УДК 004.738

О.І. Макаренко
(Національний авіаційний університет, Україна)

Вирішення проблем анонімності та безпеки персональних даних фінансових систем за допомогою технології Blockchain

Наразі централізована фінансова система має істотні недоліки. Персональні дані концентруються у централізованих базах даних та підлягають достатньому ризику бути скомпрометованими. Існує проблема захисту персональних даних користувачів. Крім того існує проблема анонімності сторін транзакції.

Централізована фінансова система має певні недоліки. Висока концентрація влади дозволяє централізованим фінансовим установам маркувати, відслідковувати та навіть блокувати особисті активи людей, а також мати контроль над їх персональними даними.

Сервіси інтернет-додатків, засновані на централізованій архітектурі (включаючи фінансові послуги), збирають персональну інформацію про користувачів з різних причин для розвитку бізнесу, проте не приділяється достатньої уваги захисту конфіденційності користувачів.

Запропоноване вирішення проблеми базується на Blockchain-протоколі Monero, який у свою чергу походить з протоколу CryptoNote.

Протокол CryptoNote в основному вирішує дві проблеми:

1) невідстежуваність — це означає, що для всіх транзакцій, що входять, всі можливі відправники можуть бути джерелом, але невідомо, хто їх відправив;

2) непов'язаність — це означає, що неможливо довести, що будь-які дві вихідні транзакції відправлені від однієї й тієї ж людини.

Функція невідстежуваності використовує технологію кільцевого підпису. Ця технологія може вирішити проблему анонімності відправника транзакції.

Технологія кільцевого підпису заснована на концепції групового підпису, запропонованого Девідом Чаумом та Е. Ван Хейстом. Кільцевий підпис використовує кілька публічних підписів, які змішуються разом, щоб приховати реальний підпис транзакції, що не вплине на можливість перевірки дійсності транзакції. І слід зазначити, що пізніше було доведено, що технологія кільцевого підпису може бути простежена за певних обставин. Пізніше це питання вирішили в компанії Monero Ring Confidential Transactions (RingCTs).

Функція непов'язаності, використовує технологію одноразового ключа, яка може вирішити проблему анонімності одержувача транзакції.

Оскільки відкритий ключ необхідний під час зміни підпису, всі вхідні транзакції адреси відкритого ключа можна спостерігати на Blockchain, тому легко викрити всі сторони, що пов'язані з транзакцією.

Таким чином, удосконалена технологія обміну ключами Діффі-Хеллмана дозволяє генерувати одноразовий ключ для захисту всіх сторін. Загальний принцип полягає в тому, що відправник транзакції використовує

власні дані для хешування відкритого ключа одержувача і, таким чином, створює унікальний одноразовий ключ для транзакції, тому тільки одержувач може генерувати закриту частину транзакції.

Механізм верифікації Blockchain в основному оцінюється за шістьома аспектами: безпека, пропускна спроможність транзакцій, масштабованість, час підтвердження транзакцій, децентралізація та зайняття ресурсів.

Розглянемо покращений механізм верифікації, що формується через три етапи — PoW, PoW+ pure-proof-of-stake (PPoS) та PPoS. Його схема трансформації повторює схему ETH. Крім того, оскільки розглянуте рішення базується на протоколі Monero, його безпека, пропускна здатність транзакцій, масштабованість і час підтвердження транзакцій успадкували здатність Monero.

Додатково, за допомогою технології BlockDAG та технології шифрування була додатково покращена безпека (анти-51 % подвійна атака), пропускна здатність (TPS збільшена до 70) та час підтвердження транзакцій (близько 2 хвилин).

Висновки

У процесі досягнення анонімності окремий користувач має два закриті та два відкриті ключі для завершення всього процесу шифрування. Ring Signature гарантує анонімність відправника транзакції, Stealth Address гарантує анонімність одержувача транзакції, а технологія Ring Confidential Transactions (RingCTs) гарантує анонімність вмісту транзакції. Виділено покращений алгоритм верифікації.

Список літератури

1. Monero Ring Confidential Transactions. URL: https://www.getmonero.org/resources/ moneropedia/ringCT.html
2. Bitcoin Whitepaper. URL: https://bitcoin.org/bitcoin.pdf
3. CryptoNote Standards. URL: https://cryptonote.org/standards/
4. Frost Jon, Gambacorta Leonardo, and Gambacorta Romina. The Matthew Effect and Modern Finance. On the Nexus between Wealth Inequality, Financial Development and Financial Technology, 2020, SSRN: https://ssrn.com/abstract=3666377
5. David Cham. Group Signatures. EUROCRYPT '91. 1991. P. 257–265.