МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Лабораторна робота №2

з предмету «Блокчейн та децентралізовані системи»

Виконав:
студент І курсу
групи ФБ-41мп
Смирнов Є. В.

Київ 2025

Для першого типу лабораторних: дослідження методів анонімізації/деанонімізації запропонованої криптовалюти із аналізом складності проведення атак деанонімізації і втрат ефективності анонімних криптовалют у порівнянні із Bitcoin/Litecoin.

Dash.

Анонімізація транзакцій у криптовалюті Dash відбувається за допомогою механузму PrivateSend.

PrivateSend базується на ідеї CoinJoin, де кілька користувачів об'єднують свої транзакції в одну спільну, так що стає незрозуміло, чия вхідна монета відповідає якій вихідній.

Анонімізація в Dash тримається на дворівневій мережі:

- 1-й рівень — звичайні ноди, які перевіряють і ретранслюють транзакції.
- 2-й рівень — masternodes, які мають мати 1000 Dash на балансі в якості застави, займаються міксуванням монет в рамках транзакцій.

Як це працює?

Коли з'являється транзакція, яку потрібно виконати (наприклад, переказати 10 монет), спочатку відбувається розбиття суми на деяку кількість дільників (100, 10, 1, 0.1, 0.01). Потім відправник надсилає запит перемішування на мастер-ноду (вона рандомізується на рівні клієнта, та не може бути одна і та сама мастер-нода декілька разів поспіль), та очікує на приєднання інших відправників задля ініціації змішування монет (якщо для змішування задіяна 1 монета, то у всіх інших теж буде така кількість). Коли до ноди підключається достатня кількість клієнтів, мастер-нода ініціює перемішування адрес в рамках цієї транзакції, надсилає клієнту назад вихідну адресу, на яку буде переказано 1 монету. Клієнт її перевіряє, підписує цю транзакцію (те саме робиться для інших учасників транзакції). Після цього транзакція ретранслюється серед всіх інших нод (1-го рівня також). Таким чином, вихідна сума (10 монет) не буде переказана із однієї адреси на якусь іншу адресу.

Для підвищення анонімності, таких раундів змішування відбувається декілька (до 16).

Після змішування, монети знаходяться на гаманці відправника у статусі "pending" (в процесі), поки користувач не вирішить витратити ці монети.

Після змішування, можна робити реальну транзакцію з рахунку відправника, з адрес, які брали участь у змішуванні, на адресу отримувача.

Звісно, все спілкування між клієнтами та нодами зашифроване. На додачу, використовується проксі (інша мастер-нода в ролі реле-ноди).

Деанонімізувати подібні транзакції цілком можливо.

Наприклад, через атаку через Multi-Input Heuristic.

Якщо транзакція має кілька входів (inputs) – і всі вони беруть участь в одному платіжному акті, то дуже ймовірно, що всі вони належать одному користувачу.

Наприклад витрачається 2.5 DASH, зібрані з 2 та 0.5. У транзакції видно 2 входи. З високою ймовірністю аналітик вважатиме, що обидва належать одній людині, і ці адреси будуть пов'язані між собою.

Ще одна атака – Sybil-атака на рівні мастер-нодів.

Якщо атакувальник розгортає велику кількість мастер-нодів (нагадаємо, що умова для системи – мати 1000 монет), то він може контролювати CoinJoin-сесії і спостерігати за тим, хто з ким змішується.

Це доволі дорогий тип атаки, але не неможливий на рівні структур, що оперують величезними коштами (держустанови, компанії з великою капіталізацією).

Також, беручи до уваги той факт, що для PrivateSend використовуються фіксовані деномінації, а треба переказати суму, що не вкладається у ці номінації, то залишок може повернутись назад до відправника, тим самим повністю зруйнувавши анонімність транзакції. Але це легко оминути на рівні системи, заблокувавши переказ подібних сум, або ручною регуляцією суми, що буде брати участь у переказах.

А якщо додавати нові, менші номінали (0.001 і так далі), то подібні транзакції ставатимуть обчислювально невигідними, бо такі номінали теж треба перемішувати, і в сумі буде на порядок більше транзакцій, як при змішуванні, так і при переказі коштів.

Наостанок, якщо при змішуванні використовується проксі для анонімізації IP-адреси ініціатора сеансу змішування, то при переказі коштів це не передбачено, тому слід використовувати VPN задля додаткового приховання IP-адреси в мережі блокчейн.

Втім, якщо порівнювати рівень анонімності Dash із Bitcoin/Litecoin, то можна побачити такі ключові аспекти ступеня анонімності:

Характеристика	Dash	Bitcoin	Litecoin
Вбудована анонімність	PrivateSend (CoinJoin)	Немає (можна вручну через CoinJoin-сервіси)	Немає
Мікшування в клієнті	Автоматичне через Core Wallet	Лише сторонні сервіси (JoinMarket, Wasabi)	Тільки через сторонні гаманці
Тип технології	CoinJoin через Masternode	Можна використовувати CoinJoin або PayJoin	Можна використовувати MimbleWimble
Публічність адрес та балансів	Публічні, але складно зв’язати при PrivateSend	Абсолютно публічні	Абсолютно публічні
IP-скритність під час змішування	Через relay-masternodes	Відкриті, якщо не використовувати Tor	Те саме
PrivateSend-транзакції у блокчейні	Виглядають як стандартні, але з типовими номіналами	Потрібно вручну формувати CoinJoin	Аналогічно
Вразливість до deanonymization	Середня (через multi-input, Sybil)	Висока (усі зв’язки відкриті)	Висока
Наявність інструментів аналізу	Обмежені, складніше аналізувати змішування	Chainalysis, Elliptic	Chainalysis
Захист від повторного зв'язування адрес	Якщо правильно використано PrivateSend (потрібні суми)	Дуже слабкий	Дуже слабкий