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.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.*

А.А. ШУМСЬКА
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *shumska-aa@ukr.net.*

МОДЕЛЮВАННЯ СПРОЩЕНОГО ВАРІАНТА АТАКИ РОЗГАЛУЖЕННЯ НА БЛОКЧЕЙН, ҐРУНТОВАНИЙ НА ПРОТОКОЛІ КОНСЕНСУСУ PROOF-OF-STAKE[1]

Анотація. Відомо, що атака розгалуження є однією з найважливіших атак на блокчейн, насамперед для протоколів Proof-of-Work та Proof-of-Stake, як найбільш поширених. На сьогодні немає явних аналітичних формул для обчислення ймовірності її успіху, що викликає певну недовіру до блокчейн-технологій. У цій роботі для спрощеної (але все одно достатньо складної з математичного погляду) моделі атаки розгалуження отримано рекурентні формули, які дають змогу знаходити точні значення ймовірності того, що зловмисник зможе побудувати розгалуження заданої довжини. Коректність цих формул перевіряється на числових прикладах методом Монте-Карло шляхом побудови оцінок із заданими достовірністю та відносною похибкою.

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

ВСТУП

Поняття блокчейну введено в історичній роботі Накамото [1], і сьогодні вже всім зрозуміло, що ця нова сутність мала значний вплив як на напрям розвитку IT-технологій, так і на світову економіку. Структура блокчейну суттєво використовує різні криптографічні механізми. У найпершій роботі це були геш-функції та цифрові підписи; на сьогодні перелік цих механізмів суттєво розширено за рахунок додавання перевірних випадкових функцій (Verifiable Random Functions, VRF) [2], гібридних алгоритмів шифрування [3], кільцевих підписів [4], різних типів доведень без розголошення — SNARK, STARK [5], One-Out-of-Many proof [6], Range proof [7] тощо. Тому блокчейн-технології можна також вважати певним новим напрямом у криптології. Блокчейн-структури зараз розглядають набагато ширше, ніж додатки для створення криптовалют. Зокрема, їх вважають зручними механізмами для проведення процедури електронного голосування [8], тендерних закупівель [9], ведення реєстрів [10]. Поняття блокчейну та протоколу консенсусу також еволюціонує. За протоколом консенсусу Proof-of-Work, єдиним, який був запропонований у [1], незабаром з'явився більш ефективний протокол Proof-of-Stake (PoS) [11], а потім ще багато нових протоколів, огляд яких наведено, приміром, у [12].

Як це завжди буває у криптології, разом з розвитком певного механізму чи протоколу розвиваються й атаки на нього. На сьогодні є значна кількість атак на блокчейн-структуру. Найпершу з них, атаку подвійної витрати (Double Spend Attack), описано створювачем блокчейну у тій самій історичній роботі [1]. Вона

[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.