УДК 621.391:519.2:519.7

Л.В. КОВАЛЬЧУК
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна;
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, e-mail: *lusi.kovalchuk@gmail.com*.

М.С. КОНДРАТЕНКО
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, e-mail: *nikolay.ns95@gmail.com.*

ВИЗНАЧЕННЯ КІЛЬКОСТІ БЛОКІВ ПІДТВЕРДЖЕННЯ У ДВОРІВНЕВОМУ БЛОКЧЕЙНІ З ПРОТОКОЛОМ КОНСЕНСУСУ PROOF-of-PROOF ЗА РІЗНИХ ТИПІВ КОНСЕНСУСУ У МЕЙНЧЕЙНІ / САЙДЧЕЙНІ ДЛЯ ЗАПОБІГАННЯ АТАКИ ПОДВІЙНОЇ ВИТРАТИ. II. PoW У МЕЙНЧЕЙНІ ТА PoS У САЙДЧЕЙНІ

Анотація. У роботі розглянуто питання безпечного функціонування дворівневого блокчейну зі складним змішаним протоколом консенсусу — Proof-of-Work в основному блокчейні (мейнчейні) та Proof-of-Stake в другорядному блокчейні (сайдчейні). Принцип побудови такого блокчейну базується на протоколі Proof-of-Proof, коли стійкий блокчейн (мейнчейн) використовується для забезпечення стійкості сайдчейну шляхом посилання блоків мейнчейну на блоки сайдчейну з використанням спеціальних транзакцій. Така структура дозволяє швидше випускати блоки у сайдчейні і відповідно швидше обробляти транзакції без зниження стійкості та без збільшення об'єму блоку. У свою чергу, такий дворівневий блокчейн становить найбільший інтерес для створення каскадної системи державних реєстрів, яка буде гарантовано захищена від підміни та підробки документів. Основним результатом роботи є отримання явних аналітичних виразів для оцінювання ймовірності атаки подвійної витрати на сайдчейни у такому дворівневому блокчейні, за умови наявності зловмисника як у сайдчейні, так і у мейнчейні. За отриманими формулами можна визначити необхідну кількість блоків підтвердження у сайдчейні, що гарантують стійкість до вказаної атаки з імовірністю, не меншою за задану.

Ключові слова: блокчейн, мейнчейн, сайдчейн, криптовалюти, майнінг, протокол консенсусу Proof-of-Proof, атака подвійної витрати.

ВСТУП. ОГЛЯД ЛІТЕРАТУРИ

Ця стаття продовжує дослідження роботи [1] і завершує серію досліджень стійкості дворівневого протоколу консенсусу Proof-of-Proof (PoP) [2, 3] до атаки подвійної витрати у блокчейні, який успадковує стійкість (security inherited blockchain).

Ідея функціонування та забезпечення стійкості протоколу консенсусу PoP є наближеною до ідеї створення сайдчейнів (sidechains). Концепція створення сайдчейнів дуже поширена у блокчейн-технології, наприклад існує велика кількість сайдчейнів у блокчейні Ethereum: Arbitrum [4], Optimizm [5], Polygon [6] тощо. Вона полягає у створенні певної надбудови (другорядного блокчейну, тобто сайдчейну) до гарантовано стійкого (основного) блокчейну. Така надбудова, з одного боку, забезпечує стійкість сайдчейну за рахунок стійкості основного блокчейну (mainchain), а з іншого — дає змогу швидше (а часто і дешевше) обробляти транзакції. Існує багато робіт, присвячених застосуванню сайдчейнів, особливо для IoT (Internet of Things) [7–10].

Автори протоколу PoP використовують іншу термінологію, ніж прийнято стосовно сайдчейнів. Основний блокчейн (mainchain) вони називають security provided blockchain, тобто блокчейн, що забезпечує стійкість щодо основних атак (на структуру блокчейну); блокчейн, що відіграє роль другорядного (тобто