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 ФБ-31мн
Швець Максим,
Чикрій Кирило

Перевірила:
Селюх П.В.

Київ — 2024

ЗВІТ

Тема: Реалізація смарт-контракту або анонімної криптовалюти.

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

Завдання на лабораторну роботу: 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.

Вступ

Криптовалюта стала революційною силою у фінансовому світі. Це цифрова форма грошей, яка не контролюється жодним центральним органом влади, таким як банк чи уряд. Натомість вона покладається на криптографію, складну систему кодів, щоб забезпечити свою безпеку та обмежити її створення. Ця цифрова валюта працює в децентралізованій мережі, яка називається блокчейн. Уявіть собі гігантську публічну книгу, яка записує кожну транзакцію, пов'язану з цією валютою. Хоча така прозорість гарантує автентичність, вона має цікавий нюанс: ідентифікаційні дані користувачів маскуються за псевдонімами. Це створює відчуття анонімності, коли ви можете надсилати та отримувати криптовалюту, не обов'язково розкриваючи своє справжнє ім'я.

Завіса анонімності, що оточує криптовалютні транзакції, є палицею з двома кінцями. З одного боку, вона пропонує користувачам рівень конфіденційності та фінансової свободи, якого немає в традиційних системах. Люди можуть здійснювати транзакції без страху перед державним моніторингом чи контролем. Крім того, це дозволяє брати участь у глобальній фінансовій системі тим, хто може бути виключений з неї традиційними банківськими

установами. Однак сама природа блокчейну з його ретельним записом транзакцій створює вразливості. За допомогою складного аналізу можна потенційно пов'язати ці анонімні адреси з реальними особами. Це викликає занепокоєння щодо потенційної деанонімізації, коли чиясь справжня особистість, яка стоїть за криптовалютною транзакцією, може бути розкрита.

Незважаючи на проблеми, пов'язані з анонімністю, криптовалюта за останні роки набула величезної популярності. Цей сплеск можна пояснити кількома факторами. Одним з ключових факторів є прагнення до децентралізації. Усуваючи контроль центральних банків та урядів, криптовалюта дає можливість людям самостійно управляти власними фінансами. Крім того, потенціал високих прибутків приваблює інвесторів, які шукають нові шляхи для створення багатства. Крім того, технологія, що лежить в основі криптовалюти, блокчейн, має величезні перспективи для інновацій у різних галузях. Його безпечний і прозорий характер розглядається як потенційна зміна правил гри в таких сферах, як управління ланцюгами поставок і безпека даних.

Майбутнє криптовалют сповнене потенціалу, але також пов'язане з викликами. З розвитком технологій методи анонімізації та деанонімізації будуть продовжувати розвиватися. Регуляторні органи по всьому світу намагаються вирішити, як інтегрувати цю проривну технологію в існуючі фінансові системи. Зрештою, успіх криптовалют залежатиме від їхньої здатності вирішувати проблеми конфіденційності, будувати довіру та сприяти інноваціям у відповідальний і безпечний спосіб.

Принципи аномізації

Основна привабливість криптовалюти полягає в тому, що вона обіцяє анонімність. Користувачі можуть надсилати та отримувати кошти, не розкриваючи свою особистість. Однак ця завіса конфіденційності не є

абсолютною. Існують методи як анонімізації, так і деанонімізації, що створює постійну боротьбу за контроль над даними користувачів.

1. Псевдонімізація: Основа анонімності

В основі більшості методів анонімізації лежить псевдонімізація. Традиційні фінансові системи пов'язують транзакції безпосередньо з обліковими записами користувачів, розкриваючи справжні імена та особисту інформацію. На відміну від них, криптовалюта використовує псевдоніми - випадково згенеровані буквено-цифрові адреси - для представлення користувачів у блокчейні. Ці адреси функціонують як псевдоніми, дозволяючи користувачам взаємодіяти з мережею, не розкриваючи своїх справжніх імен. Хоча псевдонімізовані адреси видно в блокчейні, вони не містять жодного зв'язку з реальною особою, яка за ними стоїть. Цей простий, але ефективний метод формує перший рівень анонімності в криптовалютних транзакціях.

2. Змішування сервісів: Перетасування колоди транзакцій

Сервіси змішування просувають псевдонімізацію на крок далі, активно заплутуючи сліди криптовалютних транзакцій. Уявіть собі кімнату, заповнену людьми, які тримають в руках конверти з різними сумами грошей. Сервіс змішування виступає довіреним посередником, який збирає ці конверти, перемішує їх між собою, а потім роздає учасникам. У світі криптовалют користувачі надсилають свої кошти на міксинговий сервіс, який об'єднує їх з коштами інших користувачів. Потім сервіс виплачує ці об'єднані кошти на визначені адреси одержувачів, фактично розриваючи прямий зв'язок між відправником і одержувачем початкових транзакцій. Цей метод значно ускладнює відстеження потоку коштів та ідентифікацію залучених сторін.

3. CoinJoin: Спільний підхід до анонімності

CoinJoin спирається на концепцію змішування сервісів, але додає шар децентралізації. Замість того, щоб покладатися на довірену третю сторону (сервіс змішування), CoinJoin дозволяє користувачам безпосередньо брати участь в процесі анонімізації. Ось як це працює: кілька користувачів, які мають кошти для відправки, об'єднуються для створення єдиної комбінованої транзакції. Внесок кожного користувача змішується разом, що унеможливлює розрізнення індивідуальних входів і виходів. Ця колективна транзакція потім транслюється в блокчейні, що ще більше приховує походження і призначення конкретних коштів кожного користувача. CoinJoin пропонує більш орієнтовану на конфіденційність альтернативу централізованим сервісам змішування, усуваючи потенційний ризик єдиної точки збою або компрометації.

4. Докази з нульовим рівнем знань: Криптографічна спритність рук

Докази з нульовим рівнем знань (ZKP) - це передова технологія анонімізації. Уявіть, що вам потрібно довести, що ви достатньо дорослі, щоб увійти в бар, не розкриваючи свій справжній вік. ZKP працюють за схожим принципом. У контексті криптовалюти ці передові криптографічні методи дозволяють користувачам довести, що вони володіють певною інформацією (наприклад, достатньою кількістю коштів для здійснення транзакції), не розкриваючи деталей самої інформації. Це значно підвищує рівень конфіденційності, усуваючи необхідність транслювати конфіденційні дані в блокчейні. Наприклад, користувач може використовувати ZKP, щоб довести, що він має достатньо коштів для завершення транзакції, не розкриваючи фактичний баланс свого рахунку. Хоча ZKP все ще перебувають на стадії розробки, вони мають величезні перспективи для досягнення вищого рівня анонімності в криптовалютних транзакціях.

Порівняння аномізації між Bitcoin та Solana

І Солана, і Біткоїн використовують концепцію псевдонімізації як основу для анонімізації особистих даних користувачів. Транзакції записуються у відповідних блокчейнах, але адреси користувачів функціонують як псевдоніми, не розкриваючи справжніх імен. Однак конкретні методи досягнення подальшої анонімізації можуть відрізнятися між цими двома криптовалютами.

Біткоїн:

Змішування послуг: Завдяки більшій базі користувачів і усталеній екосистемі, біткойн має ширший спектр сторонніх сервісів для змішування криптовалют. Ці сервіси можуть бути хорошим варіантом для анонімізації невеликих транзакцій.

CoinJoin: Хоча CoinJoin не настільки широко впроваджений, як сервіси змішування, його функціонал все частіше інтегрується в біткоїн-гаманці, пропонуючи більш децентралізований підхід до анонімізації.

Solana:

Протоколи, орієнтовані на конфіденційність: Solana може похвалитися екосистемою, що тільки зароджується, але кілька проектів спеціально зосереджені на підвищенні конфіденційності користувачів. Ці протоколи часто використовують передові криптографічні методи, такі як докази з нульовим знанням (ZKP) для досягнення анонімності без шкоди для швидкості транзакцій або масштабованості, які є ключовими перевагами блокчейну Solana.

Змішування в ланцюжку: Деякі проекти Solana досліджують розробку рішень для внутрішньоланцюгового міксування. Ці рішення будуть "рідними" для блокчейну Solana, усуваючи залежність від зовнішніх сервісів мікшування і потенційно пропонуючи більшу безпеку і прозорість.

Отже, і Solana, і Bitcoin пропонують певний рівень анонімності через псевдонімізацію. Однак біткоін має ширший спектр усталених інструментів анонімізації, таких як сервіси змішування, в той час як Solana може похвалитися більш інноваційним підходом з проектами, що досліджують ZKP і рішення для змішування в ланцюжку.

Принципи деаномізації

Хоча криптовалюта процвітає завдяки обіцянці анонімності, існує постійна боротьба між конфіденційністю користувачів і можливістю ідентифікувати осіб, які стоять за транзакціями. З'явилися технології, які дозволяють знімати шари псевдонімів і потенційно пов'язувати адреси в блокчейні з реальними особами. Ці методи деанонімізації становлять значний виклик для тих, хто прагне повної анонімності в криптовалютному просторі.

1. Аналіз блокчейну: Просіювання через публічний реєстр

Сама природа технології блокчейн представляє собою палицю з двома кінцями для анонімності. Хоча транзакції є псевдонімами, вони назавжди закарбовуються в публічному реєстрі, доступному будь-кому. Це дозволяє проводити глибокий аналіз шаблонів транзакцій, що є основою блокчейн-аналізу. Ретельно вивчаючи рух коштів, аналітики можуть виявити кластери транзакцій, які потенційно пов'язані з одним і тим же користувачем. Цього можна досягти за допомогою таких методів, як

Аналіз обсягу транзакцій: Вивчення кількості криптовалюти, надісланої або отриманої з певної адреси, може виявити закономірності, що вказують на одного користувача або організацію.

Аналіз за часом: Аналіз часу транзакцій іноді може виявити зв'язки між адресами, які здійснюють транзакції постійно або через певні проміжки часу.

Кластеризація адрес: Алгоритми можуть групувати адреси на основі різних факторів, таких як історія транзакцій або географічне розташування, потенційно виявляючи приховані зв'язки.

2. Евристичний аналіз: Виявлення поведінкових шаблонів

Евристичний аналіз заглиблюється глибше, ніж просто вивчення даних про транзакції. Він передбачає пошук певних шаблонів у поведінці користувача, які можуть вказувати на його особу. Ось як це працює:

Виявлення аномалій: Аналітики шукають незвичайні шаблони транзакцій, які відхиляються від типової поведінки користувачів. Це можуть бути транзакції, що відбуваються в неробочий час, постійні перекази на певні біржі або використання відомих адрес високого ризику.

Моніторинг чорних списків: Перевіряючи адреси в чорних списках, пов'язаних з незаконною діяльністю, аналітики можуть виявити користувачів, які беруть участь у підозрілих транзакціях.

Аналіз соціальних мереж: У деяких випадках аналітики можуть спробувати пов'язати адреси блокчейну з акаунтами в соціальних мережах або іншою онлайн-активністю на основі спільних поведінкових патернів.

3. Методи кластеризації: Виявлення прихованих зв'язків

Вдосконалені алгоритми відіграють вирішальну роль у деанонімізації. Методи кластеризації передбачають групування адрес блокчейну на основі різних факторів. Ці фактори можуть включати

Історія транзакцій: Адреси зі схожими шаблонами транзакцій або частими взаємодіями можуть бути згруповані разом, що вказує на потенційний зв'язок.

Аналіз мережі: Вивчення мережі взаємопов'язаних адрес може виявити приховані зв'язки між об'єктами, які, здавалося б, не пов'язані між собою.

Географічний аналіз: Якщо дані про транзакції вказують на географічний зв'язок, їх можна використати для звуження потенційного місцезнаходження користувача.

4. Зв'язок із зовнішніми даними: Подолання розриву до реальних ідентифікаційних даних

Останній шматочок пазла деанонімізації передбачає зв'язок даних блокчейну з інформацією із зовнішніх джерел. Це може включати в себе

Витік баз даних: Витоки даних можуть призвести до витоку особистої інформації, яку можна співвіднести з адресами в блокчейні.

Публічні записи: У деяких випадках інформація з публічних записів, наприклад, про власність або реєстрацію бізнесу, може бути використана для ідентифікації осіб, які стоять за конкретними адресами.

Дані KYC/AML: Регульовані організації, які дотримуються правил "Знай свого клієнта" (KYC) і протидії відмиванню грошей (AML), можуть пов'язувати підтверджені ідентифікаційні дані користувачів з конкретними адресами в блокчейні.

Ці методи висвітлюють проблеми збереження повної анонімності в криптовалютному просторі. З розвитком технологій зусилля з деанонімізації будуть ставати все більш витонченими. Це вимагає постійної розробки більш надійних методів анонімізації для забезпечення здорового балансу між конфіденційністю користувачів і необхідністю боротьби з незаконною діяльністю в криптовалютній екосистем

Порівняння деаномізації між Bitcoin та Solana

Хоча Bitcoin і Solana пропонують певний рівень анонімності через псевдонімізовані адреси, їхні публічні блокчейни роблять їх вразливими до спроб деанонімізації. Розглянемо докладніше методи, що використовуються для потенційного зв'язування цих адрес у блокчейні з реальними особами:

Методи, застосовні як до біткоїна, так і до Солани:

Аналіз блокчейну: Цей основний метод передбачає ретельне вивчення даних про транзакції в публічному реєстрі. Аналітики можуть виявити закономірності, які вказують на зв'язок між, здавалося б, розрізненими адресами. Ось як це працює в обох контекстах:

Аналіз обсягу та часу транзакцій: Вивчення суми та часу транзакцій може виявити невідповідності або закономірності, які можуть вказувати на одного користувача. Наприклад, постійне надсилання невеликих сум біткоїнів через певні проміжки часу може вказувати на торговця, в той час як великі, нечасті транзакції на Solana можуть вказувати на інвестора.

Кластеризація адрес: Складні алгоритми групують адреси на основі історії транзакцій, географічного розташування (виведеного через IP-адреси) або інших факторів. Це потенційно може виявити приховані зв'язки між адресами, що використовуються однією особою.

Евристичний аналіз: Цей метод виходить за рамки необроблених даних, зосереджуючись на моделях поведінки користувачів. Аналітики шукають червоні прапорці, які можуть викрити особу користувача. І Біткоїн, і Солана схильні до цього:

Виявлення аномалій: Незвичайні шаблони транзакцій, такі як надсилання коштів у неробочий час, постійні перекази на певні біржі або взаємодія з відомими адресами високого ризику, можуть викликати підозру.

Моніторинг чорних списків: Перевірка адрес у чорних списках, пов'язаних з незаконною діяльністю, може бути тривожним сигналом як для користувачів Bitcoin, так і для користувачів Solana.

Методи, що використовують специфічні особливості блокчейну:

Біткойн: через більшу базу користувачів і розвинену екосистему біткойн стикається з унікальними проблемами деанонімізації:

Аналіз змішаних сервісів: Оскільки багато користувачів біткоїна покладаються на сторонні сервіси міксингу, аналітики можуть відстежувати рух коштів через ці сервіси, щоб потенційно деанонімізувати користувачів.

Solana: Зосередженість Solana на масштабованості відкриває двері для нових методів деанонімізації:

Аналіз змішування в ланцюжку: Оскільки Solana досліджує власні рішення для змішування в ланцюжку, аналітики можуть розробити методи відстеження потоку коштів через ці протоколи і потенційно пов'язати користувачів.

Висновки

Ми дослідили концепцію псевдоніму, основу конфіденційності користувачів у криптовалюті, а потім заглибилися в різні методи, що застосовуються як для анонімізації (сервіси змішування, CoinJoin, докази з нульовим знанням), так і для деанонімізації (аналіз блокчейну, евристичний аналіз, методи кластеризації, прив'язка до зовнішніх даних). Ми також розглянули, як ці методи застосовуються конкретно до Біткоїна і Солани, підкресливши унікальні виклики і можливості, які представляє кожна мережа.

Насамкінець, прагнення до анонімності в криптовалюті - це постійна боротьба. З розвитком технологій методи анонімізації та деанонімізації будуть продовжувати розвиватися. Розуміння цих методів і того, як вони застосовуються до конкретних блокчейнів, таких як Bitcoin і Solana, має вирішальне значення для користувачів, які орієнтуються в цьому складному ландшафті. Зрештою, досягнення балансу між конфіденційністю користувачів і відповідальним використанням в умовах мінливого регуляторного середовища стане ключем до майбутнього успіху і стабільності криптовалют.