Оцінка Конфіденційності Децентралізованих Платіжних Систем

Світлана Халімова
Кафедра Електронні Обчислювальні Машини
Харківський національний університет радіоелектроніки
Харків, Україна
svitlana.khalimova@nure.ua

Богдан Скрябін
Кафедра Безпеки Інформаційних Технологій
Харківський національний університет радіоелектроніки
Харків, Україна
skriabin@hotmail.com

Assessment of the Confidentiality of Decentralized Payment Systems

Svetlana Khalimova
Electronic Calculating Machines Department
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
svitlana.khalimova@nure.ua

Bogdan Skryabin
Information Security Department
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
skriabin@hotmail.com

***Анотація*—проведений аналіз конфіденційності користувачів децентралізованих платіжних систем, запропоновані методи підвищення рівня конфіденційності в залежності від вимог користувача.**

***Abstract*—the analysis of the confidentiality of users of decentralized payment systems, suggested ways to increase the level of confidentiality, depending on the requirements of the user.**

Ключові слова—платіжна система, конфіденційність, невідстеженість, анонімніст, транзакції

Keywords—payment system, confidentiality, untraceability, anonymity, transactions

I. Вступ

У даний час все більше розповсюдження отримують децентралізовані платіжні системи на основі технології blockchain. Протоколи децентралізованих платіжних систем, такі як Bitcoin, Monero, Bitshares, Zcash, Dash, побудовані на принципу, коли кожна окрема робоча станція в системі не довіряє іншим. Ці системи мають типові вразливості, пов’язані з конфіденційністю користувачів. Тому актуальним питанням для децентралізованих платіжних систем є забезпечення необхідного рівня конфіденційності користувачів.

II. Конфіденційність платіжних систем

Поняття конфіденційності включає в себе дві основні складові: untraceability (невідстеженість) і anonymity (анонімність). Untraceability полягає у неможливості віднести групу дій до деякого користувача в мережі. Anonymity пов'язана з неможливістю достовірно встановити особу користувача.

Для забезпечення максимального рівня конфіденційності потрібно приховувати дані про транзакції - дані про походження монет, суму переказів, адреси відправника і одержувача в тілі транзакції. Важливо також приховати мережеві адреси користувачів, що зазвичай досягається за допомогою даркнета, де використовуються такі протоколи, як Freenet, TOR і I2P.

Результати аналізу конфіденційності платіжних систем представлені в таблиці 1 [1-5].

Аналіз показує, що деякі платіжні системи не відповідають вимогам конфіденційності. Найпростіша реалізація біткоін гаманця здатна забезпечити тільки мінімальний рівень конфіденційності.

Для підвищення конфіденційності децентралізованих платіжних систем існує декілька методів.

III. Методи підвищення конфіденційності платіжних систем

A. *Метод CoinJoin*

Найпростішим методом для заплутування графа транзакцій є CoinJoin. Суть даного методу полягає в створенні спільної транзакції, внаслідок чого походження відправляються монет стає неоднозначним. Формується група з користувачів, які створюють загальну транзакцію, в рамках якої одночасно відбувається кілька платежів (рис. 1).

TABLE I. Порівняння платіжних систем по конфіденційності

Складові конфіденційності	Monero	Zcash	Bitshares	Dash	Bitcoin	Central Bank Currency
Історія проходження монет	заплутування (за замовчуванням)	прихована (за замовчуванням)	відкрита (за замовчуванням)	заплутування (опціонально)	відкрита (за замовчуванням)	відкрита (обов'язково)
Сума переказу	прихована (за замовчуванням)	прихована (за замовчуванням)	прихована (опціонально)	заплутування (опціонально)	відкрита (завжди)	відкрита (обов'язково)
Ідентифікатори користувачів	приховані (за замовчуванням)	приховані (за замовчуванням)	приховані (опціонально)	приховані (опціонально)	приховані (опціонально)	відкриті (персональні)
Анонімність мережевого трафіку	підтримується (опціонально)	можливо (вручну)	можливо (вручну)	можливо (вручну)	можливо (вручну)	можливо (вручну)

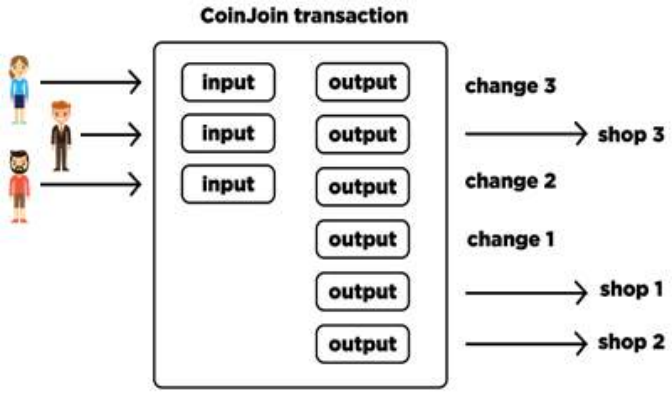

Рис.1. Схема роботи методу CoinJoin

Монета, яка пройшла ланцюжок таких транзакцій, має тисячі можливих варіантів походження.

B. *Метод Chaumian CoinJoin*

Модифікацією методу CoinJoin є Chaumian CoinJoin, заснований на використанні централізованого оператору і сліпого підпису. Оператор потрібен, щоб виконати перемішування входів і виходів, після чого скласти кінцеву транзакцію. В такому випадку ні користувачі, ні сам оператор не можуть деанонімізіровать монети на вихідних адресах. Метод містить цілий ряд механізмів захисту для протистояння несприятливим сценарієм, які дозволяють чесним користувачам гарантовано сформувати кінцеву транзакцію. Механізми захисту використовують таймаут, відстеження невитрачених виходів та інші.

C. *Метод CoinShuffle*

Модифікацію CoinJoin, під назвою CoinShuffle запропонували в 2014 році. Її перевагою є відсутність центрального оператора. Користувачі самостійно формують загальну транзакцію, спілкуючись між собою. При цьому вони не можуть порушити конфіденційність перемішування вихідних адрес. Ще одна перевага цієї методики полягає в тому, що користувачам не обов'язково використовувати додаткові мережі для анонімізації трафіку, так як всі необхідні властивості будуть досягнуті при використанні P2P- протоколу взаємодії учасників.

На даний час існують практичні реалізації CoinShuffle. Вони ефективно працюють навіть на групах з декількох десятків користувачів. Очікується інтеграція цього протоколу до деяких біткоін гаманців.

Недоліком методів, заснованих на CoinJoin, є велика складність off-chain взаємодії для формування транзакції, а також вразливість до CoinJoin Sudoku analysis, який заснований на зіставленні сум на виходах транзакцій.

Іншим методом, який вирішує проблему відкритих сум переказу, є Confidential Transactions.

D. *Метод Confidential Transactions*

Особливість методу Confidential Transactions (CT) полягає в тому, що він повністю приховує фактичні суми на входах і виходах транзакції від третіх осіб. Кожен може перевірити, що сума всіх виходів не перевищує суму всіх входів, чого вже достатньо для валідації цієї транзакції.

З метою боротьби з неконтрольованою емісією монет в цій схемі застосовується доказ використання допустимих сум на виході транзакції. Щоб перевірити, що були використані невід'ємні суми, які не перевищують порядок базової точки, застосовуються так звані Range Proofs.

Однак створення Range Proofs досить затратно з точки зору обчислювальних ресурсів, так як вони мають дуже великий обсяг. Теоретично інтегрувати Confidential Transactions в протокол біткоін можна, але практичних реалізацій на даний час не існує через їх великий обсяг. Проте вже є працюючі системи обліку, де Confidential Transactions успішно застосовуються.

E. Методика Ring Confidential Transactions

Для заплутування історії походження монет в методі Ring Confidential Transactions використовуються кільцевий підпис. Застосування кільцевих підписів таким чином було вперше запропоновано в протоколі CryptoNote, на базі якого працюють кілька криптовалют.

Ring Confidential Transactions використовує CT. Він дозволяє створювати транзакції з безліччю входів і виходів, де неможливо однозначно відстежити походження кожного входу, суми переказів приховані, а взаємодія з іншими користувачами для створення транзакції не потрібна.

F. Метод Stealth Addresses

Для прихованого розрахунку адрес, на які будуть відправлятися монети використовують метод Stealth Addresses. В якості ідентифікаторів користувачів використовуються відкриті ключі. На основі відкритого ключа отримувача та своєї пари ключів відправник розраховує новий одноразовий відкритий ключ, який вказується в транзакції в якості адреси. Для стороннього спостерігача зв'язок між ідентифікатором користувача і адресою на виході транзакції встановити неможливо.

IV. Підвищення конфіденційності за допомогою концепції MAST

Концепція MAST (Merkelized Abstract Syntax Tree) використовується дляє підвищення конфіденційністі і зменшення розміру транзакцій. Вона основана на ідеї дерева Меркле і абстрактного синтаксичного дерева для завдання взаємовиключних умов витрати монет.

Схема конструкції MAST представлена на рис. 2

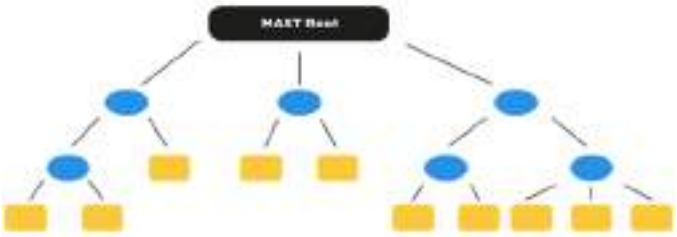

Рис.2. Схема конструкції MAST

Кореневе хеш-значення MAST Root, яке буде міститися виході транзакції, отримується на основі хеш-значень окремих елементів даних. Причому монети, які будуть витрачені найімовірніше, поміщають якомога ближче до кореня дерева.

Використання концепції MAST дозволяє вирішити проблеми:

- перекладає необхідність включення великих обсягів даних в транзакцію, тому відповідно підвищену комісію буде платити одержувач, а не відправник, що дозволяє задати більш об'ємні і складні умови витрати монет;
- зняти обмеження за розміром і кількістю операцій ScriptPubKey без шкоди для надійності за рахунок взаємовиключних умов;
- приховувати умови витрати монет до моменту самої витрати.

V. Висновки

Децентралізовані платіжні системи та незалежні цифрові валюти знайшли широке застосування завдяки високому рівню доступності та цілісності облікової системи, відсутності обмежень, простоти використання, а також за рахунок можливості значно підвищити рівень конфіденційності при їх використанні.

Проведений аналіз методів підвищення конфіденційності показав, що необхідно комбіноване використання цих методів. Перспективним для підвищення конфіденційності є використання концепції MAST.

Література References

[1] A Peer-to-Peer Electronic Cash System [Електронний ресурс]. Режим доступу: www / URL: https://bitcoin.org/bitcoin.pdf .

[2] Специфікація протоколу Bitcoin [Електронний ресурс]. Режим доступу: www / URL: https://en.bitcoin.it/wiki/Main_Page.

[3] Специфікація протоколу Ripple [Електронний ресурс]. Режим доступу: www / URL: https://wiki.ripple.com/Main_Page.

[4] Специфікація протоколу Bitshares [Електронний ресурс]. Режим доступу: www / URL: http://docs.bitshares.eu.

[5] Специфікація протоколу Ethereum [Електронний ресурс]. Режим доступу: www / URL: http://www.ethdocs.org/en/latest.