ДОКАЗИ ІЗ НУЛЬОВИМИ ЗНАННЯМИ НА БАЗІ ДЕРЕВ МЕРКЛА

Гаража Р.Ю., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Доказ із нульовими знаннями (з нульовим розголошенням) — тип доказу, який дозволяє одній стороні довести істинність певного твердження іншій стороні без розкриття будь-якої іншої інформації, крім істинності цього твердження. Можливими способами застосування доказів із нульовими знаннями є анонімні онлайн-голосування, цифрові ідентифікаційні документи, блокчейн, тощо.

Метою доповіді є аналіз можливостей застосування дерев Меркла для забезпечення надійності доказів із нульовими знаннями. В доповіді розглянуто структуру та механізм побудови дерева Меркла та проаналізовано його властивості, корисні для реалізації саме протоколів доказу з нульовими знаннями. Аналізуються різні групи доказів із нульовими знаннями (інтерактивні та неінтерактивні).

У випадку з онлайн-голосуваннями дерево Меркла може бути утвореним списком користувачів, що мають право голосувати. Дерево Меркла цифрового ідентифікаційного документу, в свою чергу, може включати ім'я та прізвище, дату народження, стать, особистий податковий номер, тощо. Блокчейн може бути використаний у якості довіреної сторони, що зберігає корені дерев Меркла розподіленим чином, гарантуючи доступність цих даних для сторони, що перевіряє, тобто для безпосереднього залучення у конкретних випадках застосування доказів із нульовими знаннями на базі дерев Меркла.

Щоб підтвердити факт входження певного блоку даних до дерева Меркла або факт володіння даними, що утворюють дерево Меркла, як такий, сторона, що доводить, має надати стороні, що перевіряє, листок (або певний блок даних, якщо це необхідно) та ті мінімально необхідні вузли дерева, що потрібні для розрахунку кореня дерева. Дерево Меркла для такої перевірки зазвичай доступне публічно або надається третьою довіреною стороною (trusted third party).

Проведений аналіз показав, що дерево Меркла є надійним засобом реалізації доказів із нульовими знаннями як таких, що гарантує нерозголошення зайвої інформації, високу масштабованість, невеликий час перевірки та розмір доказу. Дерево Меркла знайшло своє застосування для перевірки справжності й цілісності даних, що зберігаються, обробляються та передаються у peer-to-peer мережах (наприклад, BitTorrent та IPFS).

Список літератури

1. What is a zero-knowledge proof and why is it useful? [Електронний ресурс] / Режим доступу: https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/;
2. Merkle tree patent. [Електронний ресурс] / Режим доступу: https://patents.google.com/patent/US4309569.