Секція 2

ДОСЛІДЖЕННЯ МЕТОДІВ РЕАЛІЗАЦІЇ БЛОКЧЕЙН ПРОТОКОЛІВ З ДОКАЗОМ НУЛЬОВОГО ЗНАННЯ

Тяпко М. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Харченко В. С.

Актуальність. Зі зростанням використання технології блокчейну приватність стала значущою проблемою у фінансових транзакціях [1]. Традиційні системи блокчейну є прозорими, що означає, що всі транзакції є публічно доступними. Прозорість блокчейну - це функція, яка забезпечує відповідальність та усуває потребу в посередниках. Однак ця прозорість може стати проблемою для користувачів, які хочуть зберегти конфіденційність своїх транзакцій. Тому існує потреба у більш безпечному та ефективному методі проведення приватних транзакцій на блокчейні. Для можливості приватних транзакцій на блокчейні були розроблені докази нульового знання [2].

Метою цього дослідження є вивчення використання ZK-доказів для транзакцій з підвищеною приватністю в блокчейн протоколах.

Основні положення. Нинішні методи здійснення приватних транзакцій на блокчейні є обмеженими та часто ґрунтуються на довірі до третіх сторін. Наприклад, використання міксерів [3] може бути скомпрометовано зловмисниками, які можуть відстежувати рух коштів [4]. Крім того, рішення, що працюють поза ланцюжком, такі як Lightning Network [5], потребують використання довірених посередників, що суперечить децентралізованій природі блокчейну. Дослідження включає огляд літератури щодо існуючих методів здійснення приватних транзакцій на блокчейні та аналіз обмежень цих методів. Дослідження також включає оцінку використання доказів знань для підвищення приватності транзакцій.

Висновки. Використання доказів нульового знання (ZK-докази) для транзакцій з підвищеною приватністю на блокчейні є перспективним напрямом дослідження. Дослідження може допомогти в розробці більш безпечних та ефективних систем блокчейну, досліджуючи існуючі методи проведення приватних транзакцій на блокчейні з використанням ZK-доказів. Результати дослідження можуть допомогти виявити обмеження існуючих методів та дати висновки щодо оптимізації їх продуктивності. Крім того, дослідження може оцінити ефективність та продуктивність існуючих методів та надати рекомендації щодо їх удосконалення. Знання, отримані в результаті дослідження, можуть сприяти розвитку кращого розуміння використання ZK-доказів для транзакцій з підвищеною приватністю на блокчейні та можуть бути корисними для розвитку майбутніх досліджень в цій галузі.

Список літератури

1. Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies. URL: https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf (дата звернення 11.04.2023);
2. *Justin Thaler*. Proofs, Arguments, and Zero-Knowledge – с. 171. *Georgtown University*. URL: https://people.cs.georgetown.edu/jthaler/ProofsArgsAndZK.pdf (дата звернення: 13.04.2023);
3. On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy – с. 11. *ARXIV*. URL: https://arxiv.org/pdf/2201.09035.pdf (дата звернення 11.04.2023);
4. Analyzing the Bitcoin Transaction Graph: A Look at Mixers and Traceability – с. 11. *MIT* URL: http://www.css.csail.mit.edu/6.858/2013/projects/jeffchan-exue-tanyaliu.pdf (дата звернення: 11.04.2023);
5. *Joseph Poon, Traddeus Dryja.* The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. URL: https://lightning.network/lightning-network-paper.pdf (дата звернення: 11.04.2023).

Відомості про авторів

Тяпко Михайло Вікторович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», m.tiapko@student.csn.khai.edu
Харченко В'ячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н, професор, v.kharchenko@csn.khai.edu