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*.

Н.В. КУЧИНСЬКА
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: *n.kuchinska@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 АТАЦІ ПОДВІЙНОЇ ВИТРАТИ. I. PoS У МЕЙНЧЕЙНІ ТА PoW У САЙДЧЕЙНІ

Анотація. Розглянуто питання безпечного функціонування дворівневого блокчейну зі складним змішаним протоколом консенсусу Proof-of-Stake в основному блокчейні (мейнчейні) та протоколом Proof-of-Work у другорядному блокчейні (сайдчейні). Дворівневий блокчейн побудовано за принципом протоколу Proof-of-Proof, коли стійкість сайдчейну забезпечена стійкістю мейнчейну через посилання блоків мейнчейну на блоки сайдчейну з використанням спеціальних транзакцій. Ця структура дає змогу швидше створювати блоки у сайдчейні і відповідно швидше обробляти транзакції, не знижуючи стійкості та не збільшуючи обсягу блоку. Такий дворівневий блокчейн є найбільш зручним для створення каскадної системи державних реєстрів, гарантовано захищаючи від підміни та підробки документів. Основний результат роботи — отримання явних аналітичних виразів для оцінки ймовірності атаки подвійної витрати, направленої на сайдчейн у дворівневому блокчейні за умови наявності зловмисника як у сайдчейні, так і у мейнчейні.

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

ВСТУП

Поняття протоколу консенсусу в блокчейні з'явилось у роботі [1], де Сатоші Накамото вперше ввів означення блокчейну. У цій роботі розглянуто лише протокол консенсусу Proof-of-Work (PoW) [2] і при цьому взагалі не визначено можливості використання інших протоколів консенсусу. Цей протокол і наразі залишається найбільш поширеним, однак його численні недоліки спонукали дослідників іншим шляхом досягати консенсусів. Детальніші огляди основних сучасних протоколів консенсусу можна знайти в роботах [3–7].

Протокол консенсусу є базовим для коректного функціонування блокчейну, його властивості визначають стійкість блокчейну до атак [8]. Тому багато наукових робіт, дотичних до теми блокчейну, присвячено саме порівняльному аналізу протоколів консенсусу та, насамперед аналізу їхньої стійкості до основних типів атак [8, 9]. Зазначимо, що в усіх наведених вище роботах аналізували класичний однорівневий блокчейн, для якого на цей час отримано багато результатів.

Ця робота суттєво відрізняється від зазначених вище, оскільки досліджує проблему безпечного функціонування дворівневого блокчейну [10] зі складним