Науковий вісник НЛТУ України
Scientific Bulletin of UNFU
ISSN 1994-7836 (print)
ISSN 2519-2477 (online)
https://doi.org/10.36930/40360224
Article received: 12.02.2026, accepted: 03.04.2026
Article published: 30.04.2026
UDC 004.[62+75+94]
Correspondence author: N. S. Cherkas n.cherkas.ua@gmail.com

Н. С. Черкас, А. Є. Батюк
Національний університет "Львівська політехніка", м. Львів, Україна

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ЯВИЩА МАКСИМАЛЬНО ЕКСТРАКТОВАНОЇ ВИГОДИ В МЕРЕЖІ БЛОКЧЕЙН ETHEREUM

Запропоновано середовище імітаційного моделювання явища максимально екстрактованої вигоди MEV (англ. *Maximal Extractable Value*), реалізоване мовою програмування Python із використанням бібліотеки Gymnasium, яке відтворює взаємодію сховища-мемпулу, конструювальника блоків, агента MEV-екстрактора та AMM-пулу децентралізованої біржі. Формально середовище описано як розширений та частково спостережуваний процес прийняття рішень, у межах якого агент взаємодіє з дискретно-часовою моделлю епізодів, що відображає послідовність надходження транзакцій, побудови блоків і виконання swap-операцій обміну на децентралізованій крипто-біржі. Для моделювання адаптивної поведінки агента використано методи навчання з підкріпленням, а для кількісного аналізу втрат користувачів застосовано контрфактичний підхід до оцінювання, що дає змогу порівнювати результати виконання транзакцій у різних режимах впорядкування за однакових вхідних умов. У дослідженні використано раніше описаний авторами метод зменшення негативних ефектів MEV-екстракції на основі логічних часових міток Лампорта, який реалізує локальне причинно-наслідкове впорядкування транзакцій у межах окремого смарт-контракту без модифікації глобального механізму консенсусу мережі блокчейн Ethereum. Для оцінювання практичної ефективності цього підходу сформовано три сценарії моделювання: базовий сценарій без систематичної MEV-атаки для визначення накладних витрат застосування механізму захисту, сценарій систематичної sandwich-атаки для аналізу та здатності методу зменшувати втрати користувачів та обмежувати можливості MEV-екстрактора, а також сценарій параметричного аналізу, спрямований на дослідження компромісу між рівнем захисту та "вартістю" його застосування. Отримані результати показали, що запропонований метод MEV-захищеного впорядкування може зменшувати цінові втрати користувачів від sandwich-атак і, водночас, впливати на частоту відхилення транзакцій та пов'язані комісійні витрати, що вказує на наявність керованого компромісу між ефективністю захисту та накладними витратами його використання. Практична цінність роботи полягає у створенні відтворюваного середовища імітаційного моделювання для дослідження стратегічної поведінки MEV-агентів і перевірки механізмів зменшення негативних наслідків MEV у контрольованих умовах, що може бути використано для подальшого аналізу безпеки протоколів децентралізованих фінансів та проєктування нових методів впорядкування транзакцій.

Ключові слова: навчання з підкріпленням; децентралізовані системи; комп'ютерні мережі; інформаційні системи; криптографія; криптовалюти; інформаційна технологія; цифрова економіка.

Вступ / Introduction

Активний розвиток протоколів децентралізованих фінансів у публічних мережах блокчейн, зокрема в мережі Ethereum, зумовив появу складних економічних взаємодій між користувачами, вузлами-валідаторами та спеціалізованими автоматизованими агентами. Одним із наслідків відкритості та прозорості таких систем стало явище максимально екстрактованої вигоди MEV (англ. *Maximal Extractable Value*) [5, 7], що виникає внаслідок можливості впливу на порядок внесення транзакцій до блоку. Умови часткової спостережуваності мемпулу – сховища ще не підтверджених транзакцій, стохастичність надходження транзакцій та конкуренція за пріоритет виконання створюють передумови для реалізації стратегій випередження, перехоплення та інших форм транзакційної маніпуляції.

Наявність явища MEV-екстракції породжує низку негативних ефектів для користувачів децентралізованих застосувань, зокрема погіршення умов виконання swap-операцій обміну криптоактивів у протоколах децентралізованих фінансів, збільшення витрат на комісії та зростання невизначеності результатів транзакцій. Водночас, вплив MEV має системний характер і пов'язаний із фундаментальними властивостями механізмів консенсусу та формування блоків. Це ускладнює застосування традиційних аналітичних або теоретико-ігрових підходів, оскільки поведінка учасників є адаптивною, а середовище – нестаціонарним та високовимірним. Також додаткову складність становить практична неможливість оперативного розгортання експериментальних MEV-захищених механізмів побудови блоків у межах реально функціонуючих публічних мереж блокчейн, які можуть охоплювати тисячі географічно розподілених вузлів. Внесення змін до алгоритмів впорядкування транзакцій у таких системах пов'яза-

Черкас Назарій Степанович, аспірант, кафедра автоматизованих систем управління.
Email: nazarii.s.cherkas@lpnu.ua; https://orcid.org/0009-0007-9976-6530
Батюк Анатолій Євгенович, канд. техн. наук, доцент, кафедра автоматизованих систем управління.
Email: anatolii.y.batiuk@lpnu.ua; https://orcid.org/0000-0001-7650-7383
Цитування за ДСТУ: Черкас Н. С., Батюк А. Є. Імітаційне моделювання явища максимально екстрактованої вигоди в мережі блокчейн Ethereum. Науковий вісник НЛТУ України. 2026, т. 36, № 2. С. 222–233.
Citation APA: Cherkas, N. S., & Batiuk, A. Ye. (2026). Simulation modeling of the maximal extractable value in Ethereum blockchain network. *Scientific Bulletin of UNFU*, 36(2), 222–233. https://doi.org/10.36930/40360224

не з високими ризиками, потребує узгодження між учасниками мережі та не допускає широкомасштабного експериментування без потенційного впливу на економічну безпеку екосистеми.

У зв'язку з цим постає наукова проблема побудови формалізованої моделі, яка б дала можливість відтворювати динаміку взаємодії між транзакціями користувачів, агентами-екстракторами та механізмами впорядкування транзакцій у контрольованих умовах. Така модель має враховувати часткову спостережуваність, стохастичний характер потоку транзакцій та часову структуру формування блоків у мережі Ethereum. Розроблення імітаційного середовища, узгодженого з принципами навчання з підкріпленням, створює основу для дослідження стратегічної поведінки MEV-агентів та кількісного аналізу їхнього впливу на користувачів і функціонування мережі блокчейн загалом.

Актуальність цього дослідження зумовлена потребою дослідження явища MEV в публічних мережах блокчейн та розроблення ефективних рішень зменшення його негативних ефектів. Такими ефектами є втрата користувачами частини прибутку від транзакцій у протоколах децентралізованих фінансів та ширше коло ризиків, пов'язаних з негативним впливом на роботу алгоритмів блокчейн консенсусу. Розроблення середовища імітаційного моделювання дає змогу досліджувати складну взаємодію учасників процесу MEV-екстракції та скоротити цикл тестування та апробації методів MEV-захищеного впорядкування транзакцій, оскільки практична перевірка таких підходів у реальних мережах, зокрема в Ethereum, є складною, тривалою та ресурсомісткою. У зв'язку з цим перспективним підходом є використання середовищ імітаційного моделювання, здатних відтворювати наближені до реальних умови функціонування мереж блокчейн, протоколів децентралізованих фінансів і поведінки основних учасників.

Об'єкт дослідження – явище MEV-екстакції в публічних мережах блокчейн.

Предмет дослідження – моделі, методи та засоби імітаційного моделювання динамічної і багатовимірної структури мережі блокчейн та явища MEV, які дадуть змогу досліджувати складну взаємодію учасників процесу MEV-екстракції та скоротити цикл апробації і тестування методів MEV-захищеного впорядкування транзакцій.

Мета роботи – розробити підхід до імітаційного моделювання явища максимально екстрактованої вигоди (MEV) у мережі блокчейн Ethereum, орієнтований на дослідження поведінки MEV-екстракторів, оцінювання користувацьких втрат та зменшення негативних ефектів від маніпуляцій порядком транзакцій у децентралізованих обчислювальних системах блокчейн.

Для досягнення зазначеної мети визначено такі основні *завдання дослідження*:

- дослідити явище MEV та оцінити його вплив на користувачів та мережі блокчейн, що дасть змогу виявити ключові джерела користувацьких втрат і визначити вимоги до методів та засобів їх зменшення;
- розробити моделі та структури середовища імітаційного моделювання явища MEV у мережі блокчейн Ethereum за схемою PBS, що дасть можливість відтворювати взаємодію сховища-мемпулу, конструювальника блоків, користувачів і MEV-екстракторів у контрольованих умовах та досліджувати вплив правил формування блоків на результати виконання транзакцій;
- розробити модель епізодів на основі генерованих дискретних часових рядів, що дасть можливість узгодити динаміку надходження транзакцій, побудову блоків і процес оцінювання агентів у частково спостережуваному стохастичному середовищі;
- розробити програмне середовище для імітаційного моделювання явища MEV у мережі блокчейн Ethereum з підтримкою MEV-захищеного методу впорядкування транзакцій на основі логічних часових міток Лампорта [6], що дасть можливість проводити відтворювані експерименти, оцінювати практичну ефективність цього методу в різних сценаріях та досліджувати компроміс між рівнем захисту і накладними витратами його застосування.

Аналіз останніх досліджень та публікацій. Явище MEV у мережах блокчейн вперше було формально описано в роботі [7]. У ній автори провели аналогію між алгоритмізованою високочастотною торгівлею HFT (англ. *High-Frequency-Trading*) на традиційних фінансових ринках і маніпуляціями порядком транзакцій, які здійснюються в мережі блокчейн Ethereum автоматизованими ботами та вузлами-майнерами. У межах цієї роботи досліджено аукціони пріоритетних комісій транзакцій PGA (англ. *Priority Gas Auctions*), а також змодельовано поведінку автоматизованих ботів-учасників із використанням підходів теорії ігор [15]. Це дало змогу виділити характерні стратегії поведінки таких агентів і проаналізувати механізми їхньої конкурентної взаємодії. Окрему увагу приділено системним ризикам, пов'язаним із MEV-атаками з боку майнерів. У таких випадках майнери, мотивовані можливістю отримання додаткового прибутку від маніпуляцій порядком транзакцій, можуть експлуатувати особливості алгоритму консенсусу мережі для штучної реорганізації ланцюга блоків задля привласнення частини прибутку інших учасників мережі. Загалом зазначена робота зробила вагомий внесок у становлення напряму досліджень MEV, однак застосований у цій роботі метод моделювання базувався на теорії ігор, що, попри його цінність для формалізації стратегічної взаємодії учасників мережі, має низку обмежень під час дослідження явища MEV. Зокрема, такі моделі зазвичай потребують істотного спрощення простору стратегій, введення припущень щодо раціональності агентів і гірше пристосовані до відтворення нестаціонарних та стохастичних умов децентралізованої мережі блокчейн Ethereum.

У роботі [17] запропоновано модель "часових ігор" в алгоритмах блокчейн консенсусу категорії PoS (англ. *Prood-of-Stake*), де раціональні вузли-валідатори можуть стратегічно затримувати формування блоку для оптимізації доходів від MEV-екстракції. Автори також емпірично аналізують динаміку в мережі Ethereum та доходять висновку, що така поведінка потенційно вигідна для MEV-екстракторів. Сильною стороною статті є поєднання теоретичної моделі з емпіричним дослідженням цінності оптимізації часових затримок для вузла-валідатора. Однак її фокус зосереджено саме на дослідженні ролі часу в алгоритмах консенсусу, а не на моделюванні взаємодії сховища-мемпулу, протоколів DeFi, агентів-екстракторів та захищених політик впорядкування транзакцій.

У роботі [14] запропоновано підхід на основі теорії ігор для оцінювання впливу MEV-екстракції на стабільність алгоритму консенсусу мережі блокчейн, вводячи поняття "ціни MEV" (Price of MEV). Автори математично доводять, як конкуренція за прибуток може дестабі-

лізувати мережу через відгалуження ланцюга блоків та як результат – реорганізацію мережі. Перевагою роботи є глибока формалізація економічних загроз для безпеки алгоритму консенсусу. Разом з тим дослідження фокусується на макроекономічній рівновазі та статичних ігрових моделях і у ньому відсутній інструментарій для динамічного імітаційного моделювання явища MEV та не розглядаються механізми зменшення його негативних ефектів на етапі формування блоку.

У роботі [19] запропоновано ігрову модель аукціонів на основі проєкту MEV-Boost та за допомогою симуляцій досліджено стратегії ставок конструювальників блоків, зокрема вплив доступу до можливостей MEV-екстракції та якості з'єднання з компонентом-ретранслятором (relay) на прибутковість та результати MEV-атак. Перевагою роботи є якісне дослідження конкуренції у внутрішньомережевих аукціонах схеми PBS. Водночас, об'єктом моделювання є насамперед стратегії формування ставок у даних аукціонах, а не поведінка MEV-екстракторів у середовищі DeFi протоколів. Відтак, робота не охоплює моделювання користувацьких втрат від явища MEV або методи їх зменшення.

Робота [3] пропонує загальну абстрактну теорію явища MEV на основі формальної моделі блокчейну та смарт-контрактів, яка слугує підґрунтям для доведення властивостей безпеки щодо MEV-атак. Її головна перевага полягає у строгій теоретичній постановці проблеми та спробі закласти універсальну основу для подальших формальних міркувань про MEV. Водночас, робота зосереджена саме на абстрактній формалізації й не розглядає практичні аспекти симуляції стохастичного середовища мережі блокчейн та експериментального порівняння конкретних механізмів MEV-захищеного впорядкування транзакцій.

У дослідженні [11] автори запропонували підхід до оптимізації стратегій торгівлі криптоактивами, який поєднує традиційні методи машинного навчання для прогнозування ринкових змін із методами глибокого навчання з підкріпленням для вибору торгових рішень. Перевагою роботи є врахування високої волатильності криптовалютного ринку та спроба поєднати прогнозування й адаптивне прийняття рішень у єдиній моделі. Водночас, дослідження належить радше до задач алгоритмічної торгівлі, ніж до задач моделювання MEV як інфраструктурного явища блокчейн-мереж, оскільки в ньому не розглядаються мемпул, побудова блоків, стратегічне перевпорядкування транзакцій та механізми їх захищеного виконання.

Обидва підходи – RL-орієнтоване моделювання та моделі теорії ігор – є взаємодоповнювальними у дослідженнях явища MEV. RL забезпечує здатність відтворювати адаптивну поведінку агентів у змінних середовищах і дає змогу оцінити ефективність різних політик справедливого впорядкування транзакцій. Моделі на основі теорії ігор, навпаки, дають можливість визначити структуру стратегічних взаємодій та описати можливі рівноваги. Застосування цих методів під різні типи задач дає змогу розробляти середовища, здатні оцінювати вплив MEV на користувачів та мережі блокчейн загалом, та досліджувати ефективність механізмів пом'якшення його негативних ефектів.

Матеріали та методи дослідження. У дослідженні застосовано методи імітаційного моделювання, статистичного аналізу та навчання з підкріпленням для дослідження явища максимальної екстрактованої вигоди MEV (англ. *Maximal Extractable Value*) у публічних мережах блокчейн. Методологічну основу становлять формальні моделі взаємодії транзакцій у мемпулі, механізми формування блоків у мережі Ethereum та моделі поведінки агентів, що здійснюють MEV-екстракцію. Для аналізу динаміки виконання транзакцій використано дискретно-часовий підхід до моделювання, у межах якого надходження транзакцій, формування блоків і взаємодія з децентралізованими фінансовими протоколами відтворюються як послідовність епізодів. Для експериментального дослідження використано метод зменшення негативних ефектів MEV-екстракції на основі логічних часових міток Лампорта [6] та контрфактичний підхід до оцінювання втрат користувачів за системою кількісних метрик.

Результати дослідження та їх обговорення / Research results and their discussion

Під час вибору структури середовища імітаційного моделювання явища MEV в мережі блокчейн Ethereum запропоновано використати схему PBS (англ. *Proposer-Builder-Separation*) [8] розподілу функцій конструювальника блоків (Builder) та вузла-валідатора, який продукує блоки (Proposer). На практиці в подібній схемі також бере участь компонент ретранслятор (Relay), але в нашому випадку прийнято рішення знехтувати ним, оскільки його роль у взаємодії основних акторів (користувач, MEV-екстрактор, AMM-пул, конструювальник блоків) не є визначальною для цього дослідження.

Основними компонентами середовища імітаційного моделювання є:

1. Агент MEV-екстрактор, що спостерігає стан середовища та формує бандли, які містять користувацьку транзакцію та MEV-транзакції випередження/перехоплення.
2. Конструювальник блоків, який отримує користувацькі транзакції з мемпулу або через приватні канали, та приймає від агента бандли MEV-екстракції. Блоки формуються або за стандартними правилами – впорядковані за комісією, або за правилами, що мають на меті мінімізацію MEV-екстракції.
3. Uniswap-подібний AMM-пул децентралізованої біржі, який надає послуги обміну криптотокенів та визначає ціну виконання swap-операцій обміну.
4. Мемпул – тимчасове сховище непідтверджених транзакцій, які були розповсюджені мережею, але ще не включені до блоку. Вміст мемпулу наповнюється генератором синтетичних транзакцій – трансферів та swap-операцій обміну. Отже, емулюється реальний процес надходження транзакцій до мемпулу та їх подальшого поширення.
5. Абстрактний вузол-валідатор, відповідальний за продукування блоків, отриманих від компонетра-конструювальника блоків. Нові блоки формуються згідно з форматом алгоритму консенсусу мережі Ethereum та після продукування в часовому зрізі блокового інтервалу стають частиною стану середовища.
6. Історія блоків мережі від початку епізоду, що може використовуватись як MEV-агентом, так і конструювальником блоків.

Формалізовану модель середовища імітаційного моделювання задано як розширений Марковський процес прийняття рішень [4], доповнений дискретно-часовою моделлю епізодів, правилами побудови блоків та стохастичною моделлю надходження транзакцій. Зокрема, середовище формально описується у такому вигляді:

$$M = \langle S, O, A, P, R, \gamma \rangle,$$

де: S – простір внутрішніх станів; O – простір спостережень агента; A – простір дій агента; $P(s'|s, a)$ – ймовірнісний оператор переходу між станами з урахуванням реакції середовища та правил конструювання блоків; $R(s, a)$ –функція миттєвої винагороди агента; $\gamma\in[0,1]$ – коефіцієнт дисконтування. Оскільки MEV-агент спостерігає стан (мемпулу) тільки частково, фактично маємо справу з частково спостережуваним MDP (POMDP), де спостереження $o\in O$ є детермінованим або стохастичним відображенням стану $s\in S$. Простір станів S формується як декартів добуток кількох підпросторів:

$$S = S^{mempool} \times S^{amm} \times S^{chain} \times S^{builder} \times S^{time},$$

де компонента $S^{mempool}$ описує множину поточних транзакцій у мемпулі з їх параметрами (тип, обсяг swap-операції обміну, напрям, slippage-ліміт, ставка gas-комісії та інші). Компонента S^{amm} містить стан резервів токенів у AMM-пулі, параметри комісій та поточні ціни. Підпростір S^{chain} містить агреговані характеристики нещодавно продукованих блоків (кількість блоків в епізоді, агреговані показники користувацьких втрат, історія MEV-бандлів). Множина $S^{builder}$ визначає актуальні правила впорядкування транзакцій у блоці (стандартні або варіант з MEV-захистом), а S^{time} – позиція в епізоді та номер поточного блокового інтервалу. Така декомпозиція забезпечує явний поділ між конфігурацією правил схеми PBS, економічним станом (ліквідністю, ціною) та операційним станом – сховищем-мемпулом, сформованими блоками.

Для моделювання виконання swap-транзакцій використано стандартну модель автоматизованого маркет-мейкера (AMM) типу constant-product [20], у якій резерви крипто-активів x та y задовольняють співвідношення:

$$x \cdot y = k,$$

де k – стала величина, що задає інваріантну залежність між резервами пулу та визначає правило їх зміни під час виконання swap-транзакцій. Використання моделі автоматизованого маркет-мейкера (AMM) типу constant-product (постійного добутку), найвідомішої за Uniswap v2, є фундаментальним підходом для моделювання децентралізованих бірж.

Спостереження агента $o\in O$ є проєкцією стану: воно містить фактично доступну агреговану інформацію про стан AMM-пулу, підмножину найрелевантніших користувацьких swap-операцій обміну у мемпулі (наприклад, за розміром або за ставкою gas-комісії), а також стислу інформацію про останні підтверджені блоки та застосовані правила впорядкування. Дії агента $a\in A$ містять MEV-екстракцію – формування бандлу з перехопленням користувацької транзакції, формування повного бандлу сендвіч-атаки з набором параметрів, або бездіяльність за несприятливих умов чи у разі базового тесту. Конструювальник блоків, отримавши MEV-бандли та користувацькі транзакції, застосовує обрані правила впорядкування, конструює блок-кандидат і непрямо впливає на те, чи буде MEV-екстракція агента успішно виконана.

Функція винагороди $R(s, a)$ відображає позитивний економічний результат дій агента в контексті схеми PBS: вона може визначатися як різниця між доходом від MEV-екстракції та сумою витрат на gas-комісії і, за потреби, штрафів за невдалі або надлишкові транзакції у разі надмірної інтенсивності поведінки агента. У деяких сценаріях можуть додатково враховуватися компоненти, що відображають регуляторні обмеження чи штрафи за втрати користувацьких swap-операцій обміну.

У межах імітаційного моделювання умов мережі блокчейн та явища максимально екстрактованої вигоди епізод виконує роль скінченного фрагмента "часу мережі", в якому відтворюється послідовність подій: надходження транзакцій у мемпул, реакція MEV-екстрактора (агента), конструювання блоків та виконання методів смарт-контракту AMM-пулу децентралізованої біржі. Структура епізодів є зручною для керованого експерименту: воно дає змогу фіксувати тривалість симуляції, порівнювати різні політики впорядкування транзакцій, а також накопичувати агреговані метрики (прибуток агента, вплив на виконання користувацьких swap-операцій тощо) на узгодженому часовому відрізку. Кожен епізод запропоновано розбивати на дискретні часові зрізи, які дають можливість краще моделювати динаміку процесів та узгоджуються з моделлю кроків середовища RL.

Нехай епізод параметризовано трійкою (N, K, δ), де N – кількість блоків у межах епізоду, K – кількість часових зрізів у межах одного блоку, а δ – тривалість одного часового зрізу. За замовчуванням для лінійної часової моделі Ethereum приймається $K = 12$ та $\delta = 1$ с, що відповідає 12-секундному слоту під-мережі Beacon Chain в моделі консенсусу Proof-of-Stake (PoS) мережі Ethereum. Водночас, K (і відповідно $\delta = 12/K$) у моделі є конфігурованими параметрами, що дає змогу змінювати часову роздільну здатність симуляції без зміни логіки побудови блоків.

Дискретний час індексується як $\tau\in\{0,1,\ldots, T-1\}$, де $T = N{\cdot}K$. Відображення кроку τ на індекс блоку та позицію всередині блоку визначається так:

$$b(\tau) = \left\lfloor \frac{\tau}{K} \right\rfloor, k(\tau) = \tau \bmod K .$$

Множину меж блоків задаємо як $\mathcal{B} = \{\tau \mid k(\tau) = K-1\}$. Стан середовища у кроці τ позначимо s_τ і подамо як $s_\tau = (m_\tau, x_\tau, c_\tau, g_\tau, t_\tau)$, де m_τ – стан мемпулу (черга непідтверджених транзакцій), x_τ – стан AMM-пулу, c_τ – агрегована історія нещодавніх блоків, g_τ – вміст блоку (напр., накопичені бандли агента, обрані параметри екстракції), а $t_\tau=(b(\tau), k(\tau))$ – часовий індекс. Спостереження агента $o_\tau=\Omega(s_\tau)$ є проєкцією стану та реалізує часткову спостережуваність мемпулу, що узгоджується з припущеннями про обмежену локальну інформацію учасників мережі.

Прибуття непідтверджених транзакцій у межах часового зрізу в епізоді моделюється як стохастичний процес. Для синтетичної генерації зручною апроксимацією є пуассонівський потік: кількість нових транзакцій у відрізку τ задається $X\tau\sim$Poisson$(\lambda\sigma)$, після чого параметри транзакцій (тип, ставка gas-комісії, та ін.) визначаються згідно з каліброваними імовірнісними розподілами, аналогічно до підходів, що використовуються в моделях мемпулу та процесів підтвердження транзакцій. Побудова блоків виконується тільки на межах $\mathcal{B}$ білдер агрегує m_τ та g_τ, застосовує правило впорядкування (стандартне або MEV-захищене), формує блок-кандидат та фіксує зміни стану, оновлюючи стан x та історію блоків c. Отже, реалізовується послідовність подій "надходження → дія → межа блоку → виконання". Схематично таку модель епізодів на основі генерованих дискретних часових рядів продемонстровано на рис. 1.

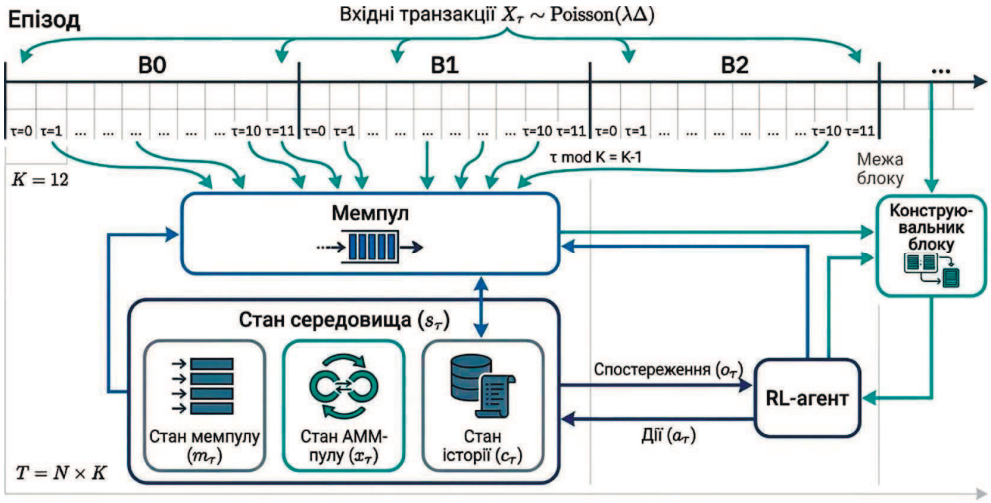

Рис. 1. Модель епізодів на основі генерованих дискретних часових рядів / Episode model based on generated discrete time series

Запропонована модель має такі переваги:

- параметризована часова дискретизація є узгодженою зі схемою слотів мережі Ethereum та сумісною з RL-моделлю "спостереження-дія-перехід" взаємодії агента та середовища";
- відокремлення високочастотної динаміки мемпулу від події включення у блок, що є критичним для аналізу явища MEV та тестування стратегій впорядкування транзакцій;
- підтримка часткової спостережуваності та стохастичності, необхідних для реалістичного відтворення MEV-сценаріїв;
- відтворюваності через можливість фіксації початкового seed-значення генератора псевдовипадкових чисел та можливості калібрування інтенсивностей/розподілів на емпіричних даних.

Визначимо набір сценаріїв імітаційного моделювання та систему метрик, задля їх використання для кількісного порівняння режимів виконання транзакцій у синтетичному середовищі. Порівняння проводиться у вигляді двох серій запусків, які відрізняються тільки режимом виконання swap-транзакцій обміну у моделі AMM-пулу децентралізованої біржі:

1. Серія A: виконання swap-операцій обміну без Local Causal Fair Ordering (LCFO) перевірки, тобто без застосування локального механізму MEV-захисту;
2. Серія B: виконання swap-операцій обміну із увімкненою LCFO-перевіркою на рівні AMM-пулу, тобто з валідацією логічної мітки $lamport_{ts}$ відносно локального лічильника *lcfo_clock* та можливістю відхилення транзакції з причиною "lcfo", що має на меті зменшити успішність MEV-екстракції.

Окремо використовується контрфактичне відтворення (replay) виконання як інструмент оцінювання метрик на рівні блока: один і той самий набір транзакцій, що потрапив до блока, може бути прогнаний двічі зі спільного снепшоту стану AMM-пулу з LCFO перевіркою вимкненою або увімкненою. Контрфактичний підхід, запозичений з причинно-наслідкового аналізу, у цій роботі використовується як метод формалізації різниці у результатах виконання за зміни режиму впорядкування для одних і тих самих вхідних даних, що забезпечує відтворюваність, деталізацію та коректність порівняння на рівні блоку.

Система метрик поділяється на дві групи: метрики користувацьких втрат та якості виконання swap-операцій обміну та метрики ефективності/успішності дій MEV-агента. У межах поданої системи агент-екстрактор оптимізує власну винагороду, тоді як метрики користувацьких втрат застосовуються як зовнішній критерій для порівняння режимів виконання та політик впорядкування. На рівні блоку та епізоду використовуються такі метрики користувацьких втрат:

- Adversarial Slippage (AS): міра погіршення ефективної ціни виконання (внаслідок її "прослизання") користувацької swap-операції обміну, спричинена атакуючими транзакціями та/або обраним режимом виконання [1] з агрегуванням за робастними статистиками;
- Output Loss (PL): невід'ємна втрата користувача у вихідному крипто-активі, що відповідає недоотриманню значення amount_out відносно порівнюваного режиму;
- Revert Rate (SR): частка swap-транзакцій користувачів, що завершилися відхиленням з окремою фіксацією *SR_lcfo*, тобто часткою відхилень, спричинених саме LCFO-перевіркою, що є прямим показником побічних втрат механізму;
- Gas Burn (GB): оцінка незворотних комісійних втрат користувачів за відхилення транзакцій у моделі EIP-1559 [13] через спалювання базової комісії, що узгоджується із сучасним механізмом алгоритму консенсусу Ethereum.

У реалізації метрик дотримується правило: якщо транзакцію відхилено у певному режимі, то значення AS/PL для неї в цьому режимі вважається невизначеним і не вносяться до агрегування, тоді як значення метрик SR і GB враховуються завжди. Це дає змогу уникнути змішування нульового погіршення з невиконаною транзакцією та спрощує інтерпретацію результатів.

Також, на рівні блоку та епізоду реалізовано такі метрики MEV агента-екстрактора:

- Reward/Profit: фінансовий результат агента-екстрактора в базовому активі (token0), мінус комісійні його витрати;
- Front/Back success: індикатори успішності транзакцій агента-екстрактора у сценаріях MEV-атак випередження та sandwich-охоплення;
- Sandwich completion rate: частка спроб sandwich-охоплення, у яких вдалося виконати обидві транзакції та отримати невід'ємний прибуток.

Нижче в табл. 1 визначено три сценарії, які використано для репрезентативного аналізу в межах програмної реалізовації середовища. Налаштування сценаріїв імітаційного моделювання – це процес визначення вхідних параметрів, зовнішніх умов та логіки роботи моделі для дослідження поведінки складної системи в різних ситуаціях. Це критичний етап, що дає змогу отримати інформацію про систему шляхом експериментів, а не безпосереднього втручання. Сценарії побудовано так, щоб

відокремити вартість механізму MEV-захищеного впорядкування, ефективність за умов MEV-екстракції та "керованість компромісу" через параметр *lamport_window_W*.

Табл. 1. Налаштування сценаріїв імітаційного моделювання / Simulation scenario settings

Сценарій	Мета	Параметри
S_1	Вартість LCFO без систематичної MEV-атаки	lcfo_enabled = 0/1 policy = random lambda_tx = 0.6 lamport_window_W = 16 n_blocks = 50 seeds = 3
S_2	Ефект LCFO під систематичною sandwich-атакою	lcfo_enabled = 0/1 policy = random lambda_tx = 1.0 lamport_window_W = 16 n_blocks = 50 seeds = 5
S_3	Вплив параметра *W* на співвідношення (MEV) захист – побічні витрати	lcfo_enabled = 0/1 policy = random lambda_tx = 1.0 lamport_window_W = 4/64 n_blocks = 50 seeds = 5

Сценарій S_1 (*random policy*) – *оцінка фонової вартості.* У цьому сценарії агент-екстрактор обирає дії випадково, без систематичного прагнення до виконання MEV-атаки типу sandwich-охоплення. Сценарій використовується для оцінювання базового рівня *SR_lcfo* і пов'язаних витрат GB у MEV-захищеному режимі за типового навантаження та помірної інтенсивності надходження транзакцій. Очікуваним результатом є невід'ємний рівень *SR_lcfo* у серії B, що відображає накладні ефекти застосування LCFO, тоді як метрики slippage/PL мають залишатися порівняно малими через відсутність систематичної MEV атаки. Для серії A очікується близький до нуля *SR_lcfo* (оскільки режим LCFO від'єднало) і відсутність відхилень, зумовлених LCFO-правилом.

Сценарій S_2 (*scripted policy*) – *систематична MEV-екстракція через sandwich-атаку.* Сценарій призначений для отримання та оцінювання виразного сигналу ефективності механізму LCFO. За наявності цільової транзакції-жертви агент у кожному блоці намагається сформувати sandwich-комбінацію з її охоплення, використовуючи підвищену пріоритетну комісію для забезпечення потрібного розміщення у порядку виконання; підвищене значення λ_{tx} збільшує насиченість сховища-мемпулу та ймовірність економічно значущих операцій транзакції-жертви. Очікується, що у серії A зростатимуть користувацькі втрати (AS/PL) та прибутковість агента, тоді як у серії B – зменшуватимуться AS/PL і/або падатиме успішність завершення MEV екстракції sandwich-охоплення, що узгоджується з теоретичним аналізом стійкості LCFO до атак, залежних від перевпорядкування конфліктних транзакцій.

Сценарій S_3 – керований компроміс через lamport_window_W. У цьому сценарії фіксується MEV-атака за заданим сценарієм, але змінюється параметр *lamport_window_W*, який контролює діапазон формування логічних міток $lamport_{tx}$ на стороні відправників. Мале значення *W* (наприклад, 4) звужує "допустиме" вікно логічних часових міток та підвищує ймовірність відхилень через LCFO навіть для неатакуючих транзакцій, тоді як великий *W* (наприклад, 64) зменшує *SR_lcfo*, але може послаблювати жорсткість локального причинно-наслідкового контролю. Очікуваним результатом є демонстрація компромісу: за малого *W* серія B матиме вищі *SR_lcfo* і *GB*, а за великого значення *W* – нижчі значення цих показників за повного або часткового збереження позитивного ефекту зменшення AS/PL.

Запропонований набір сценаріїв є мінімальним, але достатнім для досягнення двох цілей:

1. Кількісно оцінити ефективність LCFO як локального механізму зменшення негативних ефектів MEV у межах реалізованої моделі;
2. Показати керований компроміс між ефективністю захисту та накладними витратами механізму через параметри конфігурації.

Сценарій S_1 виконано з такими значеннями: *policy = random*, λ_{tx}=0,6; *W* = 16; *n_bloks* = 50. Метою є оцінювання базових накладних витрат застосування LCFO в умовах, коли MEV-агент не реалізує цілеспрямованої стратегії sandwich-атаки. Порівняння виконується між двома серіями з увімкненим та вимкненим LCFO-механізмом MEV-захисту за однакових значень seed та однакової політики агента-екстрактора. Додатково на рівні кожного блока обчислюються контрфактичні показники через дворазове відтворення виконання з одного снепшоту стану середовища. Отримано такі результати:

1) *Ефект на показники втрат від slippage-відхилення у S_1 є малим і не є домінантним сигналом.* Для трьох значень seed отримано, що різниця $\Delta = avg\_AS_b - avg\_AS_p$ має порядок 10^{-3}: типові значення лежать у діапазоні приблизно 0,0010 – 0,0013, тоді як в одному зі запусків спостерігалося значення, близьке до нуля. Така поведінка узгоджується з природою сценарію: за відсутності систематичного тиску атакуючого агента зміни в ефективній ціні виконання swap-операцій обміну переважно зумовлені стохастичною динамікою сховища-мемпулу та випадковими діями агента-екстрактора, а не цілеспрямованим перевпорядкуванням.
2) Натомість "вартість" застосування механізму LCFO проявляється у зростанні частки відхилених транзакцій та комісійних втрат користувачів. У режимі MEV-захисту (параметр lcfo_enabled=1) спостерігається систематичне зростання частки відхилених користувацьких swap-транзакцій обміну SR_p порівняно з базовим режимом SR_b, а також істотне зростання агрегованих GB_p незворотних комісійних втрат, пов'язаних із відхиленнями транзакцій (показник порівняно з GB_b). Це відображає той факт, що механізм LCFO вводить додаткове локальне обмеження виконання на рівні смарт-контракту: транзакції зі "застарілою" логічною міткою відхиляються, що зменшує допустимий простір фактичних порядків виконання, але водночас підвищує ризик відхилення за конкурентного доступу до одного і того самого ресурсу (AMM-пулу). Зазначений ефект наочно проілюстровано на рис. 2-5, де для одного зі запусків показано динаміку SR_b та SR_p за блоками, а також кумулятивні значення GB_b та GB_p – накопичення комісійних втрат користувачів на відхилених транзакціях.
3) *Показники винагороди агента-екстрактора у S_1 не використовуються як основний критерій.* Загальна винагорода агента в цьому сценарії демонструє значну варіативність між запусками, що є очікуваним наслідком випадкової політики: агент може епізодично виконувати прибуткові дії або, навпаки, зазнавати втрат, не оптимізуючи свою стратегію. Тому в межах S_1 винагорода агента розглядається тільки як додатковий контекст оцінювання якості симуляції, тоді як основний висновок сценарію полягає у кількісній фіксації накладних витрат застосування LCFO (зростання SR_p і GB_p) за фонових умов.

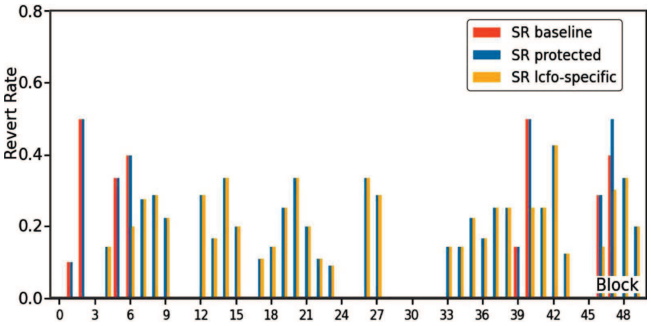

Рис. 2. Динаміка частки відхилених користувацьких swap-транзакцій без режиму LCFO / Dynamics of the rejected user swap transaction rate without LCFO

Частка відхилених користувацьких swap-транзакцій без режиму LCFO демонструє стійке зростання кількості операцій через збільшення затримок мережі та цінового проковзування (slippage). Режим LCFO (англ. *Lowest Cost Routing First Optimization*) або його аналоги у DeFi-протоколах дозволяють оптимізувати черговість та вартість транзакцій. Без цього режиму користувачі стикаються з критичними затримками оброблення операцій (рис. 2). Динаміка частки відхилених користувацьких swap-транзакцій у цьому режимі має чітку залежність від волатильності ринку, налаштувань проковзування (slippage) та завантаженості мережі (рис. 3).

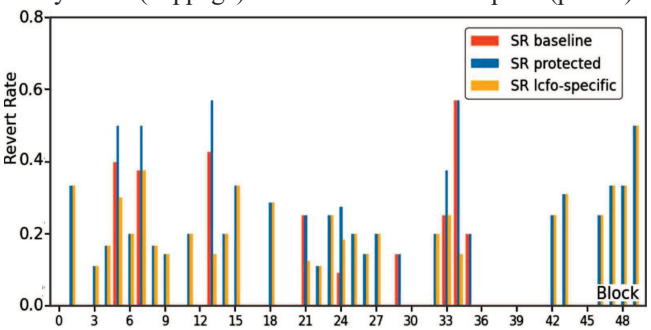

Рис. 3. Динаміка частки відхилених користувацьких swap-транзакцій у режимі LCFO / Dynamics of the rejected user swap transaction rate under LCFO

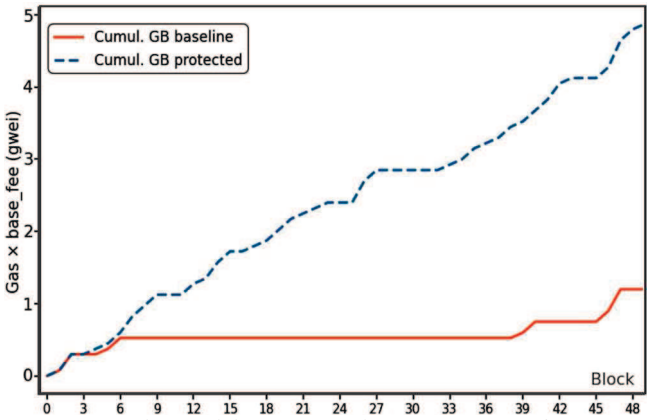

Рис. 4. Динаміка комісійних втрат без режиму LCFO / Dynamics of fee losses without LCFO

Термін LCFO у контексті виконання фінансових операцій, трейдингу або корпоративного управління найчастіше є специфічною абревіатурою (наприклад, локальною моделлю оптимізації витрат, системою автоматичного маршрутування ордерів або алгоритмом клірингу). За відсутності (вимкнення) такого режиму, динаміка комісійних втрат компанії чи інвестора зазнає негативних змін і характеризується декількома ключовими факторами:

- лінійне та прогресуюче зростання витрат – пряма залежність від обсягів транзакцій і відсутність оптових знижок;
- структурні чинники збільшення втрат – втрата транзакційного неттінгу (взаємозаліку) і каскадний ефект додаткових зборів;
- часова та ринкова динаміка – у періоди високої волатильності та кумулятивний ефект.

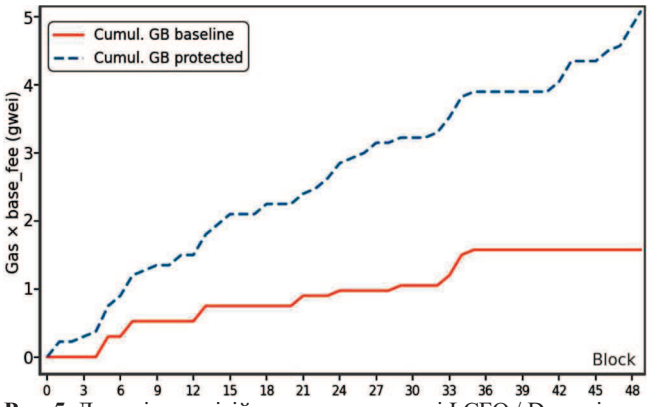

Рис. 5. Динаміка комісійних втрат у режимі LCFO / Dynamics of fee losses under LCFO

Загалом сценарій S_1 демонструє, що за відсутності систематичної атаки механізм LCFO не створює значного виграшу у показниках slippage-відхилення ціни обміну, однак формує помітну "вартість застосування" у вигляді додаткових відхилень транзакцій та комісійних втрат користувачів. Цей результат є базовою точкою порівняння для сценарію S_2, де оцінюється позитивний ефект від механізму LCFO, а також для сценарію S_3, у якому аналізується керований компроміс між ефективністю захисту та вартістю застосування механізму через параметр W.

У сценарії S_2 з MEV-атакою за наперед заданим сценарієм для всіх досліджуваних запусків симуляції зафіксовано стійкий захисний ефект механізму LCFO (*lcfo_enabled* = 1) щодо користувацьких swap-операцій обміну. Зокрема, різниця $\Delta = avg\_AS_b - avg\_AS_p$ є додатною для всіх значень seed у двох серіях з увімкненим та вимкненим LCFO-захистом, що означає зменшення медіанного значення користувацьких втрат від slippage-відхилення ціни, коли захист від MEV-атак активовано. За узгоджених параметрів моделювання (λ_{tx}=1,0; W = 16; *n_bloks* = 50) середнє значення Δ становить близько $1{,}6 \cdot 10^{-3}$ (у прийнятій шкалі AS), а спостережуваний діапазон Δ підтверджує відтворюваність ефекту за різних реалізацій епізоду. Водночас, застосування LCFO супроводжується зростанням частки відхилених користувацьких транзакцій у режимі MEV-захисту та істотним збільшенням агрегованих комісійних втрат на відхилених транзакціях *GB*, що інтерпретується як вартість застосування механізму. На рівні поведінки агента-екстрактора найпоказовішим є зниження частоти повного завершення sandwich-атак у серії MEV-захищених запусків: хоча транзакції випередження часто виконуються, закриття позиції (перехоплення) спрацьовує істотно рідше, ніж у базовій серії без MEV-захисту, що вказує на руйнування типової структури sandwich-атаки через обмеження, накладені механізмом LCFO на виконання конфліктних транзакцій. Сукупно результати S_2 (рис. 6 і 7) демонструють компроміс: зменшення цінових втрат користувачів досягається ціною підвищених відмов і комісійних витрат, а також зниженням "життєздатності" атаки.

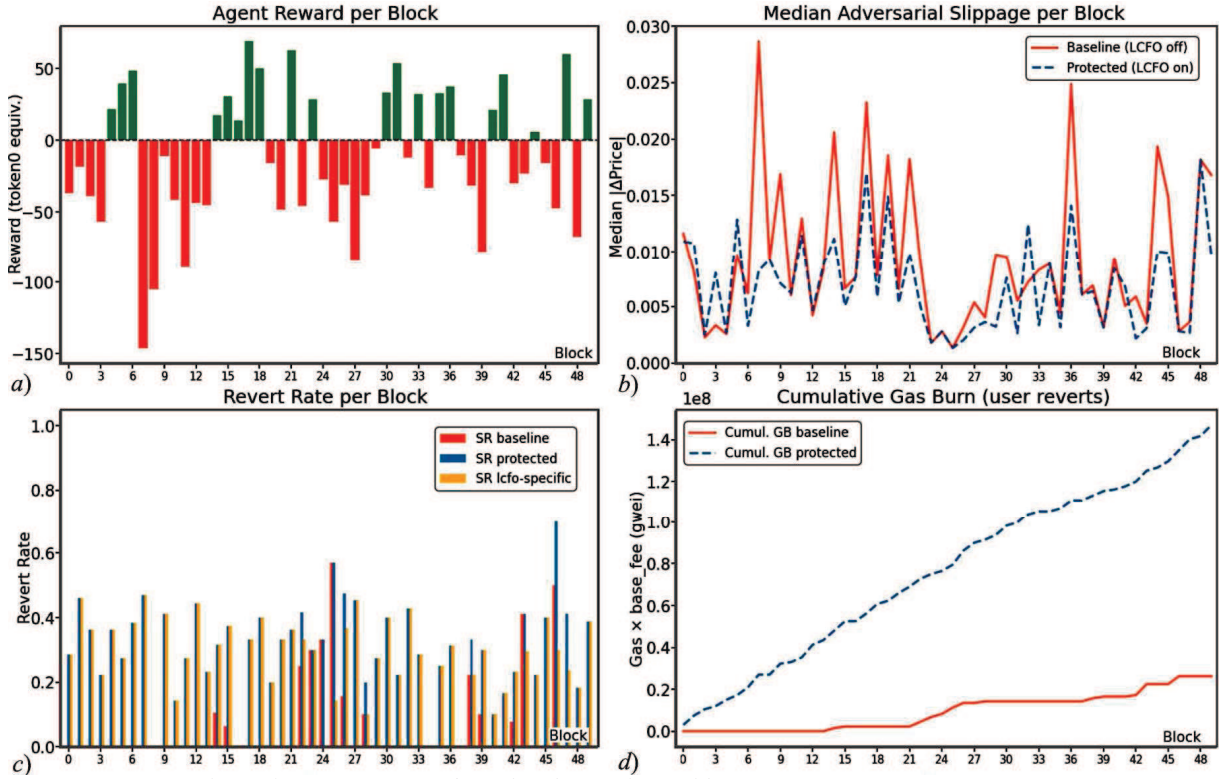

Рис. 6. Результати сценарію S_2 без режиму LCFO / Results of Scenario S_2 without LCFO

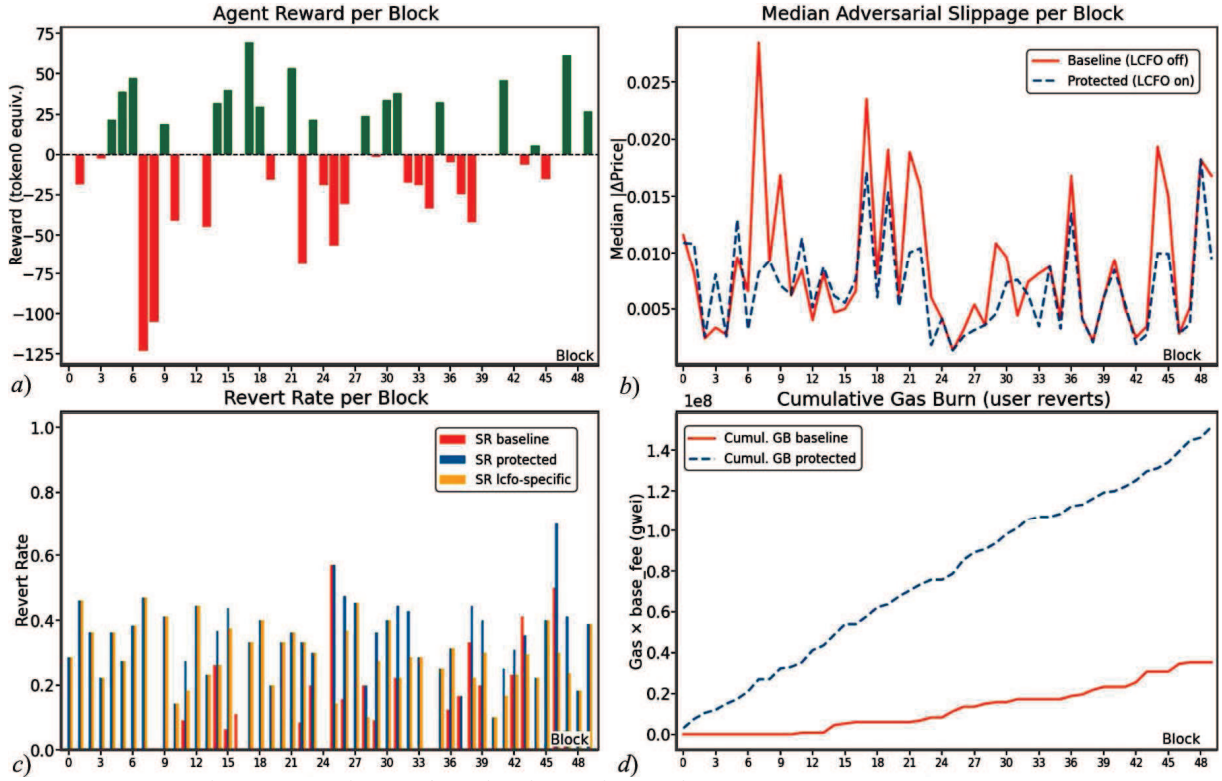

Рис. 7. Результати сценарію S_2 у режимі LCFO / Results of Scenario S_2 under LCFO

У сценарії S_3 досліджено керований компроміс ефективності механізму LCFO через параметр W = *lamport_window_W*, який задає ширину діапазону формування логічних міток *lamport_ts* під час створення транзакцій. За фіксованих умов атаки (атака за наперед заданим сценарієм, (λ_{tx}=1,0; n_{bloks} = 50) та 5 значень seed) порівнювалися два режими: коротке вікно з W = 4 та широке з W = 64. Оцінювання виконувалося на основі двох серій запуску з увімкненим та вимкненим режимом MEV-захисту LCFO, при цьому для інтерпретації компромісу ключовими є результати саме MEV-захищеної серії, оскільки саме вона визначає фактичні наслідки застосування механізму. Зведені показники наведено в табл. 2. За $W = 4$ спостерігається істотне зростання захисного ефекту: середнє $\bar{\Delta} = avg\_AS_b - avg\_AS_p$ становить 0,004306 (діапазон 0,002964 – 0,005144), що приблизно у 7-8 разів перевищує значення за W = 64 (0,000567; 0,000003 – 0,001145). Водночас, зростає "вартість застосування" механізму LCFO: частка відхилених користувацьких swap-транзакцій обміну підви-

щується до $\overline{SR_p} = 0{,}642$ (0,624 – 0,659), а агреговані комісійні втрати на відхилених транзакціях сягають до $\overline{GB_p} = 300{,}9\text{M}$ (284,25 – 315,0M), тоді як за $W = 64$ ці показники знижуються до 0,152 (0,101 – 0,209) та 70,8M (47,25 – 94,5M) відповідно. На рівні "життєздатності" sandwich-атаки коротке вікно також діє значно сильніше: середня кількість успішних транзакцій перехоплення (back-run) в MEV-захищеній серії зменшується до 8,4/50 (6–11) за $W = 4$ проти 42,6/50 (38 – 46) за $W = 64$.

Отже, робота компанії чи інвестора без режиму LCFO переводить систему на базові ринкові тарифи, позбавляє бізнес інструментів автоматичної мінімізації витрат та веде до неконтрольованого зростання операційних збитків пропорційно до масштабів діяльності.

Керований компроміс через параметр W найчастіше описує ситуацію, де вага або коефіцієнт W (англ. *Weight* або *Weighting Factor*) регулює баланс між двома протилежними цілями або характеристиками системи. Це широко використовується в математичній оптимізації, машинному навчанні та інженерії для пошуку оптимального рішення.

Табл. 2. Керований компроміс через параметр W / Controlled trade-off through the parameter W

W	$\overline{\Delta}(min-max)$	$\overline{SR_p}(min-max)$	$\overline{GB_p}(min-max)$	$\frac{\overline{back\_ok}}{50(min-max)}$
4	0,004306	0,642	300,9M	8,4
64	0,000567	0,152	70,8M	42,6

Візуально компроміс між виграшем Δ та вартістю (через SR_p і GB_p) відображено на рис. 8 і 9, що дає змогу інтерпретувати параметр W як засіб практичного налаштування механізму MEV-захисту LCFO залежно від допустимого рівня відхилень транзакцій та цільового зменшення MEV-впливу.

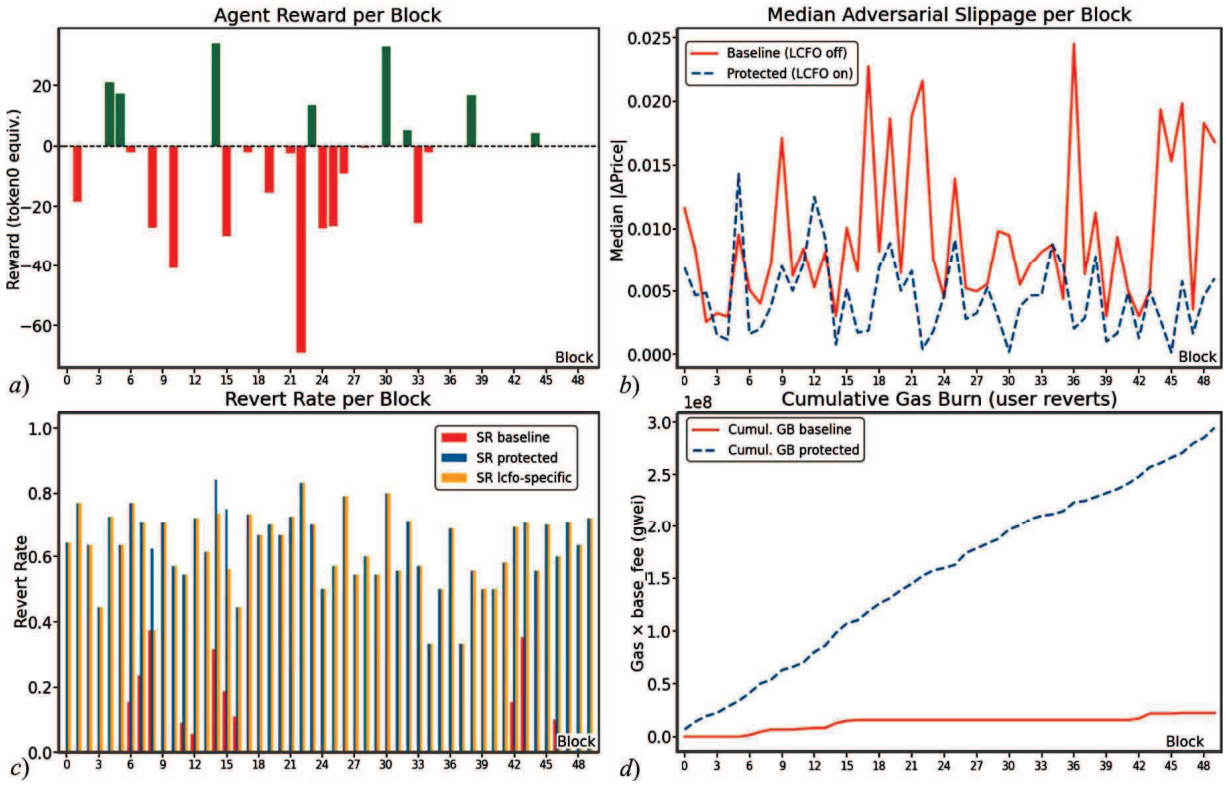

Рис. 8. Порівняння впливу параметра W=4 на результати моделювання / Comparison of the impact of parameter W = 4 on simulation results

На панелі slippage-відхилення (верхня права) зменшення W проявляється як помітніше відхилення між лініями в базовому та захищеному режимах, що відповідає більшому значенню $\Delta = avg\_AS_b - avg\_AS_p$. На панелі з показниками темпів відхилення транзакцій Revert Rate (нижня ліва) та втрат на gas-комісіях (нижня права) зменшення параметра W супроводжується зростанням SR_p і швидшим накопиченням GB_p, що відображає підвищення частоти відхилених транзакцій і вартості застосування механізму для користувачів. Отже, рисунок наочно підтверджує керований компроміс між ефективністю зменшення slippage-відхилення ціни та накладними витратами механізму MEV-захисту LCFO за зміни значення W.

Сукупно результати підтверджують, що механізм MEV-захисту LCFO може бути налаштований як практичний спосіб зменшення негативних наслідків MEV у межах одного смарт-контракту (у нашому випадку смарт-контракту AMM-пулу), однак його застосування потребує вибору параметрів з урахуванням допустимого рівня відхилень транзакцій і пов'язаних витрат. Отримані результати потрібно інтерпретувати з урахуванням обмежень синтетичних умов симуляції. По-перше, середовище відтворює спрощену економіку виконання: моделюється один AMM-пул типу constant-product, обмежений набір типів транзакцій та спрощена модель комісій, що не враховує повну семантику віртуальної машини EVM, ефекти змін стану поза AMM-пулом і різноманіття методів смарт-контракту. По-друге, генератор транзакцій задає потокові характеристики і параметри swap-транзакцій обміну у синтетичній формі, тому статистичні властивості сховища-мемпулу можуть відрізнятися від реальної мережі. По-третє, поведінка атакуючого агента задається наперед визначеною політикою, що репрезентує верхню межу тиску sandwich-атаки при MEV-екстракції, але не відображає стратегічної адаптації агента до режиму захисту та динаміки змін ставки комісій на транзакції.

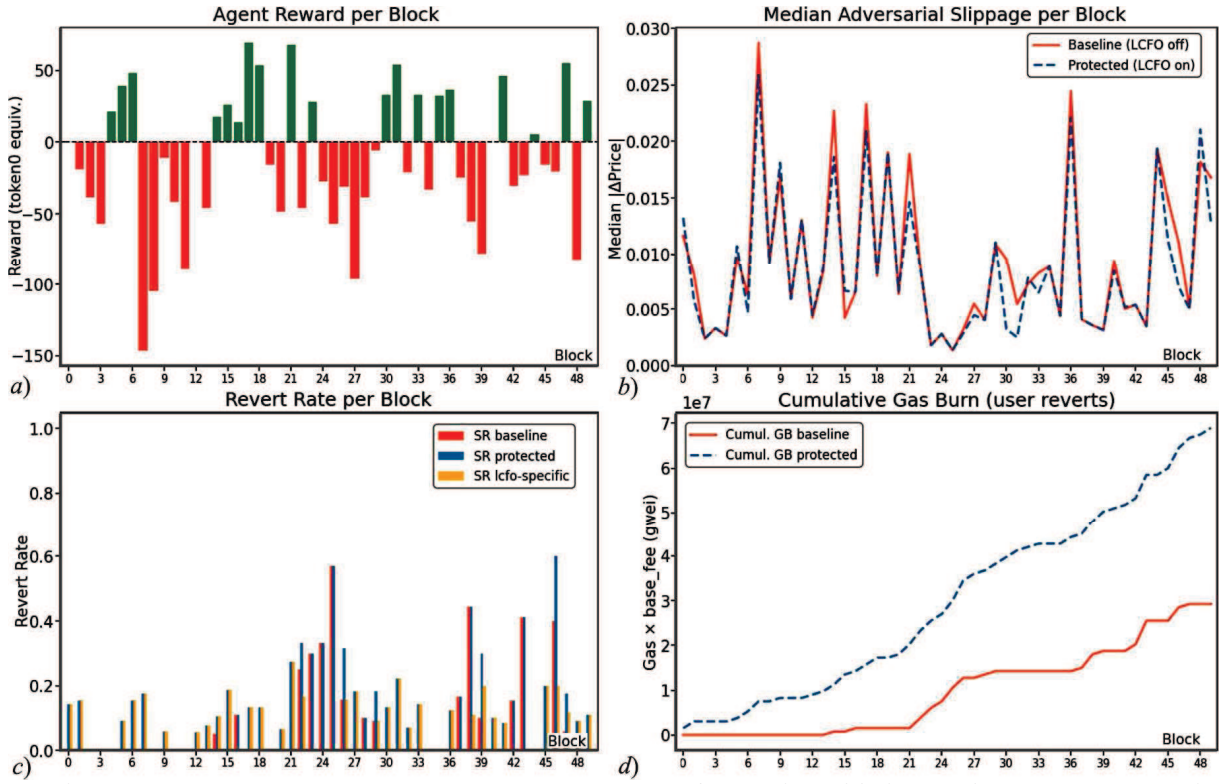

Рис. 9. Порівняння впливу параметра W = 64 на результати моделювання / Comparison of the impact of parameter W = 64 on simulation results

Порівняння впливу параметра W=64 (зазвичай означає ширину вікна, кількість нейронів, блоків або кроків затримки) на результати моделювання залежить від контексту конкретної задачі. На основі аналізу методів моделювання можна виділити такі ключові аспекти. Використання вищих значень лагів (наприклад, W=64 як ознака моделі 4-го рівня) впливає на динаміку продуктивності або економічних показників. Це дає змогу краще врахувати вплив попередніх періодів, але може вимагати більшої вибірки даних для уникнення перенавчання. Вище значення W забезпечує кращу деталізацію та точність моделювання складної поведінки економічної системи. Занадто велике значення може призвести до значного збільшення обчислювальної складності (витрат часу та ресурсів), особливо при імітаційному моделюванні. Для точного порівняння важливо знати, чи W позначає ширину вікна у часових рядах, розмір нейромережі чи параметр дискретизації.

Обговорення результатів дослідження. Порівняно із сучасними роботами на зразок [18], в яких пропонують рішення на основі навчання з підкріпленням у поєднанні з деревом пошуку Монте-Карло для активного пошуку прибуткових стратегій MEV-екстрактора, це дослідження зосереджене на використанні імітаційного моделювання передусім для аналізу процесів MEV-екстракції з погляду їх впливу на користувачів мережі блокчейн, а також розгортанні MEV-захищених методів впорядкування транзакцій [6], націлених на зменшення негативних ефектів від явища MEV.

В іншому дослідженні [16] представлено комплексне дослідження вразливостей блокчейн-мереж із застосуванням багатоагентного навчання з підкріпленням (MARL). Автори фокусуються на стратегічній взаємодії вузлів-майнерів для аналізу атак на рівні алгоритму консенсусу, що є безперечною перевагою в контексті моделювання ігрових рівноваг. Однак акцент дослідження зміщений у бік макроструктурних загроз безпеці мереж блокчейн, що залишає поза увагою мікрорівень впорядкування транзакцій у протоколах децентралізованих фінансів. Зокрема, у моделі не виділено явище MEV як окремий об'єкт симуляції та не розглянуто вплив послідовності операцій на прибуток чи втрати користувацьких транзакцій. Відсутність прикладних механізмів MEV-захищеного впорядкування, таких як, наприклад, логічні часові мітки, обмежує можливість нейтралізації економічних маніпуляцій у смарт-контрактах Ethereum.

У дослідженні [19] автори побудували модель на основі теорії ігор для аукціонів MEV-Boost і за допомогою симуляцій проаналізували стратегічну поведінку конструювальників блоків мережі Ethereum, зокрема вплив часових затримок, архітектури компонентів-ретрансляторів та природу ексклюзивного потоку транзакцій на результати участі в MEV-аукціонах. Сильною стороною цієї роботи є наближеність до сучасної схеми PBS-мережі Ethereum та якісний аналіз конкуренції на рівні конструювальників блоків. Разом із тим фокус моделювання тут зосереджений саме на поведінці за умов аукціону, а не на ширшій взаємодії сховища-мемпулу, користувацьких swap-транзакцій обміну криптоактивів, AMM-пулів децентралізованої біржі та локальних правил виконання в межах окремого смарт-контракту. Через це поза увагою залишаються користувацькі втрати від явища MEV та ефект захисних механізмів на рівні смарт-контракту.

Також варто згадати дослідження [2], в якому представлено BlockSim – розширений симулятор блокчейн-систем, орієнтований на моделювання мережевих, консенсусних і стимулятивних аспектів функціонування мереж блокчейн. Сильною стороною цієї роботи є модульність і придатність до дослідження широкого спектра системних характеристик мереж блокчейн. Водно-

час, використаний інструмент має загальносистемний характер і не спеціалізується на задачах, пов'язаних з децентралізованих фінансів та MEV-екстракції, як у випадку нашої роботи.

Іншим прикладом дослідження, де імітаційне моделювання використовується передусім для підвищення ефективності MEV-екстракції, є робота [12], де автори розглянули проблему ринкової маніпуляції в децентралізованих фінансах через призму багатоагентного навчання з підкріпленням (MARL), акцентуючи увагу на формуванні рівноваги стратегічного витіснення між основними агентами в середовищі DeFi-протоколів. Сильною стороною роботи є перенесення методів MARL до задач аналізу маніпулятивної поведінки та фокус на взаємодії кількох агентів у конкурентному середовищі, що дає змогу виявляти складні шаблони стратегічної адаптації. Натомість, дослідження, представлене в даній статті, зосереджене насамперед на дослідженні MEV-процесів безвідносно до ефективності MEV-екстракції та на аналізі негативного впливу на користувацькі транзакції за використання методів MEV-захищеного впорядкування.

Отже, внаслідок обговорення результатів дослідження можемо констатувати факт того, що наявні праці охоплюють переважно окремі аспекти проблеми: теоретико-ігрову формалізацію MEV, аукціонну поведінку конструювальників блоків, вплив часових затримок, загальносистемне симуляційне моделювання або використання методів навчання з підкріпленням для пошуку прибуткових стратегій MEV-екстракції. Разом із тим у проаналізованій літературі недостатньо представлені підходи, які одночасно поєднують імітаційне середовище, орієнтоване на сценарії протоколів децентралізованих фінансів, моделювання адаптивної поведінки агента MEV-екстрактора, контрфактичне оцінювання користувацьких втрат і дослідження прикладного MEV-захищеного методу впорядкування транзакцій. Це, водночас, вказує на доцільність проведеного саме нашого дослідження, яке має практичне значення отриманих результатів.

Отже, внаслідок виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – вперше розроблено структурну імітаційну модель середовища мережі блокчейн Ethereum за схемою Proposer-Builder-Separation (PBS), побудовану на основі агентно-орієнтованого моделювання поведінки MEV-екстракторів, формалізованих стратегій впорядкування транзакцій і механізму контрфактичного порівняння результатів виконання, що дає змогу досліджувати за контрольованих умов вплив правил формування блоків на обсяг MEV-екстракції та втрати користувачів.

Практична значущість результатів дослідження – можна використати для аналізу явища MEV ізольовано від реально працюючої розподіленої мережі блокчейн Ethereum, що скорочує цикл тестування, апробації та використання ресурсів під час дослідження процесу MEV-екстракції та методів зменшення його негативних ефектів.

Висновки / Conclusions

Розроблено підхід до імітаційного моделювання явища максимально екстрактованої вигоди (MEV) у мережі блокчейн Ethereum, який дав змогу дослідити поведінку MEV-екстракторів, оцінити користувацькі втрати та зменшити негативні ефекти від маніпуляцій порядком транзакцій у децентралізованих обчислювальних системах блокчейн. За результатами проведеного дослідження можна сформулювати такі основні висновки.

1. Обґрунтовано доцільність використання імітаційного моделювання для дослідження явища MEV у мережах блокчейн, оскільки підходи на основі теорії ігор та інші методи моделювання не повною мірою відображають стохастичний характер надходження транзакцій, часткову спостережуваність сховища-мемпулу та адаптивну поведінку автоматизованих агентів. Запропонована модель дає змогу відтворювати динаміку взаємодії між користувачами, агентами-екстракторами та механізмами впорядкування транзакцій у контрольованому середовищі, досліджувати прояви MEV та оцінювати його вплив на користувачів і мережі блокчейн, що створює основу для виявлення ключових джерел користувацьких втрат і визначення вимог до методів та засобів їх зменшення.
2. Розроблено середовище імітаційного моделювання на основі бібліотеки Gymnasium для роботи з методами навчання з підкріпленням, яке формалізує задачу дослідження MEV як процес взаємодії агента з частково спостережуваним середовищем. У межах цієї моделі реалізовано дискретно-часову організацію епізодів, що узгоджує надходження транзакцій, побудову блоків і виконання swap-операцій обміну криптоактивів у протоколі автоматизованого маркет-мейкера. Це створює основу для подальшого застосування методів навчання з підкріпленням до задач моделювання та аналізу процесів MEV-екстракції.
3. Здійснено розгортання та апробацію методу MEV-захищеного впорядкування транзакцій на основі логічних часових міток Лампорта, який реалізує локальне причинно-наслідкове впорядкування у межах окремого смарт-контракту. Проведені сценарні дослідження показали, що цей підхід здатний зменшувати цінові втрати користувачів від sandwich-атак, однак супроводжується зростанням частоти відхилення транзакцій і пов'язаних комісійних витрат. Отже, застосування захищеного впорядкування має характер керованого компромісу між рівнем захисту та накладними витратами його використання.
4. Проведені обчислювальні експерименти підтвердили практичну придатність запропонованого середовища для дослідження явища MEV та аналізу впливу політик впорядкування на MEV-екстракцію та втрати користувачів. Отримані результати демонструють, що зміна параметрів механізму захищеного впорядкування безпосередньо впливає на баланс між зменшенням негативних ефектів MEV та додатковими витратами, що створює основу для подальшого пошуку оптимальних конфігурацій таких механізмів.

Перспективи подальших етапів дослідження полягають у розширенні симуляційного середовища шляхом інтеграції з інструментами локального виконання смарт-контрактів на зразок Hardhat [10], врахування складніших сценаріїв використання DeFi-протоколів та застосування повноцінного тренування агента на основі методів навчання з підкріпленням для моделювання адаптивної, а не тільки заданої наперед поведінки агента MEV-екстрактора.

References

1. Adams, A., Chan, B. Y., Markovich, S., & Wan, X. (2024). Dont let MEV slip: The costs of swapping on the Uniswap protocol. *Financial Cryptography and Data Security: 28th International Conference* (pp. 172-191). https://doi.org/10.48550/arXiv.2309.13648

2. Alharby, M., & van Moorsel, A. (2020). BlockSim: An extensible simulation tool for blockchain systems. *Frontiers in Blockchain*, 3, article ID 28. https://doi.org/10.3389/fbloc.2020.00028
3. Bartoletti, M., & Zunino, R. (2023). A theoretical basis for Blockchain Extractable Value. arXiv. https://doi.org/10.48550/arXiv.2302.02154
4. Bellman, R. (1957). A Markovian decision process. *Journal of Mathematics and Mechanics*, *6*(5), 679–684. https://doi.org/10.1512/iumj.1957.6.56038
5. Cherkas, N. S., & Batyuk, A. Ye. (2023). Maximal extractable value (MEV) in blockchain networks and its impact on blockchain ecosystem. *Ukrainian Journal of Information Technology*, 5(2), 60–71. https://doi.org/10.23939/ujit2023.02.060
6. Cherkas, N., & Batyuk, A. (2025). Transaction ordering via Lamport logical timestamps to mitigate MEV extraction in Ethereum smart contracts. *Herald of Khmelnytskyi National University. Technical Sciences*, 357(5.2), 187–192. https://doi.org/10.31891/2307-5732-2025-357-83
7. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2020). Flash Boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. *In 2020 IEEE Symposium on Security and Privacy* (*SP*) (pp. 910–927). IEEE. https://doi.org/10.1109/SP40000.2020.00040
8. Ethereum.org. (n.d.). Proposer-builder separation. Retrieved March 17, article ID 2026. URL: https://ethereum.org/en/roadmap/pbs/
9. Farama Foundation. (n.d.). Gymnasium documentation. Retrieved March 9, 2026. URL: https://gymnasium.farama.org/
10. Hardhat. (2026, February). Hardhat 3: Rust-powered Solidity tests. Ethereum development environment for professionals. URL: https://hardhat.org/
11. Huang, R. (2025). Research on optimization of cryptocurrency trading strategies based on reinforcement learning: Combining traditional machine learning and deep reinforcement learning methods. *ITM Web of Conferences*, 78, article ID 01001. https://doi.org/10.1051/itmconf/20257801001
12. Jain, S. (2026). Algorithmic predatory equilibrium: Multi-agent reinforcement learning and market manipulation in decentralized finance [Preprint]. SSRN. 27 p. https://doi.org/10.2139/ssrn.6087766
13. Liu, Y., Lu, Y., Nayak, K., Zhang, F., Zhang, L., & Zhao, Y. (2022). Empirical analysis of EIP-1559: Transaction fees, waiting times, and consensus security. *In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2099–2113). https://doi.org/10.1145/3548606.3559341
14. Mazorra, B., Reynolds, M., & Daza, V. (2022). Price of MEV: Towards a game theoretical approach to MEV. *In Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (pp. 11–18). https://doi.org/10.1145/3560832.3563433
15. Nisan, N., Roughgarden, T., Tardos, E., & Vazirani, V. V., (Eds.). (2007). *Algorithmic Game Theory*. Cambridge University Press, 754 p. https://doi.org/10.1017/CBO9780511800481
16. Roussille, H. (2024). A case study on blockchain vulnerabilities using Multi-Agent Reinforcement Learning. Cryptography and Security [cs. CR]. *Doctoral dissertation, Université de Montpellier*. HAL. 138 p. URL: https://theses.hal.science/tel-05101983
17. Schwarz-Schilling, C., Saleh, F., Thiery, T., Pan, J., Shah, N., & Monnot, B. (2023). Time is money: Strategic timing games in Proof-of-Stake protocols. arXiv. https://doi.org/10.48550/arXiv.2305.09032
18. Wen, E., Deng, Z., Mo, Y., Zhou, Y., & Shi, X. (2025). RL-BES: Optimizing strategies using reinforcement learning for blockchain economic security. *Blockchain,* 2025(1), article ID 0005. https://doi.org/10.55092/blockchain20250005
19. Wu, F., Thiery, T., Leonardos, S., & Ventre, C. (2024). Strategic bidding wars in on-chain auctions. *In 2024 IEEE International Conference on Blockchain and Cryptocurrency* (*ICBC*) (pp. 503–511). IEEE. https://doi.org/10.1109/ICBC59979.2024.10634354
20. Xu, J., Paruch, K., Cousaert, S., & Feng, Y. (2023). SoK: Decentralized exchanges (DEX) with automated market maker (AMM) protocols. *ACM Computing Surveys 55*(11), 1-50. https://doi.org/10.1145/3570639

N. S. Cherkas, A. Ye. Batiuk

Lviv Polytechnic National University, Lviv, Ukraine

SIMULATION MODELING OF THE MAXIMAL EXTRACTABLE VALUE IN ETHEREUM BLOCKCHAIN NETWORK

Proposed a simulation environment for modeling the phenomenon of Maximal Extractable Value (MEV) with implementation in the Python programming language using the Gymnasium library. The environment reproduces the interaction between the mempool, the block builder, the MEV extractor agent, and the automated market maker (AMM) pool of a decentralized exchange. Formally, the environment is described as an extended partially observable decision-making process in which the agent interacts with a discrete-time episodic model reflecting the sequence of transaction arrivals, block construction, and the execution of swap operations on a decentralized cryptocurrency exchange. Reinforcement learning methods are used to model the adaptive behavior of the agent, while a counterfactual evaluation approach is applied to quantitatively analyze user losses by comparing transaction execution outcomes under different ordering regimes while keeping the input conditions unchanged. The study employs a previously proposed method for mitigating the negative effects of MEV extraction based on Lamport logical timestamps. This method implements local causal transaction ordering within an individual smart contract without modifying the global consensus mechanism of the Ethereum blockchain network. To assess the practical effectiveness of this approach, three simulation scenarios are defined: a baseline scenario without systematic MEV attacks to estimate the overhead associated with the protection mechanism, a systematic sandwich-attack scenario to analyze the methods ability to reduce user losses and constrain the capabilities of the MEV extractor, and a parametric analysis scenario aimed at investigating the trade-off between the level of protection and the "cost" of its application. The obtained results show that the proposed MEV-protected ordering method can reduce user price losses caused by sandwich attacks while also affecting transaction rejection rates and the associated fee expenditures, indicating the presence of a controllable trade-off between protection effectiveness and the overhead of its use. The practical value of the work lies in the creation of a reproducible simulation environment for studying the strategic behavior of MEV agents and evaluating mechanisms for mitigating the negative effects of MEV under controlled conditions. Such an environment can be used for further security analysis of decentralized finance protocols and for the design of new transaction ordering methods.

Keywords: reinforcement learning; decentralized systems; computer networks; information systems; cryptography; cryptocurrencies; information technology; digital economy.