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

Звіт з виконання комп'ютерного практикума

РЕАЛІЗАЦІЯ СМАРТ-КОНТРАКТУ АБО АНОНІМНОЇ КРИПТОВАЛЮТИ

Виконали студентки
групи ФІ-32мн
Зацаренко А. Ю.
Футурська О. В.

Перевірила:
Селюх П. В.

Київ — 2024

ЗВІТ

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.

Необхідні теоретичні відомості

Сатоші Накамото стверджував, що Bitcoin анонімний. Це привернуло увагу власників нелегального бізнесу. Вони почали користуватися криптовалютою, думаючи, що це дасть їм абсолютну свободу дій. Bitcoin же анонімний – отже, можна робити що завгодно і коли завгодно. Вони продавали нелегальні послуги і товари, не замислюючись, що можуть бути покарані. Але Сатоші Накамото мав на увазі інше.

Анонімність біткоїна полягає в тому, що його власнику не потрібно вказувати дані про свою особу під час придбання криптовалюти. Усі операції з криптовалютами засновані на технології блокчейн, де транзакції, що проводяться в мережі, відкриті всім. Однак, інформації, яка зберігається в блокчейні, цілком достатньо, щоб визначити відправника й одержувача.

Основний принцип роботи блокчейна – прозорість проведених транзакцій за відсутності можливості їх зміни. Блокчейн дає змогу розкривати корупційні схеми, пов'язані з нелегальними фінансовими потоками. Це можливо завдяки основному принципу його роботи: всі транзакції і кожна людина, яка їх здійснює, записуються в єдину базу даних, доступ до якої має кожна сторона процесу. Це дає можливість своєчасно виявляти злочинців.

Блокчейн зберігає конфіденційність даних користувачів. Наприклад, анонімність Bitcoin обумовлюють такі особливості мережі:

1) *Відсутність прив'язки криптовалютних адрес (номерів) до користувачів.* Для генерації нового сховища учасникам системи Bitcoin не потрібно вказувати особисту інформацію. Також вони можуть створювати гаманці в будь-якій кількості, коли буде потрібно.

2) *Відсутність прив'язки біткоїн-транзакцій до їхніх ініціаторів.* Для здійснення криптовалютного переказу власникам BTC теж не потрібно вказувати персональну інформацію.

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

1.1 Принцип деанонімізації

Дослідження деанонімізації криптовалют можна виконати двома засобами. Першим з них є аналіз ланцюжка транзакцій за допомогою відповідних мережевих інструментів, який полягає у відстеженні транзакцій по мережі та накопиченні загальнодоступних відомостей про них, а також пов'язуванні їх з особистими даними користувача. Інший метод – це аналіз протоколу та мережі, який використовує характеристики розповсюдження транзакцій з криптовалютою для визначення вихідної IP-адреси нової транзакції.

Існуюча методологія деанонімізації транзакцій передбачає відстеження всієї історії їх просування по мережі. Для аналізу ланцюжка і збору даних можна використовувати такі інструменти, як: Blockchain Explorer, Matbea.net, CryptoHound, Glassnode, GraphSense.

Blockchain Explorer

Це один з найбільш відомих інструментів аналізу ланцюжка блоків. Він

пропонує ряд можливостей для відстеження окремих транзакцій, а також надає інформацію у вигляді графіків і статистики всієї мережі. Крім того, з його допомогою можна провести аналіз стосовно руху коштів по мережі.

Matbea.net

Це послуга, яка дозволяє користувачам встановлювати належність біткоїн-адрес. Даний інструмент надає користувачам можливість шукати інформацію по транзакціям, адресам, блокам і видає результат у вигляді детальної текстової статистики.

ORS CryptoHound

Це ще один інструмент дослідження мережі на базі штучного інтелекту, який використовується для дослідження Bitcoin і Ethereum адрес і надає результати у вигляді списків, діаграм або таблиць. Інструмент пропонує можливості відстеження коштів за конкретною адресою, відображення залишку на балансі, візуалізацію відношень адрес і всіх транзакцій, що проведені нею, дозволяє виконувати статистичний розрахунок вартості монет, а також формування банківських звітів.

Glassnode

Сервіс являє собою аналітичну компанію, що займається аналітикою блокчейн мереж і надає оперативну інформацію про стан ринку, пропонуючи відображення результатів в різних категоріях.

GraphSense

Зручний та ефективний сервіс дозволяє виконувати розширені завдання аналітики в реальному часі, з результатами у вигляді графів і таблиць з усією історією транзакцій, що дозволяє додатково досліджувати кожне вхідне і вихідне відношення за допомогою побудови адресних графів і спостерігати за всім ланцюжком, виявляючи аномальну поведінку у мережі.

1.2 Технології анонімізації транзакцій у блокчейні

З часом люди придумали, як зробити так, щоб кінцева мета транзакції ніяк не була пов'язана з відправником. Народилося безліч міксерів, з'явилися

анонімні криптовалюти і гаманці.

1.2.1 Міксери (Mixers)

Міксер – це тип анонімайзера, який приховує ланцюжок транзакцій у блокчейні, пов'язуючи всі транзакції з однією біткоїн-адресою і надсилаючи їх разом таким чином, щоб вони виглядали так, ніби їх було надіслано з іншої адреси. Міксер відправляє транзакції через складну, напіввипадкову серію фіктивних транзакцій, що вкрай ускладнює прив'язку конкретних віртуальних токенів (адрес) до конкретної транзакції.

Такі сервіси працюють шляхом отримання інструкцій від користувача про надсилання коштів на певну біткоїн-адресу. Потім сервіс «змішує» цю транзакцію з іншими транзакціями користувача, так що стає незрозуміло, кому користувач хотів направити кошти.

По суті, ви віддаєте свої кошти третій особі, яка змішує їх із коштами інших користувачів сервісу. У підсумку зв'язок між відправником і одержувачем втрачається.

Міксери беруть за свої послуги комісію в 1-3%. Ця операція вимагає часу: на обробку однієї транзакції може йти від 30 хвилин і вище. Мінус у тому, що користувач абсолютно не контролює процес, він навіть не може спостерігати за тим, куди і кому відправлять його гроші. Залишається тільки чекати і сподіватися, що в кінцевому підсумку вас не обдурять і гроші дійсно дійдуть до одержувача. Вам ніхто не дає гарантії, що все пройде успішно і власник сервісу просто не забере ваші гроші собі. Необхідно ретельно вибирати міксери.

Прикладами змішувальних сервісів є Bitmix, Mixer.Money, SharedCoin, Bitcoin Laundry, Bitlaunder, Easycoin.

Bitmix

Найпопулярнішим таким сервісом є Bitmix. Він стягує періодичну комісію від 0,8 до 3%, яку користувач може встановити самостійно в процесі обміну. Усім біткоїнам, що надходять, присвоюється унікальна мітка, і

користувач ніколи не отримає свої власні біткоїни назад. Bitmix дає змогу проводити операцію змішування, використовуючи публічний Інтернет, але змішування без анонімної передачі даних значно підвищує ризик розкриття користувача.

Mixer.Money

Ключовою особливістю цього сервісу є поєднання класичного принципу змішування роботи сервісу та залучення світових бірж. Так, після класичного міксера монети відправляються на одну з найбільших централізованих бірж (Kraken, Poloniex, Binance), де їх замінюють токени інших трейдерів. У результаті на дві адреси, у різний час і в різних пропорціях, користувач отримує чисті токени з однієї з бірж.

Bitcoin-Laundry

Помітною особливістю, яка відрізняє її від інших платформ для змішування, є її зручний інтерфейс. Платформа розроблена для легкого доступу і пропонує безперешкодні транзакції всього за кілька кліків. Платформа використовує передові протоколи шифрування, які підвищують безпеку. Безпечний платіжний процес і сувора політика No-Logs значно знижують ризик відстеження транзакцій.

Тепер поговоримо про альтернативні технології:

1.2.2 CoinJoin

На додаток до технології Mixer існує технологія CoinJoin, яку винайшов експерт з безпеки Грегорі Максвелл.

Користувачі, які збираються використовувати CoinJoin, синхронізують свої дії, створюють загальну транзакцію з великою кількістю входів і виходів і підписують результат. Зовнішній спостерігач не може зафіксувати відповідність між учасниками будь-якої транзакції та входами/виходами їхніх коштів. Кошти зливаються в одну купу з різних джерел, а потім відправляються за іншими адресами.

1.2.3 CoinShuffle

Модифікувавши технологію CoinJoin, дослідники з Саарського університету в Німеччині запропонували новий принцип змішування під назвою CoinShuffle, який усунув головний недолік CoinJoin - деанонімізацію користувачів групових транзакцій один до одного. Користувачі домовляються про проведення транзакції, використовуючи криптографічні методи захисту інформації.

Процес ділиться на три етапи:

1) Усі користувачі оголошують свої публічні адреси, з яких вони хочуть здійснювати перекази. Вихідні адреси і сума транзакції не оголошуються. Користувачі генерують пару одноразових ключів (відкритий і секретний). Учасники знають відкриті ключі один одного, але не секретні. Крім того, кожен учасник має свій порядковий номер у ланцюжку;

2) Другий етап заснований на криптографічному шифруванні протоколу обміну секретами. Перший учасник зашифровує адреси і суми публічним ключем учасника з останнім порядковим номером, потім ключем учасника з передостаннім номером і тд. Зашифроване повідомлення передається наступному учаснику ланцюжка, який його розшифровує своїм секретним ключем, додає свою частину, зашифровує публічним ключем останнього учасника, змішує ці шифротексти і передає далі. Останньому учаснику достатньо розшифрувати все своїм секретним ключем, додати свою частину і востанє все перемішати;

3) Якщо остаточна транзакція задовольняє всіх користувачів, то кожен підписує її своїм секретним ключем, а один учасник публікує остаточну транзакцію в блокчейн для підтвердження.

CoinShuffle має важливий недолік: учасник не може бути впевненим, що інші не перебувають у змові або не є однією і тією самою особою, тому його початкова адреса в цьому разі може бути обчислена.

Варто також зазначити, що розглянуті інструменти не можуть забезпечити ідеальну анонімізацію. Існують ризики, які несе зловмисник

через можливість розкриття його особистості власником сервера. Крім того, вихідний код недоступний користувачам.

Серверна частина перебуває під контролем тільки власників. Користувачі не можуть контролювати роботу алгоритмів серверної платформи. Таким чином, може бути відтворено довільний код, спрямований на деанонімізацію користувацьких операцій.

1.2.4 The Onion Router

Браузери на основі технології The Onion Router використовують для підключення до інтернету багаторівневе шифрування з'єднання 3 ключами. Вони генеруються випадково під час проходження сигналу через проксі-сервери (проміжні ланки між користувачем і мережею). Це дає змогу приховувати IP-адресу і будь-яку іншу інформацію.

1.2.5 Спеціальні гаманці

Існують непрозорі сховища, через які можна анонімно відправляти криптовалюту. Вони закривають доступ до інформації про адреси та біткоїн-транзакції клієнтів. У цьому випадку у власників сервісу є кілька криптогаманців. Отримавши монети на один, вони відправляють аналогічну суму з інших. У результаті практично неможливо пов'язати ці транзакції.

✻ Анонімні гаманці: Теоретично, для їх створення не потрібна ніяка особиста інформація. Однак такими гаманцями часто складно користуватися і вони можуть бути не дуже безпечними.

✻ Гаманці, орієнтовані на конфіденційність: Ці гаманці надають пріоритет конфіденційності користувача, але все одно можуть вимагати певної верифікації, залежно від платформи. Вони пропонують такі функції, як:

1) Самостійне зберігання: Ви зберігаєте приватні ключі до вашої криптовалюти, що дає вам більше контролю над вашими коштами.

2) Кілька транзакцій: Деякі гаманці можуть змішувати транзакції, щоб

ускладнити їх відстеження.

3) Маскування IP-адреси: Ці гаманці можуть приховувати вашу IP-адресу під час транзакцій.

1.2.6 Анонімні криптовалюти

Коли користувачі почали усвідомлювати псевдоанонімність біткоїна, деякі розробники криптовалюти вирішили на цьому зіграти. Включити анонімність у код криптовалюти - це розумно. Вам не треба шукати ліві сервіси для анонімізації транзакцій, не треба використовувати сумнівні гаманці. Ви просто купуєте валюту, у якій процес запису блоків передбачає анонімність.

Існують монети, які використовують технології PrivateSend, яка зі свого боку заснована на CoinJoin. Анонімність таких валют досягається тими самими засобами, що були описані вище. Але, щоб така технологія могла функціонувати в криптовалюті за замовчуванням, необхідна наявність добровольців, які підтримуватимуть PrivateSend, - мастерноди. Така схема використовується у валюті Dash. Користувач під час проведення транзакції обирає кількість раундів перемішування, а випадково обрані мастерноди займаються перемішуванням монет. Мастернодам, як і майнерам, належить винагорода за підтримку мережі.

У 2012 році було розроблено протокол CryptoNote, що використовує технологію кільцевих підписів і одноразових транзакцій. Цього ж року почалося зародження сімейства анонімних криптовалют, заснованих на протоколі CryptoNote.

Кільцеві підписи – це механізм реалізації електронного підпису, який дає змогу приховати відправника. Кільцеві підписи дають змогу створювати списки з відкритих ключів для одного повідомлення. У підсумку буде відомо, що хтось зі списку підписав повідомлення, але хто саме – сторонні люди дізнатися не зможуть. CryptoNote використовує цю технологію для підписання транзакцій.

Кожен розробник криптовалюти, який використовував CryptoNote, удосконалював цю систему, додаючи якісь свої фішки. Обфускація транзакцій – заплутування вихідної інформації про транзакцію без втрати її функціональності, що ускладнює аналіз транзакції. Використання одноразових підписів – така схема ускладнює ідентифікацію відправника, адже його підпис ніколи не повторюється. Хтось намагається скоротити час верифікації, хтось – ускладнити технологію або, навпаки, спростити.

Історія цієї криптосімейки почалася з валюти Bytecoin (BCN), наступною була Monero, потім AEON і т.д. DigitalNote, DashCoin (DashCoin і Dash – різні криптовалюти), Forknote і Boolberry – усіх їх пов'язує протокол CryptoNote.

Творці Monero виявили в CryptoNote баг, який давав змогу робити подвійні витрати, іншими словами, забезпечував створення необмеженої кількості монет. Сама Monero не постраждала. Дісталося Bytecoin: штучно було створено 693 000 000 монет.

Інші криптовалюти більш творчо підійшли до анонімності. Наприклад, було створено технологію zk-Snarks. Вона використовує докази з нульовим розголошенням. Фішка в тому, що в блок записується максимально можливий мінімум інформації про транзакцію. Наприклад, ZCash записує тільки час транзакції і нічого більше. Таким чином, абсолютно неможливо дізнатися, хто, кому і скільки монет відправив. Інформація може бути прихована або відкрита за бажанням користувача. Активне впровадження цієї технології почала Zerocoin Electric Coin Company. Створення протоколів ZeroCoin, а потім – ZeroCash породило чималу кількість анонімних валют. Першою була ZCoin (XZC), випущена 2016 року, також були SmartCash і ZeroVert. Але, мабуть, найбільш ходовою та анонімною стала ZCash.

Зовсім недавно було знайдено лазівку в Monero, за допомогою якої за бажання можна виявити відправників, а ZCash взагалі можна підробити, однак це складно.

ВИСНОВКИ

У даній лабораторній роботі було розглянуто причини виникнення такого явища, як анонімізація криптовалюти. Кожен блокчейн сам по собі забезпечує анонімність в тому сенсі, що не потрібно вказувати свої персональні дані під час купівлі чи продажу. Однак за самими транзакціями, що розташовані в кожному блоці в ланцюгу, досить таки реально визначити відправника і одержувача.

Щоб боротися з цим, було розроблено багато різних механізмів, які розглянуто в даному практикумі. Крім цього, також було також надано опис роботи анонімних криптовалют, їх різноманіття та недоліки.