МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ MEV-АТАКАМ ЧЕРЕЗ МІЖЛАНЦЮГОВІ ПРОТОКОЛИ У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

Антіпін В.С., Олійников Р.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток децентралізованих фінансових систем (DeFi) та поширення міжланцюгових протоколів створили нові вектори кібератак, серед яких особливе місце займають MEV-експлойти (Maximal Extractable Value). Ці атаки дозволяють валідаторам, пошуковикам або операторам вузлів маніпулювати порядком транзакцій для отримання додаткового прибутку за рахунок звичайних користувачів. У контексті міжланцюгової взаємодії проблема набуває особливої гостроти через асинхронність підтверджень транзакцій, різну швидкість фіналізації блоків і відсутність єдиного механізму консенсусу між блокчейнами.

За результатами дослідження Lyu та ін. (2022) [1], системи приватних транзакцій у Ethereum продемонстрували суттєвий ризик централізації та уразливість до повторного впорядкування операцій, що безпосередньо пов'язано з феноменом MEV. Паралельно Öz та ін. (2025) [2] показали, що частка міжланцюгових арбітражних транзакцій у загальному обсязі MEV-активності зросла з 7,8% до 21% упродовж двох років, що вказує на стрімке поширення кросчейн-маніпуляцій. У звіті Європейського управління з цінних паперів і ринків (ESMA, 2022) [3] зазначено, що швидке зростання обсягів транзакцій у DeFi без належних механізмів контролю створює ризики для стабільності фінансової системи, включно з ринковими викривленнями, спричиненими MEV.

Метою дослідження є постановка задачі розроблення комплексного підходу до виявлення та протидії MEV-атакам у міжланцюговому середовищі з урахуванням відмінностей у механізмах консенсусу, затримках підтвердження транзакцій та топології мереж. Робота спрямована на формування методологічної основи для побудови системи захисту децентралізованих фінансових протоколів від нового класу кіберзагроз.

Аналіз наукових джерел показує, що проблематика MEV-атак активно вивчається, однак більшість робіт фокусується на внутрішньоланцюгових сценаріях.

Daian та ін. (2020) [4] уперше формалізували концепцію MEV і довели, що валідатори можуть отримувати додатковий прибуток шляхом переупорядкування, вставки або цензурування транзакцій, що порушує принцип справедливості системи. Qin, Zhou і Gervais (2022) [6] провели кількісну оцінку вилученої вартості та визначили понад 600 млн доларів збитків у період 2020–2021 років. Mazor і Rottenstreich (2024) [5] експериментально підтвердили наявність значних арбітражних можливостей у міжланцюговому обміні, які можуть бути використані для скоординованих MEV-експлойтів.

Водночас існуючі рішення не враховують асинхронність підтверджень між різними ланцюгами, різницю у протоколах фіналізації блоків і специфіку кросчейн-мостів. Öz та ін. (2025) [2] наголошують, що саме затримка між станами ланцюгів і неузгодженість їхніх фіналізацій створюють основу для появи міжланцюгових MEV.

У цьому дослідженні міжланцюгова екосистема розглядається як розподілена система з асинхронною взаємодією компонентів, де кожен блокчейн представлено як окремий процес із власним механізмом консенсусу та правилами фіналізації. Для формалізації моделі загроз вводиться поняття системи

$$S = (C, B, M, T, F),$$

де C – множина блокчейнів;

B – множина міжланцюгових мостів;

M – функція маршрутизації повідомлень між ланцюгами;

T – множина транзакцій;

F – функція фіналізації для кожного ланцюга, що визначає часові вікна та гарантії підтвердження.

MEV-атака в такій системі визначається як послідовність дій

$$A = \langle a_1, a_2, \dots, a_k \rangle,$$

де a_i – вставка, видалення або переупорядкування транзакції в межах одного чи кількох ланцюгів.

Атака вважається успішною, якщо

$$\Pi(A) = profit(A) - [cost(A) + risk(A)] > 0,$$

де $profit(A)$ – отриманий прибуток;

$cost(A)$ – витрати на виконання атаки;

$risk(A)$ – очікувані втрати через санкції або невдачу.

Основна складність виявлення таких атак полягає в необхідності кореляції подій у різних блокчейнах з урахуванням затримок фіналізації.

Для встановлення причинно-наслідкових зв'язків між подіями пропонується використовувати годинники Лампорта (для встановлення часткового порядку подій) у поєднанні з векторними годинниками Fidge–Mattern, що дозволяє визначати послідовність транзакцій між різними ланцюгами. Це дає змогу виявляти скоординовані атаки, у яких зловмисник використовує декілька адрес у різних блокчейнах для маскування маніпуляцій. Для оцінки рівня підозрілості транзакційного патерну визначається функція

$$S(p) = \alpha \cdot temporal(p) + \beta \cdot volume(p) + \gamma \cdot frequency(p) + \delta \cdot identity(p),$$

де $temporal(p)$ – часові аномалії;

$volume(p)$ – обсяг операцій;

$frequency(p)$ – частоту появи подібних дій;

$identity(p)$ – повторюваність або кореляцію між адресами вузлів.

На практичному рівні пропонується архітектура розподіленої системи моніторингу, що складається з трьох модулів. Перший – модуль збору даних, який отримує транзакційні події з публічних мемпулів у мережах типу Ethereum [1], а також через подієві стріми Geyser/Block Engine у Solana та журнали relay-повідомлень у протоколах Axelar, IBC або LayerZero [2]. Другий – модуль кореляційного аналізу, що синхронізує часові ряди та застосовує модифіковану метрику подібності Жаккара з часовим вікном для визначення відповідності транзакцій між ланцюгами. Третій – модуль виявлення аномалій, який використовує комбінацію статистичного аналізу та алгоритмів машинного навчання (Isolation Forest, DBSCAN) для класифікації підозрілих шаблонів поведінки.

Серед запропонованих механізмів протидії передбачається застосування протоколів commit-reveal для міжланцюгових транзакцій, введення випадкових часових вікон у роботі мостів, багатоджерельна агрегація цінових даних для оракулів і впровадження схем MEV-refund, що частково компенсують користувачам негативний ефект маніпуляцій [4, 6]. Особлива увага приділяється інтеграції з системами Web3-SOC та SIEM, що дозволяє перетворювати виявлені події на сигнали кіберзахисту для провайдерів ліквідності та операторів мостів.

Реалізація запропонованого підходу сприятиме підвищенню рівня захисту децентралізованих фінансових систем від MEV-атак у міжланцюговому середовищі та створить основу для подальших досліджень і розроблення стандартів кібербезпеки.

Список літератури

1. An empirical study on Ethereum private transactions and the security implications / X. Lyu та ін. 2022. URL: https://doi.org/10.48550/arXiv.2208.02858.

2. Cross-chain arbitrage: the next frontier of MEV in decentralized finance / B. Öz та ін. URL: https://arxiv.org/abs/2501.17335.

3. European Securities and Markets Authority. Crypto-assets and their risks for financial stability. 2022. URL: https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf.

4. Flash boys 2.0: frontrunning in decentralized exchanges, miner extractable value, and consensus instability / P. Daian та ін. *2020 IEEE symposium on security and privacy (SP)*, м. San Francisco, CA, USA, 18–21 трав. 2020 р. 2020. URL: https://doi.org/10.1109/sp40000.2020.00040.

5. Mazor O., Rottenstreich O. An empirical study of cross-chain arbitrage in decentralized exchanges. *2024 16th international conference on communication systems & networks (COMSNETS)*, м. Bengaluru, India, 3–7 січ. 2024 р. 2024. URL: https://doi.org/10.1109/comsnets59351.2024.10426894.

6. Qin K., Zhou L., Gervais A. Quantifying blockchain extractable value: how dark is the forest?. *2022 IEEE symposium on security and privacy (SP)*, м. San Francisco, CA, USA, 22–26 трав. 2022 р. 2022. URL: https://doi.org/10.1109/sp46214.2022.9833734.