

АНАЛІЗ СПОСОБІВ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ПРИ КРИПТОВАЛЮТНИХ ТРАНЗАКЦІЯХ

ANALYSIS OF WAYS TO ENSURE ANONYMITY IN CRYPTOCURRENCY TRANSACTIONS

Юлія Каменєва¹, Ніна Здолбіцька²

¹Волинський національний університет ім. Лесі Українки, просп. Волі, 13, м. Луцьк, 43025, Україна

²Луцький національний технічний університет, вул. Львівська, 75, Луцьк, 43018, Україна

Abstract. *This work presents an analysis of ways to ensure anonymity in cryptocurrency transactions. The research was conducted with the aim of anonymity during transactions with cryptocurrency, which is desired by the population to protect their personal privacy.*

У світі криптовалют анонімність стала важливою особливістю для користувачів. У той час як традиційні фінансові системи часто вимагають від користувачів розкривати особисту інформацію під час транзакцій, криптовалюти пропонують рівень конфіденційності та безпеки, який дуже потрібний. Розуміння необхідності анонімності в транзакціях з криптовалютою має важливе значення для всіх, хто хоче залучити цю цифрову форму обміну. Огляд сучасних досліджень показує важливість анонімності при криптовалютних транзакціях.

У дослідженні "Anonymity Analysis of Cryptocurrencies" було показано, що кожна транзакція містить ідентифікаційну інформацію щодо адрес користувачів. Для кожної транзакції в ланцюжку блоків можна побачити між якими користувачів відбулася транзакція, а також кількість переказаних біткоїнів. Ці транзакції існують в загальнодоступному записі транзакцій для захисту від подвійних операцій витрачання біткоїнів. Через публічний характер цього запису та інформації пов'язаної з кожною транзакцією, можна вивести деяку, якщо не всю інформацію про користувачів мережі [1].

Метою дослідження "Analysis of Anonymity and Privacy of Crypto Currencies" було визначити чи транзакція повідомляє мережі, що власник криптовалюти санкціонував передачу цієї вартості іншому власнику. Інший власник тепер може витратити цифрову готівку, передавши вартість іншій особі. Оскільки ланцюжок блоків є цифровою книгою лише для додавання, криптовалюти використовують цю книгу для відстеження всіх транзакцій. Електронна пошта для Інтернету – це криптовалюта для блокування: невелика частина надзвичайно інноваційної технології, яка змінює світ [2].

Метою нашого дослідження є анонімність під час транзакцій з криптовалютою, якої прагне населення для захисту їх особистої конфіденційності. У традиційних банківських системах транзакції часто пов'язані з особистими даними, що полегшує органам влади або зловмисникам відстеження та моніторинг фінансової діяльності. Однак у випадку з криптовалютами транзакції є псевдонімними, тобто вони пов'язані з унікальними адресами, а не з реальними особами. Це дозволяє користувачам підтримувати рівень конфіденційності та захистити свою особисту інформацію від потрапляння в чужі руки.

У світі криптовалют анонімність є вирішальним фактором для багатьох людей. Це дозволяє користувачам захистити свою особистість, запобігти кібератакам і зберегти конфіденційність своїх транзакцій.

Монети конфіденційності пропонують вирішення цієї проблеми, надаючи користувачам безпечний та анонімний спосіб здійснення транзакцій. Ця функція особливо важлива для тих, хто хоче зберегти конфіденційність своєї фінансової інформації.

Нами проведено дослідження важливості анонімності в криптовалютних транзакціях і те, як монети конфіденційності відіграють важливу роль у досягненні цієї мети. При цьому обговорюються такі аспекти:

- захист особистих даних;
- фінансова конфіденційність;
- запобігання цензурі;
- варіанти використання;
- регуляторні проблеми;
- відповідальність користувача.

Анонімність при транзакціях забезпечується за допомогою:

- шифрування;
- децентралізація;
- псевдонім;
- криптовалюти, орієнтовані на конфіденційність;
- захищені гаманці;
- двофакторна автентифікація.

Під час роботи було досліджено важливість анонімності в криптовалютних транзакціях і те, як монети конфіденційності відіграють важливу роль у досягненні цієї мети. Монети конфіденційності використовують розширену криптографію, щоб приховати особистість користувачів і їхні транзакції від сторонніх очей, що значно ускладнює атаку зловмисникам.

Дотримання балансу між анонімністю та прозорістю, впровадження надійних заходів безпеки, розгляд монет конфіденційності, вирішення регуляторних проблем і сприяння відповідальності користувачів – усе це важливі аспекти, які слід враховувати в цій сфері. Розуміючи ці нюанси, окремі особи та організації можуть ефективно орієнтуватися в етичному ландшафті криптовалюти в бізнесі.

Забезпечення анонімності при транзакціях виконується за допомогою шифрування; децентралізації; псевдоніму; криптовалют, орієнтованих на конфіденційність; захищених гаманців та двофакторної автентифікації.

Використовуючи ці заходи та розуміючи нюанси анонімності та безпеки в транзакціях з криптовалютою, користувачі можуть приймати обґрунтовані рішення та ефективно захищати свої цифрові активи.

Бібліографія

1. Morris L. (2015). Anonymity Analysis of Cryptocurrencies. Rochester Institute of Technology RIT Digital Institutional Repository, 20-23.
2. D. Madhusudhana Rao, Subba Rao Peram, B. Premamayudu (2020). Analysis of Anonymity and Privacy of Crypto Currencies. International Journal of Advanced Science and Technology, 44-48.