їх кількості для ухилення від сплати податків, надає можливості для подолання режимів санкцій.

Розглянемо існуючі рішення, що забезпечують анонімність користувачів криптовалюти Loki, що була створена як форк Monero.

Monero (XMR) — криптовалюта з відкритим вихідним кодом, протокол, що реалізує ряд технік анонімізації транзакцій: стелс-адресу, кільце конфіденційних транзакцій (RingCT). Запуск Monero відбувся в квітні 2014 року під назвою BitMonero. Протокол базується на кодовій базі проектів CryptoNote і Bytecoin. Згодом назву змінили. Ще в 2012 році розробник Ніколас ван Саберхаген представив CryptoNote.

Loki (LOKI) – була створена як форк Monero, яка вважається однією з анонімних та конфіденційних криптовалют. Розробники Loki намагаються створити абсолютно анонімну, конфіденційну, безпечну мережу для спілкування та торгівлі. Loki застосував надійну технологію Monero для захисту конфіденційності своїх користувачів, таку як кільцеві підписи, RingCT і стелс-адресу. Разом з цим Loki використовує Lokinet (Мережа маршрутизації Onion) і Blink (Миттєві транзакції).

Як можна зрозуміти, вищезазначені криптовалюти використовують велику кількість різноманітних протоколів, алгоритмів і сервісів, які спрямовані на забезпечення анонімності користувачів та їх діяльності, тож розглянемо їх.

CryptoNote – це протокол прикладного рівня, на основі якого базується весь спектр анонімних криптовалют. Найбільш відомі з них - Bytecoin і Monero. Анонімність у CryptoNote реалізована за допомогою

кільцевих конфіденційних транзакцій (RingCT) (приховати відправника) та стелс-адреси (приховати одержувача).

Ring signature (кільцевий підпис) – це електронний підпис, який дозволяє одному учаснику групи (так зване «кільце») підписати певне повідомлення від імені всієї групи, при цьому ніхто не буде знати напевно, хто його підписав.

Ring confidential transactions (RingCT) – RingCT представляє вдосконалену версію кільцевих підписів під назвою «Багатошаровий зв'язуваний спонтанний анонімний груповий підпис», який дозволяє визначати приховані суми, джерела та призначення транзакцій з прийнятною ефективністю та генерувати монети, які можна перевірити. RingCT було запроваджено в січні 2017 року.

Stealth-address (стелс-адреса) – це один із стандартних способів приховати платежі, незважаючи на те, що Blockchain є відкритою базою адрес. На відміну від CoinJoin і CoinShuffle, він не використовує техніку плутанини; приховування досягається за допомогою протоколу Діффі-Хеллмана.

Все більше і більше інтернет-магазинів пропонують використовувати Bitcoin для платежів. Однією з найважливіших особливостей цієї технології є анонімність: хоча транзакції є письмовими та загальнодоступними, вони пов'язані лише з електронною адресою. Тому відстежити покупця неможливо.

Але слід розуміти, що ця анонімність далеко не ідеальна. Фахівці називають це псевдонімною конфіденційністю, як і псевдоніми артистів. Ви можете залишатися анонімним, доки ваш псевдонім не буде пов'язано з вами. Але як тільки хтось дізнається, що це ви написали книгу, ваша анонімність перестає працювати. Так само, як тільки ваша адреса в мережі біткойн буде підключена до ваших особистих даних, історія ваших покупок буде розкрита. Саме тому з'явилися рішення, які вивчаються в статті.

Завдяки роботі Стівена Голдфедера та його колег з Прінстонського університету ми нарешті отримали відповідь. За їхніми словами, навіть

використовуючи додатковий захист конфіденційності, такий як CoinJoin, витік інформації під час покупки значно спрощує мережеве спілкування покупців та їхні транзакції з біткойнами.

У цьому винні веб-трекери та файли cookie. Це невеликі частини коду, спеціально вбудовані у веб-сторінки для надсилання інформації про дії користувачів третім особам. Широко розповсюджені трекери допомагають Google, Facebook та іншим відстежувати навігацію веб-сайтами, кількість покупок, звички перегляду тощо. Деякі трекери надсилають особисті дані, як-от ім'я користувача, місцезнаходження та адресу електронної пошти. В результаті інформація про операції з'являється в мережі.

Стівен Голдфедер і його колеги дізналися та довели, як легко цю інформацію можна використовувати для деанонімізації людей за їхніми чистими транзакціями. Сам процес вимагає прослуховування телефонних розмов, щоб дізнатися особисту інформацію, як-от ім'я чи електронну пошту, і зв'язати її з певною адресою Bitcoin. Команда почала зі складання списку великих компаній, які використовують біткойн-транзакції. Список включає 130 компаній, включаючи Microsoft, NewEgg і Overstock. Після цього вони вивчили, як веб-трекери зливають інформацію з сайту кожної компанії під час покупки.

Але навіть якщо певна транзакція не опублікована, можна створити посилання, використовуючи обсяг і час покупки; вебхуку потрібно лише конвертувати суму покупки в біткойни за обмінним курсом на момент покупки та знайти транзакцію з цією сумою в цей момент. Таким чином розкривається адреса користувача. Будь-які подальші покупки з цієї адреси буде дуже легко відстежити. Все це робить це поганою новиною для тих людей, які сподіваються уникнути визнання в мережі.

На практиці існує кілька способів пов'язати користувача з його псевдонімом Bitcoin. Найбільш часто досліджувані методи аналізують шаблони транзакцій у загальнодоступному блокчейні та пов'язують ці шаблони за допомогою додаткової інформації. У цій статті нас цікавить вразливість нижнього рівня: мережевий стек. Як і більшість криптовалют,

біткойн-ноди спілкуються через мережу P2P. Щоразу, коли користувач (Аліса) генерує транзакцію (тобто надсилає біткойни іншому користувачеві, Бобу), вона спочатку створює «повідомлення про транзакцію», яке містить її псевдонім, псевдонім Боба та суму транзакції. Згодом Аліса передає це повідомлення транзакції через мережу P2P, що дозволяє іншим користувачам підтвердити її транзакцію та включити її до глобального блокчейну. Наслідки трансляції транзакцій щодо анонімності в основному ігнорувалися донедавна, коли дослідники продемонстрували практичні атаки деанонімізації на мережу P2P. Ці атаки використовують «супервузол» для підключення до всіх активних біткойн-вузлів і прослуховування транзакційного трафіку, який вони ретранслюють. Використовуючи прості оцінки для визначення IP-адреси джерела кожної трансляції трансакції, цей зловмисник-підслуховувач зміг пов'язати IP-адреси з псевдонімами біткойн з точністю до 30%. Такий зв'язок і називається деанонімізацією. У 2015 році біткойн-спільнота відповіла на ці атаки, змінивши свої протоколи флуду з протоколу в стилі пліток, відомого як trickle spreading, на протокол дифузійного поширення, який поширює вміст із незалежними експоненційними затримками. Однак жодної системної мотивації цього зсуву не було. Дійсно, незрозуміло, чи справді зміна захищає від атак деанонімізації.

1.2 Функціонування смарт-контракту

Розуміння нюансів смарт-контрактів Ethereum вимагає поглибленого вивчення їх життєвого циклу. Життєвий цикл смарт-контракту охоплює всі етапи, які проходить контракт, від його початкової розробки до остаточного виконання або припинення в блокчейні. Він надає безцінну інформацію про те, як формулюються, перевіряються, взаємодіють і, зрештою, укладаються контракти, відображаючи код, який перетворюється на непорушну угоду. Життєвий цикл смарт-контракту:

– створення, перш ніж контракт буде реалізовано, він проходить

численні ітерації, сеанси налагодження та ретельний аудит. Цей етап є життєво важливим для того, щоб переконатися, що контракт не містить вразливостей, які в історії призводили до значних порушень, таких як атака DAO;

– розгортання, після ретельної розробки та тестування контракти розміщуються в мережі Ethereum. За розгортання стягується «газова» комісія, яка сплачується в Ефірі і залежить від складності контракту та перевантаженості мережі;

– виклик методу, після того, як контракт створений і активний, він очікує на взаємодію. Ці взаємодії можуть відбуватися через автоматичні тригери, встановлені іншими контрактами, або через дії, ініційовані користувачем. Кожна взаємодія з контрактом реєструється як транзакція в блокчейні і, як правило, потребує газу для виконання

Віртуальна машина Ethereum (EVM) є життєво важливим компонентом екосистеми Ethereum і слугує децентралізованим виконавчим середовищем, що відповідає за рівномірну обробку смарт-контрактів у всій мережі Ethereum. Відзначений Тьюрінг-повнотою, EVM має здатність виконувати будь-який алгоритм, незалежно від його складності. Кожна дія, від простих переказів Ефіру до більш складних функцій смарт-контракту, проходить перевірку кожним вузлом мережі, забезпечуючи консенсус щодо стану контракту і будь-яких подальших змін. Для полегшення цих операцій EVM використовує «газову» систему, яка не лише монетизує обчислення, але й забезпечує ефективне кодування та винагороджує прихильників мережі. Надаючи пріоритет безпеці, EVM ізолює кожен смарт-контракт, таким чином захищаючи мережу в цілому від потенційних вразливостей в окремих контрактах. Більше того, коли розробники використовують такі мови, як Solidity або Vyper, для створення застосунків Ethereum, вони генерують байт-код – серію відкритих кодів, які інтерпретуються EVM. В рамках EVM контракти розрізняють сховище, яке зберігає дані між викликами, і пам'ять, яка є ефемерною і скидається після кожної функції. Розуміння цих відмінностей, особливо з точки зору витрат на газ, є вкрай

важливим, оскільки операції, керовані сховищем, зазвичай споживають більше газу, ніж ті, що пов'язані з пам'яттю.

У мережі Ethereum газ відіграє ключову роль у забезпеченні належного функціонування транзакцій і смарт-контрактів. Газ є одиницею виміру обчислювальних ресурсів, необхідних для виконання певних дій в мережі, таких як виконання функцій смарт-контрактів:

– газ, як одиниця виміру обчислювальних зусиль, необхідних для виконання операцій або смарт-контрактів. Концепція газу в Ethereum не тільки є фундаментальною для її функціональності, але й слугує захисним механізмом від зловживань у мережі. Кожна операція в Ethereum, від простої транзакції до виконання складного смарт-контракту, вимагає певної кількості обчислювальних ресурсів. Газ кількісно оцінює ці обчислювальні зусилля, гарантуючи, що кожна дія має вартість, пропорційну споживаним ресурсам. Вартість газу не є статичною, а коливається залежно від попиту на обчислювальні потужності та пропускної здатності мережі

– Wei і Gwei, хоча газ є одиницею обчислення, платежі за ці обчислення здійснюються у валютних одиницях Ethereum. Wei – це найменший номінал валюти Ethereum. Gwei – це просто зручне позначення Wei, що дорівнює 10^9 Wei.

Операція	**Вартість газу**
Базова транзакція	21,000
Складні контрактні операції	Від 30,000
Запис до сховища стану	20,000
SSTORE якщо значення = 0	5,000
Операція SLOAD	800
Операції ADD/SUB/MULT/DIV	Від 3 до 5
Операція LOG	Від 375 до 8,750

Таблиця 1.1 – Вартість газу для різних операцій

Користувачі встановлюють «ціну газу» в Gwei, коли надсилають транзакцію, представляючи кількість Wei, яку вони готові заплатити за кожну одиницю газу. Таким чином, загальна вартість транзакції в Wei розраховується шляхом множення ціни газу на кількість газу, спожитого в

ході транзакції

Номінал	**Значення у Wei**
Wei	1
Gwei	10^9
Ether	10^{18}

Таблиця 1.2 – Перерахунок одиниць Ethereum

Газ є джерелом життєдіяльності мережі Ethereum, полегшуючи виконання транзакцій. Оптимізація споживання газу смарт-контрактами гарантує не лише економічну ефективність транзакцій, але й те, що вони не зупиняться через перевищення лімітів газу. Газовий механізм Ethereum слугує кільком цілям. Перш за все, він гарантує, що операції в мережі мають вартість, запобігаючи спаму або атакам на відмову в обслуговуванні. Крім того, він прив'язує обчислювальну роботу операцій до реальної вартості, забезпечуючи ефективність коду.

Зберігання є однією з найдорожчих операцій в перерахунку на газ в Ethereum. Використання відповідних структур даних, мінімізація операцій зберігання та видалення непотрібних даних може значно зменшити витрати. Solidity зберігає змінні у слотах шириною 32 байти. Коли змінні упаковуються у структуру, Solidity намагається мінімізувати кількість використовуваних слотів, що потенційно економить газ. Також потрібно знати про Оптимізацію модифікаторів, код розміщується у модифікованій функції, а код модифікатора копіюється у всіх випадках його використання. Це призведе до збільшення розміру байткоду та використання газу.

ВИСНОВКИ

Дана робота дозволила глибше зрозуміти функціонування смарт-контрактів та необхідні ресурси для їх роботи, зокрема газу і ефіру. Смарт-контракти, як і технологія блокчейн в цілому, мають велике значення для забезпечення безпеки та ефективності транзакцій у децентралізованих системах. Основні висновки з нашого дослідження свідчать, що смарт-контракти вимагають ретельного планування та оптимізації коду для мінімізації витрат на газ. Використання оптимізованих структур даних та мінімізація операцій зберігання можуть суттєво знизити витрати на виконання контрактів. Газ є ключовим елементом у забезпеченні безпеки мережі Ethereum, оскільки він прив'язує обчислювальну роботу до реальної вартості, що запобігає спаму і забезпечує ефективність виконання операцій.

Було розглянуто використання анонімних криптовалют та протоколів, таких як Monero і CryptoNote, демонструє високий рівень захисту конфіденційності користувачів. Проте, питання деанонімізації залишаються актуальними, що вимагає постійного вдосконалення методів захисту. Смарт-контракти мають широкий спектр застосувань, від фінансових операцій до реалізації складних логістичних процесів. Їх використання може суттєво підвищити прозорість і надійність систем, що в них задіяні. Таким чином, проведене дослідження підкреслює важливість правильного проектування і оптимізації смарт-контрактів для забезпечення їх ефективної роботи та мінімізації витрат. Використання сучасних протоколів захисту конфіденційності є ключовим для забезпечення безпеки користувачів в цифровому світі, що постійно розвивається.