

**ФІНАНСОВІ ОРГАНІЗАЦІЇ, ЗАСНОВАНІ НА БЛОКЧЕЙН-РОЛАПАХ
НА БАЗІ ДОКАЗІВ ІЗ НУЛЬОВИМ РОЗГОЛОШЕННЯМ**

Гаража Р.Ю.

Науковий керівник — к.т.н. Мельникова О.А.

Харківський національний університет радіоелектроніки, каф. БІТ

м. Харків, Україна

e-mail: roman.harazha@nure.ua.

This work is devoted to the research of the potential of accounting systems of financial organizations, implemented with the help of zero-knowledge blockchain rollups. Such accounting systems will allow to combine the positive qualities of traditional accounting systems and decentralized accounting systems based on the blockchain. To do this, it is necessary to use the following set of technologies: a blockchain-based accounting system, a decentralized consensus protocol, an EVM-like virtual computing environment, zero-knowledge blockchain rollups to ensure information security and low transaction costs.

Зважаючи на прогрес у галузі блокчейн-технологій, втілення банківських та інших фінансових систем на їх базі стає все більш надійним рішенням для забезпечення цілісності банківських (фінансових) даних. При цьому окремі невід’ємні якості децентралізованих облікових систем на базі блокчейну сповільнюють їх впровадження у банківському секторі. Серед таких — доступність даних, що в традиційних банківських системах є приватними (баланси і транзакції користувачів), а також висока вартість оновлення стану системи в популярних децентралізованих облікових системах, таких як Bitcoin та Ethereum.

З іншого боку, вже існують рішення, що дозволяють значно зменшити вартість оновлення стану системи. Саме до таких рішень відносяться блокчейн-ролапи (англ. Blockchain Rollups) та їх модифікація — блокчейн-ролапи на базі доказів із нульовим розголошенням (англ. Zero-Knowledge Blockchain Rollups), які здатні забезпечити приватність транзакцій.

Блокчейн — база даних у формі зв’язного списку блоків даних. Зазвичай зв’язність забезпечується не лише за допомогою порядкових номерів блоків, а й за допомогою геш-суми, що міститься у кожному блоці разом із геш-сумою попереднього блоку. Таким чином, зміна вмісту блоку призводить до зміни його геш-суми і розриву списку, що допомагає у перевірці цілісності даних. Блокчейн зазвичай лежить в основі децентралізованих облікових систем, що мають свої протоколи досягнення консенсусу (Proof-of-Work, Proof-of-Stake, Proof-of-Authority та ін.) щодо стану облікової системи.

EVM (Ethereum Virtual Machine) — віртуальне обчислювальне середовище, що лежить в основі децентралізованої облікової системи Ethereum. У цьому середовищі виконуються смарт-контракти та зберігаються дані, що є результатом їх виконання (при цьому виконання смарт-контрактів вимагає витрати нативної валюти системи Ethereum). Мова програмування смарт-контрактів Solidity є повною за Тюрінгом і дозволяє втілення наскільки завгодно складних операцій над отриманими смарт-контрактом даними. Облікова система Ethereum стала основою для багатьох застосунків у сфері децентралізованих фінансів (DeFi).

Доказ із нульовим розголошенням (англ. Zero-Knowledge Proof) — тип доказу, який дозволяє одній стороні довести істинність певного твердження іншій стороні без розкриття будь-якої іншої інформації, крім істинності цього твердження. В області інформаційних технологій доказ із нульовим розголошенням дозволяє довести правильність виконання певних обчислень, не розкриваючи при цьому вхідні дані, над якими обчислення були проведені. Особливістю доказів із нульовим розголошенням є константна, логарифмічна або поліноміальна складність перевірки доказу, значно менша у порівнянні зі складністю створення доказу (зазвичай лінійно-логарифмічна).

Блокчейн-ролапи (англ. Blockchain Rollups) — технологія для протоколів другого рівня для облікових систем на базі EVM, основною метою використання якої є зменшення витрат на виконання транзакцій. Це досягається за рахунок об'єднання великої кількості транзакцій другого рівня в єдиний пакет (батч, англ. batch), що публікується в якості однієї транзакції в цільовій обліковій системі (першого рівня), до якої висувуються ті ж вимоги щодо правильності, що й до інших транзакцій. Таким чином, використання ролапів дозволяє поєднати високу швидкість виконання транзакцій та низькі витрати із інформаційною безпекою, що гарантує значно децентралізована облікова система першого рівня.

Блокчейн-ролапи на базі доказів із нульовим розголошенням (англ. Zero-Knowledge Blockchain Rollups) — технологія ролапів, ключовою особливістю якої є застосування доказів із нульовим розголошенням для ще більшої оптимізації обчислень в обліковій системі першого рівня.

Облікова система другого рівня може мати додаткові властивості у порівнянні з обліковою системою першого рівня:

- бути приватною, тобто для доступу до неї може бути потрібен дозвіл;
- транзакції в ній можуть мати додаткові засоби забезпечення інформаційної безпеки (докази із нульовим розголошенням, гомоморфне шифрування і таке інше);
- реалізовувати вбудовані механізми управління, не властиві системі першого рівня (наприклад, голосування);

— мати додаткові обмеження щодо стану системи та перевірки на їх задовільнення (наприклад, банківська установа не повинна мати зобов'язань більше, ніж активів).

Таким чином, стає можливим окреслити особливості системи банку на базі комплексу вищезазначених технологій:

- облікова система на базі блокчейну для зберігання даних;
- децентралізований протокол досягнення консенсусу;
- EVM-подібне віртуальне обчислювальне середовище для виконання фінансових операцій;
- блокчейн-ролапи на базі доказів із нульовим розголошенням для забезпечення додаткової інформаційної безпеки засобами системи першого рівня та нижчої вартості транзакцій.

Додатковими рішеннями можуть бути блокчейн-мости (бріджі, англ. bridges), що дозволяють виконувати транзакції між різними децентралізованими обліковими системами (таким чином зможуть комунікувати між собою різні банківські установи, які використовують описаний комплекс технологій, а їх клієнти — переводити між ними кошти і т. п.).

Крім операцій з переводу коштів, можливо також реалізувати й інші банківські та біржеві фінансові інструменти, що вже знайшли своє втілення у DeFi-сфері. До таких інструментів відносяться:

- децентралізовані біржі: традиційні (побудовані на біржових ордерах) або автоматизовані маркет-мейкери (англ. Automated Market Makers); другі втілюють механізм пулів ліквідності (англ. Liquidity Pools), тобто автоматично визначають ціну одного активу відносно другого в залежності від співвідношення їх пропозиції у визначеному пулі;
- протоколи кредитування: дозволяють отримувати позику в обмін на заставу, причому управління заставою здійснюється смарт-контрактом;
- децентралізовані стейблкоїни (англ. Stablecoins) — активи, ціна яких прив'язана до вартості певних активів реального світу (національних валют, акцій, золота і т. д.);
- інші (наприклад, децентралізовані автономні організації, що керують коштами інвесторів).

Список використаних джерел

1. Кравченко П., Скрябін Б., Дубініна О. Блокчейн і децентралізовані системи: навч. посібник для студ. закл. вищ. осв. У трьох частинах. Ч. 1. Харків : ПРОМАРТ, 2023. — 460 с. — ISBN 978-617-7634-40-8.
2. Ethereum Virtual Machine (EVM). URL: <https://ethereum.org/en/developers/docs/evm/> (дата звернення: 05.03.2024).
3. Rollup. URL: <https://www.techopedia.com/definition/rollup> (дата звернення: 05.03.2024).
4. Zero-knowledge proofs explained: Part 1. URL: <https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/> (дата звернення: 05.03.2024).