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*.

А.А. ВИХЛО
Навчально-науковий фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна, e-mail: *antonvykhlo@gmail.com*.

ОЦІНЮВАННЯ ЙМОВІРНОСТІ УСПІХУ АТАКИ ВИПЕРЕДЖЕННЯ НА СМАРТКОНТРАКТИ[1]

Анотація. Розглянуто атаку випередження (frontrunning attack), яка є однією з найпоширеніших атак на смартконтракти. Її сутність полягає в маніпулюванні порядком включення транзакції в блок з метою отримання вигоди внаслідок зміни послідовності оброблення транзакцій. Особливу загрозу така атака становить для проведення аукціонів p2p продажу «зеленої» електроенергії. У цій роботі спочатку розглянуто та проаналізовано різні типи атак випередження, які формалізовано в покрокових алгоритмах виконання. Запропоновано модель, в якій оцінено ймовірність успіху такої атаки. Для запропонованої моделі отримано явну формулу для ймовірності успіху атаки заміщення та атаки вставки, які є окремими випадками атаки випередження. Показано, що ймовірність успіху залежить від параметрів мережі та від співвідношення між комісіями транзакцій, створених чесним користувачем та зловмисником. Наведено чисельні приклади практичного застосування отриманої формули, які додатково підтверджують коректність аналітичних результатів.

Ключові слова: блокчейн, смартконтракти, аукціони, p2p продаж «зеленої» електроенергії, атака випередження.

ВСТУП

Децентралізованість і публічність транзакцій, пов'язаних з проведенням аукціонів та децентралізованими обмінами активів (decentralized exchanges), а також залежність часу на оброблення транзакції від її комісії надають зловмиснику нові можливості для впливу на порядок оброблення транзакцій (тобто на порядок включення їх у блок). Однією з атак, за якої зловмисник використовує ці можливості для отримання неправомірної вигоди, є атака випередження (frontrunning attack). Ця атака базується на принципах функціонування блокчейну, а її реалізація не потребує жодних передумов чи наявності вразливостей у смартконтракті.

Нижче наведемо кілька типів таких атак. Зазначимо, що незалежно від типу атаки випередження її першим кроком є пошук інформації про транзакції певного виду, для яких зміна (очікуваного) порядку їхнього виконання може призвести до отримання зловмисником певної вигоди — зміни ціни активу або «перехоплення» пропозиції, зміни попиту тощо. Для цього зловмисник перевіряє так званий резервуар пам'яті (mempool) — умовне місце, в якому зберігаються транзакції, які раніше створені користувачами і тепер чекають на оброблення. Знайшовши відповідну транзакцію (або кілька транзакцій), зловмисник створює альтернативну транзакцію, яка може бути, зокрема, копією однієї з раніше створених транзакцій, і намагається змінити очікуваний порядок оброблення транзакцій. Наприклад, якщо зловмисник хоче «перехопити» ставку на аукціоні, то він створює

[1] Дослідження проведено за підтримки НАН України, зокрема в рамках проєкту «Розвиток децентралізованих ринкових механізмів в галузі електроенергетики, що базуються на технологіях блокчейну та смартконтрактів» з номером державної реєстрації 0123U100981.