СИСТЕМНИЙ АНАЛІЗ

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.*

І.М. КУЗНЄЦОВ
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *sea_hawk@icloud.com.*

М.Ю. КУЗНЄЦОВ
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна;
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *kuznetsov2024@ukr.net.*

ПРИСКОРЕНЕ МОДЕЛЮВАННЯ ОДНІЄЇ ІЗ СТРАТЕГІЙ АТАКИ РОЗГАЛУЖЕННЯ НА БЛОКЧЕЙН, ЯКИЙ ГРУНТУЄТЬСЯ НА ПРОТОКОЛІ КОНСЕНСУСУ PROOF-OF-STAKE[1]

Анотація. Однією з найважливіших та найнебезпечніших атак на блокчейн є атака розгалуження, коли зловмиснику вдається побудувати альтернативний ланцюг блоків якомога більшої довжини. У цій статті запропоновано нову модель здійснення такої атаки, визначено основні правила її виконання, а саме за яких умов зловмисник починає створювати розгалуження та до якої саме гілки він приєднує новий блок. При цьому використано стандартний підхід до визначення поведінки чесних слотлідерів: вони завжди приєднують нові блоки до більш довгої гілки; у випадку розгалуження (тобто наявності двох гілок однакової довжини) мають змогу вибирати будь-яку з них. Запропоновано метод прискореного моделювання, який дає змогу оцінити ймовірність того, що довжина розгалуження досягне певної величини. Цей метод ґрунтується на сумісному використанні як елементів методу Монте-Карло, так і імплантованих рекурентних формул. Для перевірки коректності запропонованого методу на числових прикладах здійснено порівняння оцінок, отриманих цим методом та стандартним методом Монте-Карло. Залежно від оцінюваної ймовірності метод прискореного моделювання дає виграш у часі, що може складати декілька порядків.

Ключові слова: блокчейн, Proof-of-Stake, атака розгалуження, стейкхолдер, таймслот, слотлідер, метод Монте-Карло, прискорене моделювання.

ВСТУП. ПОСТАНОВКА ЗАДАЧІ

У цій роботі продовжено дослідження однієї з основних атак на блокчейн — так звану атаку розгалуження (Splitting Attack) [1]. У роботі [2] надано детальний опис цієї атаки, включаючи її алгоритм та мотиви зловмисника. У цій роботі стисло подамо основні моменти атаки.

[1]Дослідження здійснено в рамках проєкту «Розвиток розподіленої енергетики в умовах ринку електричної енергії України з використанням технологій та систем цифровізації», що виконується за напрямом використання бюджетних коштів «Підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок» бюджетної програми КПКВК 6541230 в НАН України.