НТУУ "Київський політехнічний інститут імені Ігоря Сікорського" НН
Фізико-технічний інститут

Технологія блокчейн та розподілені системи

Лабораторна робота №2

Виконали:
Ярощук Владислав ФБ-31мн
Осінній Максім ФБ-31мн
Золотов Іван ФБ-31мп

Київ - 2024

Вступ

Monero – це криптовалюта, яка використовує технологію блокчейн, але з акцентом на конфіденційність. Вона була створена в 2014 році з метою забезпечення анонімності та захисту особистих даних користувачів. Monero є найпопулярнішою реалізацією протоколу CryptoNote.

Ключові особливості Monero, що стосуються конфіденційності:

- CryptoNote: Протокол, реалізацією якого є Monero
- RingCT: Ця технологія приховує суми транзакцій та адреси відправника/отримувача, роблячи їх неможливими для відстеження.
- Stealth addresses: Для кожної транзакції генерується нова адреса, що ускладнює зв'язування транзакцій з одним користувачем.

Методи анонімізації в Monero

CryptoNote

CryptoNote - це протокол прикладного рівня, який забезпечує роботу декількох децентралізованих цифрових валют, орієнтованих на конфіденційність. Його метою є розвиток ідей, що лежать в основі Bitcoin.

Основна відмінність між цими двома технологіями полягає в тому, що біткойн (і більшість цифрових валют) є менш непрозорими, ніж валюти на основі CryptoNote, оскільки блокчейн останньої є майже анонімним, на відміну від блокчейнів, що не базуються на Cryptonote. Криптовалюта CryptoNote використовує розподілений публічний реєстр, який фіксує всі баланси та транзакції вбудованої валюти, подібно до біткоіна. На відміну від біткоїна, транзакції CryptoNote не можна відстежити через блокчейн таким чином, щоб виявити, хто відправив або отримав монети. Приблизна сума транзакції може бути відома, але походження, місце призначення або фактична сума не можуть бути встановлені. Єдина доступна інформація - це те, що фактична сума була меншою, ніж відображена. Єдиними людьми, які мають доступ до всього набору даних про транзакцію, є відправник або одержувач транзакції та особа, яка володіє одним або обома секретними ключами.

Ще однією суттєвою відмінністю є алгоритм підтвердження роботи CryptoNote, що базується на хешуванні. Біткоїн використовує SHA-256, який є прив'язаною до процесора функцією. Це означає, що учасники (майнери) обмежені лише швидкістю своїх обчислень, і можна відносно дешево створити пристрій на базі прикладної інтегральної схеми (ASIC), який буде перевершувати звичайний комп'ютер за кількістю хешів на одиницю грошей. CryptoNote використовує функцію CryptoNight, яка обмежена пам'яттю і не може бути легко конвеєризована.
Кодова база CryptoNote не є відгалуженням від кодової бази Біткоїна, тому вона також має інші внутрішні алгоритми для таких речей, як перерахунок нового рівня складності або нового розміру блоку.

RingCT та Stealth addresses

Щоб приховати публічну адресу одержувача, Monero використовує одноразові адреси, і зовнішній спостерігач не може криптографічно співставити одноразові адреси з будь-якою публічною адресою. Щоб захистити відправника, мережа також використовує змішування, але у спосіб, відмінний від CoinJoin. У Monero відправнику не потрібно шукати інших учасників для завершення спільної транзакції. Замість цього гаманець сам створює випадковий набір виходів, доступних в блокчейні, ховає серед них справжній і підписує цей набір кільцевим підписом.

Кільцевий підпис тут служить для того, щоб довести валідатору транзакції, що відправник дійсно володіє одним із змішаних виходів, і ніяких подвійних витрат не відбудеться. Це робить відстеження платежу до його одержувача досить складним.

RingCT – це метод, який приховує суми транзакцій та адреси відправника/отримувача. Він робить це шляхом змішування декількох виходів транзакцій (одного, який надсилає монети, та декількох "привидів") в один криптографічний образ. Це ускладнює визначення, скільки монет було відправлено та з яких адрес.

Як працює RingCT:

1. Вибір "кільця": Користувач обирає декілька випадкових виходів транзакцій з блокчейну (їх називають "кільцем").
2. Змішування: Сума транзакції, яку хоче надіслати користувач, додається до сум вибраних виходів з "кільця".
3. Криптографічний підпис: Користувач підписує транзакцію за допомогою свого приватного ключа.

Після підтвердження транзакції в блокчейні стає неможливо визначити, який саме вихід з "кільця" був фактичним вихідним платежем, а суми всіх виходів в "кільці" стають нерозрізненими.

Також, варто зазначити, що рівень конфіденційності транзакції корелює з розміром її кільцевого підпису, оскільки чим більше випадкових виходів

використовується для змішування, тим складніше відстежити її до джерела.

В мережі Monero в 2016 році був встановлений мінімальний розмір кільцевого підпису. На той момент він був встановлений на рівні 3, але мережа збільшувала його щороку. Наразі мінімальний розмір кільцевого підпису становить 11.

Стелс-адреси є важливою частиною конфіденційності, притаманної Monero. Вони дозволяють і вимагають від відправника створювати випадкові одноразові адреси для кожної транзакції від імені одержувача.

Одержувач може опублікувати лише одну адресу, але всі вхідні платежі будуть надходити на унікальні адреси в блокчейні, де їх неможливо буде пов'язати ні з опублікованою адресою одержувача, ні з будь-якими іншими адресами транзакцій. Завдяки використанню стелс-адрес тільки відправник і одержувач можуть визначити, куди був відправлений платіж.

Коли ви створюєте акаунт Monero, ви отримуєте приватний ключ перегляду, приватний ключ витрат і публічну адресу. Ключ spend використовується для відправлення платежів, ключ view використовується для відображення вхідних транзакцій, призначених для вашого акаунта, а публічна адреса - для отримання платежів. Для створення вашої адреси Monero використовуються обидва ключі - spend key і view key. Ви можете мати гаманець «тільки для перегляду», який використовує тільки ключ перегляду. Ця функція може бути використана для цілей бухгалтерського обліку або аудиту, але наразі є ненадійною через неможливість відстежувати вихідні транзакції. Ви можете вирішити, хто може бачити ваш баланс Monero, поділившись своїм ключем перегляду. За замовчуванням Monero є приватним і за бажанням напівпрозорим!

При використанні гаманця Monero все це обробляється програмним забезпеченням. Надіслати Monero так само просто, як ввести адресу одержувача, суму і натиснути кнопку «Надіслати». Щоб отримати Monero, просто надайте відправнику свою публічну адресу.

Методи деанонімізації Monero

Незважаючи на те, що Monero використовує потужні технології для забезпечення конфіденційності, існують методи, які можуть бути використані для деанонімізації користувачів та транзакцій. Ось деякі з найпоширеніших методів:

Аналіз блокчейну

Аналіз блокчейну Monero може допомогти дослідникам виявити зв'язки між транзакціями та користувачами. Це може бути зроблено за допомогою таких методів:

- Аналіз кластерів: Цей метод ґрунтується на тому, що транзакції, які надсилаються з одного "кільця", ймовірно, пов'язані між собою. Дослідники можуть аналізувати транзакції, щоб знайти групи транзакцій, які використовують схожі "кільця", що може свідчити про те, що вони надходять від одного джерела.
- Аналіз транзакцій з нульовим балансом: Транзакції з нульовим балансом – це транзакції, в яких один вихід витрачається, а нові виходи не генеруються. Ці транзакції можуть бути використані для відстеження руху монет по мережі, адже вони показують, куди були переміщені монети з певної адреси.
- Аналіз хешів: Дослідники можуть аналізувати хеші транзакцій, щоб знайти подібності між ними. Це може допомогти їм виявити транзакції, які пов'язані між собою, навіть якщо вони не використовують одні й ті ж адреси.

Трасування транзакцій

Трасування транзакцій – це метод відстеження руху монет по мережі Monero. Це може бути зроблено за допомогою таких методів:

- Відстеження IP-адрес: Деякі дослідники намагаються відстежувати IP-адреси користувачів Monero, щоб виявити їхні транзакції. Це може бути зроблено за допомогою аналізу трафіку або використання спеціальних інструментів.
- Аналіз часових міток: Транзакції Monero мають часові мітки, які можуть бути використані для відстеження їх руху по мережі.

Дослідники можуть аналізувати часові мітки, щоб виявити транзакції, які були відправлені з одного місця в один час, що може свідчити про те, що вони пов'язані між собою.

- Аналіз поведінки: Дослідники можуть аналізувати поведінку користувачів Monero, щоб виявити закономірності, які можуть допомогти їм відстежувати транзакції. Наприклад, дослідники можуть відстежувати, як часто користувачі здійснюють транзакції, які суми вони зазвичай надсилають та які адреси вони використовують.

Трасування транзакцій може бути ефективним методом деанонімізації Monero, але воно також може бути складним та трудомістким завданням. Крім того, його ефективність може бути обмежена розміром та складністю мережі Monero.

Порівняння Monero та Bitcoin

Характеристика	Monero	Bitcoin
Швидкість	Транзакції Monero зазвичай відбуваються швидше завдяки коротшому часу блокування (приблизно 2 хвилини)	Підтвердження біткоїн-транзакцій може зайняти більше часу через 10-хвилинний час блокування
Комісї	Комісії Monero, як правило, нижчі і більш передбачувані завдяки динамічному регулюванню розміру блоків	Комісії за біткойн можуть сильно відрізнятися і, як правило, зростають під час перевантаженості мережі
Масштабованість	Monero має кращі перспективи масштабування, ніж Bitcoin, завдяки динамічному розміру блоку та постійним зусиллям з покращення масштабування	Біткойн стикається з проблемами масштабованості через фіксований розмір блоку та постійні дебати про те, як вирішити цю проблему
Майнинг	Monero використовує алгоритм RandomX, який є стійким до ASIC і призначений для майнінгу на CPU/GPU, що сприяє створенню більш децентралізованої мережі	Біткоїн використовує алгоритм SHA-256, в якому домінує ASIC, що робить його більш централізованим з точки зору потужності майнінгу
Приватність	Monero пропонує сильні функції конфіденційності, включаючи	Транзакції Bitcoin є псевдонімами, і хоча існують деякі рішення для забезпечення

	конфіденційні транзакції та кільцеві підписи, що ускладнює відстеження транзакцій	конфіденційності, вони не настільки надійні, як функції конфіденційності Monero
Використання	Monero часто надають перевагу для транзакцій, що вимагають конфіденційності, і має випадки використання в галузях, де анонімність має важливе значення	Біткойн - це насамперед цифрове сховище вартості, яке зазвичай використовується для інвестування та як цифрове золото

Висновок

Monero і Bitcoin представляють два різних підходи до криптовалюти з власними унікальними наборами функцій і переваг. Біткойн, як піонер криптовалютного простору, пропонує визнання, ліквідність і збереження вартості, подібне до цифрового золота. Його прозорість, забезпечуючи фінансове відстеження, також дозволяє проводити аудит і дотримуватися нормативних вимог.

З іншого боку, Monero ставить конфіденційність понад усе, надаючи користувачам безпрецедентну анонімність і конфіденційність транзакцій. Його взаємозамінність гарантує, що всі монети є рівними, що зменшує занепокоєння щодо забруднених коштів. Спільнота Monero активно підтримує місію фінансової конфіденційності та безпеки.

Список використаних джерел

https://www.getmonero.org/resources/moneropedia/ringCT.html

https://eprint.iacr.org/2015/1098

https://www.getmonero.org/resources/moneropedia/stealthaddress.html

https://medium.com/@exantech/methods-of-anonymous-blockchain-analysis-an-overview-d700e27ea98c

https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/